Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής
Πρόγραμμα Μεταπτυχιακών Σπουδών
«Προηγμένα Συστήματα Πληροφορικής»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**Enterprise Mobility: Applications and security strategies** **Επιχειρησιακή Φορητότητα : Εφαρμογές και στρατηγικές ασφάλειας**
Ονοματεπώνυμο Φοιτητή	**Μακρίδου Ανατολή**
Πατρώνυμο	**Γεώργιος**
Αριθμός Μητρώου	**ΜΠΣΠ/ 14050**
Επιβλέπων	**Δουληγέρης Χρήστος , Καθηγητής**

Ημερομηνία Παράδοσης **Οκτώβριος 2018**

Τριμελής Εξεταστική Επιτροπή

(υπογραφή)	(υπογραφή)	(υπογραφή)
Χρήστος Δουληγέρης	Παναγιώτης Κοτζανικολάου	Ευαγγελία Κοπανάκη
Καθηγητής	Επίκουρος Καθηγητής	Επίκουρη Καθηγήτρια

Περίληψη

Η παρακάτω έρευνα έχει ως στόχο την παρουσίαση του enterprise mobility ως μια αυξανόμενη τάση στον επιχειρηματικό κόσμο. Ο λόγος που με ώθησε να ασχοληθώ με το με το enterprise mobility είναι η συνεχώς αυξανόμενη τάση των εταιρειών προς το enterprise mobility με στόχο τον εκσυγχρονισμό, την αποδοτικότερη χρήση των δεδομένων τους, καθώς και την παροχή στους εργαζομένους ευέλικτου τρόπου εργασίας μέσω κινητών συσκευών. Ο βασικότερος μου στόχος είναι να αποδείξω με την εκπόνηση της έρευνάς μου πως τα πλεονεκτήματα που παρέχει η υιοθέτηση κάποια μορφής enterprise mobility είναι πολύ περισσότερα και σημαντικότερα από τα προβλήματα και τα τρωτά σημεία που αναπόφευκτα προκύπτουν. Έχοντας δυστυχώς υπάρξει παρατηρητής φαινομένων κωλυσιεργίας από πλευράς των εταιριών να εκσυγχρονίσουν τον τρόπο που δουλεύουν εισάγοντας κάποια μορφή enterprise mobility, επικαλούμενοι τα προβλήματα ασφάλειας, αποτελεί στόχος μου να καταλήξω πως με την εξέλιξη της τεχνολογίας και την εφαρμογή κατάλληλης στρατηγικής τα προβλήματα που τυχόν παρουσιαστούν είναι δυνατόν να εξαλειφθούν εντελώς.

Abstract

The following research aims to present enterprise mobility as a growing trend in the business world. The reason that has driven me to deal with enterprise mobility is the growing trend of companies towards enterprise mobility with the aim of streamlining, more efficient use of their data, and providing employees flexible mobile workstations. The main objective of this research was to show that the advantages of adopting a form of enterprise mobility are much more important than the problems and vulnerabilities that inevitably arise. Unfortunately, as I observed companies are often hesitant to improve their working practices by introducing a form of enterprise mobility, mainly due to security problems. However, as this research suggests with the development of technology and the implementation of an appropriate strategy the problems that may arise are likely to be completely eliminated.

Περιεχόμενα

Κεφάλαιο 1ο Εισαγωγή

1.1 Περιοχή και στόχος έρευνας

Η παρούσα έρευνα έχει ως στόχο την παρουσίαση τεσσάρων βασικών πυλώνων του enterprise mobility.

Το enterprise mobility είναι ένας τρόπος απομακρυσμένης εργασίας στην οποία οι εργαζόμενοι μπορούν να δουλεύουν από οπουδήποτε χρησιμοποιώντας μια ποικιλία συσκευών και εφαρμογών. Οι ειδικοί ορίζουν το enterprise mobility όχι μόνο ως προς την ικανότητα των εργαζομένων να εργάζονται εκτός ενός γραφείου αλλά και ως προς την μετάδοση των εταιρικών δεδομένων μέσω τεχνολογικών δικτύων.

Με τον όρο enterprise mobility εννοούμε συνήθως τη δημιουργία απομακρυσμένων πλατφορμών εργασίας, όπου οι εργαζόμενοι ολοκληρώνουν τα επαγγελματικά τους καθήκοντα αποστέλλοντας δεδομένα από το ένα μέρος στο άλλο, μέσω διαδικτύου. Με την εμφάνιση τεχνολογιών κινητής τηλεφωνίας και άλλες νέες προόδους τα τελευταία 20 χρόνια, αυτή η μορφή κινητικότητας των επιχειρήσεων έχει αποκτήσει μεγάλο μερίδιο αγοράς και έχει υιοθετηθεί από πολλές εταιρίες παγκοσμίως

Έχει επίσης δημιουργήσει μια ολόκληρη σειρά εργαλείων και πόρων για τη διαχείριση αυτής της τάσης, γνωστή ως εργαλεία διαχείρισης της κινητικότητας των επιχειρήσεων.

Οι βασικές περιοχές στις οποίες κινείται η εργασία και αναλύονται εκτενώς στα παρακάτω κεφάλαια είναι

- **ERP συστήματα**, on premises και cloud.
- **Enterprise mobility**, ορισμός, εξέλιξη, πλεονεκτήματα και τρωτά σημεια.
- **Ανάλυση προβλημάτων ασφάλειας Enterprise mobility** και στρατηγικές αντιμετώπισης.
- **Enterprise Mobility Management** τεχνικές λύσεις αντιμετώπισης προβλημάτων ασφάλειας και προτάσεις λύσεων.

Ο στόχος της παρούσας έρευνας είναι να αναλύσει τα cloud συστήματα και την εφαρμογή τους στις επιχειρήσεις αρχικά από το erp και εν τέλει μέσω ολοκληρωμένης πλατφόρμας enterprise mobility βοηθώντας έτσι στην ευελιξία της εταιρείας η οποία έχει άμεση συνέπεια την βελτίωση της απόδοσης των εργαζομένων.

Στην παρούσα έρευνα είχα ως στόχο να δώσω πλήρη εικόνα της σύγχρονης τάσης προς το enterprise mobility το οποίο ξεκίνησε από το cloud πληροφοριακό σύστημα το οποίο έδωσε την δυνατότητα γρήγορης και άμεσης επεξεργασίας δεδομένων αποθηκευμένων σε cloud συστήματα και κατέληξε πλέον να παρέχει προσβασιμότητα και δυνατότητα εργασίας από οποιοδήποτε μέρος μέσω κινητών συσκευών. Προφανώς το enterprise mobility έχει τρωτά σημεία και προβλήματα τα οποία εντοπίζονται κυρίως στο θέμα της ασφάλειας πληροφοριών και του κινδυνου διαρροής σημαντικών εταιρικών δεδομένων τα οποία είτε είναι απόρρητα είτε αποτελούν περιουσιακά στοιχεία της εταιρίας.

Ως εκ τούτου, αφού παρουσιάσω και αναλύσω τα ενδεχόμενα προβλήματα που είναι πιθανό να προκύψουν σύμφωνα με την έρευνα, παραθέτω τους πιο διαδεδομένους τρόπους αντιμετώπισης τόσο σε επίπεδο στρατηγικής όσο και σε τεχνολογικό επίπεδο.

1.2 Τρόπος διεξαγωγής έρευνας και τελικό συμπέρασμα

Στην παρούσα έρευνα επικαλέστηκα ερευνητικά άρθρα και διατριβές τα οποία προέρχονται από πανεπιστήμια και σχολές κυρίως με κατεύθυνση κυρίως πληροφορικής (computer science), ασφάλειας πληροφοριών (information security) καθώς και διοίκησης επιχειρήσεων (business administration).

Στην πορεία της έρευνάς μου διαπίστωσα πως το enterprise mobility είναι ευρέως διαδεδομένο ερευνητικό θέμα καθώς επίσης μεγάλη έκπληξη μου προκάλεσε το γεγονός πως αποτελεί αντικείμενο έρευνας από το 1996.

Παράλληλα, στόχος μου ήταν να επικαλεστώ, πέρα από τις πανεπιστημιακές πηγές, επιστημονικά και εμπορικά περιοδικά και site όπως το Forbes καθώς επίσεις και αποτελέσματα ερευνών συμβουλευτικών και τεχνολογικών εταιρειών όπως Gartner και Cisco.

Ο λόγος για τον οποίο επέλεξα να συνδυάσω τις παραπάνω πηγές ερευνών είναι κυρίως για να δείξω πως η πανεπιστημιακή έρευνα εφαρμόζεται πρακτικά στον τεχνολογικό και επιχειρηματικό πραγματικό περιβάλλον καθώς επίσης διότι θεωρώ πως ο συνδυασμός τέτοιων ερευνητικών πηγών παρέχει πιο αξιόπιστα αποτελέσματα και βοηθάει στην διεξαγωγή ρεαλιστικών και εφαρμόσιμων συμπερασμάτων.

Συνοπτικά τα συμπεράσματα της παρούσας έρευνας είναι ότι πλέον πολλές επιχειρήσεις ανεξάρτητα από το μέγεθός τους υιοθετούν κάποιο είδος enterprise mobility αποσκοπώντας στον εκσυγχρονισμό και στην βελτίωση των παρεχόμενων υπηρεσιών προς του πελάτες αλλά και την διευκόλυνση της εργασίας των εργαζομένων. Το enterprise mobility αποτελεί πλέον μια σύγχρονη τάση η οποία μέσω της τεχνολογικής εξέλιξης στον τομέα των δικτύων, των βάσεων δεδομένων καθώς και των φορητών συσκευών (κινητά, tablet) δίνει στις εταιρίες την δυνατότητα να παρέχουν ευελιξία στους εργαζόμενους μέσω πλατφορμών BYOD (Bring Your Own Device).

Φυσικά όπως ανέφερα και παραπάνω, υπάρχουν κίνδυνοι ασφάλειας δεδομένων οι οποίοι αντιμετωπίζονται μέσω στρατηγικών και πολιτικών της εταιρείας καθώς και με τεχνολογικά μέσα όπως είναι οι πλατφόρμες διαχείρισης enterprise mobility (EMM, Enterprise mobility management). Ως τελικό συμπέρασμα θα μπορούσα να πω πως τα προβλήματα ασφάλειας του enterprise mobility έχουν περιοριστεί σε τέτοιο βαθμό που πλέον δεν αποτελεί περιορισμό για τις εταιρίες που θέλουν να υιοθετήσουν κάποιο σύστημα enterprise mobility.

1.3 Περιεχόμενα Διατριβής

Στα παρακάτω κεφάλαια γίνεται εκτενής ανάλυση των τεσσάρων βασικών πυλώνων του enterprise mobility.

Πιο συγκεκριμένα, στο **δεύτερο κεφάλαιο** γίνεται η παρουσίαση των διαφόρων μορφών των erp συστημάτων από την αρχή της εμφάνισής τους στην αγορά μέχρι σήμερα. Γίνεται σύγκριση των on-premises και cloud erp συστημάτων σχετικά με την αποτελεσματικότητά τους αλλά και τα κενά ασφαλείας που έχει η κάθε μέθοδος.

Στο **τρίτο κεφάλαιο** γίνεται μια παρουσίαση του entreprise mobility, παραθέτοντας τα πλεονεκτήματα της συγκεκριμένης μεθόδου, τους τρόπους που βοηθάει την εταιρεία να αυξήσει την αποδοτικότητα της αλλά και την απόδοση των υπαλλήλων.

Στο **τέταρτο κεφάλαιο** γίνεται η παρουσίαση και ανάλυση των προβλημάτων ασφαλείας τα οποία είναι και τα βασικότερα που απασχολούν τις επιχειρήσεις και αποτελούν τον κύριο ανασταλτικό παράγοντα σχετικά με την υιοθέτηση κάποιας μεθόδου enterprise mobility.

Τέλος στο **τελευταίο κεφάλαιο** παραθέτω τους τεχνικούς τρόπου αντιμετώπισης των προβλημάτων ασφάλειας καθώς και παραδείγματα λογισμικών EMM που έχουν υιοθετηθεί από εταιρείες ώστε να γίνεται ασφαλής χρήση πλατφορμών enterprise mobility.

Κεφάλαιο 2ο Enterprise Resource Planning

2.1 ERP (Enterprise Resource Planning)

Τα συστήματα ενδοεπιχειρησιακού σχεδιασμού (enterprise resource planning, ERP) ενσωματώνουν εσωτερικές και εξωτερικές πληροφορίες διαχείρισης σε έναν ολόκληρο οργανισμό συνδυάζοντας χρηματοδότηση/λογιστική, κατασκευή, πωλήσεις και υπηρεσίες, διαχείριση πελατειακών σχέσεων κτλ. Τα συστήματα ERP αυτοματοποιούν αυτές τις δραστηριότητες με μια εφαρμογή λογισμικού.

Ο σκοπός τους είναι να διευκολύνουν τη ροή των πληροφοριών μεταξύ όλων των επιχειρησιακών λειτουργιών μέσα στα όρια της οργάνωσης και να καταφέρουν τις συνδέσεις προς τα έξω με τα ενδιαφερόμενα μέρη.

Τα συστήματα ERP μπορούν να εκτελεστούν σε μια ποικιλία υλικού και διαμορφώσεις δικτύου που απασχολούν συνήθως μια βάση δεδομένων ως αποθήκη για πληροφορίες.

(Ορισμός wikipedia)

Πλεονεκτήματα ERP συστημάτων:

Τα ERP συστήματα μπορούν να βοηθήσουν μια επιχείρηση να:

- Αυξήσει τα έσοδά της
- Βελτιώσει την αποτελεσματικότητά της, ενοποιώντας διάφορες εργασίες (Finance & Accounting, Manufacturing, Supply Chain, Customer Relationship Management, Human Resources, BI/Reporting)
- Αυξήσει την παραγωγικότητα των ανθρώπων της, αυτοματοποιώντας τις διαδικασίες της
- Μειώσει τα λειτουργικά της έξοδα
- Αυξήσει την ασφάλεια των επιχειρησιακών της δεδομένων
- Αντλήσει και να αξιοποιήσει πληροφορίες από διαφορετικά τμήματα της εταιρείας

Στην ουσία ένα σύστημα ERP, αποτελείται από επιμέρους ενσωματωμένες εφαρμογές (modules), τις οποίες η επιχείρηση αξιοποιεί για να συγκεντρώνει, να αποθηκεύει, να διαχειρίζεται και τελικά να ερμηνεύει δεδομένα για πολλές (ιδανικά όλες) από τις δραστηριότητές της. Μερικά από τα modules ενός συστήματος ERP είναι:

- Εμπορική Διαχείριση
- Οικονομική Διαχείριση
- Έσοδα-Έξοδα
- Γενική Λογιστική
- Διαχείριση Παγίων

- Διαχείριση Αποθήκης
- Διαχείριση Ανθρώπινων Πόρων (HRM)
- Μισθοδοσία
- Διαχείριση Διανομής
- Διαχείριση Εφοδιαστικής Αλυσίδας
- Διαχείριση Πελατειακών Σχέσεων (CRM)
- Διαχείριση Λιανικής
- Προϊοντικός Σχεδιασμός
- Διαχείριση Παραγωγής
- Διαχείριση Υπηρεσιών
- Χρηματοοικονομική Λογιστική
- Πωλήσεις
- Marketing
- Τιμολόγηση

2.1.1 Παραδοσιακό ERP σύστημα

Πρόκειται για ένα είδος λογισμικού το οποίο επιτελεί όλες τις απαιτούμενες λειτουργίες και είναι εγκατεστημένο στους servers και στις υπολογιστικές μονάδες της εταιρίας. Με αυτό τον τρόπο, όλα τα δεδομένα (βάση δεδομένων) καθώς και το απαιτούμενο λογισμικό για την επεξεργασία και προβολή τους βρίσκονται στην εταιρία (on-premise).

Η επιχείρηση ελέγχει όλη την υποδομή και τις πλατφόρμες που χρησιμοποιούν οι υπάλληλοι. Επιπλέον, η εταιρεία αναλαμβάνει τη συντήρηση του λογισμικού, των servers, της βάσης δεδομένων, το κόστος για την αγορά και τον χώρο που χρειάζεται η υποδομή, καθώς και το κόστος μιας ενδεχόμενης ανάκτησης των δεδομένων από ολική η μερική καταστροφή (recovery cost). Συνεπώς, το κόστος του παραδοσιακού ERP συστήματος έγκειται κυρίως σε τρία βασικά σημεία

- Κόστος για την αγορά, τον χώρο και την συντήρηση της υποδομής (βάση δεδομένων, server, λειτουργικά συστήματα)
- Κόστος εργαζομένων του τμήματος μηχανοργάνωσης της εταιρίας οι οποίοι απασχολούνται αποκλειστικά με την εγκατάσταση και συντήρηση του ERP συστήματος.
- Recovery Cost.

Από τα παραπάνω μπορεί εύκολα να βγει το συμπέρασμα πως πρόκειται για μια υλοποίηση μεγάλου κόστους για μια εταιρία. Παρόλα αυτά αρκετές εταιρίες καταφεύγουν σε on-premise ERP σύστημα λόγω της ασφάλειας των δεδομένων της εταιρίας που παρέχεται από μια τέτοια υλοποίηση. Επιπλέον, μεγάλο ρόλο παίζει και η κουλτούρα της εκάστοτε εταιρίας η οποία επιλέγει να διατηρεί ένα τέτοιο ERP σύστημα κυρίως λόγω συνήθειας παρά το μεγάλο κόστος.

2.1.2 Cloud ERP

Ο μεγάλος όγκος δεδομένων καθώς και οι αυξημένες ανάγκες των επιχειρήσεων έχουν οδηγήσει στην ανάγκη ERP συστημάτων με μικρότερο κόστος, μεγαλύτερο φάσμα χρήσης και περισσότερη ευελιξία.

Ένα τέτοιο σύστημα, που κερδίζει όλο και περισσότερο έδαφος, είναι το ERP στο Cloud, ή όπως αλλιώς ονομάζεται, το SaaS ERP (Software as a Service ERP).

Το cloud ERP αντιμετωπίζει πολλές από τις προκλήσεις που συνδέονται με μεγάλες εγκαταστάσεις ERP. Πρακτικά, το Cloud ERP (ή εναλλακτικά, Cloud-based ERP) αξιοποιεί τις δυνατότητες που προσφέρει το διαδίκτυο αναφορικά με τη διαχείριση πόρων και την αποθήκευση δεδομένων, επιτρέποντας την εκτέλεση όλων των εργασιών διαχείρισης της επιχείρησης στο Cloud. Ένα Cloud ERP μπορεί να λειτουργήσει σε ελάχιστο χρόνο, διότι δεν εγκαθίσταται καθόλου λογισμικό στους servers της εταιρείας (όπως συμβαίνει στην on-premise εγκατάσταση). Επιπλέον, αναβαθμίζεται πολύ πιο γρήγορα και η εταιρία λειτουργεί σε κάθε περίπτωση πάντα την τελευταία έκδοση και η πρόσβαση στα εταιρικά δεδομένα γίνεται από παντού και με οποιαδήποτε συσκευή.

Τα πλεονεκτήματα του Cloud ERP

Το Cloud ERP συμβάλλει στη μείωση του κόστους λειτουργίας της μηχανογράφησης της επιχείρησης.

- Δεν απαιτεί υψηλές επενδύσεις σε υποδομές όπως hardware και data servers.
- Απαλλάσσει τα στελέχη του τμήματος μηχανοργάνωσης από πολύπλοκες, χρονοβόρες και δαπανηρές εργασίες υποστήριξης του συστήματος (αναβάθμιση, δημιουργία αντιγράφων ασφαλείας κ.λπ.), επιτρέποντας την αποδοτικότερη αξιοποίησή τους

Ωστόσο, τα πλεονεκτήματα του Cloud ERP είναι ακόμη περισσότερα και εκτείνονται πέραν της εξοικονόμησης στη λειτουργία της μηχανογράφησης

- Πρόσβαση και χρήση από οπουδήποτε, αφού το λογισμικό τρέχει στο Cloud και δεν απαιτεί εγκατάσταση συστημάτων σε απομακρυσμένες τοποθεσίες
- Πρόσβαση σε μεγάλο όγκο δεδομένων καθώς τα δεδομένα δεν είναι αποθηκευμένα σε τοπικούς servers, αλλά σε data centers.
- Ταχεία και εύκολη υλοποίηση, χωρίς προηγούμενη εγκατάσταση hardware και software σε servers της επιχείρησης
- Ευέλικτη διαμόρφωση, καθώς η εγκατάσταση μπορεί να προσαρμόζεται κάθε φορά σύμφωνα με τις ανάγκες της εκάστοτε επιχείρησης
- Ευέλικτη διαχείριση χρηματικών πόρων, αφού μία cloud υλοποίηση επιτρέπει την κλιμάκωση των εξόδων βάσει της εξέλιξης των απαιτούμενων κάθε φορά μηχανογραφικών πόρων

2.2 Σύγκριση In-premises ERP με Cloud ERP

Θεωρώντας ως δεδομένο πως χρονικά βρισκόμαστε σε σημείο καμπής σχετικά με τη μετάβαση των από το In-premises ERP στο Cloud ERP θα ήταν σκόπιμο να γίνει μια σύγκριση αυτών των δύο συστημάτων σε διάφορους τομείς που απασχολούν τον επιχειρηματικό τομέα

2.2.1 Πλεονεκτήματα Cloud ERP σε σχέση με In-premises ERP

Κόστος αγοράς

Η Cloud τεχνολογία εκ των πραγμάτων μειώνει το κόστος της αγοράς του συστήματος ERP σε σχέση με την αγορά και εγκατάσταση ενός In-premises ERP (Marston et al. 2010) συνυπολογίζοντας και τα έξοδα για την αγορά φυσικών πόρων (hardware), καθώς και άδειας

χρήσης για τον κάθε εργαζόμενο χωρίς όμως να υπολογίζονται τα έξοδα της εκπαίδευσης των εργαζομένων και της παραμετροποίησης που απαιτείται (Grumman 2011). Όπως βλεπουμε και στην εικόνα 2.1 το αρχικό κόστος για Cloud ERP είναι πολύ μικρότερο από το παραδοσιακό ERP.

Λειτουργικό κόστος

Ένα cloud ERP σύστημα εκ των πραγμάτων έχει μειωμένο λειτουργικό κόστος σε ότι αφορά την ενέργεια, τη συντήρηση, τη διαμόρφωση (configuring) και την αναβάθμιση (upgrades) (Castellina et al. 2011, Marston et al. 2010).

Εκτέλεση (Implementation)

Είναι γεγονός πως τα Cloud ERP συστήματα έχουν σημαντικά καλύτερη απόδοση στην εκτέλεση σε σχέση με τα in-premises συστήματα καθώς και άμεση προσαρμογή σε αναβάθμιση η ακόμα και αλλαγή παρόχου (Benlian and Hess 2011) καθιστώντας τα πιο ευέλικτα στην εισαγωγή καινούριων υπηρεσιών (Marston et al. 2010)

Ευελιξία

Η πρόσβαση και επεξεργασία των δεδομένων ενός Cloud ERP κάνει την υποδομή ευέλικτη (Scavo et al. 2012), και έχει ως αποτέλεσμα την άμεση ενημέρωση κάθε υπαλλήλου για την τρέχουσα κατάσταση της εταιρείας (πχ αποθέματα αποθήκης, εξέλιξη πωλήσεων κτλ.) το οποίο καθιστά την εταιρεία πιο γρήγορη στη λήψη αποφάσεων καθώς και πιο ανταγωνιστική (Benlian and Hess 2011).

Human resource

Το Cloud ERP αποδεσμεύουν τους εργαζομένους του τμήματος πληροφορικής της εταιρείας από την ενασχόλησή τους με το ERP και μπορούν πλέον να απασχοληθούν σε άλλους βασικούς τομείς δραστηριότητας (Castellina et al. 2011). Σε ορισμένες περιπτώσεις, οδηγεί και σε μειωμένη πίεση στο εσωτερικό τμήμα πληροφορικής της εταιρείας που μπορεί να επικεντρωθεί στην εξυπηρέτηση άλλων αρμοδιοτήτων.

Πρόσβαση σε προηγμένη τεχνολογία

Οι Cloud εφαρμογές συχνά επιτρέπουν πρόσβαση σε εξειδικευμένη τεχνολογία και προηγμένες πηγές πληροφορικής, οι οποίες διαφορετικά δεν θα ήταν προσβάσιμες για πολλές εταιρίες (Saugatuck 2008).

Ενημερώσεις και αναβαθμίσεις

Τα Cloud ERP συστήματα συνήθως αποκτούν ταχύτερες ενημερώσεις και νέες λειτουργίες από τα παραδοσιακά συστήματα ERP (Engebrethson 2012).

Προσβασιμότητα (accessibility), ευελιξία (mobility), χρηστικότητα (usability)

Εκτός από τα χαρακτηριστικά της ευελιξίας (mobility) και της προσβασιμότητας, το Cloud ERP διαθέτει υψηλότερα επίπεδα ευχρηστίας και χρηστικότητας απ 'ό, τι άλλα είδη ERP (Engebrethson 2012, Jlelati et al. 2012).

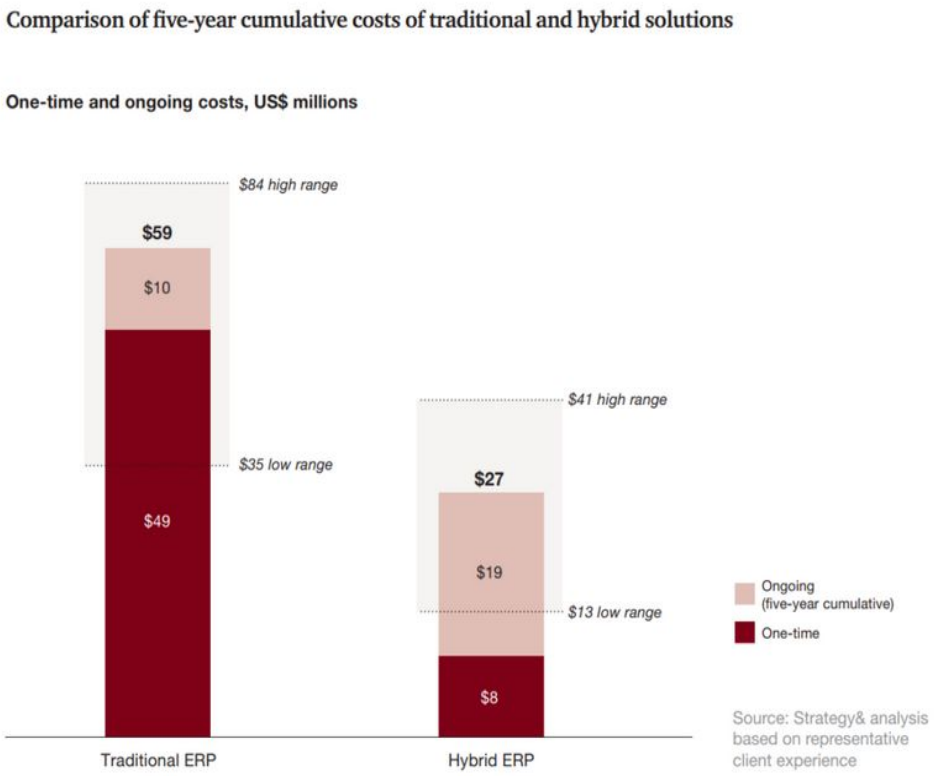
Ενσωμάτωση με άλλες υπηρεσίες cloud

Χρησιμοποιώντας τα οφέλη της κοινής υποδομής του SaaS, οι εταιρείες που υιοθέτησαν το Cloud ERP μπορούν να αποκτήσουν σχετικά ανέξοδη ενσωμάτωση με άλλες υπηρεσίες cloud όταν οι αντίστοιχοι πάροχοι cloud τις έχουν ενσωματώσει στις υποδομές τους (Scavo et al. 2012).

Διαθεσιμότητα του συστήματος και ανάκαμψη καταστροφών

Σε πολλές περιπτώσεις, οι πάροχοι SaaS εξασφαλίζουν υψηλότερης ποιότητας, από ό, τι οι περισσότερες επιχειρήσεις, μέτρα αντιμετώπισης έκτακτων περιστατικών όπως backup routines, διαδικασίες αποκατάστασης (recovery procedures), κλιματιστική ισχύς κλπ. (Scavo et al. 2012).

Εικόνα 2.1: Κόστος αγοράς (one time) και συνδρομής παραδοσιακού και hybirid ERP*



(πηγή: https://selecthub.com)

*hybirid ERP: το ERP σύστημα που έχει μέρος του software interface εγκατεστημένο στα συστήματα της εταιρίας αλλά τα δεδομένα βρίσκονται σε Cloud.

2.2.2 Μειονεκτήματα Cloud ERP σε σχέση με In-premises ERP

Κόστος συνδρομής

Ένα πρόσθετο κόστος του Cloud ERP είναι ότι απαιτεί τακτικά τέλη συνδρομής που συνήθως δε μειώνονται με την πάροδο του χρόνου, σε αντίθεση με τις επενδύσεις κεφαλαίου σε παραδοσιακό λογισμικό ERP (Bartolj et al. 2009) (εικόνα 2.1).

Κίνδυνοι ασφαλείας

Οι κίνδυνοι για την ασφάλεια και την εμπιστευτικότητα των πληροφοριών είναι οι βασικότεροι προβληματισμοί των επιχειρήσεων σχετικά με το Cloud ERP (Engebrethson 2012, Marston et al. 2010). Ταυτόχρονα, σύμφωνα με την επισκόπηση της βιβλιογραφίας, αυτή η ομάδα

κινδύνων φαίνεται να είναι μία από τις πιο αμφιλεγόμενες και εξετάζεται περαιτέρω σε επόμενο κεφάλαιο της έρευνας.

Κίνδυνοι απόδοσης

Οι κίνδυνοι απόδοσης που σχετίζονται με του Cloud ERP εξαρτώνται ουσιαστικά από την ταχύτητα και την αξιοπιστία του δικτύου, τους κινδύνους διακοπής της σωστής λειτουργίας του δικτύου και τους περιορισμούς στη μεταφορά δεδομένων (Kim et al., 2009).

Περιορισμοί προσαρμογής και ενσωμάτωσης

Πολλά συστήματα Cloud ERP έχουν σημαντικούς περιορισμούς στη συμβατότητα με ήδη υπάρχουσες εφαρμογές της εταιρίας και στην ενσωμάτωση με τις τεχνολογικές υποδομές (Karabek et al. 2011). Το Cloud ERP δεν επιτρέπει την εκτεταμένη προσαρμογή και την πολύπλοκη ενσωμάτωση με ορισμένες υπηρεσίες και συστήματα άλλων κατασκευαστών Συνεπώς σε μια τέτοια περίπτωση η εταιρία θα πρέπει να προβεί σε εκτεταμένη αλλαγή των λειτουργικών της συστημάτων προκειμένου να υιοθετήσει ένα σύστημα Cloud ERP (Scavo et al. 2012).

Στρατηγικοί κίνδυνοι

Αναθέτοντας ένα τόσο κρίσιμο για τις επιχειρήσεις σύστημα όπως το ERP, οι εταιρείες συνήθως φέρουν αυξημένο στρατηγικό κίνδυνο λόγω υψηλής εξάρτησης από τον πάροχο υπηρεσιών (Bartolj et al. 2009).

Αλλαγές στο τμήμα πληροφορικής

Ως αποτέλεσμα της εξωτερικής ανάθεσης του μεγαλύτερου μέρους της τεχνικής εγκατάστασης και υποστήριξης του ERP συστήματος, οι οργανισμοί ενδέχεται να χάσουν κάποιες τεχνικές αρμοδιότητες τι οποίες επιτελούσαν μέχρι πρωτινός υπάλληλοι του εσωτερικού τμήματος πληροφορικής της εταιρίας και να αντιμετωπίσουν την αντίσταση των εργαζομένων αυτών των τμημάτων τους σε οργανωτικές αλλαγές (Jlelati et al. 2012). Αυτές οι επιπτώσεις της υιοθέτησης νέφους θεωρούνται συχνά σημαντικές για τις μεγάλες επιχειρήσεις οι οποίες έχουν μεγάλο μέρος προσωπικού που ασχολείται με τις in-premises τεχνολογικές υποδομές.

Περιορισμοί λειτουργικότητας

Το Cloud ERP όντας μια καινούρια τεχνολογία δεν βασίζεται στα ήδη ώριμα συστήματα ERP και συνεπώς υπάρχει η πιθανότητα να μην έχει το σύνολο της λειτουργικότητας που απαιτείται ώστε να ικανοποιεί τις ανάγκες του οργανισμού σε κάθε τύπο βιομηχανίας (Scavo et al. 2012).

Περιορισμός στη στρατηγική υβριδικής ανάπτυξης

Το ERP που βασίζεται σε cloud έχει σημαντικούς περιορισμούς στη στρατηγική ανάπτυξης υβριδικών δυνατοτήτων που μπορεί να απαιτηθεί για να διατηρηθούν τα παλαιότερα συστήματα, αν χρειαστεί, να ενσωματώσει το ERP με λιγότερο ευέλικτα on-premises συστήματα (Scavo et al. 2012).

Θέματα SLA (Service Level Agreements)

Σε πολλές περιπτώσεις είναι μάλλον δύσκολο να προσδιοριστούν με ακρίβεια συμφωνίες των παρεχόμενων υπηρεσιών (SLA) που διαπραγματεύτηκαν μεταξύ του παρόχου υπηρεσιών cloud και των εταιρικών πελατών τους (Kuyoro et al. 2011). Αυτά τα SLAs συνήθως δεν καλύπτουν πρακτικά θέματα όπως η εμπιστευτικότητα και η ακεραιότητα αφήνοντας χώρο για ασαφή ευθύνη βλαβών και απώλειας δεδομένων (Rong et al. 2012).

2.2.3 Συνοπτική παρουσίαση πλεονεκτημάτων Cloud ERP και On-premises ERP

Παρακάτω παρατίθεται ένας πίνακας που παρουσιάζει συνοπτικά τα πλεονεκτήματα του κάθε είδους σε βασικούς τομείς της οργάνωσης μιας επιχείρησης.

Λειτουργίες	Cloud ERP	On-premises ERP
Άμεσες δαπάνες		
Χαμηλότερο αρχικής επένδυσης (υλικό, άδειες χρήσης, εφαρμογή, εκτός της κατάρτισης και προσαρμογής)	✓	
Χαμηλότερο λειτουργικό κόστος (ενέργεια, συντήρηση, διαμόρφωση, αναβαθμίσεις, κόστος προσωπικού IT)	✓	
Δεν υπάρχουν τέλη συνδρομής.		✓
Ανταγωνιστικά Πλεονεκτήματα και Οργάνωση		
Ευελιξία (εξαιρετικά ελαστική ικανότητα υποδομής), ταχύτερος χρόνος εξυπηρέτησης πελατών, καλύτερο εταιρικό performance.	✓	

Ταχεία εφαρμογή, πιο εύκολη εναλλαγή μεταξύ παρόχων.	✓	
Αποδέσμευση προσωπικού πληροφορικής.	✓	
Υψηλότερο επίπεδο ανεξαρτησίας από τον πάροχο ERP.		✓
Ελαχιστοποίηση της απώλειας δεξιοτήτων πληροφορικής και αντιστάσεων προσωπικού στις αλλαγές.		✓
Λειτουργικότητα & Ευχρηστία		
Λειτουργικά ικανοποιητικό για τις ανάγκες του οργανισμού σε όλα τα είδη της βιομηχανίας.		✓
Ταχεία διορθώσεων σφαλμάτων και απόκτηση νέας λειτουργικότητας	✓	
Βελτιωμένη προσβασιμότητα, κινητικότητα και χρηστικότητα.	✓	
Ενσωμάτωση, προσαρμοστικότητα και δυνατότητες απόδοσης		

Επιτρέπει την εκτεταμένη προσαρμογή και την ενοποίηση με ήδη υπάρχοντα συστήματα		✓
Ευκολότερη ενσωμάτωση με άλλες cloud υπηρεσίες	✓	
Βελτιωμένη ανάκτηση από καταστροφή η βλάβη και άμεση διαθεσιμότητα συστήματος	✓	
Η χαμηλή εξάρτηση από την ανεπάρκεια αξιοπιστίας και ταχύτητας του δικτύου		✓
Ευκολία στη διατήρηση των ήδη υπάχοντων on-premises συστήμάτων		✓
Ευκολότερη ενσωμάτωση με ήδη υπάρχοντα on-premises συστήματα		✓
Επιτρέπει τη στρατηγική υβριδικής ανάπτυξης για την ενσωμάτωση 3 παραπάνω στοιχείων		✓
Ασφάλεια & Πρότυπα		
Επιτρέπει το υψηλό επίπεδο ασφάλειας και εμπιστευτικότητας		✓

Ξεκάθαρη ευθύνη για βλάβες συστήματος, απώλεια δεδομένων καθώς και παράπλευρες απώλειες (low performance) συνθήκη SLA		✓

(Duan et al., 2013)

Συμπερασματικά, λαμβάνοντας υπόψη όλα τα παραπάνω θα μπορούσαμε να πούμε ότι:

- Τα Cloud ERP συστήματα τείνουν να ξεπεράσουν τα on-premises ERP στις άμεσες δαπάνες και στις επιπτώσεις για την ανταγωνιστική θέση και την οργάνωση της εταιρίας καθώς και στην λειτουργικότητα και στην ευχρηστία.
- Τα on-premises ERP γενικά δείχνουν να είναι πιο αξιόπιστα σε θέματα προσαρμογής με τα ήδη υπάρχοντα συστήματα καθώς και σε θέματα προσαρμογής του προσωπικού σε αυτά και επιλέον φαίνεται να προτιμούνται λόγω της φαινομενικής ασφάλειας πληροφοριών που παρέχουν.

2.3 Ανάλυση αποτελεσμάτων

Οι λύσεις Cloud ERP είναι πλέον ένα από τα ταχύτερα αναπτυσσόμενα τμήματα της βιομηχανίας πληροφορικής (Popovic 2010). Πράγματι, η μετάβαση από το παραδοσιακό ERP σε Cloud ERP είναι σαφώς αξιοσημείωτη καθώς πρόκειται για μεγάλο μέρος τον επιχειρήσεων που αποφασίζει να προβεί σε αυτή την αλλαγή (Lin and Chen 2012). Το Cloud ERP φαίνεται να παρέχει διάφορα πλεονεκτήματα και μειονεκτήματα σε σύγκριση με το on-premises ERP τα οποία αναλύθηκαν παραπάνω.

Αρχικά, όσον αφορά τα πλεονεκτήματα κόστους του Cloud ERP, μπορεί εύκολα να βγει το συμπέρασμα πως το Cloud ERP έχει χαμηλότερα προκαταβολικά και λειτουργικά έξοδα. Ο λόγος γι 'αυτό είναι το γεγονός ότι οι επιχειρήσεις δεν χρειάζεται να κάνουν τεράστιες επενδύσεις στην εσωτερική τεχνική υποδομή.

Επίσης, σε αντίθεση με το παραδοσιακό ERP, το Cloud ERP μπορεί να διαμορφωθεί κατόπιν ζήτησης και να συντηρηθεί και να αναπτυχθεί γρήγορα, γεγονός που οδηγεί σε πολύ καλύτερη αξιοποίηση της υπολογιστικής υποδομής. Αυτό με τη σειρά του οδηγεί σε χαμηλότερα λειτουργικά έξοδα.

Επιπλέον, ομολογουμένως το Cloud ERP έχει μικρότερο χρόνο υλοποίησης, σε αντίθεση με το παραδοσιακό ERP που χρειάζεται περισσότερη προσπάθεια και χρόνο. Το Cloud ERP παρέχει ένα μοντέλο ταχείας ανάπτυξης που επιτρέπει στις εφαρμογές να εξελίσσονται γρήγορα και να προσαρμόζονται με τις αυξανόμενες απαιτήσεις χρήσης. Ο χρήστης μπορεί εύκολα να αυξήσει ή να μειώσει τις εφαρμογές και την έκταση του cloud συστήματός που χρησιμοποιεί ανάλογα με τις ανάγκες του.

Παρόλα αυτά υπάρχει πιθανότητα να παρουσιαστεί αδυναμία των παρόχων να αυξήσουν την υπολογιστική τους υποδομή καθώς οι απαιτήσεις των πελατών αυξάνονται πέρα από τις αρχικές προσδοκίες. Συνεπώς, είναι σημαντικό οι επιχειρήσεις να κατανοήσουν αρχικά την ικανότητα καθώς και τα σχέδια ανάπτυξης του παρόχου υπηρεσιών όσον αφορά την παρεχόμενη υποδομή.

Επιπλέον, τα πλεονεκτήματα όπως η πρόσβαση σε εξειδικευμένη και προηγμένη τεχνολογία, η εύκολη ενσωμάτωση με άλλες υπηρεσίες cloud, οι ταχείες ενημερώσεις και αναβαθμίσεις είναι εμφανείς στα συστήματα ERP που βασίζονται σε cloud.

Σύμφωνα με την παραπάνω ανάλυση, τα ζητήματα κινδύνου ασφαλείας είναι τα πιο εμφανή μειονεκτήματα του Cloud ERP σε σύγκριση με το παραδοσιακό ERP.

Οι επιχειρήσεις ενδεχομένως θεωρούν πως δεν είναι πάντα ανασφαλείς όσον αφορά τα δεδομένα που αποθηκεύονται σε cloud σύστημα, επειδή δεν έχουν έλεγχο της ασφάλειας τους, αλλά εξαρτώνται από τους παρόχους των cloud υπηρεσιών.

Αυτό θα κάνει τα δεδομένα της επιχείρησης πιο ευάλωτα, αφού ένα cloud σύστημα υπάρχει πιθανότητα να γίνει στόχος κακόβουλης επίθεσης ή και υποκλοπής πληροφοριών. Επίσης με τις cloud εφαρμογές τα δεδομένα είναι προσπελάσιμα από τους υπαλλήλους της εταιρίας-παρόχου, κάτι που δημιουργεί ενδεχομένη ανησυχία στην επιχείρηση σχετικά με ενδεχόμενο διαρροής πληροφοριών.

Αντίθετα, τα on-premises συστήματα τείνουν να είναι πιο ασφαλή, δεδομένου ότι οι επιχειρήσεις έχουν πιο άμεσο έλεγχο των συστημάτων και των δεδομένων τους.

Ένα άλλο ζήτημα κινδύνου είναι η απόδοση που περιλαμβάνει, μεταξύ άλλων, την επικοινωνία μεταξύ του υπολογιστή-πελάτη και του παρόχου των cloud υπηρεσιών, της ταχύτητας και της αξιοπιστίας του δικτύου. Πράγματι, έχει παρατηρηθεί πως η απόδοση τείνει να μειώνεται καθώς ο αριθμός των χρηστών και ο όγκος των δεδομένων που μεταφέρονται αυξάνεται.

Ένα άλλο συχνά αναφερόμενο ζήτημα είναι η περιορισμένη προσαρμογή και η πολύπλοκη ενσωμάτωση με εσωτερικές εφαρμογές και υπηρεσίες. Το ζήτημα αυτό μπορεί να προκαλέσει πολλές τεχνικές και επιχειρηματικές προκλήσεις τόσο για τους παρόχους όσο και για τους πελάτες. Εάν ένας οργανισμός έχει ήδη εγκαταστήσει πολλές πολύπλοκες εφαρμογές που αποτελούνται από πολλά εσωτερικά συστήματα, θα είναι μια πραγματική πρόκληση όσον αφορά την προσαρμογή και υιοθέτηση ενός cloud συστήματος.

Ωστόσο, οι εταιρείες-πάροχοι μπορούν να βοηθήσουν έναν οργανισμό με τέτοιες διαδικασίες. Η ενσωμάτωση ενός cloud συστήματος με ήδη υπάρχουσες εφαρμογές είναι ένας ακόμα παράγοντας που εξαρτάται από τα συστήματα και την κουλτούρα του εκάστοτε οργανισμού (Jlelaty and Monzer 2012).

2.4 Στατιστικά στοιχεία Cloud/On-premise ERP

Από το 2018, οι παράγοντες που οδηγούν τις επιχειρήσεις να αποκτήσουν ένα νέο σύστημα cloud ERP ξεκινούν με κάποια βασικά κριτήρια και απαιτήσεις. Ειδικότερα, η ποιότητα των προϊόντων, η παραγωγή και η παρακολούθηση των διαδικασιών, η αυξημένη χρήση των εφαρμογών ανάλυσης και των επιχειρηματικών πληροφοριών (Business Inteligence) και η ανάγκη μεγαλύτερης κινητικότητας και ευελιξίας (mobility) καθίστανται απαραίτητες για τις εταιρείες που υιοθετούν ERP.

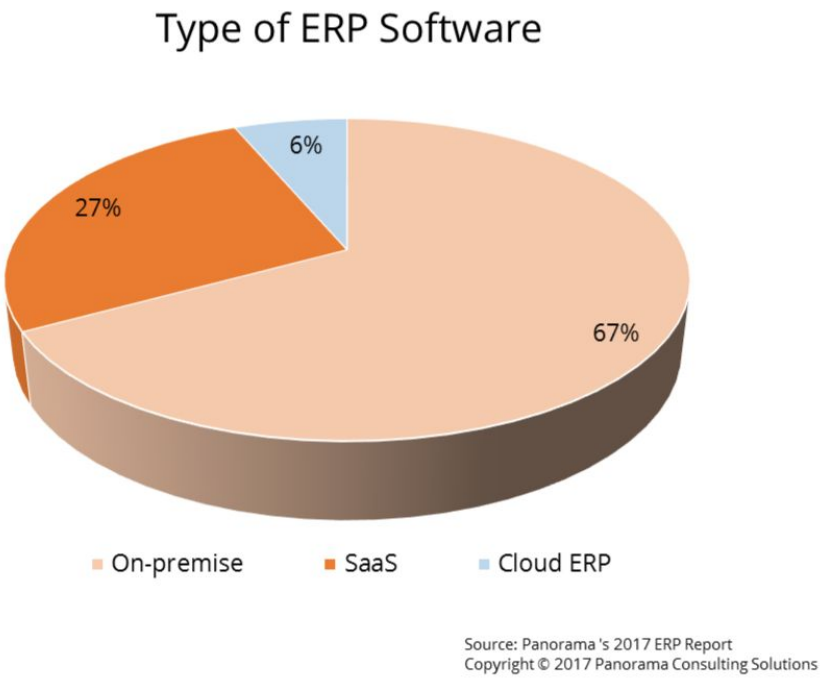
Τα ακόλουθα δεδομένα παρουσιάζουν την τρέχουσα και την εκτιμώμενη ανάπτυξη του cloud ERP:

- Σύμφωνα με την Gartner, έως το 2020, τουλάχιστον το 35% των νέων εφαρμογών ERP σε μεγάλες επιχειρήσεις θα είναι software as a service (SaaS) που θα ενσωματωθεί σταδιακά στα on-premises συστήματα.

- Η παγκόσμια αγορά ERP cloud αναμένεται να ανέλθει στα 28 δισεκατομμύρια δολάρια μέχρι το 2022, επιτυγχάνοντας ετήσιο ρυθμό ανάπτυξης 8% (compound annual growth rate (CAGR)) μεταξύ 2016 και 2022, σύμφωνα με την εταιρεία έρευνας αγοράς Statista

Παρόλα αυτά όπως φαίνεται και στην εικόνα 2.2 ακόμα και μέχρι το 2017 το μεγαλύτερο μερίδιο της αγοράς το είχε το παραδοσιακό ERP με ποσοστό 67%. Οι βασικότεροι λόγοι για τους οποίους οι εταιρείες προτιμούν το on-premises ERP είναι ο κίνδυνος της απώλειας ή διαρροής δεδομένων της εταιρείας (Panorama Consulting Solution's 2017).

Εικόνα 2.2: Μερίδιο αγοράς ERP συστημάτων 2017



Το λογισμικό ERP χαρακτηρίζεται γενικά ως μια εφαρμογή για επιχειρήσεις που έχει σχεδιαστεί για να ανταποκρίνεται στις πιο σύνθετες λειτουργίες των μεγάλων επιχειρήσεων. Συχνά, οι μεγάλες εταιρείες έχουν τα δικά τους τμήματα πληροφορικής ή ειδικές ομάδες που χρησιμοποιούν συστήματα ERP για την ανάλυση μεγάλων δεδομένων και την αντιμετώπιση των αναγκών πολλών τμημάτων. Ωστόσο, οι εφαρμογές ERP για μικρές επιχειρήσεις έχουν έρθει για να καλύψουν τις μικρότερες απαιτήσεις διαχείρισης των νεοσύστατων επιχειρήσεων και των αναπτυσσόμενων εταιρειών. Αυτός ο τύπος ERP συνήθως προσαρμόζεται για να ταιριάζει με τις μικρότερες επιχειρηματικές λειτουργίες και να ταιριάζει με τον συγκεκριμένο επιχειρηματικό κλάδο. Σε έρευνα της Panorama Consulting, το 46% των ερωτηθέντων παραθέτει την "καλύτερη λειτουργική εφαρμογή" ως τον κύριο λόγο επιλογής συγκεκριμένου λογισμικού ERP. Σύμφωνα με την ίδια έρευνα το 2018 τα τρία επικρατέστερα ERP συστήματα, σε ότι αφορά το μερίδιο αγοράς είναι:

SAP HANA 20.3%

Oracle 13.9%

Microsoft Dynamics 365 9.4%

Τα οποία δίνουν λύσεις on-premises και Cloud (SaaS)

2.5 Συμπεράσματα

Παρουσιάστηκε παραπάνω μια έρευνα σχετικά με τις επιχειρηματικές εφαρμογές που βασίζονται σε cloud, διερευνώντας τα πλεονεκτήματα και τα μειονεκτήματα του Cloud ERP σε σύγκριση με το παραδοσιακό ERP.

Στα βασικότερα πλεονεκτήματα του Cloud ERP σε σύγκριση με το παραδοσιακό ERP περιλαμβάνονται το χαμηλότερο αρχικό επενδυτικό κόστος, χαμηλότερο λειτουργικό κόστος, ταχεία εφαρμογή, άμεση αναβάθμιση όπου χρειάζεται, αποδέσμευση τεχνικού προσωπικού, πρόσβαση σε προηγμένη τεχνολογία, βελτιώσεις προσβασιμότητας, ευχρηστία, ευκολότερη ενσωμάτωση με υπηρεσίες cloud και βελτιωμένη αποκατάσταση σε περίπτωση καταστροφών.

Αντίθετα τα μειονεκτήματα του Cloud ERP σε σύγκριση με το παραδοσιακό ERP είναι: οι δαπάνες που οφείλονται στη συνδρομή της υπηρεσίας, οι κίνδυνοι ασφάλειας, οι κίνδυνοι απόδοσης, οι περιορισμοί προσαρμογής και ενσωμάτωσης στα είδη υπάρχοντα συστήματα, οι κίνδυνοι απώλειας ή διαρροής ευαίσθητων ή απόρρητων δεδομένων της εταιρίας, η απώλεια τεχνογνωσίας τους ERP συστήματος από τους υπαλλήλους της εταιρίας, οι περιορισμοί στην παράλληλη ανάπτυξη υβριδικών συστημάτων μαζί με τα ήδη υπάρχοντα συστήματα και θέματα SLA.

Είναι προφανές πως σε μια επιχείρηση που κάνει εκτεταμένη χρήση του ERP συστήματος, είναι επιτακτική η ανάγκη για εφαρμογή Cloud ERP συστήματος, τόσο για λόγους οικονομικούς όσο και για λόγους προσβασιμότητας και ευελιξίας.

Κεφάλαιο 3^{ο} Enterprise Mobility

3.1 Mobile τεχνολογία

3.1.1 Εξέλιξη φορητών συσκευών

Είναι ευρέως γνωστό πως η εξέλιξη της τεχνολογίας επενδύει πλέον κυρίως στην ανάπτυξη και εξάπλωση των φορητών κινητών συσκευών. Η χρήση των κινητών ηλεκτρονικών συσκευών δεν αποτελεί πρόφαση εξέλιξη. Στις αρχές της δεκαετίας του ’90 κυκλοφορούν στην αγορά τα πρώτα κινητά τηλέφωνα ,με μορφή και λειτουργικότητα πολύ διαφορετική από αυτή που έχουν σήμερα, και μέσα σε 10 χρόνια εξελίσσονται τόσο ώστε στις αρχές του ’00 να θεωρούνται απαραίτητο προϊόν σχεδόν για ολόκληρο τον πληθυσμό ανεξάρτητα από ηλικία και επάγγελμα.

Η εξέλιξη των κινητών συσκευών φυσικά δεν σταματάει σε αυτό το στάδιο. Στα επόμενα χρόνια η κινητή τεχνολογία έχει πλέον να επιδείξει πολλά περισσότερα από ένα κινητό τηλέφωνο. Πλέον, οι φορητές συσκευές αποτελούν πολυεργαλεία τα οποία μέσω του λειτουργικού συστήματος, της πρόσβασης στο internet και της cloud τεχνολογίας επιτελούν πολλές λειτουργίες το εύρος των οποίων είναι πολύ μεγάλο και επεκτείνεται διαρκώς.

3.1.2 Τεχνολογικοί τομείς

Οι τομείς της πληροφορικής πάνω στην εξέλιξη των οποίων βασίζεται η ύπαρξη και εξάπλωση των κινητών συσκευών είναι αρκετοί. Ο βασικότερος είναι η τεχνολογία των δικτύων μέσων των οποίων γίνεται η μεταφορά δεδομένων (ήχου, εικόνας, κειμένων, εγγράφων).

Η αναβάθμιση και εξέλιξη του λογισμικού που υπάρχει πλέον στις φορητές συσκευές, τόσο το προεγκατεστιμένο (λειτουργικό σύστημα) όσο και το πρόσθετο (εφαρμογές που εγκαθίστανται από τον χρήστη) αποτελούν πολύ σημαντικό κομμάτι στην εξέλιξη των κινητών συσκευών, καθώς μέσω του λογισμικού επιτελούνται οι λειτουργίες της συσκευής ενώ παράλληλα δίνεται μεγάλη βαρύτητα στο user interface (UI) του λογισμικού ώστε οι λειτουργίες της συσκευής να είναι εύκολα προσβάσιμες, κατανοητές και διαχειρίσιμες καθιστώντας τις φορητές συσκευές εύχρηστες σε μεγάλη μερίδα πληθυσμού.

Τέλος, στην πιο πρόσφατη εξέλιξη των φορητών συσκευών, έχουν συντελέσει σημαντικό ρόλο οι βάσεις δεδομένων σε συνδυασμό με την cloud τεχνολογία. Πλέον, χάρη στα συστήματα αποθήκευσης και διαχείρισης τεράστιου όγκου δεδομένων καθώς και η απομακρυσμένη πρόσβαση σε αυτά έχουν καταστήσει τις φορητές συσκευές ΄μονάδες εργασίας΄ (work station), καθώς ο χρήστης πλέον δεν χρειάζεται να αποθηκεύει δεδομένα τοπικά στην συσκευή του για να έχει πρόσβαση σε αυτά.

Αρκεί μια φορητή συσκευή να έχει το κατάλληλο λογισμικό και σύνδεση στο διαδίκτυο ώστε να μπορέσει ο χρήστης να αναζητήσει και να έχει πρόσβαση σε μεγάλο όγκο πληροφορίας ο οποίος είναι αποθηκευμένος σε κάποια άλλη υπολογιστική μονάδα. Αυτή η διαδικασία καθιστά τις φορητές συσκευές εύχρηστες καθώς και πολύ πιο αποδοτικές, διότι πλέον οι φυσικοί πόροι (hardware) της συσκευής χρησιμοποιούνται μόνο για τις βασικές λειτουργίες της συσκευής και όχι για την αποθήκευση δεδομένων.

3.1.3 Δυνατότητες Mobile τεχνολογίας

Ας εξετάσουμε κάποιες βασικές κατηγορίες δυνατοτήτων ιδιαίτερα σημαντικών για την κατανόηση της προσφοράς της ύπαρξης κινητής τεχνολογίας στην εργασία.

Συνδεσιμότητα (Connectivity)

Το χαμηλό κόστος στην παγκόσμια αγορά ασύρματης συνδεσιμότητας (κινητή τηλεφωνία/wireless internet) έχει σταδιακά οδηγήσει τον πληθυσμό στην επιλογή αυτή. Συγκεκριμένα το 2003 οι συνδρομές κινητής τηλεφωνίας ξεπέρασαν τις συνδρομές σταθερής τηλεφωνίας. Το 2012 οι κινητές συνδεδεμένες συσκευές ήταν περισσότερες από ό, τι οι άνθρωποι στη Γη και εκτιμάται ότι το 2016 θα υπάρχουν 16 δισεκατομμύρια κινητές συσκευές συνδεδεμένες με ασύρματη τεχνολογία δεδομένων (Cisco, 2012) (Sørensen, 2014).

Φορητότητα (Portability)

Η ανάπτυξη της τεχνολογίας έχει δημιουργήσει τις τελευταίες πιο μικρές, αλλά ισχυρές, υπολογιστικές συσκευές. Αυτή η φορητότητα της υπολογιστικής συσκευής δημιουργεί στενότερες σχέσεις μεταξύ της τεχνολογίας και της γεωγραφικής κίνησης των χρηστών, των αντικειμένων και των οχημάτων. Ο όρος «κινητή τεχνολογία» αναφέρεται συχνότερα στον συνδυασμό ενός φορητού πελάτη συνδεδεμένου σε ένα δίκτυο (Sørensen, 2014).

Εγγύτητα χρήστη με την τεχνολογία (Intimacy)

Μια από τις βασικές υποθέσεις είναι ότι όσο πιο κοντά βρίσκεται η τεχνολογία στον άνθρωπο, τόσο πιο κρίσιμη είναι η σχέση της με τον χρήστη. Ο προσωπικός υπολογιστής μπορεί να είναι

σημαντικός για τον χρήστη, αλλά όχι τόσο σημαντικός όσο το κινητό τηλέφωνο, το οποίο καταλαμβάνει μια θέση με τα κλειδιά και τις πιστωτικές κάρτες (Chipchase et al., 2004). Ο χρήστης μπορεί να θεωρεί την κινητή τεχνολογία ως οικεία αφού πλέον έχει καθημερινή και συνεχή επαφή μαζί της (Sørensen, 2014).

Μνήμη (Memory)

Η τεχνολογική ικανότητα της μνήμης υποστηρίζει μια θεμελιώδη διάκριση μεταξύ της τεχνολογίας που αντιμετωπίζει απλώς τη σχέση χρήστη-τεχνολογίας ως ξεχωριστές αυτόνομες οντότητες, σε αντίθεση με τις τεχνολογικές δυνατότητες που καθιστούν δυνατή την αλληλεπίδραση των χρηστών με μια συνεχή σχέση στην οποία η τεχνολογία μπορεί να καταγράφει δραστηριότητες και στη συνέχεια να αντιδρά σε αυτές. Όταν η τεχνολογία δεν υποστηρίζει μνήμη μιας συνεχιζόμενης διαδικασίας, τότε ο χρήστης είναι αποκλειστικά υπεύθυνος για την κατασκευή και τη διατήρηση της μνήμης της διαδικασίας. Όταν η τεχνολογία διατηρεί τη μνήμη των πτυχών της διαδικασίας, τότε η τεχνολογία μπορεί να υποστηρίξει τη διαχείριση της πολυπλοκότητας της διαδικασίας (Carstensen and Sørensen, 1996). Η μνήμη βασισμένη στην τεχνολογία αποτελεί γενικά προϋπόθεση για την ολοκληρωμένη υποστήριξη σύνθετων διαδικασιών λήψης αποφάσεων (Mathiassen and Sørensen, 2008).

3.2 Mobile Business

3.2.1 Ορισμός Mobile Business

Το mobile business αναφέρεται σε "όλες τις δραστηριότητες που πραγματοποιούνται μέσω δικτύων επικοινωνίας και χρησιμοποιούν ως μέσο διασύνδεσης κινητές συσκευές" (Camponovo and Pigneur, 2003; Do van Thanh et al., 2014; Kaczor and Kryvinska, 2013).

Ένας ευρύτερος ορισμός δίνεται από τον Buse (2002), ο οποίος ορίζει ως mobile business "όλες τις επικοινωνιακές δραστηριότητες, καθώς και τις ανταλλαγές πληροφοριών, προϊόντων και υπηρεσιών μέσω κινητών συσκευών. Αυτές οι δραστηριότητες μπορούν να πραγματοποιηθούν μεταξύ επιχειρήσεων (B2B), μεταξύ επιχειρήσεων και καταναλωτών (B2C) ή μεταξύ επιχειρήσεων και υπαλλήλων τους (B2E) "(Buse, 2002).

Ένας άλλος ορισμός για το mobile business είναι "η έναρξη, η μερική ή πλήρης υποστήριξη, εκτέλεση και συντήρηση των διαδικασιών και δραστηριοτήτων μέσω ηλεκτρονικών δικτύων και κινητών συσκευών "(Scherz, 2008). Όλα τα παραπάνω ορίζουν το mobile business ως τις επιχειρηματικές διαδικασίες και συναλλαγές, οι οποίες πραγματοποιούνται ασύρματα με τη βοήθεια κινητών συσκευών.

Οι τομείς, η ανάπτυξη των οποίων οδήγησε στην ανάπτυξη και εξέλιξη του mobile business, είναι:

1. Καινοτομίες στον τομέα της τεχνολογίας
    - Ταχύτερη μετάδοση δεδομένων
    - Καλύτερες κινητές συσκευές
    - Βελτιωμένη χωρητικότητα του υπολογιστή (computer capacity)
    - Βελτίωση στην αποθήκευση δεδομένων (data storage)
    - Πιο εύχρηστο user-interface
2. Κοινωνικοί παράγοντες
    - Αυξημένη χρήση κινητών τηλεφώνων

- Ανάγκη για άμεση επαφή με άλλους χρήστες
- Ανάγκη για διαρκή και άμεση ενημέρωση

3. Ανάπτυξη των παγκόσμιων οικονομιών
    - Ταχείς ρυθμοί ανάπτυξης
    - Ανάγκη για άμεση προσβασιμότητα (Tiwari et al., 2006; Bashah et al., 2012b).

Λόγω των τεχνολογικών καινοτομιών, κοινωνικών παραγόντων και ανάπτυξης των παγκόσμιων οικονομιών, το mobile business οφείλει την ανάπτυξή του στην ανάγκη των χρηστών να μπορούν να δουλεύουν, να διατηρούν επαφή με τους άλλους και να έχουν πρόσβαση στις πληροφορίες από οπουδήποτε κι αν βρίσκονται. Μια ταχέως αναπτυσσόμενη κοινωνία και οικονομία είναι αποτέλεσμα των καινούριων τεχνολογικών επιτευγμάτων (μικρότερες συσκευές, ασύρματες συσκευές κλπ.) και της ανάγκης να παραμένεις ανταγωνιστικός (από επιχειρηματική οπτική γωνία) και ενημερωμένος (από κοινωνική οπτική γωνία) (Tiwari et al., 2006; Bashah et al., 2012a).

Παρακάτω παρατίθενται και αναλύονται τα βασικά χαρακτηριστικά του Mobile Business τα οποία το καθιστούν σημαντικό για μια εταιρία.

3.2.2 Βασικά χαρακτηριστικά του Mobile Business

Mobility

(I. Ivanochko et al., 2015)

Η ικανότητα της πρόσβασης από οπουδήποτε (mobility) είναι το πιο βασικό χαρακτηριστικό του mobile Business και αποτελεί ένα πολύ σημαντικό πλεονέκτημα του mobile Business σε σχέση με τον παραδοσιακό τρόπο λειτουργίας μια επιχείρησης.

Θα μπορούσαμε να πούμε ότι αποτελείται από τα παρακάτω χαρακτηριστικά:

- Ελευθερία κινήσεων: ο χρήστης μπορεί να κάνει χρήση των υπηρεσιών ακόμα κι όταν βρίσκεται εν κινήση (Camponovo and Pigneur, 2003; Wayfinder, 2015).
- Προσβασιμότητα : επιτρέπει στους πελάτες να χρησιμοποιούν συσκευές ανεξάρτητα από την τοποθεσία τους. Αυτοί είναι είναι σε θέση να επικοινωνούν, να λαμβάνουν πληροφορίες και να στέλνουν πληροφορίες, από όπου κι αν βρίσκονται. Ένα πλεονέκτημα είναι, για παράδειγμα, η δυνατότητα σύγκρισης τιμών από μια συγκεκριμένη αποθήκη ή κατάστημα ενώ βρίσκονται ταυτόχρονα σε διαφορετικό κατάστημα (Camponovo and Pigneur, 2003; Buse, 2002; Clarke, 2008).
- Προσδιορισμός θέσης: αναφέρεται στη δυνατότητα ανίχνευσης των ακριβών πληροφοριών θέσης του χρήστη. Αυτό μπορεί να επιτευχθεί με την ενσωμάτωση του GPS στην κινητή συσκευή (Camponovo and Pigneur, 2003; Buse, 2002; Clarke, 2008; Wayfinder, 2015). Η λειτουργία αυτή είναι δυνατόν να βοηθήσει μια εταιρία στην καλύτερη αξιοποίηση των υπαλλήλων γνωρίζοντας την τοποθεσία που βρίσκονται.
- Εξατομίκευση: μια κινητή συσκευή είναι συνήθως μια προσωπική συσκευή, ως εκ τούτου αποθηκεύει προσωπικές πληροφορίες. Αυτό είναι χρήσιμο για τις εταιρείες κατά την παροχή εξατομικευμένων υπηρεσιών προς τον χρήστη όπως πρόσβαση σε διαφορετικές λειτουργικότητες και πληροφορίες ανάλογα με την θέση και το αντικείμενο του υπαλλήλου (Buse, 2002 · Clarke, 2008).
- Ευχρηστία: η χρήση μιας κινητής συσκευής (κινητού τηλεφώνου/tablet) είναι πολύ εύκολη και γίνεται σχεδόν οπουδήποτε γιατί πρόκειται για μικρότερες συσκευές από

τους υπολογιστές, χρειάζονται λιγότερο χρόνο για να ενεργοποιηθούν και είναι ευκολότερες στη χρήση τους (Buse, 2002 · Clarke, 2008).

Context-specificity

(I. Ivanochko et al., 2015)

Ο όρος context-specificity (I. Ivanochko et al., 2015) (συγκεκριμενοποίηση περιεχομένου) αναφέρεται στη δυνατότητα του χρήστη να έχει πρόσβαση σε συγκεκριμένες πληροφορίες που τον αφορούν σε μια δεδομένη χρονική στιγμή ανάλογα με το μέρος που βρίσκεται, με τα άτομα που έχει συναντηθεί και με το αντικείμενο στο οποίο θέλει να δουλέψει (Buse, 2002; Bashah et al., 2012a; Bashah et al., 2012b). Αυτό έχει ως αποτέλεσμα ο χρήστης να εστιάζει σε πληροφορίες και διαδικασίες που τον αφορούν τη δεδομένη χρονική στιγμή στο μέρος που βρίσκεται. Υπάρχουν τέσσερις διαφορετικοί παράγοντες με βάση τους οποίους μπορεί να γίνει η παραπάνω παραμετροποίηση:

- Βάσει τοποθεσίας: η κινητή εφαρμογή δίνει στον χρήστη την πληροφορίες που είναι πιθανό να του χρειαστούν οι οποίες σχετίζονται με την τοποθεσία που βρίσκεται (I. Ivanochko et al., 2015).
- Βάσει δραστηριότητας: πληροφορίες και εφαρμογές ανάλογα με την τοποθεσία και την δραστηριότητα που κάνει εκείνη στην στιγμή ο χρήστης (πχ. Meeting, επικοινωνία με την εφοδιαστική αλυσίδα, επικοινωνία με πελάτες κλπ)
- Βάσει χρονικού προσδιορισμού: συνδυασμός τοποθεσίας και δυναμικών δεδομένων (πχ. συμβάντα σε μια συγκεκριμένη ημέρα σε μια συγκεκριμένη τοποθεσία) (I. Ivanochko et al., 2015).
- Βάσει ενδιαφερόντων/ αντικειμένου εργασίας: προσβαση σε πληροφορίες και εφαρμογές σχετικά με το αντικείμενο εργασίας και την θέση στην εταιρία που έχει ο χρήστης (Buse, 2002; Bashah et al., 2012a; Bashah et al., 2012b).

3.2.3 Είδη χρηστών mobile Business

Στο mobile Business οι πελάτες χωρίζονται σε τρεις βασικές κατηγορίες B2C (Business-to-Consumer) , B2B (Business-to-Business) και B2E (Business-to-Employee) (I. Ivanochko et al., 2015). Ως πελάτες θα μπορούσαμε να χαρακτηρίσουμε τα άτομα ή τις επιχειρήσεις που χρησιμοποιούν τις εφαρμογές για mobile Business (mobile Business applications). Η ασύρματη τεχνολογία χωρίζεται σε κάθετες εφαρμογές για B2B και B2E και σε οριζόντιες εφαρμογές για καταναλωτές B2C (Kryvinska, 2012 · Leem et al., 2004).

Στο μοντέλο Business to Customer (B2C) οι καταναλωτές είναι οι εταιρίες και συγκεκριμένα άτομα (τελικοί καταναλωτές) (Kryvinska, 2012 · Leem et al., 2004).

Το μοντέλο B2C υποδιαιρείται στα εξής είδη υπηρεσιών:

- Εμπόριο: προσφορά κινητών υπηρεσιών/προϊόντων άμεσων εμπορικών συναλλαγών (π.χ. eBooks, e-mail, έκδοση εισιτηρίων κ.λπ.),
- Διαμεσολαβητής: προσφορά κινητών υπηρεσιών από άλλες πηγές (π.χ. καιρός, ειδήσεις κλπ)
- Πληροφορίες: προσφέροντας εξατομικευμένες πληροφορίες για τον πελάτη (π.χ. διαφημίσεις μέσω email, πληροφορίες σχετικά με την θέση που βρίσκεται ο χρήστης, πληροφορίες αποθέματος)

  (Scherz, 2008 · Kryvinska, 2012 · Leem et al., 2004).

Στο μοντέλο Business to Business (B2B) οι καταναλωτές είναι οι εταιρίες και άλλες εταιρείες ή / και εταίροι, οι οποίες συνήθως αποτελούν μέρος της αλυσίδας μιας επιχείρησης. Τέτοιες εφαρμογές κινητής τηλεφωνίας υποστηρίζουν τη γενική λήψη αποφάσεων, την ανταλλαγή πληροφοριών κλπ (Leem et al., 2004). Πιθανές εφαρμογές: έλεγχος διαδικασιών μέσω κινητού τηλεφώνου, διαχείριση του προσωπικού κλπ. (Do van Thanh et al., 2014; Berger et al., 2006).

Στο μοντέλο Business to Employee (B2E) οι καταναλωτές είναι άλλες εταιρείες και οι υπάλληλοί τους(Leem et al., 2004). Το Mobile Business χρησιμοποιείται στο μοντέλο B2E για πολλές δράσεις και βελτιώσεις, για παράδειγμα: συμμετοχή του εργαζομένου στην εσωτερική ροή δεδομένων και διαδικασιών έχοντας πρόσβαση ανεξάρτητα από την τοποθεσία του, επιτρέποντας την διαρκή πρόσβαση σε όλα τα εσωτερικά εταιρικά δεδομένα όπως το emai, το εταιρικό ημερολόγιο κλπ. μέσω κινητών συσκευών. Οι εφαρμογές κινητών συσκευών B2E βελτιώνουν την αποτελεσματικότητα τής εσωτερικής ροής εργασίας.

Εφόσον διαχωρίζουμε τους καταναλωτές στους παραπάνω τρεις τομείς, είναι σημαντικό να γνωρίζουμε τον στόχο του κάθε τομέα. Οι κύριοι στόχοι του mobile business στο B2C είναι η ανάπτυξη μιας νέας ομάδας πελατών. Τα B2B και B2E αποσκοπούν στη βελτίωση της ποιότητας και της διαθεσιμότητας των πληροφοριών τους με απώτερο στόχο την αύξηση της αποδοτικότητάς τους (Do van Thanh et al., 2014; Berger et al., 2006).

3.2.4 Επιχειρηματικά μοντέλα Mobile Business

Ένα επιχειρηματικό μοντέλο (business model) ορίζεται ως εξής: "Περιγραφή των ρόλων και των σχέσεων της εταιρείας, των πελατών της, των εταίρων και των προμηθευτών της, καθώς και των ροών αγαθών, των πληροφοριών και των χρημάτων μεταξύ αυτών των μερών και τα κύρια οφέλη των εμπλεκόμενων.” (Camponovo and Pigneur, 2003; Kryvinska,

2012; Camponovo and Pigneur, 2002)

Για να είναι επιτυχημένο ένα επιχειρηματικό μοντέλο Mobile Business είναι σημαντικό να εξεταστούν όλα ή όσο το δυνατόν περισσότερα χαρακτηριστικά, από αυτά που αναφέρθηκαν παραπάνω, καθώς και οι παράγοντες και οι ρόλοι τους στο Mobile Business (Εικόνα 3.1). Κάθε εταιρεία επικεντρώνεται σε διάφορους παράγοντες, γι 'αυτό δεν είναι δυνατό να δοθεί ένα μοντέλο Mobile Business, το οποίο να απευθύνεται και να ταιριάζει σε κάθε εταιρεία. Ως εκ τούτου, συζητούμε παρακάτω τα βασικά στοιχεία που πρέπει να ληφθούν υπόψη κατά τον σχεδιασμό ενός Mobile Business επιχειρηματικού μοντέλου:

- Καινοτομία προϊόντος:

Περιλαμβάνει όλους τους τομείς που αφορούν την προσφορά της εταιρείας. Περιέχει τα προϊόντα και τις υπηρεσίες καθώς και τον τρόπο με τον οποίο η εταιρεία ξεχωρίζει από τους ανταγωνιστές της. "Η καινοτομία των προϊόντων αποτελείται από τις προτάσεις που προσφέρει η εταιρεία σε συγκεκριμένο μερίδιο πελατών που θέλει να προσελκύσει και τις ικανότητες που πρέπει να αναπτύξει μια επιχείρηση προκειμένου να υλοποιήσει και να προσφέρει αυτές τις προτάσεις" (Camponovo and Pigneur, 2002; Rook, 2003).

- Διαχείριση πελατειακών σχέσεων:

Ο τρόπος με τον οποίο μια εταιρεία προσεγγίζει και διαχειρίζεται τους πελάτες της, (Camponovo and Pigneur, 2003; Camponovo and Pigneur, 2002). Στον τομέα των κινητών υπηρεσιών, υπάρχουν πολλοί τρόποι για τις εταιρίες να διατηρήσουν τους πελάτες τους και να προσελκύσουν νέους χρησιμοποιώντας το ήδη υπάρχον δίκτυο πελατών της (network effect). "Αυτού του είδους η προσέγγιση πελατών χρησιμοποιεί την ήδη υπάρχουσα σχέση με τον πελάτη ώστε να προσελκύσει περισσότερους "(Rook, 2003). Για να εφαρμοστούν αυτά τα

αποτελέσματα είναι απαραίτητο να σχεδιαστεί το προϊόν ή η υπηρεσία με τέτοιο τρόπο ώστε να μεγιστοποιούνται τα αποτελέσματα του network effect (Camponovo και Pigneur, 2002; Rook, 2003).

- Υποδομή:

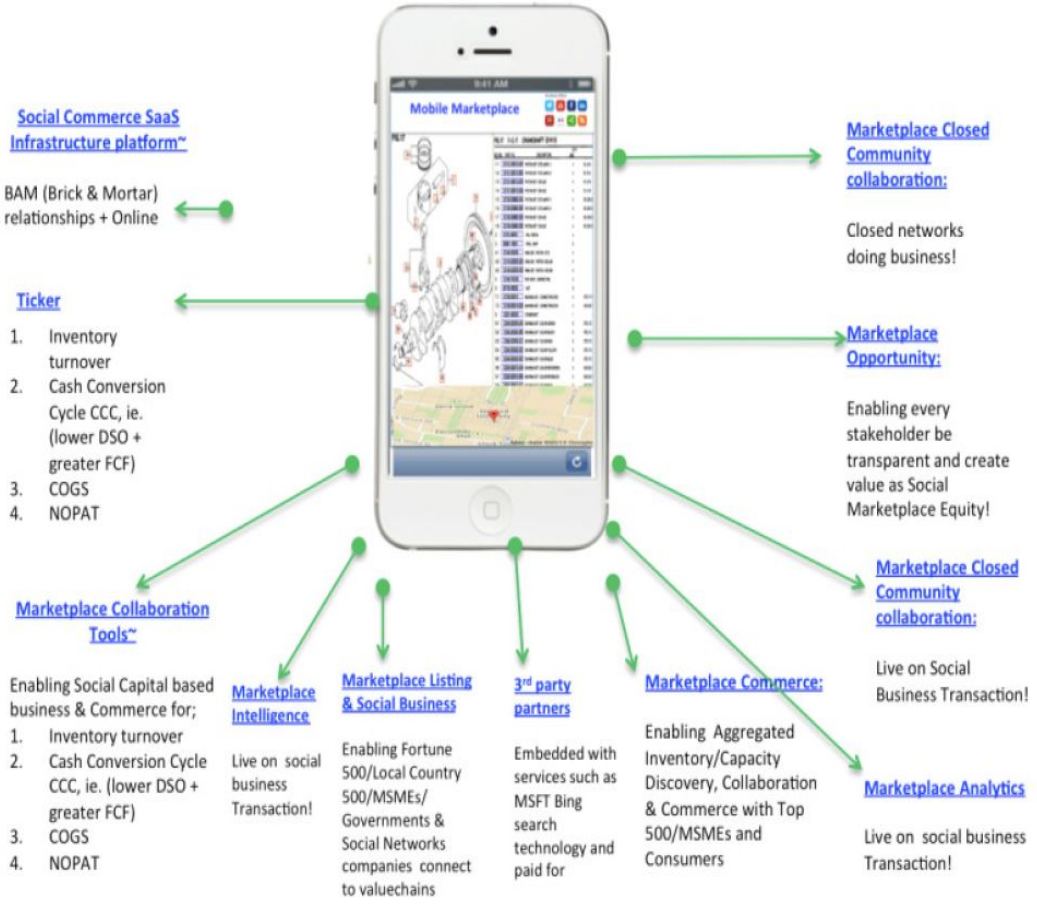
Εξηγεί τη δομή μιας επιχείρησης που αφορά, αφενός, τη δομή των εσωτερικών δραστηριοτήτων και, αφετέρου, τη δομή της εταιρικής σχέσης με άλλα μέρη(πχ πελάτες, εταιρίες που συνεργάζονται κλπ). Ο βασικός στόχος είναι η δημιουργία και η υλοποίηση προϊόντων και υπηρεσιών προς τους πελάτες ή άλλα μέρη (Camponovo and Pigneur, 2003; Camponovo and Pigneur, 2002; Kasper and Hagenhoff, 2003).

- Οικονομικά στοιχεία (finance):

Περιλαμβάνει πληροφορίες σχετικά με το μοντέλο εσόδων, τη διάρθρωση του κόστους, το μοντέλο ζημιών και το μοντέλο κέρδους (Camponovo and Pigneur, 2003, Camponovo and Pigneur, 2002, Kasper and Hagenhoff, 2003). "Τα καλύτερα προϊόντα και υπηρεσίες και οι καλύτερες σχέσεις με τους πελάτες έχουν σημασία για μια επιχείρηση εάν εγγυώνται μακροπρόθεσμη οικονομική επιτυχία " (Camponovo and Pigneur, 2002). Το μοντέλο εσόδων δείχνει την ικανότητα μιας εταιρείας να μετατρέψει την αξία που προσφέρει, σε χρήμα και έτσι να δημιουργήσει εισόδημα για την εταιρεία. Η δομή του κόστους παρουσιάζει το σύνολο των δαπανών που πρέπει να επενδύσει μια εταιρεία για να μπορέσει να δημιουργήσει

αγορά και να προσφέρει ανταγωνιστικά προϊόντα και υπηρεσίες στους πελάτες. Το μοντέλο κέρδους αντιπροσωπεύει την σύνδεση μεταξύ των εσόδων και του κόστους. Η καινοτομία προϊόντων και των υπηρεσιών καθώς και η σχέση των πελατών έχουν ως στόχο την μεγιστοποίηση του μοντέλου εσόδων. Η διαχείριση της υποδομής στοχεύει στο να ελαχιστοποιήσει το κόστος. Αυτό έχει ως αποτέλεσμα την βελτιστοποίηση του μοντέλου κέρδους (Camponovo and Pigneur, 2002; Rook, 2003).

Εικόνα 3.1 : Επιχειρηματικό μοντέλο Mobile Business



(πηγή: Gerardjrego (2014))

3.2.5 Τεχνολογικοί τομείς

Το Mobile Business βασίζεται σε πολύπλοκες, ανταγωνιστικές και μερικές φορές αναξιόπιστες τεχνολογίες (Kryvinska, 2010). Η τεχνολογία, που επιτρέπει την επικοινωνία μέσω ασύρματων δικτύων, μπορεί να χωριστεί στις παρακάτω κατηγορίες (Scherz, 2008 · Kryvinska, 2010):

- Wireless Wide Area Networks (WWAN), π.χ. 4G;
- Wireless Local Area Networks (WLAN), π.χ. Ασύρματο Internet;
- Wireless Personal Area Networks (WPAN), πχ. Bluetooth.

Αυτά τα τρία ασύρματα δίκτυα ταξινομούνται ανάλογα με την ικανότητα της κάλυψής τους (Scherz, 2008 · Kryvinska, 2010).

Οι κινητές συσκευές είναι τα προϊόντα που χρησιμοποιούνται από τους καταναλωτές για να επικοινωνούν, να λαμβάνουν πληροφορίες κ.λπ. μέσω ασύρματων δικτύων (Scherz, 2008 ·

Bashah et al., 2012b). Τα είδη των φορητών συσκευών που χρησιμοποιούνται είναι τα smartphones και τα tables (Scherz, 2008; Bashah et al., 2012a).

3.3 Enterprise Mobility

3.3.1 Αναγκαιότητα για Enterprise Mobility

Η χρήση των κινητών συσκευών στο επιχιερηματικό περιβάλλον (Enterprise Mobility) και γενικότερα η ανάγκη άμεσης απομακρυσμένης πρόσβασης στις πληροφορίες του εταιρικού συστήματος καθώς και στη βάση δεδομένων μέσω κινητών συσκευών (Bring Your own Device (BYOD)) έχει δημιουργήσει μεγάλες αλλαγές στις επιχειρήσεις.

Πράγματι, όλο και περισσότεροι εργαζόμενοι πλέον έχουν ανάγκη για πρόσβαση στα δεδομένα οπουδήποτε κι αν βρίσκονται μέσω της φορητής τους συσκευής. Είναι γεγονός πως υπάλληλοι διαφόρων ειδικοτήτων περνούν πλέον πολύ χρόνο εκτός γραφείου και οι κινητές συσκευές αποτελούν το μόνο μέσο επικοινωνίας με την επιχείρησή τους. Η εξάπλωση και η ευρεία χρήση των φορητών συσκευών έχει δημιουργήσει πλέον έναν ¨κινητό¨ τρόπο ζωής και εργασίας ο οποίος απαιτεί μεγαλύτερη ευελιξία σχετικά με τον τρόπο που λειτουργούσαν πριν οι επιχειρήσεις

Είναι εύκολα αντιληπτό πως η εκτεταμένη χρήση των φορητών συσκευών στον τομέα της επιχειρηματικότητας μπορεί να ωφελήσει σε μεγάλο βαθμό την επιχείρηση Η χρήση φορητών συσκευών μπορεί να βοηθήσει την εταιρεία στην επίτευξη των στόχων της παρέχοντάς της τη δυνατότητα να λειτουργεί πιο αποδοτικά καθώς και να προσαρμόζεται πιο γρήγορα στις αλλαγές που απαιτούνται ώστε να εκσυγχρονιστεί και να γίνει ανταγωνιστική στην αγορά.

Επιπλέον, βοηθάει στην αύξηση της παραγωγικότητας διευκολύνοντας τις διαδικασίες, μειώνοντας το κόστος και διευκολύνοντας την λήψη αποφάσεων.

Σύμφωνα με το Gartner (www.gartner.com) , οι εφαρμογές για κινητά γίνονται όλο και πιο απαραίτητες για τις επιχειρήσεις βελτιώνοντας την αποδοτικότητάς τους και την αποτελεσματικότητα της γνώσης των εργαζομένων, βελτιστοποιώντας τη γραμμή παραγωγής και παρέχοντας διευρυμένη πρόσβαση στους υπαλλήλους και στους συνεργάτες.

3.3.2 Εφαρμογές Enterprise Mobility

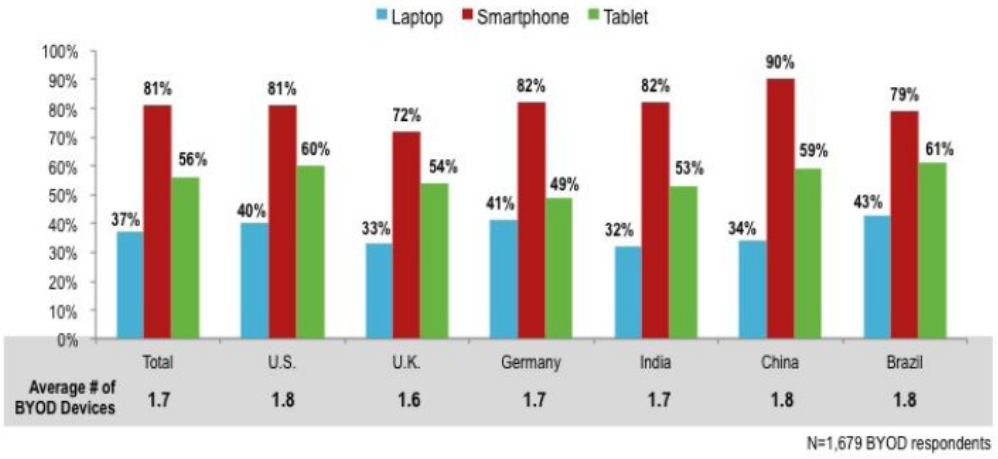
Οι εταιρείες έχουν υιοθετήσει το enterprise mobility και το BYOD επιτρέποντας στους υπαλλήλους της να μεταφέρουν τις δικές τους προσωπικές συσκευές ή παρέχοντας κινητές συσκευές που ανήκουν στην εταιρεία, επιτρέποντας στους χρήστες να έχουν πρόσβαση σε εταιρικούς πόρους όπως συστήματα και εφαρμογές εκτός των εγκαταστάσεών τους. Όλο και περισσότεροι χρήστες στους σύγχρονους χώρους εργασίας προτιμούν να φέρουν τις προσωπικές φορητές τους συσκευές για να εργαστούν Αυτό οδήγησε στην οργάνωση και στην ανάπτυξη μιας πολιτικής για τις επιχειρήσεις (Kamesh, 2012).

Το BYOD θεωρείται συχνά ως πολιτική που επιτρέπει στους υπαλλήλους να χρησιμοποιούν τις κινητές συσκευές τους κατά την εργασία τους. Ωστόσο, πλέον το BYOD έχει

γίνει κάτι περισσότερο από τη χρήση των κινητών συσκευών στην εργασία. Έχει συσχετιστεί με τα οφέλη που αποκομίζουν οι εργαζόμενοι από τη χρήση των προσωπικών τους συσκευών στην εργασία, προκειμένου να αυξήσουν την παραγωγικότητα, την ικανοποίηση από την εργασία και την κινητικότητά τους. Οι οργανισμοί μπορούν να επιλέξουν να λάβουν είτε παθητική είτε
ενεργή προσέγγιση του BYOD. Παθητική προσέγγιση σημαίνει πως οι οργανώσεις επιτρέπουν στους εργαζόμενους να φέρνουν τις προσωπικές τους συσκευές στην εργασία και να τις χρησιμοποιούν για εργασιακές δραστηριότητες. Ενεργός προσέγγιση σημαίνει ότι οργανώσεις δημιουργούν μια σαφή πολιτική του BYOD και την εφαρμόζουν στο περιβάλλον εργασίας. Μια ενεργός προσέγγιση του BYOD βασίζεται σε φορητές προσωπικές συσκευές και απαιτεί υποδομή για την υποστήριξη και την αξιολόγηση της αποτελεσματικότητας της (Hockly, 2012)
Η χρήση της έξυπνης τεχνολογίας (smart technology) στο χώρο εργασίας ξεκίνησε από την εφεύρεση του Blackberry. Οι οργανισμοί συχνά παρείχαν αυτές τις συσκευές για να αυξήσουν την κινητικότητα (mobility) και την παραγωγικότητα των υπαλλήλων τους. Ωστόσο, η εισαγωγή νέων smartphones, όπως το iPhone και το Android, αύξησαν το BYOD στον εργασιακό χώρο. Οι εργαζόμενοι επιθυμούν να χρησιμοποιούν συσκευές με τις οποίες είναι πιο εξοικειωμένοι και οι νεαροί εργαζόμενοι έχουν μεγαλώσει χρησιμοποιώντας πολλές από αυτές τις συσκευές προτού εισέλθουν στο εργατικό δυναμικό (Mansfield-Devine, 2012). Ενώ οι έξυπνες συσκευές θεωρούνται πρωταρχική πηγή της τάσης BYOD, το BYOD δεν περιορίζεται μόνο σε αυτές. Οι συσκευές BYOD περιλαμβάνουν οποιαδήποτε συσκευή που είναι κινητή και αγοράζεται από τον ίδιο τον χρήστη, όπως φορητοί υπολογιστές, netbooks, e-readers, smartphones, tablets κ.λπ. (Thomson, 2012).

Οι χρήστες κινητής τηλεφωνίας που χρησιμοποιούν τις δικές τους συσκευές για δουλειά κατέχουν κατά μέσο όρο 1,7 BYOD συσκευές. Το smartphone είναι η συντριπτική συσκευή επιλογής για τους χρήστες BYOD,αλλά και τα tables κερδίζουν γρήγορα έδαφος. Πενήντα έξι τοις εκατό των χρηστών του BYOD σε όλες τις χώρες χρησιμοποιούν το δικό τους tablet για δουλειά, δείχνοντας πόσο ζωτικής σημασίας είναι αυτές οι συσκευές (Εικόνα 3.2). Το ποσοστό των χρηστών κινητής τηλεφωνίας που χρησιμοποιούν τους δικούς τους φορητούς υπολογιστές για εργασία ήταν επίσης υψηλό (37%) και καθιερώθηκε σε όλες τις χώρες (Cisco IBSG, 2013)

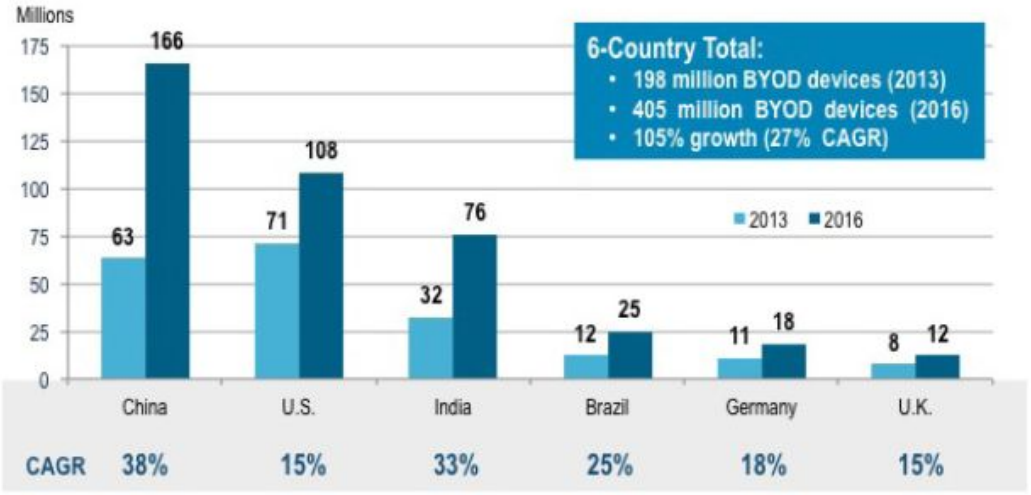
Εικόνα 3.2 Ποσοστό εργαζομένων που χρησιμοποιούν Laptops, Smartphones, Tablets ως BYOD



Source: Cisco IBSG, 2013

Το φαινόμενο του BYOD εφαρμόζεται πλέον σε παγκόσμια κλίμακα, με πάνω από το 71% των εταιρειών παγκοσμίως να αλλάζει τουλάχιστον μια διαδικασία που θα επιτρέψει την υιοθέτηση του BYOD (Qing, 2013). Οι Ηνωμένες Πολιτείες είδαν μια αύξηση κατά 18% της ενεργού εφαρμογής του BYOD το 2013 σε σχέση με το 2012 (Nusca, 2013). Ενώ η τάση του BYOD συνεχίζει να αυξάνεται στις ΗΠΑ, μεγαλύτερη χρήση του BYOD μπορεί να παρατηρηθεί στην Ασία με 77% αύξηση το 2013 έναντι του 2012 (Nusca, 2013). Οι ευρωπαϊκές εταιρείες έχουν παρουσιάσει μια διαφορετική τάση όσον αφορά την εφαρμογή του BYOD με αναφερθείσα μείωση κατά 15% της χρήσης του BYOD το 2013 σε σχέση με το 2012 (Yahoo !, 2013). Σύμφωνα με έρευνα και ανάλυση της Cisco IBSG φαίνεται ότι το BYOD είναι ένα τεράστιο και αυξανόμενο φαινόμενο. Στις έξι χώρες που φαίνονται στην εικόνα, ο αριθμός των συσκευών BYOD έχει αυξηθεί κατά 105% μεταξύ 2013 και 2016, φθάνοντας σχεδόν τα 405 εκατομμύρια, έναν σύνθετο ετήσιο ρυθμό ανάπτυξης (CAGR) 27%. Η Κίνα θα κυριαρχήσει όλες τις χώρες έως το 2016, με 166 εκατομμύρια συσκευές BYOD, ακολουθούμενες από Ηνωμένες Πολιτείες και Ινδία σε 108 εκατομμύρια και 76 εκατομμύρια, αντίστοιχα. Εταιρείες στη Βραζιλία, Γερμανία και το Ηνωμένο Βασίλειο θα σημειώσουν επίσης σημαντική αύξηση των συσκευών που ανήκουν σε εργαζόμενους τα επόμενα τρία χρόνια (εικόνα 3.3) (Cisco IBSG, 2013)

Εικόνα 3.3 Χρήση BYOD συσκευών στον εργασιακό χώρο ανά χώρα



Sources: EIU, Strategy Analytics, Cisco IBSG, 2013

Παρά την υψηλή εφαρμογή του BYOD στις εταιρείες, δεν το χρησιμοποιούν όλοι οι εργαζόμενοι στις εταιρείες που προσφέρεται. Πολλές υλοποιήσεις του BYOD περιορίζονται σε συγκεκριμένους τομείς και ρόλους σε οργανισμούς. Για παράδειγμα, η IBM έχει αναφέρει 435.000 υπαλλήλους σε όλο τον κόσμο, με μόνο 80.000 (18.4%) από αυτούς τους υπαλλήλους που έχουν ενεργοποιηθεί BYOD. Υπάρχουν ορισμένες θέσεις σε έναν οργανισμό που ταιριάζουν με μια στρατηγική BYOD. Μια κοινή παρανόηση σχετικά με τον BYOD είναι ότι η κατοχή από τους εργαζόμενους των δικών τους συσκευών μπορεί να εξοικονομήσει τα χρήματα της εταιρείας, αλλά με βάση τα πρόσφατα δεδομένα αποδεικνύεται πως κάτι τέτοιο δεν ισχύει. Όπως αναφέρει η Pepin (2013), πολλές λύσεις BYOD απαιτούν από την εταιρεία να πληρώνει χρεώσεις υπηρεσιών δεδομένων για τις συσκευές των υπαλλήλων τους. Ωστόσο, η πραγματικότητα είναι ότι πολλές εταιρείες αναφέρουν ότι εφάρμοσαν τον BYOD για να αυξήσουν την παραγωγικότητα παρά να μειώσουν το κόστος (Intel, 2012). Ενώ το BYOD έχει δείξει αρκετά πλεονεκτήματα όπως η αύξηση της κινητικότητας και της ευελιξίας, η ικανοποίηση από την εργασία και η παραγωγικότητα, υπάρχουν πολλές προκλήσεις τις οποίες αντιμετωπίζουν οι εταιρείες κατά την εφαρμογή αυτών των στρατηγικών.

Οι τρεις βασικές απαιτήσεις που αναφέρουν οι οργανώσεις για την επιτυχή υλοποίηση του BYOD είναι:

- Κώδικας δεοντολογίας των εργαζομένων,
- Εγκατάσταση προγραμμάτων ασφαλείας
- Κανόνες διαχείρισης

(Intel, 2012).

Οι φορητές συσκευές θα μπορούσαν να αποσπούν την προσοχή στο χώρο εργασίας εάν χρησιμοποιούνται για προσωπικούς λόγους. Επιπλέον, χρησιμοποιώντας μια προσωπική συσκευή για εργασία θα μπορούσε να επηρεάσει τον προσωπικό χρόνο του εργαζομένου εκτός

της εργασίας καθώς είναι συνεχώς συνδεδεμένη με την δουλειά του. Οι κώδικες δεοντολογίας και οι κανόνες διαχείρισης των εργαζομένων είναι απαραίτητοι για τον περιορισμό των εν δυνάμει αρνητικών επιπτώσεων της χρήσης προσωπικών συσκευών για σκοπούς που σχετίζονται με την εργασία.

Απαιτούνται προγράμματα ασφάλειας για να εξασφαλίσουν την ασφάλεια των ευαίσθητων εταιρικών πληροφοριών. Μερικοί από τους κορυφαίους οργανισμούς ασφάλειας επικαλούνται όταν μια εταιρεία αποφασίζει να εισάγει μια στρατηγική BYOD αναλαμβάνοντας την υλοποίηση των κυβερνητικών κανονισμών σχετικά με ζητήματα ασφάλειας πληροφοριών, την κρυπτογράφηση και την απομακρυσμένη σύνδεση (Intel, 2012). Βιομηχανίες που διαχειρίζονται δεδομένα υψηλού κινδύνου όπως ο ιατρικός τομέας και ο τραπεζικός κλάδος πρέπει να είναι ακόμη πιο προσεκτικοί εάν εφαρμόσουν ένα BYOD στρατηγική λόγω κυβερνητικών κανονισμών. Σε πολλές ευρωπαϊκές χώρες, το εθνικό δίκαιο απαγορεύει στους οργανισμούς την επεξεργασία προσωπικών δεδομένων (Vandendriessche, 2012).

Οι σημερινές εταιρείες αντιμετωπίζουν πολλούς τεχνολογικούς μετασχηματισμούς και εξελίξεις: big data, κοινωνικά μέσα ενημέρωσης και αυξανόμενη τάση της χρήσης των προσωπικών φορητών συσκευών. Οι μετασχηματισμοί αυτοί πρέπει να αντιμετωπιστούν κατάλληλα για να διατηρηθεί η συμμόρφωση από τον εξωτερικό έλεγχο στον εσωτερικό έλεγχο. Σε επιχειρησιακό επίπεδο, οι διευθυντές και τα στελέχη πρέπει να παρακολουθούν, να αξιολογούν και να χειρίζονται θέματα συμμόρφωσης, συμπεριλαμβανομένων των αναγκών των εργαζομένων, των κυβερνητικών κανονισμών, της αλλαγής των βέλτιστων πρακτικών κ.ο.κ. Για να εφαρμοστεί μια στρατηγική BYOD, απαιτείται νοοτροπία διαχείρισης συνόλου. Σύμφωνα με τον Neville Burdan, γενικό διευθυντή της Microsoft Solutions, "όλη η ιδέα είναι ότι πρέπει να υπάρχει έλεγχος, είτε πρόκειται για έναν υπάλληλο,ή για τη διαχείριση των κινητών συσκευών, είτε για τη διαχείριση των κινητών εφαρμογών" (Leong, 2013).

3.4 Οφέλη και προβλήματα Enterprise Mobility

Όταν οι εργαζόμενοι έχουν τη δυνατότητα να επιλέξουν την καταλληλότερη συσκευή για το γραφείο τους, γίνονται πιο ευέλικτοι και παραγωγικοί. Τα επιχειρηματικά οφέλη απορρέουν από την πρόσβαση των υπαλλήλων οποτεδήποτε, οπουδήποτε, γεφυρώνουν το χάσμα εργασίας και αναψυχής και μπορούν να εξοικονομήσουν χρήματα εφόσον οι εργαζόμενοι χρησιμοποιούν την προσωπική συσκευή τους αντί να παρέχουν εταιρικές συσκευές (Mahesh & Hooter, 2013). Η AirWatch (2012) και η Deloitte (2013) αναγνώρισαν κάποια πολύτιμα οφέλη από το BYOD. Αυτά τα οφέλη είναι:

- Ευελιξία διαχείρισης,
- Εξοικονόμηση κόστους,
- Ικανοποίηση των εργαζομένων
- Απλοποιημένη υποδομή πληροφορικής.
- Διευκόλυνση εργαζομένων

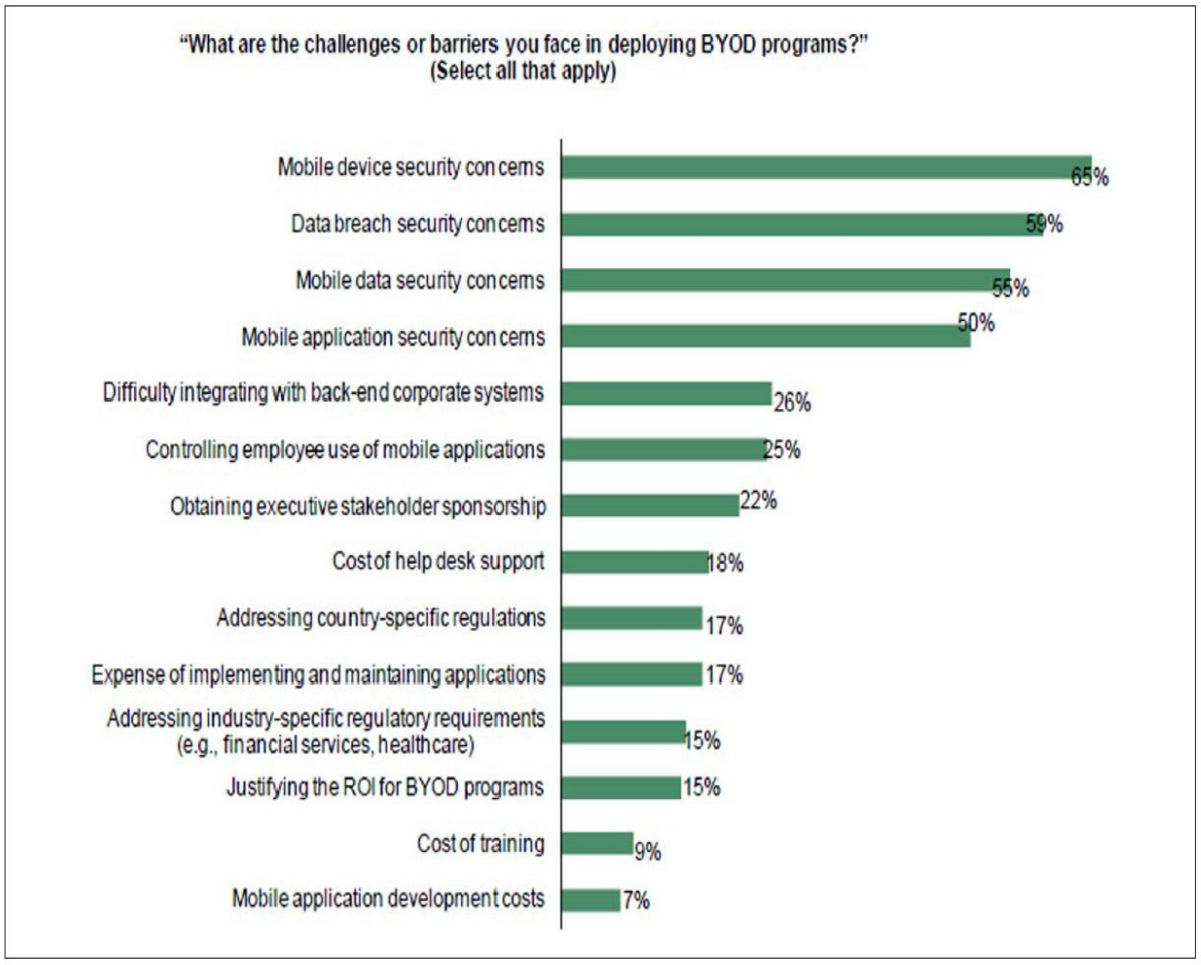
Παρόλο που οι επιχειρήσεις ενδιαφέρονται κυρίως για τη διατήρηση της ασφάλειας, οι εργαζόμενοι ανησυχούν για τη διατήρηση της ευκολίας που χρειάζονται για να εργαστούν από τις κινητές τους συσκευές, καθώς και για την προστασία των προσωπικών τους δεδομένων

(AirWatch, 2012). Μία από τις μεγαλύτερες προκλήσεις για τους οργανισμούς είναι ότι τα εταιρικά δεδομένα παραδίδονται σε συσκευές που δεν διαχειρίζεται το τμήμα πληροφορικής. Αυτό έχει συνέπειες στην ασφάλεια για διαρροή δεδομένων, κλοπή δεδομένων (Morrow, 2012).

Ο Thielens (2013) σημείωσε ότι το πραγματικό πρόβλημα του BYOD είναι η ασφάλεια και συγκεκριμένα ο έλεγχος της πρόσβασης από τις συσκευές στα εταιρικά δεδομένα. Οι προκλήσεις ασφάλειας που συνδέονται με το BYOD αποτελούν προβληματισμό για τους υπεύθυνους ασφαλείας των επιχειρήσεων. Αυτή η πρόκληση έχει προσελκύσει επίσης την προσοχή των ακαδημαϊκών ερευνητών. Οι Alharthy και Shawkat (2013) ισχυρίστηκαν ότι η απώλεια ή η κλοπή κινητών συσκευών είναι ο μεγαλύτερος κίνδυνος που μπορεί να αντιμετωπίσει μια επιχείρηση με την εφαρμογή του BYOD, επειδή οδηγεί σε απώλεια δεδομένων και πρόσβαση σε αυτά από σε άγνωστο χρήστη. Ο Thielens (2013) υποστήριξε ότι απαιτείται μια ασφαλής και κλιμακούμενη στρατηγική BYOD για τη διαχείριση των κινδύνων που εισάγονται από συσκευές που ανήκουν σε εργαζόμενους ως αποτέλεσμα της απώλειας μιας κινητής συσκευής ή κλοπής. Μια έρευνα Forrester (2012) για 202 ερωτηθέντες (Εικόνα 3.4) αποκάλυψε ότι οι ανησυχίες για την ασφάλεια συγκαταλέγονται στις κορυφαίες προκλήσεις για την εφαρμογή προγραμμάτων BYOD.

Μια έρευνα που πραγματοποιήθηκε από την Trustwave αποκάλυψε ότι το 90% των τρωτών σημείων είναι κοινά σε επιτραπέζιους υπολογιστές και κινητές συσκευές (Leavitt, 2013). Οι έρευνες δείχνουν ότι η διαρροή δεδομένων, το distributed denial of service (DDoS), και το κακόβουλο λογισμικό είναι οι μεγαλύτερες απειλές για την ασφάλεια του BYOD (Morrow, 2012).

Εικόνα 3.4 Οι προκλήσεις του BYOD σχετικά με την ασφάλεια. .



Πηγή: (Forrester, 2012)

Διαρροή δεδομένων

Η διαρροή δεδομένων προκύπτει ως αποτέλεσμα της πρόσβασης σε δεδομένα επιχείρησης οπουδήποτε και οποτεδήποτε από τους εργαζομένους. Μια επιχείρηση έχει ελάχιστο ή και καθόλου έλεγχο στα εταιρικά δεδομένα επειδή πλέον αποθηκεύονται τώρα και έχουν πρόσβαση σε αυτά από τις προσωπικές φορητές συσκευές των εργαζομένων. Εάν ένας εργαζόμενος χάσει τη συσκευή, τα δεδομένα επιχείρησης στη συσκευή θα είναι διαθέσιμα σε οποιοδήποτε άτομο που βρίσκει τη συσκευή. Εάν τα δεδομένα που είναι διαθέσιμα στην απώλεια προσωπικών συσκευών είναι εμπιστευτικά επιχειρηματικά δεδομένα, μπορούν να διατεθούν δημόσια από το άτομο που έχει στην κατοχή της η συσκευή (Olalere et al, 2015).

DDoS (Distributed Denial of Service)

Μια επίθεση DDoS είναι μια συντονισμένη επίθεση στη διαθεσιμότητα υπηρεσιών ενός συστήματος ή δικτύου που ξεκινάει έμμεσα μέσω πολλών επιμέρους υπολογιστικών συστημάτων από τα οποία αποτελείται. Το DDoS μπορεί να εμποδίσει τους υπαλλήλους να

έχουν πρόσβαση στα εταιρικά δίκτυα είτε από εταιρικές είτε από προσωπικές συσκευές. Κάθε επιχείρηση που υποβάλλεται σε επίθεση DDoS θα αντιληφθεί το πρόβλημα στον server της και αυτό τελικά θα έχει ως αποτέλεσμα την μη διαθεσιμότητα του συστήματος στους νόμιμους χρήστες (Olalere et al, 2015).

Κακόβουλο λογισμικό

Το κακόβουλο λογισμικό αναφέρεται σε κακόβουλες εφαρμογές που μπορούν να επηρεάσουν τόσο τις κινητές συσκευές όσο και τις εταιρικές εφαρμογές. Τα κακόβουλα προγράμματα για κινητά περιλαμβάνουν εφαρμογές με ενσωματωμένο κώδικα που θέτουν σε κίνδυνο την ασφάλεια μιας κινητής συσκευής ή συναφών δεδομένων. Όταν μια συσκευή δεχθεί κακόβουλο λογισμικό, τα εταιρικά εμπιστευτικά δεδομένα μπορεί να χαθούν και η εταιρική ταυτότητα μπορεί να αναπαραχθεί από τον εισβολέα. Παράλληλα, το κακόβουλο λογισμικό μπορεί να επηρεάσει τις εταιρικές εφαρμογές, καθιστώντας τες μη λειτουργικές (Olalere et al, 2015).

3.5 Συμπεράσματα

Οι επιχειρήσεις προσπαθούν να προσαρμοστούν στα νέα πρότυπα απασχόλησης που αλλάζουν λόγω ασύρματων δικτύων, φορητών συσκευών, κοινωνικών μέσων και Cloud υλοποιήσεων. Στο παρελθόν, οι εργαζόμενοι αναμενόταν να εργάζονται οχτώ ώρες στο γραφείο. Χρησιμοποιούσαν υπολογιστές, διακομιστές και δίκτυα των εταιρειών για την εκτέλεση των καθηκόντων τους. Οι περισσότεροι υπάλληλοι συνεργάζονταν μόνο κατά τις προσωπικές συναντήσεις.

Νέα πρότυπα αντικατέστησαν γρήγορα τα παλιά. Οι εργαζόμενοι εργάζονται τώρα ανά πάσα στιγμή και από οποιαδήποτε θέση. Συχνά χρησιμοποιούν κινητές συσκευές προσωπικής ιδιοκτησίας και επικοινωνούν μέσω οικιακών δικτύων Wi-Fi. Οι εργαζόμενοι ενσωματώνουν τακτικά προσωπικές και επαγγελματικές δραστηριότητες και χρησιμοποιούν τα κινητά τους τηλέφωνα για να τους βοηθήσουν να υλοποιήσουν αυτές τις δραστηριότητες. Αποθηκεύουν δεδομένα επιχείρησης σε δημόσιους διακομιστές cloud και συγχρονίζουν τα δεδομένα μεταξύ συσκευών που ανήκουν σε εργοδότες και εργαζόμενους. Η συνεργασία μπορεί τώρα να πραγματοποιηθεί οπουδήποτε χρησιμοποιώντας κοινωνικές πλατφόρμες όπως το Apple FaceTime, το Google Chat και το Microsoft Lync.

Η κινητικότητα άλλαξε τον τρόπο με τον οποίο οι εργαζόμενοι αλληλοεπιδρούν με τα μέσα που έχουν στην διάθεσή τους για να εργαστούν. Αντί να χρησιμοποιούν τον επιτραπέζιο υπολογιστή για να κάνουν τα πάντα, οι εργαζόμενοι έχουν πλέον τη δυνατότητα να κάνουν τμήματα της δουλειάς τους σε διαφορετικές συσκευές, χρησιμοποιώντας την καλύτερη συσκευή για την τρέχουσα εργασία. Ένας εργαζόμενος μπορεί να λάβει μια ειδοποίηση μέσω ηλεκτρονικού ταχυδρομείου σε ένα smartphone, να δώσει μια γρήγορη απάντηση σε ένα tablet, να συγκεντρώσει περισσότερα δεδομένα μέσω ορισμένων τηλεφωνικών κλήσεων από το αυτοκίνητο και στη συνέχεια να συντάξει ένα λεπτομερές έγγραφο - με υποστηρικτικά υπολογιστικά φύλλα - μόλις επιστρέψει στο γραφείο μέσω επιφάνειας εργασίας PC.

(Gartner, 2012)

Κεφάλαιο 4ο Ασφάλεια πληροφοριών BYOD

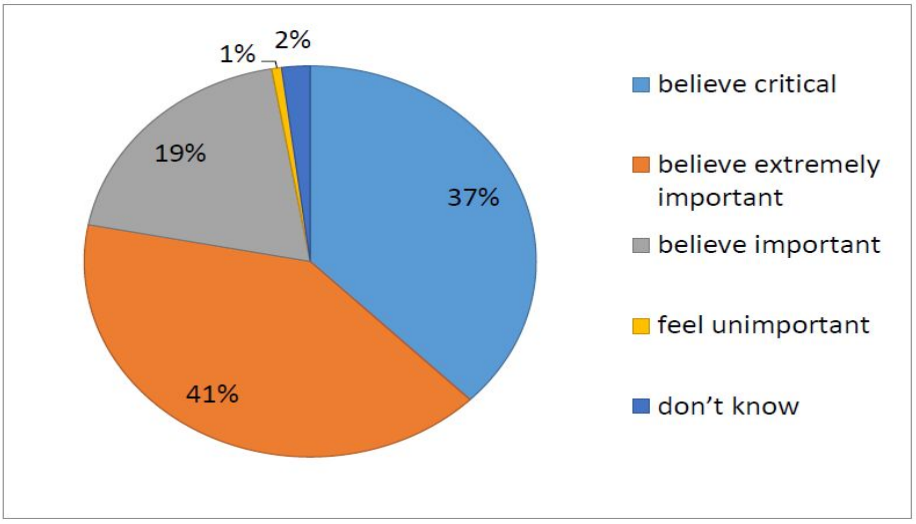
4.1 Ανάγκη για Information Security στο BYOD

Σήμερα, η χρήση συσκευών BYOD είναι πολύ συχνή σε εταιρικά περιβάλλοντα και επαναπροσδιορίζει την ιδιοκτησία και τον έλεγχο των εταιρικών πληροφοριακών συστημάτων και πόρων. Το BYOD αλλάζει τον τρόπο με τον οποίο λειτουργούν οι επιχειρήσεις κυρίως λόγω της αύξησης του αριθμού των οργανισμών που δίνουν πρόσβαση στα εταιρικά δίκτυα και δεδομένα, σε φορητές κινητές συσκευές καταναλωτών, όπως συσκευές iOS ή Android (Gens et al, 2011). Σύμφωνα με μια έρευνα που διεξήχθη από την Cisco, περίπου το 95% των συμμετεχόντων ανέφερε ότι η εταιρία τους, επιτρέπει στους εργαζόμενους να χρησιμοποιούν τις προσωπικές συσκευές για να εργαστούν απομακρυσμένα (Cisco Networks, 2012). Η έρευνα διαπίστωσε επίσης ότι οι εταιρείες αναφέρουν αύξηση της παραγωγικότητας και της αποδοτικότητας των εργαζομένων. Σε αυτή τη βάση, πολλές άλλες εταιρείες άρχισαν να τροποποιούν τα συστήματα πληροφορικής τους για να ενσωματώσουν το BYOD. Παρ 'όλα αυτά, παρά τα οφέλη του BYOD, η ασφάλεια των πληροφοριών και η ιδιωτικότητα είναι τα βασικά προβλήματα(K. W. Miller et al, 2012).

Η χρήση συσκευών BYOD στο χώρο εργασίας έχει υιοθετηθεί από πολλούς οργανισμούς (Hayes and Kotwica, 2013). Οι εργαζόμενοι χρησιμοποιούν τα smartphones τους, τα tablet, τους φορητούς υπολογιστές και άλλες προσωπικές συσκευές χωρίς ενδεχομένως να γνωρίζουν τους κινδύνους ασφάλειας που πιθανό να δημιουργήσουν στις εταιρείες καθώς και στα προσωπικά τους δεδομένα. Ενώ υπάρχουν σημαντικά στοιχεία, όπως είδαμε σε προηγούμενα κεφάλαια, που δείχνουν ότι το BYOD μπορεί να προσφέρει τα πλεονεκτήματα της ευελιξίας της εργασίας, της αυξημένης παραγωγικότητας και της αποδοτικότητας (French et al, 2014; Keyes, 2013), οι κίνδυνοι απώλειας εμπιστευτικών πληροφοριών μπορεί να αντισταθμίσουν αυτά τα οφέλη εάν η ασφάλεια και η ιδιωτικότητα του BYOD διαχειριστούν αναποτελεσματικά (K. W. Miller et al, 2012).

Ο στόχος της ασφάλειας των πληροφοριών είναι να παρέχουν εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα (Whitman and H. J. Mattord,2010). Ομοίως, ο στόχος της προστασίας της ιδιωτικότητας είναι να διασφαλιστεί η εμπιστευτικότητα (Mooradian, 2009). Αυτά μπορούν ιδανικά να επιτευχθούν εάν οι συσκευές BYOD περιοριστούν υπό τον έλεγχο του εκάστοτε οργανισμού. Ωστόσο, η υψηλή κινητικότητα των συσκευών BYOD, οι οποίες δεν ελέγχονται από τον οργανισμό, καθιστά δύσκολη την ασφάλεια των πληροφοριών και τη συντήρησή τους πολύπλοκη και δύσκολη. Στο παρακάτω σχήμα φαίνεται η άποψη των χρηστών BYOD σχετικά με την αναγκαιότητα της εφαρμογής προτύπων για την ασφάλεια πληροφοριών.

Εικόνα 4.1: Άποψη χρηστών BYOD σχετικά με την αναγκαιότητα εφαρμογής προτύπων για την ασφάλεια πληροφοριών



(Πηγή: K. Almarhabi et al, 2017)

Η ετήσια έκθεση ασφαλείας του Pricewaterhousecoopers (PWC) (PWC, 2015) δήλωσε ότι το 59% των παγκόσμιων επιχειρήσεων δεν κατάφεραν να εξασφαλίσουν ασφαλές έλεγχο πρόσβασης για να συμβαδίσουν με πιθανές επιθέσεις στον κυβερνοχώρο. Υπάρχουν ουσιαστικά απεριόριστα οφέλη από το BYOD από οργανωτική σκοπιά, τα οποία περιλαμβάνουν οικονομικά οφέλη, καλύτερο επίπεδο ικανοποίησης των εργαζομένων, αυξημένη υποχρέωση ηθικής, υψηλότερη αποδοτικότητα εργασίας, κινητικότητα και βελτιωμένη ευελιξία (P. Beckett, 2014).

Ωστόσο, υπάρχουν πολλές προκλήσεις που αντιμετωπίζει η τάση του BYOD από την οπτική του οργανισμού. Ο κακός έλεγχος του διαχειριστή δεδομένων στις ατομικές συσκευές BYOD. Οι εργαζόμενοι χρησιμοποιούν εφαρμογές και εργαλεία που βασίζονται στο cloud, όπως το OneDrive, που δεν υπόκεινται στην εποπτεία των εταιρειών και στις κατευθυντήριες γραμμές ελέγχου πρόσβασης για την εκτέλεση των καθηκόντων τους (P. Beckett, 2014).

Για να διασφαλιστεί η εμπιστευτικότητα των πληροφοριών απαιτείται περιορισμός της πρόσβασης σε πληροφορίες μόνο σε εξουσιοδοτημένους χρήστες (Peltier, 2013). Καθώς οι χρήστες του BYOD βρίσκονται συχνά εκτός του περιβάλλοντος εργασίας τους, χρησιμοποιούν ασύρματες συνδέσεις, οι οποίες δεν υλοποιούνται με την βέλτιστη ασφάλεια όσον αφορά την ασφάλεια πληροφοριών. Αυτό σημαίνει ότι τα δίκτυα δεν είναι ασφαλή και δυνητικά θα μπορούσαν να αποκτήσουν πρόσβαση στις πληροφορίες της εταιρείας μέσω των φορητών συσκευών των υπαλλήλων όταν συνδέονται μέσω αυτού του καναλιού για να εργαστούν. Τέτοιου είδους επιθέσεις (Man-in-the-middle) θα μπορούσαν να ξεκινήσουν μέσω τέτοιων συνδέσεων για τη συλλογή μη κρυπτογραφημένων δεδομένων. Επιπλέον, ακόμη και όταν οι χρήστες του BYOD χρησιμοποιούν τα δικά τους δεδομένα κινητής τηλεφωνίας, η μεταφορά δεδομένων από τις συσκευές τους ενδέχεται να μην είναι πάντα κρυπτογραφημένη, επειδή μερικές από τις εφαρμογές που χρησιμοποιούνται μπορούν να μεταδώσουν δεδομένα μέσω μη ασφαλών καναλιών. Αν και οι συσκευές BYOD ενδέχεται να έχουν πιστοποιηθεί και εξουσιοδοτηθεί πριν αποκτήσουν πρόσβαση σε εταιρικούς πόρους, οι κακόβουλες εφαρμογές

θα μπορούσαν να το κάνουν χωρίς τη γνώση των χρηστών του BYOD, στέλνοντας δεδομένα σε μη εξουσιοδοτημένες τοποθεσίες ή άτομα. Εκτός αυτού, δεν έχουν όλοι οι χρήστες του BYOD τη γνώση ότι τα προσωπικά τους δεδομένα μεταδίδονται ή συλλέγονται (K. W. Miller et al, 2012), πόσο μάλλον να έχουν επίγνωση των ρυθμίσεων απορρήτου για την πρόληψή τους. Η πιθανότητα να χάνονται ή να κλαπούν οι συσκευές BYOD είναι επίσης υψηλή και οι συσκευές που χρησιμοποιούν μη κρυπτογραφημένες κάρτες μνήμης και προεπιλεγμένους κωδικούς πρόσβασης μπορούν εύκολα να παραβιαστούν.

Μια έρευνα σχετικά με τους κινδύνους για την ασφάλεια των πληροφοριών και τους κινδύνους της ιδιωτικότητας που σχετίζονται με το BYOD έδειξε ότι το BYOD μπορεί να επηρεάσει τους οργανωτικούς πόρους και τα στοιχεία ενεργητικού, όπως δίκτυα και εφαρμογές, καθώς επίσης, και τις ίδιες τις κινητές συσκευές των τελικών χρηστών (Garba et al, 2015 (a); Eslahi et al, 2014). Επιπλέον με τη χρήση συσκευών BYOD είναι εύκολο να προκύψουν νομικά ζητήματα και προβλήματα αξιοπιστίας. Μια μελέτη που εξέτασε και ανέλυσε τις πρακτικές του BYOD, τα πρότυπα χρήσης, τις αντιλήψεις και τη συμπεριφορά, σε οργανισμούς έδειξε ότι υπάρχουν πολλοί κίνδυνοι που συνδέονται με τον BYOD στους τομείς των φυσικών απειλών, του ελέγχου πρόσβασης, των επικοινωνιών και των εφαρμογών (Garba et al, 2015 (b)). Περαιτέρω στοιχεία από αυτή τη μελέτη υποδηλώνουν ότι οι περισσότερες οργανώσεις είτε δεν κατανοούν πλήρως τη μηχανική πίσω από το BYOD, είτε δεν γνωρίζουν τον πιθανό αντίκτυπό τους στους πόρους εμπιστευτικών πληροφοριών. Οι οργανισμοί δεν διέθεταν επαρκείς γνώσεις σχετικά με τον τρόπο εφαρμογής των κατάλληλων ελέγχων και την επίτευξη κατάλληλης ισορροπίας μεταξύ ασφάλειας και ιδιωτικού απορρήτου, προκειμένου να ελαχιστοποιηθούν οι ελλείψεις από την εμπειρία των χρηστών. Επιπλέον, πολλοί οργανισμοί εφάρμοζαν μόνο τεχνικούς ελέγχους για τη διαχείριση του BYOD, αγνοώντας τους μη τεχνικούς ελέγχους όπως οι πολιτικές και οι διαδικασίες.

Δεδομένου ότι πολλοί από τους υπάρχοντες μηχανισμούς ή προσεγγίσεις που προστατεύουν τις πληροφορίες σε περιβάλλον BYOD δημιουργούν προβλήματα στο σύστημα τα οποία επηρεάζουν την εμπειρία των χρηστών (User Experience) (Garba et al, 2015 (a); Rivera et al, 2013), υπάρχει αυξημένη ανησυχία για την έλλειψη επαρκών και αποτελεσματικών πολιτικών, προτύπων και διαδικασίες για το BYOD (Smith and Forman, 2014; Guan,2012). Αυτό έχει ως αποτέλεσμα την ανάγκη εύρεσης αποτελεσματικών και λειτουργικών λύσεων για τη διαχείριση του BYOD.

Σε εταιρικό επίπεδο, η ασφάλεια των πληροφοριών αφορά την προστασία των πολύτιμων δεδομένων των οργανισμών τα οποία θα μπορούσαν να θεωρηθούν και περιουσιακό στοιχείο της εταιρείας. Πρόκειται για πληροφορίες που είτε υποβάλλονται σε επεξεργασία, καταγράφονται ή αποθηκεύονται και ανήκουν στον οργανισμό. Οι ανησυχίες για την ασφάλεια των πληροφοριών στο BYOD επικεντρώνονται κυρίως στην εμπιστευτικότητα των δεδομένων εφόσον πρόκειται για το εταιρικό περιουσιακό στοιχείο που εκτίθεται σε κίνδυνο. Άλλες ανησυχίες σχετικά με την ασφάλεια αφορούν τον κίνδυνο που προκύπτει από την ανάμειξη προσωπικών και εργασιακών δεδομένων. Σε αντίθεση με τις εταιρικές συσκευές που διαθέτουν μόνο εγκεκριμένο λογισμικό, οι συσκευές BYOD ενδέχεται να έχουν εγκαταστήσει διαφορετικές εφαρμογές. Υπάρχει επίσης η δυνατότητα αντιγραφής ή διάδοσης δεδομένων από μια εφαρμογή σε άλλη στις συσκευές BYOD. Ένα άλλο θέμα ανησυχίας είναι η έλλειψη επαρκών διασφαλίσεων και η κατοχύρωση εμπιστευτικών εταιρικών δεδομένων που διαχειρίζονται οι συσκευές BYOD, από τους υπαλλήλους και κλεμμένες, χαμένες ή πειρατικές συσκευές. Όλα αυτά θα μπορούσαν εύκολα να εισάγουν κακόβουλα προγράμματα και ιούς που μπορούν να μολύνουν συσκευές και πιθανόν να οδηγήσουν σε διαρροή σε εμπιστευτικών δεδομένων. Επτά είδη τύπων απειλών ασφάλειας BYOD εξετάζονται στην ενότητα που

ακολουθεί. Παρόλο που υπάρχουν πολλές από αυτές τις απειλές, επιδεινώνονται από την κινητικότητα των συσκευών (Garba et al, 2015 (b)).

4.2 Προβλήματα Ασφάλειας πληροφοριών BYOD

Mobile malware

Το κακόβουλο λογισμικό για κινητά είναι μια γνωστή απειλή για τις κινητές συσκευές και αναπτύσσεται ραγδαία ως αποτέλεσμα της υιοθέτησης του BYOD (Felt et al, 2011). Ο σκοπός του κακόβουλου λογισμικού είναι να εισέλθει σε μια κινητή συσκευή για να κατασκοπεύσει ή να κλέψει τις πληροφορίες των χρηστών και να βλάψει τη συσκευή. Οι χρήστες κινητών συχνά εξαπατώνται από τους εισβολείς για την εγκατάσταση εφαρμογών κακόβουλου λογισμικού στη συσκευή τους. Σε ορισμένες περιπτώσεις, οι χάκερ περιμένουν ευκαιρίες όταν η κινητή συσκευή είναι ευάλωτη για να αποκτήσει απομακρυσμένη πρόσβαση στη συσκευή. Οι απειλές κακόβουλου λογισμικού είναι πιθανό να είναι: ιοί, worms, trojans και botnets. Υπολογίζεται ότι 11,6 εκατομμύρια κινητές συσκευές μολύνονται ανά πάσα στιγμή με κακόβουλο λογισμικό (Alcatel-Lucent, 2013). Το κακόβουλο λογισμικό που αναπτύσσεται σε κινητές συσκευές, έχει τη δυνατότητα να επικοινωνεί χωρίς διακοπή με απομακρυσμένες περιοχές εντολών και ελέγχου, αποφεύγοντας πολλά μέτρα εταιρικής ασφάλειας

Phishing, social engineering

Αυτές οι επιθέσεις είναι καλά μελετημένες μέθοδοι εξαπάτησης οι οποίες χρησιμοποιούνται για τη συλλογή εμπιστευτικών πληροφοριών από τους χρήστες κινητών συσκευών (Dodge, 2007). Αυτό μπορεί να χρησιμοποιηθεί για να εξαπατήσει τους χρήστες BYOD να κατεβάσουν κακόβουλο λογισμικό στην κινητή συσκευή τους. Άλλες μέθοδοι εξαπάτησης μπορούν να είναι μηνύματα ηλεκτρονικού ταχυδρομείου που αποστέλλονται από πρόσωπα αναγνωρισμένα από τους παραλήπτες που τους ζητούν να απαντήσουν με εμπιστευτικές πληροφορίες. Η πρόσκληση για την καταχώρηση προσωπικών στοιχείων σε έναν ιστότοπο ή για να πειστούν τα άτομα να εγκαταστήσουν λογισμικό (κακόβουλο λογισμικό) ή να κατεβάσουν ένα συνημμένο που εκτελεί ένα κρυφό πρόγραμμα καταγραφής πληροφοριών (πχ password) στη συσκευή BYOD είναι επίσης μια άλλη μέθοδος που χρησιμοποιείται (Garba et al, 2015 (b)).

Άμεσες επιθέσεις

Οι επιθέσεις γίνονται σε ένα συγκεκριμένο σύστημα κινητών συσκευών, ο σκοπός της επίθεσης είναι συνήθως η πρόσβαση, η καταστροφή, η επανεγγραφή / τροποποίηση και η εξαγωγή εμπιστευτικών πληροφοριών. Η άμεση επίθεση με σκοπό την κλοπή, την καταστροφή ή την τροποποίηση εμπιστευτικών δεδομένων μπορεί να έχει τεράστιες επιπτώσεις στις εταιρίες, ιδιαίτερα εκείνες που παρέχουν υπηρεσίες στους πελάτες μέσω του Διαδικτύου (Imperva, 2013).

Υποκλοπή δεδομένων

Πρόκειται για απειλές των ασύρματων δικτύων που χρησιμοποιούνται από συσκευές BYOD. Εάν ένας χρήστης κινητής τηλεφωνίας στείλει πληροφορίες μέσω του Διαδικτύου και υποκλαπούν, αυτό δημιουργεί σοβαρή ανησυχία, εξαιτίας του κινδύνου πρόσβασης, τροποποίησης ή ακόμη και καταστροφής των δεδομένων. Ταυτόχρονα, εάν μια κινητή συσκευή μπορεί να πλαστογραφηθεί μέσω ασύρματου δικτύου και να εξαπατηθεί να στέλνει πληροφορίες σε λάθος παραλήπτη ή να λαμβάνει οποιοδήποτε είδος κακόβουλων δεδομένων, μπορεί να οδηγήσει σε ακόμη μεγαλύτερη ανησυχία για την ασφάλεια. Ακόμα και αν το δίκτυο είναι κρυπτογραφημένο, εξακολουθεί να υπάρχει ο κίνδυνος κάποιος (δηλαδή οι ιδιοκτήτες σημείων πρόσβασης ή κακόβουλοι εσωτερικοί χρήστες) να έχουν κάτι φυσικά συνδεδεμένο στο

δίκτυο που θα μπορούσε να επιχειρήσει να εκμεταλλευτεί μια επικοινωνία μέσω VPN. Η συνεχής παρακολούθηση και πλαστογράφηση ασύρματων ροών δεδομένων και η χρήση παραπλανητικών τρόπων προσέγγισης χρηστών κινητών συσκευών σε δόλια ασύρματα σημεία πρόσβασης έχουν γίνει μια σημαντική απειλή για την ίδια την τεχνολογία κινητών επικοινωνιών και μια μεγάλη πρόκληση για την ασφάλεια στους οργανισμούς του BYOD (Ashford, 2012) . Για παράδειγμα, μια ευπάθεια που αποκαλείται "Hole 196" έχει ανακαλυφθεί από τους ερευνητές ασφαλείας στο πρωτόκολλο ασφαλείας Wi-Fi (WPA2) που χρησιμοποιούν οι περισσότεροι οργανισμοί για να εξασφαλίσουν τα δίκτυα Wi-Fi τους (AirTight Networks, 2010). Εάν οι οργανώσεις συνδέονται μέσω του Hole 196, οι επιτιθέμενοι θα μπορούσαν να εκμεταλλευτούν αυτήν την ευπάθεια για την πρόσβαση σε προσωπικά δεδομένα άλλων, καθώς και να εισάγουν κακόβουλες απειλές στο ασύρματο δίκτυο.

Απώλεια / κλοπή συσκευών

Η απώλεια και η κλοπή κινητής συσκευής αποτελεί παράγοντα επικινδυνότητας γιατί είναι πιο πιθανό να συμβεί με κινητές συσκευές από τους παραδοσιακούς υπολογιστές. Ενώ οι κινητές συσκευές έχουν φέρει αυξημένη ευελιξία, μπορούν εύκολα να χαθούν ή να κλαπούν. Πάνω από 2 εκατομμύρια κινητές συσκευές εκλάπησαν στο Ηνωμένο Βασίλειο κατά τη διάρκεια του 2005 (Braue, 2007). Ομοίως, έχει αναφερθεί από την Αυστραλιανή Ένωση Κινητών Τηλεπικοινωνιών ότι, σχεδόν κάθε χρόνο, υπάρχουν πάνω από 100.000 κινητές συσκευές που έχουν δηλωθεί κλεμμένες ή χαμένες (AMTA, 2013). Όταν χάνονται οι κινητές συσκευές, πολύτιμες πληροφορίες μπορούν εύκολα να πέσουν σε λάθος χέρια και μπορούν να χρησιμοποιηθούν για δόλιους και άλλους παράνομους σκοπούς. Στην πλειονότητα των περιπτώσεων, το κόστος της συσκευής στους ιδιοκτήτες ή τους οργανισμούς δεν είναι εξίσου σημαντικό με την αξία των πληροφοριών που είναι αποθηκευμένες στη συσκευή.

Κακόβουλοι χρήστες BYOD

Έχει αναφερθεί πως χρήστες κινητών συσκευών BYOD έχουν αποκαλύψει εμπιστευτικές πληροφορίες και εμπιστευτικά δεδομένα. Οι κακόβουλοι υπάλληλοι είναι ένα από τα πιο δύσκολα και προβληματικά ζητήματα ασφάλειας που πρέπει να αντιμετωπιστούν. Οι εσωτερικοί συνεργάτες έχουν άμεση πρόσβαση σε οργανωτικούς πόρους και δίκτυα πληροφοριών. Ως εκ τούτου, είναι ευκολότερο για αυτούς να κλέψουν, να τροποποιήσουν ή να καταστρέψουν δεδομένα. Με το BYOD, οι κακόβουλες απειλές εσωτερικών χρηστών είναι ευκολότερο να πραγματοποιηθούν, αφού οι χρήστες των κινητών συσκευών έχουν πρόσβαση σε εταιρικά συστήματα και πόρους οποιαδήποτε στιγμή οπουδήποτε. Οι υπάλληλοι του BYOD, οι οποίοι είναι κακόβουλοι, έχουν τη δυνατότητα εκτέλεσης επιθέσεων κακόβουλου λογισμικού, ηλεκτρονικού "ψαρέματος" (phishing), υποκλοπής δεδομένων και πλαστογράφησης (Garba et al, 2015 (b)).

Παραβιάσεις στους όρους χρήσης

Η παραβίαση των όρων χρηστών από τους χρήστες είναι ένας από τους ευκολότερους τρόπους για να εκθέσετε μια συσκευή BYOD σε ευπάθειες. Οι χρήστες του BYOD δεν έχουν κακόβουλη πρόθεση. Η άγνοια και η απροσεξία, όπως η πρόσβαση και η λήψη ακατάλληλου περιεχομένου ιστού που μπορεί να περιέχει κακόβουλο λογισμικό και η απενεργοποίηση εφαρμογών προστασίας από ιούς και τείχους προστασίας για την αύξηση της ταχύτητας και της απόδοσης, μπορούν να εκθέσουν τις συσκευές BYOD σε τρωτά σημεία και απειλές (Garba et al, 2015 (b)).

Είναι προφανές πως η χρήση συσκευών BYOD εκτίθεται σε πολλούς κινδύνους. Τα δεδομένα και οι πολιτικές που ελέγχουν τη διαδικασία εξουσιοδότησης μπορούν να τροποποιηθούν από επιθέσεις. Οι εργαζόμενοι μπορούν να εγκαταστήσουν διαφορετικά είδη εφαρμογών, όπως παιχνίδια και εφαρμογές κοινωνικής δικτύωσης, οι οποίες ενδέχεται να

περιλαμβάνουν επικίνδυνα δεδομένα κακόβουλης λειτουργίας και έκθεσης κατά τη διάρκεια των φάσεων μεταφοράς, επεξεργασίας και αποθήκευσης. Ακόμη χειρότερα, ο οργανισμός δεν μπορεί να ελέγξει εάν η συσκευή BYOD περιέχει ήδη εφαρμογή κακόβουλου λογισμικού ή όχι χωρίς να παραβιάζει το απόρρητο των εργαζομένων. Η αντιμετώπιση ενός μη ασφαλούς δικτύου είναι επίσης επικίνδυνο, ειδικά εάν ένας υπάλληλος εργάζεται από διαφορετικές τοποθεσίες και συνδέεται με άλλα διαφορετικά δίκτυα (K.Almarhabi et al, 2017). Οι επιθέσεις συμβαίνουν σε πολλά διαφορετικά λειτουργικά συστήματα κινητής τηλεφωνίας, όπως το IOS, το Android και τα Windows Mobile, όπως φαίνεται στην παρακάτω εικόνα:

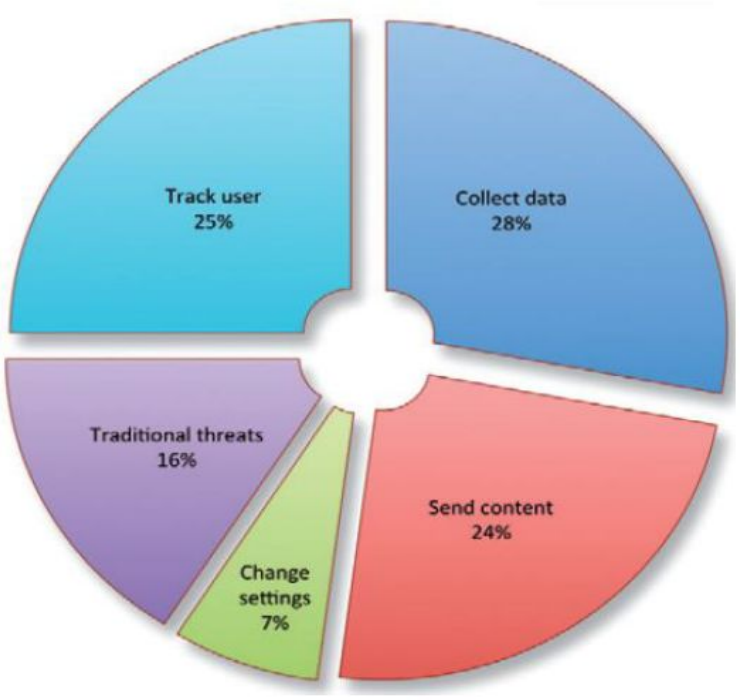
Εικόνα 4.2 Επιθέσεις στα λειτουργικά συστήματα

Name	*Attack(s)*	*Mobile OS*
Zeus (Zitmo)	• Mobile Banking Attacks • TAC Thefts • Illegal Transactions	• Symbian • Win Mobile • BlackBerry • Android
DroidDream	• Theft of Private Data • Downloading Malicious Applications	• Android
Android.Bmaster (SmartRoot)	• Revenue Generation • Theft of Private Data	• Android
AnserverBot	• Theft of Private Data	• Android
Ikee.B	• Revenue Generation • Theft of Private Data	• iPhone
TigerBot	• Theft of Private Data • Changing Device Settings	• Android

(Πηγή: K. Almarhabi et al, 2017)

Αυτό σημαίνει ότι σχεδόν όλα τα λειτουργικά συστήματα ευάλωτα σε κακόβουλες επιθέσεις και δεν υπάρχει εξαίρεση σε ορισμένα λειτουργικά συστήματα για την αποφυγή του κινδύνου επιθέσεων. Οι λύσεις πρέπει να λειτουργούν συμβατά με όλα τα λειτουργικά συστήματα. Εφαρμογές κακόβουλου λογισμικού σχεδιασμένες να επιτελούν επιβλαβείς εργασίες όπως η συλλογή δεδομένων, η αλλαγή πολιτικής (J. M. Chang et al, 2014), η αποστολή περιεχομένου και η παρακολούθηση του χρήστη όπως φαίνεται στην παρακάτω εικόνα

Εικόνα 4.3 Σκοπός κακόβουλων επιθέσεων στα συστήματα BYOD



(Πηγή: J. M. Chang et al, 2014)

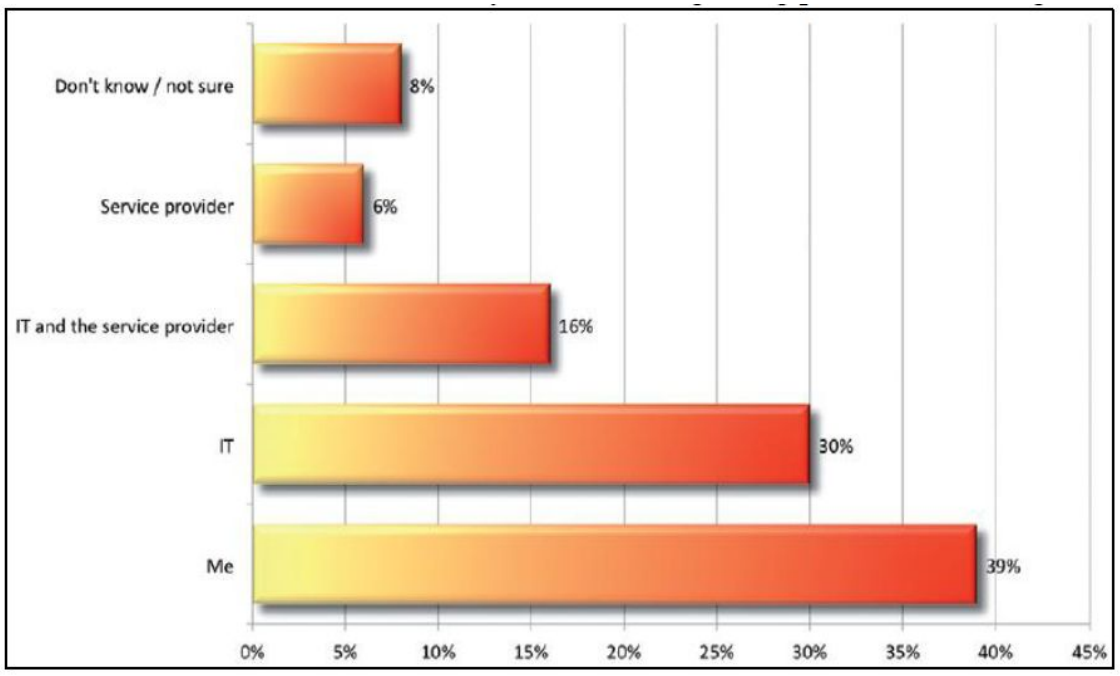
4.3 Ανάλυση παραμέτρων Information Security για BYOD

Η Stanford Encylopedia of Philosopphy αναφέρεται στα δικαιώματα ως: Οι νόμιμες, κοινωνικές ή ηθικές αρχές ελευθερίας ή δικαιώματος, δηλαδή τα δικαιώματα είναι οι θεμελιώδεις κανόνες σχετικά με το τι επιτρέπεται στους ανθρώπους, σύμφωνα με κάποιο νομικό σύστημα, κοινωνική σύμβαση ή ηθική θεωρία (Stanford University, 2014).

Αυτό είναι ένα γενικό νόημα που μπορεί να εφαρμοστεί σε όλα τα μέρη στο περιβάλλον του BYOD. Σε ότι αφορά τον έλεγχο πρόσβασης πρόκειται για τα δικαιώματα τα οποία παρέχονται στον χρήστη ή σε μια εφαρμογή για τη γραφή, ανάγνωση και διαγραφή δεδομένων. Οι διαδικασίες αναφέρονται σε μη τεχνικές προσεγγίσεις που εφαρμόζονται στην ενίσχυση πολιτικών χρήσης των δεδομένων μέσω συσκευών BYOD (B. Ballad et al, 2011). Τα πλεονεκτήματα και η αδυναμία ενός BYOD επικεντρώνεται στις προληπτικές προσεγγίσεις που εμπλέκονται σε όλα τα μέρη, τόσο στον εργαζόμενο όσο και στον εργοδότη, ώστε να κατανοήσουν τα δικαιώματά τους, τις πολιτικές τους και τις κυρώσεις τους για τη νόμιμη χρήση του BYOD (P. Beckett, 2014). Πρέπει να παραπέμψουμε την οργάνωση να τηρεί όσο το δυνατόν τα διεθνή πρότυπα σχετικά με τις τάσεις του BYOD. Το ερευνητικό έγγραφο (PWC, 2015) περιγράφει τον τρόπο με τον οποίο οι χρήστες του BYOD δεν ενημερώνονται σχετικά με τα μέτρα ασφάλειας πληροφοριών ή έχουν ελάχιστες γνώσεις σχετικά με τις συμπεριφορές

αποφυγής κακόβουλου λογισμικού. Ο Hovav και άλλοι ερευνητές (A. Hovav and F. F. Putri, 2016) εξήγησαν το λόγο για τον οποίο οι εργαζόμενοι που αντιλαμβάνονται την απειλή της ελευθερίας στην χρήση των συσκευών BYOD επηρεάζουν αρνητικά την πρόθεση συμμόρφωσης. Οι ερευνητές προτείνουν την ανάπτυξη πρακτικής κατάρτισης για τη δημιουργία και διατήρηση της εμπιστοσύνης των χρηστών στις ικανότητές τους να αντιμετωπίσουν τις απειλές κακόβουλου λογισμικού. Ο Thomson (G.Thomson, 2012) επέδειξε ένα σημαντικό σημείο σχετικά με την ευθύνη του χρήστη να προστατεύσει τα δεδομένα του. Αυτό βασίστηκε σε μια μελέτη που διεξήχθη στον κύριο υπεύθυνο για την προστασία των δεδομένων και στο σχήμα φαίνονται τα αποτελέσματα.

Εικόνα 4.4 Η γνώμη των εργαζομένων σχετικά με το ποιος είναι υπεύθυνος για τη διασφάλιση συσκευών BYOD



(Πηγή: K. Almarhabi et al, 2017)

Το BYOD εκτείνεται σε πολλές λειτουργικές περιοχές ενός οργανισμού, που περιλαμβάνουν ανθρώπινους πόρους, νομικά, οικονομικά και λειτουργικά τμήματα (B. Hayes et al, 2013; Mooradian, 2009). Ως εκ τούτου, οι προκλήσεις του BYOD μπορούν να προσεγγιστούν από πολλαπλές οπτικές γωνίες, συμπεριλαμβανομένων των οργανωτικών και τεχνικών. Αυτές παρέχουν αρκετές διαστάσεις ελέγχου για το BYOD που σχετίζονται με τον έλεγχο των δεδομένων, τον έλεγχο της πρόσβασης, τον έλεγχο των δικτύων και τη διαχείριση των συσκευών, καθώς και τη δημιουργία ρητών πολιτικών και διαδικασιών (Dedeche et al, 2013; Ghosh et al, 2013). Ενώ υπάρχουν πολλές τεχνικές λύσεις που βασίζονται σε προμηθευτές για τη διαχείριση του BYOD, δεν υπάρχουν ρητές πολιτικές και διαδικασίες που αφορούν την ασφάλεια πληροφοριών για να υποστηρίξουν αυτές τις τεχνικές λύσεις (ZixCorp, 2013; Rivera et al, 2013). Η εφαρμογή ρητών πολιτικών ασφάλειας και προστασίας προσωπικών δεδομένων

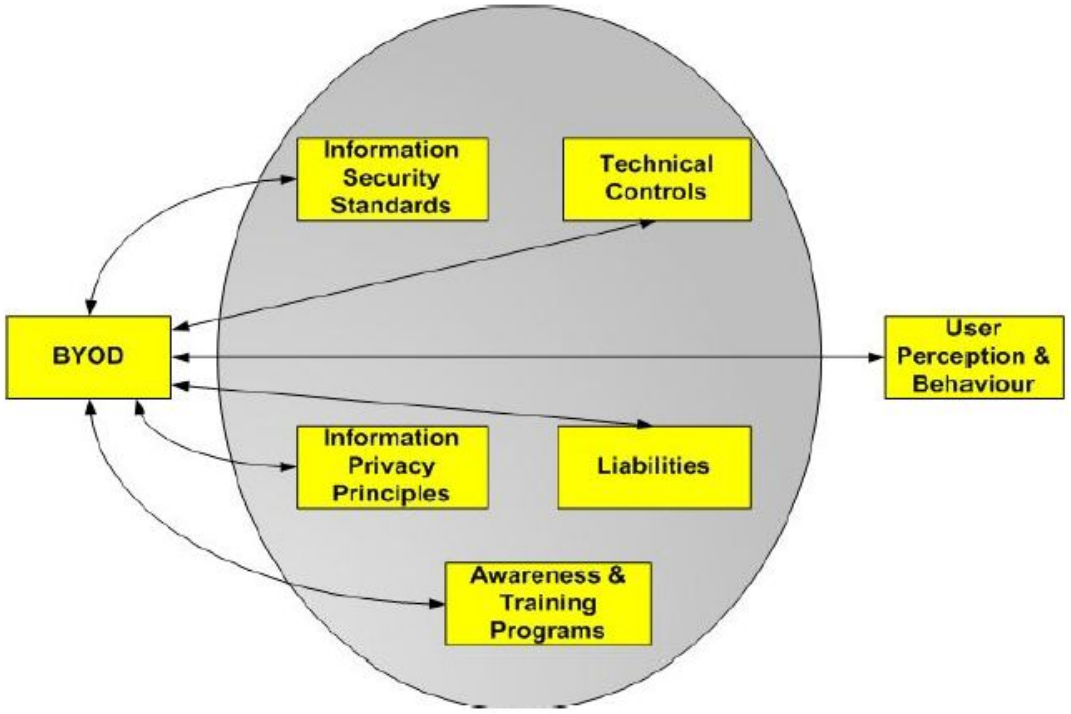
είναι ένας βασικός έλεγχος που απαιτείται στα περιβάλλοντα BYOD, επειδή μπορεί επίσης να ενσωματώσει ή να υποστηρίξει τις άλλες ανάγκες ελέγχου του BYOD (Garba et al, 2015 (b)).

Ωστόσο, πριν αναπτυχθούν και εφαρμοστούν οι πολιτικές του BYOD, πρέπει να εξεταστούν διάφορα ζητήματα σχετικά με: νομικές πτυχές και πτυχές αξιοπιστίας, τις διαδικασίες και τα μέτρα τεχνικού ελέγχου που πρέπει να χρησιμοποιηθούν, τον αντίκτυπο των ελέγχων στους χρήστες του BYOD, τον ψυχολογικό αντίκτυπο της πολιτικής του BYOD στους χρήστες όσον αφορά τη συμπεριφορά τους και την αποδοχή της πολιτικής ελέγχου (Andrew and Yang, 2013; Garba et al, 2015 (b)). Για την αντιμετώπιση αυτών των ζητημάτων, θα πρέπει να εξεταστεί ένα προτεινόμενο μοντέλο διαχείρισης βάσει του οποίου συνιστούν έξι στοιχεία ελέγχου:

- Πρότυπα και διαδικασίες ασφάλειας πληροφοριών (Information security standards and procedures)
- Αρχές προστασίας της ιδιωτικότητας (Information privacy principles)
- Τεχνικοί έλεγχοι ασφάλειας και προστασίας της ιδιωτικότητας (Information security and privacy technical controls)
- Υπευθυνότητα και δεσμεύσεις (Liabilities)
- Πρόγραμμα γνωστοποίησης και κατάρτισης (Awareness and training program)
- Η αντίληψη και η συμπεριφορά του χρήστη BYOD (BYOD user perception and behaviour)

Αυτά τα στοιχεία επιλέγονται με βάση τις ενδείξεις από την ασφάλεια των πληροφοριών και τις θεωρίες περί ιδιωτικότητας (Pfleeger and Shari, 2006) είναι σημαντικά στην προσπάθεια να επιτευχθεί υψηλό επίπεδο προστασίας δεδομένων σε οργανισμούς. Το σχήμα 1 απεικονίζει το μοντέλο διαχείρισης βασισμένο στην πολιτική BYOD, το οποίο εξετάζει κάθε στοιχείο για να προσδιορίσει τα κατάλληλα μέτρα ελέγχου που μπορούν να συμπεριληφθούν στις πολιτικές του BYOD. Διεξάγεται μια διασταυρούμενη ανάλυση των σχέσεων μεταξύ των συνιστωσών ώστε να επιτευχθεί ισορροπία μεταξύ ασφάλειας και ιδιωτικότητας, ώστε να εντοπιστούν μέτρα ελέγχου που δεν θα επηρεάσουν την εμπειρία των οργανώσεων και των εργαζομένων του BYOD.

Εικόνα 4.5 Μοντέλο πολιτικής ασφάλειας πληροφοριών BYOD



Πηγή: Garba et al, 2015 (c)

4.4 Απαραίτητα βήματα για την εφαρμογή συστήματος ελέγχου στις συσκευές BYOD

Προσαρμογή των προτύπων ασφάλειας πληροφοριών για το BYOD

Τα πρότυπα ασφάλειας πληροφοριών διασφαλίζουν ότι επιτυγχάνεται επαρκές επίπεδο ασφάλειας πληροφοριών εφόσον υιοθετούνται και εφαρμόζονται οι καλύτερες πρακτικές ασφαλείας σε έναν οργανισμό. Σε ότι αφορά το BYOD, τα πρότυπα ασφάλειας πληροφοριών μπορούν να βοηθήσουν τους οργανισμούς να εφαρμόσουν αποτελεσματικούς μηχανισμούς ελέγχου ασφάλειας για να διασφαλίσουν την εμπιστευτικότητα και την ακεραιότητα των πληροφοριών. Υπάρχουν διαφορετικοί τύποι προτύπων ασφάλειας πληροφοριών που μπορούν να εφαρμοστούν από οργανισμούς για τη διαχείριση απειλών και τρωτών σημείων σε περιβάλλοντα BYOD. Αυτά περιλαμβάνουν τα πρότυπα σειράς ISO 27000 (ISO 27000 Directory, 2014), COBIT (ISACA, "COBIT 5, 2012), SOGP (Information Security Forum, 2014) και ITIL (IT Infrastructure Library, 2007).

Προσαρμογή αρχών προστασίας απορρήτου πληροφοριών για το BYOD

Οι αρχές για την προστασία της ιδιωτικότητας περιλαμβάνουν κατευθυντήριες γραμμές και διαδικασίες για την προστασία των ιδιωτικών και εμπιστευτικών πληροφοριών. Αυτές οι αρχές μπορούν επίσης να ελέγξουν τις παραβιάσεις της ιδιωτικότητας και την έκθεση προσωπικών

πληροφοριών σε περιβάλλοντα BYOD. Υπάρχουν διάφοροι τύποι αρχών για την προστασία της ιδιωτικότητας που είναι διεθνώς αναγνωρισμένοι και αποδεκτοί. Μεταξύ αυτών περιλαμβάνονται οι αρχές προστασίας της ιδιωτικότητας του Οργανισμού Οικονομικής Συνεργασίας και Ανάπτυξης (Organisation for Economic Co-operation and Development (OECD)) (OECD Publishing, 2002), οι οποίες αποτέλεσαν τη βάση για τη δημιουργία προγραμμάτων προστασίας της ιδιωτικότητας για την αντιμετώπιση των προβλημάτων εμπιστευτικότητας που σχετίζονται με τη χρήση της τεχνολογίας των πληροφοριών.

Προσαρμογή των τεχνικών ελέγχων ασφάλειας πληροφοριών και ιδιωτικού απορρήτου στο BYOD

Οι οργανισμοί που υιοθετούν το BYOD εξετάζουν τους τεχνικούς ελέγχους προκειμένου να μειώσουν τους κινδύνους και την πιθανότητα νομικών ζητημάτων και ζητημάτων αξιοπιστίας στις πρακτικές του BYOD (Rivera et al, 2013). Οι οργανισμοί πρέπει να διασφαλίζουν ότι οι έλεγχοι που επιβάλλονται ή χρησιμοποιούνται για τη διαχείριση του BYOD, δεν παραβιάζουν σημαντικούς κανονισμούς ή νόμους. Η εφαρμογή τεχνικών ελέγχων για την αντιμετώπιση των κινδύνων του BYOD μπορεί να έχει συγκεκριμένες επιπτώσεις στην εμπειρία των χρηστών του BYOD (users' experience). Οι πιο συνηθισμένοι μηχανισμοί τεχνικού ελέγχου που χρησιμοποιούν οι οργανισμοί για το BYOD είναι πλήρη συστήματα διαχείρισης κινητών συσκευών, τα οποία θεωρούνται παρεμβατικά και δίνουν υπερβολικό έλεγχο στους οργανισμούς (Dedeche et al, 2013). Ωστόσο, η αξιολόγηση των συστημάτων διαχείρισης του BYOD (Garba et al, 2015 (a)) έδειξε ότι ορισμένες προσεγγίσεις που αφορούν το δίκτυο, το Virtual Private Network (VPN), η κρυπτογράφηση δεδομένων, ο έλεγχος πρόσβασης μπορούν να εφαρμοστούν για τη διαχείριση του BYOD.

Καταγραφή των υποχρεώσεων για το BYOD

Οι υποχρεώσεις καθιστούν το BYOD όχι μόνο θέμα πληροφορικής, αλλά προκαλούν την ανησυχία των οργανωτικών και νομικών τμημάτων. Οι νομικές μονάδες πρέπει να διασφαλίζουν ότι τόσο ο οργανισμός όσο και οι κίνδυνοι ευθύνης των χρηστών του BYOD διαχειρίζονται και περιορίζονται. Όταν εκτίθενται εταιρικά ή προσωπικά δεδομένα, εκ προθέσεως ή όχι, ούτε ο εργαζόμενος ούτε ο οργανισμός θα θέλουν να είναι υπεύθυνοι. Κατά συνέπεια, κατά την εφαρμογή των μέτρων ελέγχου για το BYOD, η ευθύνη των χρηστών πρέπει να αξιολογηθεί για διαρροή εταιρικών δεδομένων και νομικές συνέπειες των ζημιών και η εταιρική ευθύνη έγκειται στην προστασία των προσωπικών δεδομένων των χρηστών του BYOD (Garba et al, 2015 (c)).

Προγράμματα ενημέρωσης και κατάρτισης για το BYOD

Τα ζητήματα ασφάλειας και ιδιωτικής ζωής του BYOD απαιτούν προγράμματα ενημέρωσης και κατάρτισης. Είναι πιθανό, όταν οι χρήστες του BYOD ενημερώνονται μέσω των προγραμμάτων κατάρτισης σχετικά με το ενδεχόμενο να διακυβεύεται η ταυτότητά τους κατά τη χρήση μιας κινητής συσκευής, θα είναι περισσότερο προσεκτικοί ως προς την ασφάλεια και την προστασία της ιδιωτικότητας (Harris et al, 2013). Ένα πρόγραμμα ευαισθητοποίησης και κατάρτισης σχετικά με την ασφάλεια και το ιδιωτικό απόρρητο του BYOD θα πρέπει να περιλαμβάνει δίκτυα, εφαρμογές πιθανές απειλές και τρωτά σημεία της ασφάλειας και της ιδιωτικότητας που βασίζονται στο διαδίκτυο. Αυτό είναι σημαντικό, καθώς οι χρήστες του BYOD δεν έχουν συνήθως την τάση να δέχονται πλήρη διαχείριση των φορητών συσκευών από τις εταιρείες τους (Garba et al, 2015 (b)). Τα προγράμματα κατάρτισης θα πρέπει να είναι προσαρμοσμένα ώστε να αποδεικνύουν επαρκώς τα τρωτά σημεία της συσκευής BYOD. Προκειμένου να αποφευχθούν οι χρήστες του BYOD να θεωρούν την κατάρτιση ως επιβάρυνση, οι συνεδρίες

του προγράμματος κατάρτισης πρέπει να είναι σύντομες και συνοπτικές και να παραμένουν αποτελεσματικές στη μετάδοση πληροφοριών στους χρήστες.

Αντίληψη της οπτικής και της συμπεριφοράς του χρήστη BYOD

Το BYOD μπορεί να έχει απροσδόκητο αντίκτυπο στις αντιλήψεις και τη συμπεριφορά των εργαζομένων όσον αφορά την αποδοχή των υποχρεώσεων και τους τεχνικούς ελέγχους που χρησιμοποιούν οι οργανισμοί. Έχει γίνει δεκτό στην έρευνα των συστημάτων πληροφοριών ότι οι αντιλήψεις των χρηστών σε σχέση με ένα συγκεκριμένο τεχνολογικό σύστημα καθορίζουν την πρόθεσή τους να το χρησιμοποιήσουν, γεγονός που καθορίζει επίσης τη συμπεριφορά τους (Venkatesh et al, 2003). Κατά τη διερεύνηση των μέτρων ασφαλείας και προστασίας της ιδιωτικής ζωής για το BYOD, είναι σημαντικό να εξετάζονται οι αντιλήψεις, τα χαρακτηριστικά και η συμπεριφορά των χρηστών, καθώς μπορούν να προσδιορίσουν εάν τα μέτρα είναι πιθανόν να είναι επιτυχημένα.

4.5 Συμπεράσματα

Η ασφάλεια και η προστασία των εταιρικών δεδομένων είναι μια συνεχής διαδικασία που απαιτεί προσοχή, διαχείριση, επανεξέταση και ευελιξία. Προκειμένου η ασφάλεια και η ιδιωτικότητα του BYOD να είναι επιτυχείς σε οργανισμούς, κάθε οργανωτική οντότητα οφείλει να κατανοεί και να εκτελεί τα καθήκοντά της κατάλληλα και έγκαιρα. Το τμήμα διαχείριση της ασφάλειας των πληροφοριών καθώς και το προσωπικό σε οργανισμούς θα πρέπει να είναι υπεύθυνοι για τη διατήρηση των πολιτικών ασφαλείας και ιδιωτικού απορρήτου του BYOD, συμπεριλαμβανομένης της ευαισθητοποίησης / κατάρτισης των εργαζομένων και της παροχής συμβουλών σχετικά με τα μέτρα και τις πρακτικές ασφάλειας. Επιπλέον, θα πρέπει να είναι υπεύθυνοι για την επικύρωση και την έγκριση συσκευών BYOD, καθώς και για την παρακολούθηση δικτύων για μη εξουσιοδοτημένη πρόσβαση, κυκλοφορία και άλλες απειλές.

Συνοπτικά, όπως είδαμε και παραπάνω, η διαχείριση του BYOD αφορά:

- τον καθορισμό και την κατανόηση των πρακτικών BYOD που υποστηρίζονται από την εκάστοτε εταιρεία
- τον εντοπισμό των πιθανών απειλών
- τον εντοπισμό των τρωτών σημείων και των περιστατικών διαρροής δεδομένων
- την εφαρμογή των σωστών διαδικασιών ή ελέγχων που είναι σύμφωνες με τις ορθές πρακτικές σχετικά με την κουλτούρα της εταιρείας καθώς και σύμφωνα με το υπάρχον νομοθετικό πλαίσιο.
- Η σωστή ενημέρωση και κατάρτιση του προσωπικού της εταιρείας σχετικά με την στρατηγική ελέγχου και προστασίας δεδομένων του BYOD.

Λαμβάνοντας υπόψη τον αυξανόμενο αριθμό των κινδύνων που σχετίζονται με το BYOD, οι οργανισμοί θα πρέπει να επανεξετάσουν την αποτελεσματικότητα των πλαισίων ασφάλειας και προστασίας των προσωπικών δεδομένων τους σε ένα ευρύ φάσμα που περιλαμβάνει: τεχνικούς ελέγχους, πολιτικές, πρότυπα και διαδικασίες, προγράμματα ευαισθητοποίησης / κατάρτισης των χρηστών σχετικά με τους κινδύνους ασφάλειας. Όλα αυτά μπορούν να συνδυαστούν για να αναπτυχθεί ένα πλαίσιο λύσης BYOD που περιλαμβάνει αρχιτεκτονική πολιτικής και κατευθυντήριες γραμμές για τους οργανισμούς.

Κεφάλαιο 5ο Enterprise mobility management

5.1 Τεχνικές λύσεις ασφάλειας BYOD

Είναι γεγονός πως πλέον οι οργανισμοί επιτρέπουν την ολοκλήρωση σχεδόν όλων των επιπέδων εργασίας από χώρους εκτός γραφείου. Οι εργαζόμενοι και οι εργοδότες επωφελούνται από την ευελιξία και την αποτελεσματικότητα που προκύπτουν όταν οι εργαζόμενοι μπορούν να εκτελέσουν τα καθήκοντά τους από χώρους εκτός εταιρείας. Ως εκ τούτου, η παροχή στους υπαλλήλους της δυνατότητας να εργάζονται εξ αποστάσεως είναι ένας εξαιρετικός τρόπος για μια εταιρεία να προσελκύσει και να διατηρήσετε μια ταλαντούχα, παραγωγική ομάδα.

Οι συσκευές και τα μέτρα ασφαλείας που χρησιμοποιούνται σε ολόκληρο τον οργανισμό διαδραματίζουν σημαντικό ρόλο στη διευκόλυνση της ασφαλούς και αποτελεσματικής απομακρυσμένης εργασίας. Δυστυχώς, μπορεί να είναι αρκετά δύσκολο να καθοριστεί σε ποιες συσκευές θα πρέπει να δοθεί πρόσβαση σε εταιρικά δεδομένα. Το τμήμα πληροφορικής του οργανισμού θα πρέπει να εξετάσει πώς οι πολιτικές συσκευών και οι λύσεις ασφάλειας επηρεάζουν την αποδοτικότητα των χρηστών, το απόρρητο των χρηστών και την ασφάλεια των εταιρικών δεδομένων.

Η αυξανόμενη δημοτικότητα του BYOD περιπλέκει την προσπάθεια της ασφαλούς απομακρυσμένης εργασίας. Μια προσωπική συσκευή, που χρησιμοποιείται για επαγγελματικές και προσωπικές δραστηριότητες, έχει πρόσβαση στο εταιρικό δίκτυο και στις προσωπικές εφαρμογές του χρήστη - αυξάνοντας την πιθανότητα πρόσβασης σε εταιρικά δεδομένα από μη εξουσιοδοτημένους χρήστες ή μολυσμένα από κακόβουλο λογισμικό. Τα smartphones, τα tablets, και γενικότερα τα φορητά εργαλεία του εργατικού δυναμικού αντιπροσωπεύουν ένα σημείο εισόδου για διαδικτυακές απειλές που εκμεταλλεύονται τις συσκευές για να στοχεύοντας εταιρικά δεδομένα.

Για την ασφάλεια των κινητών συσκευών και του BYOD, το τμήμα ασφάλειας πληροφοριών του οργανισμού μπορεί να επιλέξει από μια μεγάλη ποικιλία λύσεων για την ασφάλεια των κινητών συσκευών και τη διαχείριση δεδομένων. Ωστόσο, ο μεγάλος αριθμός επιλογών μπορεί να οδηγήσει σε υπερβολές. Ως εκ τούτου, οι οργανισμοί θα πρέπει να εξετάσουν τις παρακάτω λύσεις κατά την επιλογή μιας στρατηγικής ασφάλειας κινητής τηλεφωνίας.

5.1.1 Βασικές κατηγορίες τεχνικών λύσεων ασφάλειας BYOD

Mobile Device Management (MDM)

Οι λύσεις διαχείρισης κινητών συσκευών (MDM) ευνοούνται γενικά από μεγάλες επιχειρήσεις που επιδιώκουν την εφαρμογή των πολιτικών ασφάλειας σε μεγάλο αριθμό εταιρικών συσκευών. Τυπικά, οι λύσεις MDM απαιτούν εγκατάσταση λογισμικού σε όλες τις συσκευές των εργαζομένων. Αυτό επιτρέπει στους IT administrators της εταιρείας να διαχειρίζονται όλες τις συσκευές που έχουν πρόσβαση στα εταιρικά δεδομένα και να εφαρμόζουν τεχνικές ασφάλειας όπως κωδικούς πρόσβασης, remote data wiping, απόρριψη μη ασφαλών δικτύων WLAN και πολλά άλλα.

Ωστόσο, ένα σημαντικό πρόβλημα μπορεί να προκύψει με το MDM, εάν το περιβάλλον κινητής τηλεφωνίας είναι ετερογενές ή περιέχει διαφορετικές κινητές συσκευές και λειτουργικά συστήματα. Σε αυτά τα διαφορετικά περιβάλλοντα, οι λειτουργίες διαχείρισης συσκευών είναι

συχνά μη διαθέσιμες για ορισμένες από τις συσκευές των εργαζομένων. Επειδή τα ετερογενή κινητά συστήματα είναι δύσκολο να εξασφαλιστούν με το MDM, είναι απαραίτητο οι οργανισμοί να εμπλέκουν τους εργαζομένους σε πρώιμο στάδιο της εφαρμογής του MDM. Αυτό βοηθά τους οργανισμούς να αξιολογήσουν εάν η λύση MDM υποστηρίζει όλες τις ροές εργασίας των εργαζομένων και εάν η ανάπτυξη θα είναι υπερβολικά δύσκολη για ορισμένες συσκευές.

Ενώ οι λύσεις MDM μπορούν να εξασφαλίσουν συσκευές που ανήκουν σε στις εταιρείες, οδηγούν παρόλα αυτά σε προκλήσεις ιδιωτικού απορρήτου όταν αναπτύσσονται σε προσωπικές κινητές συσκευές. Αυτές οι λύσεις μπορούν να επιτρέψουν σε εταιρείες να επαναφέρουν τις ρυθμίσεις της συσκευής, να προσδιορίσουν τις τοποθεσίες συσκευών και να συλλέξουν πληροφορίες σχετικά με τη χρήση της συσκευής και του τρόπου χρήσης του διαδικτύου. Όταν αυτές οι δυνατότητες χρησιμοποιούνται σε προσωπικές συσκευές, θεωρείται συχνά ως εισβολή στην ιδιωτική ζωή των χρηστών. Ως αποτέλεσμα, πολλοί υπάλληλοι αρνούνται να εγκαταστήσουν οποιοδήποτε λογισμικό ασφαλείας στα τηλέφωνά τους ή τα tablet, δημιουργώντας σημαντικές προκλήσεις για την ασφάλεια των επιχειρήσεων.

Mobile Application Management (MAM)

Σε αντίθεση με το MDM, η διαχείριση εφαρμογών για κινητά (MAM) επικεντρώνεται στην παροχή εφαρμογών, οι οποίες θα διαχειρίζονται ευαίσθητα δεδομένα. Όπου επιτρέπεται το BYOD, το MAM χρησιμοποιείται περιστασιακά για την εξασφάλιση της πρόσβασης σε δεδομένα μέσω κινητού τηλεφώνου. για παράδειγμα, όταν ένας πωλητής χρησιμοποιεί μια εταιρική εφαρμογή στο προσωπικό του τηλέφωνο για να αποκτήσει πρόσβαση σε συστήματα διαχείρισης σχέσεων πελατών (CRM). Για να εξασφαλιστεί ότι τα εταιρικά δεδομένα είναι επαρκώς προστατευμένα, οι εφαρμογές που έχουν πρόσβαση σε δεδομένα της εταιρείας διαχειρίζονται από το προσωπικό του τμήματος IT της εταιρείας.

Ωστόσο, το MAM έχει πολλαπλούς περιορισμούς. Παρόλο που το MAM μπορεί να εφαρμοστεί σε μια σειρά από εταιρικές εφαρμογές, δεν καλύπτει τις δημοφιλείς cloud εφαρμογές όπως το Gmail, το Dropbox και το Slack. Όπως οι λύσεις MDM που εφαρμόζονται στις συσκευές, η ανάπτυξη του MAM απαιτεί την εγκατάσταση λογισμικού στις συσκευές των εργαζομένων. Επιπλέον, καθώς η λύση δεν παρέχει άμεση διαχείριση συσκευών, πρέπει να εγκατασταθεί μια πολιτική χρήσης σε κάθε συσκευή.

Agentless Mobile Security

Σε αντίθεση με τα παραπάνω υπάρχουν λύσεις ασφάλειας για κινητές συσκευές, οι οποίες μπορούν να προστατεύσουν τα δεδομένα χωρίς να απαιτούν την εγκατάστασή τους στις συσκευές των εργαζομένων. Παρόλο που δεν απαιτούνται ενέργειες σε μεμονωμένες συσκευές, αυτές οι λύσεις μπορούν ακόμα να παρέχουν λειτουργίες MDM όπως την πρόληψη της απώλειας δεδομένων και την απομακρυσμένη διαγραφή δεδομένων της εταιρείας από συσκευές BYOD. Προσφέρουν επίσης κρυπτογράφηση δεδομένων, η οποία μπορεί να επεκταθεί σε όλες τις δημοφιλείς cloud εφαρμογές, όπως το G Suite, το Office 365 και το Salesforce. Αυτό σημαίνει ότι τα ευαίσθητα δεδομένα είναι ασφαλή ανεξάρτητα από την εφαρμογή στην οποία είναι αποθηκευμένα ή από τη συσκευή μέσω της οποίας παρέχεται η πρόσβαση σε αυτά.

Μέσω αυτών των λύσεων, οι διαχειριστές ασφαλείας μπορούν να ελέγχουν την πρόσβαση των συσκευών στις εταιρικές πληροφορίες χωρίς την εγκατάσταση επιπλέον λογισμικού. Ως αποτέλεσμα, προσφέρουν γρήγορη ανάπτυξη και αποφεύγονται οι ανησυχίες των χρηστών σχετικά με την ιδιωτικότητάς τους και με την πρόσβαση των εργοδοτών στις προσωπικές τους πληροφορίες. Με βάση τα παραπάνω, οι λύσεις αυτές υιοθετούνται συχνά από επιχειρήσεις που επιδιώκουν την εξασφάλιση δεδομένων εταιρικού cloud, καθώς έχουν πρόσβαση σε μια

ποικιλία συσκευών. Με την αυξανόμενη δημοτικότητα των cloud υπηρεσιών και του BYOD, η υιοθέτηση τέτοιου είδους λύσεων θα συνεχίσει να αυξάνεται.

Οι οργανισμοί πρέπει να εξετάσουν πολλούς παράγοντες κατά την επιλογή μιας στρατηγικής ασφάλειας κινητών συσκευών. Πρώτον, οι διαχειριστές πρέπει να συντάξουν έναν μεγάλο κατάλογο των κυβερνητικών κανονισμών που αφορούν τις επιχειρήσεις τους. Από εκεί, πρέπει να διασφαλίσουν ότι η ανάπτυξη στρατηγικής ασφάλειας δεν θα παρεμποδιστεί από χρήστες που θέλουν να διατηρήσουν τα προσωπικά τους δεδομένα ιδιωτικά. Με βάση τις κλιμακούμενες τάσεις του BYOD, οι οργανισμοί θα πρέπει επίσης να καταγράψουν τις συσκευές και τα λειτουργικά συστήματα που χρησιμοποιούνται, καθώς και τις ανάγκες των εργαζομένων για κινητές εφαρμογές. Τέλος, όλοι οι ενδιαφερόμενοι οφείλουν να συμμετέχουν στη διαδικασία λήψης αποφάσεων προκειμένου να εξασφαλιστεί η υιοθέτηση μιας λύσης ασφάλειας για κινητά δίκτυα που να είναι δίκαιη και αποτελεσματική για όλους.

(CSOonline, 2017)

5.1.2 Τεχνολογίες ασφάλειας για BYOD

Virtual Desktop Infrastructure (VDI) και Containerization

Μια δημοφιλής μέθοδος ασφάλειας βασισμένη στο λογισμικό που κερδίζει έδαφος σε περιβάλλοντα BYOD είναι η Virtual Hosted Desktop (VHD). Το VHD (γνωστό και ως Virtual Desktop Infrastructure ή VDI) δημιουργεί μια πλήρη επιφάνεια εργασίας που περιλαμβάνει ένα λειτουργικό σύστημα, όλες τις εφαρμογές και τις ρυθμίσεις. Η φιλοξενούμενη επιφάνεια εργασίας μπορεί να προσεγγιστεί από οποιοδήποτε συμβατό μηχάνημα και η επεξεργασία και η αποθήκευση πραγματοποιούνται σε κεντρικό διακομιστή. Με αρκετό εύρος ζώνης δικτύου και ισχυρό εξοπλισμό, αυτός ο τύπος εικονικού περιβάλλοντος μπορεί να συνδυάσει αποδεκτή απόδοση με υψηλά επίπεδα ασφάλειας.

Το Containerization είναι ένας τρόπος αντιμετώπισης των προβλημάτων του VHD τοποθετώντας native εφαρμογές στην συσκευή. Ένας διαχειριστής εικονικών μηχανών (virtual machine manager VMM) επωμίζεται την εκτέλεση και την διαχείριση της λειτουργικότητας της εφαρμογης, ενισχύοντας την απόδοση και μειώνοντας την κατανάλωση πόρων διακομιστή, επιτρέποντας την εκτέλεση από την πλευρά του πελάτη (client-side execution) - βελτιώνοντας ταυτόχρονα την ασφάλεια απομονώνοντας την τελική συσκευή από ορισμένες λειτουργίες, όπως ασύρματες συνδέσεις δικτύου, κάμερες. Ορισμένα εικονικά περιβάλλοντα περιέχουν ολόκληρο το λειτουργικό σύστημα και τη σουίτα εταιρικών εφαρμογών, ενώ άλλα είναι εικονικές συσκευές μιας χρήσης που παρέχουν υπηρεσίες όπως παρακολούθηση ή εφαρμογές υψηλής ασφάλειας.

Chipset Level Security Technologies

Οι τεχνολογίες ασφάλειας σε επίπεδο chipset επιτρέπουν στο MDM να φτάσει μέσα στο λειτουργικό σύστημα μιας διαχειριζόμενης συσκευής, εκτελώντας απομακρυσμένα σαρώσεις ιού πριν από την εκκίνηση, ανεξάρτητα από την κατάσταση της συσκευής. Παρέχοντας πρόσβαση στο λειτουργικό σύστημα, η τεχνολογία αυτή επιτρέπει στους διαχειριστές να διορθώνουν προβλήματα εγκαθιστώντας κώδικες λογισμικού (software patches) και η ολοκληρωμένη υποστήριξή δημόσιων κλειδιών (Public Key Infrastructure PKI) επιτρέπει στο IT της εταιρείας να χρησιμοποιεί τις ίδιες τις συσκευές για τον έλεγχο ταυτότητας χρηστών. Η τεχνολογία Anti-Theft από κάποιον αξιόπιστο προμηθευτή επεκτείνει τα χαρακτηριστικά ασφαλείας όπως το απομακρυσμένο, ανεξάρτητο από το λειτουργικό σύστημα κλείδωμα και ξεκλείδωμα των συσκευών στους επεξεργαστές.

Network Access Control (NAC)

Η τεχνολογία που επιτρέπει στους εργαζόμενους να χρησιμοποιούν τις προσωπικές τους συσκευές στο δίκτυο παρέχοντας ταυτόχρονα την ασφάλεια και τον έλεγχο πρόσβασης που απαιτεί η επιχείρηση. Η προσέγγιση αυτή συνδυάζει τις λεπτομερείς πολιτικές πρόσβασης, την αυτοματοποιημένη εφαρμογή και την πλήρη ορατότητα σε κάθε συσκευή και χρήστη στο δίκτυο. Χρησιμοποιεί λύσεις λογισμικού και υλικού για να διαχειριστεί τις συσκευές ενώ ταυτόχρονα διαφυλάσσει τα εταιρικά δεδομένα. Τα ασύρματα δίκτυα πρέπει να κατασκευαστούν για ασφαλή πρόσβαση του BYOD και ο τρόπος για να γίνει αυτό είναι η υλοποίηση του NAC για κινητές συσκευές

Data Loss Prevention (DLP)

Η ανάπτυξη αυτών των πρακτικών επιτρέπει στους διαχειριστές να παρακολουθούν την κυκλοφορία δεδομένων και να αποκλείουν αμέσως τους ύποπτους χρήστες ή τη δραστηριότητα. Για παράδειγμα, οι διαχειριστές παρατήρησαν ότι η κυκλοφορία με "xxx-xx-xxx" στη συμβολοσειρά της πρέπει να παρεμποδιστεί, καθώς θα μπορούσε να υποδηλώνει ότι μεταδίδεται ένας αριθμός κοινωνικής ασφάλισης.

Τα εργαλεία DLP μπορούν να εφαρμόσουν μια πολιτική χρήσης για τις πληροφορίες που δημιουργούνται, ανεξάρτητα από το αν πρόκειται για αρχείο, για email ή για εφαρμογή. Αυτό σημαίνει ότι τα δεδομένα, κατά τη χρήση ή τη μεταφορά τους μπορούν να καταγραφούν, να αναφερθούν σε ετικέτες και να κρυπτογραφηθούν σε οποιοδήποτε στάδιο, διασφαλίζοντας την πρόληψη μη εξουσιοδοτημένης δραστηριότητας. Καθώς περισσότερες επιχειρήσεις επιτρέπουν στους εργαζομένους την ελευθερία πρόσβασης στην εταιρική βάση δεδομένων από μια προσωπική συσκευή, οι τεχνολογίες DLP θα είναι επιτακτικές για τη διατήρηση της ασφαλούς διαχείρισης δεδομένων.

(Ciso Platform)

5.1.3 Θετικά και αρνητικά τεχνολογιών ασφάλειας BYOD

Virtual Desktop Infrastructure (VDI)

- **Πλεονεκτηματα**

1. Το VDI και η ροή εφαρμογών βοηθούν στην αντιμετώπιση προβλημάτων του BYOD επειδή εκτελούν εφαρμογές και εικονικά λειτουργικά συστήματα σε back-end servers και όχι στις τελικές συσκευές.
2. Οι συσκευές επικοινωνούν με servers που φιλοξενούν το λειτουργικό σύστημα και τις εφαρμογές, έτσι ώστε οι πόροι που αποστέλλονται στις συσκευές να είναι συμβατοί και ασφαλείς. Με αυτόν τον τρόπο, οι συσκευές λαμβάνουν τις εφαρμογές και τα δεδομένα που χρειάζονται οι χρήστες για να δουλέψουν. Το μόνο που χρειάζονται οι χρήστες είναι μια εφαρμογή στις συσκευές τους για να ανοίξει τη σύνδεση με το διακομιστή VDI.
3. Χρησιμοποιώντας το VDI και το BYOD μαζί, απελευθερώνει τους υπαλλήλους του IT από την διαχείριση του hardware.

- **Μειονεκτήματα**

1. Οι κινητές συσκευές δεν πληρούν πάντα τις απαιτήσεις υλικού (hardware requirements) που απαιτούνται για την εκτέλεση εικονικών μηχανών (virtual desktops).
2. Παρά το γεγονός ότι το VDI διευκολύνει τη διαχείριση της συσκευής με τεχνολογία πληροφορικής και αυξάνει θεωρητικά την παραγωγικότητα, οι προκλήσεις στον τομέα

της εικονικοποίησης μπορούν να δυσκολέψουν τους χρήστες στην δουλειά τους. Η προσπάθεια να χρήσης του VDI στις οθόνες αφής μπορεί να είναι ιδιαίτερα δύσκολη.

3. Για να χρησιμοποιήσουν μια απομακρυσμένη επιφάνεια εργασίας, οι χρήστες tablet χρειάζονται τα πληκτρολόγια και τα ποντίκια με τον ίδιο τρόπο που θα κάνανε αν κάθονταν στους υπολογιστές τους.

Chipset Level Security Technologies

- Πλεονεκτηματα

1. Εκτεταμένη πολιτική ασφάλειας.
2. Περιλαμβάνονται επιπλέον έλεγχοι.
3. Παρέχεται μια πλατφόρμα για τη διαχείριση όλων των συσκευών smartphone και tablet.

- Μειονεκτήματα
    1. Δεν υπάρχει διαχωρισμός προσωπικών και εταιρικών δεδομένων.
    2. Επιπλέον κόστος.

Network Access Control (NAC)

- Πλεονεκτηματα

1. Ελεγχος στον ρόλο του χρήστη (Role Based Access Control). Σημαίνει πως το δίκτυο πρέπει να αναγνωρίσει την ταυτότητα του χρήστη και να του επιτρέπει μόνο την πρόσβαση στους πόρους που είναι του απαραίτητοι εφαρμόζοντας τον κατάλληλο User Role. Για παράδειγμα: ένα ασύρματο δίκτυο πανεπιστημιουπόλεων με το NAC θα έχει ένα ρόλο φοιτητή, καθηγητή και επισκέπτη. Κάθε ένα με το συγκεκριμένο σύνολο προνομίων, προβάσεων αλλά και περιορισμών που τους αρμόζει.
2. Επιβολή πολιτικών ασφαλείας - Αυτό ονομάζεται "έλεγχος ακεραιότητας" ή "endpoint compliance". Για παράδειγμα: Έλεγχος αν έχει η τελική συσκευή anti-virus. Έλεγχος αν έχει η τελική συσκευή τις πιο πρόσφατες ενημερώσεις. Αυτές είναι μερικές από τις πολιτικές που ελέγχονται από τον παραδοσιακό έλεγχο πρόσβασης.

- Μειονεκτήματα

1. Αυτές οι συσκευές είναι ιδιαίτερα ευάλωτες μέσω των «τρυπών» ευπάθειας και έκθεσης και είναι πολύ πιθανό να μολυνθούν με λογισμικό υποκλοπής.
2. Εκτός από τη συνδεσιμότητα WIFI, μπορούν να λειτουργούν ταυτόχρονα σε κυψελοειδή δίκτυα, αφήνοντας έτσι μια ανομοιογενή τρύπα κινδύνου στον τομέα της κλοπής δεδομένων και των διαρροών
3. Είναι πιθανό να περιέχουν και να μεταφέρουν εταιρικά δεδομένα, όπως αρχεία πελατών, λίστες επαφών, υπολογιστικά φύλλα, έγγραφα, παρουσιάσεις κλπ., Τα οποία ενδέχεται να κινδυνεύουν από κλοπή μέσω κακόβουλου λογισμικού κλοπής δεδομένων ή απώλειας/κλοπής του εξοπλισμού.

Data Loss Prevention (DLP)

- Πλεονεκτηματα

1. Το DLP εμποδίζει είτε την τυχαία αποκάλυψη εταιρικών δεδομένων η οποία είναι πιθανό να συμβεί είτε τυχαία είτε από υπάλληλο της εταιρείας που αποστέλλει δεδομένα σε κάποιον εκτός της εταιρείας.
2. Παρακολούθηση σε πραγματικό χρόνο και αποφυγή κινδύνου πρόσβασης ή αποστολής ευαίσθητων δεδομένων από κινητές συσκευές

- Μειονεκτήματα

1. Σε περίπτωση που δεν εφαρμοστούν σωστά οι κανόνες μπορεί να επηρεάσουν αρνητικά την εμπειρία χρήστη (user experience) του BYOD.

5.2 Enterprise mobility management (EMM)

Η διαχείριση του enterprise mobility (Enterprise mobility management, EMM) είναι λογισμικό που επιτρέπει στους οργανισμούς να παρέχουν με ασφάλεια τη χρήση των φορητών συσκευών και εφαρμογών στους εργαζομένους.

Εκτός από την αντιμετώπιση προβλημάτων ασφάλειας, το λογισμικό EMM βοηθά τους υπαλλήλους να είναι πιο παραγωγικοί, επειδή το τμήμα πληροφορικής μπορεί να τους παρέχει τις εφαρμογές και τα δεδομένα που χρειάζονται για την εκτέλεση εργασιών στις κινητές συσκευές.

Το EMM εξελίχθηκε από τη διαχείριση των κινητών συσκευών (mobile device management, MDM), η οποία εστιάζει αποκλειστικά στον έλεγχο και την ασφάλεια σε επίπεδο συσκευών. Μετά την έκδοση των Windows 10 της Microsoft το 2015, οι περισσότεροι πάροχοι λογισμικού EMM επεκτάθηκαν σε ενοποιημένη διαχείριση συσκευών (unified endpoint management UEM), η οποία επιτρέπει στο τμήμα IT να διαχειρίζεται υπολογιστές και κινητές συσκευές μέσω μιας ενιαίας κονσόλας.

5.2.1 Εξέλιξη EMM

Το EMM περιλαμβάνει συνήθως κάποιο συνδυασμό διαχείρισης κινητών συσκευών (mobile device management, MDM), διαχείρισης κινητών εφαρμογών (mobile application management MAM), διαχείρισης περιεχομένου κινητού (mobile content management MCM) και διαχείρισης ταυτότητας και πρόσβασης (identity and access management). Αυτές οι τέσσερις τεχνολογίες ξεκίνησαν ως μεμονωμένα προϊόντα, αλλά είναι όλο και περισσότερο διαθέσιμες συνδυαστικά μέσω μεγαλύτερων προγραμμάτων λογισμικού EMM.

Τα περισσότερα λογισμικά enterprise mobility ξεκίνησα από MDM. Πρόκειται για τον συνδυασμό μιας εφαρμογής, η οποία είναι εγκατεστημένη σε μια ατομική συσκευή, και του server που εκτελείται στο εταιρικό κέντρο δεδομένων ή στο cloud. Οι διαχειριστές χρησιμοποιούν την κονσόλα διαχείρισης του MDM για να ορίσουν πολιτικές και να διαμορφώσουν τις ρυθμίσεις μέσω του API που βρίσκεται στις κινητές συσκευές.

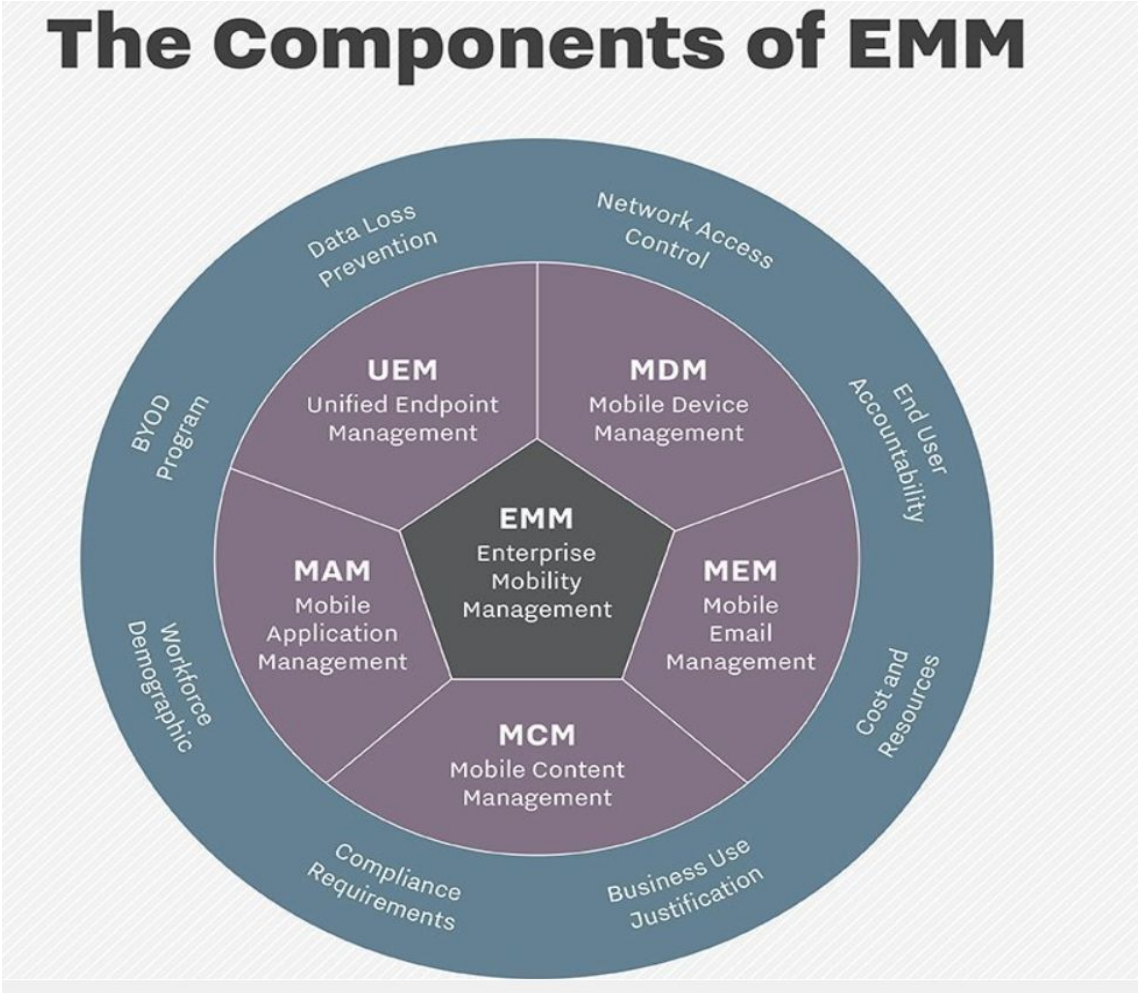
Το MAM παρέχει πιο λεπτομερή διαχείριση και ασφάλεια. Επιτρέπει στους διαχειριστές να ορίζουν πολιτικές για συγκεκριμένη εφαρμογή ή υποσύνολο εφαρμογών και όχι για ολόκληρη τη συσκευή. Ορισμένες εφαρμογές έχουν ενσωματωμένα συγκεκριμένα API MAM, ενώ άλλα βασίζονται στα API MAM σε επίπεδο συσκευής στα περισσότερα μεγάλα λειτουργικά συστήματα κινητής τηλεφωνίας.

Με το MCM, μόνο εγκεκριμένες εφαρμογές μπορούν να έχουν πρόσβαση σε εταιρικά δεδομένα. Και η διαχείριση της ταυτότητας και της πρόσβασης ελέγχει τον τρόπο που οι εργαζόμενοι μπορούν να χρησιμοποιούν εταιρικές εφαρμογές και δεδομένα, ενώ παράλληλα προσφέρουν και κάποιες φιλικές προς το χρήστη λειτουργίες, όπως η ενιαία σύνδεση.

Όλες αυτές οι τεχνολογίες καλύπτουν συγκεκριμένες ανάγκες και η επικάλυψη μεταξύ των MDM, MAM και MCM είναι πολύ μικρή. Δεδομένου ότι περισσότεροι οργανισμοί χρησιμοποιούν λογισμικά enterprise mobility, ξεκίνησε η ανάπτυξη λογισμικών EMM, συνήθως προσθέτοντας χαρακτηριστικά MAM ή MCM στα προϊόντα MDM.

Η Microsoft δημιούργησε MDM APIs στα Windows 10, το οποίο βοήθησε τα λογισμικά EMM στη διαχείριση των υπολογιστών με τον ίδιο τρόπο που διαχειρίζονται τα smartphones και τα tablet. Η Apple επιτρέπει, επίσης, τη διαχείριση των επιτραπέζιων και φορητών υπολογιστών MacOS με αυτόν τον τρόπο. Όλοι οι μεγάλοι προμηθευτές EMM υποστηρίζουν αυτή τη λειτουργία, σημειώνοντας μια μεταστροφή της αγοράς από το EMM σε UEM.
(TechTarget.com)

Εικόνα 5.1 Σχεδιάγραμμα EMM



(Πηγή: techtarget.com)

5.2.2 Λογισμικά EMM

Το 2017, η Gartner ονόμασε τέσσερις βασικούς προμηθευτές - VMware, MobileIron, IBM και BlackBerry - στο Magic Quadrant της. Η IDC, η οποία κατατάσσει τους προμηθευτές με βάση τις δυνατότητες και τις στρατηγικές τους, κατονόμασε τους VMware, MobileIron, BlackBerry, IBM

και Citrix ως ηγέτες. Και η Strategy Analytics δημοσίευσε αυτά τα στοιχεία για τα μερίδια αγοράς:

- VMware: 19%
- BlackBerry: 18%
- MobileIron: 10%
- Citrix: 9%
- Microsoft: 9%
- others: 35%

VMware

Τον Σεπτέμβριο του 2016, η Dell Technologies ολοκλήρωσε την εξαγορά της EMC, η οποία περιελάμβανε τη VMware. Η AirWatch έχει συγχωνευθεί πλήρως στην επιχειρηματική μονάδα End-User Computing της VMware και έχει γίνει πιο ολοκληρωμένη με διάφορες τεχνολογίες VMware, κυρίως IAM (Identity and Access Management) του VMware και προϊόντα λογισμικού που καθορίζονται από το λογισμικό (software-defined networking, SDN), δημιουργώντας μια κοινή λύση γνωστή ως Workspace One . Ωστόσο, αυτή η κοινή λύση χρησιμοποιήθηκε ελάχιστα λόγω του μικρού της χρόνου στην αγορά.

Η VMware AirWatch έχει κάνει σημαντικά βήματα προς την κατεύθυνση της εμφάνισης ενός πλήρους UEM, με σημαντική πρόοδο στη διαχείριση των Windows 10 και macOS σε μια ενιαία κονσόλα. Η ίδια η κονσόλα είναι μια από τις πιο εύχρηστες, με ενσωματωμένα εκπαιδευτικά βίντεο βοηθόντας τους νέους διαχειριστές να γίνουν παραγωγικοί γρήγορα. Η VMware έχει επεκταθεί σε IoT (Internet of Things) με ένα νέο προϊόν που ονομάζεται VMware Pulse IoT Center, το οποίο αξιοποιεί την τεχνολογία AirWatch καθώς έχει εκτεταμένη λειτουργικότητα για να υποστηρίξει ένα ευρύ φάσμα συστημάτων IoT και συνδεδεμένων συσκευών.

Ο συνδυασμός του VMware AirWatch, της διαχείρισης δεδομένων της EMC και των δυνατοτήτων υπηρεσιών και υλικού της Dell, θέτει το VMware σε ισχυρή θέση για να αντιμετωπίσει τις προκλήσεις του UEM. Το VMware AirWatch εμφανίζεται πιο συχνά στους καταλόγους προμηθευτών EMM των πελατών του Gartner. Το VMware AirWatch είναι μια καλή εφαρμογή για οργανισμούς που απαιτούν μια ολοκληρωμένη λειτουργία EMM σε ένα ευρύ φάσμα πλατφορμών, συμπεριλαμβανομένων κινητών τηλεφώνων, tablet, υπολογιστών και προηγμένων συσκευών IoT.

BlackBerry

Το 2016, το BlackBerry ολοκλήρωσε την ενσωμάτωση της Good Technology με το BlackBerry Enterprise Server (BES). Το BlackBerry Enterprise Server v.12.6, το οποίο είναι τώρα ο BlackBerry Unified Endpoint Manager (UEM), κυκλοφόρησε τον Δεκέμβριο του 2016. Η UEM σηματοδοτεί την προσπάθεια της BlackBerry να επεκτείνει τις υπάρχουσες δυνατότητές της για τη διαχείριση συσκευών PC, Mac και Internet of Things (IoT) συσκευές. Το BlackBerry διαθέτει μια ενιαία ολοκληρωμένη λύση με το BlackBerry Enterprise Mobility Suite, το οποίο περιλαμβάνει BlackBerry UEM, πλατφόρμα και εφαρμογές BlackBerry Dynamics, BlackBerry Enterprise Identity και BlackBerry Workspaces.

Η απόκτηση και η επιτυχημένη ενσωμάτωση του Good Technology αποδείχθηκε σωστή καθώς το BlackBerry απέκτησε άμεση αξιοπιστία ως ένα εργαλείο διαχείρισης πολλαπλών πλατφορμών και γνώρισε σταθερή χρήση το 2016. Η ανακατασκευή του PIM Good Work ως BlackBerry Work και των δυνατοτήτων του ως πάροχο Network Operations Center (NOC), μαζί με βελτιώσεις προϊόντων, συνέβαλαν στη διατήρηση του παραδοσιακά προτιμώμενου

προιοντος με τακτικούς και υψηλής ασφάλειας πελάτες, ιδιαίτερα στον οικονομικό και τραπεζικό τομέα. Ωστόσο, ορισμένοι πελάτες εξέφρασαν την ανησυχία τους για το προγραμματισμένο τέλος του Good for Enterprise, το οποίο έχει προγραμματιστεί για τον Αύγουστο του 2017.

Η BlackBerry έφερε στην αγορά μία από τις πιο αξιόπιστες προσφορές στον χώρο του IoT που διαχειρίζεται το EMM με το προϊόν Radar BlackBerry, μια λύση διαχείρισης περιουσιακών στοιχείων που κατασκευάστηκε για τη βιομηχανία φορτηγών για διαχείριση ρυμουλκούμενων, πλαισίων και εμπορευματοκιβωτίων. Αν και μια εξειδικευμένη λύση, αποτελεί μια αρχική υλοποίηση για την end-to-end IoT διαχείρηση . Παρόλο που η Gartner αναμένει ότι μόνο ένα μικρό τμήμα της αναδυόμενης αγοράς IoT θα είναι κατάλληλο για διαχείριση με το EMM, το Radar παρέχει μια υπηρεσία σε μια αγορά στην οποία οι περισσότεροι άλλοι πάροχοι έχουν μόνο φιλοδοξίες. Το BlackBerry UEM είναι μια καλή εφαρμογή για οργανισμούς με αυστηρές απαιτήσεις ασφάλειας, σε εταιρείες που χρειάζονται να προσφέρουν εφαρμογές και περιεχόμενο χωρίς να διαχειρίζονται ολόκληρη τη συσκευή.

MobileIron

Η MobileIron είναι μια εταιρεία που εξακολουθεί να είναι ένας από τους λίγους ανεξάρτητους παρόχους EMM. Το MobileIron EMM προσφέρει πλήρη υποστήριξη για το iOS, το Android και τα Windows 10 από την αρχή, όχι όμως και για macOS. Το MobileIron έχει επικεντρωθεί στη διαχείριση smartphones, tablet και υπολογιστών.

Το MobileIron χρησιμοποιείται συνήθως ως κεντρικό σημείο ανάπτυξης πολιτικών για κινητά, λόγω των πολλών δυνατοτήτων ενσωμάτωσής του με συστατικά στοιχεία της υποδομής, όπως αρχές πιστοποίησης, πληροφορίες ασφάλειας και διαχείρισης συμβάντων (security information and event management SIEM), έλεγχοι πρόσβασης δικτύου (network access controls NAC) και το AppConfig. Η MobileIron έχει επεκτείνει την δραστηριότητάς της στην βιομηχανία διαχείρισης λογισμικού λόγω σημαντικών βημάτων στον τομέα της ασφάλειας μέσω πιστοποιήσεων όπως η Common Criteria Certification for Mobile Device Management Protection Profile Version 2.0 (MDMPP V2.0), το Πρόγραμμα Διαχείρισης Κινδύνων και Εξουσιοδότησης Federal Risk and Authorization Management Program (FedRAMP).

Citrix

Το 2017, διατηρώντας παράλληλα την χρήση του XenMobile ως ανεξάρτητο προϊόν, η Citrix πραγματοποίησε σημαντική ανακοίνωση συνεργασίας με τη Microsoft για τη διάθεση της λύσης XenMobile σε πελάτες που χρησιμοποιούν το προϊόν Intune EMM της Microsoft. Σε αυτά τα σενάρια, το Citrix τοποθετεί το XenMobile EMM ως πρόσθετο εργαλείο στο Intune όταν το τελευταίο αναπτύσσεται σε διαμόρφωση "χωρίς εγγραφή". Η σουίτα εφαρμογών κινητής τηλεφωνίας της Citrix μπορεί επίσης να είναι διαχειρίσιμη τώρα χρησιμοποιώντας τους ελέγχους Microsoft Intune MAM. Η Citrix συνεχίζει να προσθέτει στα προϊόντα EMM, ενσωματώνοντας την διαχείριση των IoT και της τεχνολογίας ανάλυσης που προστίθεται στη Citrix μέσω της εξαγοράς του Octoblu.

Οι ευρύτερες δυνατότητες διαχείρισης του endpoint της Citrix επικεντρώνονται στα περιβάλλοντα desktop και στις εφαρμογές που παρέχονται μέσω των Citrix virtualization. Το XenMobile παραμένει κατάλληλο για οργανισμούς με υπάρχουσα τεχνολογία Citrix virtualization.

Microsoft

Το 2016, η Gartner είδε το ευρύτατο ενδιαφέρον για το Enterprise Mobility + Security (EMS) να μεταφράζεται σε έναν αυξανόμενο αριθμό εφαρμογών, καθώς το προϊόν συνέχισε να εξελίσσεται σε χαρακτηριστικά και λειτουργικότητα. Η μετανάστευση των χρηστών στην

πλατφόρμα Azure, η οποία ξεκίνησε τον Δεκέμβριο του 2016 ως "Intune στο Azure Portal Preview" και έγινε γενικά διαθέσιμη τον Μάιο του 2017, αποτέλεσε βασικό ορόσημο που επέτρεψε στη Microsoft να αντιμετωπίσει πολλές από τις ιστορικές αδυναμίες του προϊόντος. Βασικό στοιχείο μεταξύ αυτών των βελτιώσεων είναι η μακρόχρονη ανανέωση της πύλης Intune Admin με βάση το Silverlight και η κατακερματισμένη εμπειρία διαχείρισης με την πύλη Azure, η οποία περιλαμβάνει βελτιωμένες δυνατότητες διοικητικής εξουσιοδότησης και πλήρη υποστήριξη για τις διαχειριζόμενες επιλογές διαμόρφωσης για τις εφαρμογές του καταστήματος Google Play. Οι πελάτες με υβριδικές εφαρμογές (ενσωματωμένες στο System Center Configuration Manager [SCCM]) δεν επηρεάζονται από αυτήν την ενημερωμένη έκδοση. Οι νέοι αυτοτελείς πελάτες θα έχουν πρόσβαση σε αυτές τις λειτουργίες αμέσως.

Τα API Intune περιλαμβάνονται τώρα στο Microsoft Graph. Τα API θα παρέχουν μια διασύνδεση για την ενσωμάτωση προμηθευτών EMM για τη διαχείριση των εφαρμογών του Office 365, αλλά θα εξακολουθούν να απαιτούν άδεια Intune ή EMS. Η Microsoft έχει σημειώσει σημαντικές βελτιώσεις των χαρακτηριστικών, αλλά εξακολουθεί να υστερεί σε σχέση με τα κορυφαία EMM σε ορισμένες περιοχές.

Το Intune είναι μια καλή εφαρμογή για χρήστες που είναι ήδη πελάτες της Microsoft Enterprise και βλέπουν τη Microsoft ως στρατηγικό συνεργάτη, οι οποίοι θα υποστηρίξουν κυρίως τις περιπτώσεις χρήσης με προσανατολισμό την παραγωγικότητα που βασίζονται στο Microsoft Office 365 και οι οποίοι έχουν αναπτύξει ή θα αναπτύξουν Azure AD ως λύση IAM τους.

Κεφάλαιο 6ο Προτάσεις σχετικα με την επιλογή κατάλληλου EMM

Στο κεφάλαιο αυτό παρουσιάζονται οι προτάσεις μου σχετικά με τα κριτήρια και τα χαρακτηριστικά που θα πρέπει να έχει υπ' όψιν της η κάθε εταιρεία για την επιλογή του κατάλληλου γι' αυτήν λογισμικού EMM. Οι προτάσεις αυτές βασίζονται κυρίως στην βιβλιογραφία και στα στοιχεία που παρουσιάστηκαν στα προηγούμενα κεφάλαια σχετικά με τις ανάγκες της κάθε επιχείρησης σε enterprise mobility και security.

6.1 Κριτήρια επιλογής EMM

Σύμφωνα με τα παραπάνω και με την έρευνα που εκπόνησα παρουσιάζω παρακάτω τις προτάσεις μου σχετικά με τα κριτήρια επιλογής που θεωρώ πως θα πρέπει να λάβει υπ' όψιν της μια εταιρεία ώστε να επιλέξεις το κατάλληλο λογισμικό EMM.

Η σωστή λύση διαχείρισης της φορητότητας των επιχειρήσεων (EMM) μπορεί να βοηθήσει το τμήμα του IT να ανταποκριθεί στις προκλήσεις ασφάλειας που προσφέρει η πλήρη επιχειρηματική κινητικότητα, αλλά η εσφαλμένη επιλογή μπορεί να δημιουργήσει σοβαρά προβλήματα και να αποτρέψει την εταιρία απο τη υιοθέτηση τεχνολογιών BYOD. Παρακάτω παρουσιάζονται τα κριτήρια τα οποία θα πρέπει να συνυπολογίσει μια εταιρία για να υιοθετήσει το κατάλληλο λογισμικό EMM, επιγραμματικά πρόκειται για τους παρακάτω παράγοντες

- Ασφάλεια (Security)
- Παραγωγικότητα (Productivity)
- Ενσωμάτωση (Integration)
- Πρόσβαση στο δίκτυο (Network access)
- Επεκτασιμότητα (Scalability)

Το βασικότερο πρόβλημα μιας επιχείρησης στην επιλογή λογισμικού EMM είναι να βρει πιο καλύπτει καλύτερα τις ανάγκες τις σύμφωνα με τους παραπάνω παράγοντες. Κατα την διαδικασία επιλογής θα πρέπει να ακολουθηθούν τα παρακάτω βήματα:

1. Ενημέρωση σχετικα με τα προϊόντα EMM που υπάρχουν στην αγορά, ποια προϊόντα ενδείκνυται για το είδος και το μέγεθος την επιχείρησης
2. Καταγραφή σε: πλατφόρμες λειτουργίας, περιπτώσεις χρήσης του EMM,προφίλ χρηστών και απαιτούμενες πολιτικές ασφάλειας που θα εφαρμοστούν από το εργαλείο EMM.
3. Τρόπος λειτουργίας: on-premises, cloud / SaaS.
4. Αξιολόγηση παρόχων EMM με βάση τις απαιτήσεις που ορίζονται παραπάνω.
5. Σταδιακή ανάπτυξη της εφαρμογής, αυξάνοντας σταδιακά τον αριθμό των χρηστών και των διαθέσιμων λειτουργιών.
6. Συχνή επικοινωνία και εκπαίδευση των χρηστών στα νέα λογισμικά για μείωση του αριθμού των κλήσεων υποστήριξης και καλύτερη αξιοποίηση του συστήματος από τους χρήστες.

Σήμερα υπάρχουν πάνω από 125 προμηθευτές EMM που προσφέρουν λύσεις. Η επιλογή του σωστού σημαίνει εύρεση ενός τρόπου ελέγχου και διαχείρισης του λογισμικού BYOD που ταιριάζει καλύτερα στις ανάγκες της εταιρείας.

Για να γίνει αυτό, αρχικά θα πρέπει να περιορίστει τη λίστα προμηθευτών με βάση την απαιτούμενη λειτουργικότητα. Δεδομένου ότι πρόκειται για μια ταχέως αναπτυσσόμενη και άκρως ανταγωνιστική αγορά όπου οι λειτουργικότητες δεν είναι κοινές σε όλους τους παρόχους. Θα πρέπει να ληφθεί υπ όψιν ότι πολλοί προμηθευτές αυτού του χώρου είναι γνωστό ότι αναπτύσσουν μια ελάχιστη λειτουργικότητα για να είναι σε θέση να είναι ανταγωνιστικοί, και ότι η ελάχιστη λειτουργικότητα μπορεί να μην ανταποκρίνεται στις ανάγκες της εταιρείας. Στη συνέχεια, θα πρέπει να διερευνηθεί η κάθε πάροχος σχετικά με την βιωσιμότητά του στην εταιρεία σύμφωνα με τα παρακάτω κριτήρια

- Εάν είναι ο μόνος που προσφέρει την απαιτούμενη λειτουργικότητα (καθώς οι περισσότεροι προμηθευτές EMM προσφέρουν παρόμοιες δυνατότητες)
- Η εταιρία του προμηθευτή έχει την δυνατότητα και το εύρος εργασιών για να συνεχίσει να καινοτομεί σε ένα συνεχώς μεταβαλλόμενο περιβάλλον κινητής τηλεφωνίας.
- Υποστήριξη διαφορετικών φορητών συσκευών και λειτουργικών συστημάτων
- Διαχειριση των smartphones, tablet και κινητών συσκευών από μια μοναδική πλατφόρμα.
- Ύπαρξη καλής τεχνικής υποστήριξης από τον πάροχο.

6.2 Χαρακτηριστικά κατάλληλου EMM

Γενικότερα θεωρώ πως σύμφωνα την έρευνα που έχω κάνει πως δεν υπάρχει σωστός τρόπος για την διαχείριση του enterprise mobility ο οποίος να μπορεί να εφαρμοστεί σε κάθε εταιρεία.

Σε γενικές γραμμές, οι εταιρείες αποφεύγουν τις επιμέρους λύσεις σε πλατφόρμες που αντιμετωπίζουν την ανάγκη διαχείρισης και ασφάλειας σε διάφορες συσκευές, εφαρμογές και δεδομένα. Μια λύση διαχείρισης της κινητικότητας των επιχειρήσεων (EMM) πρέπει να παρέχει στους πελάτες την ευελιξία να εφαρμόζουν ελέγχους σε επίπεδο συσκευής ή εφαρμογών βάσει της εταιρικής στρατηγικής για την κινητικότητα. Για παράδειγμα, μια εταιρεία μπορεί να επιλέξει

να χρησιμοποιήσει MDM σε συσκευές που παρέχονται από την εταιρεία και MAM σε προσωπικές συσκευές. Οι κορυφαίες λύσεις EMM προσφέρουν ολοκληρωμένα εργαλεία διαχείρισης πολιτικής και διαμόρφωσης, παρέχοντας στους οργανισμούς τη δυνατότητα να εφαρμόζουν συνεπείς ελέγχους σε διάφορες πλατφόρμες κινητής τηλεφωνίας χρησιμοποιώντας έναν συνδυασμό πολιτικών για συσκευές και εφαρμογές. Μια λύση EMM θα πρέπει να έχει τα πέντε παρακάτω χαρακτηριστικά:

Διαχείριση συσκευών (MDM)

Ίσως το πιο πολύτιμο χαρακτηριστικό του MDM είναι ότι επιτρέπει στο IT της εταιρίας να απενεργοποιεί από απόσταση μία συσκευή όταν χαθεί ή κλαπεί. Οι καλύτερες εφαρμογές EMM προσφέρουν MDM καθώς επίσης απομακρυσμένη επαναφορά συσκευών. Πρέπει να προσφέρουν υποστήριξη για μια ποικιλία λειτουργικών συστημάτων κινητής τηλεφωνίας, διασφαλίζοντας την πρόσβαση από μια μεγαλύτερη ποικιλία συσκευών. Οι εταιρείες θα πρέπει να επιλέξουν μια λύση EMM που να έχει ευρεία κάλυψη πλατφόρμας. Αυτό τους δίνει τη δυνατότητα να παρέχουν επιλογή συσκευών και τους επιτρέπει να διαχειρίζονται πολλές συσκευές κινητής τηλεφωνίας από το ίδιο λογισμικό.

Διαχείριση εφαρμογών (MAM)

Η διαχείριση εφαρμογών αφορά την εφαρμογή πολιτικών σε μεμονωμένες εφαρμογές, έτσι ώστε να μην χρειάζεται να ελέγχετε τη συσκευή, όπως στην περίπτωση προσωπικών συσκευών για συνεργάτες ή υπαλλήλους. Οι προσεγγίσεις περιλαμβάνουν το de Software Development Kit (SDK), το οποίο επιτρέπει στους προγραμματιστές να ενσωματώνουν χαρακτηριστικά όπως έλεγχο ταυτότητας χρηστών, εντοπισμό συμβάντων κινδύνου, πολιτικές πρόληψης απώλειας δεδομένων, πιστοποιητικά και διαμορφώσεις εφαρμογών over-the-air. Οι πολιτικές ενδέχεται να περιλαμβάνουν απαιτήσεις εξακρίβωσης ταυτότητας, περιορισμούς αντιγραφής / επικόλλησης, περιορισμούς κοινής χρήσης περιεχομένου ή μη επιτρέποντας την αποθήκευση τοπικών δεδομένων.

Προστασία από απειλές

Μια λύση EMM θα πρέπει να επιτρέπει στο IT της εταιρείας να διαχειρίζεται κεντρικά την προστασία των κινητών απειλών και να αξιοποιεί τα δεδομένα κινδύνου εφαρμογών εφαρμόζοντας πολιτικές, όπως για παράδειγμα τη δυνατότητα μαύρης λίστας εφαρμογών που βασίζονται σε συγκεκριμένα χαρακτηριστικά κινδύνου ή μιας εφαρμογής με υψηλή χρήση δεδομένων. Η κεντρική διαχείριση περιλαμβάνει πράγματα όπως η παροχή μιας εφαρμογής ασφαλείας σε συσκευές, η εκτέλεση απομακρυσμένων σαρώσεων της συσκευής, η προβολή απειλών και η καθιέρωση πολιτικών συμμόρφωσης (για παράδειγμα, δυνατότητα αποκλεισμού πρόσβασης μέσω ηλεκτρονικού ταχυδρομείου αν εντοπιστεί κακόβουλο λογισμικό). Η προστασία από κινητές απειλές προστατεύει τόσο τους χρήστες όσο και την επιχείρηση από το κακόβουλο λογισμικό, τους κινδύνους ιδιωτικού απορρήτου, τους κινδύνους απόδοσης, τις πλαστές ιστοσελίδες και άλλες ψηφιακές απειλές. Οι καλύτερες λύσεις εφαρμόζουν πληροφορίες σχετικά με τις πραγματικές συμπεριφορές για την προστασία της ιδιωτικής ζωής, την ανίχνευση κακόβουλου λογισμικού και τον μετριασμό των κινδύνων απόδοσης όπως η γρήγορη κατανάλωση της μπαταρίας.

Έλεγχοι πρόσβασης και ελέγχου ταυτότητας

Τα στοιχεία ελέγχου πρόσβασης και ελέγχου ταυτότητας διαχειρίζονται την πρόσβαση απαιτώντας την επιτυχή αναγνώριση ενός κωδικού πρόσβασης, βιομετρικής σάρωσης, αναγνώρισης φωνής ή προσώπου. Οι καλύτερες λύσεις EMM επιτρέπουν στο IT να ομαδοποιεί χρήστες - ανά τμήμα, για παράδειγμα - και να χορηγεί πρόσβαση μόνο στους πόρους που χρειάζεται μια συγκεκριμένη ομάδα. Η δυνατότητα αυτή σας επιτρέπει να ορίσετε τι μπορούν να

κάνουν οι χρήστες στο δίκτυο με συγκεκριμένες συσκευές και υπό ποιες συνθήκες. Μια ισχυρή λύση EMM πρέπει να προσφέρει έλεγχο ταυτότητας με χαρακτηριστικά εξοικονόμησης χρόνου, όπως ενιαία σύνδεση, όπου οι εργαζόμενοι μπορούν να χρησιμοποιούν τα ίδια διαπιστευτήρια για να συνδεθούν σε φορητό υπολογιστή και σε άλλα εταιρικά συστήματα. Η ενιαία σύνδεση επίσης διευκολύνει τον χρήστη να μετακινηθεί από την εφαρμογή σε εφαρμογή χωρίς την διαδικασίας επαλήθευσης κάθε φορά που ανοίγει μια εφαρμογή. Η ιδέα είναι ότι μόλις οι χρήστες έχουν πιστοποιήσει τον εαυτό τους σε μια εφαρμογή, η εφαρμογή αυτή είναι σε θέση να "μεταβιβάσει" τα διαπιστευτήρια σε άλλη εφαρμογή του δικτύου.

Διαχείριση περιεχομένου

Το MCM επιτρέπει στους χρήστες να έχουν πρόσβαση σε περιεχόμενο από κινητές συσκευές με έναν ασφαλή τρόπο. Μια εταιρία που παρέχει mobility οφείλει να είναι σε θέση να παρέχει πρόσβαση σε ασφαλές εταιρικό περιεχόμενο από οπουδήποτε. Μια λύση EMM θα πρέπει να παρέχει στους εργαζομένους έναν ασφαλή τρόπο πρόσβασης σε εταιρικά αρχεία. Η διαχείριση περιεχομένου περιλαμβάνει επίσης την πρόληψη της απώλειας δεδομένων. Οι βέλτιστες λύσεις θα προσφέρουν κρυπτογραφημένη αποθήκευση δεδομένων στη συσκευή, επιλογές εξακρίβωσης ταυτότητας, ελέγχους αντιγραφής και επικόλλησης (για την αποφυγή διαρροής δεδομένων) και αλλαγή σε ελέγχους ανοιχτού κώδικα για την αποφυγή προσπέλασης περιεχομένου από μη εγκεκριμένες εφαρμογές. Για την προώθηση περιεχομένου, μια λύση EMM θα πρέπει να είναι σε θέση να ελέγχει τις εκδόσεις εγγράφων, να ειδοποιεί τους χρήστες για νέα αρχεία και να καταργεί το περιεχόμενο μόλις έχει λήξει.

6.3 Συμπεράσματα

Οι κινητές συσκευές έχουν ενσωματωθεί σε μεγάλο βαθμό στις επιχειρήσεις και όλα δείχνουν πως πρόκειται για μια τάση που θα αυξάνεται διαρκώς. Καθώς οι κινητές συσκευές συνεχίζουν να γίνονται ισχυρότερες και χρησιμοποιούνται όλο ένα και περισσότερο από τις επιχειρήσεις, οι οργανισμοί πρέπει να εξασφαλίσουν και να διαχειρηστούν καλύτερα αυτά τα συστήματα όχι μόνο με τα προϊόντα διαχείρισης κινητών συσκευών (Mobile Device Management MDM), αλλά και με την ολοκληρωμένη διαχείριση της χρήσης κινητών συσκευών (Enterprise Mobility Management EMM)

Εφαρμόζοντας προσαρμοσμένες, από την εκάστοτε εταιρία, πολιτικές σε smartphones και tablet μέσω του MDM και του EMM, ένας διαχειριστής μπορεί, για παράδειγμα, να ρυθμίζει αυτές τις συσκευές ώστε να χρησιμοποιούνται μόνο με τρόπους που ο οργανισμός θεωρεί κατάλληλους σύμφωνα με την πολιτική ασφαλείας του. Αυτό μπορεί να περιορίσει τον κίνδυνο απώλειας δεδομένων, να σταματήσει τις μη εγκριθείσες εγκαταστάσεις λογισμικού και να αποτρέψει την μη εξουσιοδοτημένη πρόσβαση σε κινητές συσκευές που έχουν πρόσβαση σε εταιρικά δεδομένα και δίκτυα.

Οι μονάδες διαχείρισης της κινητικότητας των επιχειρήσεων (EMM) είναι ο συνδετικός κρίκος που συνδέει τις κινητές συσκευές με την υποδομή και την πολιτική της επιχείρησής τους. Οι οργανισμοί χρησιμοποιούν εργαλεία EMM για την εκτέλεση των ακόλουθων λειτουργιών:

- Προστασία δεδομένων: Τα λογισμικά EMM έχουν ως βασικό στόχο την ελαχιστοποίηση της απώλειας ή διαρροής εταιρικών δεδομένων ή παρόμοιων περιστατικών που απειλούν τα ευαίσθητα δεδομένα της εταιρείας, αυτό επιτυγχάνεται μέσω της κρυπτογράφησης δεδομένων, των δικαιωμάτων πρόσβασης σύμφωνα με το προφίλ του χρήστη, αποφυγή σύνδεσης σε μη ασφαλή δίκτυα.

- Αναβάθμιση: Τα λογισμικά EMM διαμορφώνουν τις εφαρμογές ώστε να είναι κατάλληλες για εταιρική χρήση, διαχειρίζονται τις ενημερώσεις και βοηθούν στην αναβάθμιση της συσκευής.
- Υποστήριξη: Τα λογισμικά EMM βοηθούν τα τμήματα πληροφορικής να εντοπίζουν τα προβλήματα των κινητών συσκευών και των εταιρικών εφαρμογών και να παρέχουν άμεση βοήθεια για την επίλυσή τους.

Κεφάλαιο 7ο Συμπεράσματα

7.1 Συμπεράσματα

7.1.1 Γενικά συμπεράσματα

Είναι ευρέως γνωστό πως η εξέλιξη της τεχνολογίας επενδύει πλέον κυρίως στην ανάπτυξη και εξάπλωση των φορητών κινητών συσκευών. Οι τομείς της πληροφορικής πάνω στην εξέλιξη των οποίων βασίζεται η ύπαρξη και εξάπλωση των κινητών συσκευών είναι αρκετοί. Ο βασικότερος είναι η τεχνολογία των δικτύων μέσων των οποίων γίνεται η μεταφορά δεδομένων (ήχου, εικόνας, κειμένων, εγγράφων).Αρκεί μια φορητή συσκευή να έχει το κατάλληλο λογισμικό και σύνδεση στο διαδίκτυο ώστε να μπορέσει ο χρήστης να αναζητήσει και να έχει πρόσβαση σε μεγάλο όγκο πληροφορίας ο οποίος είναι αποθηκευμένος σε κάποια άλλη υπολογιστική μονάδα. Αυτή η διαδικασία καθιστά τις φορητές συσκευές εύχρηστες καθώς και πολύ πιο αποδοτικές διότι πλέον οι φυσικοί πόροι (hardware) της συσκευής χρησιμοποιούνται μόνο για τις βασικές λειτουργίες της συσκευής και όχι για την αποθήκευση δεδομένων.

Η χρήση των κινητών συσκευών στον τομέα της επιχειρηματικότητας (Enterprise Mobility) και γενικότερα η ανάγκη άμεσης απομακρυσμένης πρόσβασης στις πληροφορίες του εταιρικού συστήματος καθώς και στη βάση δεδομένων μέσω κινητών συσκευών (Bring Your own Device (BYOD)) έχει δημιουργήσει μεγάλες αλλαγές στις επιχειρήσεις

Πλέον όλο και περισσότεροι εργαζόμενοι έχουν ανάγκη για πρόσβαση στα δεδομένα οπουδήποτε κι αν βρίσκονται μέσω της φορητής τους συσκευής. Η εξάπλωση και η ευρεία χρήση των φορητών συσκευών έχει δημιουργήσει πλέον έναν ¨κινητό¨ τρόπο ζωής και εργασίας ο οποίος απαιτεί μεγαλύτερη ευελιξία σχετικά με τον τρόπο που λειτουργούσαν πριν οι επιχειρήσεις

Η εκτεταμένη χρήση των φορητών συσκευών στον τομέα της επιχειρηματικότητας μπορεί να ωφελήσει σε μεγάλο βαθμό την επιχείρηση Η χρήση φορητών συσκευών μπορεί να βοηθήσει την εταιρεία στην επίτευξη των στόχων της παρέχοντάς της την δυνατότητα να λειτουργεί πιο αποδοτικά καθώς και να προσαρμόζεται πιο γρήγορα στις αλλαγές που απαιτούνται ώστε να εκσυγχρονιστεί και να γίνει ανταγωνιστική στην αγορά.

Επιπλέον, βοηθάει στην αύξηση της παραγωγικότητας διευκολύνοντας τις διαδικασίες, μειώνοντας το κόστος και διευκολύνοντας την λήψη αποφάσεων. Οι εφαρμογές για κινητά γίνονται όλο και πιο απαραίτητες για τις επιχειρήσεις βελτιώνοντας την αποδοτικότητάς τους και την αποτελεσματικότητα της γνώσης των εργαζομένων, βελτιστοποιώντας την γραμμή παραγωγής και παρέχοντας διευρυμένη πρόσβαση στους υπαλλήλους και στους συνεργάτες.

Παρά τα πολλά θετικά και οφέλη που έχει η υιοθέτηση τεχνικών entreprise mobility, σύμφωνα με την βιβλιογραφία υπάρχουν έντονες ανησυχίες στον τομέα της ασφάλειας πληροφοριών, τόσο σε επίπεδο εταιρικό όσο και σε ατομικό επίπεδο. Συγκεκριμένα οι εταιρείες ανησυχουν για την ασφάλεια των ευαίσθητων εταιρικών δεδομένων, τυχόν διαρροές ή κακόβουλες επιθέσεις στα συστήματά τους και οι υπάλληλοι που χρησιμοποιούν συσκευές και λογισμικά BYOD ανησυχούν για την παραβίαση της ιδιωτικότητάς τους.
Λύση στα παραπάνω σύμφωνα πάντα με την βιβλιογραφία δίνουν αρχικά η εφαρμογή στρατηγικής για την ασφάλεια πληροφοριών καθώς και τα λογισμικά enterprise mobility (Enterprise mobility management, EMM). Η εταιρεία που θα υιοθετήσει κάποια λύση BYOD οφείλει πλέον να έχει και μια στρατηγική ασφάλειας ώστε να αποφευχθούν τα διαρροές πληροφοριών αλλά και να διασφαλίζεται η ιδιωτικότητα των υπαλλήλων.

Σαν τελικό συμπέρασμα θα μπορούσα να πω πως το entreprise mobility είναι μια αυξανόμενη τάση τον επιχειρηματικό κόσμο, η οποία μπορεί πλέον να εφαρμοστεί σχεδόν σε όλα τα είδη των εταιρειών, ανεξάρτητα από το μέγεθος της εταιρείας, προσφέροντας ευελιξία και άμεση πρόσβαση των υπαλλήλων στο εταιρικό πληροφοριακό σύστημα και στα δεδομένα που χρειάζονται για να δουλέψουν εξ αποστάσεως. Παράλληλα παρουσιάζει και μεγάλο τεχνολογικό ενδιαφέρον καθώς πολλές εταιρείες παρέχουν BYOD και EMM λογισμικά.

7.1.2 Συμπεράσματα επιμέρους κεφαλαίων

Συνοπτικά τα συμπεράσματα της έρευνας είναι:

ERP συστήματα

Σε μια επιχείρηση που κάνει εκτεταμένη χρήση του ERP συστήματος, είναι και για λόγους οικονομικούς αλλά και για λόγους προσβασιμότητας και ευελιξίας επιτακτική η ανάγκη για εφαρμογή Cloud ERP συστήματος.

Enterprise mobility

Η κινητικότητα άλλαξε τον τρόπο με τον οποίο οι εργαζόμενοι αλληλεπιδρούν με τα μέσα που έχουν στην διάθεσή τους για να εργαστούν. Αντί να χρησιμοποιούν τον επιτραπέζιο υπολογιστή για να κάνουν τα πάντα, οι εργαζόμενοι έχουν πλέον τη δυνατότητα να κάνουν τμήματα της δουλειάς τους σε διαφορετικές συσκευές, χρησιμοποιώντας την καλύτερη συσκευή για την τρέχουσα εργασία.

Ανάλυση προβλημάτων ασφάλειας Enterprise mobility

Λαμβάνοντας υπόψη τον αριθμό των κινδύνων που σχετίζονται με το BYOD, οι οργανισμοί θα πρέπει να επανεξετάσουν την αποτελεσματικότητα των πλαισίων ασφάλειας και προστασίας των προσωπικών δεδομένων τους σε ένα ευρύ φάσμα που περιλαμβάνει: τεχνικούς ελέγχους, πολιτικές, πρότυπα και διαδικασίες, προγράμματα ευαισθητοποίησης / κατάρτισης των χρηστών σχετικα με τους κινδύνους ασφάλειας. Όλα αυτά μπορούν να συνδυαστούν για να αναπτυχθεί ένα πλαίσιο λύσης BYOD που περιλαμβάνει αρχιτεκτονική πολιτικής και κατευθυντήριες γραμμές για τους οργανισμούς.

Enterprise Mobility Management

Οι κινητές συσκευές έχουν ενσωματωθεί σε μεγάλο βαθμό στις επιχειρήσεις και πρόκειται για μια τάση που θα αυξάνεται διαρκώς. Καθώς οι κινητές συσκευές συνεχίζουν να γίνονται ισχυρότερες και χρησιμοποιούνται όλο ένα και περισσότερο από τις επιχειρήσεις, οι οργανισμοί

πρέπει να εξασφαλίσουν και να διαχειρηστούν καλύτερα αυτά τα συστήματα με την ολοκληρωμένη διαχείριση της χρήσης κινητών συσκευών (Enterprise Mobility Management EMM). Οι μονάδες διαχείρισης της κινητικότητας των επιχειρήσεων (EMM) είναι ο συνδετικός κρίκος που συνδέει τις κινητές συσκευές με την υποδομή και την πολιτική της επιχείρησής τους

7.2 Βιβλιογραφια - Αδυναμίες - Προτάσεις για περαιτέρω έρευνα

Στην παρούσα έρευνα επικαλέστηκα ερευνητικά άρθρα και διατριβές τα οποία προέρχονται από πανεπιστήμια και σχολές κυρίως με κατεύθυνση κυρίως πληροφορικής (computer science), ασφάλειας πληροφοριών (information security) καθώς και διοίκησης επιχειρήσεων (business administration).

Παράλληλα, στόχος μου ήταν να επικαλεστώ, πέρα από τις πανεπιστημιακές πηγές, επιστημονικά και εμπορικά περιοδικά και site όπως το Forbes καθώς επίσεις και αποτελέσματα ερευνών συμβουλευτικών και τεχνολογικών εταιρειών όπως Gartner και Cisco.

Ο λόγος για τον οποίο επέλεξα να συνδυάσω τις παραπάνω πηγές ερευνών είναι κυρίως για να δείξω πως η πανεπιστημιακή έρευνα εφαρμόζεται πρακτικά στον τεχνολογικό και επιχειρηματικό πραγματικό περιβάλλον καθώς επίσης διότι θεωρώ πως ο συνδυασμός τέτοιων ερευνητικών πηγών παρέχει πιο αξιόπιστα αποτελέσματα και βοηθάει στην διεξαγωγή ρεαλιστικών και εφαρμόσιμων συμπερασμάτων.

Παρότι προσπάθησα να αναλύσω εκτενώς το θέμα του enterprise mobility υπάρχουν σημεία που αναφέρθηκαν στα πλαίσια της παρούσας έρευνας αλλά δεν αναλύθηκαν εκτενώς παρόλο που διαπίστωσα πως υπάρχει μεγάλος όγκος πληροφοριών σε ότι αφορά την βιβλιογραφία. Αρχικά θα μπορούσε να γίνει επιπλέον αναφορά και ανάλυση σχετικά με τα λογισμικά BYOD που υπάρχουν στην αγορά, καθώς και με τα πλεονεκτήματα και μειονεκτήματα αυτών. Παράλληλα σημαντικό θεωρώ πως θα ήταν να γίνει μια ανάλυση σχετικά με τα λογισμικά BYOD που θα ταίριαζαν σε κάθε είδος εταιρίας ανάλογα με το μέγεθος και το τομέα δραστηριοτήτων καθώς και τα προβλήματα ασφαλείας που πιθανόν να αντιμετωπίζει.

Επιπλέον σημαντικό μέρος της ασφάλειας πληροφοριών είναι η κρυπτογράφηση δεδομένων καθώς και οι τεχνικές που ακολουθούνται. Η κρυπτογράφηση αποτελεί πολύ σημαντικό πεδίο έρευνας τόσο από επιχειρηματικής όσο και από τεχνολογικής άποψης το οποίο συμβάλλει στην ασφαλή μετάδοση των πληροφοριών και χωρίς αυτή δεν θα ήταν εφικτή η εφαρμογή των τεχνικών entreprise mobility.

Τέλος σε ότι αφορά την τεχνολογική προσέγγιση του entreprise mobility, εκτενής έρευνα θα μπορούσε να γίνει στην προγραμματιστικές τεχνικές και βελτιστοποιήσεις των native εφαρμογών για κινητά και tablet οι οποίες προσφέρουν λύσεις BYOD, καθώς στα πρωτόκολλα των δικτύων που χρησιμοποιούνται ώστε να γίνει η μετάδοση των δεδομένων όσο των δυνατόν πιο γρήγορα και με μεγαλύτερη ασφάλεια.

ΒΙΒΛΙΟΓΡΑΦΙΑ - REFERENCES

Bartolj T., Liu L., Santiago S. & Torth O. (IMMIT). 2009. Risks and limitations of using SaaS for ERP. Master thesis.

Benlian A. & Hess T. 2011. Opportunities and risks of SaaS. Findings from a survey of IT executives. Decision Support Systems Vol. 52:232–246.

Castellina N. 2011. Saas and Cloud ERP trends, observations, and performances. Aberdeen Group.

Engebrethson R. 2012. Comparative analysis of ERP emerging technologies (MSc thesis). Faculty of California Polytechnic State University.

Grumman N. 2011. In-house ERP systems vs. cloud computing. IT solutions.

Karabek M.R., Kleinert J. & Pohl A. 2011. Cloud Services for SMEs: Evolution or Revolution. Business + Innovation Vol. 1.

Kim W., Kim S.D., Lee E. & Lee S. 2009. Adoption Issues for Cloud Computing. iiWAS2009, December:14–16.

Kuyoro S.O., Ibikunle F. & Awodele O. 2011 Cloud computing security issues and challenges. International Journal of Computer Networks (IJCN), Volume (3) : Issue (5).

Lin A. and Chen N.C. 2012. Cloud computing as an innovation: Perception, attitude, and adoption International Journal of Information Management. Vol. 4 No.1.

Marston.S., Li Z. Bandyopadhyay S., Zhang J. & Ghalsasi A. 2010 Cloud computing — The business perspective. Decision Support Systems 51 (2011):176–189.

Popovic K. 2010. Cloud computing security issues and challenges. Institute of Automation and Process Computing. Vol. 2b:344-349.

Rong et al. 2012. Beyond lightning: A survey on security challenges in cloud computing. Computers and Electrical Engineering.

Saugatuck 2008. SaaS Realities: Business Benefits for Small and Midsized Business. Saugatuck Technology Inc.

Scavo F., Newton, B. & Longwell, M. 2012. Choosing between cloud and hosted ERP, and why it matters. Computer Economics Report. Vol. 34 No. 8.

Duan J, Faker P, Fesak A & Stuart T 2013 Benefits and drawbacks of cloud based versus traditional ERP systems

Gartner available at www.gartner.com/document/3587259

Gartner, 2012 " Enterprise Mobility and Its Impact on IT" available at https://www.gartner.com/doc/1985016/enterprise-mobility-impact-it

Statista Cloud enterprise resource planning software revenue worldwide from 2016 to 2022 available at https://www.statista.com/statistics/681753/worldwide-cloud-erp-software-revenue/

Panorama Consulting Solution's 2017 available at http://go.panorama-consulting.com/rs/603-UJX-107/images/2017-ERP-Report.pdf https://www.panorama-consulting.com/overview-of-the-top-10-erp-systems/

Bashah, N.S.K., Kryvinska, N. and Thanh van, D. (2012a) 'Novel service discovery techniques for open mobile environments and their business applications', Proceedings of the 3rd International Conference on Exploring Services Science (IESS 1.2), 15–17 February, Geneva, Switzerland, Springer LNBIP-103, pp.186–200.

Bashah, N.S.K., Kryvinska, N. and Thanh van, D. (2012b) 'Quality-driven service discovery techniques for open mobile environments and their business applications', Journal of Service Science Research, Vol. 4, No. 1, pp.71–96.

Berger, F., Bublitz, S. and Eikerling, H.-J. (2006) 'Mobilisierung und Adaption von e-Services am Beispiel von Wartungs - und Instandhaltungsprozessen', Proceedings of the Workshop Mobile Anwendungssysteme im beruflichen und privaten Bereich, GI Tagung, pp.234–240.

Buse, S. (2002) 'Der mobile Erfolg – Ergebnisse einer empirischen Untersuchung in ausgewählten

Camponovo, G. and Pigneur, Y. (2002) 'Analyzing the actor game in m-business', Proceedings of the 1st International Conference on Mobile Business, Athens, July.

Camponovo, G. and Pigneur, Y. (2003) 'Business model analysis applied to mobile business', Proceedings of the 5th International Conference on Enterprise Information Systems (ICEIS), 23–26 April, Angers, France.

Clarke, I. (2008) 'Emerging value propositions for m-commerce', Journal of Business Strategies, Vol. 25, No. 2, Fall.

Gerardjrego (2014) The Circular business model and economy. Sustainable competitive advantage, 16 March. Available online at: http://gerardjrego.com/tag/business-model/.

Kaczor, S. and Kryvinska, N. (2013) 'It is all about services – fundamentals, drivers, and business models', Journal of Service Science Research, Vol. 5, No. 2, pp.125–154.

Kasper, C. and Hagenhoff, S. (2003) 'Geschäftsmodelle im Mobile Business aus Sicht der Medienbranche', Arbeitsbericht Nr.15, M.Schumann (Hrsg.), Institut für Wirtschaftsinformatik, Georg-August-Universität Göttingen.

Kryvinska, N. (2010) Converged Network Service Architecture: A Platform for Integrated Services Delivery and Interworking, Electronic Business series edited by C. Strauss, Vol. 2, International Academic Publishers, Peter Lang Publishing Group.

Kryvinska, N. (2012) 'Building consistent formal specification for the service enterprise agility foundation', Journal of Service Science Research, Vol. 4, No. 2, pp.235–269.

Leem, C.S., Sik, S.H. and Seong, K.D. (2004) 'A classification of mobile business models and its applications', Industrial Management & Data Systems, Vol. 4, No. 1, pp.78–87.

Pigneur, Y. (2002) An ontology for m-business models, University of Lausanne. Available online at: www.psu.edu .

Rook, C. (2003) A method for selecting successful m-business alternatives for Imode and MMs, University of Twente. Available online at: www.psu.edu .

Scherz, M. (2008) Mobile Business – Schaffung eines Bewusstseins für mobile Potenziale im Geschäftsprozesskontext, VdM Verlag Dr. Müller.

Thanh van, D., Hallingby, H.S., Khuong, L.H. and Kryvinska, N. (2014) 'A disruption analysis of mobile communication services using Business Ecosystem concept', International Journal of Services, Economics and Management, Vol. 6, No. 3, pp.248–262.

Tiwari, R., Buse, S. and Herstatt, C. (2006) 'From electronic to mobile commerce – opportunities through technology convergence for business services', Asia Pacific Tech Monitor, Vol. 23, No. 5, pp.38–45.

Ivanochko, I., Gregus, M., Urikova, O. and Masiuk, V. (2015) 'mBusiness, mMarkets and

mServices: exploration of opportunities', Int. J. Services, Economics and Management, Vol. 7, No. 1, pp.74–93.
Kamesh P. 2012, The what, why, who and how of enterprise mobility adoption. Senior Product Manager Dell Inc.
Hockly, N. (2012). Tech-savvy teaching: BYOD. Modern English Teacher, 21(4), 44-45.
Intel. (2012). Peer research report: Insights on the current state of BYOD. Intel's IT Manager survey. Intel IT Center. available at:
http://www.intel.com/content/dam/www/public/us/en/documents/whitepapers/consumerization-enterprise-byod-peer-research-paper.pdf
Leong, K. B. (2013). How to fit BYOD into an enterprise mobility strategy. Network World Asia, 12-14. Mansfield-Devine, S. (2012). Interview: BYOD and the enterprise network. Computer Fraud & Security, 2012(4), 14-17.
Nusca, A. (2013). BYOD: North America and Asia embrace it; Western Europe, not so much. ZDNet. Available at:
http://www.zdnet.com/byod-north-america-and-asia-embrace-it-western-europe-not-so-much-7000016802/
Pepin, C. (2013). IBM Connection 2013: BYOD at IBM. Slideshare IBM Network. Retrieved July 29, 2013, available at:
http://www.slideshare.net/chrispepin/ibm-connect-2013-byod-at-ibm
Qing, L. Y. (2013). BYOD on rise in Asia, but challenges remain. ZDNet. Retrieved July 29, 2013,
available at:
http://www.zdnet.com/byod-on-rise-in-asia-but-challenges-remain-7000010660/
Thomson, G. (2012). BYOD: Enabling the chaos. Network Security, 2012(2), 5-8.
Vandendriessche, J. (2012). Understanding BYOD legal issues under European privacy and data
protection law. ISACA. available at:
http://www.slideshare.net/Johan_Vdd/understanding-byod-legal-issuesunder-european-privacy-and-data-protection-law
Yahoo! (2013). Q1 BYOD smartphone sales surge in North America and Asia but Western Europe
fights the growing trend. Available at:
http://finance.yahoo.com/news/q1-byod-smartphone-sales-surge-120000004.html
Aaron M. F, Chengqi G., J.P. Shim (2014) Current Status, Issues, and Future of Bring Your Own Device (BYOD) available at:
https://www.researchgate.net/profile/Jung_Shim/publication/268445822_Current_Status_Issues_and_Future_of_Bring_Your_Own_Device_BYOD/links/549493960cf29b944820fff1/Current-Status-Issues-and-Future-of-Bring-Your-Own-Device-BYOD.pdf
Loucks J., MedcalfLauren R., Buckalew F.F. 2013 The Financial Impact of BYOD A Model of BYOD's Benefits to Global Companies. Available at:
http://www.webtorials.com/main/resource/papers/cisco/paper235/BYOD-Economics_Econ_Analysis.pdf
B. Hayes and K. Kotwica, Bring Your Own Device (BYOD) to Work: Trend Report. Oxford UK: Elsevier, 2013.
A. M. French, C. Guo, and J. Shim, "Current Status, Issues, and Future of Bring Your Own Device (BYOD)," Communications of the Association for Information Systems, vol. 35, p. 10, 2014.
J. Keyes, Bring Your Own Devices (BYOD) Survival Guide. Boca Raton, FL: CRC Press, 2013.

K. W. Miller, J. Voas, and G. F. Hurlburt, "BYOD: Security and Privacy Considerations," IT Professional, vol. 14, pp. 53-55, 2012.
M. E. Whitman and H. J. Mattord, Principles of information security. Boston USA: Cengage Learning, 2010.
N. Mooradian, "The importance of privacy revisited," Ethics and Information Technology, vol. 11, pp. 163- 174, 2009.
T. R. Peltier, Information security fundamentals: CRC Press, 2013.
A. B. Garba, J. Armarego, D. Murray, and W. Kenworthy, "Review of the Information Security and Privacy Challenges in Bring Your Own Device (BYOD) Environments," Journal of Information Privacy and Security, vol. 11, pp. 38-54, 2015. **(a)**
A. B. Garba, J. Armarego, and D. Murray, "Bring your own device organizational information security and privacy," ARPN Journal of Engineering and Applied Sciences, vol. 10, pp. 1279-1287, 2015. **(b)**
A. B. Garba, J. Armarego, and D. Murray, "A Policy-Based Framework for Managing Information Security and Privacy Risks in BYOD Environments", vol.2, 2015 **(c)**
M. Eslahi, M. V. Naseri, H. Hashim, N. Tahir, and E. H. M. Saad, "BYOD: Current state and security challenges," in Computer Applications and Industrial Electronics (ISCAIE), IEEE Symposium, pp. 189-192, 2014.
D. Rivera, G. George, P. Peter, S. Muralidharan, and S. Khanum, "Analysis of Security Controls for BYOD (Bring your own Device)," The University of Melbourne, Melbourne, 2013.
K. J. Smith and S. Forman, "Bring Your Own Device—Challenges and Solutions for the Mobile Workplace," Employment Relations Today, vol. 40, pp. 67-73, 2014.
L. Guan, "Established BYOD management policies needed," Government News, vol. 32, p. 9, 2012.
A. Dedeche, F. Liu, M. Le, and S. Lajami, "Emergent BYOD security challenges and mitigation strategy" The University of Melbourne, Melbourne, 2013.
A. Ghosh, P. K. Gajar, and S. Rai, "Bring your own device (BYOD): Security risks and mitigating strategies," Journal of Global Research in Computer Science, vol. 4, pp. 62-70, 2013.
ZixCorp. "Zix Corporation and Ponemon Institute Survey Reveals Limitations and Frustration with First Generation Bring-Your-Own-Device Security Products," Jul. 29, 2013. [Online]. Available at: http://investor.zixcorp.com/phoenix.zhtml?c=108645&p=irol-newsArticle&ID=1875802&highliht
T. Y. Andrew and A. T. Yang, "Risk Management in the Era of BYOD," in Symposium on Usable Privacy and Security (SOUPS), 2013.
C. P. Pfleeger and L. P. Shari, Security In Computing. Upper Saddle River, NJ: Prentice Hall PTR, 2006.
OECD, "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," Commonwealth law bulletin, vol. 7, p. 1078, 1980.
ISO 27000 Directory. An Introduction to ISO 27001, ISO 27002....ISO 27008. Mar. 13th 2014. [Online]. Available: http://www.27000.org/ contact.htm
ISACA, "COBIT 5: A Business Framework for the Governance and Management of Enterprise IT," ed. Rolling Meadows, USA: ISACA, 2012.
Information Security Forum. The Standard of Good Practice for Information Security. Mar. 20th 2014. [Online]. Available: http://www.netbotz.com/library/Info_Security_Forum_Standard_Good_Practices.pdf
ITIL, IT Infrastructure Library, Service design, 2nd ed.: Stationery Office., 2007.

OECD, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data: OECD Publishing, 2002.
M. A. Harris, K. Patten, and E. Regan, "The need for byod mobile device security awareness and training," in Americas Conference on Information Systems, Chicago, 2013.
V. Venkatesh, M. G. Morris, D. B. Gordon, and F. D. Davis, "User acceptance of information technology: Toward a unified view," MIS quarterly, pp. 425-478, 2003.
Felt, A. P., Finifter, M., Chin, E., Hanna, S., & Wagner, D. (2011). A survey of mobile malware in the wild. Paper presented at the Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices.
Alcatel-Lucent. (2013). Kindsight Security Labs: Malware Report – Q4 2013. available at: http://www.alcatel-lucent.com/solutions/kindsight-security
Dodge, R. C. (2007). Phishing for user security awareness. Computers & security, 26, 73-80.
Imperva. (2013). Imperva's Hacker Intelligence Summary Report: The Anatomy of an Anonymous Attack. Retrieved 3rd May, 2013, available at: http://www.imperva.com/docs/hii_the_anatomy_of_an_anonymous_attack.pdf
Ashford, W. (2012). Nearly half of firms supporting BYOD report data breaches. available at: http://www.computerweekly.com/news/2240161202/Nearly-half-of-firms-supporting-BYOD-report-databreaches
AirTight Networks. (2010). WPA2 Hole 196 Vulnerability. Available at: www.airtightnetworks.com/WPA2-Hole196
Braue, D. (2007). Lost mobile phones: a survival guide. Available at: www.cnet.com.au/lostmobile-phones-a-survival-guide-339276173.htm
AMTA. (2013). The Mobile Phone Industry Statement. Available at: www.amta.org.au/pages/amta/The.Mobile.Phone.Industry.Statement
J. M. Chang, P.-C. Ho, and T.-C. Chang, "Securing byod," IT Professional, vol. 16, pp. 9-11, 2014.
Khalid Almarhabi Kamal Jambi, Fathy Eassa, Omar Batarfi, "Survey on Access Control and Management Issues in Cloud and BYOD Environment" International Journal of Computer Science and Mobile Computing, Vol.6 Issue.12, December- 2017, pg. 44-54
Gens, F., Levitas, D., & Segal, R. (2011). 2011 Consumerization of IT Study: Closing the "Consumerization Gap". Framingham: International Data Corporation (IDC).
Cisco Networks. (2012). Cisco Study: IT Saying Yes to BYOD, Targeted News Service. Available at: http://0-search.proquest.com.prospero.murdoch.edu.au/docview/1013951859?accountid=12629
K. W. Miller, J. Voas, and G. F. Hurlburt, "BYOD: Security and Privacy Considerations," IT Professional, vol. 14, pp. 53-55, 2012.
P. Beckett, "BYOD–popular and problematic," Network Security, vol. 2014, pp. 7-9, 2014
PricewaterhouseCoopers (PWC), "The Global State of Information Security Survey," 2015
The Metaphysics Research Lab, "Stanford Encyclopedia of Philosophy," Stanford University, 2014
B. Ballad, T. Ballad, and E. K. Banks, Access control, authentication, and public key infrastructure. Sudbury, MA: Jones & Bartlett Learning, 2011
A. Hovav and F. F. Putri, "This is my device! Why should I follow your rules? Employees' compliance with BYOD security policy," Pervasive and Mobile Computing, vol. 32, pp. 35-49, 2016.

G. Thomson, "BYOD: enabling the chaos," Network Security, vol. 2012, pp. 5-8, 2012.
CSOonline "3 options for securing BYOD data" 2017, available at:
https://www.csoonline.com/article/3242151/byod/3-options-for-securing-byod-data.html
CisoPlatform "Technologies For Security Of BYOD" 2017, available at:
http://www.cisoplatform.com/profiles/blogs/technologies-for-security-of-byod