Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής

Πρόγραμμα Μεταπτυχιακών Σπουδών

«Προηγμένα Συστήματα Πληροφορικής»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**Ανάλυση επικινδυνότητας σε λύσεις Υπολογιστικού Νέφους (Risk analysis in Cloud Solutions)**
Ονοματεπώνυμο Φοιτητή	**Ιωάννης Ασλάνης-Βασιλείου**
Πατρώνυμο	**Σπυρίδων**
Αριθμός Μητρώου	**ΜΠΣΠ/10034**
Επιβλέπων	**Νινέτα Πολέμη, Αναπληρώτρια Καθηγήτρια**

Ημερομηνία Παράδοσης **Μήνας Έτος**

Πίνακας Περιεχομένων

Τριμελής Εξεταστική Επιτροπή

(υπογραφή)	(υπογραφή)	(υπογραφή)
Όνομα Επώνυμο Βαθμίδα	Όνομα Επώνυμο Βαθμίδα	Όνομα Επώνυμο Βαθμίδα

Περίληψη (Abstract)

Όλο και περισσότερες εταιρείες εξετάζουν σοβαρά το ενδεχόμενο να χρησιμοποιήσουν τις υπηρεσίες ενός υπολογιστικού νέφους ως μέρους των λειτουργιών τους, τόσο ως προμηθευτές όσο και ως καταναλωτές. Υπάρχει βέβαια και η άλλη πλευρά, η οποία περιλαμβάνει πελάτες και προμηθευτές οι οποίοι εκφράζουν την ανασφάλεια τους σχετικά με τη διαθεσιμότητα, δέσμευση, νομοθεσία, απόδοση, ασφάλεια μίας πλατφόρμας υπολογιστικού νέφους. Ένα από τα σημαντικά κριτήρια που λαμβάνεται υπόψη από τους πελάτες στην απόφαση τους να εμπιστευτούν υποδομές υπολογιστικού νέφους για τις εφαρμογές και τα δεδομένα τους είναι όντως η ασφάλεια. Σκοπός αυτός της πτυχιακής εργασίας είναι η ανάλυση επικινδυνότητας σε λύσεις Υπολογιστικού Νέφους, δηλαδή να εξετάσει αν υπάρχουν θεμελιώδη εμπόδια στο να γίνει μία πλατφόρμα Υπολογιστικού Νέφους όσο ασφαλής όσο μία υπολογιστική υποδομή στο περιβάλλον εντός του οργανισμού, και αν τα μέτρα που λαμβάνονται από μία τέτοια πλατφόρμα είναι αρκετά για να οχυρώσουν μία cloud υποδομή όσο καλά όσο μία τοπική υποδομή. Στόχος επίσης της εργασίας είναι να συγκρίνει το επίπεδο ασφάλειας των υποδομών ΥΝ που έχουν αναπτυχθεί σε διεθνές επίπεδο και να βοηθήσει μέσα από αυτή την σύγκριση στον ορισμό κριτηρίων αξιολόγησης για την απόφαση ενός οργανισμού να κάνει χρήση υπολογιστών πόρων μίας υποδομής υπολογιστικού νέφους ή όχι. Εξετάζεται η περίπτωση της cloud υποδομής της EMC στην οποία πραγματοποιείται ανάλυση κινδύνων με μία ορισμένη μεθοδολογία για την εξαγωγή συμπερασμάτων.

More and more companies are seriously considering to use the services of a cloud computing as part of their operations, both as suppliers and as consumers. There is of course the other side, which includes customers and suppliers who express uncertainty about their availability, commitment, legislation, performance, security of a cloud computing platform. One of the important criteria to be considered by customers in their decision to trust infrastructure for cloud computing applications and their data is actually security. The purpose of this thesis is to examine whether there are fundamental obstacles to become a platform for cloud computing as secure as a computing infrastructure on the environment within the organization, and whether the measures taken by such a platform is enough to fortify one cloud infrastructure as well as a local infrastructure. Also aim of this essay is to compare the level of security infrastructure cloud providers developed at international level and help through this comparison in the definition of evaluation criteria for the decision of an organization to make use of a computer resource infrastructure cloud computing or not. Examine the case of EMC's cloud infrastructure to which a risk analysis is pursued with a defined methodology for drawing conclusions.

1. ΕΙΣΑΓΩΓΗ

Το cloud computing είναι μία από τις μεγάλες τάσεις στον κλάδο της πληροφορικής σήμερα. Η περιοχή εξακολουθεί να είναι νέα και διαρκώς αναπτυσσόμενη και πολλές εταιρείες προσαρμόζουν τις λειτουργίες τους σε αυτό το πρότυπο, τόσο ως προμηθευτές όσο και ως καταναλωτές. Η υπηρεσία υπολογιστικού νέφους που προσφέρεται από τους προμηθευτές ποικίλλει, αλλά κοινή συνισταμένη όλων είναι η παροχή πρόσβασης από απόσταση σε υπολογιστικούς πόρους. Οι πόροι αυτοί μπορεί να είναι διακομιστές, χώροι αποθήκευσης, εφαρμογές και πολλά άλλα.

Το πλεονέκτημα του Υπολογιστικού Νέφους (ΥΝ) είναι ότι ένας οργανισμός που έχει ανάγκη της εγκατάστασης μίας εφαρμογής μπορεί να το κάνει αυτό χωρίς να χρειάζεται να προβεί σε αγορά και συντήρηση υλικού και λογισμικού υπό την ιδιοκτησία του. Αντί αυτού η φιλοξενία της εφαρμογής στο ΥΝ σημαίνει ότι η αντίστοιχη υπηρεσία προσφέρει την δυνατότητα της αυτόματης προσαρμογής στη τρέχουσα κίνηση και με αυτόν τον τρόπο, η αύξηση ή η μείωση του αριθμού των χρηστών είναι διαχειρίσιμη.

Υπάρχει μία ευρέως χρησιμοποιούμενη κατηγοριοποίηση των μοντέλων υπηρεσιών η οποία τα καθιστά διαφορετικά με βάση το επίπεδο εικονικής υποδομής που παρέχεται. Τα τρία πιο συχνά αναφερόμενα μοντέλα είναι το Λογισμικό-, Πλατφόρμα-, και Υπηρεσία- ως-Υπηρεσία. Λογισμικό-ως-Υπηρεσία (Software-as-a-Service, SaaS) είναι ένα κομμάτι του λογισμικού που διατίθενται στους πελάτες μέσω του Διαδικτύου. Η εφαρμογή τρέχει στην υποδομή του παρόχου ΥΝ και είναι συνήθως προσβάσιμη στους χρήστες μέσω ενός web browser. Οι χρήστες της υπηρεσίας δεν ασχολούνται με την εγκατάσταση του λογισμικού ή την ενημέρωση τους και συνήθως οι χρήστες χρεώνονται σε μηνιαία βάση ή σύμφωνα με κάποιο άλλο σχέδιο τιμολόγησης προπληρωμένου χρόνου (pay-as-you-go). Το μοντέλο Πλατφόρμα-ως-Υπηρεσία (Platform-as-a-Service, PaaS) επιτρέπει στο χρήστη να αναπτύξει εφαρμογές με γλώσσες προγραμματισμού και εργαλεία που διατίθενται από τον προμηθευτή της πλατφόρμας. Αυτές οι εφαρμογές μπορεί στη συνέχεια να τρέχουν από την υποδομή της πλατφόρμας που ο χρήστης δεν διαχειρίζεται ή ελέγχει άμεσα. Το μοντέλο Υποδομή-ως-Υπηρεσία (Infrastructure-as-a-Service, IaaS) παρέχει στους πελάτες υπολογιστικούς πόρους, όπως επεξεργαστική ισχύ, χώρο αποθήκευσης και δικτυακές υπηρεσίες. Οι πόροι αυτοί μπορούν να χρησιμοποιηθούν για την ανάπτυξη και εγκατάσταση λογισμικού και ο πελάτης είναι πλήρως υπεύθυνος για τη διαχείριση των λειτουργικών συστημάτων και για όποιο άλλο λογισμικό εγκαθίσταται.

Από την άλλη πλευρά υπάρχουν πολλές αντιρρήσεις για τη χρήση του Υπολογιστικού Νέφους και απόψεις σχετικά με το γιατί δεν θα πρέπει να χρησιμοποιείται. Οι αντιρρήσεις μπορούν να βασίζονται σε πραγματικά προβλήματα αλλά ορισμένα από αυτά μπορούν να ξεπεραστούν ή να μην μη σχετίζονται απόλυτα με το ΥΝ. Μερικές από τις πιο κοινές αντιρρήσεις χρήσης του ΥΝ είναι:

1. η διαθεσιμότητα
2. η δέσμευση
3. η αδειοδότηση του λογισμικού
4. νομοθεσία και νομικά ζητήματα
5. απόδοση
6. ασφάλεια

Για παράδειγμα η διαθεσιμότητα είναι πολύ κρίσιμη σε πολλά συστήματα και η αίσθηση της απώλειας του ελέγχου, μπορεί να αποθαρρύνει την μετάβαση σε πλατφόρμες υπολογιστικού νέφους. Ακόμη και μεγάλοι πάροχοι είχαν διακοπή της λειτουργίας τους που μπορεί να διαρκέσουν ακόμα και μέρες (πχ η Amazon, στο κέντρο δεδομένων της στη North Virginia). Βέβαια σοβαρές διακοπές της λειτουργίας των συστημάτων ΥΝ παρουσιάζονται σπάνια και από την άλλη πλευρά τίθεται το αντίστροφο ερώτημα: οι υποδομές που τρέχουν εντός του οργανισμού-πελάτη είναι ανθεκτικές και ασφαλείς;

Η ασφάλεια είναι η πιο συχνή ένσταση ως προς τη χρήση του ΥΝ, αλλά χωρίς να είναι αρκετά τεκμηριωμένη. Μία άποψη είναι ότι οι πάροχοι εγγυώνται ότι πραγματοποιούν τις απαραίτητες αναλύσεις για την ασφάλεια των υποδομών και ότι υπάρχουν ευρέως δοκιμασμένες τεχνικές λύσεις που μπορούν να χρησιμοποιηθούν. Η ασφάλεια των καναλιών επικοινωνίας, η κρυπτογράφηση των αποθηκευμένων δεδομένων αποτελούν παραδείγματα τομέων όπου γνωστές τεχνικές μπορεί να χρησιμοποιηθούν. Επίσης μία άλλη άποψη είναι ότι οι μελέτες σχετικά με παραβιάσεις της ασφάλειας δείχνουν ότι σημαντικός αριθμός των παραβάσεων πραγματοποιούνται από το εσωτερικό του οργανισμού, γεγονός που υποδηλώνει ότι το υπολογιστικό νέφος θα μπορούσε να κάνει την πληροφοριακή υποδομή του οργανισμού πιο ασφαλής από την άποψη αυτή.

Από την άλλη πλευρά, η αξιολόγηση της ασφάλειας των πλατφόρμων που διατίθενται ως επί το πλείστο θα εξαρτάται από τη φήμη των παρόχων και των πραγματικών αποτελεσμάτων τους στην πράξη, παραδεχόμενοι ότι οι παραβιάσεις της ασφάλειας ενδεχομένως να μη μπορούν να αποκαλυφθούν στο κοινό. Η υπεράσπιση αυτής της προσέγγισης για την αξιολόγηση της ασφάλειας πηγάζει από την άποψη ότι η ασφάλεια είναι εξαιρετικά δύσκολο να συγκριθεί ποσοτικά ή ποιοτικά (Hogberg, 2012). Η ασφάλεια των δεδομένων αποτελεί μία γενικότερη ερευνητική πρόκληση στον τομέα του Υπολογιστικού Νέφους. Οι πάροχοι πρέπει να είναι σε θέση να παρέχουν εμπιστευτικότητα και δυνατότητα ελέγχου για να εξασφαλιστεί η ασφαλής πρόσβαση και αποθήκευση δεδομένων και ότι οι ρυθμίσεις ασφαλείας δεν έχουν πειραχτεί. Η εμπιστευτικότητα μπορεί να επιτευχθεί χρησιμοποιώντας πρωτόκολλα κρυπτογράφησης και δυνατότητας ελέγχου με τεχνικές βεβαίωσης εξ αποστάσεως.

Σκοπός αυτός της πτυχιακής εργασίας είναι να πραγματοποιήσει ανάλυση επικινδυνότητας σε λύσεις Υπολογιστικού Νέφους αξιολογώντας αν υπάρχουν θεμελιώδη εμπόδια στο να γίνει μία πλατφόρμα Υπολογιστικού Νέφους όσο ασφαλής όσο μία υπολογιστική υποδομή στο περιβάλλον εντός του οργανισμού, και αν τα μέτρα που λαμβάνονται από μία τέτοια πλατφόρμα (πχ κρυπτογραφημένοι χώροι αποθήκευσης, εικονικά τοπικά δίκτυα, τείχη προστασίας) είναι αρκετά για να οχυρώσουν μία cloud υποδομή όσο καλά όσο μία τοπική υποδομή. Στόχος της ανάλυσης επικινδυνότητας είναι να συγκρίνει το επίπεδο ασφάλειας των υποδομών ΥΝ που έχουν αναπτυχθεί σε διεθνές επίπεδο και να βοηθήσει μέσα από αυτή την σύγκριση στον ορισμό κριτηρίων αξιολόγησης για την απόφαση ενός οργανισμού να κάνει χρήση υπολογιστών πόρων μίας υποδομής ΥΝ ή όχι.

Σε αυτό το πλαίσιο θα βοηθήσει η πραγματοποίηση μίας ανάλυσης κινδύνου για μία από τις υπό σύγκριση υποδομές. Η ανάλυση αυτή περιλαμβάνει:

1. την καταγραφή των κινδύνων (απειλές, αδυναμίες) για κάθε σύνολο πληροφοριακών πόρων (δηλαδή μίας τυπικής υποδομής υπολογιστικού νέφους)
2. την αξιολόγηση των μέτρων ασφαλείας σε μία τέτοια υποδομή υπό την μορφή είτε υπολογιστών μέσων ή δικλείδων ασφαλείας (πχ ρήτρες μέσα σε συμβάσεις πελάτη-προμηθευτή)

3. το ευρύτερο περιβάλλον που διέπει την λειτουργία και χρήση της εκάστοτε υποδομής (πχ νομοθεσία, αρχές προστασίας προσωπικών δεδομένων στη χώρα ή χώρες στις οποίες λειτουργεί μία τέτοια υποδομή).

Η ανάλυση αυτή σίγουρα είναι δύσκολο να πραγματοποιηθεί με επιτυχία μελετώντας τις πληροφορίες που παρέχουν οι προμηθευτές. Αντίθετα, είναι προτιμότερο να συλλεχθούν στοιχεία από επιθεωρητές που έχουν εμπειρία στην αξιολόγηση συστημάτων ασφαλείας είτε IT υποδομών εντός του οργανισμού ή σε υπολογιστικό νέφος για την παροχή της σχετικής πιστοποίησης (ISO 27001 Auditor).

Επομένως η εργασία αυτή έχει την εξής δομή:

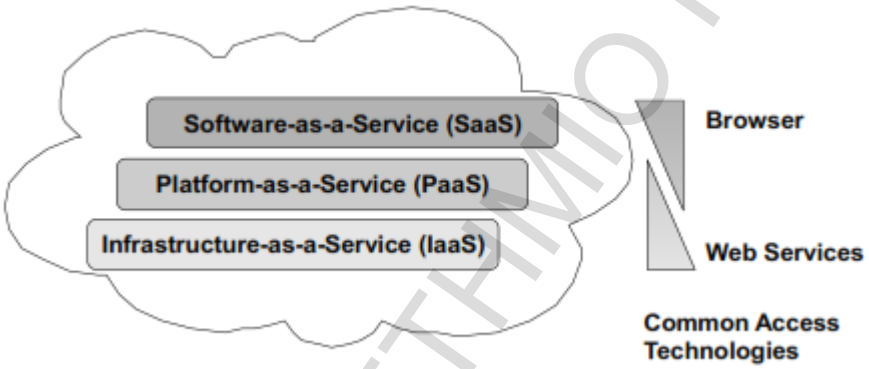
- Το κεφάλαιο 2 κάνει μία καταγραφή των πρακτικών και των μοντέλων διαχείρισης ασφάλειας όπως εφαρμόζονται στις τωρινές υποδομές ΥΝ. Από την άλλη πλευρά, καταγράφει επίσης και ταξινομεί τις ευπάθειες και επιθέσεις που έχουν αντιμετωπίσει κατά καιρούς οι πλατφόρμες αυτές.
- Το κεφάλαιο 3 κάνει μία εκτενή αναφορά σε τρεις σημαντικές υποδομές υπολογιστικού νέφους: τις cloud υπηρεσίες της Amazon, EMC, και της Oracle. Κάθε μία εξειδικεύεται σε ένα διαφορετικό τύπο υπηρεσιών (public, hybrid, private cloud αντίστοιχα). Με βάση συγκεκριμένα κριτήρια κόστους, επιπέδου παροχής υπηρεσιών, ασφάλειας πραγματοποιείται μία σύγκριση τους στο τέλος του κεφαλαίου.
- Στο κεφάλαιο 4 έχει επιλεχθεί η πλατφόρμα ΥΝ της EMC για την ανάλυση κινδύνων που έχει να αντιμετωπίσει ένας χρήστης της πλατφόρμας και πόσο σοβαροί ή μη αξιολογούνται με βάση μία ορισμένη μεθοδολογία η οποία εφαρμόζεται στην ενότητα αυτή.

2. ΑΣΦΑΛΕΙΑ ΥΠΟΛΟΓΙΣΤΙΚΟΥ ΝΕΦΟΥΣ

Υπολογιστικό Νέφος (ΥΝ)

Σε μία έκθεση του οίκου Gartner (Brodkin 2008) το υπολογιστικό νέφος ορίζεται ως μία υπηρεσία με μαζικά επεκτάσιμες δυνατότητες πληροφορικής οι οποίες παρέχονται σε εξωτερικούς πελάτες χρησιμοποιώντας τις τεχνολογίες του Διαδικτύου. Η υπηρεσία αυτή διαθέτει μοναδικά χαρακτηριστικά που απαιτούν την αξιολόγηση του κινδύνου σε τομείς όπως η ακεραιότητα των δεδομένων, η ανάκτηση και προστασία προσωπικών και απόρρητων δεδομένων, καθώς και την αξιολόγηση των νομικών ζητημάτων σε τομείς όπως ο αυτόματος εντοπισμός νέων υπηρεσιών (e-discovery), η συμμόρφωση με τους κανονισμούς, και η πραγματοποίηση ελέγχων. Υπηρεσίες ΥΝ με τις παραπάνω δυνατότητες προσφέρουν μεγάλοι πάροχοι όπως η Amazon (EC2), Google (App Engine).

Σύμφωνα με τον ορισμό του ΥΝ, ένα τέτοιο σύστημα προσφέρει δυναμική επεκτάση πόρων για την παροχή μίας υπηρεσίας μέσω του Διαδικτύου και ως εκ τούτου υπόσχεται πολλά οικονομικά οφέλη που θα διανεμηθούν μεταξύ των εμπλεκομένων. Ανάλογα με τον τύπο των πόρων που παρέχονται από ΥΝ, μπορούν να οριστούν διακριτά στρώματα (Εικόνα 1).



Εικόνα 1: στρώματα υπολογιστικού νέφους και τεχνολογίες πρόσβασης (Jensen, M. ; Horst Gortz; Schwenk, J. ; Gruschka, N. ; Iacono, L.L., 2009)

Το πιο χαμηλό στρώμα παρέχει βασικές υποδομές και συστατικά όπως επεξεργαστική ισχύ, μνήμη και αποθήκευση, και ονομάζονται Υποδομές-ως-Υπηρεσία (IaaS). Η υποδομή Elastic Compute Cloud (EC2) της Amazon είναι ένα σημαντικό παράδειγμα για το μοντέλο IaaS. Στην κορυφή του IaaS, επιτρέπει την φιλοξενία εφαρμογών σε ένα συγκεκριμένο περιβάλλον ειδικά διαμορφωμένο για τις υπηρεσίες αυτές. Το μοντέλο αυτό ονομάζεται Πλατφόρμα-ως-Υπηρεσία με χαρακτηριστικό παράδειγμα την πλατφόρμα App Engine της Google. Το πιο πάνω επίπεδο, Εφαρμογές-ως-Υπηρεσία, προσφέρει στους χρήστες έτοιμες προς χρήση εφαρμογές. Για την πρόσβαση σε όλες τις παραπάνω υποδομές του ΥΝ απαιτούνται δύο ειδών τεχνολογίες: υπηρεσίες ιστού είναι απαραίτητες για την πρόσβαση σε υπηρεσίες IaaS, ενώ ο περιηγητής ιστού είναι χρήσιμος για τη πρόσβαση σε εφαρμογές SaaS. Η πρόσβαση σε υπηρεσίες PaaS γίνεται και με τους δύο τρόπους (Jensen, M. ; Horst Gortz; Schwenk, J. ; Gruschka, N. ; Iacono, L.L., 2009).

Όλα τα παραπάνω μοντέλα υπόσχονται μείωση των κεφαλαιακών δαπανών (κόστος επένδυσης), και περιλαμβάνει μείωση του κόστους του υλικού στο στρώμα IaaS και μειωμένο κόστος αδειών σε όλα τα στρώματα. Ειδικά το στρώμα IaaS εξασφαλίζει για ένα πελάτη ένα εικονικό κέντρο δεδομένων με τη μέγιστη δυνατή απόδοση και βέλτιστη αξιοποίηση των διαθέσιμων πόρων . Επιπλέον, εξασφαλίζονται μειώσεις των λειτουργικών δαπανών (OpEx) λόγω της χρήσης λιγότερου υλικού, αδειών και ενημερωμένων εκδόσεων προγραμμάτων.

Μία σύγχρονη υποδομή ΥΝ περιλαμβάνει πέντε βασικά χαρακτηριστικά (Takabi, H;Joshi, J.B.D.;Gail-Joon Ahn, 2010): αυτό εξυπηρέτηση κατά απαίτηση, πανταχού πρόσβαση στο δίκτυο, διάθεση πόρων ανεξάρτητα από την τοποθεσία τους, ταχεία ελαστικότητα, και μετρήσιμη παροχή υπηρεσίας. Η ταχεία ελαστικότητα επιτρέπει τη γρήγορη κλιμάκωση ή αποκλιμάκωση της διάθεσης πόρων για μία υπηρεσία. Μετρήσιμη παροχή υπηρεσιών σημαίνει την εφαρμογή συγκεκριμένων επιχειρησιακών μοντέλων και βοηθούν τους παρόχους να διαχειριστούν και να βελτιστοποιήσουν τη χρήση των υπολογιστικών πόρων μέσω εργαλείων αυτοματοποιημένης κατανομής πόρων, εξισορρόπησης φορτίου, και καταμέτρησης.

Στο ΥΝ εφαρμόζονται επιπρόσθετα τα εξής μοντέλα υλοποίησης: δημόσια, ιδιωτικά, υβριδικά και ΥΝ για μία συγκεκριμένη κοινότητα χρηστών. Τα ΥΝ δημόσιας χρήσης είναι διαθέσιμα στο ευρύ κοινό ενώ τα ιδιωτικής χρήσης ΥΝ είναι διαθέσιμα για αποκλειστική χρήση των εκάστοτε οργανισμών. Υπάρχουν επίσης ΥΝ που είναι αφιερωμένα σε μία ορισμένη κοινότητα ή ομάδα.

Προσωπικά Δεδομένα

Προσωπικά στοιχεία (Tharam Dillon, Chen Wu, Elizabeth Chang 2010) ενός χρήστη του ΥΝ αφορούν κάθε πληροφορία που θα μπορούσε να χρησιμοποιηθεί για τον εντοπισμό ενός ατόμου (π.χ. περιοχή, όνομα, διεύθυνση) ή πληροφορίες που μπορεί να συσχετιστούν με άλλες πληροφορίες για τον εντοπισμό ενός ατόμου (π.χ. αριθμός πιστωτικής κάρτας, η IP[1] διεύθυνση).

- Πληροφορίες σχετικά με τη θρησκεία, τη φυλή, την υγεία, τον συνδικαλισμό, τον σεξουαλικό προσανατολισμό, την απόδοση στην εργασία, χρηματοοικονομικές πληροφορίες, βιομετρικές πληροφορίες ή οποιαδήποτε άλλες πληροφορίες που μπορεί να θεωρηθούν ευαίσθητες.
- Τα δεδομένα που συλλέγονται από τις συσκευές υπολογιστή (π.χ. λάπτοπ, έξυπνο τηλέφωνο, ταμπλέτα-υπολογιστής).
- Πληροφορίες μοναδικά ανιχνεύσιμες σε μια συσκευή του χρήστη (π.χ. διεύθυνση IP, Radio Frequency Identity (RFID), Διεύθυνση MAC).

2.1 ΠΡΑΚΤΙΚΕΣ ΔΙΑΧΕΙΡΙΣΗΣ ΑΣΦΑΛΕΙΑΣ – ΠΡΟΤΥΠΑ

Σύμφωνα με τους (Tharam Dillon, Chen Wu, Elizabeth Chang 2010) πρότυπα που έχουν σχέση με τη διαχείριση της ασφάλειας πρακτικών στο ΥΝ είναι το Information Technology Infrastructure Library (ITIL), ISO / IEC 27001/27002 και το Open Virtualization Format (OVF).

[1] Internet Protocol

Information Technology Infrastructure Library (ITIL)

Αποτελεί ένα σύνολο από βέλτιστες πρακτικές και κατευθυντήριες γραμμές οι οποίες ορίζουν μια ολοκληρωμένη διαδικασία προσέγγισης για τη διαχείριση υπηρεσιών πληροφορικής (Tharam Dillon, Chen Wu, Elizabeth Chang 2010). Το ITIL μπορεί να εφαρμοστεί σχεδόν κάθε είδος περιβάλλον πληροφορικής, συμπεριλαμβανομένων το περιβάλλον λειτουργίας του ΥΝ. Το ITIL επιδιώκει να διασφαλίσει ότι λαμβάνονται αποτελεσματικά μέτρα ασφάλειας των πληροφοριών σε στρατηγικό, τακτικό και επιχειρησιακό επίπεδο. Η ασφάλεια των πληροφοριών θεωρείται μια επαναληπτική διαδικασία που πρέπει να είναι ελεγχόμενη, σχεδιασμένη, να έχει υλοποιηθεί, αξιολογηθεί και να ενημερώνεται με στόχο τη βελτίωση της.

Το ITIL διακρίνει την ασφάλεια των πληροφοριών στις παρακάτω ενότητες:

- Πολιτικές: Οι γενικοί στόχοι που ένας οργανισμός προσπαθεί να επιτύχει
- Διεργασίες: Τι πρέπει να συμβεί για να επιτευχθούν οι στόχοι
- Διαδικασία: Ποιος κάνει τι και πότε για την επίτευξη των στόχων
- Οδηγίες εργασίας: Οδηγίες για τη πραγματοποίηση συγκεκριμένων δράσεων

Ένας βασικός στόχος της διαχείρισης της ασφάλειας είναι να διασφαλίσει επαρκή ασφάλεια των πληροφοριών. Ο πρωταρχικός στόχος της ασφάλειας πληροφοριών, με τη σειρά της, είναι η προστασία των πληροφοριών έναντι των κινδύνων, και έτσι να διατηρηθεί η αξία τους στον οργανισμό. Αυτό συνήθως εκφράζεται σε όρους διασφάλισης της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας τους, μαζί με τις σχετικές ιδιότητες ή στόχους όπως η αυθεντικότητα, λογοδοσία, μη άρνηση και αξιοπιστία.

International Organization for Standardization (ISO) 27001/27002

Το πρότυπο ISO / IEC 27001 καθορίζει επίσημα τις υποχρεωτικές απαιτήσεις για ένα Σύστημα Διαχείρισης της Ασφάλειας των Πληροφοριών (ISMS). Είναι επίσης ένα πρότυπο πιστοποίησης και χρησιμοποιεί το πρότυπο ISO / IEC 27002 για να υποδείξει κατάλληλους μηχανισμούς ελέγχου της ασφάλειας των πληροφοριών εντός του Συστήματος Διαχείρισης της Ασφάλειας των Πληροφοριών.

Το πρότυπο βοηθά τους οργανισμούς να εσωτερικεύουν και να απαντούν σε βασικά ερωτήματα, όπως:

- Πώς μπορεί να βεβαιωθεί ο οργανισμός ότι τα τρέχοντα επίπεδα ασφαλείας είναι κατάλληλα για τις ανάγκες του;
- Πώς μπορεί να εφαρμόσει μια βασική γραμμή ασφάλειας σε ολόκληρη την τη λειτουργία του οργανισμού;
- Πώς μπορεί να βεβαιωθεί ότι οι υπηρεσίες του είναι ασφαλείς;

Open Virtualization Format

Το OVF επιτρέπει την αποτελεσματική, ευέλικτη και ασφαλή διανομή του λογισμικού των επιχειρήσεων, διευκόλυνση της κινητικότητας των εικονικών μηχανών και δίνοντας στους πελάτες ανεξαρτησία προμηθευτή και πλατφόρμας. Οι πελάτες μπορούν να αναπτύξουν μια διαμορφωμένη εικονική με βάση το πρότυπο OVF για την εικονική πλατφόρμα της επιλογής τους.

Η αύξηση των επενδύσεων σε υποδομές εικονικών συσκευών (IBM, Microsoft, Hewlett-Packard, Dell, VMware και XenSource) βοήθησε στην απλοποίηση της ανάπτυξης εφαρμογών για μεμονωμένους χρήστες αλλά επίσης ενδυναμώνουν τις αρχιτεκτονικές ΥΝ επόμενης γενιάς. Είναι πλέον εύκολο να αναπαραχθούν και να διανεμηθούν εικονικές μηχανές με όλες τις απαραίτητες διαμορφώσεις για την ασφάλεια και την προστασία του απόρρητου της λειτουργίας τους.

2.2 ΜΟΝΤΕΛΑ ΔΙΑΧΕΙΡΙΣΗΣ ΑΣΦΑΛΕΙΑΣ ΣΤΟ ΥΝ

Οι (Tharam Dillon, Chen Wu, Elizabeth Chang 2010) έχουν μελετήσει είκοσι τέτοια μοντέλα διαχείρισης ασφάλειας και τις απαιτήσεις τους σχετικά με το ΥΝ. Κρίνουν ότι οι απαιτήσεις αυτές πρέπει να λαμβάνονται σοβαρά υπόψη από τους παρόχους ΥΝ καθώς καταρτίζουν τα προγράμματα συμμόρφωσης:

1. Λογισμικό-ως-Υπηρεσία – ασφάλεια: SaaS[2] είναι το κυρίαρχο μοντέλο υπηρεσιών στο ΥΝ για το εγγύς μέλλον και ο τομέας στον οποίο θα παραμείνει η κρίσιμη ανάγκη για πρακτικές ασφάλειας και εποπτείας. Ακριβώς όπως με ένα πάροχο υπηρεσιών, εταιρείες ή οι τελικοί χρήστες θα πρέπει να ερευνήσουν τις πολιτικές των προμηθευτών ΥΝ για την ασφάλεια των δεδομένων πριν από τη χρήση των υπηρεσιών του προμηθευτή για να αποφευχθεί η απώλεια ή να μην είναι σε θέση να έχουν πρόσβαση στα δεδομένα τους.

2. Διαχείριση Ασφάλειας (Άνθρωποι): θα πρέπει ο πάροχος να έχει καταρτίσει ένα οργανόγραμμα της ομάδας ανθρώπων οι οποίοι είναι υπεύθυνοι για την ασφάλεια και τον όλο σχεδιασμό. Το οργανόγραμμα θα πρέπει να αποτυπώνει συγκεκριμένους ρόλους και αρμοδιότητες οι οποίοι να συμβαδίζουν με τον στρατηγικό σχεδιασμό του οργανισμού, τα στελέχη της ομάδας αυτής να έχουν γνώση πως οι γνώσεις και ικανότητες τους συμβαδίζουν με τους επιχειρησιακούς στόχους του οργανισμού.

Ο οίκος Gartner (Brodkin 2008) τονίζει τη σημασία του ελέγχου των προνομίων των χρηστών (εσωτερικών και εξωτερικών) κατά τη πρόσβαση τους στο σύστημα. Καθώς οι πελάτες ενός ΥΝ επεξεργάζονται ευαίσθητα δεδομένα έξω από την επιχείρηση τους, αυτή η πραγματικότητα φέρνει μαζί της ένα εγγενή επίπεδο κινδύνου. Οι υπηρεσίες που παρέχονται από τρίτους (outsourcing) όπως αυτές του ΥΝ παρακάμπτουν πλέον τους συνήθεις φυσικούς, λογικούς και ανθρώπινου δυναμικού ελέγχους που εφαρμόζονται εσωτερικά μίας επιχείρησης.

[2] Software-as-a-Service

Συνεπώς οι πελάτες ενός ΥΝ πρέπει να αποκτήσουν όσο το δυνατόν περισσότερες πληροφορίες για το ανθρώπινο δυναμικό που διαχειρίζεται τα δεδομένα. Θα πρέπει να απευθύνουν ερωτήματα προς τους παρόχους για την παροχή συγκεκριμένων πληροφοριών σχετικά με την πρόσληψη και την εποπτεία των διαχειριστών οι οποίοι έχουν τα περισσότερα δικαιώματα, και τον τρόπο με τον οποίο ελέγχουν την πρόσβαση τους.

1. Διακυβέρνηση για την ασφάλεια: Μια διευθύνουσα επιτροπή ασφάλειας θα πρέπει να αναπτυχθεί, στόχος της οποίας είναι να επικεντρωθεί στο να παρέχει καθοδήγηση σχετικά με τις πρωτοβουλίες για την ασφάλεια και της ευθυγράμμισης των σχετικών στόχων με τους στόχους των επιχειρήσεων και των στρατηγικών.

2. Διαχείριση κινδύνου: Η διαχείριση του κινδύνου αφορά τον προσδιορισμό των τεχνολογιών που αποτελούν περιουσιακά στοιχεία του οργανισμού, τη ταυτοποίηση δεδομένων και των δεσμών τους με τις επιχειρηματικές διαδικασίες, τις εφαρμογές, και τις βάσεις δεδομένων, καθώς και τη μεταβίβαση της κυριότητας και την επιμέλεια των αρμοδιοτήτων. Οι ιδιοκτήτες έχουν την εξουσία και λογοδοσία για τα περιουσιακά στοιχεία, συμπεριλαμβανομένων απαιτήσεων για την προστασία πληροφοριών, και οι θεματοφύλακες ασχολούνται με την εφαρμογή της εμπιστευτικότητας, ακεραιότητας, διαθεσιμότητας και ελέγχου των απόρρητων δεδομένων.

3. Αξιολόγηση του κινδύνου: η αξιολόγηση του κινδύνου για την ασφάλεια είναι ζωτικής σημασίας για τον οργανισμό βοηθώντας στη λήψη αποφάσεων έχοντας την απαραίτητη ενημέρωση και διατηρώντας σε μία ισορροπία την το τι είναι χρήσιμο για την επιχείρηση και την προστασία των περιουσιακών στοιχείων της. Μια τυπική διαδικασία διαχείρισης κινδύνων ασφάλειας πληροφοριών θα πρέπει να αξιολογεί τις πληροφορίες για τους κινδύνους, να δημιουργεί ένα σχέδιο για τη διαχείρισή τους σε περιοδική ή μία αναγκαία βάση. Περισσότερο λεπτομερείς και τεχνικές αξιολογήσεις για τους κινδύνους υπό τη μορφή μοντελοποίησης απειλών θα πρέπει επίσης να εφαρμόζεται σε εφαρμογές και τις υποδομές.

4. Ενημέρωση σε θέματα ασφάλειας: Οι άνθρωποι είναι ο πιο αδύναμος κρίκος για την ασφάλεια. Η γνώση και μία συγκεκριμένη κουλτούρα στον οργανισμό είναι από ορισμένα αποτελεσματικά εργαλεία για τη διαχείριση των κινδύνων που σχετίζονται με τους ανθρώπους. Χωρίς τη παροχή κατάλληλης ενημέρωσης και κατάρτισης για τους ανθρώπους μπορεί να εκθέσει την εταιρεία σε ένα φάσμα κινδύνων στους οποίους οι άνθρωποι αποτελούν την κύρια πηγή ευπαθειών παρά τα συστήματα και οι εφαρμογές. Επιθέσεις τύπου social engineering, αναφορές με φτωχά στοιχεία, καθυστερημένη ανταπόκριση σε ενδεχόμενα περιστατικά ασφάλειας, και ακούσιες διαρροές δεδομένων από τη πλευρά των πελατών είναι όλοι δυνατοί και πιθανοί κίνδυνοι που μπορεί να προκληθούν από την έλλειψη ενός αποτελεσματικού προγράμματος ευαισθητοποίησης σε θέματα ασφάλειας.

5. Εκπαίδευση και κατάρτιση: πρέπει να αναπτυχθούν προγράμματα εκπαίδευσης για την κατάρτιση σε βασικές δεξιότητες διαχείρισης κινδύνου και διάχυσης γνώσης προς την ομάδα ασφαλείας.

6. Πολιτικές και πρότυπα: η ομάδα ασφάλειας ενός ΥΝ πρέπει πρώτα να προσδιορίσει την ασφάλεια των πληροφοριών και τις επιχειρηματικές απαιτήσεις ειδικά για την ασφάλεια

του ΥΝ, του λογισμικού ως υπηρεσία (SaaS), ή για λογισμικό συλλογικών εφαρμογών. Πρέπει να αναπτυχθούν πολιτικές, να τεκμηριωθούν να εφαρμοστούν μαζί με την τεκμηρίωση για σχετικά πρότυπα που τις υποστηρίζουν όπως και κατευθυντήριες γραμμές.

Η κανονιστική συμμόρφωση (Brodkin 2008) μέσα στην οποία λειτουργεί ο κάθε πάροχος υπηρεσιών ΥΝ, αναγνωρίζει ότι οι πελάτες έχουν την τελική ευθύνη για την ασφάλεια και την ακεραιότητα των δικών τους δεδομένων, ακόμη και όταν κατέχονται από ένα φορέα παροχής υπηρεσιών. Οι πάροχοι υπηρεσιών υπόκεινται σε εξωτερικούς ελέγχους και απαιτείται να ανανεώνουν τις πιστοποιήσεις για την ασφάλεια. Οι πάροχοι που αρνούνται να υποβληθούν σε ένα τέτοιο έλεγχο "σηματοδοτούν ότι οι πελάτες μπορούν να τα χρησιμοποιούν μόνο για τις πιο ασήμαντες λειτουργίες.

7. Διαχείριση κινδύνου τρίτων: Έλλειψη προγράμματος διαχείρισης κινδύνου τρίτων μπορεί να οδηγήσει σε βλάβη της φήμης του παρόχου, απώλειες εσόδων, καθώς και μη εκτέλεση νομικών ενεργειών λόγω κακής επιμέλειας των προμηθευτών.

8. Αξιολόγηση ευπαθειών: ταξινομεί τα περιουσιακά στοιχεία του δικτύου για να θέσει τις προτεραιότητες ανάμεσα σε προγράμματα μείωσης των ευπαθειών, όπως προγράμματα επιδιόρθωσης και αναβάθμισης του συστήματος.

9. Έλεγχος εικόνων ασφαλείας: η υποδομή των εικονικών μηχανών του ΥΝ παρέχει τη δυνατότητα να δημιουργηθούν "δοκιμαστικές εικόνες υπολογιστών" οι οποίες αφού χτιστούν με ασφάλεια μπορούν μετά να κλωνοποιηθούν σε πολλαπλά αντίγραφα.

10. Διακυβέρνηση δεδομένων: Το πλαίσιο αυτό θα πρέπει να περιγράψει ποιός μπορεί να εκτελέσει ποιες ενέργειες με ποιες πληροφορίες, και πότε, κάτω από ποιες συνθήκες και με ποιές μεθόδους.

11. Ασφάλεια των δεδομένων: Η ασφάλεια θα πρέπει να μετακινηθεί στο επίπεδο των δεδομένων, έτσι ώστε οι επιχειρήσεις να μπορούν να είναι βέβαιοι ότι τα δεδομένα τους προστατεύονται όπου και αν πηγαίνουν.

12. Ασφάλεια εφαρμογών: τα χαρακτηριστικά και οι απαιτήσεις για την ασφάλεια των εφαρμογών ορίζονται και αξιολογούνται τα αποτελέσματα των δοκιμών ασφάλειας.

13. Ασφάλεια των εικονικών μηχανών: Στο περιβάλλον του ΥΝ, οι φυσικοί εξυπηρετητές ενοποιούνται σε πολλαπλές εικονικές μηχανές. Αυτό διευκολύνει την αναπαραγωγή τυπικών ελέγχων ασφαλείας στο ευρύτερο κέντρο δεδομένων προκειμένου να εξασφαλιστεί η μέγιστη δυνατή ασφάλεια για τις εικονικές μηχανές. Με τον τρόπο αυτό ακόμη και οι μηχανές που πρόκειται να μεταβούν στο ΥΝ μπορούν να προετοιμαστούν κατάλληλα.

14. Ταυτότητα και διαχείριση της πρόσβασης: η ταυτότητα και η διαχείριση της πρόσβασης είναι μια κρίσιμη λειτουργία για κάθε οργανισμό, και μία από τις βασικές αρχές των πελατών, γνωστή και ως αρχή της «ελάχιστης πρόσβασης». Η αρχή της ελάχιστης πρόσβασης είναι ότι χορηγείται μόνο η ελάχιστη πρόσβαση για να εκτελεστεί μια λειτουργία, και ότι η πρόσβαση χορηγείται μόνο για το ελάχιστο χρονικό διάστημα που απαιτείται.

15. Διαχείριση αλλαγών: η ομάδα ασφαλείας μπορεί να δημιουργήσει κατευθυντήριες γραμμές ασφαλείας για τα πρότυπα και μικρές αλλαγές, για να παρέχει δυνατότητες αυτόματης πραγματοποίησης αυτών των αλλαγών και να ορίσει την προτεραιότητα στο χρόνο και τους πόρους της ομάδας ασφαλείας για τη πραγματοποίηση περισσότερων πολύπλοκων και σημαντικών αλλαγών στην παραγωγή.

16. Φυσική ασφάλεια: η μαζική επένδυση που απαιτείται για την κατασκευή υψηλού επιπέδου ασφάλειας είναι ο κύριος λόγος που οι εταιρείες δεν χτίζουν πλέον τα δικά τους κέντρα δεδομένων, και ένας από τους πολλούς λόγους για τους οποίους απευθύνονται σε υπηρεσίες ΥΝ.

17. Αποκατάσταση λειτουργίας μετά από καταστροφή: σε ένα περιβάλλον Λογισμικό-ως-Υπηρεσία, οι πελάτες εξαρτώνται σε μεγάλο βαθμό στην 24/7/365 πρόσβαση στις υπηρεσίες τους και κάθε διακοπή πρόσβασης μπορεί να είναι καταστροφική.

18. Προστασία των προσωπικών δεδομένων: Μια διευθύνουσα επιτροπή πρέπει να δημιουργηθεί για να βοηθήσει τη λήψη αποφάσεων που σχετίζονται με τα απόρρητα και προσωπικά δεδομένα των πελατών.

Επιπλέον τονίζεται η ανάγκη προσδιορισμού της θέσης των δεδομένων με σαφή και συμβατικό τρόπο (Brodkin 2008). Οι πελάτες θα πρέπει να γνωρίζουν ακριβώς πού φιλοξενούνται τα δεδομένα τους και να ζητούν από τους παρόχους να δεσμευτούν για την αποθήκευση και επεξεργασία των δεδομένων σε συγκεκριμένες χώρες. Θα πρέπει επίσης να υπάρχει συμβατική δέσμευση ότι ο πάροχος θα υπακούσει στις τοπικές απαιτήσεις προστασίας των προσωπικών δεδομένων και κάθε τι άλλο σχετικά με το λογαριασμό των πελατών τους.

Ένας άλλος κρίσιμος παράγοντας είναι ο διαχωρισμός των δεδομένων σύμφωνα με τον οίκο Gartner (Brodkin 2008). Τα δεδομένα στο σύννεφο είναι συνήθως σε ένα περιβάλλον από κοινού μαζί με δεδομένα από άλλους πελάτες. Η κρυπτογράφηση είναι αποτελεσματική, αλλά δεν είναι πανάκεια. Ωστόσο οι πελάτες θα πρέπει να γνωρίζουν πως οι πάροχοι φροντίζουν να διαχωρίζουν τα δεδομένα όταν αποθηκεύονται. Ο πάροχος θα πρέπει να παρέχει αποδεικτικά στοιχεία ότι τα συστήματα κρυπτογράφησης έχουν σχεδιαστεί και δοκιμαστεί από έμπειρους ειδικούς. Ατυχήματα κατά την κρυπτογράφηση μπορούν να κάνουν τα δεδομένα εντελώς άχρηστα, και ακόμη και η κανονική κρυπτογράφηση μπορεί να περιπλέξει τη διαθεσιμότητα των δεδομένων.

Επίσης ο πάροχος πρέπει να περιγράψει τι θα συμβεί στα δεδομένα και πώς θα εξυπηρετήσει τους πελάτες σε περίπτωση καταστροφής. Κάθε προσφορά υπηρεσιών ΥΝ που δεν αναπαράγει την υποδομή δεδομένων και εφαρμογών σε πολλαπλές θέσεις είναι ευάλωτη σε μια συνολική αποτυχία. Ο πελάτης θα πρέπει να αξιολογήσει αν ο πάροχος έχει την ικανότητα να κάνει μια πλήρη αποκατάσταση, και πόσο καιρό θα πάρει.

Υποστήριξη νομικής διερεύνησης. Η διερεύνηση ακατάλληλης ή παράνομη δραστηριότητας μπορεί να είναι αδύνατο στο υπολογιστικό νέφος, γιατί πρέπει να διερευνηθεί η καταγραφή δεδομένων για πολλαπλούς πελάτες που συστεγάζονται. Επίσης η καταγραφή ενδέχεται να εξαπλώνεται σε πολλαπλούς εξυπηρετητές και κέντρα δεδομένων. Στη περίπτωση αυτή είτε θα θα υπάρχει συμβατική δέσμευση για την υποστήριξη ειδικών μορφών έρευνας, μαζί με την

απόδειξη ότι ο πωλητής έχει ήδη υποστηρίξει με επιτυχία τέτοιες δραστηριότητες, ή θα πρέπει να ληφθεί υπόψη ότι η ανακάλυψη και εξερεύνηση τέτοιων αιτήσεων θα είναι αδύνατη.

Η μακροπρόθεσμη βιωσιμότητα των δεδομένων είναι επίσης σημαντική καθώς ένας πάροχος ΥΝ μπορεί να διακόψει τη λειτουργία του ή να αποκτηθεί από μια μεγαλύτερη εταιρεία. Ο πελάτης θα πρέπει να βεβαιωθεί ότι τα δεδομένα θα παραμείνουν διαθέσιμα, ακόμη και μετά από ένα τέτοιο γεγονός. Η σύμβαση στη περίπτωση αυτή θα πρέπει να προβλέπει πως θα γίνει η επιστροφή των δεδομένων και σε ποια μορφή έτσι ώστε να γίνει άμεσα η μετάπτωση των δεδομένων σε μία άλλη υποδομή.

2.2.1 Επεκτασιμότητα και Κοινή Ευθύνη

Οι πάροχοι ΥΝ και οι πελάτες θα πρέπει να μοιραστούν την ευθύνη για την ασφάλεια και την προστασία των προσωπικών δεδομένων, αλλά ο επιμερισμός των ευθυνών διαφέρει στα διάφορα μοντέλα υλοποίησης, και ο βαθμός επιμερισμού επηρεάζει με τη σειρά του τον βαθμό επεκτασιμότητας του ΥΝ (Takabi, H;Joshi, J.B.D.;Gail-Joon Ahn, 2010):

- Σε υποδομές Λογισμικό-ως-Υπηρεσία, οι πάροχοι προσφέρουν υπηρεσίες με μεγάλο αριθμό ολοκληρωμένων χαρακτηριστικών, επιτρέποντας έτσι μικρότερη επεκτασιμότητα για τους πελάτες. Οι πάροχοι είναι περισσότερο υπεύθυνοι για την ασφάλεια και την ιδιωτικότητα των υπηρεσιών. Αυτό ισχύει αρκετά στα ιδιωτικά ΥΝ στα οποία ο πελάτης-οργανισμός θέτει αυστηρές απαιτήσεις ασφάλειας, ενώ ενδεχομένως ζητούν περισσότερες επεκτάσεις για να ικανοποιήσουν όλες τις ανάγκες εντός του οργανισμού.
- Σε υποδομές Πλατφόρμα-ως-Υπηρεσία, οι πάροχοι δίνουν τον απαραίτητο χώρο σε προγραμματιστές για να υλοποιήσουν τις δικές τους εφαρμογές και να τις διαθέσουν στους πελάτες τους. Επομένως οι ίδιοι οι προγραμματιστές είναι αρμόδιοι για τη διασφάλιση της προστασίας των εφαρμογών, ενώ οι πάροχοι οφείλουν να απομονώσουν τις εφαρμογές και τους χώρους εργασίας των πελατών-προγραμματιστών.
- Το μοντέλο Υποδομή-ως-Υπηρεσία θεωρείται το πιο επεκτάσιμο ενώ προσφέρει πολύ λίγα χαρακτηριστικά σε επίπεδο εφαρμογών. Το μοντέλο αυτό υποθέτει ότι οι πελάτες διαμορφώνουν τον μηχανισμό ασφάλειας των λειτουργικών συστημάτων, εφαρμογών και περιεχομένου. Ο πάροχος εξασφαλίζει τις ελάχιστες προϋποθέσεις προστασίας των δεδομένων.

Η πολύ-μίσθωση είναι ένα άλλο μοναδικό χαρακτηριστικά των υποδομών ΥΝ, ιδιαίτερα για τα δημόσιου τύπου (Takabi, H;Joshi, J.B.D.;Gail-Joon Ahn, 2010). Ουσιαστικά επιτρέπει στους παρόχους να εκμεταλλεύονται τους πόρους πιο αποδοτικά διαχωρίζοντας μία εικονική κοινή υποδομή ανάμεσα σε πολλούς πελάτες. Η πραγματικότητα αυτή συνήθως προκαλεί ανησυχία στους πελάτες ωστόσο το επίπεδο διαμοιρασμού των πόρων και οι διαθέσιμοι μηχανισμοί προστασίας μπορούν να κάνουν μεγάλη διαφορά. Ένα χαρακτηριστικό παράδειγμα είναι η υπηρεσία Salesforce.com: εφαρμόζει επανεγγραφή ερωτημάτων στη βάση δεδομένων της υπηρεσίας ενώ η Amazon εφαρμόζει μηχανισμό εποπτικού ελέγχου (hypervisor) σε επίπεδο υλικού.

2.2.2 Επίπεδα Παροχής Υπηρεσιών

Ένα SLA[3] ορίζει το επίπεδο παροχής υπηρεσιών και διατυπώνεται ρητά στη σύμβαση ανάμεσα στον πελάτη και τον πάροχο (Takabi, H;Joshi, J.B.D.;Gail-Joon Ahn, 2010). Καταγράφει την κοινή αντίληψη ανάμεσα στα δύο μέρη σχετικά με υπηρεσίες, προτεραιότητες, ευθύνες, εγγυήσεις και ρήτρες. Έτσι στο ΥΝ τα επίπεδα παροχής υπηρεσιών που διατυπώνονται ελέγχουν τη χρήση των υπολογιστών πόρων. Ως εκ τούτου, το κύριο ζήτημα για το ΥΝ είναι να χτίσει ένα νέο στρώμα για να υποστηρίξει τη δυναμική διαπραγμάτευση μίας σύμβασης και να παρακολουθεί την εφαρμογή των κανόνων της σύμβασης.

Η ασφάλεια, προστασία των προσωπικών δεδομένων και η εμπιστοσύνη δεν μπορούν να ποσοτικοποιηθούν ωστόσο μπορούν να εφευρεθούν μηχανισμοί για τη διασφάλιση των πελατών. Οι καταναλωτές μπορεί να μην εμπιστεύονται πλήρως το επίπεδο εμπιστοσύνης που διατίθεται από ένα φορέα παροχής υπηρεσιών, και μπορεί να απαιτεί συμφωνημένη μεσολάβηση τρίτων για να αξιολογήσουν κρίσιμες παραμέτρους του συμφωνηθέντος επιπέδου υπηρεσιών και να συντάξει έκθεση με τυχόν παραβιάσεις.

2.2.3 Επόπτες Εικονικότητας (Hypervisors)

Ο επόπτης εικονικότητας διατίθεται ως μέρος του λογισμικού διαχείρισης εικονικών μηχανών και επιτρέπει σε πολλαπλά λειτουργικά συστήματα να τρέχουν σε έναν κεντρικό υπολογιστή ταυτόχρονα. Εξασφαλίζει μεν ένα τεχνολογικό μέσο για τη δημιουργία και επιμερισμό εικονικών πόρων, η παρουσία αυτής της τεχνολογίας αυξάνει επίσης την πιθανότητα επιθέσεων. Χρειάζονται μηχανισμοί που διασφαλίζουν ισχυρή απομόνωση, κατανομή πόρων με μεσολάβηση, και ασφαλή επικοινωνία ανάμεσα στις εικονικές μηχανές (Takabi, H;Joshi, J.B.D.;Gail-Joon Ahn, 2010).

Για παράδειγμα ο μηχανισμός αυτός θα μπορούσε να επιτρέπει ευέλικτη πρόσβαση σε εικονικές μηχανές όπως και δυνατότητες καταμερισμού μέσα σε ένα εξυπηρετητή ΥΝ. Επιπρόσθετα, είναι αναγκαίο ορισμένες διαδικασίες και το αποτέλεσμα τους να ταυτιστούν με συγκεκριμένες φυσικές μηχανές για τη διασφάλιση της αυθεντικότητας των δεδομένων που παράγονται ή την αυθεντικότητα των φυσικών μηχανών που έχουν επιλεχθεί.

2.2.4 Ταυτοποίηση χρηστών

Ο μηχανισμός ταυτοποίησης επιτρέπει την αναγνώριση των χρηστών με βάση τις διαπιστεύσεις και τους κωδικούς πρόσβασης που διαθέτουν. Η χρήση πολλαπλών πρωτοκόλλων διαπραγμάτευσης και πιστοποίησης των κωδικών πρόσβασης των χρηστών είναι ένα σημαντικό μειονέκτημα στη διαλειτουργικότητα μεταξύ υπηρεσιών ΥΝ. Υπάρχοντες μηχανισμοί που βασίζονται στη χρήση κωδικών πρόσβασης είναι ευάλωτοι ενώ το πλαίσιο λειτουργίας της πολύ-ιδιοκτησίας σε ένα ΥΝ και του τρόπου χειρισμού της ιδιωτικότητας και των στοιχείων πιστοποίησης των χρηστών δεν είναι ξεκάθαρο (Takabi, H;Joshi, J.B.D.;Gail-Joon Ahn, 2010).

Μία από τις προσεγγίσεις σε ερευνητικό επίπεδο είναι η υλοποίηση ομόσπονδων τεχνικών ταυτοποίησης. Οι τεχνικές αυτές εξετάζουν τον σχεδιασμό πρωτοκόλλων ειδικά για την διατήρηση της ιδιωτικότητας χρησιμοποιώντας ορισμένες ιδιότητες της ταυτότητας του χρήστη

[3] Service Level Agreement

και αξιοποιώντας τεχνικές πιστοποίησης που δεν βασίζονται σε υπάρχουσα γνώση. Επιπλέον οι νέες αυτές τεχνικές λαμβάνουν υπόψη την ύπαρξη πολλαπλών ψευδωνύμων και αναγνωριστικών για ένα χρήστη σε μία ομόσπονδη βάση πάνω από την οποία ο χρήστης αποκτά πρόσβαση σε υπηρεσίες από διαφορετικά ΥΝ.

2.2.5 Τιμολόγηση χρηστών

Απαιτείται ένα σύστημα ελέγχου πρόσβασης το οποίο διαχειρίζεται την κατανομή προνομίων αποδοτικά και εξασφαλίζεται διαλειτουργικότητα ανάμεσα στα διαφορετικά μοντέλα ΥΝ. Το μοντέλο ελέγχου πρόσβασης ενσωματώνει προδιαγραφές που έχουν τεθεί στο επίπεδο παροχής υπηρεσιών και που έχει συμφωνηθεί μεταξύ παρόχου και πελάτη. Οι προδιαγραφές αυτές εξασφαλίζουν ότι οποιαδήποτε προσωπικά δεδομένα έχουν δοθεί από τον πελάτη στον πάροχο για λόγους τιμολόγησης δεν θα γίνουν εκμετάλλευση οποιουδήποτε άλλου σκοπού. Οι προδιαγραφές αυτές θα πρέπει να είναι προσβάσιμες προς αξιολόγηση από τις κανονιστικές αρχές (Takabi, H;Joshi, J.B.D.;Gail-Joon Ahn, 2010).

2.2.6 Διασύνδεση πολιτικών

Σε περίπτωση διασύνδεσης πολλαπλών παρόχων για την δημιουργία συνεργειών μεταξύ επιλεγμένων υπηρεσιών τους θα πρέπει να αντιμετωπιστεί το ζήτημα της ασυμβατότητας ανάμεσα στις πολιτικές τους. Αυτό απαιτείται για τον δυναμικό έλεγχο από τον εκάστοτε εμπλεκόμενο για τυχόν παραβιάσεις των πολιτικών ασφαλείας. Παρόλο που οι επιμέρους πολιτικές έχουν ελεγχθεί δεν διασφαλίζεται εξίσου η ασφάλεια των διασυνδεδεμένων πολιτικών. Απαιτείται η δημιουργία ενός πλαισίου εμπιστοσύνης το οποίο να τίθεται σε εφαρμογή δυναμικά σε περίπτωση συνέργειας μεταξύ υπηρεσιών. Το πλαίσιο αυτό πρέπει να συμπεριλαμβάνει όλες τις απαραίτητες παραμέτρους αλληλεπίδρασης, και των επιμέρους πολιτικών που ολοκληρώνονται δυναμικά σε μία ενιαία πολιτική προς διαχείριση (Takabi, H;Joshi, J.B.D.;Gail-Joon Ahn, 2010).

Πλαίσιο Διαχείρισης Εμπιστοσύνης

Για την επίτευξη της διασύνδεσης πολιτικών ανάμεσα σε διαφορετικούς υπολογιστικούς τομείς (domains) σε περιβάλλον ΥΝ απαιτείται η υλοποίηση ενός ανάλογου πλαισίου με γνώμονα την εξασφάλιση της μέγιστης εμπιστοσύνης. Το πλαίσιο αυτό καλείται να διαχειριστεί τη μεταβίβαση προνομίων και δικαιωμάτων πρόσβασης από υποκείμενο (πχ μία υπηρεσία) σε υποκείμενο (πχ μία άλλη υπηρεσία) με τη χρήση μηχανισμών κρυπτογράφησης. Οι μηχανισμοί αυτοί εκτυλίσσουν μία πολύπλοκη αλυσίδα επαλήθευσης και ανάκλησης ανάμεσα στα εμπλεκόμενα μέρη απαιτώντας επίσης σοβαρή υποδομή διαχείρισης κλειδιών κρυπτογράφησης. Το πλαίσιο αυτό θα συνδράμει στην υλοποίηση πλαισίων διασύνδεσης υπηρεσιών τα οποία θα ελέγχονται για την εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα στο σύνολο τους (Takabi, H;Joshi, J.B.D.;Gail-Joon Ahn, 2010).

Η τεχνική που ονομάζεται έλεγχος πρόσβασης βάση ρόλου (RBAC[4]) είναι μία πολλά υποσχόμενη τεχνική εξαιτίας της απλότητας και της ευελιξίας που προσφέρει και του τρόπου με τον οποίο εξασφαλίζει την αρχή του ελάχιστου δυνατού δικαιώματος πρόσβασης σε δυναμικές καταστάσεις. Είναι μία τεχνική ανεξάρτητη από πολιτικές επομένως μπορεί να αξιοποιηθεί κατά

[4] Role based access control

την σύνθεση πολλαπλών πολιτικών όπως αναφέρθηκε παραπάνω. Σε αυτό το πλαίσιο ορίζονται οι υποχρεώσεις και οι επιτρεπτές συνθήκες δέσμευσης πόρων με βάση την έννοια του ρόλου. Επιπλέον το πλαίσιο αυτό μπορεί να διευρυνθεί αξιοποιώντας επιπλέον διαστάσεις όπως τον χρόνο, ή την τοποθεσία αιτήματος πρόσβασης σε μία υπηρεσία. Προς το παρόν απαιτούνται ορισμένες πολιτικές αναγνώρισης των κωδικών ασφαλείας ή άλλων στοιχείων στο προφίλ του χρήστη για τον προσδιορισμό του ρόλου του.

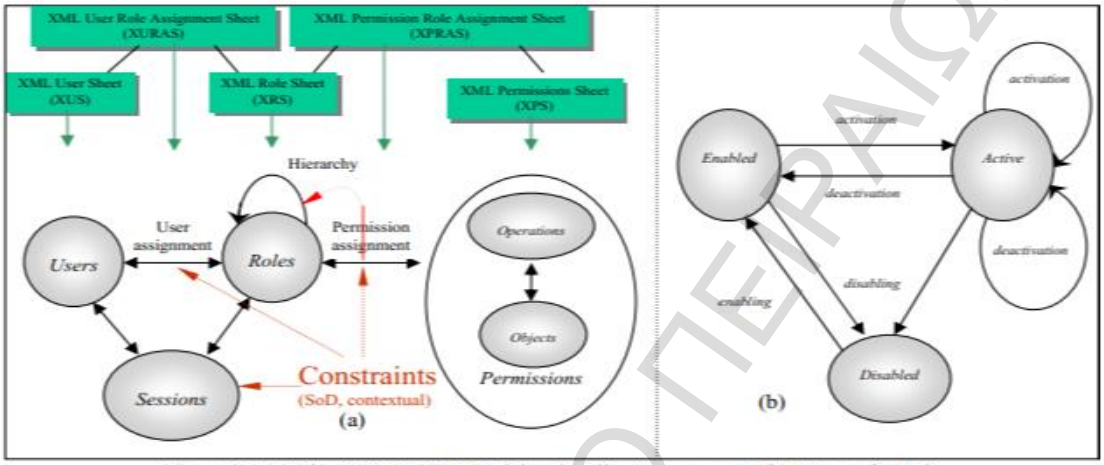


Figure 1.1 (a) The NIST RBAC Model and Policy Components (b) States of a Role

Εικόνα 2: Το μοντέλο RBAC (Takabi, H;Joshi, J.B.D.;Gail-Joon Ahn, 2010)

2.2.7 Διαχείριση ασφαλών υπηρεσιών

Πολλοί σύγχρονοι πάροχοι ΥΝ χρησιμοποιούν το πρότυπο WSDL για τη περιγραφή των μεταδεδομένων των υπηρεσιών που είναι διαθέσιμες για τους πελάτες τους. Ωστόσο η γλώσσα αυτή δεν μπορεί να καλύψει όλες τις απαιτήσεις περιγραφής υπηρεσιών ΥΝ. Για παράδειγμα, η ποιότητα των υπηρεσιών, η τιμή, και το επίπεδο παροχής υπηρεσιών έχουν σημαντικό ρόλο στην αναζήτηση και σύνθεση υπηρεσιών. Επομένως απαιτείται ένα νέο πλαίσιο διατύπωσης προδιαγραφών διαθεσιμότητας και σύνθεσης υπηρεσιών ΥΝ με γνώμονα την ασφάλεια και την προστασία της ιδιωτικότητας (Takabi, H;Joshi, J.B.D.;Gail-Joon Ahn, 2010).

Νέα πρότυπα στο web όπως η Security Assertion Markup Language[5] (SAML), και η Extensible Access Control Markup Language[6] (XACML) θα βοηθήσουν προς τη παραπάνω κατεύθυνση. Η SAML είναι ένα XML πρότυπο για την επικοινωνία πληροφοριών σχετικά με την ταυτότητα, δικαιώματα και χαρακτηριστικών ενός χρήστη, Μέσω της SAML μια επιχειρηματική οντότητα μπορεί να δημιουργεί ισχυρισμούς σχετικά με την ταυτότητα δικαιώματα και χαρακτηριστικά ενός αντικειμένου (συνήθως ανθρώπινου χρήστη) σε άλλες οντότητες όπως μια συνεργαζόμενη εταιρεία ή άλλη επιχειρηματική εφαρμογή. Στην XACML χρησιμοποιείτε και εκεί ένα XML πρότυπο δηλωτικής γλώσσας πολίτικης ελέγχου πρόσβασης και ένα μοντέλο επεξεργασίας που περιγράφει πώς να αξιολογούνται οι αιτήσεις πρόσβασης, σύμφωνα με τους κανόνες που ορίζονται στο πλαίσιο των πολιτικών. Παρόμοια προσπάθεια πραγματοποιείται

[5] http://xml.coverpages.org/saml.html

[6] http://tools.ietf.org/html/rfc7061

από όσους ασχολούνται με την πλατφόρμα Open Services Gateway Initiative[7] (OSGi),για παράδειγμα ένας νέος μηχανισμός εξουσιοδότησης της πρόσβασης σε μία web υπηρεσία εφαρμόζει την RBAC τεχνική που αναφέραμε παραπάνω. Μία άλλη προσπάθεια αφορά την υλοποίηση ενός συστήματος συνεργασιών βασισμένο σε προγράμματα-παράγοντες (agents) για την δυναμική σύνθεση υπηρεσιών.

2.2.8 Προστασία των δεδομένων

Με κάθε τρόπο οι πάροχοι πρέπει να διασφαλίσουν την προστασία των προσωπικών δεδομένων των χρηστών. Ο μηχανισμός προστασίας των δεδομένων πρέπει να ενσωματωθεί σε κάθε άλλο τρόπο προστασίας της ασφάλειας και να προσφέρει διαφάνεια ως προς το ποιος δημιούργησε ή τροποποίησε τα δεδομένα και για ποιο σκοπό, κ.α (Takabi, H;Joshi, J.B.D.;Gail-Joon Ahn, 2010). Η νέα προσέγγιση για την κάλυψη των παραπάνω αναγκών μπορεί να είναι η χρήση κρυπτογράφησης και κανόνων (πολιτικών) χρήσης των δεδομένων αυτών.

2.2.9 Διαχείριση ασφάλειας σε επίπεδο οργανισμού

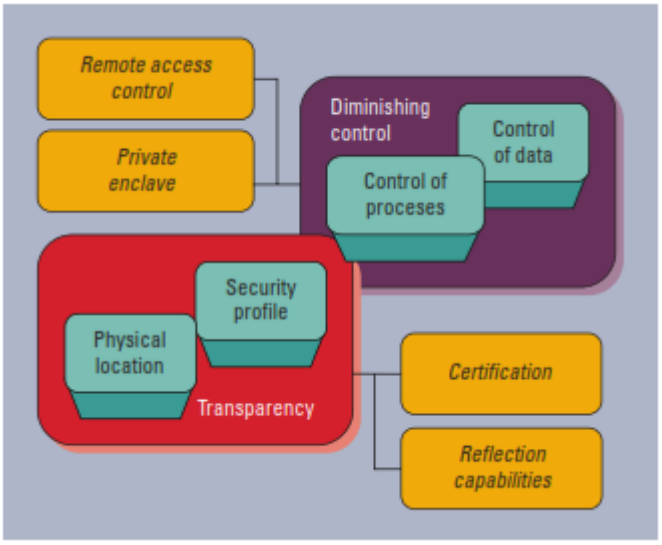
Από τη πλευρά του οργανισμού η εξάρτηση των υποδομών του από τρίτους (πχ ΥΝ) σημαίνει την έκθεση σε ορισμένους κινδύνους και επιπτώσεις σε περίπτωση συμβάντων σχετικά με την ασφάλεια. Επιπλέον γεννιούνται νέες απαιτήσεις οι οποίες πρέπει να συμπεριληφθούν σε όποια πλάνα επιχειρησιακής συνέχειας και ανάληψης από καταστροφή. Η ανάλυση κινδύνου ή ακόμα και κόστους-οφέλους όσον αφορά την εμπλοκή τρίτων (ΥΝ) σε σημαντικές λειτουργίες του οργανισμού είναι απαραίτητη σε τακτική βάση για την διασφάλιση ότι δεν έχει προκύψει διαρροή δεδομένων ειδικά σε πολύ-χρηστικά περιβάλλοντα, ο πάροχος παραμένει οικονομικά υγιής και δεν έχουν διαπιστωθεί κίνδυνοι (πχ ζημιές) μέσα και έξω από την υποδομή του. Ο οργανισμός πρέπει να ζητάει από τον πάροχο τα αποτελέσματα πρόσφατων ελέγχων για απειλές, δοκιμές διείσδυσης και όποια άλλες μετρικές εκτίμησης κινδύνου έχουν αξιοποιηθεί (Takabi, H;Joshi, J.B.D.;Gail-Joon Ahn, 2010).

2.3 ΜΟΝΤΕΛΑ ΕΜΠΙΣΤΟΣΥΝΗΣ ΣΤΟ ΥΝ

2.3.1 Μοντέλο Εμπιστοσύνης Α'

Οι *(Khan, K.M. ; Malluhi, Q., 2010)* τονίζουν την αδυναμία των πελατών να εμπιστευθούν τις σύγχρονες πλατφόρμες ΥΝ εξαιτίας της έλλειψης διαφάνειας, απώλεια ελέγχου και μη ξεκάθαρες διασφαλίσεις για την ασφάλεια. Στο παρακάτω διάγραμμα (Εικόνα 3) απεικονίζεται ένα μοντέλο εμπιστοσύνης που προτείνουν για την αντιμετώπιση των παραπάνω ζητημάτων.

[7] http://www.osgi.org/Main/HomePage



Εικόνα 3: Μοντέλο Εμπιστοσύνης (Khan, K.M. ; Malluhi, Q., 2010)

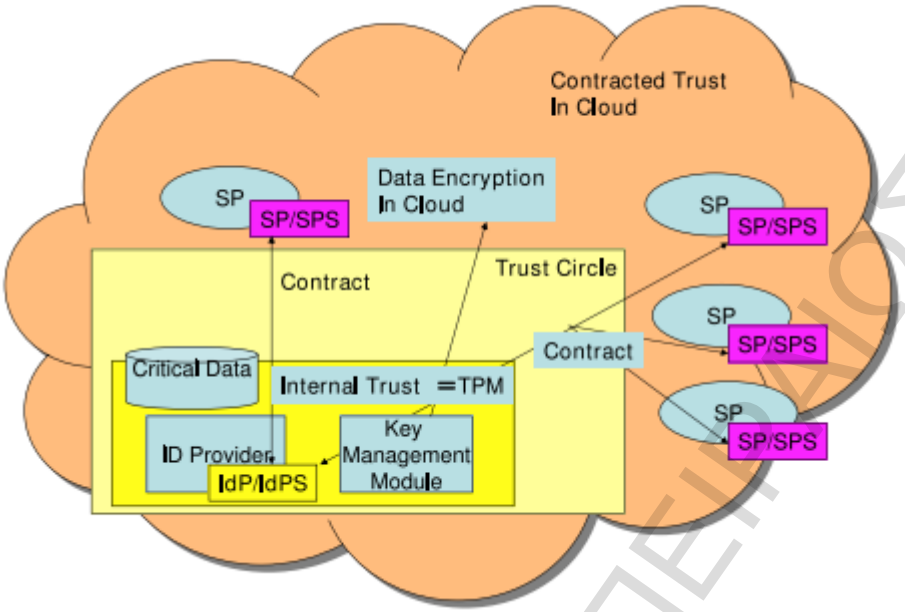
Σύμφωνα με την προτεινόμενη αρχιτεκτονική, ο πάροχος ενημερώνει τον πελάτη κάθε φορά που μία οντότητα έχει πρόσβαση στα αρχεία του. Το συγκεκριμένο κέντρο δεδομένων του παρόχου αλλά και οποιοδήποτε άλλο κέντρο δεδομένων του δεν θα αποθηκεύσουν αρχεία του πελάτη ή αντίγραφα τους για τα οποία δεν έχουν λάβει εξουσιοδότηση. Επίσης ο πάροχος θα πρέπει να καταστρέψει προσωρινά δεδομένα, ενδιάμεσα αποτελέσματα ή αρχεία που δεν είναι πλέον χρήσιμα σε όλα τα κέντρα δεδομένα που διαχειρίζεται.

Επιπλέον, η προτεινόμενη αρχιτεκτονική διασφαλίζει ότι έχει έλεγχο των διεργασιών και των εφαρμογών που επεξεργάζονται τα δεδομένα των πελατών (είναι αξιόπιστα και έμπιστα). Ο πελάτης πρέπει να γνωρίζει που βρίσκεται ο φυσικός χώρος αποθήκευσης των δεδομένων του και που συντελείται η επεξεργασία τους. Ο πάροχος γνωστοποιεί προς τον πελάτη όλα τα χαρακτηριστικά ασφάλειας που έχει ορίσει σε επίπεδο υπηρεσιών για τον ίδιο.

Το προτεινόμενο μοντέλο εμπιστοσύνης απαιτεί συγκεκριμένες τεχνολογίες. Η κρυπτογράφηση των δεδομένων και της ιδιωτικότητας παίζει σημαντικό ρόλο, όπως επίσης εφαρμογή ψηφιακών υπογραφών και μηχανισμών λογικής πρόσβασης για την εξασφάλιση της ακεραιότητας των δεδομένων. Σύγχρονες τεχνικές κρυπτογράφησης επιτρέπουν σε παρόχους ΥΝ την επεξεργασία δεδομένων χωρίς να απαιτείται αποκρυπτογράφηση τους ή την εν μέρει κρυπτογράφηση τους.

2.3.2 Μοντέλο Εμπιστοσύνης Β’

Σε άλλο μοντέλο εμπιστοσύνης που προτείνεται στη βιβλιογραφία (Sato, H. ; Univ. of Tokyo, Tokyo, Japan ; Kanai, A. ; Tanimoto, S., 2010), ορίζεται μία ιεραρχία επιπέδων εμπιστοσύνης. Σε αυτή διακρίνονται δύο κύρια επίπεδα: το επίπεδο εσωτερικής εμπιστοσύνης, και το επίπεδο συμβατικής εμπιστοσύνης (Εικόνα 4).



Εικόνα 4: Μοντέλο Εμπιστοσύνης B' (Sato, H. ; Univ. of Tokyo, Tokyo, Japan ; Kanai, A. ; Tanimoto, S., 2010)

Το επίπεδο εσωτερικής εμπιστοσύνης ορίζει μια πλατφόρμα στην οποία υπάρχει εγγύηση ότι η διοίκηση/λειτουργία σε αυτό το κύκλο εμπιστοσύνης είναι κάτω από το συνηθισμένο εσωτερικό έλεγχο ενός οργανισμού. Εμπιστοσύνη εξασφαλίζεται με την εφαρμογή συστημάτων TPM (Trust Platform Models) όπως αυτά που αναφέρονται στην §2.4.4. Αν κάτι πρέπει να ελέγχεται αυστηρά από ένα οργανισμό πρέπει να τοποθετείται σε αυτό το κύκλο. Προτείνεται επίσης αυτός ο κύκλος εμπιστοσύνης να παραμείνει στο εσωτερικό του οργανισμού (in-house). Για παράδειγμα η διαχείριση κωδικών πρόσβασης (Id Providers, Εικόνα 4), ή η επεξεργασία απόρρητων δεδομένων θα πρέπει να εκτελείται στον κύκλο εσωτερικής εμπιστοσύνης.

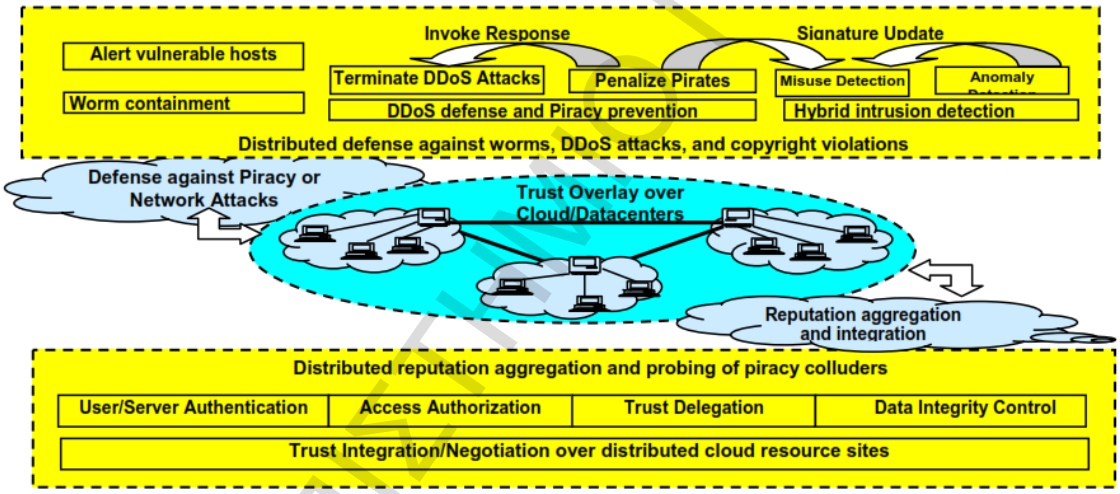
Το επίπεδο συμβατικής εμπιστοσύνης προσδιορίζει ότι η εμπιστοσύνη εξασφαλίζεται μέσω συμβολαίου. Ένα τέτοιο συμβόλαιο εμπιστοσύνης περιλαμβάνει τρεις τύπους εγγράφων:

1. Δήλωση Πολιτικής / Πρακτικής Υπηρεσιών: ορίζει το επίπεδο ποιότητας και ασφάλειας των παρεχόμενων υπηρεσιών που εγγυάται ο πάροχος
2. Δήλωση Πολιτικής / Πρακτικής Αναγνωριστικών Ταυτοποίησης: ορίζει το επίπεδο ποιότητας και ασφάλειας των παρόχων αναγνωριστικών συνεπώς και το βαθμό εμπιστοσύνης από τη πλευρά του παρόχου ΥΝ προς αυτούς τους παρόχους.
3. Σύμβαση: ουσιαστικά δηλώνει ότι ένας οργανισμός χρησιμοποιεί τις υπηρεσίες ενός παρόχου ΥΝ και επιβεβαιώνει ότι ο οργανισμός έχει γνώση των όσων αναφέρονται στη Δήλωση Πολιτικής /Πρακτικής Υπηρεσιών, και στη Δήλωση Πολιτικής/Πρακτικής Αναγνωριστικών Ταυτοποίησης.

Τα παραπάνω επίπεδα εμπιστοσύνης περιλαμβάνουν μετρήσιμες συνιστώσες σχετικά με την ασφάλεια. Επομένως μπορούν να γίνουν πιο αυστηρά ή πιο χαλαρά με βάση τις ανάγκες του οργανισμού και κυρίως με γνώμονα το κόστος.

2.3.3 Μοντέλο Εμπιστοσύνης Γ'

Το μοντέλο αυτό αναφέρεται στην προστασία δημοσίων αρχιτεκτονικών YN (public cloud architectures). Προτείνει τη δημιουργία μίας ιεραρχίας από δίκτυα επικάλυψης τα οποία συνδυάζονται μεταξύ τους με τη χρήση κατανεμημένων hash πινάκων (Kai Hwang ; Kulkareni, S. ; Hu, Yue , 2009) και διαμορφώνουν συστήματα ελέγχου του βαθμού αξιοπιστίας και της εμπιστοσύνης των συστημάτων. Όπως εξηγείται στο παρακάτω διάγραμμα (Εικόνα 5) το κάτω επίπεδο συγκεντρώνει στοιχεία για το επίπεδο αξιοπιστίας των διαθέσιμων κόμβων στο YN και επικοινωνεί στοιχεία για τυχόν χρήση παράνομων προγραμμάτων λογισμικού (πειρατεία). Σε πιο πάνω επίπεδο ενεργοποιούνται μηχανισμοί για την προστασία από ιούς, εντοπισμό προσπάθειας εισβολής σε συστήματα, αλλοίωσης περιεχομένου ή πνευματικών δικαιωμάτων προγραμμάτων λογισμικού.



Εικόνα 5: μοντέλο εμπιστοσύνης για τη προστασία δημόσιας υποδομής YN (Kai Hwang ; Kulkareni, S. ; Hu, Yue , 2009)

Επιπρόσθετα από άκρο-σε-άκρο συστήματα ελέγχου αξιοπιστίας συμβάλλουν στην προστασία ιεραρχίας πόρων του YN (πχ σε επίπεδο ιστότοπων, βάσεων δεδομένων, αρχείων). Δεδομένα που αφορούν πελάτες αντιγράφονται σε κατανεμημένα κέντρα δεδομένων και ειδικότερα σε δίκτυα αποθήκευσης δεδομένων. Έτσι οι χρήστες μπορούν να τα προσπελάζουν από οπουδήποτε καθώς η επιλογή του κέντρου δεδομένων που θα εξυπηρετήσει ένα αίτημα ακολουθεί χωροταξικά κριτήρια. Οι χρήστες έχουν στη διάθεση τους τα απαραίτητα κλειδιά για την πρόσβαση στις υπηρεσίες.

2.3.4 Μοντέλο Εμπιστοσύνης Δ'

Για μεγάλης κλίμακας αρχιτεκτονικές ΥΝ στις οποίες διαφορετικοί πάροχοι αλληλεπιδρούν με σκοπό την παροχή ενιαίων υπηρεσιών προς τους πελάτες προτείνεται το παρακάτω μοντέλο εμπιστοσύνης (Wenjuan Li, Lingdi Ping, 2009). Σε αυτό, οι πελάτες διατηρούν ένα πίνακα εμπιστοσύνης (customer trust table) σημειώνοντας το επίπεδο εμπιστοσύνης των υπηρεσιών που τους προσφέρει ο συγκεκριμένος πάροχος. Την πληροφορία αυτή την λαμβάνουν μέσω ενός μηχανισμού δημοπρασίας και ουσιαστικά υποδέχονται συστάσεις για τις υπηρεσίες ενός παρόχου από άλλους παρόχους που συνεργάζονται μαζί του (cross-cloud environment) και τις καταγράφουν στην εξέλιξη τους με βάση αυτό τον πίνακα (Πίνακας 1).

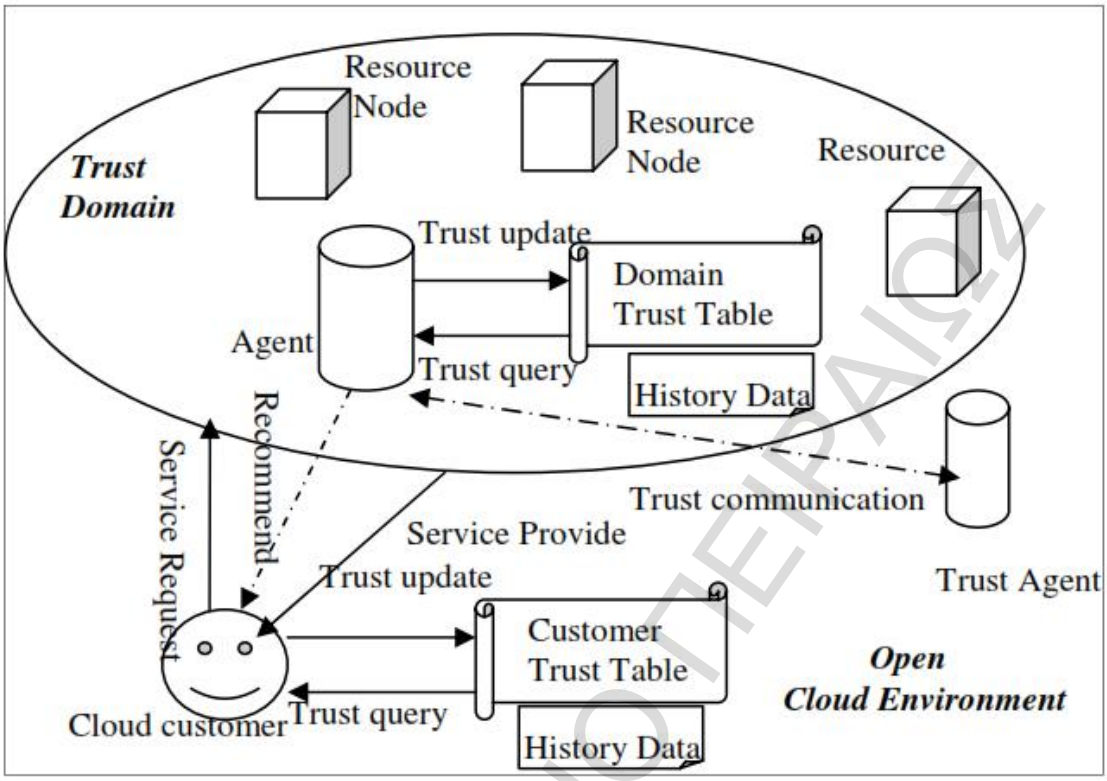
Domain name	Service type	Trust value/trust degree	Generation time

Domain name	Cooperation type	Trust value/trust degree	Generation time

Πίνακας 1: Πίνακας καταμέτρησης βαθμού εμπιστοσύνης παρόχου, και πίνακας καταμέτρησης βαθμού εμπιστοσύνης συνεργάτη αντίστοιχα (Wenjuan Li, Lingdi Ping, 2009)

Αντίστοιχα οι πάροχοι διατηρούν τον δικό τους πίνακα εμπιστοσύνης (domain trust table). Οι πάροχοι λειτουργούν κατανεμημένα ωστόσο ορίζουν από κοινού ένα πεδίο παροχής υπηρεσιών (domain) με χρήση κατανεμημένων πόρων. Ο πίνακας τους βοηθάει να μετρούν την αξιοπιστία των υποψήφιων συνεργατών πριν διαμορφώσουν μία συγκεκριμένη πρόταση προς τον πελάτη. Η αλληλεπίδραση μεταξύ συνεργατών για την διαμόρφωση του επιπέδου εμπιστοσύνης γίνεται μέσω παραγόντων (agents).

Η παρακάτω αρχιτεκτονική (Εικόνα 6) επιτρέπει σε πελάτες να λαμβάνουν αποφάσεις για το ποιον πάροχο να επιλέξουν για την εξυπηρέτηση τους με βάση τις πληροφορίες που διαθέτουν. Αντίστοιχα οι πάροχοι επιλέγουν τους συνεργάτες τους αξιολογώντας τον βαθμό εμπιστοσύνης ανά τύπο υπηρεσίας που έχει καταγραφεί στον σχετικό πίνακα. Σε κάθε περίπτωση ορίζεται ένα όριο κάτω από το οποίο η συνεργασία με ένα υφιστάμενο πάροχο ή συνεργάτη αντίστοιχα διακόπτεται ενώ συνεχίζεται (ή μπορεί να διαπραγματευτεί τη συνεργασία) με όποιον έχει το μέγιστο βαθμό εμπιστοσύνης. Η ενημέρωση του αντίστοιχου πίνακα γίνεται μετά από κάθε συναλλαγή.



Εικόνα 6: μοντέλο εμπιστοσύνης για μεγάλες, κατανεμημένες υποδομές YN (Wenjuan Li, Lingdi Ping, 2009)

2.4 ΟΡΙΣΜΟΣ ΕΠΙΘΕΣΕΩΝ ΣΤΟ ΥΠΟΛΟΓΙΣΤΙΚΟ ΝΕΦΟΣ

Στην βιβλιογραφία (Tharam Dillon, Chen Wu, Elizabeth Chang 2010) γίνεται λόγος για αυξημένες απειλές για την ασφάλεια πρέπει να ξεπεραστούν προκειμένου οι χρήστες να επωφεληθούν πλήρως από αυτό το νέο πεδίο της πληροφορικής. Μερικές από τις απειλές για την ασφάλεια αναφέρονται και αναλύονται κατωτέρω:

1. Στο μοντέλο λειτουργίας του YN ο έλεγχος της φυσικής ασφάλειας χάνεται λόγω της κοινής χρήσης των υπολογιστικών πόρων με άλλες εταιρείες. Δεν υπάρχει γνώση ή έλεγχος για το που τρέχουν οι πόροι.
2. Αν μία εταιρεία παραβιάσει το νόμο τότε υπάρχει ο κίνδυνος κατάσχεσης δεδομένων από μία κυβέρνηση (ξένων).
3. Οι υπηρεσίες αποθήκευσης που παρέχονται από ένα πάροχο YN μπορεί να είναι ασυμβίβαστη με τις υπηρεσίες ενός άλλου παρόχου αν ο χρήστης αποφασίσει να μετακινηθεί από το ένα στο άλλο (π.χ. το YN της Microsoft είναι ασυμβίβαστο με το YN της Google).
4. Ποιος ελέγχει τα κλειδιά κρυπτογράφησης / αποκρυπτογράφησης, αν όχι ο πελάτης;
5. Διασφάλιση της ακεραιότητας των δεδομένων (μεταφορά, αποθήκευση και ανάκτηση), σημαίνει πραγματικά ότι τα δεδομένα αλλάζουν μόνο ως αποτέλεσμα

εγκεκριμένων συναλλαγών. Ένα κοινό πρότυπο για τη διασφάλιση της ακεραιότητας των δεδομένων δεν υπάρχει ακόμη.

6. Σύμφωνα με το Πρότυπο Ασφάλειας Δεδομένων (PCI DSS) της βιομηχανίας καρτών πληρωμής καταγραφικά των δεδομένων πρέπει να παρέχονται στους διαχειριστές της ασφάλειας και των ρυθμιστικών αρχών.
7. Οι χρήστες πρέπει να φροντίζουν για έγκαιρες βελτιώσεις στις εφαρμογές τους για να βεβαιωθούν ότι προστατεύονται.
8. Ορισμένοι κυβερνητικοί κανονισμοί θέτουν αυστηρά όρια για το τι στοιχεία σχετικά με τους πολίτες της μπορούν να αποθηκεύονται και για πόσο καιρό, και ορισμένοι οργανισμοί ελέγχου τραπεζών απαιτούν τα οικονομικά στοιχεία των πελατών να παραμένουν στη χώρα τους.
9. Η δυναμική και ρευστή φύση των εικονικών μηχανών καθιστά αρκετά δύσκολο τον έλεγχο της συνοχής της ασφάλειας και να διασφαλίσουν την ικανότητα ελέγχου των αρχείων.
10. Οι πελάτες ενδέχεται να μηνύσουν παρόχους υπηρεσιών ΥΝ σε περίπτωση παραβίασης των δικαιωμάτων της ιδιωτικής τους ζωής, και σε κάθε περίπτωση μπορεί να προκληθεί ζημιά στη φήμη των παρόχων. Ανησυχίες προκύπτουν όταν δεν είναι σαφές σε ιδιώτες ο λόγος για τον οποίο τους ζητούνται τα προσωπικά στοιχεία ή πως θα χρησιμοποιηθούν ή μεταφερθούν σε τρίτους.

Επιπλέον οι (Tharam Dillon, Chen Wu, Elizabeth Chang 2010) θέτουν επιπλέον ζητήματα σχετικά με τη πρόσβαση, διατήρηση, συμμόρφωση, αποθήκευση, καταστροφή, καταγραφή και παρακολούθηση, παραβίαση απόρρητων δεδομένων.

- Πρόσβαση: Οι κάτοχοι των δεδομένων έχουν δικαίωμα να γνωρίζουν τις προσωπικές πληροφορίες που κατέχει ο πάροχος και, σε ορισμένες περιπτώσεις, μπορεί να υποβάλει αίτηση για να σταματήσει την επεξεργασία αυτή. Ένας χρήστης έχει το δικαίωμα να ζητήσει από τον οργανισμό για να διαγράψει τα δεδομένα του, αλλά πως θα είναι δυνατό να εξασφαλιστεί ότι όλα τα στοιχεία του έχουν πράγματι διαγραφεί από το ΥΝ;
- Συμμόρφωση: Ποιοι είναι οι ισχύοντες νόμοι, κανόνες, πρότυπα, και συμβατικές δεσμεύσεις που διέπουν τις εν λόγω πληροφορίες, και ποιός είναι υπεύθυνος για τη διατήρηση της συμμόρφωσης; Τα ΥΝ μπορούν να διασχίσουν πολλαπλές δικαιοδοσίες σε πολλές χώρες.
- Αποθήκευση: Πού είναι τα δεδομένα που αποθηκεύονται στο ΥΝ; Έχουν μεταφερθεί σε άλλο κέντρο δεδομένων σε άλλη χώρα; Αρχές προστασίας προσωπικών δεδομένω σε διάφορες χώρες θέτουν περιορισμούς στην δυνατότητα οργανισμών (πχ τράπεζες) να μεταφέρουν ορισμένες κατηγορίες προσωπικών δεδομένων σε άλλες χώρες.
- Διατήρηση: Πόσο καιρό τα προσωπικά δεδομένα (τα οποία έχουν αποθηκευτεί στο ΥΝ) διατηρούνται; Ποιος επιβάλλει την πολιτική διατήρησης στο ΥΝ, και πώς είναι διαχείρισιμες οι εξαιρέσεις σε αυτήν την πολιτική (πχ νομικές υποθέσεις);
- Καταστροφή: Πώς μπορούμε να ξέρουμε ότι ο πάροχος ΥΝ δεν διατηρεί πρόσθετα αντίγραφα; Μήπως ο πάροχος δεν έχει πραγματικά καταστρέψει τα δεδομένα, αλλά απλά τα έχει καταστήσει απρόσιτα για τον οργανισμό; Υπάρχει το ενδεχόμενο ο

πάροχος ΥΝ να διατηρεί τις πληροφορίες περισσότερο από ότι είναι αναγκαίο έτσι ώστε να μπορεί να εξορύξει δεδομένα για τις δικές του σκοπιμότητες;

- Καταγραφικός έλεγχος και εποπτεία: Πώς μπορούν οι οργανισμοί-πελάτες του παρόχου ΥΝ και να διασφαλίζουν τους πελάτες τους και τα ενδιαφερόμενα μέρη από τη πλευρά τους ότι οι απαιτήσεις προστασίας των προσωπικών δεδομένων πληρούνται όταν αποθηκεύονται στο ΥΝ;
- Παραβιάσεις των προσωπικών δεδομένων: Πώς μπορούμε να διασφαλίσουμε ότι ο πάροχος υπηρεσιών ΥΝ μας ειδοποιεί όταν διαπράχθηκε μια παράβαση, και ποιος είναι υπεύθυνος για την διαχείριση της διαδικασίας κοινοποίησης για την παραβίαση (και τη διαχείριση του κόστους που συνδέεται με τη διαδικασία); Αν οι συμβάσεις περιλαμβάνουν την ευθύνη για παραβάσεις που προκύπτουν από αμέλεια του παρόχου, πώς τίθεται σε εφαρμογή ο σχετικός όρος της σύμβασης και πώς καθορίζεται ποιος φταίει;

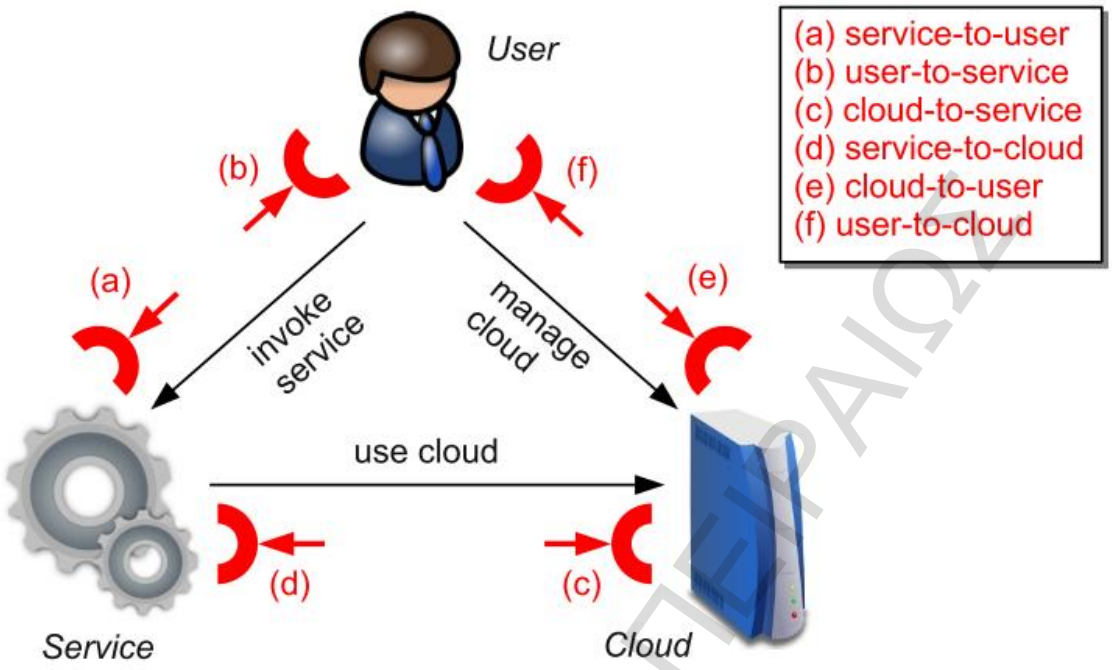
2.5 ΤΑΞΙΝΟΜΗΣΗ ΕΠΙΘΕΣΕΩΝ ΣΤΟ ΥΠΟΛΟΓΙΣΤΙΚΟ ΝΕΦΟΣ

Σύμφωνα με τους (Gruschka, N. ; NEC Eur. Ltd., Heidelberg, Germany ; Jensen, M 2010) συγκεκριμένες απειλές για την ασφάλεια και τρωτά σημεία των υπηρεσιών και υπηρεσιο-κεντρικών αρχιτεκτονικών απαιτούν νέες ταξινομήσεις και κριτήρια ταξινόμησης καθώς το ίδιο συμβαίνει και από την πλευρά των επιθέσεων στο υπολογιστικό νέφος. Στην έρευνα αυτή γίνεται προσπάθεια κατάταξης των ευάλωτων σημείων στο πεδίο του υπολογιστικού νέφους και από την άλλη πλευρά γίνεται προσπάθεια κατάταξης των επιθέσεων σε τάξεις, τις οποίες ονομάζουν επιφάνειες επίθεσης.

Σενάριο υπηρεσιών υπολογιστικού νέφους

Ένα σενάριο υπολογιστικού νέφους μπορεί να μοντελοποιηθεί χρησιμοποιώντας τρεις διαφορετικές κατηγορίες συμμετεχόντων (Εικόνα 7):

1. οι χρήστες των υπηρεσιών
2. οι υπηρεσίες που παρέχονται
3. ο πάροχος του ΥΝ.



Εικόνα 7: το τρίγωνο του ΥΝ – κατηγορίες επιθέσεων (Gruschka, N. ; NEC Eur. Ltd., Heidelberg, Germany ; Jensen, M 2010)

Καθένα από τους τρεις συμμετέχοντες ρόλους παρέχει ένα συγκεκριμένο είδος διεπαφής με κάθε άλλη κατηγορία συμμετέχοντα. Για παράδειγμα, το ΥΝ παρέχει υπηρεσίες με μια συγκεκριμένη διεπαφή (API[8] με βάση τον τύπο των υπηρεσιών, πχ IaaS[9], PaaS[10], SaaS[11]). Κατά τον ίδιο τρόπο, μια υπηρεσία παρέχεται σε έναν χρήστη με μια ειδική διεπαφή (π.χ. μέσω ιστοσελίδας, SSH[12] σύνδεσης, υπηρεσία ιστού, κ.ά). Όπως παρουσιάζεται στην Εικόνα 7 κάθε αλληλεπίδραση σε ένα σενάριο ΥΝ μπορεί να απευθύνεται σε δύο από τους τρείς συμμετέχοντες (π.χ. ένας χρήστης ζητά μια υπηρεσία, ή μία υπηρεσία ζητά περισσότερη επεξεργαστική ισχύ από την υποδομή του ΥΝ συστήματος). Έχοντας τρείς ρόλους στο σενάριο αυτό πρέπει να εξεταστούν έξι διαφορετικές διεπαφές.

Σε αυτό το πλαίσιο, κάθε απόπειρα επίθεσης μπορεί να αναλυθεί με βάση αυτό το σύνολο αλληλεπιδράσεων. Για παράδειγμα, μεταξύ ενός χρήστη και μίας υπηρεσίας επιδρούν οι ίδιοι παράγοντες επιθέσεων που υπάρχουν και έξω από ένα σενάριο ΥΝ (π.χ. παρέμβαση SQL κώδικα, επιθέσεις πλημμύρας, κά). Η διαφορά στο σενάριο ενός ΥΝ είναι ότι στις επιθέσεις σε ένα ΥΝ εμπλέκεται και ο πάροχος της υποδομής. Αυτό δεν σημαίνει απαραίτητα ότι ο πάροχος

[8] Application Programming Interface

[9] Infrastructure as a Service

[10] Platform as a Service

[11] Software as a Service

[12] Secure Shell

είναι κακόβουλος ο ίδιος, ωστόσο μπορεί να παίξει ένα ενδιάμεσο ρόλο σε μια συνεχή συνδυασμένη επίθεση.

2.5.1 Επιφάνειες επιθέσεων

Οι (Gruschka, N. ; NEC Eur. Ltd., Heidelberg, Germany ; Jensen, M 2010) διακρίνουν τις παρακάτω επιφάνειες επιθέσεων:

Επιφάνεια επιθέσεων 1: επίθεση μίας υπηρεσίας προς ένα χρήστη

Σε αυτή κατατάσσονται όλα τα είδη των επιθέσεων που είναι δυνατόν σε μία κοινή πελάτη-διακομιστή αρχιτεκτονική:

- επιθέσεις υπερχείλισης

Πολλές γλώσσες επιτρέπουν/ωθούν τον προγραμματιστή να εκχωρήσει μια περιοχή ενδιάμεσης αποθήκευσης σταθερού μεγέθους για την αποθήκευση συμβολοσειρών που εισάγει ο χρήστης, όπως π.χ. το όρισμα μιας εντολής. Μια συνθήκη υπερχείλισης συμβαίνει όταν η εφαρμογή δεν ενεργεί επαρκείς ελέγχους ορίων στις συμβολοσειρές και δέχεται μεγαλύτερες από το διαθέσιμο χώρο στην περιοχή αποθήκευσης. Ένας επιτιθέμενος μπορεί έτσι να προκαλέσει υπερχείλιση της περιοχής αποθήκευσης με τρόπο ώστε το πρόγραμμα να εκτελέσει μη αυθεντικές εντολές

- επίθεση με δηλητηρίαση SQL κώδικα

Μια ευπάθεια δηλητηρίασης SQL κώδικα εντοπίζεται όταν ένας επιτιθέμενος μπορεί να εισάγει μια σειρά δικών του εντολών σε ένα SQL ερώτημα, για παράδειγμα παραποιώντας τα δεδομένα που μια εφαρμογή ιστού θα ήθελε να εισάγει στη βάση δεδομένων. Αυτό γίνεται καθώς η ευπαθής εφαρμογή ιστού αλληλεπιδρά με τη βάση δεδομένων μέσω της εκτέλεσης δυναμικών SQL ερωτημάτων (διαμορφώνονται με βάση τα δεδομένα εισόδου του χρήστη). Οι επιτιθέμενοι μπορούν να τροποποιήσουν συντακτικά ή σημασιολογικά τα αρχικά SQL ερωτήματα, ενσωματώνοντας κακόβουλο SQL κώδικα στα πεδία εισόδου. Αυτό το είδος επίθεσης ονομάζεται *δηλητηρίαση SQL κώδικα (SQL code poisoning)* ή *SQL έγχυση (SQL injection)* και μπορεί να επηρεάσει τη λειτουργία της βάσης δεδομένων.

- κλιμάκωση προνομίων

Ο εισβολέας προσπαθεί να αποκτήσει περισσότερα προνόμια στη βάση δεδομένων.

Επιφάνεια επιθέσεων 2: επίθεση χρήστη προς μία υπηρεσία

Αφορά το κοινό περιβάλλον που ένα πρόγραμμα-πελάτης παρέχει σε ένα διακομιστή:

- επιθέσεις μέσω σελιδοδεικτών για τύπου HTML υπηρεσίες

Αφορά επιθέσεις μέσω δέσμης ενεργειών από άλλη τοποθεσία με σκοπό τη προσθήκη κώδικα δέσμης ενεργειών από μια τοποθεσία Web σε άλλη

- παραπλάνηση SSL[13] πιστοποιητικού

Αφορά προσπάθεια παραπλάνησης των χρηστών μίας ιστοσελίδας με σκοπό την ανάσχεση των δεδομένων που έχει στείλει ο χρήστης στο διακομιστή μέσω της χρήσης προβληματικού πιστοποιητικού ασφαλείας στη τοποθεσία Web.

- επιθέσεις στη κρυφή μνήμη των προγραμμάτων περιήγησης

Ο χρήστης μπορεί να δώσει τη συγκατάθεση του για την εγκατάσταση πρόσθετων προγραμμάτων στην εφαρμογή περιήγησης. Ένα τέτοιο κακόβουλο πρόγραμμα προσθέτει κρυφά αρχεία στη μνήμη της εφαρμογής περιήγησης με σκοπό την ανάσχεση δεδομένων του χρήστη.

- επιθέσεις (Phishing) πελατών ηλεκτρονικού ταχυδρομείου

Στη περίπτωση του ηλεκτρονικού ψαρέματος ο εισβολέας υποδύεται μία υπαρκτή οντότητα (πχ τη τράπεζα με την οποία πιθανότατα ο χρήστης συνδιαλλάσσεται) και επικοινωνεί με τον χρήστη μέσω ηλεκτρονικού ταχυδρομείου με σκοπό την εξαπάτηση του και την λήψη ευαίσθητων προσωπικών δεδομένων.

Επιφάνεια επιθέσεων 3: επίθεση μίας υπηρεσίας προς την υποδομή του ΥΝ

Περιλαμβάνει κάθε επίθεση από μία υπηρεσία που φιλοξενείται σε μία υποδομή προς το ίδιο το σύστημα του ΥΝ. Παραδείγματα τέτοιων περιπτώσεων μπορεί να είναι:

- επιθέσεις εξάντλησης πόρων με συνεχή αιτήματα προς τον πάροχο για περισσότερους πόρους μέχρι να επιτευχθεί άρνηση της υπηρεσίας (Denial-of-Service)

Στις περισσότερες επιθέσεις εξάντλησης πόρων στόχος είναι το επίπεδο των εφαρμογών (application layer). Τα πακέτα δεδομένων που μεταδίδονται από διαφορετικές εφαρμογές-ρομπότ των εισβολέων (bots) δεν εμποδίζονται από συσκευές όπως πύλες προστασίας (firewalls) και συστήματα ανίχνευσης εισβολών (IDS) καθώς η δομή και τα περιεχόμενά τους ακολουθούν τα απαραίτητα πρότυπα. Πραγματοποιώντας τέτοιες επιθέσεις από πολλές διαφορετικές πηγές, οι εισβολείς επιτυγχάνουν την εξάντληση κρίσιμων πόρων του συστήματος, όπως η χωρητικότητα ενός συνδέσμου, η δυνατότητα εξυπηρέτησης μίας συναλλαγής (session) ή μιας εφαρμογής (π.χ. HTTP και DNS), ή η υπερφόρτωση μιας βάσης δεδομένων.

- επιθέσεις στο υποσύστημα-επόπτη του ΥΝ

Χαρακτηριστικό παράδειγμα αυτού του τύπου επιθέσεων είναι η επίθεση παραίνεσης κακόβουλου λογισμικού (Injection Cloud Malware). Ένας εισβολέας ανεβάζει ένα αντίγραφο της υπηρεσίας του θύματος που ήδη λειτουργεί στο σύστημα. Το αντίγραφο είναι κατάλληλα χειραγωγημένο, έτσι ώστε κάποια αιτήματα προς την υπηρεσία αιτήσεις των θυμάτων να διεκπεραιώνονται μέσα σε αυτό το κακόβουλο αντίγραφο. Για να επιτευχθεί αυτό, ο εισβολέας πρέπει να αποκτήσει τον έλεγχό των δεδομένων του θύματος στο σύννεφο του συστήματος.

[13] Secure Socket Layer

Επιφάνεια επιθέσεων 4: επίθεση της υποδομής του ΥΝ προς μία υπηρεσία

Η περίπτωση αυτή είναι η πιο σημαντική καθώς εύκολα μπορεί να παρουσιαστεί ένα τέτοιο σενάριο. Ορισμένα παραδείγματα σε αυτή τη κατηγορία επιθέσεων είναι:

- περιορισμό της διαθεσιμότητας (πχ εκτέλεση εντολών τερματισμού της υπηρεσίας)

Ο εισβολέας (ο οποίος μπορεί να είναι εσωτερικός χρήστης ή κακόβουλο πρόγραμμα) έχει αποκτήσει πρόσβαση στη διεπαφή διαχείρισης των υπηρεσιών ή των εφαρμογών των χρηστών και παρεμβαίνει στις διαχειριστικές εντολές.

- παραβίαση της ιδιωτικότητας των δεδομένων που διαχειρίζεται η υπηρεσία

Εσωτερικοί χρήστης με διαχειριστικό ρόλο μπορεί να υποκλέψουν απόρρητα δεδομένων των χρηστών για σκοπούς marketing ή κενά ασφαλείας μπορεί να προκαλέσουν διαρροή των δεδομένων από τη βάση δεδομένων της υπηρεσίας.

Οι συνέπειες της κακόβουλης παρεμβολή προς υποκλοπή δεδομένων και της εκτέλεση παρένθετων λειτουργιών μίας υπηρεσίας είναι τεράστιες.

Επιφάνεια επιθέσεων 5: επίθεση της υποδομής του ΥΝ προς ένα χρήστη

Είναι δύσκολο ο τύπος αυτών των επιθέσεων να είναι διακριτός γιατί πάντοτε παρεμβαίνει μία υπηρεσία. Ωστόσο, αφορά κυρίως εκείνη τη διεπαφή που παρέχει το ΥΝ προς τους χρήστες για την διαχείριση των υπηρεσιών τους. Ο ελεγκτής νέφους είναι αυτή η διεπαφή που επιτρέπει τη προσθήκη νέων υπηρεσιών, αύξηση του ορίου δημιουργίας νέων αντιγράφων των υπηρεσιών, διαγραφή αντιγράφων, κά.

Επιφάνεια επιθέσεων 6: επίθεση ενός χρήστη προς την υποδομή του ΥΝ

- επιθέσεις τύπου phishing με κίνητρο να προκαλέσουν ένα χρήστη να χρησιμοποιήσει τις υπηρεσίες του παρόχου.
- Κάθε άλλη επίθεση που στοχεύει στον εξαπάτηση του χρήστη με σκοπό τη πρόσβαση στις υπηρεσίες του παρόχου

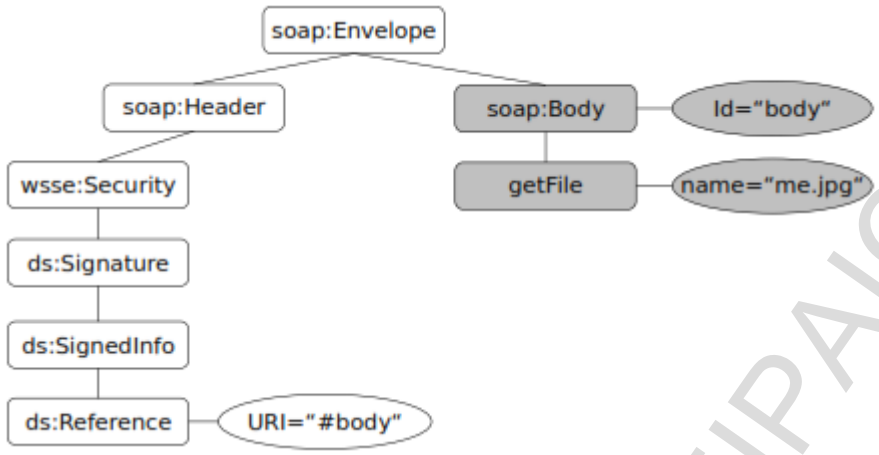
2.5.2 Επιθέσεις σε πρωτόκολλα

Στη βιβλιογραφία αναφέρεται ένα άλλο είδος επιθέσεων, αυτό σε πρωτόκολλα (Jensen, M. ; Horst Gortz Inst. for IT Security, Ruhr Univ., Bochum, Germany ; Schwenk, J. ; Gruschka, N. ; Iacono, L.L. 2009). Μία τέτοια περίπτωση αφορά επιθέσεις σε πρωτόκολλα τα οποία χρησιμοποιούν XML[14] υπογραφές για έλεγχο ταυτότητας ή προστασία της ακεραιότητας, και ονομάζονται επιθέσεις αναδίπλωσης (XML Signature Element Wrapping).

Το παρακάτω παράδειγμα (Εικόνα 8 και Εικόνα 9) περιγράφει μία επίθεση αναδίπλωσης σε ένα SOAP[15] μήνυμα.

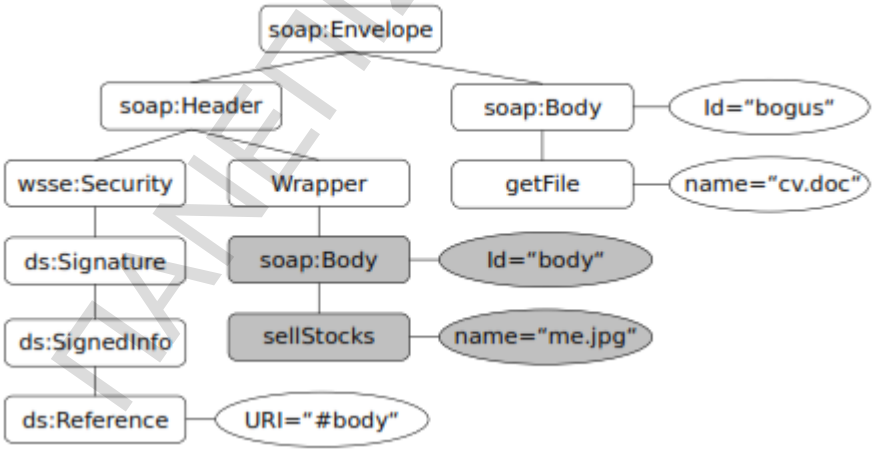
[14] eXtensible Markup Language

[15] Simple Object Access Protocol



Εικόνα 8: παράδειγμα SOAP μηνύματος έχοντας υπογεγραμμένο σώμα (Jensen, M. ; Horst Gortz; Schwenk, J. ; Gruschka, N. ; Iacono, L.L., 2009)

Η πρώτη εικόνα παρουσιάζει ένα μήνυμα SOAP που αποστέλλεται από ένα νόμιμο πελάτης. Το σώμα SOAP περιέχει ένα αίτημα για το αρχείο "me.jpg" και υπογράφεται από τον αποστολέα. Η υπογραφή περικλείεται στην επικεφαλίδα SOAP και παραπέμπει στο υπογεγραμμένο κομμάτι του μηνύματος χρησιμοποιώντας ένα δείκτη (Xpointer) προς την ιδιότητα Id και την τιμή «σώμα». Εάν ένας εισβολέας κρυφακούει ένα τέτοιο μήνυμα, μπορεί να εκτελέσει την ακόλουθη επίθεση. Το αρχικό σώμα μετακινείται σε ένα νέο στοιχείο μέσα στην επικεφαλίδα SOAP, και δημιουργείται ένα νέο σώμα. Αυτό το σώμα περιέχει τη λειτουργία που θέλει να εκτελέσει ο εισβολέας με την εξουσιοδότηση του αρχικού αποστολέα, στο συγκεκριμένο παράδειγμα, η αίτηση για το αρχείο "CV.doc". Το μήνυμα εξακολουθεί να περιέχει μια έγκυρη υπογραφή ενός νόμιμου χρήστη, επομένως η υπηρεσία παραλήπτης θα εκτελέσει το τροποποιημένο αίτημα.



Εικόνα 9: SOAP μήνυμα μετά από επίθεση (Jensen, M. ; Horst Gortz; Schwenk, J. ; Gruschka, N. ; Iacono, L.L., 2009)

Μία τέτοια επίθεση πραγματοποιήθηκε στην υποδομή ΥΝ της Amazon (EC2) το 2008. Χρησιμοποιώντας μία διαφοροποίηση του σεναρίου που παρουσιάστηκε παραπάνω ο εισβολέας μπορούσε να εκτελέσει οποιεσδήποτε EC2 εντολές εκ μέρους ενός νόμιμου χρήστη. Η ενεργοποίηση ενός πλήθους εικονικών μηχανών για την αποστολή κακόβουλων (spam) μηνυμάτων χρησιμοποιώντας τη ταυτότητα και το λογαριασμό (προς χρέωση) ενός νόμιμου χρήστη ήταν ένα από τα χαρακτηριστικά παραδείγματα αυτού του τρόπου επιθέσεων παρεμβαίνοντας στα SOAP μηνύματα της πλατφόρμας EC2.

Επιπρόσθετα, προγράμματα περιήγησης στο Web δεν μπορούν να κάνουν άμεσα χρήση της XML υπογραφής ή XML κρυπτογράφησης (Jensen, M. ; Horst Gortz; Schwenk, J. ; Gruschka, N. ; Iacono, L.L., 2009): τα δεδομένα μπορεί να είναι κρυπτογραφημένα μόνο μέσω του πρωτοκόλλου TLS[16], και οι υπογραφές χρησιμοποιούνται μόνο εντός της διαδικασίας «χειραψία TLS». Για όλα τα άλλα κρυπτογραφημένα σύνολα δεδομένων εντός του μηχανισμού ασφάλειας υπηρεσιών web (WS-Security), το πρόγραμμα περιήγησης λειτουργεί μόνο ως μια παθητική πηγή αποθήκευσης δεδομένων. Μερικές απλές λύσεις έχουν προταθεί π.χ. η χρήση TLS κρυπτογράφησης αντί για κρυπτογράφηση μέσω XML, αλλά και στη περίπτωση αυτή έχουν αναφερθεί στη βιβλιογραφία σοβαρά προβλήματα ασφάλειας με τη προσέγγιση αυτή.

Χρησιμοποιώντας προγράμματα περιήγησης στον ιστό (web browsers) για τη πρόσβαση σε web υπηρεσίες ενός ΥΝ κρύβουν μία σημαντική ευπάθεια, αυτή της πολιτικής «Ίδιας Προέλευσης» που εφαρμόζουν τα προγράμματα αυτά. Με βάση τη πολιτική SOP (Same Origin Policy) ο εξυπηρετητής ενός ΥΝ κάνει αποδεκτά μηνύματα-αιτήματα που προέρχονται από την ίδια εφαρμογή. Η προέλευση προσδιορίζεται από την πλειάδα «όνομα domain, πρωτόκολλο, θύρα». Η πολιτική αυτή δεν είναι ασφαλής γιατί η φύλαξη του ονόματος ενός domain στη κρυφή μνήμη δεν είναι ασφαλής καθώς οι κρυφές μνήμες μπορεί να μολυνθούν με ψεύτικα δεδομένα.

Για την αντιμετώπιση των ευπαθειών των προγραμμάτων περιήγησης απαιτείται συνδυασμός των πρωτοκόλλων TLS και SOP, για την ενίσχυση των μηχανισμών διαχείρισης ομόσπονδης ταυτότητας (Federated Identity Management). Ακόμη και με αυτές τις εναλλακτικές λύσεις, χρησιμοποιώντας TLS, το πρόγραμμα περιήγησης εξακολουθεί να διαθέτει πολύ περιορισμένες ικανότητες ως κέντρο ελέγχου ταυτότητας ενός ΥΝ (Jensen, M. ; Horst Gortz; Schwenk, J. ; Gruschka, N. ; Iacono, L.L., 2009).

Ορισμένες από τις λειτουργικές δυνατότητες των web services μπορούν να ενσωματωθούν, για παράδειγμα μέσω της δυναμικής φόρτωσης μίας κατάλληλης βιβλιοθήκης javascript, σε ένα πρόγραμμα περιήγησης (πχ για την αποστολή SOAP μηνυμάτων με ασφάλεια). Ωστόσο δεν μπορεί να γίνει κάτι αντίστοιχο για τους μηχανισμούς της XML υπογραφής και κρυπτογράφησης γιατί απαιτούν πολύ μεγαλύτερη προστασία. Οι δύο αυτές απαιτήσεις (XML υπογραφή και XML κρυπτογράφηση) πρέπει να ενισχύσουν τη προγραμματιστική βιβλιοθήκη (API[17]) μελλοντικών εκδόσεων των προγραμμάτων περιήγησης.

[16] Transport Layer Security

[17] Application Programming Interface

2.5.3 Επιθέσεις στην Ακεραιότητα και Δέσμευση Δεδομένων Υπηρεσιών ΥΝ

Μια σημαντική ευθύνη ενός συστήματος ΥΝ συνίσταται στη διατήρηση και το συντονισμό εικονικών μηχανών (IaaS) ή συγκεκριμένων υπηρεσιών-εφαρμογών που έχουν υλοποιηθεί προς εκτέλεση (PaaS). Κατόπιν αιτήματος του κάθε χρήστη, το ΥΝ σύστημα είναι υπεύθυνο για τον καθορισμό και εκτέλεση της πρώτης διαθέσιμης μηχανής ή υπηρεσίας. Κατόπιν τα στοιχεία της μηχανής ή της υπηρεσίας πρέπει να γνωστοποιούνται πίσω στον χρήστη που υπέβαλλε το αίτημα. Η παροχή αυτή από τη πλευρά του ΥΝ απαιτεί κάποια μεταδεδομένα σχετικά με την υπηρεσία ή την εφαρμογή, τουλάχιστον για σκοπούς ταυτοποίησης.

Οι περισσότερες από αυτές τις περιγραφές μεταδεδομένων απαιτούνται συνήθως από κάθε χρήστη πριν από την επίκληση υπηρεσιών προκειμένου να προσδιοριστεί η καταλληλότητα μιας υπηρεσίας για ένα συγκεκριμένο σκοπό. Επιπλέον, αυτές οι περιγραφές αποτελούν επίσης ορισμένα προκαταρκτικά αναγνωριστικά των υπηρεσιών, όπως για παράδειγμα στη περίπτωση web υπηρεσιών με πανομοιότυπη περιγραφή WSDL που παρέχουν την ίδια λειτουργία. Για το λόγο αυτό, αυτά τα μεταδεδομένα πρέπει να αποθηκεύονται εκτός του ΥΝ, και συγχρόνως δημιουργείται η ανάγκη να διατηρηθεί η σωστή σύνδεση των μεταδεδομένων και των υπηρεσιών που υλοποιούνται και γίνονται διαθέσιμα.

Επίθεση Ενσωμάτωσης Κακόβουλης Υπηρεσίας σε Εικονική Μηχανή (Cloud Malware Injection)

Σύμφωνα με τους (Jensen, M. ; Horst Gortz; Schwenk, J. ; Gruschka, N. ; Iacono, L.L., 2009), αυτού του είδους η απόπειρα επίθεσης στοχεύει στην ενσωμάτωση κακόβουλης εφαρμογής ή εικονικής μηχανής μέσα στο ΥΝ. Τέτοιου είδους κακόβουλο λογισμικό θα μπορούσε να εξυπηρετεί κάποιο συγκεκριμένο σκοπό, από υποκλοπές μέσω τροποποιήσεων δεδομένων μέχρι παραπλάνηση αλλαγών σε λειτουργίες ή προκαλώντας εμπλοκές σε αυτές. Αν η συγκεκριμένη επίθεση είναι επιτυχής, δηλαδή ο εισβολέας καταφέρει να φορτώσει στο σύστημα μία τέτοια υπηρεσία, τότε το σύστημα ανακατευθύνει αυτόματα τα όποια αιτήματα ενός έγκυρου χρήστη προς την κακόβουλη εφαρμογή της υπηρεσίας, και ο κώδικας της εκτελείται. Μια πολλά υποσχόμενη προσέγγιση ως αντίμετρο στην απειλή αυτή συνίσταται στο να εκτελεί το σύστημα ένα έλεγχο ακεραιότητας της κάθε δημιουργημένης υπηρεσίας πριν από τη χρήση της για τα εισερχόμενα αιτήματα.

Επίθεση πλαστογράφησης μεταδεδομένων

Η επίθεση αυτή στοχεύει στον στοχεύει στον κακόβουλο ανασχεδιασμό περιγραφών μεταδεδομένων διαφόρων web υπηρεσιών (Jensen, M. ; Horst Gortz; Schwenk, J. ; Gruschka, N. ; Iacono, L.L., 2009). Έχοντας αυτή τη δυνατότητα ένας εισβολέας θα μπορούσε να τροποποίηση τη σημασιολογία μίας κλήσης στο αρχείο WSDL και να εισάγει μία άλλη κλήση που τον ενδιαφέρει (πχ αλλαγή δικαιωμάτων πρόσβασης επιπέδου διαχειριστή). Αυτή η επίθεση μπορεί να είναι επιτυχής μόνο αν ο αντίπαλος καταφέρει να παρέμβει σε μία μόνο στιγμή όταν ο προγραμματιστής της υπηρεσία επικοινωνήσει το αρχείο WSDL της υπηρεσίας. Επιπλέον, μία τέτοια επίθεση ανακαλύπτεται σχετικά εύκολα, ιδιαίτερα υπό την παρουσία ορθών μεθόδων δοκιμών.

Η επαλήθευση της ακεραιότητας των μεταδεδομένων με τη μέθοδο του κατακερματισμού πριν την χρησιμοποίηση του σχετικού αρχείου περιγραφής είναι απαραίτητη. Για παράδειγμα η εφαρμογή ψηφιακής υπογραφής XML στο αρχείο WSDL θα βοηθήσει στην εξασφάλιση της ακεραιότητας. Αν επιπλέον το αρχείο των μεταδεδομένων (WSDL) αποθηκεύσει τη τιμή κατακερματισμού του κάθε αντίγραφου της υπηρεσίας που δημιουργείται αυτό θα διασφαλίσει ένα επιπλέον τρόπο σύνδεσης ανάμεσα στα δύο με κρυπτογραφημένο τρόπο.

Επίθεση πλημμύρας

Το ΥΝ υπόσχεται επιπλέον την εξασφάλιση συγκεκριμένης υπολογιστικής ισχύς διαθέτοντας περισσότερα του ενός εικονικά μηχανήματα σε σποραδικά υπολογιστικά κέντρα. Ωστόσο η περίπτωση αυτή θέτει σοβαρά προβλήματα στην παρουσία ενός εισβολέα. Η απειλή αυτή ονομάζεται επίθεση πλημμύρας, και συνίσταται στο ότι ένας επιτιθέμενος στέλνει ένα τεράστιο ποσό από ασήμαντες αιτήσεις προς μία συγκεκριμένη υπηρεσία. Δεδομένου ότι η εφαρμογή της υπηρεσίας πρέπει να επεξεργαστεί κάθε μία από τις αιτήσεις αυτές πριν καθορίσει αν το σχετικό αίτημα είναι έγκυρο ή όχι, αυτό έχει ήδη προκαλέσει φόρτο εργασίας ανά αίτημα της επίθεσης. Με αυτό τον τρόπο μία πλημμύρα αιτήσεων συνήθως θα προκαλέσουν άρνηση υπηρεσίας (Denial Of Server) στο υλικό του εξυπηρετητή (Jensen, M. ; Horst Gortz; Schwenk, J. ; Gruschka, N. ; Iacono, L.L., 2009).

Διακρίνονται οι εξής περιπτώσεις άρνησης υπηρεσίας:

- Άμεση Άρνηση Υπηρεσίας: Όταν το λειτουργικό σύστημα του ΥΝ παρατηρήσει το υψηλό φόρτο εργασίας στη πλημμυρισμένη υπηρεσία, θα αρχίσουν να παρέχει περισσότερη υπολογιστική ισχύ (πχ περισσότερες εικονικές μηχανές, περισσότερα αντίγραφα υπηρεσιών) για να αντιμετωπίσει το πρόσθετο φόρτο εργασίας. Έτσι, τα όρια του υλικού διακομιστή για μέγιστη φόρτο εργασίας δεν ισχύουν πλέον. Υπό αυτή την έννοια, το σύστημα προσπαθεί να εργαστεί έναντι του εισβολέα (παρέχοντας περισσότερη υπολογιστική ισχύ), αλλά στην πραγματικότητα-σε κάποιο βαθμό-στηρίζει τον εισβολέα επιτρέποντάς του να κάνει πιο μεγάλη ζημιά στη διαθεσιμότητα μιας υπηρεσίας, αρχής γενομένης από ένα ενιαίο σημείο εισόδου επίθεσης πλημμύρας.

- Έμμεση Άρνηση Υπηρεσίας: ανάλογα με την υπολογιστική ισχύ υπό έλεγχο του εισβολέα μία παράπλευρη συνέπεια της άμεσης επίθεσης πλημμύρας είναι ότι επιπρόσθετες υπηρεσίες στο ίδιο υλικό θα υποφέρουν εξαιτίας του μεγάλου φόρτου που προκλήθηκε από την επίθεση. Ανάλογα με το επίπεδο της πολυπλοκότητας του ΥΝ συστήματος, αυτή η παρενέργεια μπορεί να επιδεινωθεί εάν το σύστημα παρατηρήσει την έλλειψη διαθεσιμότητας, και προσπαθήσει να μεταφέρει τα πληγέντα αντίγραφα των υπηρεσιών σε άλλους εξυπηρετητές. Αυτό έχει ως αποτέλεσμα πρόσθετο φόρτο εργασίας για όσους άλλους εξυπηρετητές εμπλακούν, και ως εκ τούτου η επίθεση με πλημμύρες εξαπλώνεται σε όλο το ΥΝ.

Καθώς το μεγαλύτερο οικονομικό κίνητρο πίσω από τη λειτουργία μιας ΥΝ υπηρεσίας αποτελεί η χρέωση των πελατών σύμφωνα με τη πραγματική χρήση (π.χ. φόρτος εργασίας που προκαλείται), μια άλλη σημαντική επίπτωση από τις επιθέσεις πλημμυρών αποτελεί η δραστική αύξηση των λογαριασμών για τη χρήση του ΥΝ. Έτσι ο χρήστης που συνήθως εκτελεί την πλημμυρισμένη υπηρεσία πιθανότατα πρέπει να πληρώσει το τίμημα για το φόρτο εργασίας που προκαλείται από την εισβολή-τουλάχιστον αν ο επιτιθέμενος δεν μπορεί να προσδιοριστεί.

2.4.4. Επιθέσεις σε Εικονικές Μηχανές

Εικονικές μηχανές που χρησιμοποιούν το λειτουργικό σύστημα του Linux και το πρόγραμμα διαχείρισης εικονικών μηχανών Xen φανέρωσαν σημαντικές ευπάθειες σε επιθέσεις όπως (Rocha, F. ; Abreu, S. ; Correia, M., 2011):

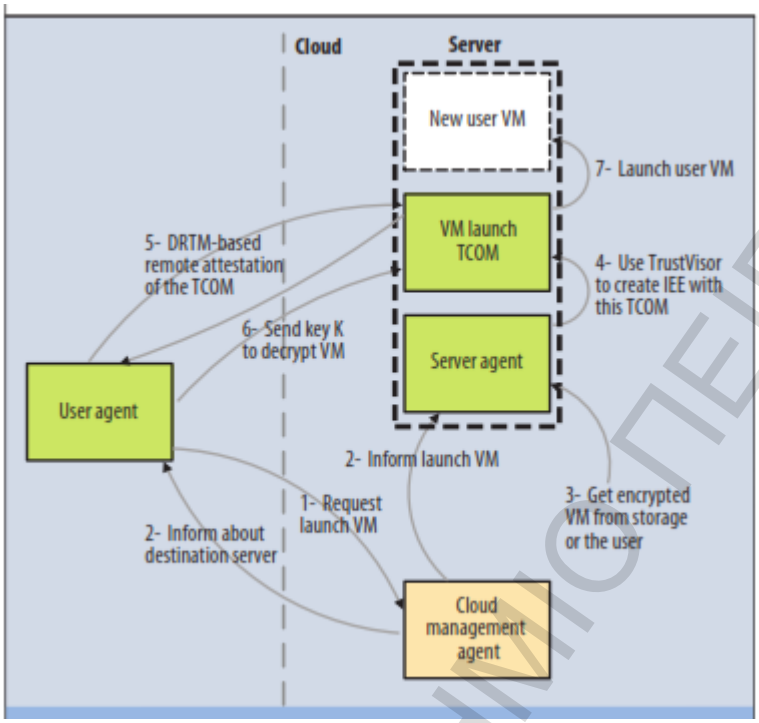
- Εξαγωγή των κωδικών πρόσβασης από τη μνήμη των εικονικών μηχανών: η επίθεση αυτή είναι εφικτή εφόσον το σύστημα αποθηκεύει τους κωδικούς πρόσβασης σε μορφή απλού κειμένου
- Εξαγωγή ιδιωτικών κλειδιών από τη μνήμη των εικονικών μηχανών: εφόσον το σύστημα χρησιμοποιεί αλγορίθμους κρυπτογράφησης που χρησιμοποιούν ασύμμετρα κλειδιά (πχ RSA) τότε υπάρχουν τεχνικές που μπορούν να υποκλέψουν τους αριθμούς των κλειδιών και παρόλο που αποθηκεύονται σε δυαδική μορφή είναι εύκολα αναγνωρίσιμοι καθώς αποθηκεύονται ακολουθώντας ένα ορισμένο πρότυπο (PKCS#1).
- Εξαγωγή αρχείων από το δίσκο: οι εισβολείς χρησιμοποιούν το πρόγραμμα του λειτουργικού συστήματος για τη διαχείριση λογικών τευχών (Logical Volume Manager) για να αποκτήσουν πρόσβαση σε αντίγραφα αρχείων.

Για την προστασία του απορρήτου των δεδομένων, το ΥΝ πρέπει να αποτρέψει ορισμένες επιθέσεις και να δώσει στους χρήστες τη δυνατότητα να αξιολογήσουν κατά πόσο οι απαραίτητοι μηχανισμοί έχουν τεθεί σε εφαρμογή, αντί να εμπιστευθούν απλώς τον πάροχο του ΥΒ. Αυτό μπορεί να είναι μία προφανής απαίτηση, αλλά το πιθανό πρόβλημα εδώ είναι ένας κακόβουλος εισβολέας που μεταδίδει αυθαίρετα ανακριβής πληροφορίες εκ μέρους του παρόχου, συνεπώς η εμπιστοσύνη προς τον πάροχο δεν είναι αρκετή. Οι εικονικές μηχανές ορίζονται και χρησιμοποιούνται σε τρία σημεία ενός ΥΝ: στους εξυπηρετητές, στο δίκτυο κατά τη φάση της υλοποίησης και μετανάστευσης σε άλλο φυσικό μηχάνημα, στην αποθήκευση τους ως αντίγραφο ασφαλείας σε ένα φυσικό δίσκο.

Οι εξυπηρετητές πρέπει να εκτελούν τις μηχανές σε ένα έμπιστο εικονικό περιβάλλον (Trusted Virtualization Environment- TVE) το οποίο αποτελείται από ένα υπερ-επόπτη και ένα εικονικό μηχάνημα διαχειριστή: τα παραπάνω δίνουν πρόσβαση σε ελεγχόμενες («έμπιστες») λειτουργίες των εικονικών μηχανών προς τους διαχειριστές (εκτέλεση, μετανάστευση σε άλλο φυσικό μηχάνημα, δημιουργία αντιγράφου ασφαλείας) και όχι στις συνήθεις λειτουργίες εξαιτίας των ευπαθειών που αναφέρθηκαν παραπάνω. Η Εικόνα 10 εξηγεί την ευρύτερη διαδικασία χρήσης μίας εικονικής μηχανής στο προτεινόμενο προστατευμένο περιβάλλον για τη διαχείριση εικονικών μηχανών. Η διαδικασία αυτή περιλαμβάνει μία υποδομή δημόσιου κλειδιού (PKI[18])

[18] Public Key Infrastructure

για την παροχή πιστοποιητικών προς χρήση σε κάθε λειτουργία διαχείρισης εικονικών μηχανών. Ο φορέας πιστοποίησης ή κάποιος άλλος φορέας που εμπιστεύεται ο χρήστης είναι μέρος αυτής της διαδικασίας για την προστατευμένη διαχείριση και κατανομή των στοιχείων παραμετροποίησης του εκάστοτε TVE μηχανισμού.



Εικόνα 10: διαδικασία κλήσης μίας εικονικής μηχανής προς εκτέλεση σε ένα έμπιστο περιβάλλον διαχείρισης εικονικών μηχανών (Rocha, F. ; Abreu, S. ; Correia, M., 2011)

Στο παραπάνω παράδειγμα (Εικόνα 10) απεικονίζεται η διαδικασία εκτέλεσης ενός εικονικού μηχανήματος. Ο παράγοντας χρήστη στέλνει το σχετικό αίτημα στον παράγοντα-διαχειριστή ΥΝ και ο τελευταίος αποφασίζει σε ποιο φυσικό μηχάνημα θα γίνει η μετάπτωση του εικονικού μηχανήματος και ενημερώνεται τόσο ο παράγοντας χρήστη όσο και ο παράγοντας του αντίστοιχου διακομιστή. Ο παράγοντας-διακομιστή φορτώνει το εικονικό μηχάνημα είτε από τον αποθηκευτικό χώρο του ΥΝ ή απευθείας από τον παράγοντα χρήστη.

Ο παράγοντας-διακομιστή χρησιμοποιεί τον TrustVistor για να δημιουργήσει ένα περιβάλλον απομονωμένης εκτέλεσης στο οποίο θα ξεκινήσει η εκτέλεση του εικονικού μηχανήματος. Ο TrustVisor, είναι ένας υπέρ-επόπτης ειδικού σκοπού που παρέχει την ακεραιότητα κώδικα, καθώς και την ακεραιότητα και το απόρρητο των δεδομένων για επιλεγμένα τμήματα μίας εφαρμογής ή μίας εικονικής μηχανής. Ο TrustVisor επιτυγχάνει ένα υψηλό επίπεδο ασφάλειας, πρώτον γιατί μπορεί να προστατεύσει ευαίσθητο κώδικα σε σημαντική λεπτομέρεια, και, δεύτερον, διότι χρησιμοποιεί μια πολύ μικρή βάση κώδικα (μόνο περίπου 6K γραμμές κώδικα) που καθιστά εφικτή την επαλήθευση. Ο TrustVisor μπορεί επίσης να πιστοποιήσει την ύπαρξη χώρων απομονωμένων εκτέλεσης σε έναν εξωτερικό φορέα.

Κατόπιν ο παράγοντας-χρήστη πιστοποιηθεί την αξιοπιστία της μηχανής εφαρμόζοντας την τεχνική πιστοποίησης DRTM (dynamic root of trust measurement). Η τεχνική αυτή αξιοποιεί την πλατφόρμα υλικού και λογισμικού TPM (Trust Platform Module) που είναι εγκατεστημένη σε ειδικό τσιπ στον υπολογιστή του χρήστη για να λάβει μετρήσεις αξιοπιστίας της μηχανής,

3. ΑΞΙΟΛΟΓΗΣΗ ΚΑΙ ΣΥΓΚΡΙΣΗ ΠΛΑΤΦΟΡΜΩΝ ΥΠΟΛΟΓΙΣΤΙΚΟΥ ΝΕΦΟΥΣ

3.1 ΚΡΙΤΗΡΙΑ ΑΞΙΟΛΟΓΗΣΗΣ ΤΩΝ ΥΠΗΡΕΣΙΩΝ CLOUD

Στη βιβλιογραφία, σημαντικά κριτήρια αξιολόγησης των προσφερόμενων υπηρεσιών ΥΝ από διαφορετικούς παρόχους θεωρούνται τα παρακάτω (Hogberg, 2012):

- επίπεδο υποστήριξης πελάτη
- επίπεδο ασφάλειας (πχ εμπιστευτικότητα, και ταυτοποίηση)
- επίπεδο παροχής υπηρεσιών (πχ ποσοστό διαθεσιμότητας που προσφέρει ένας οργανισμός)
- κόστος και ικανότητα κλιμάκωσης υπηρεσιών
- πολυπλοκότητα μεταφοράς σε άλλη υποδομή

Τα περισσότερα από τα παραπάνω κριτήρια είναι δύσκολο να ποσοτικοποιηθούν και να μετρηθούν σύμφωνα με κάποια κλίμακα. Ως εκ τούτου οι πλατφόρμες θα συγκριθούν μεταξύ τους μέσα από μία SWOT[19] αξιολόγηση.

Το κόστος της λειτουργίας μίας εφαρμογής σε μία πλατφόρμα είναι δύσκολο να προβλεφθεί καθώς οι περισσότεροι προμηθευτές εφαρμόζουν πολύπλοκα μοντέλα τιμολόγησης λαμβάνοντας υπόψη τον αριθμό των κύκλων ρολογιού του επεξεργαστή που θα καταναλωθούν, ή τον αριθμό των εισερχόμενων και εξερχόμενων συναλλαγών. Σε μία σύμβαση ορίζεται το επίπεδο παροχής υπηρεσιών που υπόσχεται ένας προμηθευτής ΥΝ, για παράδειγμα ποιό ποσοστό αδιάλειπτης λειτουργίας εγγυάται η επιχείρηση και ποιο θα είναι το πρόστιμο αν αυτό δεν τηρηθεί για κάποιο χρονικό διάστημα. Το επίπεδο παροχής υπηρεσιών βοηθάει στην αξιολόγηση της ποιότητας μίας υπηρεσίας, ωστόσο αν το σύστημα καθίσταται μία διαθέσιμο οι συνέπειες για τον πελάτη είναι πιθανότητα πιο σοβαρές από την αποζημίωση. Επίσης οι πληροφορίες που διαθέτουν οι προμηθευτές για τα μέτρα ασφαλείας που λαμβάνουν, οι τεχνικές και ο βαθμός διαφάνειας τους είναι μία σημαντική πτυχή για την αξιολόγηση τους.

Επιπλέον κριτήριο είναι η προσφερόμενη υποστήριξη από τους προμηθευτές, η διαθεσιμότητα και η μεγάλη ανταπόκριση δεδομένου ότι οι συνέπειες μίας πτώσης της υπηρεσίας για ορισμένο χρονικό διάστημα μπορεί να είναι δαπανηρές. Η ποιότητα και η έκταση της τεκμηρίωσης από πλευράς προμηθευτή είναι σοβαρό κριτήριο καθώς η καλή τεκμηρίωση βοηθά να μειωθεί το κόστος της μετάβασης σε μία άλλη πλατφόρμα.

Στο ζήτημα της ασφάλειας, όπως αναφέρθηκε και στο κεφάλαιο 2 κίνδυνοι για μία ΥΝ υποδομή θεωρούνται οι παρακάτω:

- απώλεια της διακυβέρνησης από τη πλευρά του χρήστη
- σημαντική εξάρτηση από τις υπηρεσίες του ΥΝ

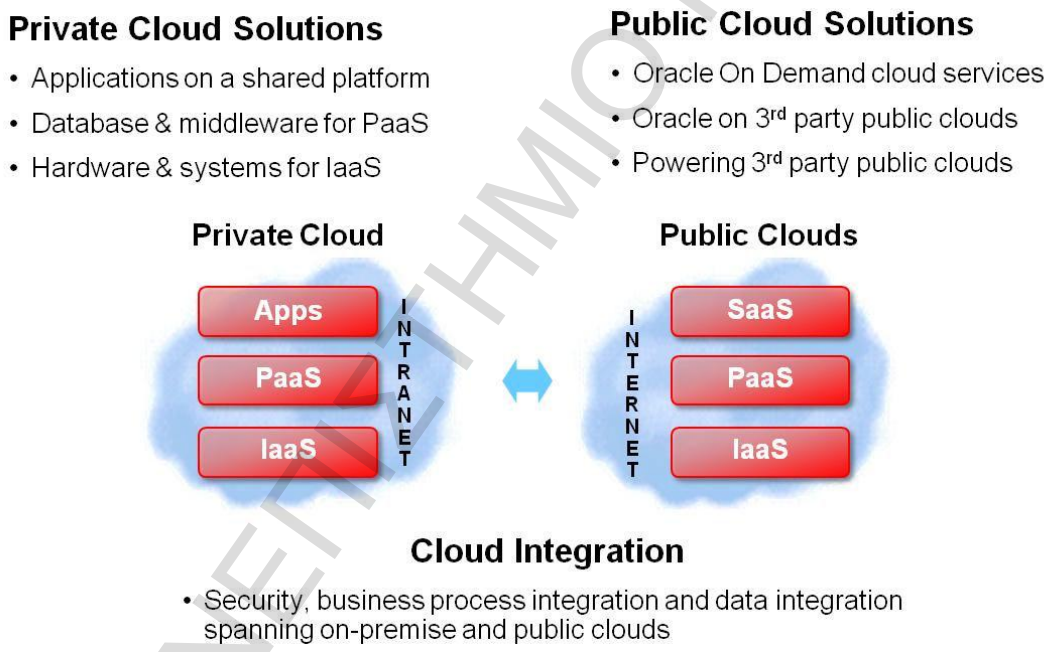
[19] Strengths, Weaknesses, Opportunities, Threats

- αποτυχία απομόνωσης των δεδομένων του χρήστη
- κίνδυνοι σχετικά με το κανονιστικό πλαίσιο συμμόρφωσης
- συμβιβαστική χρήση της διεπαφή διαχείρισης
- προστασία δεδομένων
- ανασφαλής ή ελλιπής διαγραφή δεδομένων
- εισβολή κακόβουλου χρήστη

3.2 ORACLE CLOUD - PRIVATE CLOUD

3.2.1 Πλεονεκτήματα της στρατηγικής της Oracle για το cloud computing (strengths)

Η στρατηγική της Oracle για το ΥΝ (Oracle, 2011) είναι ευρεία και ολοκληρωμένη για να παρέχει στους πελάτες την επιλογή και έναν ρεαλιστικό οδικό χάρτη για την υιοθέτηση του ΥΝ. Η Oracle παρέχει λογισμικό για επιχειρήσεις και προϊόντα υλικού τόσο για ιδιωτικά όσο και για δημόσια clouds, όπως απεικονίζεται στην Εικόνα 11.



Εικόνα 11: Λύσεις Oracle για ιδιωτικά και δημόσια ΥΝ (Oracle, 2011)

Οι λύσεις για ιδιωτικά ΥΝ περιλαμβάνουν:

- Ένα εκτεταμένο χαρτοφυλάκιο από οριζόντιες και ειδικές για την βιομηχανία εφαρμογές της Oracle, οι οποίες τρέχουν σε πλατφόρμες ΥΝ που βασίζονται σε πρότυπα, είναι κοινόχρηστες και ελαστικά επεκτάσιμες.
- Το Oracle middleware και την βάση δεδομένων για ιδιωτικές PaaS αρχιτεκτονικές που επιτρέπουν στους πελάτες να εδραιώσουν τις υπάρχουσες εφαρμογές και να δημιουργήσουν αποτελεσματικότερα καινούργιες εφαρμογές.

- Τον διακομιστή της Oracle, αποθηκευτικό και δικτυακό υλικό σε συνδυασμό με λογισμικό για virtualization και λειτουργικά συστήματα για ιδιωτικές IaaS αρχιτεκτονικές οι οποίες επιτρέπουν στους πελάτες να ενοποιήσουν τις εφαρμογές τους σε ένα κοινόχρηστο υλικό.

Οι λύσεις για δημόσια ΥΝ περιλαμβάνουν:

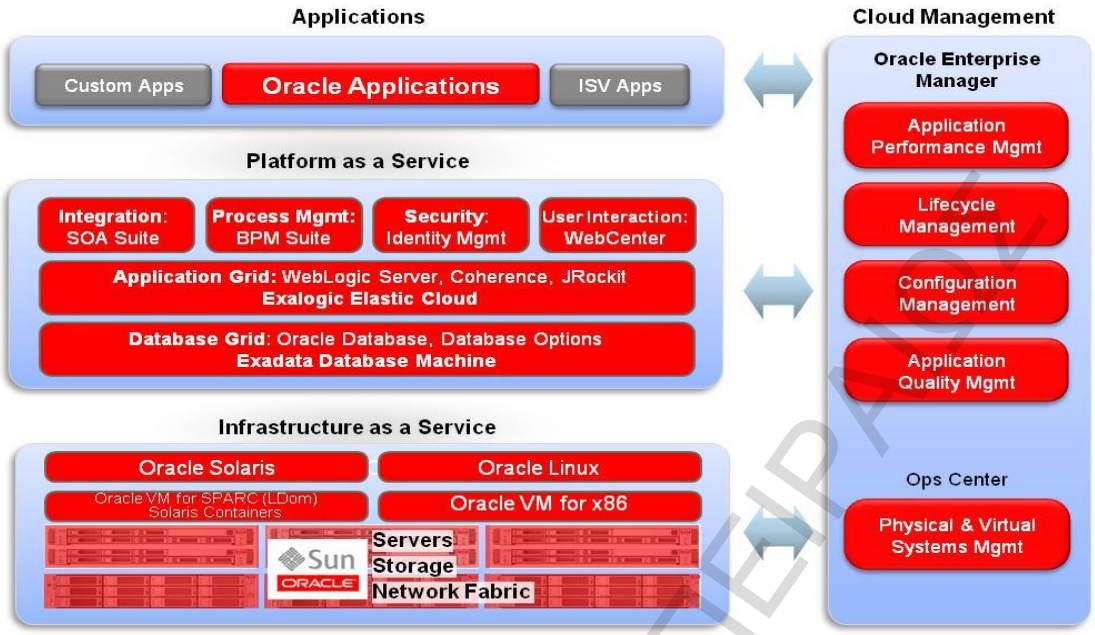
- Το Oracle On Demand το οποίο είναι ένας πάροχος υπηρεσιών ΥΝ για τις εφαρμογές, το middleware και την βάση δεδομένων της Oracle.
- Τα προϊόντα της Oracle τα οποία οι πελάτες μπορούν να αναπτύξουν σε άλλα δημόσια ΥΝ, συμπεριλαμβανομένων των εφαρμογών, του middleware της βάσης δεδομένων, των λειτουργικών συστημάτων και του virtualization της Oracle.
- Το middleware και την βάση δεδομένων της Oracle που τροφοδοτούν άλλα ΥΝ, συμπεριλαμβανομένων και των παρόχων SaaS και PaaS.

Διασύνδεση μεταξύ των ΥΝ:

- Η Oracle επιτρέπει την διασύνδεση (integration) σε δημόσια και ιδιωτικά ΥΝ με ένα σύνολο προϊόντων για την διαχείριση της ταυτότητας και της πρόσβασης, για τις υπηρεσιοστρεφείς αρχιτεκτονικές (SOA[20]) και την διασύνδεση διεργασιών, και τέλος για την διασύνδεση των δεδομένων.

Σε αντίθεση με τους άλλους παρόχους προϊόντων και υπηρεσιών με στενούς ορίζοντες για το ΥΝ, η προσέγγιση της Oracle είναι πλήρης και ολοκληρωμένη. Η Oracle παρέχει στους πελάτες λύσεις για ιδιωτικά και δημόσια ΥΝ, για όλα τα επίπεδα στης στοίβας του ΥΝ (SaaS, PaaS, IaaS), καθώς και αντίστοιχες λύσεις για την ανάπτυξη εφαρμογών στο ΥΝ, την διαχείριση του ΥΝ, την ασφάλεια του ΥΝ και την διασύνδεσή του.

[20] Service Oriented Architecture



Εικόνα 12, Επισκόπηση λύσεων της Oracle για το cloud (Oracle, 2011)

Oracle PaaS (Platform-as-a-Service)

Το Oracle PaaS (Oracle, 2011) είναι μια κοινόχρηστη και ελαστικά επεκτάσιμη πλατφόρμα για εφαρμογές που προσφέρεται σαν μια ιδιωτική ή δημόσια υπηρεσία ΥΝ. Το Oracle PaaS βασίζεται στα τεχνολογικά πρωτοπόρα προϊόντα βάσεων δεδομένων και middleware της Oracle και μπορεί να εξυπηρετήσει όλο το φόρτο εργασίας που κυμαίνεται από εφαρμογές μεγάλης σημασίας μέχρι και σε εφαρμογές επιπέδου τμήματος, είτε είναι εφαρμογές της Oracle είτε είναι εφαρμογές από άλλους προμηθευτές ή εσωτερικά αναπτυγμένες εφαρμογές.

Το Oracle PaaS επιτρέπει στις επιχειρήσεις να ενσωματώσουν τις υπάρχουσες εφαρμογές τους σε μία κοινόχρηστη (shared), κοινή αρχιτεκτονική, καθώς επίσης και να αναπτύξουν καινούργιες εφαρμογές που αξιοποιούν τις κοινόχρηστες (shared) υπηρεσίες που παρέχονται από την πλατφόρμα. Η πλατφόρμα Oracle PaaS προσφέρει εξοικονόμηση κόστους μέσω της τυποποίησης και της υψηλότερης αξιοποίησης της κοινόχρηστης πλατφόρμας σε πολλαπλές εφαρμογές. Επίσης, το Oracle PaaS παρέχει μεγαλύτερη ευελιξία μέσω της ταχύτερης ανάπτυξης εφαρμογών αξιοποιώντας κοινόχρηστες υπηρεσίες που βασίζονται σε πρότυπα και επεκτείνονται ελαστικά ανάλογα με την ζήτηση.

Το Oracle PaaS περιλαμβάνει βάση δεδομένων σαν υπηρεσία (Database-as-a-Service) βασισμένη στην βάση δεδομένων της Oracle και στην μηχανή βάσεων δεδομένων Oracle Exadata, καθώς επίσης και middleware σαν υπηρεσία (Middleware-as-a-Service) βασισμένο στον Oracle Weblogic και στο Oracle Exalogic 10 Elastic Cloud. Συστήματα όπως το Exadata και το Exalogic είναι προ-ενσωματωμένα και βελτιστοποιημένοι συνδυασμοί υλικού και λογισμικού για να προσφέρουν εξαιρετική απόδοση, αποτελεσματικότητα, ασφάλεια και διαχειρισιμότητα σε χαμηλότερο χρόνο επεξεργασίας. Το Oracle Exadata είναι μια μηχανή βελτιστοποιημένη για εκτέλεση εφαρμογών σε Java στο επίπεδο του middleware / εφαρμογών.

Και τα δύο συστήματα προσφέρουν κορυφαία απόδοση που τα καθιστά αποτελεσματικά για την ενοποίηση της βάσης δεδομένων και του μεσαίου επίπεδου για εκατοντάδες εφαρμογών. Και οι δύο μηχανές είναι ελαστικά επεκτάσιμες τόσο κάθετα όσο και οριζόντια, και πλήρως ανεκτικές στα λάθη. Προσφέρουν απλοποιημένη ανάπτυξη εφαρμογών, δεδομένου ότι είναι προ-ενσωματωμένες και προ-ρυθμισμένες από την Oracle και όχι από τον πελάτη στο κέντρο δεδομένων του. Επίσης, προσφέρουν χαμηλότερο χρόνο επεξεργασίας επειδή μπορούν να ελαττώσουν το συνολικό υλικό και την πολυπλοκότητα του περιβάλλοντος του πελάτη.

Oracle IaaS (Infrastructure-as-a-Service)

Η Oracle (Oracle, 2011) προσφέρει μια πλήρη γκάμα υπολογιστικών διακομιστών, αποθήκευσης, δικτύωσης, λογισμικό virtualization, λειτουργικά συστήματα, και το λογισμικό διαχείρισης που απαιτείται για το πρότυπο IaaS. Παρέχει όλο το υλικό της υποδομής και τα τμήματα λογισμικού που απαιτούνται για την υποστήριξη των διαφορετικών απαιτήσεων των εφαρμογών.

Η ευέλικτη και ισχυρή υποδομή cloud της Oracle υποστηρίζει συγκέντρωση των πόρων, ελαστική επεκτασιμότητα, ταχεία ανάπτυξη εφαρμογών και υψηλή διαθεσιμότητα. Η μοναδική ικανότητα να παραδίδει εφαρμογές υποστηρίζουν εγγενώς τις αρχές του virtualization και της διαχείρισης με ενσωματωμένες τεχνολογίες υπολογισμού, αποθήκευσης και δικτύωσης, επιτρέπει την ταχεία ανάπτυξη και την αποτελεσματική διαχείριση δημόσιων και ιδιωτικών IaaS.

3.2.2 Αδυναμίες των λύσεων της Oracle

Η Oracle δεν τοποθετήθηκε από νωρίς στην αγορά του ΥΝ, και η ανάπτυξη του συγκεκριμένου τομέα πραγματοποιείται με χαμηλούς ρυθμούς (0-8%) ενώ συνεχώς μειώνονται τα έσοδα της εταιρίας στην αγορά εξοπλισμού και υλικών. Το PaaS το οποίο ουσιαστικά αποτελεί εξέλιξη του SaaS (Λογισμικό-ως-Υπηρεσία) δεν έχει πείσει ευρύτερα μεγάλους οργανισμούς.

Κατά το παρελθόν εντοπίστηκαν σημαντικές ευπάθειες στην υπηρεσία Java Cloud της Oracle που απευθύνεται σε χιλιάδες προγραμματιστές εφαρμογών με αποτέλεσμα την πρόσβαση σε δεδομένα κρίσιμων εφαρμογών. Επιπλέον η Oracle δέχθηκε την κριτική για το γεγονός ότι δεν έδωσε έγκαιρα στη δημοσιότητα τις λεπτομέρειες του συγκεκριμένου συμβάντος.

3.2.3 Προκλήσεις και ευκαιρίες για τις λύσεις της Oracle στο ΥΝ

Η Oracle (Oracle, 2011) πρωτοστάτησε στην ιδέα για την πρόσβαση στις κατά παραγγελία (on demand) εφαρμογές σαν υπηρεσία στο cloud πριν από περισσότερο μια δεκαετία. Αναγνωρίζεται σαν μία από τις κορυφαίες εταιρείες παροχής υπηρεσιών cloud, με περισσότερους από 5,5 εκ. χρήστες σε όλο τον κόσμο που έχουν πρόσβαση στις εφαρμογές της στο σύννεφο. Προσφέρει την δυνατότητα επιλογής μοντέλων ανάπτυξης από συνδρομητικές υπηρεσίες με βάση και τις εφαρμογές των πελατών που φιλοξενούνται στην Oracle, σε τρίτα ή σε ιδιόκτητα κέντρα δεδομένων, και ιδιωτικά clouds.

Το χαρτοφυλάκιο της Oracle είναι εκτεταμένο για οριζόντιες και συγκεκριμένων βιομηχανιών εφαρμογές και όλες οι οντότητες μπορούν να φιλοξενηθούν μέσα στο Oracle On Demand ή μέσα στους συνεργαζόμενους παρόχους υπηρεσιών. Επίσης, η Oracle προσφέρει

ένα πλούσιο σύνολο συνδρομητικών υπηρεσιών, όπως το Customer Relationship Management (CRM), το Human Capital Management (HCM) και οι συμβάσεις.

Σύγκριση PaaS και Iaas

Για πολλές επιχειρήσεις το βασικό ζήτημα στην επιλογή μεταξύ της δημιουργίας ενός PaaS ή της χρησιμοποίησης ενός προσφερόμενου IaaS, είναι το κατά πόσον μια τυποποιημένη, επαναχρησιμοποιήσιμη και κοινόχρηστη (shared) πλατφόρμα θα κάνει αυτό που θέλουν οι επιχειρήσεις να παρέχουν στους πελάτες τους. Ένα IaaS προσφέρει τις βασικές ικανότητες υπολογισμού, αποθήκευσης και δικτύωσης, με συνέπεια να είναι περισσότερο ευέλικτο. Όμως το IaaS απαιτεί από τους χρήστες να παρέχουν τα υπόλοιπα, συμπεριλαμβανομένων των εφαρμογών, του middleware και των βάσεων δεδομένων, με αποτέλεσμα να υπάρχει μεγαλύτερο κόστος ανάπτυξης, χρόνου και ανομοιογένειας. Για πολλές επιχειρήσεις ένα ιδιωτικό PaaS είναι μια φυσική στρατηγική που ωφελεί τους χρήστες καθώς επίσης και τον πάροχο υπηρεσιών πληροφορικής. Ένα PaaS δίνει στους χρήστες έναν τυποποιημένο, επαναχρησιμοποιήσιμο και κοινόχρηστο σημείο εκκίνησης για την ανάπτυξη εφαρμογών, παρέχοντας έναν γρηγορότερο και απλούστερο τρόπο ανάπτυξης εφαρμογών με επαρκή ευελιξία. Από την πλευρά των τμημάτων πληροφορικής η χρησιμοποίηση μιας υποδομής PaaS σημαίνει μεγαλύτερη διαχειρισιμότητα, ασφάλεια, συνέπεια και έλεγχο.

Εξέλιξη των επιχειρήσεων στο cloud computing

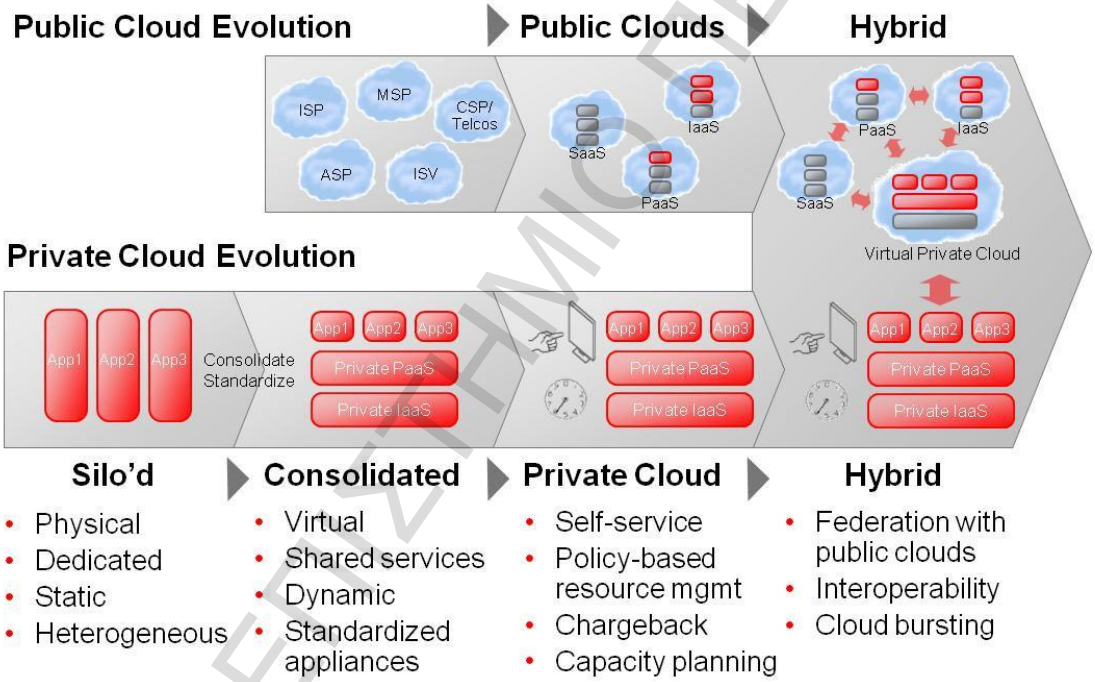
Οι περισσότερες επιχειρήσεις εξελίσσουν την τρέχουσα υποδομή πληροφορικής τους για να υιοθετήσουν περισσότερα cloud χαρακτηριστικά με την πάροδο του χρόνου, αντί να μετακινήσουν άμεσα τα πάντα στο cloud. Η τεχνολογία εξελίσσεται και αναπτύσσεται ραγδαία, έχοντας σαν αποτέλεσμα οι επιχειρήσεις να πρέπει να αλλάξουν τις πολιτικές και τις διεργασίες τους. Σε πολλές περιπτώσεις θα πρέπει να είναι διαθέσιμες οι τεχνικές υποδομές των κτιρίων που στεγάζουν τις επιχειρήσεις, έτσι να μπορούν να γίνουν άμεσα οι απαραίτητες οργανωτικές αλλαγές που απορρέουν από την εφαρμογή των καινούργιων τεχνολογικών αλλαγών.

Για πολλά κέντρα δεδομένων κατά την μετάπτωση σε ένα ιδιωτικό cloud το πρώτο βήμα είναι η ενοποίηση, μεταβαίνοντας από αποκλειστικά περιβάλλοντα σε κοινόχρηστες και ελαστικά επεκτάσιμες πλατφόρμες και υποδομές. Οι εφαρμογές σιλό που λειτουργούν σε αποκλειστικό middleware, βάσεις δεδομένων, διακομιστές και αποθηκευτικά μέσα είναι σχεδιασμένες για ένα συγκεκριμένο φόρτο εργασίας, έτσι δεν υπάρχει εγγενώς πλεονάζουσα διαθεσιμότητα και πόροι που να μπορούν να χρησιμοποιηθούν για αυτές τις εφαρμογές. Κάθε σιλό μπορεί να περιλαμβάνει 12 ετερογενή συστήματα από πολλαπλούς προμηθευτές, οδηγώντας σε μεγάλη πολυπλοκότητα και υψηλά διαχειριστικά κόστη. Με την μετάβαση σε μια ενοποιημένη αρχιτεκτονική με τυποποιημένες, κοινόχρηστες υπηρεσίες, μπορεί να πραγματοποιηθεί σημαντική εξοικονόμηση κόστους.

Η ενοποίηση μπορεί να γίνει είτε στο επίπεδο του IaaS, συνήθως αξιοποιώντας την τεχνολογία των εικονικών διακομιστών (server virtualization technology), είτε στο επίπεδο του PaaS, μέσω της τυποποίησης και της εδραίωσης σε μια ενιαία βάση δεδομένων ή / και σε μια middleware αρχιτεκτονική. Η ενοποίηση στο επίπεδο του PaaS προσφέρει περισσότερη αξία, επειδή μειώνει την ετερογένεια των χρησιμοποιούμενων λογισμικών, πράγμα το οποίο είναι ο πραγματική κινητήρια δύναμη της πολυπλοκότητας και του κόστους, πέρα από την αύξηση της αξιοποίησης των πόρων της τεχνολογιών πληροφορικής. Η ενοποίηση στο επίπεδο του IaaS μπορεί επίσης να προσφέρει υψηλότερη απόδοση με τον διαμοιρασμό του υλικού, αλλά δεν κάνει τίποτα για να μειώσει την πολυπλοκότητα των χρησιμοποιούμενων λογισμικών που

εκτελούνται πάνω από το υλικό. Μια πρόσφατη έρευνα στους πελάτες της Oracle έδειξε ότι η ενοποίηση στο επίπεδο του middleware και της βάσης δεδομένων ήταν ποιο δημοφιλής από την ενοποίηση στο επίπεδο του υπολογιστικού διακομιστή και των αποθηκευτικών μέσων. Ορισμένοι πελάτες βέβαια κάνει ενοποίηση και στα δύο επίπεδα.

Ενώ το virtualization είναι μια σημαντική τεχνολογία για το cloud computing, είναι επίσης σημαντικό να κατανοήσουμε ότι μια άλλη τεχνολογία που ονομάζεται ομαδοποίηση (clustering) είναι συμπληρωματική και επίσης πολύ σημαντική. Το virtualization είναι ένας πολύ καλός τρόπος για να διαμοιράζεται το υλικό και να επιτρέπεται η εύκολη ανάπτυξη εφαρμογών. Η ομαδοποίηση (clustering) είναι κρίσιμη για ενεργοποίηση της κλιμάκωσης πέρα από μια απλή φυσική μηχανή και για την ανοχή στα σφάλματα. Η Oracle προσφέρει μια επιλογής για της τεχνολογίες virtualization, συμπεριλαμβανομένων των Oracle VM για x86, Oracle VM για την αρχιτεκτονική SPARC και Oracle Solaris Containers. Η Oracle προσφέρει επίσης μια ολοκληρωμένη σειρά συγκεντρωμένων προϊόντων, συμπεριλαμβανομένων των Oracle Database Real Application Clusters, Oracle TimesTen In-Memory Database, Oracle WebLogic application server και Oracle Coherence in-memory data grid.



Εικόνα 13: Εξέλιξη δημοσίων και ιδιωτικών clouds Invalid source specified.

Το επόμενο βήμα στην εξέλιξη είναι η προσθήκη αυτό-εξυπηρέτησης (self-service), αυτόματης κλιμάκωσης και χρέωσης. Ένας εργαζόμενος μπαίνει στην ηλεκτρονική πύλη των εργαζομένων, ταυτοποιείται επιτυχώς, κάνει αίτηση για ένα εικονικό μηχάνημα με ένα ορισμένο ποσό CPU, μνήμης και δίσκου, παίρνει μια εικόνα (image) μιας βάσης δεδομένων ή ενός middleware και στην συνέχεια πατάει «υποβολή». Εάν ο ρόλος και τα δικαιώματα αυτού του εργαζομένου του επιτρέπουν να έχει αυτό το ποσό πόρων πληροφορικής, τότε αυτά αυτόματα του τροφοδοτούνται χωρίς να εμπλακεί κάποιος διαχειριστής (administrator) από το τμήμα πληροφορικής (IT). Εάν όχι, τότε η αίτησή του μπορεί να δρομολογηθεί για έγκριση σε έναν διευθυντή (manager), είτε του τμήματος πληροφορικής (IT) είτε όχι. Με την εφαρμογή αυτής της φαινομενικά απλής διαδικασίας θα είναι έτοιμο και θα λειτουργεί ένα στιγμιότυπο μιας PaaS

Πλατφόρμας. Αφού αυτό το στιγμιότυπο έχει τεθεί στην παραγωγή, το σύστημα κάνει διαχείριση των πόρων με βάση μια πολιτική για την αυτόματη προσαρμογή της χωρητικότητας. Κάθε μήνα η επιχειρηματική μονάδα του εργαζόμενου χρεώνεται με μια εσωτερική επιβάρυνση με βάση το ποσό των πόρων πληροφορικής που καταναλώνει αυτό το στιγμιότυπο. Για να γίνουν όλα αυτά πραγματικότητα θα πρέπει η επιχείρηση να έχει καθορισμένες πολιτικές και διαδικασίες, και η τεχνολογία θα πρέπει να είναι σε θέση να τις εφαρμόσει.

Πρέπει να επισημανθεί ότι δεν ωφελούνται όλες οι επιχειρήσεις από την αυτό-εξυπηρέτηση (self-service) και την ελαστική επεκτασιμότητα, αλλά πολλές όμως ωφελούνται, συνεπώς οι επιχειρήσεις το υπολογίζουν αυτό και κάνουν την κίνησή τους ή όχι προς αυτή την κατεύθυνση. Ορισμένες επιχειρήσεις δεν είναι έτοιμες να εφαρμόσουν πλήρως την αυτό-εξυπηρέτηση, δεδομένου ότι πρέπει να καθοριστούν πολλές πολιτικές και διαδικασίες, και μπορεί να προτιμούν μοντέλα χρέωσης πληρωμής κατά την χρήση (pay-per-use). Επίσης, μπορεί να υπάρχουν και άλλες προκλήσεις όπως η δια-επιχειρησιακή οργανωτική υποστήριξη, η δημιουργία του επιχειρηματικού μοντέλου και του μοντέλου χρηματοδότησης, και διάφορα πολιτιστικά (cultural) θέματα.

3.2.4 Απειλές για τις λύσεις της Oracle στο ΥΝ

Τα αυξημένα κόστη συντήρησης του εξοπλισμού που διαθέτει δεν της επιτρέπουν να ανταγωνιστεί μικρότερου βεληνεκούς προμηθευτές που έχουν χαμηλότερα κόστη. Επιπλέον, στις σημαντικές εμπορικά εφαρμογές που διαθέτει ως υπηρεσία μέσω του cloud έχει να αντιμετωπίσει σημαντικό ανταγωνισμό (πχ την Salesforce.com στον τομέα των CRM εφαρμογών).

Η στρατηγική της Oracle είναι να καθιερωθεί ως ένας προμηθευτής από τον οποίο οι πελάτες θα προμηθευτούν κάθε υπηρεσία. Αυτό το μοντέλο δεν προσελκύει όσους πελάτες επιθυμούν την σποραδικότητα, δηλαδή την συνεργασία με κάθε προμηθευτή ο οποίος διακρίνεται σε μία ορισμένη περιοχή. Επιπλέον, οι πελάτες να μην ενδιαφέρονται τόσο για την επιλογή του κατάλληλου μοντέλου (δημόσιου, ιδιωτικού, υβριδικού) όσο αν το συγκεκριμένο ΥΝ του προσφέρει επιχειρησιακή αξία και ευελιξία για να μπορέσει να προσφέρει από τη δική του σκοπιά προϊόντα και υπηρεσίες στους πελάτες τους.

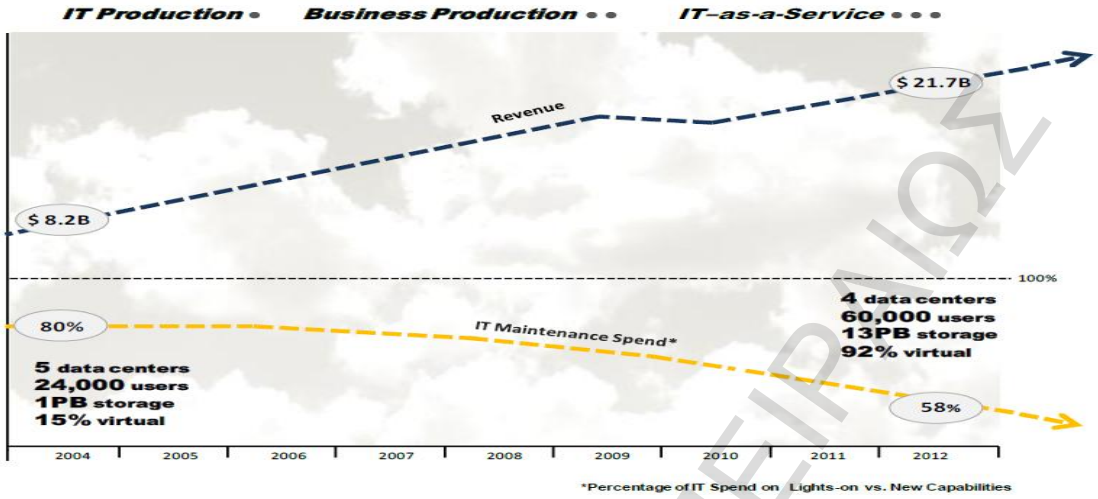
3.3 EMC HYBRID CLOUD SOLUTION - HYBRID CLOUD

3.2.1 Επισκόπηση επιχειρησιακών επιτευγμάτων

Στην Εικόνα 14 παρέχεται μια επισκόπηση σε υψηλό επίπεδο για τα επιχειρησιακά επιτεύγματα της EMC στο πλαίσιο της εταιρικής της ανάπτυξης (Garrett, et al., 2013) μεταξύ του 2004 και του 2012. Εκτός από την αύξηση του αριθμού των χρηστών που υποστηρίζει, τα έσοδα της EMC αυξήθηκαν από 8.2 δις. $ σε 21.7 δις. $, και η συνολική πληροφορία που διαχειρίζεται αυξήθηκε από το 1 PB σε 5 σε πέντε κέντρα δεδομένων (data centers) στα 13 PB σε 4 σε πέντε κέντρα δεδομένων.

Για την EMC οι δαπάνες συντήρησης της πληροφοριακής (IT) υποδομής έχουν μειωθεί από το 80% στο 58% επιτρέποντας την αύξηση των δαπανών για την καινοτομία από 20% έως και 42%. Την ίδια στιγμή όμως αυξήθηκαν και τα έσοδα, με αποτέλεσμα η EMC να έχει την δυνατότητα να διεκδικήσει σημαντικούς οικονομικούς πόρους για επενδύσεις σε νέα έργα. Η

ανάπτυξη μια ιδιωτικής υποδομής cloud που περιλαμβάνει 92% εικονικούς διακομιστές (virtual servers) είναι πρωταρχική κινητήρια δύναμη σε αυτά τα αποτελέσματα.



Εικόνα 14: Έσοδα της EMC σε σύγκριση με τις δαπάνες συντήρησης της πληροφοριακής (IT) υποδομής (Garrett, et al., 2013)

3.2.2 Οι τρεις φάσης ανάπτυξης του EMC cloud

Το 2004 η εταιρεία ξεκίνησε μια πρωτοβουλία για την βελτίωση της αποδοτικότητας των χρησιμοποιούμενων τεχνολογιών πληροφορικής και της επιχειρηματικής ευελιξίας, ενώ παράλληλα προχωρούσε σε βελτίωση της ασφάλειας και της περαιτέρω ενίσχυσης των διαθέσιμων επιλογών των υπηρεσιών πληροφορικής για την εταιρεία. Κατά την διάρκεια των τελευταίων 8 χρόνων η εταιρεία μεταμόρφωσε την πληροφοριακή της υποδομή (Garrett, et al., 2013).

1η Φάση: Νέες τεχνολογίες πληροφορικής στην παραγωγή (2004 – 2008)

Ο πρωταρχικός στόχος αυτής της φάσης στόχευε στην παγίωση της πληροφοριακής (IT) υποδομής και του virtualization των διακομιστών που χρησιμοποιούνταν τόσο για δοκιμές / ανάπτυξη λογισμικού όσο και για τις ιδιόκτητες εφαρμογές πληροφορικής. Στην αρχή το περιβάλλον εξυπηρετούσε 24000 εσωτερικούς χρήστες και η πληροφοριακή (IT) υποδομή αποτελούνταν από 5 κέντρα δεδομένων με 168 διαφορετικούς τύπους υποδομών, συμπεριλαμβανομένου 1 PB αποθηκευτικού χώρου και 2000 φυσικών διακομιστών. Η εταιρεία χρησιμοποιούσε / υποστήριζε σχεδόν 400 εφαρμογές και εργαλεία, με λύσεις διαχείρισης και ασφάλειας που είχαν υλοποιηθεί μετά την δημιουργία της υποδομής. Τα Windows ήταν η μοναδική προσφερόμενη πλατφόρμα για τον τελικό χρήστη. Μερικές από τις χρόνιες λειτουργικές απαιτήσεις ήταν:

- Μεγάλο διάστημα για την παροχή πληροφοριακών (IT) υποδομών που υπερβαίνει τους τρεις μήνες
- Χαμηλή χρησιμοποίηση (30%) της παραγωγικής αποθηκευτικής ικανότητας, με περισσότερο από 60% ετήσια ανάπτυξη των συστημάτων αποθήκευσης
- Κάτω από 10% χρησιμοποίηση της επεξεργαστικής ισχύς (CPU) με πάνω από 20% ετήσια αύξηση των διακομιστών

- Ανεπαρκής χώρος και ενέργεια στα κέντρα δεδομένων
- Κουρασμένο πληροφοριακό (IT) προσωπικό από την ζήτηση υπηρεσιών

Αυτές οι προκλήσεις δεν είναι μοναδικές στην EMC, ή ακόμα και σε μεγάλες εταιρείες ή σε εταιρείες σε έναν συγκεκριμένο τομέα. Τα χαμηλά ποσοστά χρησιμοποίησης των υποδομών, οι μεγάλοι χρόνοι για την παροχή υπηρεσιών, τα όρια στον χώρο και στην ενέργεια στην ενέργεια στα κέντρα δεδομένων και το τεντωμένο πληροφοριακό (IT) προσωπικό είναι μερικά από τα συχνά προβλήματα μεταξύ πληροφοριακών οργανισμών κάθε μεγέθους σε όλο τον κόσμο.

Από νωρίς λήφθηκε μια βασική απόφαση για την τυποποίηση στην x86 αρχιτεκτονική και στο virtualization των διακομιστών. Επίσης, η εταιρεία μετέβη σε λύση αντιγράφων ασφαλείας βασισμένη σε δίσκους. Υλοποιήθηκαν αρκετά βασικά προγράμματα για την συνεχή αύξηση της αναλογίας εικονικών έναντι φυσικών διακομιστών. Οι προσπάθειες για ενοποίηση, virtualization και για βαθμιδωτά επίπεδα αποθήκευσης παρείχαν στο τμήμα πληροφορικής την εμπειρία και την έκθεση στις τεχνολογίες που θα είναι η κινητήριος δύναμη της μεταμόρφωσης.

2η Φάση: Αλλαγή επιχειρησιακών δραστηριοτήτων (2009 – 2010)

Αυτή η φάση επικεντρώνεται στο virtualization κρίσιμων εφαρμογών όπως τα MS Exchange, Active Directory, Oracle 11i E-Business Suite, τα εργαλεία υποβολής έξυπνων επιχειρηματικών και επιχειρησιακών αναφορών, και πολλά άλλα εργαλεία και εφαρμογές. Μέχρι το τέλος αυτής της φάσης η EMC είχε κάνει εικονικούς το 70% περίπου των διακομιστών της. Στοίβες υφιστάμενων κλειστών υποδομών καταργήθηκαν και αντικαταστάθηκαν από κλιμακωτά και διαμοιραζόμενα συμπλέγματα εικονικής υποδομής (VMware clusters) με ενσωματωμένη διαχείριση και ασφάλεια. Ατό είχε σαν αποτέλεσμα τα συμπλέγματα της εικονικής υποδομής να αρχίσουν να συγκλίνουν σε μια συνεκτική στρατηγική πλατφόρμα.

Μεταξύ του 2004 και του 2010 έγιναν και άλλες σημαντικές βελτιώσεις. Για παράδειγμα, η EMC αύξησε την βελτιστοποίηση των παρεχόμενων λύσεων με το virtualization της υποδομής των δικτυακών χώρων αποθήκευσης (SAN), με την τυποποίηση της αρχιτεκτονικής (VCE VBlock, VSPEX), και δημιουργώντας ένα ολοκληρωμένο περιβάλλον ΥΝ. Ο βελτιωμένος τρόπος ταυτοποίησης (authentication) και οι τεχνολογίες πρόληψης απώλειας δεδομένων έχουν κάνει το ιδιωτικό ΥΝ πολύ ποιο ασφαλές, μαζί με τις βελτιώσεις στην παρακολούθηση και στην αυτοματοποιημένη διαχείρισή του. Η δεύτερη φάση οδήγησε σε πρόσθετη μείωση του κόστους καθώς και στην μεγαλύτερη απόδοση των εφαρμογών, την υψηλότερη διαθεσιμότητα, την αύξηση της παραγωγικότητας των τελικών χρηστών καθώς και στην μείωση του κινδύνου. Έχοντας επενδύσει τόσο χρόνο όσο και προσπάθεια στην αναδιαμόρφωση της η EMC έχει δημιουργήσει μία εικονική, ενοποιημένη και κλιμακωτή υποδομή.

3η Φάση: Παροχή τεχνολογιών πληροφορικής σαν υπηρεσία (2011 – παρών)

Ο στόχος αυτής της φάσης είναι η επίτευξη της επιχειρηματικής ευελιξίας μέσω της προσφοράς πληροφοριακών πόρων ως υπηρεσία (IT-as-a-Service – ITaaS). Ενώ συνεχίζονται όλες οι προσπάθειες πλέον η προσοχή στρέφεται στην αλλαγή σε ένα μοντέλο παροχής υπηρεσιών. Αυτό έχει σαν αποτέλεσμα ένα μεγάλο μέρος της προσπάθειας να βρίσκεται τώρα σε ανθρώπους και σε διαδικασίες παρά στην τεχνολογία, όπως ακριβώς το ITaaS απαιτεί η EMC να δουλέψει / τρέξει τις τεχνολογίες πληροφορικής ως επιχείρηση.

Στη φάση αυτή η εταιρεία έχει δημιουργήσει σημαντικά αποτελέσματα. Η EMC τώρα έχει 60000 εσωτερικούς χρήστες και 5 κέντρα δεδομένων με δυνατότητα αποθήκευσης 13 PB.

Επίσης, έχει αυξηθεί και ο αριθμός των χρησιμοποιούμενων εφαρμογών και εργαλείων από 400 σε 500. Σε παγκόσμιο επίπεδο υπάρχουν 9000 εικονικά λειτουργικά συστήματα (virtual machines), αλλά έχουν καταφέρει να μειώσουν τον αριθμό των φυσικών Intel x86 διακομιστών από 2000 σε 1500. Το 92% των διακομιστών είναι εικονικοί και ο στόχος να είναι το 100% των διακομιστών εικονικός είναι κοντά στο να επιτευχθεί. Αξίζει επίσης να σημειωθεί ότι το τμήμα πληροφορικής της EMC έχει τυποποιήσει τις υποδομές πληροφορικής στην VCE Vblock αρχιτεκτονική.

3.2.3 Πλεονεκτήματα των υπηρεσιών της EMC (Strengths)

Μείωση κόστους

Οι προσπάθειες της EMC έχουν οδηγήσει στην αποφυγή του κόστους κεφαλαίου και την εξοικονόμηση δαπανών λειτουργίας. Στην συνέχεια παρατίθενται μερικά από τα επιτεύγματα μείωσης του κόστους από το 2004:

- 157 εκ. $ από την αποφυγή του κόστους επένδυσης κεφαλαίου. Η εικονική υποδομή και η ενοποίηση των διακομιστών και του αποθηκευτικού χώρου επέτρεψε την δραστική μείωση των αναγκών για φυσικό εξοπλισμό. Επιπλέον, ενώ τα δεδομένα έχουν αυξηθεί σημαντικά, οι ανάγκες των κέντρων δεδομένων παραμένουν ίδιες. Αυτό έχει σαν αποτέλεσμα τα ποσοστά χρησιμοποίησης της πληροφοριακής (IT) υποδομής (υπολογιστική ισχύς, αποθήκευση και δίκτυο) να έχουν αυξηθεί σε ποσοστό 75%. Η πραγματοποίηση περισσότερων εργασιών χρησιμοποιώντας λιγότερο εξοπλισμό με υψηλότερα ποσοστά χρησιμοποίησης του είναι αποτέλεσμα της δραματικής βελτίωσης της αποτελεσματικότητας.
- 66 εκ. $ από εξοικονόμηση λειτουργικών εξόδων. Αυτό κυρίως ήταν το αποτέλεσμα της ανάπτυξης ενός ιδιωτικού ΥΝ με διάχυτη εικονική υποδομή επιτυγχάνοντας μία αναλογία ενοποίησης των εικονικών μηχανών προς τους φυσικούς διακομιστές της τάξης του 14:1. Τα συστήματα πλέον σχεδιάζονται με έναν τέτοιο τρόπο ώστε να επιτυγχάνουν υψηλότερους λόγους ενοποίησης, προσφέροντας δυνατότητες για ακόμα μεγαλύτερη εξοικονόμηση.
- Λόγω της εικονικής διαμόρφωσης και της ενοποίησης έχουν δημιουργηθεί εξοικονομήσεις στον προϋπολογισμό των υποδομών πληροφορικής επιτρέποντας της επανεπένδυση αυτών των κεφαλαίων. Όπως έχει αναφερθεί και προηγούμενα, η EMC έχει μειώσει την αναλογία των λειτουργικών εξόδων για πληροφοριακές υποδομές προς τα έσοδά της κατά 28%, απελευθερώνοντας κεφάλαια για νέα έργα.

Αποδοτικότητα προσωπικού

Οι πρόσφατες υλοποιήσεις βελτιωμένων και αυτοματοποιημένων εργαλείων διαχείρισης έχουν επιτρέψει στην EMC να χρησιμοποιεί αποτελεσματικότερα το προσωπικό που ασχολείται με θέματα πληροφορικής. Για παράδειγμα, το τμήμα IT Operations Intelligence (SMARTS) της EMC παρέχει καλύτερη ορατότητα και έλεγχο του συνόλου της υποδομής ΥΝ και της «υγείας» της για την αποφυγή βλαβών σε κρίσιμες υποδομές. Επιπλέον, από το 2009 και μετά, κατά την περίοδο μιας ισχυρής αύξησης των εσόδων, ο αριθμός του συνολικού προσωπικού που απασχολούνταν με θέματα πληροφορικής παρέμεινε σταθερός.

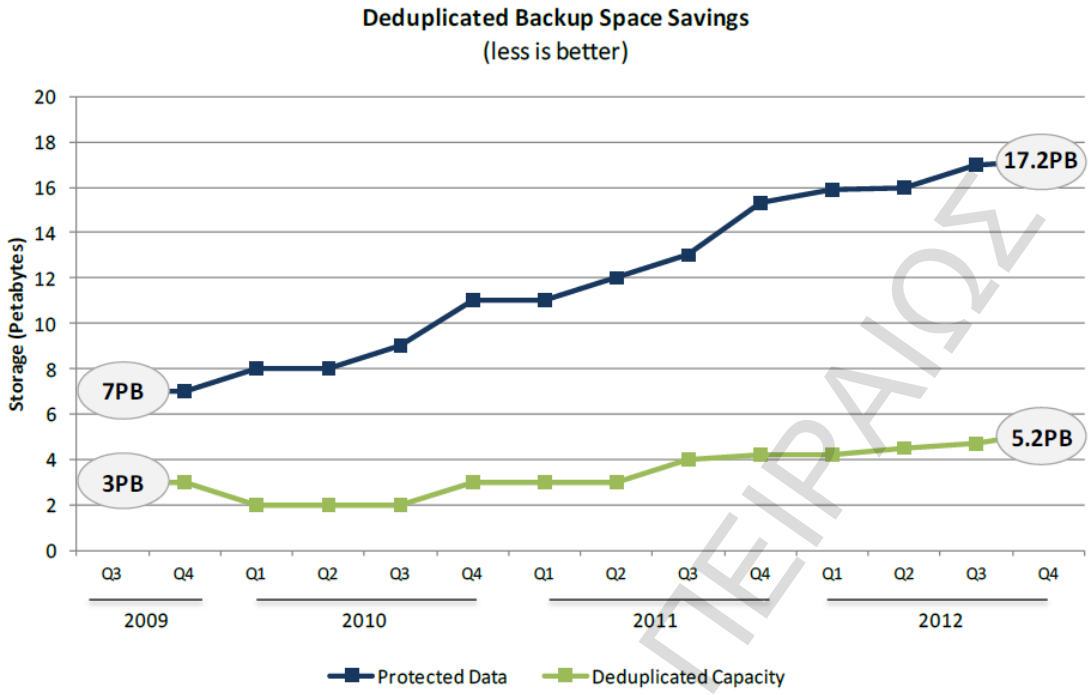
Ενεργειακή αποδοτικότητα

Η ενοποιημένη και η φυσική υποδομή έχουν ως αποτέλεσμα την αύξηση κατά 34% στην ενεργειακή απόδοση, καθώς και στην μείωση της παραγωγής CO_2 κατά 100 εκατομμύρια λίβρες. Το νέο εικονικό κέντρο δεδομένων στο Durham της βόρειας Καρολίνας των Η.Π.Α. είναι ένα μοντέλο ενεργειακής απόδοσης. Για παράδειγμα, από την συγκομιδή όμβριων υδάτων έχει μειωθεί η χρήση του πόσιμου νερού κατά 40% και το 57% του χρόνου χρησιμοποιείται εξωτερικός αέρας για την ψύξη των εγκαταστάσεων. Το κέντρο δεδομένων χρησιμοποιεί Flywheel UPS, επιτρέποντας την πλήρη εξάλειψη των μπαταριών από την εγκατάσταση. Παρά την αυξημένη ζήτηση για διακομιστές και αποθηκευτικούς χώρους έχει γίνει εξοικονόμηση 271 watt ανά διακομιστή με την χρήση virtualization, μειώνοντας την ηλεκτρική ισχύ κατά 73% για κάθε TB, εξοικονομώντας ηλεκτρική ενέργεια για περίπου 2000 νοικοκυριά.

Αποδοτικότητα αντιγράφων ασφαλείας

Με την μόχλευση των λύσεων της η EMC έχει καταφέρει να μεταμορφώσει την διαδικασία λήψης και επαναφοράς των αντιγράφων ασφαλείας. Έχει καταφέρει να εξαλείψει την ανάγκη λήψης αντιγράφων ασφαλείας για συγκεκριμένες εφαρμογές παρέχοντας αρχειοθέτηση (archiving) σε πραγματικό χρόνο. Αυτό έχει σαν αποτέλεσμα την μείωση του αποθηκευτικού χώρου κατά 1 PB για τα μηνύματα ηλεκτρονικής αλληλογραφίας, το σύστημα αρχείων και τα αρχεία των βάσεων δεδομένων, μετά την διαγραφή τους από το χρονοδιάγραμμα δημιουργίας αντιγράφων ασφαλείας λόγω της αρχειοθέτησης σε πραγματικό χρόνο. Στα κέντρα δεδομένων ο μηχανισμός δημιουργίας αντιγράφων ασφαλείας *deduplication* έχει μειώσει περαιτέρω το ποσό των δεδομένων που πρέπει να γραφούν σε αντίγραφα ασφαλείας καθώς και τον χρόνο που παίρνει η διαδικασία δημιουργίας αντιγράφων ασφαλείας κατά 75%. Το Avamar χρησιμοποιείται επίσης για την κεντρικοποιημένη συλλογή και διαχείριση των αντιγράφων ασφαλείας για 121 απομακρυσμένες περιοχές (sites), αυξάνοντας την διαθεσιμότητα των δεδομένων και εκμηδενίζοντας παράλληλα τα κόστη για αντίγραφα ασφαλείας εκτός αυτών των περιοχών. Οι αστοχίες στα αντίγραφα ασφαλείας έχουν μειωθεί κατά 99%. Εν κατακλείδι, οι χρήστες είναι ποιο παραγωγικοί (ακόμα και οι κλήσεις στο help desk έχουν μειωθεί) με την χρήση του Avamar desktop backup και με την αποκατάσταση αρχείων με ίδιες ενέργειες των χρηστών.

Τα οφέλη που προκύπτουν από το deduplication είναι πολλά και αξίζει να γίνει μια ποιο επισταμένη αναφορά σε αυτά. Όπως φαίνεται στην Εικόνα 15 από το τρίτο τρίμηνο του 2009 έως το 2012 το συνολικό ποσό των δεδομένων που προστατεύθηκε αυξήθηκε από τα 7 PB στα 17,2 PB, συμπεριλαμβανομένων των προσωρινών δεδομένων που απαιτούνται για την μετάβαση στο κέντρο δεδομένων του Durham. Ωστόσο, λόγω της αποτελεσματικότητας του deduplication των Avamar και Data Domain η χωρητικότητα που απαιτείται για τα αντίγραφα ασφαλείας αυξήθηκε μόνο από τα 3 PB στα 5,2 PB.



Εικόνα 15: Το deduplication της EMC μειώνει την χωρητικότητα των αντιγράφων ασφαλείας (Garrett, et al., 2013)

Απόδοση κρίσιμων εφαρμογών με την χρήση του VCE Vblock

Η EMC έχει κάποια τρανταχτά παραδείγματα από την αποτελεσματικότητα του virtualization σε κρίσιμες εφαρμογές. Η σουίτα εφαρμογών για την διαχείριση των πελατών (CRM) αγγίζει σχεδόν κάθε τμήμα της EMC συμπεριλαμβανομένων των τμημάτων κατασκευής, χρηματοδότησης, αναφορών, εξυπηρέτησης πελατών, επαγγελματικών υπηρεσιών (professional services) πωλήσεων και μάρκετινγκ. Το περιβάλλον του CRM είναι τεράστιο με μερικά από τα χαρακτηριστικά του να είναι: περισσότερα από 70 επίπεδα εφαρμογών, 8,8 δις. σειρές δεδομένων σε μια βάση 12 TB και 57 εκ. καθημερινών συναλλαγών που πραγματοποιούνται από 40000 επώνυμους χρήστες (και 4000 ταυτόχρονους χρήστες σε ώρες αιχμής). Η EMC μετέφερε την γερασμένη φυσική υποδομή (η οποία υπέφερε από προβλήματα στην απόδοση των CPU, κακή απόδοση και επεκτασιμότητα και από υποβαθμισμένη εμπειρία χρήσης από τον χρήστη) σε μια εικονική υποδομή με 7x24x365 διαθεσιμότητα. Αυτή η διαδικασία ξεκίνησε με την μεταφορά 210 φυσικών διακομιστών σε 20 multi-tenant ESX διακομιστές σε vBlock αρχιτεκτονική με Cisco UCS διακομιστές, Red Hat Linux και VMware vSphere, και Symmetrix VMAX βαθμωτά μέσα αποθήκευσης. Τα αποτελέσματα δείχνουν 60% - 90% βελτίωση της παραγωγικότητας και εξοικονόμηση 7 εκ. $ από τον τομέα του περιβάλλοντος, των αδειών, της συντήρησης και της υποστήριξης, καθώς επίσης και επί 10 καλύτερη απόδοση.

Η EMC επίσης έχει προβεί στο πλήρες virtualization του καινούργιου της ERP συστήματος το οποίο βασίζεται στο SAP, έχοντας αντικαταστήσει περισσότερα από 50 απαρχαιωμένα συστήματα, σε μια ολοκληρωμένη VCE Vblock αρχιτεκτονική που αποτελείται από 14 Cisco

UCS blade διακομιστές με σύνολο 280 πυρήνες και 3,5 TB RAM. Το Application Integration Cloud (AIC), οι εφαρμογές του SAP και οι βάσεις δεδομένων βρίσκονται σε 100 εικονικές θέσεις (hosts), όπου εξυπηρετούνται 18000 χρήστες με την εικονική εφαρμογή ThinApp της VMware. Το cluster των 32 κόμβων έχει σύνολο 68 συνδέσεις ρεύματος, δικτύου και SAN, ενώ μια παραδοσιακή αρχιτεκτονική θα χρησιμοποιούσε 448. Αυτή η αρχιτεκτονική παρέχει μικρότερο αποτύπωμα και λιγότερα σημεία για ρυθμίσεις και παραμετροποιήσεις (και συνεπώς λιγότερες πιθανότητες λάθους). Επιπλέον, είναι περισσότερο ευέλικτη γιατί η προσθήκη ή η αντικατάσταση διακομιστών απαιτεί ώρες αντί για μέρες όπως στο παρελθόν. Επιπλέον, ο αναπροσανατολισμός των διακομιστών μπορεί να επιτευχθεί χωρίς φυσική αναδιάρθρωση και οι νέες εργασίες διαμόρφωσης του VLAN έχουν μειωθεί κατά 10 φορές.

Διαφάνεια στη τιμολόγηση και χρεώσεις

Η απόδειξη της αξίας των τεχνολογιών πληροφορικής στην πράξη είναι ένα σημαντικό στοιχείο για την λειτουργία των τεχνολογιών πληροφορικής σαν επιχείρηση. Οι πελάτες αξιολογούν τα προϊόντα και τις υπηρεσίες από το τι προσφέρουν και σε ποια τιμή, και το τμήμα πληροφορικής (IT) της EMC πρέπει να προσδιορίσει αυτά ακριβώς τα χαρακτηριστικά για να μπορέσει να πουλήσει την αξία τους. Καθώς το τμήμα πληροφορικής (IT) της EMC αρχίζει να παραδίδει ITaaS, θα πρέπει να είναι σε θέση να μπορεί να ανταγωνιστεί με εξωτερικές υπηρεσίες παροχής cloud και να μετριάσει τον κίνδυνο του «Shadow IT». Αυτός ο κίνδυνος προέρχεται όταν οι επιχειρηματικές μονάδες είναι δύσκολο να συνεργαστούν με το τμήμα πληροφορικής (IT), και πηγαίνουν στην ελεύθερη αγορά να αγοράσουν δικτυακά (online) με την πιστωτική τους κάρτα μια εφαρμογή ή υπηρεσίες υποδομών από το cloud.

Αυτό είχε σαν αποτέλεσμα η EMC να ξεκινήσει μια προσπάθεια για την διαφάνεια των οικονομικών της συναλλαγών για να προσφέρει μια σαφή εικόνα για τις πραγματικές δαπάνες της πληροφορικής και των εξόδων της αντίστοιχης επιχειρηματικής μονάδας πληροφορικής με βάση την πραγματική κατανάλωση. Αυτή η πληροφορία κάνει τόσο τις επιχειρηματικές μονάδες όσο και το τμήμα πληροφορικής ποιο συνετά και λιγότερο πιθανό να υπέρ χρησιμοποιήσουν πόρους, έχοντας ως αποτέλεσμα την καλύτερη ευθυγράμμιση της χρήσης της τεχνολογίας με την ζήτηση. Η EMC έχει δημιουργήσει ένα καινούργιο σύνολο διαδικασιών για την τιμολόγηση των υπηρεσιών πληροφορικής, την ανάλυση κόστους και την μέτρηση / τιμολόγησή τους. Η εταιρεία καθόρισε κατηγορίες υπηρεσιών και κατένειμε σταθερά και μεταβλητά κόστη, ενώ παράλληλα καθόριζε τα προγράμματα λειτουργίας (drivers) και τα κόστη των μονάδων. Με βάση αυτές τις πληροφορίες η EMC δημιούργησε τις τιμές για τις υπηρεσίες πληροφορικής που αντανακλούν τους εταιρικούς στόχους. Η αρχή έγινε με την επίδειξη στις επιχειρηματικές μονάδες των τιμολογίων τους με βάση την μηνιαία χρήση των υπηρεσιών. Στην συνέχεια παρείχε έναν απλό μηχανισμό μεταφοράς κεφαλαίων για την πληρωμή των τιμολογίων.

Αυτή η διαφάνεια στο κόστος έχει οδηγήσει σε αύξηση της χρέωσης των υπηρεσιών από 54% έως και 89%, με αυτά τα πρόσθετα κεφάλαια να χρησιμοποιούνται για την αύξηση των δαπανών για καινοτομίες. Αυτό προσθέτει όφελος για την επιχείρηση στο σύνολο και όχι σε επιμέρους επιχειρηματικές μονάδες.

3.2.4 Αδυναμίες για τις υπηρεσίες της EMC (Weaknesses)

Η εταιρία έχει μακρόχρονη εμπειρία στο χαμηλό επίπεδο της υποδομής ΥΝ και λιγότερο σε επίπεδο εφαρμογών και επιχειρησιακών υπηρεσιών. Ενδεχομένως οι χρήστες-πελάτες να ενδιαφέρονται λιγότερο να αποκτήσουν πρόσβαση στο διαχειριστικό περιβάλλον της υποδομής

που τους έχει δοθεί προκειμένου να ελέγχουν μόνοι τους παραμέτρους όπως ταχύτητα ή τροφοδοσία ρεύματος και περισσότερο για τις εφαρμογές και την προστασία των δεδομένων τους. Επιπλέον θα πρέπει να ενισχύσει τη μονάδα ασφάλειας που διαθέτει της RSA. Το 2010 παρουσιάστηκε ένα κενό ασφάλειας στον μηχανισμό RSA με αποτέλεσμα να αποχωρήσουν δέκα πελάτες.

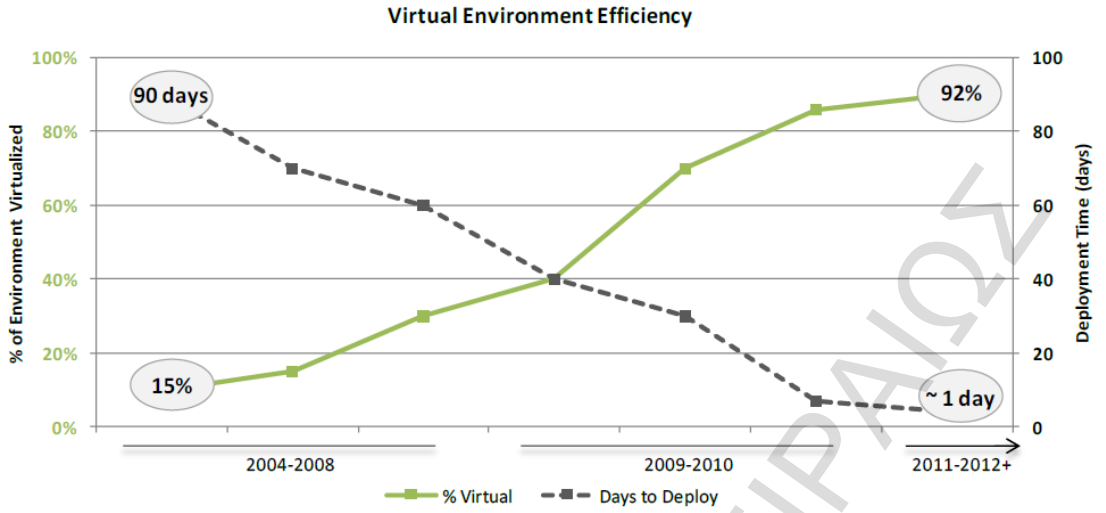
3.2.5 Ευκαιρίες για τις υπηρεσίες της EMC (Opportunities)

Δημιουργία επιχειρησιακών ευκολιών

Οι βελτιώσεις στην απόδοση επέτρεψαν στην EMC να ξοδεύει τα περισσότερα χρήματα από τον προϋπολογισμό της πληροφορικής σε νέες εφαρμογές και λειτουργίες, αντί απλά να συντηρεί τις υφιστάμενες και να τις κρατάει στην ζωή. Αν και πάντα θα πρέπει να ξοδεύονται χρήματα για την συντήρηση και την λειτουργία των υποδομών, ωστόσο η δυνατότητα να επενδύονται στρατηγικά χρήματα σε νέες δυνατότητες αλλάζει την εξίσωση και προχωράει μπροστά την επιχείρηση. Η αποτελεσματικότητα που κερδίζει η EMC βρίσκεται στην πραγματοποίηση καινοτομιών που οδηγούν σε ευκινησία αυξάνοντας την ανταγωνιστικότητά της και την κερδοφορία της (Garrett, et al., 2013).

Χρόνος παροχής υπηρεσιών

Πολλοί οργανισμοί δυσκολεύονται να προσαρμοστούν στις μεταβαλλόμενες επιχειρηματικές συνθήκες. Μια ιδιαίτερα χρονοβόρα διαδικασία προετοιμασίας για την παροχή υπηρεσιών ή προϊόντων είναι συχνά ένας βασικός αναστολέας. Για παράδειγμα εάν κάποιος θέλει να ξεκινήσει μια εφαρμογή για να αποκτήσει ανταγωνιστικό πλεονέκτημα, εάν περνούν οι εβδομάδες αναμονής χωρίς είναι έτοιμη ακόμα η εφαρμογή, τότε είναι δυνατόν να χαθεί το ανταγωνιστικό πλεονέκτημα. Το 2004 ο απαιτούμενος χρόνος για την προετοιμασία ενός διακομιστή ήταν 90 ημέρες. Κατά τα τελευταία 8 χρόνια, όπως δείχνει η Εικόνα 16, που ξεκίνησε να λαμβάνει χώρα το cloud computing και το virtualization οι χρόνοι έχουν μειωθεί. Την παρούσα χρονική συγκυρία το 92 % των διακομιστών είναι εικονικοί και ο χρόνος παροχής ενός καινούργιου διακομιστή είναι λιγότερος από μία ημέρα. Λόγω του virtualization τα τμήματα πληροφορικής (IT) μπορούν να ανταποκριθούν γρηγορότερα σε οποιεσδήποτε ανάγκες για επιχειρησιακές εφαρμογές.



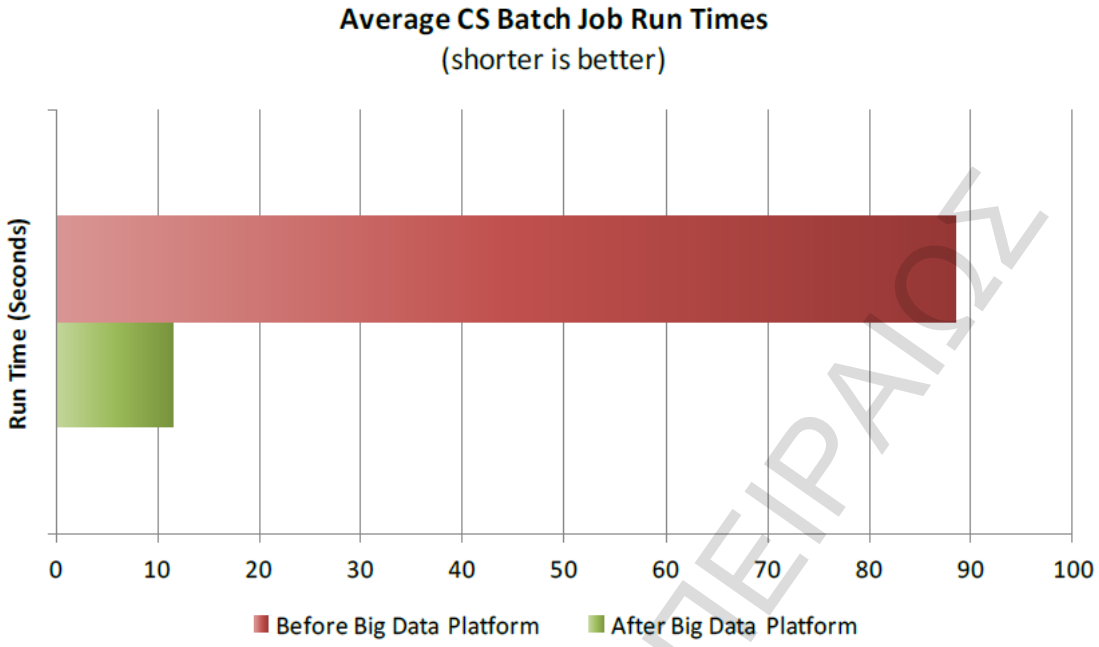
Εικόνα 16, Χρονικός ορίζοντας παροχής εικονικού περιβάλλοντος (Garrett, et al., 2013)

Big Data και βελτιωμένο Business Intelligence (BI)

Οι ευκολίες που παρέχονται από την EMC περιλαμβάνουν και τις ολοένα και γρηγορότερες απαντήσεις στις ερωτήσεις που τίθενται. Η υποδομή cloud της EMC επέτρεψε την αξιοποίηση της βάσης δεδομένων Greenplum, καθώς επίσης του Hadoop για αδόμητα δεδομένα και του SAS για analytics, για την δημιουργία μιας ευέλικτης και επεκτάσιμης Επιχειρησιακής Νοημοσύνης (Business Intelligence - BI) πλατφόρμας. Αυτή η πλατφόρμα παρέχει σαν υπηρεσία το BI και τα συνεργατικά εργαλεία ανάλυσης, καθώς και υπηρεσίες επιστημόνων για τα δεδομένα εάν και εφόσον απαιτούνται. Οι επιχειρήσεις έχουν κέρδη από τις καινούργιες δυνατότητες που τους παρέχει η πρόσβαση σε εργαλεία με προηγμένες δυνατότητες πρόβλεψης και λήψης αποφάσεων σε πραγματικό χρόνο.

Οι διευθυντές των επιχειρηματικών μονάδων της EMC εκτιμούν ιδιαίτερα αυτή την πλατφόρμα για «Big Data» καθώς τους επιτρέπει να βρουν περισσότερους τρόπους να αντιμετωπίσουν τους ανταγωνιστές τους και να διασφαλίσουν μια ποιοτικότερη εμπειρία χρήσης των πελατών τους. Με την αύξηση του όγκου δεδομένων, των τύπων τους και της πολυπλοκότητάς τους αυτές οι ενισχυμένες δυνατότητες για ανάλυση δεδομένων παρέχουν ανταγωνιστικό πλεονέκτημα στην εταιρεία. Για παράδειγμα η επιχειρηματική μονάδα του απευθείας μάρκετινγκ (direct marketing) χρησιμοποιεί την πλατφόρμα BI για προγνωστικά analytics και για την κατανόηση των 170 εκ. αλληλεπιδράσεων στα μέσα κοινωνικής δικτύωσης, το οποίο μεταφράζεται σε περίπου 130 TB δεδομένων. Η ικανότητα να αναλύσουν αυτά τα δεδομένα είναι ζωτικής σημασίας για το μάρκετινγκ.

Σαν παράδειγμα αναφέρεται ότι οι πλατφόρμες για «Big Data» μείωσαν τους χρόνους εκτέλεσης των αυτοματοποιημένων διαδικασιών για την υπηρεσία εξυπηρέτησης πελατών της EMC κατά 87%, γεγονός το οποίο επιτρέπει στην EMC την επιτάχυνση της ανάκτησης δεδομένων και την γρηγορότερη δημιουργία συμβάσεων.



Εικόνα 17, Η πλατφόρμα «Big Data» επιταχύνει τις αυτοματοποιημένες διαδικασίες (Garrett, et al., 2013)

Παροχή ποιοτικών υπηρεσιών

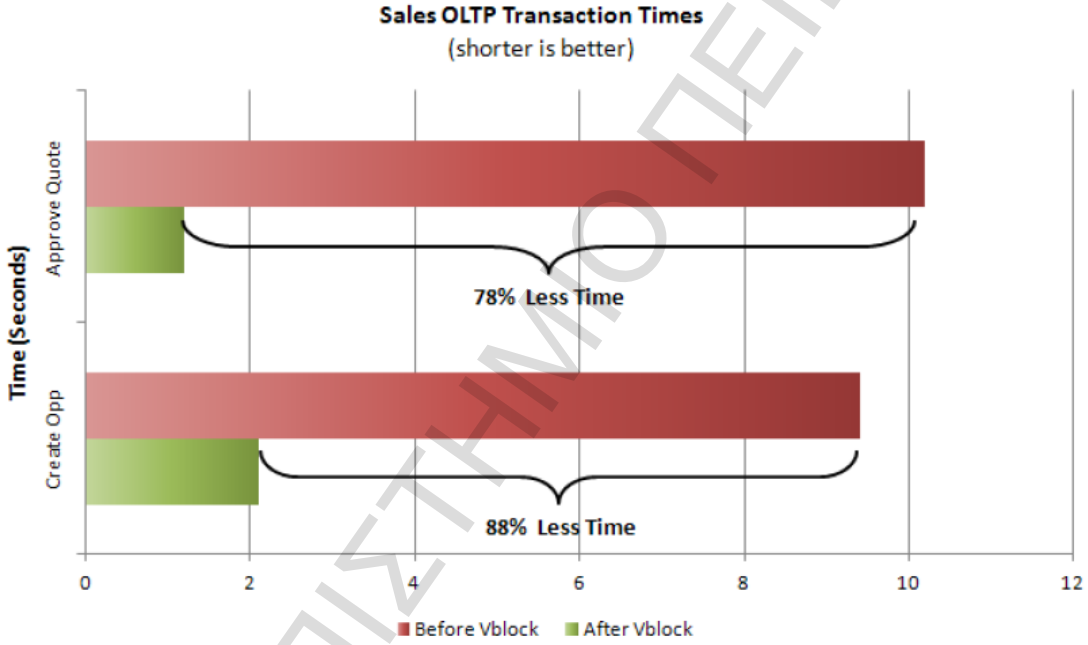
Πάντοτε υπήρξε στόχος της EMC (Garrett, et al., 2013) η παροχή υψηλής ποιότητας υπηρεσιών πληροφορικής, αλλά το ITaaS κάνει αυτό τον στόχο ακόμα σημαντικότερο. Η λειτουργία των τεχνολογιών πληροφορικής (IT) σαν επιχείρηση σημαίνει την παράδοση και την μέτρηση της ποιότητας των υπηρεσιών και της ικανοποίησης των πελατών. Το τμήμα πληροφορικής (IT) της EMC δεν θέλει οι επιχειρηματικές μονάδες να προμηθεύονται μονομερώς δημόσιες υπηρεσίες cloud, όπως κοινή χρήση αρχείων ή άλλες λύσεις βασισμένες στο cloud. Το νέο μοντέλο παράδοσης υπηρεσιών ITaaS προσφέρει την δυνατότητα στο τμήμα πληροφορικής (IT) της EMC να φέρει οποιοδήποτε «Shadow IT» πίσω στο «σπίτι». Τα τμήματα πληροφορικής (IT) αντιλαμβάνονται την πραγματικότητα, ανεξάρτητα από τις βελτιώσεις στο κόστος, την αποτελεσματικότητα, την ευελιξία, και την ποιότητας αν δηλαδή οι επιχειρηματικές μονάδες καταλαβαίνουν ότι τα εσωτερικά οργανωμένα τμήματα πληροφορικής (IT) είναι δυσκίνητα για να ικανοποιούν τις ανάγκες τους ή να δουλεύουν με αυτά, ότι αυτά θα συνεχίσουν να δουλεύουν γύρω από αυτά.

Εφόσον αυτό είναι ασυμβίβαστο με το μοντέλο χρηματοδότησης του τμήματος πληροφορικής (IT), τότε αυτές οι πρακτικές θα πρέπει να το αποθαρρύνουν. Για αυτό το σκοπό οι προσπάθειες για το ITaaS της EMC βοηθούν αυτές τις εταιρείες να μετατρέψουν την εικόνα τους από ένα σιλό συλλογής τεχνολογιών πληροφορικής σε εταιρείες παροχής λύσεων ως επιχειρηματικοί εταίροι. Η υπάρχουσα υποδομή το υποστηρίζει αυτό πλέον και οι προσπάθειες της EMC κατευθύνονται στο να γίνει ένας μεσίτης προστιθέμενης ποιοτικής αξίας στην επιχείρηση. Επιπλέον, δημιουργούνται επίπεδα αυτοματισμού στο ιδιωτικό cloud προκειμένου να βελτιστοποιηθεί η παραγωγή των τμημάτων πληροφορικής (IT) για τις καταναλωτικές επιχειρήσεις. Η αυτοματοποίηση θα επιτρέψει την αυτό-εξυπηρέτηση, την γρήγορη

τροφοδότηση και την παροχή υπηρεσιών που ζητούν οι εσωτερικοί πελάτες. Αυτό είναι μέρος του μετασχηματισμού της EMC, μετατρέποντας την σε μια ανταγωνιστική εταιρεία παροχής ολοκληρωμένων υπηρεσιών πληροφορικής.

Ικανοποίηση πελατών

Η βελτίωση της αποτελεσματικότητας μπορεί να επηρεάσει τους τελικούς χρήστες με πολύ συγκεκριμένους τρόπους επιτρέποντας την αύξηση της παραγωγικότητας τους. Μια ματιά στον πραγματικό κόσμο των επιχειρήσεων αποδεικνύει αυτή την επισήμανση. Μια αποδοτική αρχιτεκτονική βασισμένη στο cloud επιτρέπει την οργάνωση των πωλήσεων για συρρικνωθεί ο χρόνος των OLTP συναλλαγών για εργασίες όπως ενεργοποίηση και αποθήκευση καινούργιων ρυθμίσεων, δημιουργία ευκαιριών και έγκριση προσφορών (Εικόνα 18). Αυτά είναι κέρδη σε πραγματικό χρόνο που επιταχύνουν την παραγωγικότητα και βελτιώνουν την ικανοποίηση των πελατών.



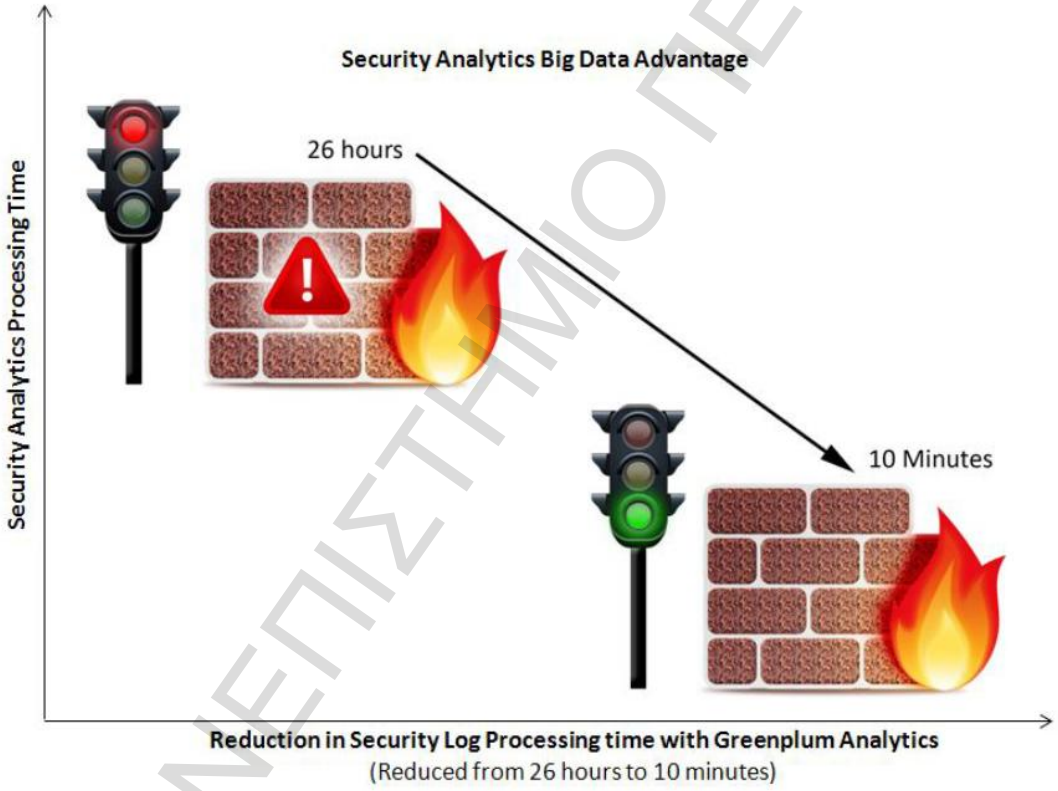
Εικόνα 18, Χρόνος OLTP συναλλαγών για τις πωλήσεις (Garrett, et al., 2013)

«Ασφαλίζοντας» το cloud

Η EMC γνωρίζοντας τις πολύ διαφορετικές ανάγκες ασφάλειας σε ένα περιβάλλον βασισμένο στο cloud, ανέλαβε να προάγει την ασφάλεια σε επόμενο επίπεδο. Η διαχείριση όλων των κέντρων δεδομένων είναι κεντρικοποιημένη στο Global Command Center με την χρήση εργαλείων διαχείρισης υποδομών τελευταίας τεχνολογίας των EMC και VMware. Επιπλέον, ένα Critical Incident Response Center (CIRC) παρακολουθεί με έξυπνο τρόπο τις υποδομές για κυβερνό-επιθέσεις. Χρησιμοποιούνται προηγμένα εργαλεία και analytics από την RSA technologies, καθώς επίσης και εξειδικευμένους αναλυτές ασφάλειας, για να προλάβουν παραβιάσεις και να αποκαταστήσουν βλάβες, εάν και όποτε αυτό απαιτείται. Με την νέα αρχιτεκτονική αξιοποιώντας μια βάση δεδομένων Greenplum και άλλες εφαρμογές η CIRC

μπορεί να ελέγξει τεράστιες ποσότητες δεδομένων, όπως 100 GB καθημερνών logs από έναν proxy, σε δέκα λεπτά για την πρόληψη παραβιάσεων ασφάλειας. Πριν από την θέση σε παραγωγή της καινούργιας αρχιτεκτονικής αυτός ο τύπος ανάλυσης ήταν σχεδόν αδύνατος. Οι προσπάθειες για να γίνουν τέτοιες εργασίες έπαιρναν 26 ώρες και συχνά αποτύγχαναν λόγω ανεπαρκούς μνήμης (Εικόνα 19).

Σήμερα η ασφάλεια έχει αρχίσει να κατασκευάζεται μέσα στην υποδομή της EMC. Στην αρχή η EMC είχε επικεντρωθεί στην κατανόηση των κινδύνων και στον έλεγχο του περιβάλλοντος με την διαχείριση των προσβάσεων, αλλά με την πάροδο του χρόνου εικονικά εργαλεία με ενσωματωμένους ελέγχους έγιναν μέρος της εικόνας. Η ωρίμανση της βασικής υποδομής έφερε μαζί τις επαναλαμβανόμενες, επεκτάσιμες και μετρήσιμες υλοποιήσεις ασφάλειας. Μαζί με αυτές τις υλοποιήσεις υπάρχει μεγαλύτερη προβλεψιμότητα και καλύτερη κατανόηση των συμπεριφορών με αποτέλεσμα καλύτερη ασφάλεια. Η ασφάλεια υλοποιείται τόσο στα προϊόντα όσο και στις υπηρεσίες καθιστώντας ποιο εύκολη και αποτελεσματική την προστασία από απειλές.



Εικόνα 19, Ανάλυση συμβάντων ασφάλειας (Garrett, et al., 2013)

Αυτό είναι ζωτικής σημασίες όταν η υποδομή γίνεται ρευστή σε ένα περιβάλλον cloud, όπου η διατήρηση του ελέγχου της υποδομής γίνεται δύσκολη υπόθεση. Τα καινούργια συστήματα μπορούν εύκολα να παραμετροποιηθούν και να μεταφερθούν, η συνεργατικότητα και τα μέσα κοινωνικής δικτύωσης είναι συνήθεις επιχειρηματικές δραστηριότητες και οι χρήστες έχουν πρόσβαση στις εφαρμογές από πολλές τοποθεσίες, τερματικές συσκευές και δίκτυα. Όταν η πολιτική ασφάλειας εξακολουθεί να εφαρμόζεται από το λειτουργικό σύστημα και τις εφαρμογές καταντάει να είναι περίπλοκη και λιγότερο αποτελεσματική. Η EMC εργάζεται για να προωθήσει την εφαρμογή των πολιτικών ασφάλειας από τους τομείς του virtualization, των

δικτύων και της αποθήκευσης. Αυτό θα επιτρέψει στις εφαρμογές να μετακινούνται μεταξύ των διακομιστών και των κέντρων δεδομένων, διατηρώντας όμως την ικανότητα να μετρηθούν και να υποβάλλουν αναφορές έτσι ώστε να μπορούν να ελέγχονται και να διαχειρίζονται.

Η EMC θεωρεί ότι οι άνθρωποι είναι η καινούργια παράμετρος λόγω της μεγαλύτερης κινητικότητάς τους και της ικανότητας για πρόσβαση από έναν αυξανόμενο αριθμό τερματικών συσκευών. Αυτό καθιστά δύσκολη την παροχή καλής εμπειρίας στον χρήστη, εξασφαλίζοντας παράλληλα τον εξωτερικό έλεγχο πρόσβασης. Η διαχείριση της προστασίας των δεδομένων, των αντιικών προγραμμάτων, και άλλων παρόμοιων με βάση την εκάστοτε συσκευή είναι σχεδόν αδύνατο, ιδιαίτερα για όσες συσκευές δεν έχουν δοθεί από το τμήμα πληροφορικής. Αυτή η αδυναμία αφήνει μεγάλα τρωτά σημεία. Η εταιρεία εργάζεται στην υλοποίηση εφαρμογών ενήμερων για το cloud σε ασφαλή containers που μπορούν να τρέξουν σε οποιαδήποτε σημείο του EMC hybrid cloud, βάσει προκαθορισμένων πολιτικών συμμόρφωσης και διακυβέρνησης που θα ενοποιούνται με τον container.

Για παράδειγμα, οι προγραμματιστές προσθέτουν δυνατότητες για την πρόληψη απώλειας δεδομένων στα API και κάνουν ανάλυση για κακόβουλα αρχεία όταν ένα αρχείο λαμβάνεται στην συσκευή. Αυτό το έργο απαιτεί μεγάλη συνεργασία μεταξύ των ομάδων για να εξασφαλιστεί η ασφάλεια ενώ παράλληλα θα βελτιώνεται η χρησιμότητα, η απόδοση και η αξιοπιστία. Αυτό θα απαλλάξει τα εκάστοτε τμήματα πληροφορικής από την υποχρέωση παροχής περιμετρικής ασφάλειας και θα επιτρέψει στους τελικούς χρήστες να μπορούν να επιλέγουν περισσότερες διαφορετικές τερματικές συσκευές.

3.2.6 Απειλές για τις υπηρεσίες της EMC (Threats)

Η κυριότερη απειλή για την EMC είναι η παγκόσμια οικονομική κρίση καθώς αυτή επηρεάζει τις επενδύσεις στον τομέα της πληροφορικής. Στο διάστημα από το 2008 οι εταιρίες αναζητούν τρόπους μείωσης των δαπανών, αύξησης της αποδοτικότητας και της προσφοράς προϊόντων και υπηρεσιών στους πελάτες τους χωρίς να αυξήσουν σημαντικά τις τιμές. Όταν οι εταιρίες δεν μπορούν να πετύχουν καινοτομίες και στόχους αποδοτικότητας στο εσωτερικό τους τότε καταφεύγουν σε εξαγορές διαφορετικά διακινδυνεύουν να χάσουν μερίδιο της αγοράς από τον ανταγωνισμό. Καθώς η EMC συγκεντρώνει το 30% από την Ευρώπη, την Αφρική και τη Μέση Ανατολή μελλοντικά έσοδα σε αυτές τις περιοχές μπορεί να περικοπούν εξαιτίας της παραμένουσας οικονομικής κρίσης στην Ευρώπη.

Άλλη μία απειλή για την EMC αποτελούν οι δικαστικές διαμάχες για πατέντες, παραβίαση ασφάλειας δεδομένων που είχαν αποθηκευτεί σε χώρους της και άλλα. Εξαιτίας του υψηλού ανταγωνισμού και των επενδύσεων της εταιρίας σε έρευνα και ανάπτυξη οι δικαστικές διαμάχες προκειμένου να υπερασπιστεί πατέντες της μπορεί να αποδειχθούν αρκετά δαπανηρές και να επηρεάσουν το ευρύτερο επενδυτικό της πλάνο.

3.4 AMAZON EC2- PUBLIC CLOUD

3.4.1 Ιστορική Αναδρομή

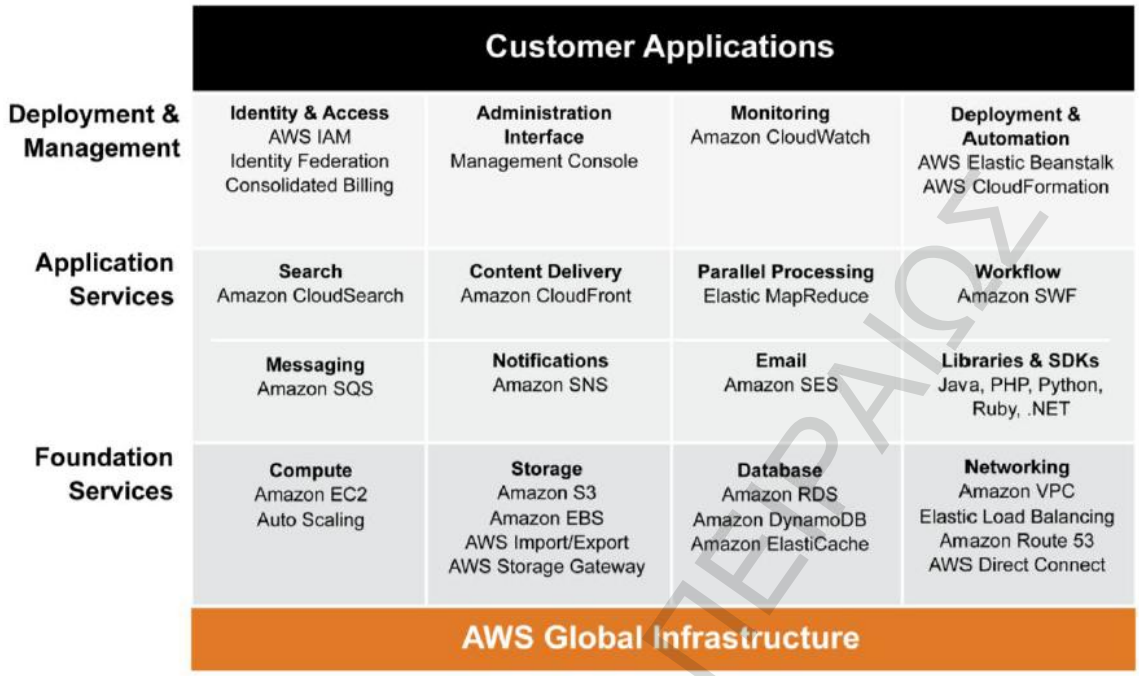
Η Amazon ιδρύθηκε το 1994 και ξεκίνησε την παράδοση υπηρεσιών στο ΥΝ το 2006. Η εταιρεία είναι ένα από τα νεώτερα μέλη του Fortune 100 (το Amazon.com πρωτοεμφανίστηκε στο Fortune 100 το 2010). Τα Amazon Web Services (AWS) είναι μία από τις παλαιότερες πλατφόρμες παροχής υπηρεσιών cloud της βιομηχανίας (τα AWS ξεκίνησαν να προσφέρουν

υπηρεσίες τον Μάρτιο του 2006). Παρά το γεγονός ότι το YN δεν ήταν μέσα στον αρχικό σχεδιασμό της Amazon, οι απαιτήσεις για την δημιουργία μιας αξιόπιστης, ασφαλούς και επεκτάσιμης υποδομής ηλεκτρονικού εμπορίου σε συνδυασμό με την επιθυμία για χαμηλότερες τιμές στους καταναλωτές, οδήγησαν την Amazon να επικεντρωθεί στη μείωση του κόστους της πληροφοριακής (IT) της υποδομής. Η εστίαση της Amazon στην δημιουργία μια αρχιτεκτονικής εστιασμένης στις υπηρεσίες έθεσε την εταιρεία στον δρόμο για την παροχή υπηρεσιών πληροφορικής.

Οι τρέχουσες υπηρεσίες της Amazon για την υποστήριξη της φιλοξενίας εφαρμογών, της διαχείρισης εφαρμογών, της ασφάλειας, της διαχείρισης δεδομένων, των σχεσιακών βάσεων δεδομένων, των μη σχεσιακών βάσεων δεδομένων, των πληρωμών, των τιμολογήσεων, της αποθήκευσης, της δικτύωσης, της διαχείρισης περιεχομένου, της ανάπτυξης, της θέσης σε παραγωγή και των ροών εργασίας έρχονται κάτω από την αιγίδα των AWS. Αυτό το εύρος και βάθος των AWS επέτρεψε στα AWS να γίνουν ο ηγέτης στο cloud computing. Ενώ στην αρχή πολλές επιχειρήσεις είχαν θεωρήσει ότι τα AWS είναι μια υποδομή παροχής υπηρεσιών, αυτή η αντίληψη έχει επεκταθεί τα τελευταία χρόνια υπό το πρίσμα των υπηρεσιών εκτέλεσης εφαρμογών σε παραγωγικό περιβάλλον που παρέχει η AWS ως πλατφόρμα ανάπτυξης εφαρμογών (Perry, R., & Hendrick, S., 2012).

3.4.2 Amazon Web Services

Στα τέλη της δεκαετίας του 1990 και στις αρχές της δεκαετίας του 2000 η Amazon αναδυόταν ως η κορυφαία εταιρεία στο χώρο του ηλεκτρονικού εμπορίου (Perry, R., & Hendrick, S., 2012). Οι εσωτερικές επιχειρηματικές απαιτήσεις επέβαλλαν στην Amazon να χτίσει μια υποδομή εφαρμογών που θα υποστήριζε μαζική κλίμακα και αξιοπιστία στους ακόλουθους τομείς: υπολογισμοί, παράλληλη επεξεργασία, αποθήκευση, διαχείριση περιεχομένου, διαχείριση δεδομένων (σχεσιακές και μη σχεσιακές βάσεις δεδομένων), επεξεργασία συναλλαγών, ανταλλαγή μηνυμάτων, ουρές μηνυμάτων, πληρωμές, ασφάλεια, παρακολούθηση και διαχείριση. Οι αντικρουόμενοι και συχνά ανταγωνιστικοί στόχοι που είχαν τεθεί για τις τεχνολογίες πληροφορικής που έπρεπε να χρησιμοποιηθούν και περιελάμβαναν την επεκτασιμότητα και τον έλεγχο του κόστους κατεύθυναν την Amazon στο δρόμο των υπηρεσιών. Οι υπηρεσίες που δημιουργήθηκαν μέσα σε αυτή την διαδικασία μετασχηματισμού της πληροφοριακής υποδομής έθεσαν τα οριστικά θεμέλια για τα AWS. Στην (Perry, R., & Hendrick, S., 2012) παρουσιάζονται οι βασικές υπηρεσίες που παρέχονται από τα AWS.



Εικόνα 20: Amazon Web Services (Perry, R., & Hendrick, S., 2012)

Ο προσανατολισμός της Amazon στην ελάπτωση του κόστους από τις λειτουργίες σε μεγάλη κλίμακας για το ηλεκτρονικό εμπόριο, την οδήγησε προς τον προσανατολισμό στις υπηρεσίες και στην έκθεση όλων των πόρων της ως επεκτάσιμες και αναλώσιμες υπηρεσίες. Αυτή η κίνηση της Amazon επίσης εξασφάλισε ότι η κουλτούρα ανάπτυξης εφαρμογών θα είναι ευθυγραμμισμένη με τις σύγχρονες τεχνικές ανάπτυξης λογισμικού και αυτό είχε ως αποτέλεσμα μία πλατφόρμα που ήταν ευέλικτη, ευκίνητη και επεκτάσιμη. Η πλατφόρμα που προέκυψε, το AWS API, ήταν αντικείμενο συγχρόνως θαυμασμού και φθόνου για όλο τον κλάδο της πληροφορικής. Από την σκοπιά του πελάτη των AWS αυτή το API του δίνει την δυνατότητα να αναπτύξει ποιο εύκολα εφαρμογές που χρησιμοποιούν AWS, ποιο εύκολα να θέσουν σε παραγωγή εφαρμογές που προϋπήρχαν στα AWS και ποιο εύκολα να δημιουργήσουν υβριδικές εφαρμογές που διαμοιράζονται μεταξύ των AWS και ιδιωτικών κέντρων δεδομένων.

3.4.3 Πλεονεκτήματα των υπηρεσιών της Amazon (Strengths)

Στις αρχές του 2012 ερωτήθηκαν από την εταιρία στατιστικών αναλύσεων και μελετών IDC[21] (Perry, R., & Hendrick, S., 2012) 12 οργανισμοί που είχαν αναπτύξει εφαρμογές στις υπηρεσίες υποδομής cloud της Amazon. Ο σκοπός της ανάλυσης ήταν να κατανοήσουν τις οικονομικές επιπτώσεις των υπηρεσιών υποδομής cloud της Amazon με την πάροδο του χρόνου, πέρα από τα καλά τεκμηριωμένα οφέλη της μείωσης των κεφαλαιακών δαπανών και των λειτουργικών εξόδων. Ειδικότερα τέθηκε ως στόχος σε αυτή τη μελέτη η κατανόηση των μακροπρόθεσμων οικονομικών επιπτώσεων της μετακίνησης του φόρτου εργασίας στις υπηρεσίες υποδομής cloud της Amazon, το αντίκτυπο από την μετακίνηση των εφαρμογών στην παραγωγικότητα των προγραμματιστών και στην επιχειρηματική ευελιξία, και τις νέες ευκαιρίες που θα

[21] International Data Corporation

μπορούσαν να εκμεταλλευτούν οι επιχειρήσεις με την μετακίνηση πόρων στις υπηρεσίες υποδομής cloud της Amazon. Οι επιχειρήσεις που έλαβαν μέρος στην έρευνα κυμαίνονται από μικρομεσαίες επιχειρήσεις έως και επιχειρήσεις με 160000 εργαζόμενους και χρησιμοποιούσαν τα AWS από 7 μήνες έως και 3,5 χρόνια.

Συνολικά όλοι οι οργανισμοί που συμμετείχαν στην έρευνα (και χρησιμοποιούσαν AWS) ανέφεραν ετήσια οικονομικά οφέλη κατά μέσο όρο 518000 $ ανά εφαρμογή. Τα ποιο σημαντικά οφέλη προέρχονται από την μετάβαση των εφαρμογών στην υποδομή AWS λόγω χαμηλότερων κεφαλαιακών αναγκών και λειτουργικών δαπανών. Αυτή η μείωση των κεφαλαιακών δαπανών και των λειτουργικών εξόδων αντιπροσωπεύουν πάνω από το 50% των συνολικών ωφελειών που προέκυψαν.

Η IDC παρατήρησε ότι αυξήθηκε η παραγωγικότητα των προγραμματιστών χρησιμοποιώντας τις υπηρεσίες υποδομής cloud της Amazon σε σχέση με προηγούμενες υλοποιήσεις. Σε όλες τις εταιρείες που έλαβαν μέρος στην έρευνα παρατηρήθηκε αυξημένη παραγωγικότητα των προγραμματιστών σε όλες τις βασικές δραστηριότητες του κύκλου ζωής ανάπτυξης λογισμικού, το οποίο ήταν ένα άμεσο αποτέλεσμα των εκτεταμένων υπηρεσιών ανάπτυξης και εκτέλεσης που παρέχονται από τις υπηρεσίες υποδομής YN της Amazon. Η αύξηση της παραγωγικότητας των προγραμματιστών και του προσωπικού που απασχολείται με τεχνολογίες πληροφορικής (IT) αντιπροσώπευε σχεδόν το 30% των συνολικών οικονομικών ωφελειών. Τα υπόλοιπα οφέλη προέκυψαν από την ευελιξία και την ευκινησία των υπηρεσιών υποδομής cloud της Amazon, οι οποίες κάνουν ευκολότερη την δοκιμή καινούργιων επιχειρηματικών μοντέλων, την υποστήριξη εφαρμογών που δημιουργούν έσοδα και παρέχουν ποιο αξιόπιστες υπηρεσίες στους τελικούς χρήστες. Αυτά τα οφέλη περιλαμβάνουν:

- Τα οφέλη αυξάνονται με την πάροδο του χρόνου. Υπάρχει μια σαφής συσχέτιση μεταξύ της διάρκειας του χρόνου που χρησιμοποιούν οι πελάτες τις υπηρεσίες υποδομής YN της Amazon και της απόδοσή τους. Στους 36 μήνες χρήσης των υπηρεσιών οι επιχειρήσεις έχουν κέρδη 3,50 $ για κάθε 1 $ που επενδύουν στα AWS. Μετά από 60 μήνες χρήσης των υπηρεσιών οι επιχειρήσεις έχουν κέρδη 8,40 $ για κάθε 1 $ που επενδύουν στα AWS. Αυτή η σχέση μεταξύ του χρονικού διαστήματος χρήσης των υπηρεσιών υποδομής cloud της Amazon και την αυξανόμενων κερδών των πελατών οφείλεται στο ότι οι πελάτες αξιοποιούν το πιο βελτιστοποιημένο περιβάλλον για να δημιουργήσουν περισσότερες εφαρμογές κατά μήκος μιας καμπύλης μάθησης.
- Το συνολικό κόστος ιδιοκτησίας (Total Cost of Ownership – TCO) για πέντε έτη ανάπτυξης, θέσης σε παραγωγή και διαχείρισης κρίσιμων εφαρμογών στην υποδομή cloud της Amazon αντιπροσωπεύει μια εξοικονόμηση κατά 70% σε σύγκριση με την ανάπτυξη χρησιμοποιώντας ίδιους πόρους σε ιδιόκτητα ή φιλοξενούμενα περιβάλλοντα. Τα ευρήματα έδειξαν απόσβεση της επένδυσης (Return of Investment –ROI) της τάξης του 626% σε διάστημα 5 ετών.
- Οι τελικοί χρήστες επωφελούνται από τις λιγότερες διακοπές στην εξυπηρέτησή τους και την ταχύτερη ανάκαμψη των υπηρεσιών υποδομής της Amazon, μειώνοντας το χρόνο εκτός λειτουργίας κατά 72% και βελτιώνοντας την διαθεσιμότητα των εφαρμογών κατά ένα μέσο όρο 3,9 ωρών ανά χρήστη ανά έτος.
- Η παραγωγικότητα του προσωπικού που απασχολείται με τεχνολογίες πληροφορικής αυξήθηκε κατά 52%. Αυτό έχει σαν άμεση συνέπεια το προσωπικό να είναι σε θέση να βελτιώσει την υποστήριξη κρίσιμων λειτουργιών. Οι υπηρεσίες υποδομής της Amazon έχουν άμεσο αντίκτυπο στην ανάπτυξη και θέση σε λειτουργία εφαρμογών μειώνοντας το συνολικό χρόνο του έργου κατά 80%.

3.4.4 Αδυναμίες της Υποδομής (Weaknesses)

Οι κυριότερες αδυναμίες της υποδομής των υπηρεσιών της Amazon σχετίζονται με το γεγονός ότι απευθύνεται σε καταναλωτές που ενδιαφέρονται για τον δημόσιο χαρακτήρα του ΥΝ. Κατά καιρούς έχουν παρουσιαστεί διακοπές της λειτουργίας του (ακόμη και για ημέρες) ενώ καταναλωτές που δεν διαθέτουν προγραμματιστικές δυνατότητες ενδεχομένως να θεωρούν πολύπλοκη τη διαδικασία ανάπτυξης προγραμμάτων κάνοντας χρήση των AWS.

Οι (Gruschka, N. ; NEC Eur. Ltd., Heidelberg, Germany ; Jensen, M 2010) καταγράψανε το 2008 μία ευπάθεια στον ελεγκτή νέφους του EC2 η οποία μπορούσε να προκαλέσει επίθεση με σκοπό την τροποποίηση ή πλαστογράφηση ενός ψηφιακά υπογεγραμμένου μηνύματος (Signature Wrapping Attack). Μέσω αυτής της ευπάθειας ο κακόβουλος χρήστης μπορούσε να εκτελέσει οποιεσδήποτε εντολές εκ μέρους ενός εγγεγραμμένου χρήστη έχοντας σαν αντίκτυπο είτε την άρνηση υπηρεσίας ή την υπερχρέωση του λογαριασμού του χρήστη. Η συγκεκριμένη ευπάθεια μπορούσε να αντιστοιχηθεί σε δύο επιφάνειες επιθέσεων:

- επίθεση της υποδομής του ΥΝ προς ένα χρήστη
- επίθεση μίας υπηρεσίας προς την υποδομή του ΥΝ

Οι (Gruschka, N. ; NEC Eur. Ltd., Heidelberg, Germany ; Jensen, M 2010) διαπίστωσαν ότι μπορούσαν να χειριστούν την πρώτη περίπτωση επιθέσεων για τη δημιουργία αντιγράφου μίας υπηρεσίας στο ίδιο υλικό όπου λειτουργεί και κάποιο άλλο αντίγραφο της υπηρεσίας του θύματος-χρήστη. Στη συνέχεια, χρησιμοποιώντας την κακόβουλη υπηρεσία, μπορούν να προσβάλλουν τη διεπαφή «ΥΝ-υπηρεσία» για να αποκτήσουν πληροφορίες σχετικά με το υποσύστημα-επόπτη και το υλικό της υποδομής. Εναλλακτικά μπορούν να εκμεταλλευτούν μία επίθεση κατά της διεπαφής «υπηρεσία-ΥΝ» προκειμένου προκειμένου να εκτελέσουν επιθέσεις από υπηρεσία σε υπηρεσία.

3.4.5 Προκλήσεις και Ευκαιρίες (Opportunities)

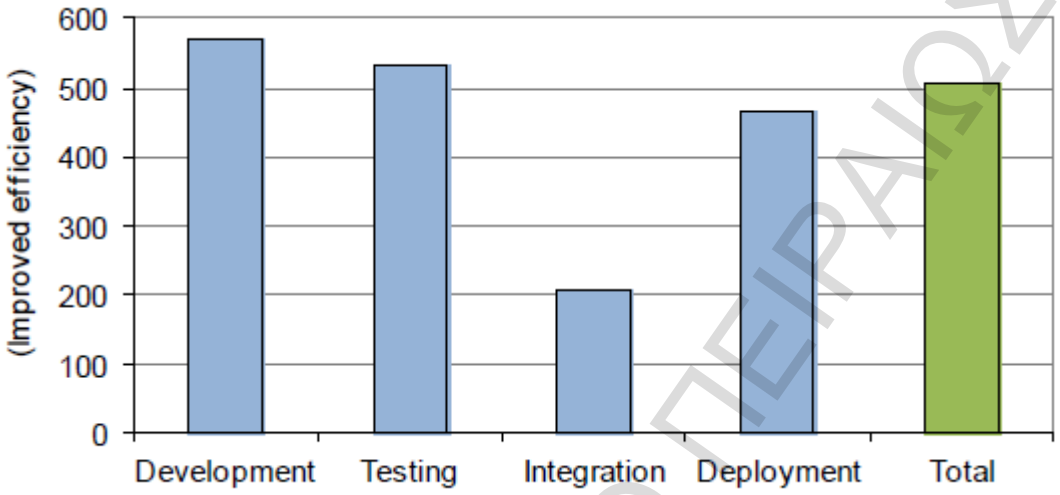
3.4.5.1 Προκλήσεις

<u>Ενσωμάτωση παλιών συστημάτων</u>

Η αλλαγή του χώρου φιλοξενίας των εφαρμογών μπορεί να απαιτήσει κάποιου είδους αναδιοργάνωση, ειδικά εάν η πλευρά του πελάτη της εφαρμογής απαιτεί έναν συγκεκριμένο χρόνο εκτέλεσης και / ή η εφαρμογή δεν αξιοποιεί την τεχνολογία των Web Services για την επικοινωνία μεταξύ του πελάτη και του διακομιστή. Η επικοινωνία ή η ενσωμάτωση παλιών συστημάτων (legacy systems) που τρέχουν σε διακομιστές είναι πιο εύκολη γιατί ο κώδικας μπορεί ποιο εύκολα να ενσωματωθεί χωρίς να απαιτηθεί ο προγραμματισμός εκ νέου τμημάτων της εφαρμογής. Κατά συνέπεια η ενσωμάτωση εξακολουθεί να αποτελεί πρόκληση, γιατί η αρχιτεκτονική και η προσαρμοστικότητα των παλιών εφαρμογών είναι εξαιρετικά μεταβλητή.

Μια ανάλυση που έχει γίνει από την IDC (Perry, R., & Hendrick, S., 2012) φαίνεται να επιβεβαιώνει αυτή την άποψη. Η Εικόνα 21 δείχνει μια αύξηση κατά 200% στην παραγωγικότητα των προγραμματιστών στις ενέργειες ενσωμάτωσης εφαρμογών, ενώ οι ενέργειες που σχετίζονται με την ανάπτυξη, τον έλεγχο και την θέση σε παραγωγή δείχνουν αύξηση στην παραγωγικότητα κατά 500%.

Τα AWS εξακολουθούν να βρίσκονται σε ευνοϊκότερη θέση σε σύγκριση με άλλες εναλλακτικές όσον αφορά την ολοκλήρωση και το πακετάρισμα των εφαρμογών λόγω των ευρύτερων συνόλων βιβλιοθηκών ανάπτυξης εφαρμογών (APIs) που υποστηρίζονται από τα AWS. Επίσης, μειώνουν την ποσότητα του κώδικα που είναι αναγκαίος για την αντιμετώπιση των πιο δύσκολων εργασιών ολοκλήρωσης.



Εικόνα 21: **Σύγκριση της αποτελεσματικότητας των προγραμματιστών χρησιμοποιώντας και ιδιόκτητες εναλλακτικές Invalid source specified.**

Επέκταση του κύκλου ζωής ανάπτυξης λογισμικού

Τα AWS έχουν ήδη εμφυσήσει σημαντική λειτουργικότητα σε όλους τους σημαντικούς τομείς της ανάπτυξης εφαρμογών και θέσης τους στην παραγωγή, συμπεριλαμβανομένων των υπηρεσιών εφαρμογών, δικτύωσης βάσεων δεδομένων, σχεσιακών και μη σχεσιακών βάσεων δεδομένων, ταυτοποίησης και πρόσβασης, διανομή περιεχομένου και θέσης σε παραγωγή. Όπως τα AWS χτίζουν την πλατφόρμα τους, έτσι και οι επιχειρήσεις θα θελήσουν να αναπτύξουν και να θέσουν σε παραγωγή πιο σύνθετες εφαρμογές. Αυτό θέτει ένα ζήτημα σχετικά με το πως θα γίνει η διαχείριση του κύκλου ζωής των εφαρμογών (Application Life-cycle Management, ALM).

Το ALM περιλαμβάνει εργαλεία που υποστηρίζουν τον πλήρη κύκλο ζωής μιας εφαρμογής, συμπεριλαμβανομένων των απαιτήσεων, της ομαδικής ανάπτυξης, των εκδόσεων, της διασφάλισης της ποιότητας της εφαρμογής, της διαχείριση του έργου, την συνεχή ενσωμάτωση και διαχείριση των αλλαγών, την διαχείριση της δημιουργίας του λογισμικού και την παρακολούθηση των ελαττωμάτων. Ενώ υπάρχουν εργαλεία ανοικτού κώδικα που υποστηρίζουν ορισμένες από τις δραστηριότητες και οι βιβλιοθήκες των AWS επιτρέπουν την ενοποίηση μερικών από τα κορυφαία σημερινά εργαλεία ALM, παραμένει πρόκληση η παροχή και η διασύνδεση αυτών των δυνατοτήτων σε όλα τα υβριδικά περιβάλλοντα.

Επίσης αναγνωρίζεται (Perry, R., & Hendrick, S., 2012) ότι όσο τα AWS ωριμάζουν, τόσο οι πελάτες θα κοιτάζουν ολοένα και αυξανόμενα προς τα AWS για να ευθυγραμμιστούν με τα κορυφαία εργαλεία του κύκλου ζωής και για να παρέχουν προγραμματιστικές διεπαφές για την καλύτερη ενσωμάτωση και θέσης σε παραγωγή των τρεχόντων δραστηριοτήτων με την

ανάπτυξη εφαρμογών. Η πολυπλοκότητα της ανάπτυξης εφαρμογών απαιτεί υψηλότερα επίπεδα υιοθέτησης των ALM. Η ανάγκη για μια πιο ολοκληρωμένη προσέγγιση των ALM δημιουργεί μια σημαντική ευκαιρία για τα AWS και θα ανυψώσουν την προοπτική τους στις μικρομεσαίες επιχειρήσεις που επιδιώκουν όλο και περισσότερο να ενσωματώσουν τις σχετιζόμενες με τις τεχνολογίες πληροφορικής δραστηριότητές τους που εκτελούνται σε ιδιόκτητες εγκαταστάσεις σε δημόσια clouds.

3.4.5.2 Ευκαιρίες

Τα AWS έχουν ένα εξαιρετικό ιστορικό σχετικά με την διαθεσιμότητα των υπηρεσιών που παρέχουν. Ωστόσο, είναι αναπόφευκτη η διακοπή παροχής υπηρεσιών ανεξάρτητα από το εάν οι εφαρμογές έχουν αναπτυχθεί σε ιδιόκτητες εγκαταστάσεις, στα AWS ή οπουδήποτε αλλού. Για να μεγιστοποιηθούν οι δυνατότητες των υλοποιήσεων σε cloud computing οι πελάτες θα πρέπει να αξιολογήσουν την αρχιτεκτονική των εφαρμογών του. Αν η διαθεσιμότητα των εφαρμογών είναι σημαντική για τις επιχειρήσεις η IDC (Perry, R., & Hendrick, S., 2012) προτείνει στις επιχειρήσεις να προσαρμόζουν την αρχιτεκτονική των εφαρμογών τους με βάση τις ζώνες διαθεσιμότητας των AWS είτε με παθητικούς είτε με ενεργητικούς τρόπους ανάλογα με το απαιτούμενο επίπεδο διαθεσιμότητας. Αυτό το είδος των αρχιτεκτονικών αποφάσεων είναι απλές παράμετροι που πρέπει να τεθούν στα AWS και είναι εύκολο να υλοποιηθούν. Πολλές εταιρείες παροχής υπηρεσιών πληροφορικής αποτυγχάνουν να εκτιμήσουν το επίπεδο της πολυπλοκότητας που παρέχουν πολλές υπηρεσίες cloud, συμπεριλαμβανομένων των AWS, και πολύ συχνά προσεγγίζουν τις αποφάσεις εγκατάστασης χωρίς να έχουν κατανοήσει πλήρως πόσο αξιόπιστες και διαθέσιμες θέλουν να είναι οι εφαρμογές τους, οδηγώντας σε αδικαιολόγητη αύξηση του λειτουργικού κόστους.

Καθώς οι επιχειρήσεις εξετάζουν τις επιλογές που προσφέρουν τα AWS γύρω από την ανάπτυξη των εφαρμογών, αυτή είναι και η κατάλληλη στιγμή να εξετάσουν πώς θα αυξηθούν οι δυνατότητες των υπό ανάπτυξη εφαρμογών. Τα AMIS (Amazon Machine Images) είναι διαθέσιμα σαν στιγμιότυπα μετά από αίτηση, σαν δεσμευμένα στιγμιότυπα και σαν επιτόπου στιγμιότυπα. Ως εκ' τούτου, η επιλογή του τρόπου ανάπτυξης και αναβάθμισης έχει σημαντική επίδραση στην διαθεσιμότητα και το κόστος των εφαρμογών. Η IDC (Perry, R., & Hendrick, S., 2012) συμβουλεύει τις επιχειρήσεις να είναι σίγουρες ότι έχουν κατανοήσει το πλήρες φάσμα των εναλλακτικών λύσεων εγκατάστασης, πριν από την δέσμευση σε κάποια συγκεκριμένη αρχιτεκτονική ανάπτυξης εφαρμογών.

3.4.6 Απειλές για τις υπηρεσίες της Amazon (Threats)

Η Amazon έχει να αντιμετωπίσει τον ανταγωνισμό νέων παιχτών στην αγορά του ΥΝ όπως είναι η Google και η IBM. Επίσης το μοντέλο του δημόσιο ΥΝ ενδεχομένως να χάνει έδαφος έναντι προμηθευτών ιδιωτικού ΥΝ οι οποίοι υπόσχονται ιδιωτικότητα στη χρήση των υπηρεσιών τους και προσαρμοστικότητα στις ανάγκες των πελατών τους. Επίσης το επενδυτικό της πλάνο θα πρέπει να λάβει υπόψη τις σύγχρονες τάσεις στον σχεδιασμό βάσεων δεδομένων που δίνει έμφαση στη χρήση μη σχεσιακών βάσεων δεδομένων, αποφυγή της χρήσης SQL, ενώ οι τιμές των εξοπλισμών συνεχώς θα μεταβάλλονται εξαιτίας του διευρυμένου ανταγωνισμού.

3.4.7 Συμπεράσματα Χρήσης των Υπηρεσιών της Amazon

Η ανάλυση του ROI (Perry, R., & Hendrick, S., 2012) επιβεβαιώνει την επικρατούσα άποψη ότι οι τελικοί χρήστες περιμένουν από τις υπηρεσίες cloud μακροπρόθεσμα σημαντική βελτίωση της εξοικονόμησης κεφαλαίων. Οι βασικοί τομείς στους οποίους η ανάλυση ROI είναι ευθυγραμμισμένη με τις προσδοκίες των χρηστών είναι οι εξής:

- Διαθεσιμότητα σε βαθμό επιχείρησης σε όλο το κόσμο για τις υπηρεσίες υποδομής για λειτουργίες κάθε τύπου φόρτου (συναλλαγές, MapReduce, υψηλής απόδοσης, διαδικτύου ή προγραμματιστικές).
- Μια ιδιαίτερα οικονομικά αποδοτική εναλλακτική λύση για ιδιόκτητες λύσεις υποδομής που μειώνει σημαντικά το κόστος για συστήματα πληροφορικής και διαχείρισης.
- Εξαιρετική παραγωγικότητα και πλεονεκτήματα στον χρόνο παράδοσης εφαρμογών στην αγορά λόγω των δυνατοτήτων που παρέχουν τα APIs των AWS σε όλες τις φάσεις ανάπτυξης, εγκατάστασης και διαχείρισης εφαρμογών.
- Υψηλά επίπεδα ασφάλειας στο κέντρο δεδομένων, στις υπηρεσίες και τα δεδομένα συμπεριλαμβανομένων και των ακόλουθων συμμορφώσεων και πιστοποιήσεων:
    - τα επαγγελματικά πρότυπα Statement on Standards for Attestation Engagements No.16 (SSAE 16) και International Standards for Assurance Engagement No. 3402 (ISAE 3402)
    - το Federal Information Security Management Act (FISMA) Moderate level
    - το Information Assurances Certification and Accreditation Program (DIACAP)
    - πιστοποίηση ISO 27001 του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών του AWS οργανισμού καλύπτοντας την υποδομή, τα κέντρα δεδομένων και τις υπηρεσίες
    - επιτυχημένα επικυρωμένος πάροχος υπηρεσιών Level 1 στο πλαίσιο του Payment Card Industry (PCI) του Data Security Standard (DSS)
    - το International Traffic In Arms Compliance (ITAR)
    - το Federal Information Processing Standard (FIPS) Publication 140-2,
    - το HIPAA και Cloud Security Appliance (CSA) Consensus Assessment Initiative Questionnaire (CAIQ).

Η απόφαση της Amazon να αναπτύξει τα AWS από το μηδέν για να υποστηρίξει τις δικές τις πολύπλοκες και πολυπληθείς ανάγκες πληροφορικής (IT) σαν εταιρεία του Fortune 100, παρέχει ένα εκπληκτικό πρότυπο αναφοράς για τον τρόπο με τον οποίο γίνεται η αρχιτεκτονική υπηρεσιών cloud. Επίσης, το μέγεθος και η κλίμακα των AWS παρέχουν έναν υψηλό βαθμό ευελιξίας στην αγορά και την δυνατότητα προσφοράς υπηρεσιών σε ανταγωνιστικές τιμές σε σχέση με άλλους παρόχους υπηρεσιών cloud ή πολύ μεγάλες επιχειρήσεις. Οι τιμές των AWS έχουν μειωθεί 20 φορές μέσα στα τελευταία 6 χρόνια, καθιστώντας με αυτό τον τρόπο τα AWS ελκυστικά για οργανισμούς όλων των μεγεθών.

4. ΑΝΑΛΥΣΗ ΚΙΝΔΥΝΟΥ

4.1 ΚΑΘΟΡΙΣΜΟΣ ΣΤΟΧΟΥ

Στο κεφάλαιο αυτό εξετάζουμε την εφαρμογή μίας συγκεκριμένης μεθοδολογίας Ανάλυσης Κινδύνου στην VSEPX λύση ιδιωτικού ΥΝ της EMC.

Όπως αναφέρθηκε στις προηγούμενες ενότητες τα διάφορα μοντέλα ΥΝ είναι πλέον αρκετά δημοφιλή και καθιστούν διαθέσιμα μία ευρύτερη γκάμα υπηρεσιών και εργαλείων. Από την άλλη πλευρά υφίσταται ένας σημαντικός αριθμός προκλήσεων και κινδύνων όπως εξηγήσαμε αναλυτικά στο κεφάλαιο 2. Επομένως, οι προμηθευτές, οι προγραμματιστές και οι τελικοί χρήστες πρέπει να εξετάσουν αυτές τις προκλήσεις και τους κινδύνους προκειμένου να επιλέξουν το κατάλληλο μοντέλο ΥΝ και βέβαια τον πιο ασφαλή πάροχο.

Οι κίνδυνοι πρέπει να προσδιοριστούν και να αξιολογηθούν έχοντας υπόψη τις απαιτήσεις των πελατών-χρηστών για τη προστασία των προσωπικών δεδομένων των χρηστών, ασφάλεια των δεδομένων, κλείδωμα των δεδομένων, διαθεσιμότητα της υπηρεσίας, αποκατάσταση μετά από καταστροφές, και άλλα. Με γνώμονα τη προστασία των προσωπικών δεδομένων των χρηστών οι οποίοι θα εμπιστευτούν την EMC για την αποθήκευση δεδομένων, και τη χρήση υπηρεσιών πληροφορικής, ο απώτερος στόχος είναι η ανάλυση της ασφάλειας της πλατφόρμας με βάση τις απαιτήσεις των χρηστών. Επίσης είναι ο καθορισμός των κινδύνων που ενδέχεται να προσβάλουν τμήματα ή ακόμα και ολόκληρη τη πλατφόρμα ΥΝ, καθώς και το μέγεθος των συνεπειών που απορρέουν από την εφαρμογή των απειλών σε αυτά.

Η ανάλυση αυτή πραγματοποιήθηκε από την οπτική γωνία ενός φαρμακευτικού οργανισμού-πελάτη βοηθώντας τον στην απόφαση να μεταβεί στην λύση αρχιτεκτονικής VSPEX της EMC για το υπολογιστικό νέφος ή όχι. Η μελέτη αυτή δεν μπορεί να βασιστεί στη συλλογή πληροφοριών από τους ιστότοπους των προμηθευτών ενώ θα ήταν αρκετά χρονοβόρα η οποιαδήποτε προσπάθεια απευθείας επικοινωνίας μαζί τους. Ως πιο άμεσος τρόπος, προτιμήθηκε η συλλογή στοιχείων από ISO 27001 επιθεωρητή που έχει εμπειρία στην αξιολόγηση συστημάτων ασφαλείας είτε IT υποδομών εντός του οργανισμού ή σε υπολογιστικό νέφος για την παροχή της σχετικής πιστοποίησης.

Στη συνέχεια παρατίθενται τα αποτελέσματα της μελέτης στο πλαίσιο ανάλυσης επικινδυνότητας στη VSEPX λύση ιδιωτικού ΥΝ της EMC.

4.2 ΕΠΙΛΟΓΗ ΜΕΘΟΔΟΛΟΓΙΑΣ ΚΑΙ ΕΡΓΑΛΕΙΩΝ

Η αποδοχή, αποτροπή ή μείωση των κινδύνων απαιτεί τον σχεδιασμό και την υλοποίηση αποδοτικών οικονομικά λύσεων στα πλαίσια ενός συστήματος διαχείρισης ασφαλείας. Για το σκοπό αυτό θα πρέπει να εφαρμοστεί μία μεθοδολογίας ανάλυσης κινδύνων που εξετάζει την εφαρμογή των εναλλακτικών λύσεων με βάση το κόστος και το όφελος. Έχουν προταθεί αρκετές μεθοδολογίες στη βιβλιογραφία. Κοινή συνισταμένη τους είναι ότι η διαχείριση κινδύνων περιλαμβάνει τις διαδικασίες εντοπισμού, ανάλυσης και αντιμετώπισης των κινδύνων με σκοπό να προβλεφθούν και να αποφευχθούν οι κίνδυνοι και οι συνέπειες τους κατά τη διάρκεια υλοποίησης ή εκτέλεσης ενός έργου. Οι διαδικασίες αυτές καταλήγουν σε ορισμένα παραδοτέα όπως: οι πιθανές αιτίες κινδύνου και κρίσεων, τα συμπτώματα των προβλημάτων, οι μέθοδοι ποσοτικοποίησης, αξιολόγησης των δικτύων, τα σχέδια αντιμετώπισης κρίσεων, οι εφεδρείες, οι νομικές καλύψεις, οι διορθωτικές ενέργειες.

Στη περίπτωση ενός ΥΝ η ανάλυση κινδύνων περιλαμβάνει τη διαδικασία αναγνώρισης και αξιολόγησης των κινδύνων ασφαλείας που εισάγει το σύστημα ΥΝ στην λειτουργία ενός οργανισμού, καθώς και το κόστος των απωλειών που θα προκληθούν σε περίπτωση που δημιουργηθεί πρόβλημα ασφαλείας. Έτσι προσδιορίζεται ο βαθμός κινδύνου του ΥΝ και οι απαιτήσεις ασφαλείας που υπάρχουν. Επίσης είναι σημαντικό να υπολογιστεί και το κόστος πρόληψης κάθε απώλειας για να βοηθήσει στην λήψη ορθών αποφάσεων.

Ένας κίνδυνος αξιολογείται λαμβάνοντας υπόψη την αξιολόγηση των απειλών και των τρωτών σημείων που έχουν εντοπιστεί και βαθμολογηθεί, στη συνέχεια, με τον προσδιορισμό των πιθανοτήτων και των επιπτώσεων για κάθε κίνδυνο. Η εκτίμηση των κινδύνων με ακρίβεια είναι μια πολύ δύσκολη προσπάθεια γιατί απαιτεί πρόσβαση σε αρκετά δεδομένα κάτι που είναι αδύνατο σχεδόν στην πραγματικότητα. Οι δύο κατηγορίες που συνιστούν την τεχνική ανάλυσης κινδύνων είναι η *ποσοτική (quantitative)* και η *ποιοτική (qualitative)*.

Η ποσοτική ανάλυση προσπαθεί να προσδιορίσει αντικειμενικές αριθμητικές τιμές για την κάθε συνιστώσα της ανάλυσης κινδύνων. Τα αποτελέσματα έχουν το κύρος της μαθηματικής απόδειξης και αυτό βοηθάει στην μεγαλύτερη αποδοχή της ασφάλειας. Από την άλλη πλευρά είναι αρκετά πολύπλοκη διαδικασία καθώς εμπλέκονται στατιστικές μέθοδοι για την εκτίμηση πιθανοτήτων, τον περιορισμό του λάθους κατά την εκτίμηση και την αξιοποίηση αξιόπιστων πηγών πληροφορίας για την παραγωγή προβλέψεων με ακρίβεια.

Η ποιοτική ανάλυση χαρακτηρίζει τις συνιστώσες με εκφράσεις (π.χ μέτριο, μικρό) ή δίνει τιμές από μία προαποφασισμένη κλίμακα. Μ' αυτό τον τρόπο επιτυγχάνεται η ταξινόμησή τους και κατ' επέκταση η προτεραιότητά τους στην αντιμετώπιση των κινδύνων. Στην παρούσα ανάλυση θα χρησιμοποιηθεί η ποιοτική ανάλυση για τον λόγο ότι μία ποσοτική ανάλυση θα απαιτούσε απευθείας πρόσβαση σε στοιχεία που θα έπρεπε να παραθέσει η διεύθυνση ασφάλειας ή πληροφορικής της EMC (πχ μέσω συνεντεύξεων).

Στη περίπτωση της ανάλυσης κινδύνου ως προς τη χρήση της πλατφόρμας EMC από τη πλευρά του χρήστη χρησιμοποιούμε μια υλοποίηση τη βασικής μέθοδου της CRAMM. Λόγο έλλειψης αδείας χρήση του λογισμικού της CRAMM για την παραγωγή των αποτελεσμάτων των ενδιάμεσων φάσεων και της τελικής φάσης της μεθοδολογίας χρησιμοποιήθηκε το excel.

4.2.1 Η μέθοδος CRAMM

Η μέθοδος CRAMM (*CCTA Risk Analysis and Management Methodology*) αναπτύχθηκε από την Κεντρική Υπηρεσία Υπολογιστών και Τηλεπικοινωνιών (*Central Computer and Telecommunications Agency – CCTA*) του Ηνωμένου Βασιλείου το 1987 και αποτελεί πρότυπο για τους οργανισμούς του ευρύτερου δημόσιου τομέα στο Ηνωμένο Βασίλειο. Η CRAMM ταιριάζει στην ανάλυση κινδύνου της πλατφόρμας ΥΝ της EMC για τους εξής λόγους:

- Αποτελεί πρότυπη μέθοδο και έχει αναπτυχθεί με σκοπό να εφαρμοστεί κυρίως σε μεγάλης κλίμακας οργανισμούς και επιχειρήσεις κοινής ωφέλειας.
- Από το 1987 μέχρι σήμερα έχει εφαρμοστεί σε χιλιάδες περιπτώσεων, συνεπώς είναι ώριμη μεθοδολογία ευρισκόμενη ήδη στην τέταρτη εκδοχή της (version).
- Συνοδεύεται από αυτοματοποιημένο εργαλείο λογισμικού που υποστηρίζει όλα τα στάδια της εφαρμογής της, καθώς και την επιλογή αντιμέτρων.
- Καλύπτει όλες τις συνιστώσες της ασφάλειας, περιλαμβανομένων του τεχνικού παράγοντα, των θεμάτων διαδικασιών και προσωπικού, της φυσικής ασφάλειας, της ασφάλειας δικτύων κ.λπ.

Η CRAMM αποτελείται από τρία βασικά στάδια τα οποία και ξεδιπλώνονται στις παρακάτω ενότητες για την περίπτωση της EMC:

1. Προσδιορισμός-αξιολόγηση των αγαθών (*identification and valuation of assets*).
2. Ανάλυση επικινδυνότητας (*risk analysis*).
3. Διαχείριση επικινδυνότητας (*risk management*).

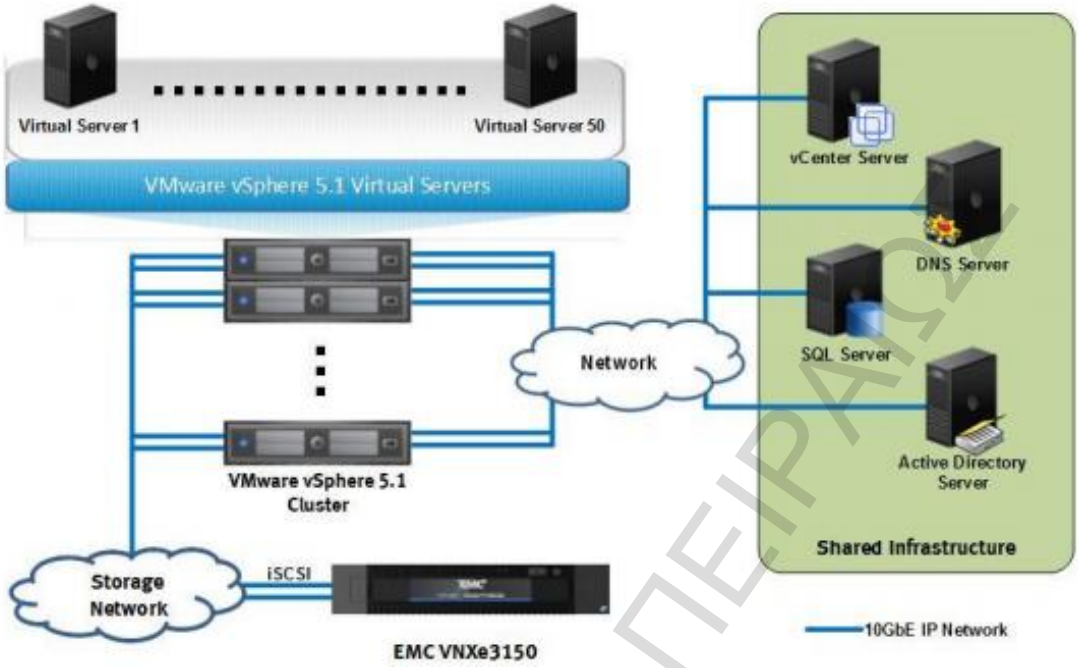
4.2.2 Προσδιορισμός –αξιολόγηση αγαθών

Το πρώτο βήμα αναφέρεται στον προσδιορισμό των στοιχείων του ΥΝ που απαιτούν προστασία. Τα στοιχεία αυτά είναι, μεταξύ άλλων, τα δεδομένα που χειρίζονται, όπως επίσης το λογισμικό και το υλικό των Πληροφοριακών Συστημάτων του ΥΝ. Τα στοιχεία αυτά βρίσκονται σε αλληλεπίδραση.

Η συλλογή των απαραίτητων στοιχείων βασίζεται στην τεκμηρίωση του συστήματος και σε κύκλο συνεντεύξεων που αφορά το τεχνικό προσωπικό και τους κύριους χρήστες του ΥΝ. Αυτές οι κατηγορίες προσωπικού μπορούν να προσφέρουν πλήρη εικόνα για τη λειτουργικότητα του ΥΝ. Στόχος είναι ο προσδιορισμός της αξίας των αγαθών, για παράδειγμα από τη πλευρά των χρηστών, από την οπτική γωνία της ασφάλειας των προσωπικών δεδομένων των πελατών της EMC. Από τη πλευρά της διαχειριστικής ομάδας της EMC στόχος είναι να εκμηδενιστεί η πιθανότητα απώλειας πληροφορίας μετά από την επίδραση μιας ενδεχόμενης απειλής γιατί αυτό θα είχε οικονομικές και νομικές προεκτάσεις. Όλα τα παραπάνω μπορούν να προληφθούν και να επιτευχθούν καθορίζοντας και απαριθμώντας μία προς μία τις απειλές που μπορεί να προκύψουν και να προσβάλουν τη πλατφόρμα της EMC, με αποτέλεσμα την μείωση της φήμης της πλατφόρμας, απώλεια εσόδων από πλευράς EMC, φυγή πελατών ή υποβολή μηνύσεων από πελάτες, ή ακόμα και υποβολή προστίμων από τις τοπικές ρυθμιστικέ αρχές.

4.2.3 Καταγραφή αγαθών και εκτίμηση συνεπειών

Η λύση VSPEX αρχιτεκτονική της EMC προτάθηκε στον φαρμακευτικό οργανισμό που επιθυμεί να δημιουργήσουν το δικό τους ιδιωτικό υπολογιστικό νέφος. Μια λύση VSPEX αρχιτεκτονικής αποτελείται από προϊόντα διαφόρων κατασκευαστών που η EMC εγγυάται ότι θα αποφέρουν τα επιθυμητά αποτελέσματα στον πελάτη για την δημιουργία του ιδιωτικού του υπολογιστικού νέφους και δίνει την δυνατότητα ευελιξίας στην επιλογή αυτών.(EMC, 2014) Στην προκείμενη περίπτωση χρησιμοποιήθηκαν προϊόντα των εταιριών EMC, VMware και Cisco. Στην συνέχεια φαίνεται η λογική απεικόνιση της αρχιτεκτονικής που προτάθηκε(Εικόνα 22).



Εικόνα 22 Αρχιτεκτονική λύσης VSPEX (EMC, 2014)

Πέρα από τα απεικονιζόμενα κομμάτια της αρχιτεκτονικής VSPEX υπάρχουν και άλλα τα οποία κατηγοριοποιήθηκαν σε φυσικά αγαθά, αγαθά δεδομένων και λογισμικά αγαθά. Εν συνεχεία ακολουθεί μια σύντομη περιγραφή του κάθε αγαθού που συμπεριλαμβάνεται στην λύση

Φυσικά Αγαθά

- VMware VSphere 5.1 cluster: Αποτελείται από 3 διακομιστές VMware VSphere και παρέχει ένα κοινό επίπεδο για την φιλοξενία του περιβάλλοντος των εικονικών διακομιστών.
- Διακομιστής VMware vCenter: Παρέχει μια πλατφόρμα για την διαχείριση του VMware VSphere 5.1 cluster.
- Διακομιστής Microsoft SQL Server 2012: Αποτελεί την βάση δεδομένων που ο διακομιστής VMware vCenter αποθηκεύει πληροφορίες σχετικά με τις ρυθμίσεις και τον έλεγχο τον εικονικών διακομιστών.
- IP δίκτυο: Όλη η κίνηση του δικτύου γίνεται μέσα από ένα κοινό Ethernet δίκτυο με πολλαπλή καλωδίωση και διπλούς μεταγωγούς (switches) Cisco
- Cisco Nexus 3048: 2 μεταγωγοί για την δρομολόγηση των δεδομένων του δικτύου
- EMC VNXe3150: Προσφέρει αποθηκευτικό χώρο στους εικονικούς διακομιστες. Σε αυτόν τον χώρο αποθηκεύονται αρχεία με προσωπικά δεδομένα των χρηστών, αρχεία ως αντικείμενο των εφαρμογών και κλειδιά κρυπτογράφησης.
- EMC Data Domain DD160: 3 συσκευές που προσφέρουν αποθηκευτικό χώρο για την διατήρηση αντιγράφων ασφαλείας

Λογισμικά Αγαθά

- Εικονικοί διακομιστες VMware VSphere: Λειτουργικά συστήματα διαθέσιμα σε διαμορφωμένες υποδομές τύπου Vmware και ειδικά παραμετροποιημένα για τη πρόσβαση ομάδας χρηστών. Ο διακομιστής DNS που χρησιμοποιείται για την πραγματοποίηση ανάλυσης των ονομάτων από τα επιμέρους κομμάτια της αρχιτεκτονικής και ο διακομιστής Active Directory χρησιμοποιείται για την δημιουργία ενιαίου χώρου λειτουργίας πολλών χρηστών του ίδιου οργανισμού θα είναι εικονικοί καθώς αυτή η δυνατότητα δίνεται από την αρχιτεκτονική VSPEX)
- VMware vCenter: Εφαρμογή για όλους τους τομείς έλεγχου, διαχείρισης και διατήρησης της εικονικής υποδομής και έλεγχος πρόσβασης (VMware Single Sing-on))
- Vmware VSphere 5.1: Εφαρμογή διαχείρισης πόρων εικονικών διακομιστών
- NetWorker: Εφαρμογή δημιουργίας/διαχείρισης αντιγράφων ασφαλείας
- Εφαρμογή SAP
- Εφαρμογή Microsoft Exchange
- Βάση δεδομένων υποδομής VMware vCenter (Microsoft SQL Server 2012)

Αγαθά Δεδομένων

- Προσωπικά δεδομένα χρηστών: είναι το σύνολο των δεδομένων και αρχείων του κάθε χρήστη στα οποία επιθυμεί να έχει πρόσβαση από οποιοδήποτε σημείο στον κόσμο και οποιαδήποτε συσκευή (πχ. email)
- Επιχειρησιακά δεδομένα του οργανισμού: είναι το σύνολο των δεδομένων και αρχείων του οργανισμού (πχ οικονομικά μεγέθη, πελατολόγιο)

Ακολουθεί η ποιοτική ανάλυση των άμεσων και έμμεσων συνεπειών με την παρακάτω κλίμακα για το κάθε αγαθό όπου αυτές ορίζονται. Στην ποιοτική ανάλυση που κάναμε χρησιμοποιήσαμε μια κλίμακα 1-7 με τα παρακάτω σημασιολογικά χαρακτηριστικά με σκοπό την πιο λεπτομερή ανάλυση στην οποία υπόκειται το κάθε αγαθό.

ΚΛΙΜΑΚΑ	ΠΕΡΙΓΡΑΦΗ
1	ΣΧΕΔΟΝ ΚΑΘΟΛΟΥ
2	ΠΟΛΥ ΜΙΚΡΗ
3	ΜΙΚΡΗ
4	ΜΕΤΡΙΑ
5	ΜΕΓΑΛΗ
6	ΠΟΛΥ ΜΕΓΑΛΗ
7	ΚΑΤΑΣΤΡΟΦΙΚΗ

Η ανάλυση μας θα γίνει ως προς την έλλειψη διαθεσιμότητας, την καταστροφή, την αποκάλυψη και την τροποποίηση των αγαθών του ΥΝ. Με τον όρο έλλειψη διαθεσιμότητας εννοούμε την μερική απώλεια του αγαθού και όχι την ολοκληρωτική καταστροφή του.

- **Άμεσες συνέπειες:** Οι οικονομικές συνέπειες.
- **Έμμεσες συνέπειες:** παρεμπόδιση της λειτουργίας του ΥΝ, απώλεια καλής πίστης των χρηστών, την ευρύτερη εικόνα του ΥΝ απέναντι στους χρήστες.

Κατά την αποτίμηση των στοιχείων των παραπάνω πληροφοριακών πόρων μίας υποδομής ΥΝ, δίνεται ιδιαίτερη έμφαση στην αποτίμηση των δεδομένων που διαχειρίζεται προκειμένου να προσδιοριστεί η σπουδαιότητα που έχουν αυτά για την υπηρεσία. Η αξία κάθε ομάδας / κατηγορίας δεδομένων αποτιμάται με βάση την Επίπτωση (impact) που θα είχε η απώλειά της. Εξετάζεται το μέγεθος της επίπτωσης στις περιπτώσεις καταστροφής, μη εξουσιοδοτημένης μεταβολής (modification), αποκάλυψης (disclosure) και μη-διαθεσιμότητας (unavailability). Συγκεκριμένα εξετάζονται οι εξής περιπτώσεις:

- *Μη-διαθεσιμότητα* [Λιγότερο από 15 λεπτά, 1 ώρα, 3 ώρες, 12 ώρες, 1 μέρα, 2 μέρες, 1 εβδομάδα, 2 εβδομάδες, 1 μήνα, 2 μήνες και περισσότερο].
- *Καταστροφή* [Απώλεια των δεδομένων μετά τη λήψη του τελευταίου αντιγράφου ασφαλείας, Απώλεια όλων των δεδομένων μαζί με το τηρούμενο αντίγραφο].
- *Αποκάλυψη* [Αποκάλυψη των δεδομένων σε μη εξουσιοδοτημένα άτομα εντός του οργανισμού, Αποκάλυψη των δεδομένων σε άτομα εκτός του οργανισμού, Αποκάλυψη των δεδομένων σε παρόχους υπηρεσιών].
- *Μη-εξουσιοδοτημένη μεταβολή* [Μικρής έκτασης σφάλματα, Μεγάλης έκτασης σφάλματα].
- *Εκούσια μεταβολή των δεδομένων*.
- *Σφάλματα μετάδοσης δεδομένων* [Παρεμβολή λανθασμένων μηνυμάτων, Άρνηση αποστολής μηνύματος (*repudiation of origin*), Άρνηση παραλαβής μηνύματος (*repudiation of receipt*), Αποτυχία αποστολής μηνύματος, Επανάληψη μηνύματος (*replay*), Λανθασμένη δρομολόγηση (*misrouting*), Παρακολούθηση κίνησης (*traffic monitoring*), Απώλεια ακολουθίας μηνυμάτων (*out of sequence*)].

Με βάση τα παραπάνω κριτήρια υπολογίστηκαν οι άμεσες και έμμεσες συνέπειες για κάθε πληροφοριακό πόρο.

ΕΙΔΟΣ ΑΓΑΘΟΥ	ΑΓΑΘΑ ΥΠΟΛΟΓΙΣΤΙΚΟΥ ΝΕΦΟΥΣ	ΑΜΕΣΕΣ ΣΥΝΕΠΕΙΕΣ (ΟΙΚΟΝΟΜΙΚΕΣ)			
		ΕΛΛΕΙΨΗ ΔΙΑΘΕΣΙΜΟΤΗΤΑΣ	ΚΑΤΑΣΤΡΟΦΗ	ΑΠΟΚΑΛΥΨΗ	ΤΡΟΠΟΠΟΙΗΣΗ
ΦΥΣΙΚΑ ΑΓΑΘΑ	Διακομιστές VMware VSphere	3	3	5	5
	Διακομιστής VMware vCenter	3	3	5	5
	Διακομιστής Microsoft SQL	3	3	5	5
	IP δίκτυο	3	2		
	Μεταγωγός δικτύου	3	2		
	Αποθηκευτικός Χώρος	3	2	5	5

	Αποθηκευτικός Χώρος (Backup)	3	2	5	5
ΑΓΑΘΑ ΔΕΔΟΜΕΝΩΝ	Προσωπικά δεδομένα χρηστών	3	6	6	6
	Επιχειρησιακά δεδομένα του οργανισμού	4	6	6	7
ΛΟΓΙΣΜΙΚΑ ΑΓΑΘΑ	Εικονικοί διακομιστές VMware Vsphere	3	3	5	5
	VMware vCenter	2	2		
	Vmware VSphere 5.1	2	2		
	Εφαρμογή Backup	2	2		
	Εφαρμογή SAP	3	3		
	Εφαρμογή Microsoft Exchange	3	3		
	Βάση δεδομένων VMware vCenter	2	2	4	4

ΕΙΔΟΣ ΑΓΑΘΟΥ	ΑΓΑΘΑ ΥΠΟΛΟΓΙΣΤΙΚΟΥ ΝΕΦΟΥΣ	ΕΜΜΕΣΕΣ ΣΥΝΕΠΕΙΕΣ			
		ΕΛΛΕΙΨΗ ΔΙΑΘΕΣΙΜΟΤΗΤΑΣ	ΚΑΤΑΣΤΡΟΦΗ	ΑΠΟΚΑΛΥΨΗ	ΤΡΟΠΟΠΟΙΗΣΗ
ΦΥΣΙΚΑ ΑΓΑΘΑ	Διακομιστές VMware VSphere	5	6	6	6
	Διακομιστής VMware vCenter	5	6	6	6
	Διακομιστής Microsoft SQL	5	6	6	6
	IP δίκτυο	4	5	3	3
	Μεταγωγός δικτύου	4	5	3	3
	Αποθηκευτικός Χώρος	5	6	6	6
	Αποθηκευτικός Χώρος (Backup)	5	6	6	6
ΑΓΑΘΑ ΔΕΔΟΜΕΝΩΝ	Προσωπικά δεδομένα χρηστών	6	7	7	7
	Επιχειρησιακά δεδομένα του οργανισμού	6	7	7	7
ΛΟΓΙΣΜΙΚΑ ΑΓΑΘΑ	Εικονικοί διακομιστές VMware Vsphere	5	6	6	6
	VMware vCenter	5	4	4	4
	Vmware VSphere 5.1	5	4	4	4
	Εφαρμογή Backup	5	4	4	4
	Εφαρμογή SAP	5	4	4	4
	Εφαρμογή Microsoft Exchange	5	4	4	4
	Βάση δεδομένων VMware vCenter	5	4	4	4

Ορίζοντας τη βαθμολόγηση των άμεσων και έμμεσων συνεπειών για κάθε πληροφοριακό πόρο προκύπτει ο πίνακας αξίας του κάθε αγαθού :

ΑΓΑΘΑ ΥΠΟΛΟΓΙΣΤΙΚΟΥ ΝΕΦΟΥΣ	ΑΞΙΑ ΑΓΑΘΟΥ	
Επιχειρησιακά δεδομένα του οργανισμού	Α (41-50)	50
Προσωπικά δεδομένα χρηστών	Α (41-50)	48
Διακομιστές VMware VSphere	Β (31-40)	39
Διακομιστής VMware vCenter	Β (31-40)	39
Διακομιστής Microsoft SQL	Β (31-40)	39
Εικονικοί διακομιστες VMware Vsphere	Β (31-40)	39
Αποθηκευτικός Χώρος	Β (31-40)	38
Αποθηκευτικός Χώρος (Backup)	Β (31-40)	38
Βάση δεδομένων VMware vCenter	Γ (21-30)	29
Εφαρμογή SAP	Γ (21-30)	23
Εφαρμογή Microsoft Exchange	Γ (21-30)	23
VMware vCenter	Γ (21-30)	21
Vmware VSphere 5.1	Γ (21-30)	21
Εφαρμογή Backup	Γ (21-30)	21
IP δίκτυο	Δ (11-20)	20
Μεταγωγός δικτύου	Δ (11-20)	20

4.2.4 Ανάλυση και εκτίμηση απειλών

Για κάθε αγαθό του ΥΝ που έχει καταγραφεί παρατίθεται πίνακας με τις απειλές που μπορεί να δεχθεί το καθένα από αυτά. Για κάθε απειλή οι παράγοντες που εξετάζονται είναι:

1) Η συχνότητα απειλής, δηλαδή η πιθανότητα που υπάρχει να συμβεί μια απειλή
2) Η απώλεια που θα επιφέρει η συγκεκριμένη απειλή και
3) Η πραγματική απειλή, η οποία προκύπτει από το μέσο όρο της συχνότητας απειλής και της απώλειας. (στρογγυλοποιημένο προς τα πάνω).

Τα είδη απειλών που έχουν καταγραφεί είναι:

- Επιθέσεις όπως αυτές έχουν ταξινομηθεί στην ενότητα 2.5
- Φυσικές καταστροφές (πχ τυφώνες, κυκλώνες, πλημμύρες, κεραυνοί, χιονοθύελλα, παγετός, χαλάζι, καύσωνας, σεισμός, τσουνάμι)
- Κακόβουλες ανθρώπινες καταστροφές (πχ φυσική εισβολή, απάτη, εμπρησμός, απεργία, διαδηλώσεις, βανδαλισμοί, βομβιστική επίθεση, τρομοκρατική επίθεση, ομηρία)
- Μη σκόπιμες ανθρώπινες καταστροφές (πχ. λάθος χειριστή, προγραμματιστικό λάθος, έκρηξη, πυρκαγιά, ενεργοποίηση πυροσβεστήρα, διαρροή νερού, ενεργοποίηση συστήματος πυρόσβεσης)

Σε κάθε αγαθό εξετάζονται μόνο οι απειλές εκείνες που υπάρχει πιθανότητα να συμβούν και μάλιστα σε μία συγκεκριμένη τοποθεσία. Η μέθοδος CRAMM δεν περιορίζεται στον προσδιορισμό των πιθανών απειλών που υφίσταται ένα πληροφοριακό σύστημα, αλλά επικεντρώνεται στον προσδιορισμό συγκεκριμένων απειλών για κάθε Αγαθό. Η CRAMM παρέχει μία ενδεικτική λίστα απειλών, καθώς και συστάσεις για το ποιες κατηγορίες στοιχείων ενός πληροφοριακού συστήματος αντιμετωπίζουν συνήθως τη συγκεκριμένη απειλή. Όταν ένα

από τα στοιχεία των πληροφοριακών συστημάτων αντιμετωπίζει απειλή τότε και τα δεδομένα ή οι υπηρεσίες που αυτό υποστηρίζει αντιμετωπίζουν την ίδια απειλή. Παρατίθενται οι πίνακες εκτίμησης συνεπειών για καθένα από τα αγαθά του ΥΝ.

ΣΤΟΙΧΕΙΟ ΠΟΥ ΑΝΑΛΥΕΤΑΙ: Διακομιστές VMware VSphere			
ΑΠΕΙΛΕΣ	ΣΥΧΝΟΤΗΤΑ ΑΠΕΙΛΗΣ	ΑΠΩΛΕΙΑ	ΠΡΑΓΜΑΤΙΚΗ ΑΠΕΙΛΗ
ΕΠΙΘΕΣΕΙΣ	4	6	5
ΦΥΣΙΚΕΣ ΚΑΤΑΣΤΡΟΦΕΣ	1	6	4
ΚΑΚΟΒΟΥΛΕΣ ΑΝΘΡΩΠΙΝΕΣ ΚΑΤΑΣΤΡΟΦΕΣ	2	5	4
ΜΗ ΣΚΟΠΙΜΕΣ ΑΝΘΡΩΠΙΝΕΣ ΚΑΤΑΣΤΡΟΦΕΣ	2	4	3

ΣΤΟΙΧΕΙΟ ΠΟΥ ΑΝΑΛΥΕΤΑΙ: Διακομιστής VMware vCenter			
ΑΠΕΙΛΕΣ	ΣΥΧΝΟΤΗΤΑ ΑΠΕΙΛΗΣ	ΑΠΩΛΕΙΑ	ΠΡΑΓΜΑΤΙΚΗ ΑΠΕΙΛΗ
ΕΠΙΘΕΣΕΙΣ	4	6	5
ΦΥΣΙΚΕΣ ΚΑΤΑΣΤΡΟΦΕΣ	1	6	4
ΚΑΚΟΒΟΥΛΕΣ ΑΝΘΡΩΠΙΝΕΣ ΚΑΤΑΣΤΡΟΦΕΣ	2	5	4
ΜΗ ΣΚΟΠΙΜΕΣ ΑΝΘΡΩΠΙΝΕΣ ΚΑΤΑΣΤΡΟΦΕΣ	2	4	3

ΣΤΟΙΧΕΙΟ ΠΟΥ ΑΝΑΛΥΕΤΑΙ: Διακομιστής Microsoft SQL			
ΑΠΕΙΛΕΣ	ΣΥΧΝΟΤΗΤΑ ΑΠΕΙΛΗΣ	ΑΠΩΛΕΙΑ	ΠΡΑΓΜΑΤΙΚΗ ΑΠΕΙΛΗ
ΕΠΙΘΕΣΕΙΣ	4	6	5
ΦΥΣΙΚΕΣ ΚΑΤΑΣΤΡΟΦΕΣ	1	6	4
ΚΑΚΟΒΟΥΛΕΣ ΑΝΘΡΩΠΙΝΕΣ ΚΑΤΑΣΤΡΟΦΕΣ	2	5	4
ΜΗ ΣΚΟΠΙΜΕΣ ΑΝΘΡΩΠΙΝΕΣ ΚΑΤΑΣΤΡΟΦΕΣ	2	4	3

ΣΤΟΙΧΕΙΟ ΠΟΥ ΑΝΑΛΥΕΤΑΙ: IP δίκτυο			
ΑΠΕΙΛΕΣ	ΣΥΧΝΟΤΗΤΑ ΑΠΕΙΛΗΣ	ΑΠΩΛΕΙΑ	ΠΡΑΓΜΑΤΙΚΗ ΑΠΕΙΛΗ
ΕΠΙΘΕΣΕΙΣ	6	5	6
ΦΥΣΙΚΕΣ ΚΑΤΑΣΤΡΟΦΕΣ	1	5	3
ΚΑΚΟΒΟΥΛΕΣ ΑΝΘΡΩΠΙΝΕΣ ΚΑΤΑΣΤΡΟΦΕΣ	2	4	3
ΜΗ ΣΚΟΠΙΜΕΣ ΑΝΘΡΩΠΙΝΕΣ ΚΑΤΑΣΤΡΟΦΕΣ	2	4	3

ΣΤΟΙΧΕΙΟ ΠΟΥ ΑΝΑΛΥΕΤΑΙ: Μεταγωγός δικτύου			
ΑΠΕΙΛΕΣ	ΣΥΧΝΟΤΗΤΑ ΑΠΕΙΛΗΣ	ΑΠΩΛΕΙΑ	ΠΡΑΓΜΑΤΙΚΗ ΑΠΕΙΛΗ
ΕΠΙΘΕΣΕΙΣ	6	5	6
ΦΥΣΙΚΕΣ ΚΑΤΑΣΤΡΟΦΕΣ	1	5	3
ΚΑΚΟΒΟΥΛΕΣ ΑΝΘΡΩΠΙΝΕΣ ΚΑΤΑΣΤΡΟΦΕΣ	2	4	3
ΜΗ ΣΚΟΠΙΜΕΣ ΑΝΘΡΩΠΙΝΕΣ ΚΑΤΑΣΤΡΟΦΕΣ	2	4	3

ΣΤΟΙΧΕΙΟ ΠΟΥ ΑΝΑΛΥΕΤΑΙ: Αποθηκευτικός Χώρος			
ΑΠΕΙΛΕΣ	ΣΥΧΝΟΤΗΤΑ ΑΠΕΙΛΗΣ	ΑΠΩΛΕΙΑ	ΠΡΑΓΜΑΤΙΚΗ ΑΠΕΙΛΗ
ΕΠΙΘΕΣΕΙΣ	4	6	5
ΦΥΣΙΚΕΣ ΚΑΤΑΣΤΡΟΦΕΣ	1	6	4
ΚΑΚΟΒΟΥΛΕΣ ΑΝΘΡΩΠΙΝΕΣ ΚΑΤΑΣΤΡΟΦΕΣ	3	5	4
ΜΗ ΣΚΟΠΙΜΕΣ ΑΝΘΡΩΠΙΝΕΣ ΚΑΤΑΣΤΡΟΦΕΣ	2	5	4

ΣΤΟΙΧΕΙΟ ΠΟΥ ΑΝΑΛΥΕΤΑΙ: Αποθηκευτικός Χώρος (Backup)			
ΑΠΕΙΛΕΣ	ΣΥΧΝΟΤΗΤΑ ΑΠΕΙΛΗΣ	ΑΠΩΛΕΙΑ	ΠΡΑΓΜΑΤΙΚΗ ΑΠΕΙΛΗ
ΕΠΙΘΕΣΕΙΣ	2	4	3
ΦΥΣΙΚΕΣ ΚΑΤΑΣΤΡΟΦΕΣ	1	4	3
ΚΑΚΟΒΟΥΛΕΣ ΑΝΘΡΩΠΙΝΕΣ ΚΑΤΑΣΤΡΟΦΕΣ	2	3	3
ΜΗ ΣΚΟΠΙΜΕΣ ΑΝΘΡΩΠΙΝΕΣ ΚΑΤΑΣΤΡΟΦΕΣ	2	3	3

ΣΤΟΙΧΕΙΟ ΠΟΥ ΑΝΑΛΥΕΤΑΙ: Εικονικοί διακομιστές VMware Vsphere			
ΑΠΕΙΛΕΣ	ΣΥΧΝΟΤΗΤΑ ΑΠΕΙΛΗΣ	ΑΠΩΛΕΙΑ	ΠΡΑΓΜΑΤΙΚΗ ΑΠΕΙΛΗ
ΕΠΙΘΕΣΕΙΣ	3	4	4
ΦΥΣΙΚΕΣ ΚΑΤΑΣΤΡΟΦΕΣ	1	5	3
ΚΑΚΟΒΟΥΛΕΣ ΑΝΘΡΩΠΙΝΕΣ ΚΑΤΑΣΤΡΟΦΕΣ	2	3	3
ΜΗ ΣΚΟΠΙΜΕΣ ΑΝΘΡΩΠΙΝΕΣ ΚΑΤΑΣΤΡΟΦΕΣ	2	3	3

ΣΤΟΙΧΕΙΟ ΠΟΥ ΑΝΑΛΥΕΤΑΙ: VMware vCenter			
ΑΠΕΙΛΕΣ	ΣΥΧΝΟΤΗΤΑ ΑΠΕΙΛΗΣ	ΑΠΩΛΕΙΑ	ΠΡΑΓΜΑΤΙΚΗ ΑΠΕΙΛΗ
ΕΠΙΘΕΣΕΙΣ	3	5	4
ΦΥΣΙΚΕΣ ΚΑΤΑΣΤΡΟΦΕΣ	1	5	3
ΚΑΚΟΒΟΥΛΕΣ ΑΝΘΡΩΠΙΝΕΣ ΚΑΤΑΣΤΡΟΦΕΣ	2	4	3
ΜΗ ΣΚΟΠΙΜΕΣ ΑΝΘΡΩΠΙΝΕΣ ΚΑΤΑΣΤΡΟΦΕΣ	2	4	3

ΣΤΟΙΧΕΙΟ ΠΟΥ ΑΝΑΛΥΕΤΑΙ: Vmware VSphere 5.1			
ΑΠΕΙΛΕΣ	ΣΥΧΝΟΤΗΤΑ ΑΠΕΙΛΗΣ	ΑΠΩΛΕΙΑ	ΠΡΑΓΜΑΤΙΚΗ ΑΠΕΙΛΗ
ΕΠΙΘΕΣΕΙΣ	3	5	4
ΦΥΣΙΚΕΣ ΚΑΤΑΣΤΡΟΦΕΣ	1	5	3
ΚΑΚΟΒΟΥΛΕΣ ΑΝΘΡΩΠΙΝΕΣ ΚΑΤΑΣΤΡΟΦΕΣ	2	4	3
ΜΗ ΣΚΟΠΙΜΕΣ ΑΝΘΡΩΠΙΝΕΣ ΚΑΤΑΣΤΡΟΦΕΣ	2	4	3

ΣΤΟΙΧΕΙΟ ΠΟΥ ΑΝΑΛΥΕΤΑΙ: Εφαρμογή Backup			
ΑΠΕΙΛΕΣ	ΣΥΧΝΟΤΗΤΑ ΑΠΕΙΛΗΣ	ΑΠΩΛΕΙΑ	ΠΡΑΓΜΑΤΙΚΗ ΑΠΕΙΛΗ
ΕΠΙΘΕΣΕΙΣ	3	3	3
ΦΥΣΙΚΕΣ ΚΑΤΑΣΤΡΟΦΕΣ	1	3	2
ΚΑΚΟΒΟΥΛΕΣ ΑΝΘΡΩΠΙΝΕΣ ΚΑΤΑΣΤΡΟΦΕΣ	2	2	2
ΜΗ ΣΚΟΠΙΜΕΣ ΑΝΘΡΩΠΙΝΕΣ ΚΑΤΑΣΤΡΟΦΕΣ	2	2	2

ΣΤΟΙΧΕΙΟ ΠΟΥ ΑΝΑΛΥΕΤΑΙ: Βάση δεδομένων VMware vCenter			
ΑΠΕΙΛΕΣ	ΣΥΧΝΟΤΗΤΑ ΑΠΕΙΛΗΣ	ΑΠΩΛΕΙΑ	ΠΡΑΓΜΑΤΙΚΗ ΑΠΕΙΛΗ
ΕΠΙΘΕΣΕΙΣ	3	4	4
ΦΥΣΙΚΕΣ ΚΑΤΑΣΤΡΟΦΕΣ	1	4	3
ΚΑΚΟΒΟΥΛΕΣ ΑΝΘΡΩΠΙΝΕΣ ΚΑΤΑΣΤΡΟΦΕΣ	2	3	3
ΜΗ ΣΚΟΠΙΜΕΣ ΑΝΘΡΩΠΙΝΕΣ ΚΑΤΑΣΤΡΟΦΕΣ	2	3	3

ΣΤΟΙΧΕΙΟ ΠΟΥ ΑΝΑΛΥΕΤΑΙ: Προσωπικά δεδομένα χρηστών			
ΑΠΕΙΛΕΣ	ΣΥΧΝΟΤΗΤΑ ΑΠΕΙΛΗΣ	ΑΠΩΛΕΙΑ	ΠΡΑΓΜΑΤΙΚΗ ΑΠΕΙΛΗ
ΕΠΙΘΕΣΕΙΣ	6	7	7
ΦΥΣΙΚΕΣ ΚΑΤΑΣΤΡΟΦΕΣ	1	5	3
ΚΑΚΟΒΟΥΛΕΣ ΑΝΘΡΩΠΙΝΕΣ ΚΑΤΑΣΤΡΟΦΕΣ	4	7	6
ΜΗ ΣΚΟΠΙΜΕΣ ΑΝΘΡΩΠΙΝΕΣ ΚΑΤΑΣΤΡΟΦΕΣ	2	5	4

ΣΤΟΙΧΕΙΟ ΠΟΥ ΑΝΑΛΥΕΤΑΙ: Επιχειρησιακά δεδομένα του οργανισμού			
ΑΠΕΙΛΕΣ	ΣΥΧΝΟΤΗΤΑ ΑΠΕΙΛΗΣ	ΑΠΩΛΕΙΑ	ΠΡΑΓΜΑΤΙΚΗ ΑΠΕΙΛΗ
ΕΠΙΘΕΣΕΙΣ	6	7	6
ΦΥΣΙΚΕΣ ΚΑΤΑΣΤΡΟΦΕΣ	5	5	3
ΚΑΚΟΒΟΥΛΕΣ ΑΝΘΡΩΠΙΝΕΣ ΚΑΤΑΣΤΡΟΦΕΣ	4	7	6
ΜΗ ΣΚΟΠΙΜΕΣ ΑΝΘΡΩΠΙΝΕΣ ΚΑΤΑΣΤΡΟΦΕΣ	3	5	3

ΣΤΟΙΧΕΙΟ ΠΟΥ ΑΝΑΛΥΕΤΑΙ: Εφαρμογή SAP			
ΑΠΕΙΛΕΣ	ΣΥΧΝΟΤΗΤΑ ΑΠΕΙΛΗΣ	ΑΠΩΛΕΙΑ	ΠΡΑΓΜΑΤΙΚΗ ΑΠΕΙΛΗ
ΕΠΙΘΕΣΕΙΣ	3	6	5
ΦΥΣΙΚΕΣ ΚΑΤΑΣΤΡΟΦΕΣ	1	6	4
ΚΑΚΟΒΟΥΛΕΣ ΑΝΘΡΩΠΙΝΕΣ ΚΑΤΑΣΤΡΟΦΕΣ	2	5	4
ΜΗ ΣΚΟΠΙΜΕΣ ΑΝΘΡΩΠΙΝΕΣ ΚΑΤΑΣΤΡΟΦΕΣ	2	5	4

ΣΤΟΙΧΕΙΟ ΠΟΥ ΑΝΑΛΥΕΤΑΙ: Εφαρμογή Microsoft Exchange			
ΑΠΕΙΛΕΣ	ΣΥΧΝΟΤΗΤΑ ΑΠΕΙΛΗΣ	ΑΠΩΛΕΙΑ	ΠΡΑΓΜΑΤΙΚΗ ΑΠΕΙΛΗ
ΕΠΙΘΕΣΕΙΣ	3	6	5
ΦΥΣΙΚΕΣ ΚΑΤΑΣΤΡΟΦΕΣ	1	6	4
ΚΑΚΟΒΟΥΛΕΣ ΑΝΘΡΩΠΙΝΕΣ ΚΑΤΑΣΤΡΟΦΕΣ	2	5	4
ΜΗ ΣΚΟΠΙΜΕΣ ΑΝΘΡΩΠΙΝΕΣ ΚΑΤΑΣΤΡΟΦΕΣ	2	5	4

4.2.5 Ανάλυση και εκτίμηση αδυναμιών

Στο σημείο αυτό καθορίζονται τα σημεία τα οποία επιτρέπουν την εμφάνιση απειλών, χρησιμοποιώντας μία κλίμακα από 1 έως 3, δηλώνοντας έτσι το επίπεδο αδυναμίας του αγαθού όταν μια απειλή εμφανιστεί σε αυτό.

1. Υψηλή Αδυναμία
2. Μέτρια Αδυναμία
3. Μικρή Αδυναμία

ΕΙΔΟΣ ΑΓΑΘΟΥ	ΑΓΑΘΑ ΥΠΟΛΟΓΙΣΤΙΚΟΥ ΝΕΦΟΥΣ	ΑΔΥΝΑΜΙΑ			
		ΕΠΙΘΕΣΕΙΣ	ΦΥΣΙΚΕΣ ΚΑΤΑΣΤΡΟΦΕΣ	ΚΑΚΟΒΟΥΛΕΣ ΑΝΘΡΩΠΙΝΕΣ ΚΑΤΑΣΤΡΟΦΕΣ	ΜΗ ΣΚΟΠΙΜΕΣ ΑΝΘΡΩΠΙΝΕΣ ΚΑΤΑΣΤΡΟΦΕΣ
ΦΥΣΙΚΑ ΑΓΑΘΑ	Διακομιστές VMware VSphere	2	3	2	3
	Διακομιστής VMware vCenter	2	3	2	3
	Διακομιστής Microsoft SQL	2	3	2	3
	IP δίκτυο	3	3	3	3
	Μεταγωγός δικτυου	3	3	2	3
	Αποθηκευτικός Χώρος	2	3	2	3
	Αποθηκευτικός Χώρος (Backup)	2	3	2	3
ΑΓΑΘΑ ΔΕΔΟΜΕΝΩΝ	Προσωπικά δεδομένα χρηστών	2	3	1	3
	Επιχειρησιακά δεδομένα του οργανισμού	2	3	1	3
ΛΟΓΙΣΜΙΚΑ ΑΓΑΘΑ	Εικονικοί διακομιστες VMware Vsphere	2	3	1	2
	VMware vCenter	3	3	2	2
	Vmware VSphere 5.1	3	3	2	2
	Εφαρμογή Backup	3	3	2	2
	Εφαρμογή SAP	3	3	3	3
	Εφαρμογή Microsoft Exchange	3	3	3	3
	Βάση δεδομένων VMware vCenter	3	3	2	3

4.3 ΥΠΟΛΟΓΙΣΜΟΣ ΚΑΙ ΜΕΤΡΗΣΗ ΚΙΝΔΥΝΟΥ

Στο σημείο αυτό αξιολογούμε και συσχετίζουμε όλες τις προηγούμενες πληροφορίες για κάθε πιθανό συνδυασμό αξίας ή συνέπειας αγαθού, επιπέδου απειλής και επιπέδου αδυναμίας. Θέλοντας να κατηγοριοποιήσουμε τα αγαθά σύμφωνα με την αξία που έχει το καθένα για το ΥΝ που εξετάζουμε, ορίσαμε μία κλίμακα από το Α έως το Ε, θεωρώντας ως αγαθό με μεγαλύτερη αξία αυτό που παίρνει την τιμή Α και ως μικρότερης αξίας αυτό που λαμβάνει την τιμή Ε. Όσον αφορά τα επίπεδα απειλής ή αδυναμίας, ως χαμηλό θεωρούμε αυτό που παίρνει την τιμή από 1 έως 3, ως μεσαίο αυτό με εύρος τιμών από 4 έως 5 και ως μεγάλο αυτό με τιμές από 6 έως 7.

ΕΠΙΠΕΔΑ	ΤΙΜΗ
ΧΑΜΗΛΟ	1-3
ΜΕΣΑΙΟ	4-5
ΥΨΗΛΟ	6-7

Για κάθε απειλή ξεχωριστά και λαμβάνοντας υπόψη το επίπεδο απειλής και το επίπεδο αδυναμίας και κάνοντας χρήση του παρακάτω πίνακα προχωράμε στον υπολογισμό του κινδύνου για κάθε αγαθό ξεχωριστά όπως φαίνεται στον τελευταίο πίνακα.

ΕΠΙΠΕΔΟ ΑΠΕΙΛΗΣ		ΧΑΜΗΛΟ			ΜΕΣΑΙΟ			ΥΨΗΛΟ		
ΕΠΙΠΕΔΟ ΑΔΥΝΑΜΙΑΣ		Χ[22]	Μ[23]	Υ[24]	Χ	Μ	Υ	Χ	Μ	Υ
ΑΞΙΑ Ή ΣΥΝΕΠΕΙΑ ΑΓΑΘΟΥ	Ε	0	1	2	1	2	3	2	3	4
	Δ	1	2	3	2	3	4	3	4	5
	Γ	2	3	4	3	4	5	4	5	6
	Β	3	4	5	4	5	6	5	6	7
	Α	4	5	6	5	6	7	6	7	8

[22] ΧΑΜΗΛΟ

[23] ΜΕΣΑΙΟ

[24] ΥΨΗΛΟ

		ΕΠΙΠΕΔΟ ΑΠΕΙΛΗΣ	ΕΠΙΠΕΔΟ ΑΔΥΝΑΜΙΑΣ	ΚΙΝΔΥΝΟΣ
ΑΠΕΙΛΗ	ΕΠΙΘΕΣΕΙΣ			
ΑΓΑΘΑ	Διακομιστές VMware VSphere	ΜΕΣΑΙΟ	ΜΕΣΑΙΟ	5
	Διακομιστής VMware vCenter	ΜΕΣΑΙΟ	ΜΕΣΑΙΟ	5
	Διακομιστής Microsoft SQL	ΜΕΣΑΙΟ	ΜΕΣΑΙΟ	5
	IP δίκτυο	ΥΨΗΛΟ	ΧΑΜΗΛΟ	3
	Μεταγωγός δικτυου	ΥΨΗΛΟ	ΧΑΜΗΛΟ	3
	Αποθηκευτικός Χώρος	ΜΕΣΑΙΟ	ΜΕΣΑΙΟ	5
	Αποθηκευτικός Χώρος (Backup)	ΧΑΜΗΛΟ	ΜΕΣΑΙΟ	4
	Προσωπικά δεδομένα χρηστών	ΥΨΗΛΟ	ΜΕΣΑΙΟ	7
	Επιχειρησιακά δεδομένα του οργανισμού	ΥΨΗΛΟ	ΜΕΣΑΙΟ	7
	Εικονικοί διακομιστες VMware Vsphere	ΜΕΣΑΙΟ	ΜΕΣΑΙΟ	5
	VMware vCenter	ΜΕΣΑΙΟ	ΧΑΜΗΛΟ	3
	Vmware VSphere 5.1	ΜΕΣΑΙΟ	ΧΑΜΗΛΟ	3
	Εφαρμογή Backup	ΧΑΜΗΛΟ	ΧΑΜΗΛΟ	2
	Εφαρμογή SAP	ΜΕΣΑΙΟ	ΧΑΜΗΛΟ	3
	Εφαρμογή Microsoft Exchange	ΜΕΣΑΙΟ	ΧΑΜΗΛΟ	3
	Βάση δεδομένων VMware vCenter	ΜΕΣΑΙΟ	ΧΑΜΗΛΟ	3

		ΕΠΙΠΕΔΟ ΑΠΕΙΛΗΣ	ΕΠΙΠΕΔΟ ΑΔΥΝΑΜΙΑΣ	ΚΙΝΔΥΝΟΣ
ΑΠΕΙΛΗ	ΦΥΣΙΚΕΣ ΚΑΤΑΣΤΡΟΦΕΣ			
ΑΓΑΘΑ	Διακομιστές VMware VSphere	ΜΕΣΑΙΟ	ΜΕΣΑΙΟ	5
	Διακομιστής VMware vCenter	ΜΕΣΑΙΟ	ΜΕΣΑΙΟ	5
	Διακομιστής Microsoft SQL	ΜΕΣΑΙΟ	ΜΕΣΑΙΟ	5
	IP δίκτυο	ΧΑΜΗΛΟ	ΧΑΜΗΛΟ	1
	Μεταγωγός δικτυου	ΧΑΜΗΛΟ	ΧΑΜΗΛΟ	1
	Αποθηκευτικός Χώρος	ΜΕΣΑΙΟ	ΜΕΣΑΙΟ	5
	Αποθηκευτικός Χώρος (Backup)	ΧΑΜΗΛΟ	ΜΕΣΑΙΟ	4
	Προσωπικά δεδομένα χρηστών	ΧΑΜΗΛΟ	ΜΕΣΑΙΟ	5
	Επιχειρησιακά δεδομένα του οργανισμού	ΧΑΜΗΛΟ	ΜΕΣΑΙΟ	5
	Εικονικοί διακομιστες VMware Vsphere	ΧΑΜΗΛΟ	ΜΕΣΑΙΟ	4
	VMware vCenter	ΧΑΜΗΛΟ	ΧΑΜΗΛΟ	2
	Vmware VSphere 5.1	ΧΑΜΗΛΟ	ΧΑΜΗΛΟ	2
	Εφαρμογή Backup	ΧΑΜΗΛΟ	ΧΑΜΗΛΟ	2
	Εφαρμογή SAP	ΜΕΣΑΙΟ	ΧΑΜΗΛΟ	3
	Εφαρμογή Microsoft Exchange	ΜΕΣΑΙΟ	ΧΑΜΗΛΟ	3
	Βάση δεδομένων VMware vCenter	ΧΑΜΗΛΟ	ΧΑΜΗΛΟ	2

		ΕΠΙΠΕΔΟ ΑΠΕΙΛΗΣ	ΕΠΙΠΕΔΟ ΑΔΥΝΑΜΙΑΣ	ΚΙΝΔΥΝΟΣ
ΑΠΕΙΛΗ	ΚΑΚΟΒΟΥΛΕΣ ΑΝΘΡΩΠΙΝΕΣ ΚΑΤΑΣΤΡΟΦΕΣ			
ΑΓΑΘΑ	Διακομιστές VMware VSphere	ΜΕΣΑΙΟ	ΜΕΣΑΙΟ	5
	Διακομιστής VMware vCenter	ΜΕΣΑΙΟ	ΜΕΣΑΙΟ	5
	Διακομιστής Microsoft SQL	ΜΕΣΑΙΟ	ΜΕΣΑΙΟ	5
	IP δίκτυο	ΧΑΜΗΛΟ	ΧΑΜΗΛΟ	1
	Μεταγωγός δικτυου	ΧΑΜΗΛΟ	ΧΑΜΗΛΟ	1
	Αποθηκευτικός Χώρος	ΜΕΣΑΙΟ	ΜΕΣΑΙΟ	5
	Αποθηκευτικός Χώρος (Backup)	ΧΑΜΗΛΟ	ΜΕΣΑΙΟ	4
	Προσωπικά δεδομένα χρηστών	ΥΨΗΛΟ	ΜΕΣΑΙΟ	7
	Επιχειρησιακά δεδομένα του οργανισμού	ΥΨΗΛΟ	ΜΕΣΑΙΟ	7
	Εικονικοί διακομιστες VMware Vsphere	ΧΑΜΗΛΟ	ΜΕΣΑΙΟ	4
	VMware vCenter	ΧΑΜΗΛΟ	ΧΑΜΗΛΟ	2
	Vmware VSphere 5.1	ΧΑΜΗΛΟ	ΜΕΣΑΙΟ	3
	Εφαρμογή Backup	ΧΑΜΗΛΟ	ΜΕΣΑΙΟ	3
	Εφαρμογή SAP	ΜΕΣΑΙΟ	ΧΑΜΗΛΟ	3
	Εφαρμογή Microsoft Exchange	ΜΕΣΑΙΟ	ΧΑΜΗΛΟ	3
	Βάση δεδομένων VMware vCenter	ΧΑΜΗΛΟ	ΜΕΣΑΙΟ	3

		ΕΠΙΠΕΔΟ ΑΠΕΙΛΗΣ	ΕΠΙΠΕΔΟ ΑΔΥΝΑΜΙΑΣ	ΚΙΝΔΥΝΟΣ
ΑΠΕΙΛΗ	ΜΗ ΣΚΟΠΙΜΕΣ ΑΝΘΡΩΠΙΝΕΣ ΚΑΤΑΣΤΡΟΦΕΣ			
ΑΓΑΘΑ	Διακομιστές VMware VSphere	ΧΑΜΗΛΟ	ΜΕΣΑΙΟ	5
	Διακομιστής VMware vCenter	ΧΑΜΗΛΟ	ΜΕΣΑΙΟ	5
	Διακομιστής Microsoft SQL	ΧΑΜΗΛΟ	ΜΕΣΑΙΟ	5
	IP δίκτυο	ΧΑΜΗΛΟ	ΧΑΜΗΛΟ	1
	Μεταγωγός δικτυου	ΧΑΜΗΛΟ	ΧΑΜΗΛΟ	1
	Αποθηκευτικός Χώρος	ΜΕΣΑΙΟ	ΜΕΣΑΙΟ	5
	Αποθηκευτικός Χώρος (Backup)	ΧΑΜΗΛΟ	ΜΕΣΑΙΟ	4
	Προσωπικά δεδομένα χρηστών	ΜΕΣΑΙΟ	ΜΕΣΑΙΟ	5
	Επιχειρησιακά δεδομένα του οργανισμού	ΜΕΣΑΙΟ	ΜΕΣΑΙΟ	5
	Εικονικοί διακομιστες VMware Vsphere	ΧΑΜΗΛΟ	ΜΕΣΑΙΟ	4
	VMware vCenter	ΧΑΜΗΛΟ	ΧΑΜΗΛΟ	2
	Vmware VSphere 5.1	ΧΑΜΗΛΟ	ΜΕΣΑΙΟ	3
	Εφαρμογή Backup	ΧΑΜΗΛΟ	ΜΕΣΑΙΟ	3
	Εφαρμογή SAP	ΜΕΣΑΙΟ	ΧΑΜΗΛΟ	3
	Εφαρμογή Microsoft Exchange	ΜΕΣΑΙΟ	ΧΑΜΗΛΟ	3
	Βάση δεδομένων VMware vCenter	ΧΑΜΗΛΟ	ΜΕΣΑΙΟ	3

4.4 ΔΙΑΧΕΙΡΙΣΗ ΚΙΝΔΥΝΟΥ

Με βάση τις παραπάνω μετρήσεις παράγεται ένα σχέδιο ασφάλειας για τα πληροφοριακά αγαθά του υπολογιστικού νέφους EMC. Αυτό αποτελείται από μία σειρά αντιμέτρων τα οποία κρίνονται απαραίτητα για την αντιμετώπιση και διαχείριση της επικινδυνότητας και τα οποία θα πρέπει να εφαρμοστούν. Το σχέδιο ασφάλειας περιλαμβάνει και μία σειρά επιλογών και εναλλακτικών λύσεων, ώστε να παρέχεται ευελιξία στην εφαρμογή του.

Για συστήματα τα οποία έχουν αναπτυχθεί και λειτουργούν ήδη, το προτεινόμενο σχέδιο ασφάλειας μπορεί να συγκριθεί με τα υπάρχοντα αντίμετρα. Η τελική επιλογή των αντιμέτρων που θα εφαρμοστούν λαμβάνει υπόψη και το κόστος που έχουν τα αντίμετρα για τον οργανισμό. Τα βήματα του τρίτου σταδίου περιλαμβάνουν:

- Τον προσδιορισμό των προτεινόμενων αντιμέτρων.
- Το σχεδιασμό του σχεδίου ασφάλειας

5 ΣΥΜΠΕΡΑΣΜΑΤΑ – ΠΕΡΙΛΗΨΗ

Ένα από τα σημαντικά κριτήρια που λαμβάνεται υπόψη από τους πελάτες (επιχειρήσεις, καταναλωτές) στην απόφαση τους να εμπιστευτούν υποδομές υπολογιστικού νέφους για τις εφαρμογές και τα δεδομένα τους είναι η ασφάλεια. Η ασφάλεια βέβαια συμπληρώνεται και πολλές φορές αλληλοσυγκρούεται με παράγοντες όπως το κόστος, το επίπεδο παροχής υπηρεσιών, η διαθεσιμότητα, το ισχυρό όνομα του προμηθευτή ΥΝ στην ευρύτερη αγορά.

Στην εργασία αυτή ασχοληθήκαμε με τη μελέτη του θεωρητικού υπόβαθρου μίας πλατφόρμας ΥΝ και μέσα σε αυτό το πλαίσιο εντάχθηκε η διαχείριση της ασφάλειας για την προστασία των δεδομένων των χρηστών. Οι κίνδυνοι που καταγράφηκαν για επιμέρους περιπτώσεις υποδομών υπολογιστικού νέφους δείχνουν ότι οι περισσότεροι από αυτούς πηγάζουν από το γεγονός ότι οι προμηθευτές επενδύουν σε συμπλέγματα εικονικών υπολογιστικών υποδομών (virtualisation clusters) με αποτέλεσμα να αυξάνεται η πολυπλοκότητα του ελέγχου και της αλληλεπίδρασης εξωτερικών χρηστών – εικονικών μηχανών, αλλά και εσωτερικών λειτουργιών διαχείρισης των μηχανών αυτών.

Η αρχιτεκτονική ασφάλειας μίας υποδομής ΥΝ δεν διαφοροποιείται σημαντικά από μία ανάλογη υποδομή στο περιβάλλον μίας επιχείρησης. Σε αρκετές περιπτώσεις η αρχιτεκτονική αυτή θα είναι περισσότερη ενισχυμένη εξαιτίας της επένδυσης των παρόχων υπολογιστικού νέφους. Ωστόσο, γίνονται όλο και συχνότερες αναφορές στην βιβλιογραφία, και ορισμένες εκ των οποίων υπάρχουν και στο κεφάλαιο 2 της εργασίας, ότι οι πιο σοβαρές επιθέσεις συσχετίζονται με τους χρήστες του συστήματος (εσωτερικούς ή εξωτερικούς). Από την άλλη πλευρά, η διαχείριση της ασφάλειας (διαχείριση κινδύνων, μέτρα προστασίας υποδομής και προσωπικών δεδομένων, και άλλα) πρέπει να ενταχθεί σε ένα γενικότερο πλαίσιο ορθών πρακτικών (best practices) το οποίο θα διευκολύνει την αξιολόγηση των εκάστοτε προμηθευτών υπολογιστικού νέφους. Στην εργασία αυτή αξιολογήθηκαν τρεις τέτοιοι προμηθευτές (Oracle, EMC, Amazon) οι οποίοι εκπροσωπούν τρία διαφορετικά μοντέλα παροχής υπηρεσιών ΥΝ (SaaS, IaaS, PaaS). Σίγουρα υπάρχουν αρκετοί άλλη σημαντικοί ανταγωνιστές τους στην παγκόσμια αγορά (Microsoft, Google, IBM) αλλά σε κάθε χώρα υπάρχουν δεκάδες άλλοι μικρότεροι ανταγωνιστές τους.

Επομένως ένα πλαίσιο ορθών πρακτικών στη διαχείριση της ασφάλειας κάθε υποδομής ΥΝ περιλαμβάνει:

- Τον ορισμό διευθύνουσας επιτροπής ασφάλειας για την επίβλεψη της υλοποίησης των μέτρων ασφάλειας, της συμμόρφωσης με πρότυπα και κανονισμούς αλλά και την νομοθεσία στις χώρες στις οποίες λειτουργούν τα κέντρα δεδομένων του οργανισμού.
- Ολοκληρωμένο σύστημα διαχείρισης κινδύνων (προσδιορισμός των πληροφοριακών αγαθών σε επίπεδο υποδομής, δεδομένων, εφαρμογών και υπηρεσιών, έλεγχος των επιμέρους πολιτικών ασφάλειας για την διασφάλιση της εμπιστευτικότητας, ακεραιότητας, διαθεσιμότητας των απόρρητων δεδομένων).
- Έλεγχος εικονικών μηχανών μέσω μηχανισμών παρόμοιων με αυτών που εφαρμόζουν προγράμματα προστασίας από ιούς ή κακόβουλα προγράμματα στο περιβάλλον ενός φυσικού υπολογιστή (πχ sandbox προγράμματα). Τα προγράμματα διαχείρισης και εποπτείας των εικονικών μηχανών (Vmware, HyperV) θα πρέπει να εξελιχθούν για να εντάξουν σαφείς διαδικασίες δοκιμαστικής λειτουργίας των εικονικών μηχανών πριν την παραγωγική τους λειτουργία αλλά και τον χρονοπρογραμματισμό πραγματοποίησης

ελέγχων στις μηχανές αυτές (πχ μετακίνηση στο “sandbox” του διακομιστή για ανίχνευση ευπαθειών).

- Διαχείριση της πρόσβασης των χρηστών μέσω νέων μηχανισμών ελέγχου και διαχείρισης της πρόσβασης σε δεδομένα και μηχανές με δυναμικό τρόπο (dynamic role based access control) και τηρώντας την αρχή της «ελάχιστης πρόσβασης».
- Η ασφάλεια των δεδομένων που συναλλάσσονται μεταξύ χρηστών και εφαρμογών ή στο εσωτερικό των συστημάτων μπορεί να διασφαλιστεί με ένα ολοκληρωμένο πρότυπο κρυπτογράφησης. Στη πρώτη φάση λειτουργίας των πλατφόρμων ΥΝ αποτελούσε πρόκληση η δημιουργία υποδομής τεράστιων χώρων αποθήκευσης για την κάλυψη της υψηλής ζήτησης για φθηνή χωρητικότητα δεδομένων και εφαρμογών. Σε μία δεύτερη φάση η νέα πρόκληση είναι η εκτέλεση διαδικασιών κρυπτογράφησης και αποκρυπτογράφησης σε κάθε στάδιο μετακίνησης δεδομένων ή ακόμα και εικονικών μηχανών (πχ από το χώρο αποθήκευσης τους στη μνήμη του διακομιστή) διατηρώντας ταυτόχρονα υψηλή ταχύτητα και αποδοτικότητα.

Εξετάζοντας την περίπτωση της VSPEX cloud υποδομής της EMC αναλύθηκαν οι κίνδυνοι που μπορεί να επηρεάσουν τη σύγχρονη υποδομής των υπηρεσιών ΥΝ που προσφέρει η εταιρία κυρίως σε χαμηλό επίπεδο (IaaS). Στην αρχική υπόθεση για το αν υπάρχουν θεμελιώδη εμπόδια στο να γίνει η συγκεκριμένη πλατφόρμα Υπολογιστικού Νέφους όσο ασφαλής όσο μία υπολογιστική υποδομή στο τοπικό περιβάλλον ενός πελάτη της EMC, η ανάλυση με τη βοήθεια της τεχνογνωσίας ενός επιθεωρητή Συστημάτων Διαχείρισης Ασφάλειας (ISO 27001 Auditor) έδειξε τα παρακάτω:

1. Ο οργανισμός έχει κάνει μία σημαντική επένδυση για τη φυσική ασφάλεια, την προστασία των δεδομένων των πελατών από φυσικές καταστροφές, και τη διασφάλιση της εμπιστευτικότητας, διαθεσιμότητας και ακεραιότητας των δεδομένων τους.
2. Απαιτείται περισσότερη διαφάνεια στον τρόπο με τον οποίο διασφαλίζει το απόρρητο των προσωπικών δεδομένων των χρηστών, τη πολιτική πρόσβασης χρηστών και τη πολιτική κρυπτογράφησης των δεδομένων που εφαρμόζει. Στους συγκεκριμένους τομείς είχαν διαπιστωθεί και σοβαρές ευπάθειες κατά το παρελθόν. Επιπρόσθετα η εταιρία έχει το πλεονέκτημα του ελέγχου ενός σημαντικού οργανισμού παροχής υπηρεσιών κρυπτογράφησης παγκοσμίως, της RSA. Μέσω της τελευταίας θα μπορεί να εφαρμόσει ένα νέο φάσμα μέτρων ασφάλειας που να περιλαμβάνει δυναμικό έλεγχο της πρόσβασης χρηστών (dynamic role based access control), κρυπτογράφηση των δεδομένων και εικονικών μηχανών κατά την μετακίνηση τους από τον χώρο αποθήκευσης στην μνήμη και το αντίστροφο.

Στη παραπάνω ανάλυση εφαρμόστηκε η μια παραλλαγή της μεθοδολογίας της CRAMM. Η μεθοδολογία αυτή όπως και κάθε άλλη αντίστοιχη μεθοδολογία απαιτεί την συλλογή δεδομένων κάνοντας συνήθως μία επί τόπου ανασκόπηση και αξιολόγηση ενός συστήματος διαχείρισης ασφάλειας. Με άλλα λόγια έχουν σχεδιαστεί για την εφαρμογή τους σε υποδομές πληροφοριακών συστημάτων στις οποίες ο επιθεωρητής έχει απευθείας πρόσβαση. Αυτό είναι δύσκολο να συμβεί στην περίπτωση των κατανεμημένων πληροφοριακών υποδομών που ορίζουν ένα ΥΝ (πχ τα κέντρα δεδομένων βρίσκονται σε διαφορετικά σημεία του πλανήτη) κυρίως αν οι πελάτες επιδιώκουν την επιθεώρηση τους. Απαιτείται επέκταση αυτών των μεθόδων για να λάβουν υπόψη ένα άλλο τρόπο συλλογής και επεξεργασίας δεδομένων σχετικά με την ασφάλεια οργανισμών που δραστηριοποιούνται σε αυτή τη βιομηχανία.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Brodkin, J., 2008. *Gartner: Seven cloud-computing security risks.* [Online]
Available at: http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853
[Accessed 14 March 2014].

EMC, 2014. *VMware vSphere 5.1 for 50 and 100 Virtual Machines.* [Online]
Available at: http://www.emc.com/collateral/technical-documentation/h11328-vspex-pi-pc-vmw-vnxe.pdf
[Accessed 2 May 2014].

Garrett, B., Choinski, V. & Dolan, K., 2013. *EMC IT: Leading the Transformation,* s.l.: The Enterprise Strategy Group.

Gruschka, N. ; NEC Eur. Ltd., Heidelberg, Germany ; Jensen, M, 2010. *Attack Surfaces:A Taxonomy for Attacks on Cloud Services.* Miami, FL, IEEE, pp. 276 - 279.

Hogberg, D., 2012. *An Applied Evaluation and Assessment of Cloud Computing Platforms,* UMEA SWEDEN: Umea University.

Jensen, M. ; Horst Gortz; Schwenk, J. ; Gruschka, N. ; Iacono, L.L., 2009. *On Technical Security Issues in Cloud Computing.* Bangalore, IEEE, pp. 109-116.

Kai Hwang ; Kulkareni, S. ; Hu, Yue , 2009. *Cloud Security with Virtualized Defense and Reputation-Based Trust Mangement.* Chengdu , IEEE.

Khan, K.M. ; Malluhi, Q., 2010. Establishing Trust in Cloud Computing. *IT Professional,* 12(5), pp. 20-27.

Oracle, 2011. *Oracle Cloud Computing.* [Online]
Available at: http://www.oracle.com/us/solutions/cloud/overview/index.html
[Accessed 09 04 2014].

Perry, R., & Hendrick, S., 2012. *The Business Value of Amazon Web Services Accelerates Over Time,* s.l.: IDC.

Rocha, F. ; Abreu, S. ; Correia, M., 2011. The Final Frontier: Confidentiality and Privacy in the Cloud. *Computer, IEEE,* 44(9), pp. 44-50.

Sato, H. ; Univ. of Tokyo, Tokyo, Japan ; Kanai, A. ; Tanimoto, S., 2010. *A Cloud Trust Model in a Security Aware Cloud.* Seoul, IEEE.

Takabi, H;Joshi, J.B.D.;Gail-Joon Ahn, 2010. Security and Privacy Challenges in Cloud Computing Environments. *Security & Privacy, IEEE ,* 8(6), pp. 24-31.

Tharam Dillon, Chen Wu, Elizabeth Chang , 2010. *Cloud Computing: Issues and Challenges.* Washington, DC, IEEE Computer Society, pp. 27-33.

Wenjuan Li, Lingdi Ping, 2009. Trust Model to Enhance Security and Interoperability of Cloud Environment. *Lecture Notes in Computer Science ,* Volume 5931, pp. 69-79.