Κατανεμημενα Συστηματα και Υπολογιστικα Νεφη

Δ.Δ. ΒΕΡΓΑΔΟΣ

Θ. ΜΑΥΡΟΕΙΔΑΚΟΣ

Τεχνολογία Υπολογιστικού Νέφους

- Η τεχνολογία του υπολογιστικού νέφους προσφέρει εικονικοποιημένους πόρους,
  - όπως αποθηκευτικός χώρος και διακομιστές
  - οι οποίοι είναι διασυνδεδεμένοι μεταξύ τους χρησιμοποιώντας αρχιτεκτονική,
  - η οποία επιτρέπει την παροχή νέων δυνατοτήτων στους τελικούς χρήστες.
- Το πλήθος των δυνατοτήτων τις οποίες προσφέρει το υπολογιστικό νέφος καλύπτει
  - τις ήδη υπάρχουσες,
  - αλλά και μελλοντικές ανάγκες τόσο της κοινωνίας όσο και της βιομηχανίας.

Τεχνολογία Υπολογιστικού Νέφους

- Το πλήθος των νέων δυνατοτήτων δημιουργεί προκλήσεις,
  - τις οποίες ο πάροχος του υπολογιστικού νέφους είναι υπεύθυνος να αντιμετωπίσει,
  - ώστε να ελαχιστοποιηθούν τα προβλήματα και οι απειλές που δημιουργούνται σε επίπεδο ασφάλειας δεδομένων.

Τεχνολογία Υπολογιστικού Νέφους

- Το υπολογιστικό νέφος όπως ορίζεται από το Διεθνή Ινστιτούτο Προτύπων και Τεχνολογίας (NIST),
  - αποτελεί ένα μοντέλο το οποίο καθιστά δυνατή τη κατ' απαίτηση πρόσβαση μέσω ενός δικτύου σε μοιραζόμενους και διαρθρώσιμους πόρους
  - οι οποίοι είναι σε θέση να γίνουν λειτουργικοί με ελάχιστη διαχείριση.
- Το NIST είναι υπεύθυνο για τη δημιουργία προτύπων, κατευθυντήριων οδηγιών και αναγκαίων προϋποθέσεων ως προς τη χρήση και εφαρμογή νέων τεχνολογιών.

Τεχνολογία Υπολογιστικού Νέφους

- Το NIST ορίζει πέντε βασικά χαρακτηριστικά του μοντέλου του υπολογιστικού νέφους:
  - α) κατ’ απαίτηση αυτοεξυπηρέτηση,
  - β) ευρεία δικτυακή πρόσβαση,
  - γ) ομαδοποίηση πόρων,
  - δ) ελαστικότητα και
  - ε) μετρούμενη υπηρεσία.

Τεχνολογία Υπολογιστικού Νέφους

- Η κατ’ απαίτηση αυτοεξυπηρέτηση αναφέρεται
  - στην αυτόματη παροχή πόρων στο τελικό χρήστη χωρίς να είναι αναγκαία η επέμβαση φυσικού προσώπου ώστε να πραγματοποιηθεί.
- Η ευρεία δικτυακή πρόσβαση αναφέρεται στη
  - δυνατότητα των υπηρεσιών να είναι διαθέσιμες στους τελικούς χρήστες μέσω του διαδικτύου ανεξάρτητα από το μέσο που χρησιμοποιείται.
- Η ομαδοποίηση πόρων αναφέρεται
  - στο πλήθος των εικονικοποιημένων οι οποίοι μπορούν να διατεθούν στους χρήστες σύμφωνα με τις ανάγκες που υπάρχουν.

Τεχνολογία Υπολογιστικού Νέφους

- Η ελαστικότητα αναφέρεται
  - στις δυνατότητες οι οποίες παρέχονται στους τελικούς χρήστες για την διαχείριση των διανεμόμενων πόρων.
- Η μετρούμενη υπηρεσία
  - αναφέρεται στα συστήματα τα οποία ελέγχουν και βελτιστοποιούν τους πόρους σύμφωνα με το τύπο της υπηρεσίας που παρέχεται.

Τεχνολογία Υπολογιστικού Νέφους

- Οι υπηρεσίες οι οποίες προσφέρονται μέσω του υπολογιστικού νέφους χαρακτηρίζονται
  - από τη διαθεσιμότητα,
  - τη κλιμακοθετησιμότητα,
  - την ευελιξία,
  - την ανθεκτικότητα και
  - την ακεραιότητα.

Τεχνολογία Υπολογιστικού Νέφους

- Το υπολογιστικό νέφος λειτουργεί και διαχειρίζεται από τρείς δράστες:
  - ο πελάτης,
  - ο πάροχος και
  - τρίτο μέρος επιθεώρησης(third-party).
- Ο πελάτης είναι μια οντότητα η οποία χρησιμοποιεί τις υπηρεσίες οι οποίες παρέχονται από το πάροχο του υπολογιστικού νέφους.
- Ο πελάτης προκειμένου να ορίσει τις απαιτήσεις του ως προς τη λειτουργία και χρήση της παρεχόμενης υπηρεσίας χρησιμοποιεί συμφωνία στάθμης υπηρεσίας(SLA).

Τεχνολογία Υπολογιστικού Νέφους

- Ο πάροχος είναι υπεύθυνος για την εκπλήρωση όσων ορίζονται στη συμφωνία στάθμης υπηρεσίας και την επίτευξη των προβλεπόμενων στόχων οι οποίοι προκύπτουν από αυτήν.
- Ο πάροχος του υπολογιστικού νέφους είναι υπεύθυνος για τη διαθεσιμότητα της παρεχόμενης υπηρεσίας στους τελικούς πελάτες.
- Ο πάροχος διαχειρίζεται την υποδομή του υπολογιστικού νέφους μέσω της οποίας παρέχονται οι υπηρεσίες.

Τεχνολογία Υπολογιστικού Νέφους

- Στις αρμοδιότητες του παρόχου είναι
  - η έκθεση της υπηρεσίας,
  - η συντήρηση και η συνεχής ενημέρωση των πόρων οι οποίοι συντελούν στην λειτουργία του παρόχου,
  - η ασφάλεια τόσο των εγκαταστάσεων όσο και των δεδομένων,
    - που διαχειρίζεται και το απόρρητο των προσωπικών πληροφοριών των φυσικών ατόμων που χρησιμοποιούν τις παρεχόμενες υπηρεσίες.

Τεχνολογία Υπολογιστικού Νέφους

- Το τρίτο μέρος επιθεώρησης πρόκειται
  - για μια ομάδα ατόμων η οποία έχει δυνατότητες που υπερέχουν των πελατών και
  - κύριο έργο τους αποτελεί η ανεύρεση και αντιμετώπιση απειλών.
- Τρίτο μέρος επιθεώρησης αποτελούν συνήθως ένας οργανισμός προτυποποίησης ή μια κυβερνητική αρχή,
  - οι οποίοι ελέγχουν κατά πόσο ένας πάροχος ικανοποιεί όλες τις ποιοτικές απαιτήσεις που πρέπει να πληρούνται ώστε να λειτουργεί με ασφάλεια η υποδομή του υπολογιστικού νέφους.

Μοντέλα Εξάπλωσης

- Οι υπηρεσίες του υπολογιστικού νέφους μπορούν να γίνουν διαθέσιμες στους τελικούς χρήστες μέσω τεσσάρων μοντέλων εξάπλωσης(deployment models).
- Τα τέσσερα μοντέλα είναι
  - το δημόσιο(public),
  - το ιδιωτικό(private),
  - το κοινοτικό(community) και
  - το υβριδικό(hybrid).
- Τα συγκεκριμένα μοντέλα ορίζονται από το NIST και περιγράφουν την σχέση μεταξύ των παρόχων και των χρηστών.

Μοντέλα Εξάπλωσης

- Στο δημόσιο υπολογιστικό νέφος, η υποδομή προβλέπεται για ανοιχτή χρήση από τους τελικούς χρήστες.
- Ο πάροχος διανέμει τους πόρους μέσω μιας υπηρεσίας χωρίς χρέωση επί της χρήσης.
- Το δημόσιο υπολογιστικό νέφος υπερέχει ως προς την κλιμακοθετησιμότητα, την απλότητα και του κόστους της παρεχόμενης υπηρεσίας έναντι του ιδιωτικού υπολογιστικού νέφους.

Μοντέλα Εξάπλωσης

- Το δημόσιο υπολογιστικό νέφος δε παρέχει κατάλληλο επίπεδο ασφαλείας για την αντιμετώπιση των υφιστάμενων απειλών.
- Έτσι, θα πρέπει να αποφεύγεται η αποθήκευση και διαχείριση ευαίσθητων δεδομένων όπως
  - φορολογικές δηλώσεις και έγγραφα τα οποία περιέχουν προσωπικές πληροφορίες όπως ΑΜΚΑ και ΑΦΜ.

Μοντέλα Εξάπλωσης

- Στο ιδιωτικό υπολογιστικό νέφος, η υποδομή προβλέπεται
  - για αποκλειστική χρήση από έναν οργανισμό ή επιχείρηση και
  - περιλαμβάνει περιορισμένο πλήθος χρηστών.
- Η υποδομή λειτουργεί και διαχειρίζεται από τον οργανισμό ή την επιχείρηση και
  - κατασκευάζεται ώστε να αντιμετωπίζει απειλές που παρουσιάζονται.
- Στο κοινοτικό υπολογιστικό νέφος,
  - η υποδομή προβλέπεται για αποκλειστική χρήση από μια συγκεκριμένη κοινότητα ατόμων οι οποίοι έχουν κοινές απαιτήσεις.
- Το κοινοτικό υπολογιστικό νέφος ανήκει, λειτουργεί και διαχειρίζεται από την ίδια τη κοινότητα ή από τρίτους.

Μοντέλα Εξάπλωσης

- Στο υβριδικό υπολογιστικό νέφος, η υποδομή κατασκευάζεται από τη σύνθεση τουλάχιστον δύο διαφορετικών υποδομών (δημόσιο, ιδιωτικό, κοινοτικό).
- Η κατάλληλη τεχνολογία χρησιμοποιείται προκειμένου να συνδεθούν δύο διαφορετικές υποδομές σε μια νέα.
- Με αυτόν τον τρόπο αθροίζονται οι δυνατότητες των υποδομών που επιλέγονται και δημιουργείται μια βελτιωμένη.
- Ιδανικά στο υβριδικό υπολογιστικό νέφους θα μπορούσαν να ληφθούν οι δυνατότητες του δημόσιου και να συνδυαστούν με δυνατότητες του ιδιωτικού όπως το βελτιωμένο επίπεδο ασφάλειας.

Μοντέλα Υπηρεσιών

- Η τεχνολογία του υπολογιστικού νέφους έχει την δυνατότητα παροχής τριών τύπων υπηρεσιών.
- Οι συγκεκριμένοι κύριοι τύποι υπηρεσιών είναι
  - IaaS,
  - PaaS και
  - SaaS.

Μοντέλα Υπηρεσιών

- Ο πρώτος τύπος υπηρεσιών είναι ο SaaS
  - κατά τον οποίο η διανεμόμενη υπηρεσία είναι μια εφαρμογή της οποίας το λογισμικό λειτουργεί και στεγάζεται στην υποδομή του παρόχου.
- Οι πελάτες δεν διαχειρίζονται τις εφαρμογές και δεν έχουν τη δυνατότητα επέμβασης στο τρόπο λειτουργίας τους.

Μοντέλα Υπηρεσιών

- Επιπλέον, οι πελάτες δε φέρουν ευθύνη
  - για το hardware(hardware) το οποίο χρησιμοποιείται από αυτές
  - αλλά ούτε και για το λειτουργικό σύστημα και περιβάλλον μέσα στο οποίο πραγματοποιούνται οι δράσεις τους.
- Οι εφαρμογές του υπολογιστικού νέφους είναι προσβάσιμες στους πελάτες μέσω ενός περιηγητή ή μέσω ενός προγράμματος το οποίο εγκαθίσταται στο υπολογιστικό σύστημα του πελάτη και επικοινωνεί μέσω του διαδικτύου με τον πάροχο (Google Drive).

Μοντέλα Υπηρεσιών

- Για να αποκτήσει πρόσβαση στην εκάστοτε εφαρμογή υπολογιστικού νέφους
  - ο πελάτης, κρίνεται απαραίτητο να δημιουργήσει έναν λογαριασμό με προσωπικές πληροφορίες,
    - όπως ονοματεπώνυμο και λογαριασμό ηλεκτρονικού ταχυδρομείου.
- Χρησιμοποιώντας υπηρεσίες τύπου SaaS,
  - εξοικονομείται αποθηκευτικός χώρος και
  - επεξεργαστική ισχύ του τοπικού υπολογιστή αφού μεταφέρεται ο φόρτος εργασίας στους πόρους του παρόχου.

Μοντέλα Υπηρεσιών

- Με αυτόν τον τρόπο, μέσω εφαρμογών όπως είναι για παράδειγμα το Google Docs
  - παρέχεται η δυνατότητα επεξεργασίας και δημιουργίας αρχείων τύπου .doc και .xls χωρίς να υπάρχει η ανάγκη εγκατάστασης λογισμικού τύπου Microsoft Office.
- Έτσι, επιχειρήσεις και οργανισμοί έχουν τη δυνατότητα χρήσης υπολογιστικών συστημάτων ισχνού πελάτη(thin client)
  - μέσω των οποίων δεν θα μειώνεται η απόδοση των εργαζομένων και λόγω του μειωμένου κόστους τους,
  - θα εξοικονομούνται χρηματικοί πόροι οι οποίοι θα μπορούν να διατεθούν για διαφορετικές ανάγκες.

Μοντέλα Υπηρεσιών

- Ο δεύτερος τύπος υπηρεσιών είναι ο PaaS
  - κατά τον οποίο ο πάροχος δίνει τη δυνατότητα στους πελάτες να κατασκευάσουν και
  - στη συνέχεια να εκθέσουν τις εφαρμογές τους μέσω της υποδομής του υπολογιστικού νέφους.
- Οι εφαρμογές κατασκευάζονται σε γλώσσα προγραμματισμού και σε περιβάλλον ανάπτυξης τα οποία υποστηρίζονται από το πάροχο και επιλέγονται από τους πελάτες.

Μοντέλα Υπηρεσιών

- Η ιδέα πίσω από αυτόν το τύπο υπηρεσιών είναι
  - πως ο πελάτης έχει πρόσβαση σε πόρους ώστε να ολοκληρώσει την εφαρμογή του
  - με μόνη απαίτηση τη συγγραφή του πηγαίου κώδικα του λογισμικού το οποίο θα αποτελέσει το πυρήνα της εφαρμογής.

Μοντέλα Υπηρεσιών

- Σε αυτόν το τύπο υπηρεσιών ο πελάτης δεν έχει τη δυνατότητα ελέγχου της υποδομής του υπολογιστικού νέφους ,
  - όπως είναι για παράδειγμα η δικτυακή κίνηση των εσωτερικών δικτύων μέσω των οποίων επικοινωνούν οι διακομιστές, τα λειτουργικά συστήματα ή τον αποθηκευτικό χώρο.
- Ο μόνος χώρος στον οποίο μπορούν να πραγματοποιηθούν ρυθμίσεις από το πελάτη είναι η πλατφόρμα
  - στην οποία γράφεται ο πηγαίος κώδικας της εφαρμογής.

Μοντέλα Υπηρεσιών

- Ο πελάτης είναι υπεύθυνος για την ασφάλεια του κώδικα της εφαρμογής έναντι επιθέσεων
  - τύπου υπερχείλισης ενδιαμέσου καταχωρητή
  - και συμβολοσειράς μορφοποίησης.
- Η παροχή του κατάλληλου επιπέδου ασφάλειας για τη πλατφόρμα και για τους πόρους οι οποίοι χρησιμοποιούνται από τις εφαρμογές είναι αρμοδιότητα του παρόχου.

Μοντέλα Υπηρεσιών

- Το μοντέλο υπηρεσιών PaaS
  - μειώνει τις ενέργειες οι οποίες πρέπει να εφαρμοστούν
  - και τις απαιτήσεις οι οποίες πρέπει να πληρούνται ώστε να γίνει διαθέσιμη μια εφαρμογή στο διαδίκτυο.
- Επιπλέον, αυξάνεται η παραγωγικότητα εφόσον ο εκπονητής της εφαρμογής επικεντρώνεται στη βελτίωση του κώδικα της εφαρμογής
  - χωρίς να ασχολείται με την κλιμακοθετησιμότητα ή τον αποθηκευτικό χώρο που θα χρειαστεί μελλοντικά η εφαρμογή.
- Υπηρεσίες τύπου PaaS είναι η AppScale, η Cloudera, η Google App Engine και η IBM Bluemix.

Μοντέλα Υπηρεσιών

- Ο τρίτος τύπος υπηρεσιών είναι ο IaaS.
- Σε αυτόν το τύπο υπηρεσιών ο πάροχος του υπολογιστικού νέφους προσφέρει εικονικοποιημένους πόρους
  - όπως είναι ο αποθηκευτικός χώρος, τείχη προστασίας, κατανεμητές φορτίου και την δυνατότητα διαχείρισης των εσωτερικών δικτύων μέσω των οποίων διασυνδέονται οι διακομιστές.
- Οι συγκεκριμένοι πόροι παρέχονται από το υπολογιστικό νέφος σύμφωνα με τις ανάγκες των πελατών.

Μοντέλα Υπηρεσιών

- Σε αυτόν τον τύπων υπηρεσιών, οι πελάτες είναι υπεύθυνοι
  - για τους εικονικοποιημένους πόρους,
  - για την διαχείριση του δικτύου στο οποίο είναι συνδεδεμένα τα εικονικά μηχανήματα
  - και για την εξισορρόπηση του φόρτου εργασίας, όμως δεν φέρουν ευθύνη για την φυσική ασφάλεια των πόρων.
- Έτσι, δεν ασχολούνται με θέματα πυρόσβεσης, υπερφόρτωσης του δικτύου ή διακοπής της ηλεκτρικής ισχύος.

Μοντέλα Υπηρεσιών

- Αναγκαία προϋπόθεση για τη χρήση αυτού του τύπου υπηρεσιών είναι
  - οι πελάτες να έχουν τις απαιτούμενες γνώσεις για την εγκατάσταση λειτουργικών συστημάτων και ρύθμιση του παρεχόμενου hardware.
- Υπηρεσίες τύπου IaaS αποτελούν
  - το Microsoft Azure,
  - το Google Compute Engine και
  - το vCloud Terremark.
- Το 2012 το πλήθος των υπηρεσιών διευρύνεται από 3 σε 5 από τον Διεθνή Οργανισμό Τηλεπικοινωνιών (ITU).

Μοντέλα Εξάπλωσης

- Οι δύο νέοι τύποι υπηρεσιών είναι οι:
  - Network-as-a-Service (NaaS) και
  - Communication-as-a-Service (CaaS).
- Ο πάροχος υπολογιστικού νέφους τύπου υπηρεσιών NaaS προσφέρει υπηρεσίες οι οποίες σχετίζονται με εικονικά δίκτυα.
- Αυτού του τύπου υπηρεσίες είναι
  - VPN,
  - εύρος κατ’ απαίτηση(BoD) και
  - εικονικοποίηση δικτύων κινητής τηλεφωνίας.

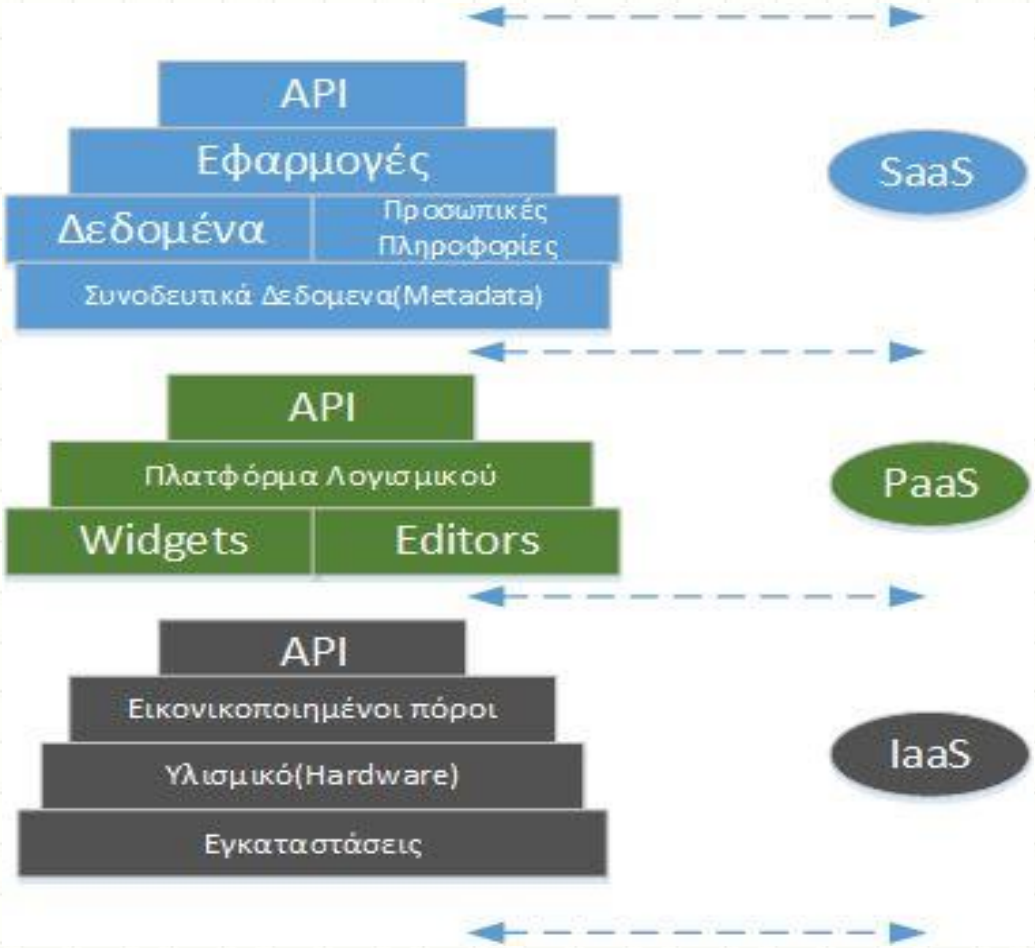
Μοντέλα Εξάπλωσης

- Η υπηρεσία VPN επιτρέπει
  - την αποστολή και λήψη δεδομένων διαμέσου δημοσίων και κοινόχρηστων δικτύων
  - αλλά με το επίπεδο ασφάλειας το οποίο παρέχεται στα ιδιωτικά δίκτυα.
- Με την έλευση των VOIP τεχνολογιών και εφαρμογών τηλεπικοινωνίας
  - καθίσταται αναγκαία η ύπαρξη ενός κέντρου αντιστοίχου των PBXs το οποίο θα εξυπηρετεί αυτού του τύπου τις τεχνολογίες.
- Το συγκεκριμένο κέντρο μπορεί να δημιουργηθεί και να διαχειρίζεται μέσω του μοντέλου CaaS.

Μοντέλα Εξάπλωσης

- Διαμέσου του τύπου υπηρεσιών CaaS, ένας οργανισμός ή μια επιχείρηση μπορούν να έχουν δικό τους αυτόνομο και ανεξάρτητο τηλεπικοινωνιακό κέντρο στο υπολογιστικό νέφος.
- Οι εργαζόμενοι του τμήματος τεχνολογίας πληροφοριών θα μπορούν
  - να ρυθμίζουν και
  - να διαχειρίζονται τις τηλεπικοινωνιακές εφαρμογές με ταχύτητα και ευκολία
  - εξοικονομώντας χρόνο τον οποίο θα μπορούν να διαθέτουν προς τη βελτίωση του επιπέδου ασφαλείας αυτών.

Πόροι Μοντέλων Υπηρεσιών



Θέματα Ασφάλειας στα Μοντέλα Υπηρεσιών

- Προτού αναλυθούν οι προκλήσεις ως προς τα θέματα ασφαλείας τα οποία υπάρχουν στο υπολογιστικό νέφος,
  - κρίνεται απαραίτητο να κατανοηθούν οι σχέσεις και οι εξαρτήσεις οι οποίες υπάρχουν μεταξύ των τριών μοντέλων υπηρεσιών.
- Τα μοντέλα SaaS και PaaS φιλοξενούνται στην υποδομή του υπολογιστικού νέφους από το μοντέλο IaaS.
- Οι απειλές και οι κίνδυνοι που υπάρχουν στο μοντέλο IaaS επαγωγικά υφίστανται και για τα άλλα δύο μοντέλα.

Θέματα Ασφάλειας στα Μοντέλα Υπηρεσιών

- Το μοντέλο PaaS παρέχει στους πελάτες μια πλατφόρμα η οποία δίνει τη δυνατότητα κατασκευής εφαρμογών SaaS.
- Η σχέση των δύο μοντέλων δημιουργεί μια ισχυρή εξάρτηση ως προς την ασφάλεια μεταξύ τους.
- Η συγκεκριμένη εξάρτηση έχει ως αποτέλεσμα οι εφαρμογές οι οποίες κατασκευάζονται στο μοντέλο PaaS να αποτελούνται από δύο επίπεδα ασφαλείας.

Θέματα Ασφάλειας στα Μοντέλα Υπηρεσιών

- Τα δύο επίπεδα αφορούν την ασφάλεια της πλατφόρμας και την ασφάλεια των δεδομένων της παρεχόμενης εφαρμογής SaaS.
- Λόγω των εξαρτήσεων που υπάρχουν μεταξύ των μοντέλων υπηρεσιών και του τρόπου λειτουργίας του υπολογιστικού νέφους,
  - κρίνεται απαραίτητο ο κάθε πάροχος υπηρεσιών να κατέχει υπό τον έλεγχό του και τα τρία μοντέλα.

Θέματα Ασφάλειας στα Μοντέλα Υπηρεσιών

- Με αυτόν το τρόπο, ο πάροχος
  - παρακολουθεί την λειτουργία τους και
  - αντιμετωπίζει απειλές οι οποίες παρουσιάζονται σε κάθε ένα και επηρεάζουν τα υπόλοιπα κατά την παροχή των υπηρεσιών.

Θέματα Ασφάλειας στα Μοντέλα Υπηρεσιών

- Σε διαφορετική περίπτωση όπου τρείς πάροχοι συνεργάζονται για τη παροχή των υπηρεσιών
  - τότε θα παρουσιάζονταν περιορισμοί.
- Ο κάθε πάροχος θα είχε υπό τον έλεγχό του ένα από τα μοντέλα υπηρεσιών και σε περίπτωση που πραγματοποιηθεί επιτυχής επίθεση σε ένα εξ' αυτών
  - τότε θα υπάρξουν συνέπειες σε όλα
  - με αποτέλεσμα να μην υπάρχει διαφάνεια ως προς το ποιός είναι υπεύθυνος για την αδυναμία παροχής των προσδοκώμενου επιπέδου υπηρεσιών.

Θέματα Ασφάλειας στα Μοντέλα Υπηρεσιών

- Το υπολογιστικό νέφος είναι μια τεχνολογία η οποία περιστοιχίζεται από στοιχεία
  - της επικοινωνίας RPC
  - των SDN δικτύων
  - του υπολογιστικού πλέγματος (grid computing) και
  - της πληροφορικής χρησιμότητας(utility computing)
  - τα οποία συνδυάζονται και γίνονται διαθέσιμα μέσω μιας νέας καινοτομικής αρχιτεκτονικής.
- Μέσω αυτής της αρχιτεκτονικής κατασκευάζεται το περιβάλλον υπολογιστικού νέφους
  - το οποίο δίνει πρόσβαση στους τελικούς χρήστες σε ένα πλήθος υπηρεσιών.

Θέματα Ασφάλειας στα Μοντέλα Υπηρεσιών

- Οι συγκεκριμένες υπηρεσίες χαρακτηρίζονται από δυνατότητες όπως:
  - διαθεσιμότητα,
  - ακεραιότητα,
  - ελαστικότητα και
  - κλιμακοθετησιμότητα.
- Ωστόσο, το πλήθος των δυνατοτήτων δημιουργεί απειλές και περιορισμούς
  - οι οποίοι σχετίζονται με τα δεδομένα και τις προσωπικές πληροφορίες των φυσικών προσώπων που χρησιμοποιούν τις υπηρεσίες.

Διαθεσιμότητα

- Η διαθεσιμότητα είναι η ιδιότητα ενός συστήματος ή υπηρεσίας να παραμένει προσβάσιμο και χρηστικό στους τελικούς χρήστες χωρίς διακοπή.
- Επιπλέον, η διαθεσιμότητα αναφέρεται
  - στην ικανότητα παροχής υπηρεσιών από ένα σύστημα
  - ακόμα κι όταν τα υποσυστήματα αυτού αντιμετωπίζουν προβλήματα.
- Οι περισσότερες υπηρεσίες οι οποίες παρέχονται επί του παρόντος δεν λειτουργούν σε μοιραζόμενη υποδομή όπως εκείνη του υπολογιστικού νέφους.

Διαθεσιμότητα

- Πρόκειται μια σχέση 1 προς 1
  - κατά την οποία η αποτυχία ενός στοιχείου του hardware, όπως για παράδειγμα ο αποθηκευτικός χώρος
  - θα έχει συνέπειες σε συγκεκριμένο μέρος της παρεχόμενης υπηρεσίας και θα είναι εφικτός ο προσδιορισμός του πλήθους χρηστών οι οποίοι θα αντιμετωπίσουν πρόβλημα.
- Αντιθέτως, το περιβάλλον του υπολογιστικού νέφους είναι κατασκευασμένο σε μοιραζόμενη υποδομή
  - με αποτέλεσμα η αποτυχία ενός στοιχείου του hardware
  - να έχει πολλαπλές επιπτώσεις σε διαφορετικές υπηρεσίες και σε διαφορετικούς πληθυσμούς χρηστών.

Διαθεσιμότητα

- Η διαθεσιμότητα δεν αποτελεί χαρακτηριστικό μόνο του λογισμικού αλλά και του hardware.
- Επιπλέον, οι πάροχοι υπηρεσιών υπολογιστικού νέφους κρίνεται απαραίτητο
  - να ορίζουν τους χρόνους επίλυσης και απόκρισης,
  - για την αντιμετώπιση προβλημάτων τα οποία σχετίζονται με τη διαθεσιμότητα μιας υπηρεσίας, στη συμφωνία στάθμης υπηρεσίας.
- Από τη πλευρά των παρόχων, το πλήθος των τελικών χρηστών οι οποίοι επηρεάζονται από την αποτυχία ενός συστήματος ή υπηρεσίας θα ορίζουν το επίπεδο δριμύτητας.

Διαθεσιμότητα

- Όσο περισσότεροι χρήστες χρησιμοποιούν μια υπηρεσία τόσο υψηλότερο θα είναι το επίπεδο δριμύτητας.
- Για κάθε επίπεδο δριμύτητας θα ορίζονται διαφορετικοί χρόνοι απόκρισης και επίλυσης.
- Σε περίπτωση που η αποτυχία ενός συστήματος επηρεάζει μόνο έναν χρήστη,
  - το επίπεδο δριμύτητας θα είναι χαμηλό
  - και οι χρόνοι θα έχουν μεγαλύτερη διάρκεια
  - δηλαδή ο χρόνος επίλυσης θα είναι για παράδειγμα 2 ώρες και ο χρόνος απόκρισης θα είναι 8 ώρες.

Διαθεσιμότητα

- Οι πάροχοι υπηρεσιών υπολογιστικού νέφους χρησιμοποιούν μετρήσιμα μεγέθη
  - για την υπολογισμό της διαθεσιμότητας
  - και την υποστήριξη την οποία βρίσκονται σε θέση να προσφέρουν.
- Τα συγκεκριμένα μεγέθη είναι
  - ο μέσος χρόνος ανάκτησης, MTTR
  - και ο μέσος χρόνος αποτυχίας MTTF.
- Η διαθεσιμότητα ορίζεται συνάρτηση των δύο μεγεθών από την ακόλουθη σχέση
- :

$$Διαθεσιμότητα = \frac{MTTF}{MTTF + MTTR}$$

Διαθεσιμότητα

- Ο μέσος χρόνος ανάκτησης είναι ίσος με τον χρόνο απόκρισης.
- Οι δύο μέσοι χρόνοι οι οποίοι ορίστηκαν παραπάνω
  - χρησιμοποιούνται από τους παρόχους για τη μέτρηση της αξιοπιστίας των συστημάτων που χρησιμοποιούνται.
- Το νέο μέγεθος το οποίο προκύπτει είναι ο μέσος χρόνος αξιοπιστίας, MTBF και ορίζεται από την ακόλουθη σχέση

$$MTBF = MTTF + MTTR$$

Διαθεσιμότητα

- Ο μέσος χρόνος αξιοπιστίας είναι το χρονικό διάστημα κατά το οποίο μια υπηρεσία θα διανέμεται φυσιολογικά μέχρι να αποτύχει.
- Ο μέσος χρόνος ανάκτησης είναι το χρονικό διάστημα το οποίο απαιτείται από το πάροχο
  - για την επιδιόρθωση της αποτυχίας
  - και την επαναφορά της υπηρεσίας στη κανονική της λειτουργία.

Διαθεσιμότητα

- Οι δύο χρόνοι θα πρέπει
  - να υπολογίζονται σύμφωνα με τα συστήματα τα οποία διαθέτουν οι πάροχοι
  - και από την ακόλουθη σχέση να υπολογίζεται η διαθεσιμότητα μιας υπηρεσίας.

$$Διαθεσιμότητα = \frac{MTBF}{MTBF + MTTR}$$

Διαθεσιμότητα

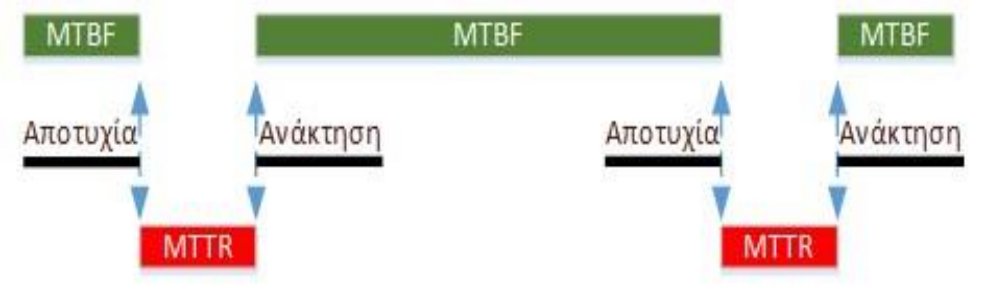
- Πρωταρχικός στόχος των παρόχων πρέπει να είναι
  - ο σχεδιασμός διαδικασιών και συστημάτων
  - τα οποία θα μειώνουν το χρόνο MTTR.
- Ιδανικά, κάθε περίπτωση αποτυχίας θα αντιμετωπιζόταν αυτόματα από την υποδομή χωρίς την επέμβαση του ανθρώπινου παράγοντα.
- Για να συμβεί αυτό, οι πάροχοι πρέπει να θέσουν σε εφαρμογή κατάλληλα συστήματα πλεονασμού.

Διαθεσιμότητα

- Τα συστήματα πλεονασμού σε περίπτωση αποτυχίας
  - θα απομονώνουν το στοιχείο που προκαλεί την αποτυχία
  - και θα το αντικαθιστούν από ένα εφεδρικό.
- Αυτό θα πρέπει να συμβαίνει εφόσον
  - ο χρόνος ο οποίος απαιτείται για να τεθεί σε λειτουργία ένα εφεδρικό σύστημα
  - είναι μικρότερος από το χρόνο επιδιόρθωσης του αρχικού συστήματος το οποίο προκαλεί την αποτυχία.
- Στην συνέχεια, το σύστημα θα επιδιορθώνεται και θα τίθεται σε λειτουργία χωρίς να επηρεάζεται η διαθεσιμότητα της παρεχόμενης υπηρεσίας.

Διαθεσιμότητα

- Ο χρόνος ο οποίος θα απαιτείται για να τεθεί σε εφαρμογή το εφεδρικό σύστημα θα ισούται με τον χρόνο MTTR.



MTBF-MTTR

Διαθεσιμότητα

- Στο υπολογιστικό νέφος ισχύει και εφαρμόζεται το θεώρημα CAP (όπως σε όλα τα κατανεμημένα(distributed) συστήματα).
- Σύμφωνα με το συγκεκριμένο θεώρημα
  - κάθε κατανεμημένο σύστημα είναι σε θέση να ικανοποιεί κάθε χρονική στιγμή δύο μόνο από τις ιδιότητες **συνοχής**, **διαθεσιμότητας** και **ανοχής διαμέρισης**.
- Η ιδιότητα συνοχής εκφράζει την ικανότητα των κόμβων ενός συστήματος να έχουν πρόσβαση στα ίδια δεδομένα.

Διαθεσιμότητα

- Η ιδιότητα ανοχής διαμέρισης
  - εκφράζει την ικανότητα του συστήματος να παραμένει λειτουργικό ένα σύστημα ανεξάρτητα από τις επιμέρους αποτυχίες υποσυστημάτων.
- Σύμφωνα τον Coda Hale, η ανοχή διαμέρισης είναι υποχρεωτική για όλα τα κατανεμημένα συστήματα,
  - έτσι οι πάροχοι πρέπει να επιλέξουν μεταξύ διαθεσιμότητας και συνοχής.

Διαθεσιμότητα

- Η επιλογή μεταξύ των ιδιοτήτων δεν είναι δυαδική
  - δηλαδή σε περίπτωση επιλογής της διαθεσιμότητας ότι θα υπάρχει μειωμένη συνοχή και το αντίστροφο.
- Η επιλογή της ιδιότητας είναι αναγκαίο να πραγματοποιείται
  - σύμφωνα με το τύπο της παρεχόμενης υπηρεσίας
  - και το τρόπο λειτουργίας της

Διαθεσιμότητα

- Για παράδειγμα, η εταιρία Facebook λόγω του πλήθους χρηστών έχει υιοθετήσει μοντέλο το οποίο αναδεικνύει τη διαθεσιμότητα της υπηρεσίας έναντι της συνοχής.
- Παράμετροι οι οποίοι μπορούν να λειτουργήσουν βοηθητικά για την επιλογή του κατάλληλου μοντέλου από ένα πάροχο είναι
  - ο τύπος της υπηρεσίας,
  - ο όγκος και τύπος των δεδομένων
  - και το είδος και πλήθος των χρηστών.
- Η κατασκευή μοντέλων τα οποία αναδεικνύουν τη διαθεσιμότητα έχουν επιλεχθεί από εταιρίες όπως Facebook, Dropbox και Google.

Διαθεσιμότητα

- Η διαθεσιμότητα ενός συστήματος και μιας υπηρεσίας επηρεάζεται από ρήγματα ασφαλείας.
- Οι επιθέσεις άρνησης παροχής υπηρεσιών έχουν ως στόχο τη βλάβη της διαθεσιμότητας αφού καταστούν μη λειτουργική τη παρεχόμενη υπηρεσία.
- Οι συγκεκριμένες επιθέσεις στοχεύουν κρίσιμους πόρους χωρίς τους οποίους η υπηρεσία δε μπορεί να παρέχεται απρόσκοπτα.

Διαθεσιμότητα

- Οι μέθοδοι οι οποίες χρησιμοποιούνται καθώς και τα αντίστοιχα εργαλεία για αυτόν το τύπο επιθέσεων έχουν πλέον γίνει εξειδικευμένα και αποτελεσματικά σε τέτοιο βαθμό
  - που οι πραγματικοί επιτιθέμενοι είναι πολύ δύσκολο να ανιχνευθούν
  - ενώ οι τεχνικές άμυνας δεν μπορούν να αντισταθούν σε επιθέσεις ευρείας κλίμακας.
- Οι επιθέσεις άρνησης παροχής υπηρεσιών μπορούν να κατηγοριοποιηθούν βάση του είδους του πόρου που καταναλώνουν.

Διαθεσιμότητα

- Υπάρχουν οι επιθέσεις εσωτερικού πόρου κατά τις οποίες
  - πραγματοποιείται πλημμύρα πακέτων SYN προς το σύστημα-στόχο
  - και οι επιθέσεις οι οποίες καταναλώνουν πόρους μετάδοσης δεδομένων.
- Στο δεύτερο είδος επιθέσεων, ο επιτιθέμενος αποκτά τον έλεγχο πολλαπλών κόμβων στο διαδίκτυο
  - στους οποίους υπαγορεύει να στείλουν πακέτα ICMP τύπου ECHO σε ένα σύνολο κόμβων
  - οι οποίοι δρουν ως ανακλαστήρες
  - όπου όμως τα πακέτα εμφανίζουν ως IP διεύθυνσης αποστολέα την διεύθυνση του συστήματος-στόχου.

Διαθεσιμότητα

- Στη συνέχεια οι κόμβοι-ανακλαστήρες
  - λαμβάνουν πολλαπλές μη γνήσιες αιτήσεις
  - και απαντούν στέλνοντας πακέτα υπό τη μορφή ηχούς στο σύστημα το οποίο θεωρούν ως αποστολέα των πακέτων δηλαδή το σύστημα-στόχο.
- Το σύστημα-στόχος πλημμυρίζει με πακέτα με αποτέλεσμα να υπάρχει χωρητικότητα για μετάδοση δεδομένων τα οποία αποτελούν την νόμιμη κίνηση του δικτύου.
- Σε αυτό το είδος επίθεσης,
  - ο επιτιθέμενος υπαγορεύει στους κόμβους που ελέγχει να αποστείλουν πακέτα ICMP με διεύθυνση αποστολέα, τη δημόσια διεύθυνση (public IP)
  - μέσω της οποίας διανέμεται μια υπηρεσία υπολογιστικού νέφους.

Διαθεσιμότητα

- Οι επιθέσεις άρνησης παροχής υπηρεσιών μπορούν να κατηγοριοποιηθούν ως
  - άμεσες
  - ή ανακλαστικές.
- Στις άμεσες επιθέσεις άρνησης παροχής υπηρεσιών,
  - ο επιτιθέμενος εμφυτεύει κακόβουλο λογισμικό σε δύο είδη συστημάτων(zombie),
  - τα κύρια(master) και τα δευτερεύοντα(slaves), τα οποία είναι κατανεμημένα σε διάφορα σημεία στο διαδίκτυο.

Διαθεσιμότητα

- Στις ανακλαστικές επιθέσεις άρνησης παροχής υπηρεσιών, προστίθεται ένα ακόμη είδος συστημάτων,
  - οι ανακλαστήρες οι οποίοι ελέγχονται μέσω των δευτερευόντων συστημάτων
  - και δημιουργούν πλημμύρα πακέτων προς το σύστημα-στόχο.
- Τα δύο τελευταία είδη επιθέσεων καταστούν πολύ δύσκολη την διαδικασία ανίχνευσης του επιτιθέμενου.

Διαθεσιμότητα

- Η υποδομή του υπολογιστικού νέφους λειτουργεί με τρόπο κατά τον οποίο προσπαθεί να ικανοποιήσει όλες τις αιτήσεις που δέχεται.
- Αυτό επιτυγχάνεται μέσω της δυνατότητας της κλιμακοθετησιμότητας των υπηρεσιών του υπολογιστικού νέφους.
- Έτσι, η υποδομή των παρόχων διευκολύνει τις επιθέσεις άρνησης παροχής υπηρεσιών να επιτύχουν
  - εφόσον η υπηρεσία προκειμένου να ικανοποιήσει τις κακόβουλες αιτήσεις του επιτιθέμενου θέτει σε εφαρμογή περισσότερους πόρους.

Διαθεσιμότητα

- Αυτό έχει ως αποτέλεσμα να προκαλείται βλάβη στην υποδομή του παρόχου,
  - πέραν της αρχικής υπηρεσίας η οποία δέχτηκε την επίθεση.
- Συνεπώς, επηρεάζεται η διαθεσιμότητα όλων των υπηρεσιών οι οποίες διανέμονται από το πάροχο.
- Επιθέσεις αυτού του τύπου μπορούν να χρησιμοποιηθούν για την επίθεση σε εσωτερικές υπηρεσίες του υπολογιστικού νέφους.

Διαθεσιμότητα

- Για παράδειγμα, η εταιρία Amazon,σύμφωνα με τα επίσημα έγγραφα τα οποία έχει εκδώσει για τη λειτουργία της υποδομής της,
  - είναι σε θέση να προστατεύσει τους πελάτες της από επιθέσεις άρνησης παροχής υπηρεσιών.

Διαθεσιμότητα

- Ωστόσο, οι πόροι της εταιρίας και ο τρόπος κατά τον οποίο αλληλεπιδρούν διευκολύνουν τη πραγματοποίηση αυτού του τύπου επιθέσεων μέσω της υπηρεσίας τύπου IaaS, EC2.
- Πιο συγκεκριμένα, σε περίπτωση που ένας χρήστης
  - κατασκευάσει 20 λογαριασμούς
  - και σε κάθε έναν κατασκευάσει 20 εικονικά μηχανήματα
  - και παράλληλα συνεχίσει την κατασκευή εικονικών μηχανημάτων μέσω αυτών των λογαριασμών
  - τότε ύστερα από συγκεκριμένο χρονικό διάστημα θα έχει κατασκευάσει 800 δισεκατομμύρια εικονικά μηχανήματα τα οποία θα προκαλέσουν δυσλειτουργία της υποδομής της Amazon.

Διαθεσιμότητα

- Αυτό συμβαίνει κυρίως γιατί η εταιρία δεν έχει προβλέψει την αντιμετώπιση αυτών των συμβάντων
  - με τη κατασκευή ενός συστήματος το οποίο θα περιορίζει του διανεμόμενους πόρους ανά χρήστη.
- Επιθέσεις αυτού του τύπου μπορούν να επιτευχθούν μέσω της χρήσης εικονικών συστημάτων από την υποδομή ενός παρόχου
  - με στόχο συγκεκριμένη υπηρεσία η οποία παρέχεται από την υποδομή ενός δεύτερου παρόχου.

Διαθεσιμότητα

- Εκτός των παραπάνω, η διαθεσιμότητα μιας υπηρεσίας επηρεάζεται
  - από βλάβες του εξοπλισμού των παρόχων και
  - από φυσικές καταστροφές.
- Βλάβη στον εξοπλισμό του παρόχου μπορεί να προκληθεί από υπερφόρτωση του δικτύου ηλεκτρικής ισχύος
- Φυσική καταστροφή μπορεί να αποτελέσει σεισμική δραστηριότητα
  - η οποία θα οδηγήσει στη καταστροφή εγκαταστάσεων του παρόχου
  - και κατά συνέπεια καταστροφή των στεγαζόμενων συστημάτων.

Διαθεσιμότητα

- Επιπλέον, σε περίπτωση χρεωκοπίας του παρόχου επηρεάζεται
  - η διαθεσιμότητα τόσο των παρεχόμενων υπηρεσιών
  - όσο και των δεδομένων των φυσικών προσώπων.
- Για την αντιμετώπιση των παραπάνω καταστάσεων και την αποφυγή βλάβης της διαθεσιμότητα μιας υπηρεσίας ή των δεδομένων
  - θα πρέπει να ορίζονται σχέδια έκτακτης ανάγκης στη συμφωνία στάθμης υπηρεσίας.
- Στη συμφωνία στάθμης υπηρεσίας
  - θα καθορίζονται ακόμη οι περιορισμοί ως προς τη διαθεσιμότητα
  - οι οποίοι είναι απαραίτητοι για τη διανομή του προσδοκώμενου επιπέδου υπηρεσιών.

Διαθεσιμότητα

- Αυτού του είδους περιορισμοί θα αποτελούν οι προγραμματισμένες διακοπές της διανεμόμενης υπηρεσίας
  - ώστε να αναβαθμιστούν οι χρησιμοποιούμενοι πόροι.
- Μέσω κατάλληλης συμφωνίας στάθμης υπηρεσίας θα μπορούσε να οριστεί
  - τρόπος για την παροχή των διανεμόμενων υπηρεσιών κατά τα συγκεκριμένα χρονικά διαστήματα
  - χωρίς να επηρεάζεται η διαθεσιμότητα αυτών.

Διαθεσιμότητα

- Εάν η υποδομή των παρόχων υπολογιστικού νέφους κατασκευαστεί με γνώμονα την αποτυχία της,
  - δηλαδή λαμβάνοντας ως δεδομένο πως σε κάποια χρονική στιγμή τα συστήματα τα οποία την υποστηρίζουν
  - θα αρχίσουν να αποτυγχάνουν τότε θα πρέπει να κατασκευαστεί το κατάλληλο σύστημα πλεονασμού.
- Τα συστήματα πλεονασμού θα αντιμετωπίζουν αυτόματα τις αποτυχίες.
- Ο ανθρώπινος παράγοντας θα έχει τη δυνατότητα να επικεντρωθεί στην αντιμετώπιση απειλών και κινδύνων οι οποίοι σχετίζονται με την ασφάλεια της παρεχόμενης υπηρεσίας.

Κλιμακοθετησιμότητα

- Η κλιμακοθετησιμότητα είναι
  - η ικανότητα των υπηρεσιών του υπολογιστικού νέφους να εξυπηρετούν τον φόρτο εργασίας κάθε χρονική στιγμή με το κατάλληλο πλήθος πόρων.
- Αυτό επιτυγχάνεται μέσω κλιμάκωσης των χρησιμοποιούμενων πόρων.
- Από την μεριά του πελάτη, η κλιμακοθετησιμότητα αντιλαμβάνεται
  - ως η ικανότητα η οποία του παρέχεται να χρησιμοποιεί ένα μεγάλο πλήθος πόρων οι οποίοι του παρέχονται κατά δική του βούληση.

Κλιμακοθετησιμότητα

- Από την μεριά του παρόχου της υπηρεσίας υπολογιστικού νέφους,
  - η κλιμακοθετησιμότητα είναι η υποχρέωση η οποία του έχει ανατεθεί για την ικανοποίηση των αναγκών των χρηστών χωρίς να δημιουργούνται περιορισμοί.
- Η υποδομή του υπολογιστικού νέφους έχει την ικανότητα κλιμάκωσης
  - οριζόντια(scale out) και
  - κάθετα(scale up)
  - σύμφωνα με το είδος της παρεχόμενης υπηρεσίας και τις απαιτήσεις των χρηστών της.
- Η οριζόντια κλιμάκωση αναφέρεται στη πρόσθεση νέων υπολογιστικών συστημάτων στην υπάρχουσα υποδομή.

Κλιμακοθετησιμότητα

- Η κάθετη κλιμάκωση αναφέρεται
  - στην αναβάθμιση των υπολογιστικών συστημάτων που χρησιμοποιούνται με περισσότερο αποθηκευτικό χώρο, επεξεργαστική ισχύ και μνήμη.
- Η οριζόντια κλιμάκωση περιορίζεται
  - από το πλήθος των υπολογιστικών συστημάτων τα οποία μπορούν να διατεθούν,
- Η κάθετη κλιμάκωση περιορίζεται
  - από τα ίδια τα υπολογιστικά συστήματα τα οποία χρησιμοποιούνται.

Κλιμακοθετησιμότητα

- Παρά τα πλεονεκτήματα από τα οποία χαρακτηρίζεται η οριζόντια κλιμάκωση
  - όπως για παράδειγμα ότι δεν επηρεάζει τη διαθεσιμότητα της παρεχόμενης υπηρεσίας κατά την εφαρμογή της,
  - κρίνεται απαραίτητο να ληφθούν υπόψη από τον πάροχο οι περιορισμοί οι οποίοι τίθονται.
- Περιορισμοί αποτελούν
  - το κόστος που απαιτείται για την αγορά των αδειών του λογισμικού το οποίο θα εγκατασταθεί στα νέα υπολογιστικά συστήματα,
  - το κόστος ηλεκτρικής ισχύος
  - και το κόστος για τη ψύξη αυτών ώστε να λειτουργούν ανελλιπώς χωρίς προβλήματα.

Κλιμακοθετησιμότητα

- Η οριζόντια κλιμάκωση υπερτερεί της κάθετης εφόσον το κόστος αγοράς υπολογιστικών συστημάτων σε σύγκριση με τις δυνατότητες οι οποίες προσφέρονται, είναι μικρό.
- Η υποδομή του υπολογιστικού νέφους δίνει στους παρόχους τη δυνατότητα
  - να αυξάνουν και να μειώνουν τους πόρους οι οποίοι βρίσκονται σε χρήση σύμφωνα με τη ζήτηση
  - η οποία υπάρχει προκειμένου να μειώσουν το κόστος λειτουργίας τους
  - χωρίς βέβαια να παραβιάζεται η συμφωνία στάθμης υπηρεσίας η οποία βρίσκεται σε ισχύ.

Κλιμακοθετησιμότητα

- Οι πάροχοι προκειμένου
  - να αυξήσουν την χρήση των παρεχόμενων υπηρεσιών κατά τα χρονικά διαστήματα που τα υπολογιστικά συστήματα βρίσκονται σε άεργη κατάσταση,
  - κατασκευάζουν διαφορετικά μοντέλα χρέωσης των υπηρεσιών τους για να προσελκύσουν τους χρήστες.
- Δημιουργείται η ανάγκη για την κατασκευή μοντέλων πρόβλεψης της συμπεριφοράς των χρηστών σε συγκεκριμένα χρονικά διαστήματα
  - ώστε οι πάροχοι να είναι σε θέση να ικανοποιήσουν τις ανάγκες των χρηστών και παράλληλα να γίνεται αποδοτικά χρήση της υποδομής τους.

Κλιμακοθετησιμότητα

- Γι’ αυτό το λόγο χρησιμοποιείται λογισμικό εικονικοποίσης (hypervisors),
  - ώστε να αυξάνονται
  - και να μειώνονται οι χρησιμοποιούμενοι πόροι ταχύτατα
  - και επειδή παρέχεται η δυνατότητα κατασκευής στιγμιότυπων (snapshots)
    - σύμφωνα με την οποία η λειτουργία ενός εικονικοποιημένου συστήματος μπορεί να αδρανοποιηθεί σε μια συγκεκριμένη κατάσταση
    - και κατά την επιστροφή του χρήστη στην υποδομή να συνεχιστεί η λειτουργία αυτού.
- Οι εικονικοποιητές χρησιμοποιούν βέλτιστα το hardware το οποίο τους παρέχεται
  - ώστε να ικανοποιείται η ικανότητα της κλιμακοθετησιμότητας για τους χρήστες και να εξοικονομούνται χρηματικοί πόροι για τους παρόχους

Κλιμακοθετησιμότητα

- Η διαδικασία εικονικοποίησης καταστεί εφικτή την εκτέλεση πολλών εικονικών συστημάτων (VMs) ταυτόχρονα σε ένα φυσικό στοιχείο hardware.
- Αυτή η διαδικασία λειτουργεί με μεγάλη ταχύτητα με αποτέλεσμα μέσω αυτής να βελτιώνεται η κλιμαθετησιμότητα.
- Η διαδικασία της εικονικοποίησης πραγματοποιείται
  - από τους εικονικοποιητές
  - οι οποίοι διαμοιράζουν τους φυσικούς πόρους στα φιλοξενούμενα συστήματα(guests).

Κλιμακοθετησιμότητα

- Με την υποστήριξη του περιβάλλοντος εικονικοποίησης από τις εταιρίες κατασκευής επεξεργαστών, AMD και Intel, καθίσταται δυνατή η υιοθέτηση της διαδικασίας.
- Κάθε ένα από τα φιλοξενούμενα συστήματα αποκτά πρόσβαση σε συγκεκριμένους πόρους οι οποίοι του ανατίθενται.
- Υπάρχουν τρείς διαφορετικές τεχνικές με τις οποίες μπορεί να επιτευχθεί εικονικοποίηση των φυσικών πόρων:
  - εικονικοποίηση βασισμένη στην εφαρμογή,
  - εικονικοποίηση βασισμένη στο λειτουργικό σύστημα,
  - εικονικοποίηση βασισμένη σε σύστημα εικονικοποίησης.

Κλιμακοθετησιμότητα

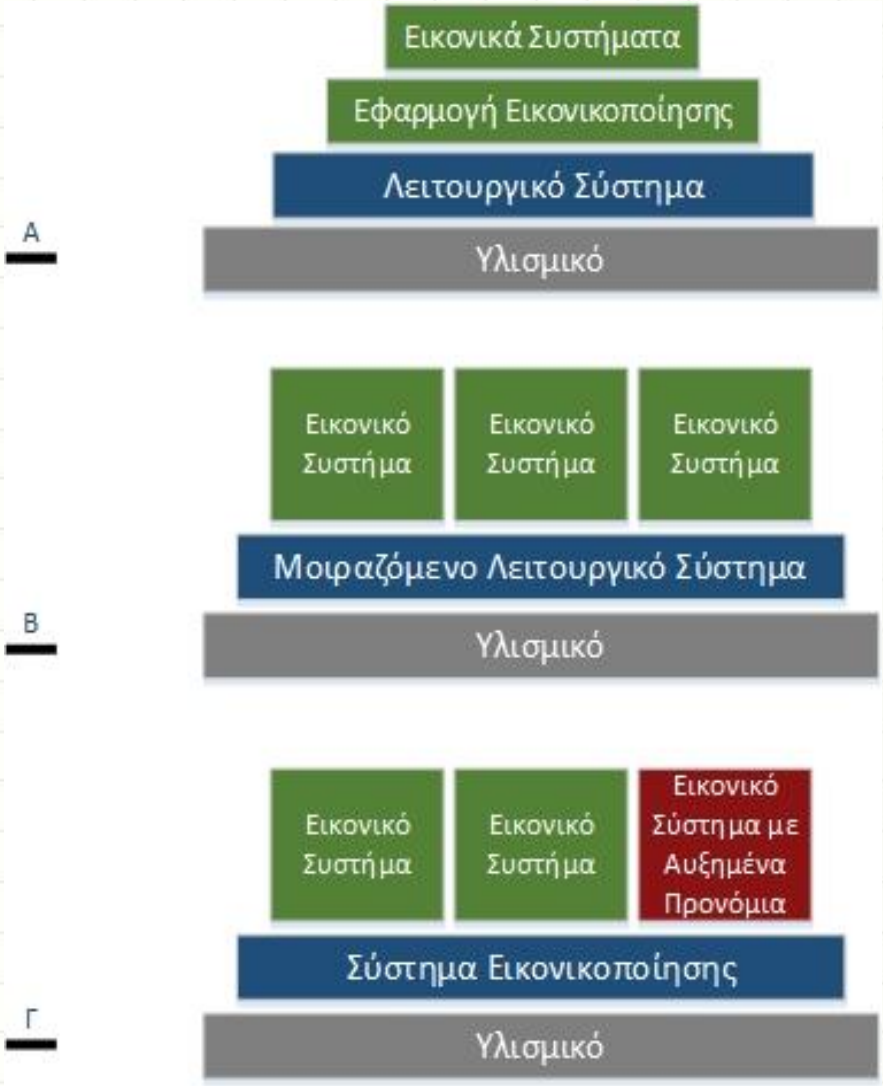
- Κατά την πρώτη τεχνική,
  - μια εφαρμογή εικονικοποίησης εγκαθίσταται στο περιβάλλον ενός λειτουργικού συστήματος Windows, UNIX ή Linux
  - και μέσω αυτής μπορούν να κατασκευαστούν εικονικοποιημένα μηχανήματα.
- Εφαρογές αυτού του τύπου αποτελούν τα VMware Server και Microsoft Virtual Machine.
- Κατά την δεύτερη τεχνική(hosted),
  - η χρήση του πυρήνα ενός λειτουργικού συστήματος διαμοιράζεται μεταξύ των φιλοξενούμενων συστημάτων.

Κλιμακοθετησιμότητα

Α) Εικονικοποίηση βασισμένη στην εφαρμογή,

Β) Εικονικοποίηση βασισμένη στο λειτουργικό σύστημα,

Γ) Εικονικοποίηση βασιμένη στο σύστημα εικονικοποίησης



Κλιμακοθετησιμότητα

- Κατά την τρίτη τεχνική(bare metal),
  - το σύστημα εικονικοποίησης είναι ενσωματωμένο ή εγκαθίσταται στο hardware.
- Κατά την εκκίνηση του συστήματος πραγματοποιείται ο διαμοιρασμός των φυσικών πόρων στα φιλοξενούμενα συστήματα.
- Ορισμένα από τα φιλοξενούμενα συστήματα κατέχουν αυξημένα προνόμια και χρησιμοποιούνται
  - για τη διαχείριση και τη ρύθμιση χαρακτηριστικών των υπολοίπων
  - όπως επίσης και του ίδιου του συστήματος εικονικοποίησης.

Κλιμακοθετησιμότητα

- Εφαρμογές αυτού του τύπου είναι
  - τα IBM AIX Logical Partitioning,
  - HP-UX Virtual Partitions(VPAR) και
  - VMware ESX Server.
- Οι περισσότεροι πάροχοι και εταιρίες χρησιμοποιούν τη τεχνική εικονικοποίησης βασισμένη σε σύστημα εικονικοποίησης.
- Ωστόσο, με την υιοθέτηση της διαδικασίας της εικονικοποίησης από τους παρόχους υπολογιστικού νέφους δημιουργούνται
  - κίνδυνοι και
  - απειλές για την ασφάλεια της υποδομής.

Κλιμακοθετησιμότητα

- Αυτό συμβαίνει επειδή το λογισμικό εικονικοποίησης προσθέτει ενα επιπλέον αφαιρετικό επίπεδο μεταξύ των λειτουργικών συστημάτων και του hardware.
- Το περιβάλλον εικονικοποίησης
  - είναι αρκετά πολύπλοκο και
  - ο τρόπος λειτουργίας του θέτει προκλήσεις ως προς τη διαχείριση των φιλοξενούμενων συστημάτων.
- Μέσω του περιβάλλοντος εικονικοποίησης είναι αδύνατη η απομόνωση ενός φιλοξενούμενου συστήματος από τα υπόλοιπα επειδή χρησιμοποιούν κοινό λογισμικό.

Κλιμακοθετησιμότητα

- Έτσι, δεν υπάρχει η δυνατότητα των κληροδοτημένων δικτύων (legacy) για απομόνωση δύο συστημάτων με την εγκατάσταση ενός τείχους προστασίας
  - εφόσον ακόμη κι ένα εικονικοποιημένο τείχος προστασίας να τεθεί σε εφαρμογή για απομόνωση δύο εικονικοποιημένων συστημάτων
  - θα υπάρχει σύνδεση μεταξύ τους μέσω του λογισμικού που τους αναθέτει πόρους.
- Επιπλέον, τα τρωτά σημεία ενός συστήματος εικονικοποίησης θα μπορούσαν να οδηγήσουν σε εκμετάλλευση(exploitation) αυτού
  - και κατά συνέπεια σε εκμετάλλευση όλων των φιλοξενούμενων συστημάτων του.

Κλιμακοθετησιμότητα

- Για παράδειγμα, το τρωτό σημείο με αναγνωριστικό CVE-2005-4459
  - επιτρέπει την απομακρυσμένη εκτέλεση κώδικα μέσω της υπερχείλισης του χώρου της σωρού που χρησιμοποιείται από το σύστημα εικονικοποίησης
  - με συγκεκριμένες κακόβουλες αιτήσεις του πρωτοκόλλου File Transfer Protocol(FTP).
- Το συγκεκριμένο τρωτό σημείο αναφέρεται στις εφαρμογές VMware ACE, VMware Gsx Server, VMware Player, VMware Workstation.

Κλιμακοθετησιμότητα

- Εκτός αυτού, το τρωτό σημείο με αναγνωριστικό CVE-2018-3456 και κωδικό όνομα VENOM από το Virtualized Environment Neglected Operations Manipulations,
  - επιτρέπει την εκμετάλλευση του συστήματος εικονικοποίησης μέσω ενός σφάλματος της δυνατότητας χρήσης εικονικού εύκαμπτου δίσκου(floppy drive).
  - Το συγκεκριμένο τρωτό σημείο επηρεάζει τα συστήματα εικονικοποίησης XEN, KVM και QEMU.

Κλιμακοθετησιμότητα

- Αυτά έχουν ως αποτέλεσμα τον έλεγχο των συστημάτων εικονικοποίησης,
  - όπως επίσης και όλων των φιλοξενούμενων συστημάτων από τον επιτιθέμενο.
- Επιπρόσθετα, βρέθηκε ένα μεγάλο πλήθος από κομμάτια κώδικα εκμετάλλευσης (exploits) μέσω του *searchsploit*
  - τα οποία θα μπορούσαν να χρησιμοποιηθούν για την εκμετάλλευση συστημάτων εικονικοποίησης και να αποκτηθεί ο έλεγχος τους.
- Τα συγκεκριμένα κομμάτια κώδικα στοχεύουν γνωστά τρωτά σημεία των συστημάτων εικονικοποίησης.

Κλιμακοθετησιμότητα

- Τα αναγνωριστικά γνωστών τρωτών σημείων είναι τα ακόλουθα: CVE-2007-1744, CVE-2008-0923, CVE-2009-1244, CVE-2012-0217 και CVE-2014-0983.
- Το *searchsploit* πρόκειται για ένα πρόγραμμα το οποίο αναζητά κώδικα εκμετάλλευσης στο τοπικό αντίγραφό της βάσης δεδομένων exploit,
  - το οποίο βρίσκεται στο λειτουργικό σύστημα Kali.

Κλιμακοθετησιμότητα

```
root@kali:~# searchsploit vmware fusion
------------------------------------------------------------------------------------------------------------------------
 Description                                                                                          |  Path
------------------------------------------------------------------------------------------------------------------------
VMWare Fusion <= 2.0.5 vmx86 kext Local kernel Root Exploit                                           | /osx/local/10076.c
VMWare Fusion <= 2.0.5 vmx86 kext Local PoC                                                           | /osx/local/10078.c
------------------------------------------------------------------------------------------------------------------------
root@kali:~# searchsploit vmware esx
------------------------------------------------------------------------------------------------------------------------
 Description                                                                                          |  Path
------------------------------------------------------------------------------------------------------------------------
VMware ESX 2.x - Multiple Information Disclosure Vulnerabilities                                      | /multiple/remote/28312.txt
VMware Server <= 2.0.1_ESXi Server <= 3.5 - Directory Traversal Vulnerability                        | /multiple/remote/33310.nse
------------------------------------------------------------------------------------------------------------------------
root@kali:~# searchsploit microsoft virtual
------------------------------------------------------------------------------------------------------------------------
 Description                                                                                          |  Path
------------------------------------------------------------------------------------------------------------------------
Microsoft Virtual Machine 2000 Series/3000 Series getSystemResource Vulnerability                     | /windows/remote/19734.java
Microsoft IIS 4.0 UNC Mapped Virtual Host Vulnerability                                               | /multiple/remote/19824.txt
Microsoft Virtual Machine 2000/3100/3200/3300 Series - com.ms.activeX.ActiveXComponent Arbitrary Program Execution | /windows/remote/20266.txt
Microsoft Virtual Machine Arbitrary Java Codebase Execution Vulnerability                             | /windows/remote/20306.html
Microsoft Java Virtual Machine 3802 Series - Bytecode Verifier Vulnerability                          | /windows/remote/22027.txt
------------------------------------------------------------------------------------------------------------------------
root@kali:~# searchsploit virtualbox
------------------------------------------------------------------------------------------------------------------------
 Description                                                                                          |  Path
------------------------------------------------------------------------------------------------------------------------
Sun xVM VirtualBox < 1.6.4 Privilege Escalation Vulnerability PoC                                     | /multiple/dos/6218.txt
VirtualBox 2.2 - 3.0.2 r49928 - Local Host Reboot PoC                                                 | /multiple/dos/9323.txt
Sun VirtualBox <= 3.0.6 - Privilege Escalation                                                        | /multiple/local/9973.sh
Oracle VM VirtualBox 4.1 - Local Denial of Service Vulnerability                                      | /lin_x86-64/dos/21224.c
Oracle VirtualBox 3D Acceleration - Multiple Vulnerabilities                                          | /multiple/dos/32208.txt
Sun xVM VirtualBox 2.0/2.1 - Local Privilege Escalation Vulnerability                                 | /linux/local/32848.txt
VirtualBox 3D Acceleration Virtual Machine Escape                                                     | /win64/remote/34334.rb
VirtualBox Guest Additions VBoxGuest.sys Privilege Escalation                                         | /windows/local/34333.rb
------------------------------------------------------------------------------------------------------------------------
```

Κλιμακοθετησιμότητα

- Στο περιβάλλον εικονικοποίησης παρουσιάζονται κίνδυνοι ως προς το επίπεδο απομόνωσης,
  - το οποίο μπορεί να επιτευχθεί μεταξύ των εικονικών συστημάτων.
- Σε περίπτωση που ένα εκ των εικονικών μηχανημάτων προσβληθεί από έναν ιό ή σκουλήκι
  - τότε τίθεται σε κίνδυνο η ασφάλεια όλων των εικονικών μηχανημάτων τα οποία αλληλεπιδρούν με αυτό.

Κλιμακοθετησιμότητα

- Αυτό συμβαίνει λόγω της αρχιτεκτονικής του υπολογιστικού νέφους κατά την οποία για τη παροχή μιας υπηρεσίας είναι αναγκαίο
  - να αλληλεπιδρούν τα εικονικά συστήματα μεταξύ τους
  - και λόγω του τύπου του κακόβουλου λογισμικού το οποίο προσπαθεί να διαδοθεί ή να μεταδώσει ένα αντίγραφο του εαυτού του σε άλλα συστήματα του δικτύου.
- Επιπλέον, η ανίχνευση ενός κακόβουλου εικονικού συστήματος και η λήψη των κατάλληλων αντίμετρων
  - όπως η απομόνωση του προσβεβλημένου συστήματος αποτελεί μια αργή διαδικασία για την υποδομή του υπολογιστικού νέφους.

Κλιμακοθετησιμότητα

- Αιτία αυτού, είναι η αλληλεπίδραση εικονικών συστημάτων τα οποία βρίσκονται εγκατεστημένα σε διαφορετικά δίκτυα.
- Τη χρονική στιγμή την οποία θα ανιχνευθεί ένα προσβεβλημένο εικονικό σύστημα θα πρέπει να εξεταστούν
  - τα εικονικά συστήματα με τα οποία έχει αλληλεπιδράσει
  - και να συνεχιστεί αυτή η διαδικασία
  - ενώ παράλληλα το κακόβουλο λογισμικό συνεχίζει να μεταδίδεται μεταξύ των διαφορετικών δικτύων.

Κλιμακοθετησιμότητα

- Η αντιμετώπιση θα μπορούσε να καταστεί εύκολη
  - εάν υπήρχε μόνο μια πύλη εισόδου/εξόδου δεδομένων από το ένα δίκτυο στο άλλο,
  - ωστόσο στο υπολογιστικό νέφος διαφορετικά εικονικά συστήματα αλληλεπιδρούν με εικονικά συστήματα σε διαφορετικά δίκτυα.

Κλιμακοθετησιμότητα

- Οι περισσότεροι πάροχοι υπολογιστικού νέφους υιοθετούν περιβάλλοντα εικονικοποίησης
  - τα οποία δεν εφαρμόζουν αυστηρή απομόνωση μεταξύ των εικονικών συστημάτων
  - προκειμένου να αποφεύγεται η δημιουργία προβλημάτων στην διαχείριση των υπηρεσιών.
- Έτσι, δημιουργείται ένα τρωτό σημείο το οποίο εκμεταλλεύεται από τις επιθέσεις τύπου διαφυγής εικονικού συστήματος (vm escape).
- Σε αυτό το τύπο επίθεσης,
- εκμεταλλεύεται ένα πρόγραμμα
- το οποίο λειτουργεί στο εικονικό σύστημα
- με στόχο τη παραβίαση του συστήματος εικονικοποίησης.

Κλιμακοθετησιμότητα

- Με αυτόν τον τρόπο, ο επιτιθέμενος αποκτά προνόμια διαχειριστή
  - με δυνατότητα εκτέλεσης οποιασδήποτε ενέργειας
  - όπως αντιγραφής των διαπιστευτηρίων του διαχειριστή για άλλες υπηρεσίες ή κατασκευή κερκόπορτας (backdoor)
  - η οποία θα επιτρέπει τη πρόσβαση μελλοντικά στο σύστημα.
- Επιπλέον, ο επιτιθέμενος αποκτά την ικανότητα καταγραφής της δικτυακής κίνησης μεταξύ των εικονικών δικτύων
  - και κατά συνέπεια αποκτά πληροφορίες και δεδομένα τα οποία σχετίζονται με τους πελάτες
  - οι οποίοι χρησιμοποιούν τη παρεχόμενη υπηρεσία υπολογιστικού νέφους.

Κλιμακοθετησιμότητα

- Με την απόκτηση προνομίων διαχειριστή, σε περιβάλλον το οποίο κατασκευάζεται με τη τεχνική εικονικοποίησης βασισμένη στο λειτουργικό σύστημα,
  - οι ενέργειες του επιτιθέμενου περιορίζονται από τον πυρήνα του λειτουργικού συστήματος.
- Στην περίπτωση που το εικονικό σύστημα έχει κατασκευαστεί με τη τεχνική εικονικοποίησης βασισμένη στο σύστημα εικονικοποίησης,
  - ο επιτιθέμενος περιορίζεται μόνο από τα αντίμετρα τα οποία έχουν τεθεί σε εφαρμογή από το διαχειριστή.

Κλιμακοθετησιμότητα

- Κρίσιμης σημασίας επίσης είναι τα εικονικά δίκτυα τα οποία χρησιμοποιούνται για την επικοινωνία των εικονικών συστημάτων.
- Σε περίπτωση κατά την οποία παραβιαστεί η ασφάλεια ενός εικονικού συστήματος και ο επιτιθέμενος αποκτήσει τον έλεγχο του λογισμικού εικονικοποίησης τότε
  - είναι σε θέση να συλλέξει πληροφορίες σχετικά με τα εικονικά δίκτυα τα οποία χρησιμοποιούνται.
- Αυτού του τύπου οι πληροφορίες χρησιμοποιούνται στη πραγματοποίηση επίθεσης τύπου παραπλάνησης IP διευθύνσεων(IP spoofing).

Κλιμακοθετησιμότητα

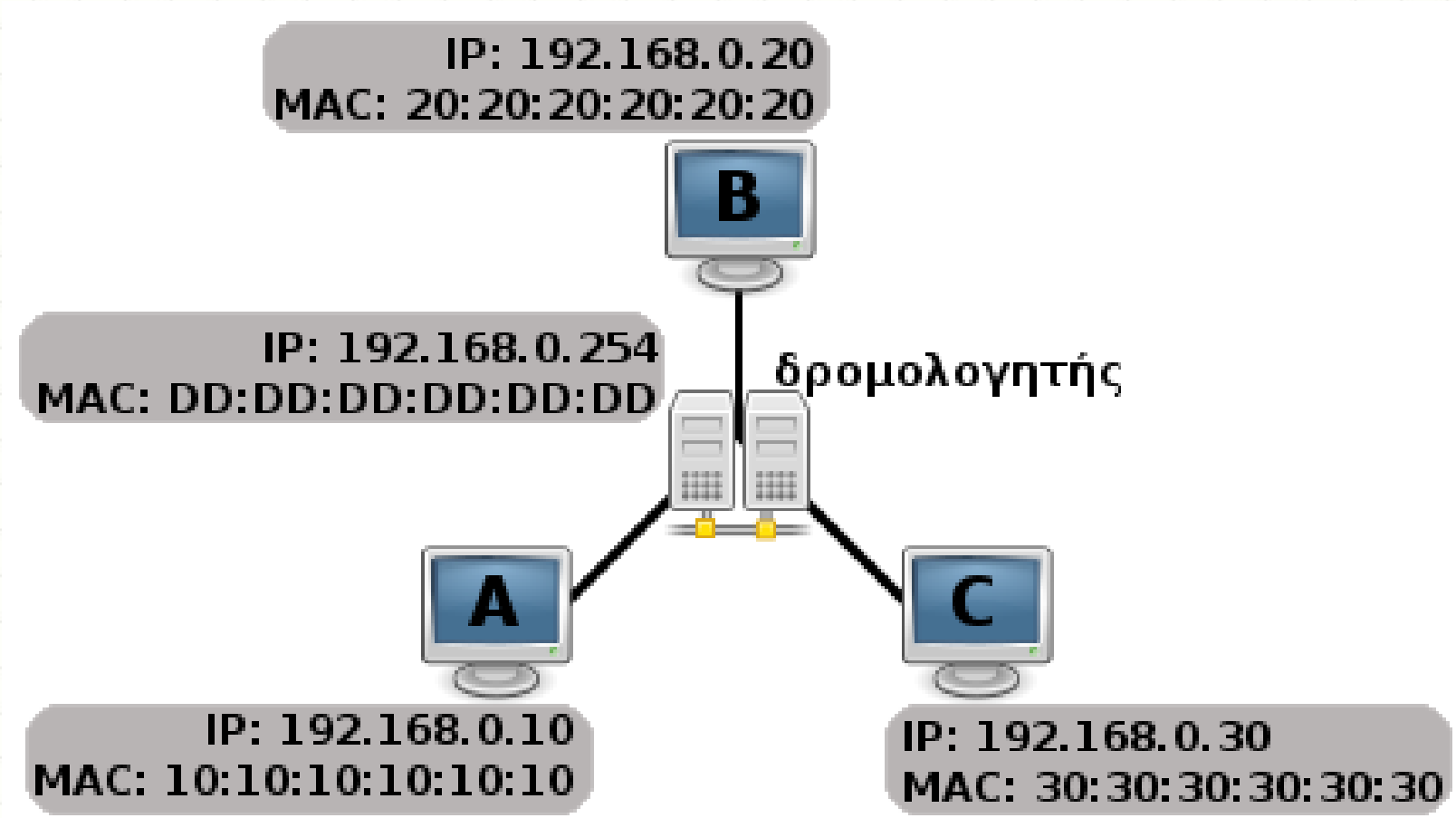
- Ωστόσο, το συγκεκριμένο τρωτό σημείο μπορεί να μετριαστεί μέσω του πρωτοκόλλου IPSec και τεχνικών κρυπτογράφησης.
- Το πρωτόκολλο IPSec ενσωματώνει λειτουργίες αυθεντικοποίησης, εμπιστευτικότητας και διαχείρισης κλειδιού.
- Επιπλέον, το IPSec είναι διαφανές στους τελικούς χρήστες
  - και όταν υλοποιείται σε τελικό σύστημα, το λογισμικό των ανώτερων επιπέδων δεν επηρεάζεται.
- Έτσι, οι υπηρεσίες οι οποίες λειτουργούν σε κάθε εικονικό σύστημα δεν επηρεάζονται από το συγκεκριμένο πρωτόκολλο.
- Για παράδειγμα, το σύστημα εικονικοποίησης Xen παρέχει δύο τύπους εικονικών δικτύων, γέφυρας(bridge) και δρομολόγησης(route).

Κλιμακοθετησιμότητα

- Στα εικονικά δίκτυα τύπου γέφυρας, όλα τα εικονικά συστήματα επικοινωνούν μεταξύ τους μέσω μιας πλήμνης(hub),
  - έτσι μέσω ενός εικονικού συστήματος μπορεί να πραγματοποιηθεί καταγραφή της δικτυακής κίνησης όλων τους με εργαλεία όπως
    - το tcpdump και το Wireshark.
- Η καταγραφή της κίνησης θα οδηγήσει
  - στη συγκέντρωση πληροφοριών σχετικά με τις υπηρεσίες,
  - οι οποίες παρέχονται από τα υπόλοιπα εικονικά συστήματα και δεδομένα τα οποία σχετίζονται με αυτές.

Κλιμακοθετησιμότητα

- Η συγκέντρωση πληροφοριών είναι κρίσιμη
  - επειδή μπορεί να οδηγήσει τον επιτιθέμενο στην αναγνώριση τρωτών σημείων
  - τα οποία θα του επιτρέψουν τον έλεγχο περισσότερων εικονικών συστημάτων.
- Στα εικονικά δίκτυα τύπου δρομολόγησης, τα εικονικά συστήματα επικοινωνούν μέσω ενός εικονικού μεταγωγέα (virtual switch).
- Μπορεί να χρησιμοποιηθεί το πρωτόκολλο ανάλυσης διευθύνσεων(ARP)
  - προκειμένου να πραγματοποιηθεί παραπλάνηση πακέτων ARP(ARP spoofing).


IP: 192.168.0.20
MAC: 20:20:20:20:20:20
B
IP: 192.168.0.254
MAC: DD:DD:DD:DD:DD:DD
δρομολογητής
A
C
IP: 192.168.0.10
MAC: 10:10:10:10:10:10
IP: 192.168.0.30
MAC: 30:30:30:30:30:30

Κλιμακοθετησιμότητα

- Στην περίπτωση κατά την οποία ο επιτιθέμενος έχει θέσει υπό τον έλεγχο του ένα εικονικό σύστημα τότε
  - μέσω της τεχνικής ARP spoofing θα έχει τη δυνατότητα να συσχετίσει την MAC διεύθυνση του με την IP διεύθυνση της προεπιλεγμένης πύλης.
- Με αυτό το τρόπο, θα κατευθύνει τη δικτυακή κίνηση
  - η οποία προοριζόταν για την προεπιλεγμένη πύλη
  - στο εκτεθειμένο σύστημά μέσω του οποίου θέσει υπό τον έλεγχό του πακέτα με πληροφορίες σχετικά με την αρχιτεκτονική του δικτύου και τους χρήστες των υπηρεσιών.

Κλιμακοθετησιμότητα

- Στο πλαίσιο αυτό γίνεται κατανοητό πως
  - η υποδομή των παρόχων υπηρεσιών υπολογιστικού νέφους λόγω της κατανεμημένης φύσης της δημιουργεί μια αλληλουχία από τρωτά σημεία.
- Στα περισσότερα περιβάλλοντα, τα συστήματα ανίχνευσης εισβολής χρησιμοποιούνται από τους διαχειριστές για τη βελτίωση του παρεχόμενου επιπέδου ασφάλειας.

Κλιμακοθετησιμότητα

- Υπάρχουν δύο κατηγορίες συστημάτων ανίχνευσης εισβολών:
  - τα Host-based IDSs και
  - τα Network-based IDSs.
- Τα συστήματα ανίχνευσης εισβολών host-based,
  - συγκεντρώνουν και αναλύουν πληροφορίες σχετικά με τις ενέργειες οι οποίες υλοποιούνται από ένα χρήστη ή μια εφαρμογή σε ένα σύστημα.

Κλιμακοθετησιμότητα

- Τα συστήματα ανίχνευσης εισβολών network-based,
  - αναλύουν πληροφορίες οι οποίες συλλέγονται από τα πακέτα
  - αφού προηγηθεί ανάλυση των πρωτοκόλλων επιπέδου δικτύου, μεταφοράς και εφαρμογής για τον εντοπισμό ύποπτης δραστηριότητας.
- Λόγω του μεγάλου όγκου δεδομένων τα οποία διακινούνται μεταξύ των εικονικών συστημάτων, δεν είναι εφικτή η χρήση των παραπάνω συστημάτων ανίχνευσης εισβολών.

Κλιμακοθετησιμότητα

- Τα συστήματα network-based,
  - δεν είναι σε θέση να παρακολουθήσουν κρυπτογραφημένη δικτυακή κίνηση και τα συστήματα host-based
  - δεν έχουν την δυνατότητα να ανιχνεύσουν κρυφές διόδους επίθεσης στα συστήματα τα οποία προστατεύουν.
- Τα συστήματα ανίχνευσης εισβολών παρακολουθούν τη δικτυακή κίνηση, ανιχνεύουν ύποπτη δραστηριότητα και ενημερώνουν τον διαχειριστή του συστήματος ή του δικτύου.

Κλιμακοθετησιμότητα

- Σε περίπτωση
  - που πραγματοποιηθεί επίθεση σε υπηρεσία του υπολογιστικού νέφους
  - και καταστραφούν ή υποκλαπούν δεδομένα
  - ενώ παράλληλα υπάρχει εγκατεστημένο σύστημα ανίχνευσης εισβολών
  - τότε ο χρήστης δεν θα ειδοποιηθεί άμεσα.
- Η εισβολή θα γνωστοποιηθεί σε ένα χρήστη μόνο αφού επιτραπεί από το πάροχο της υπηρεσίας.

Κλιμακοθετησιμότητα

- Στην προσπάθειά του ο πάροχος του υπολογιστικού νέφους να προστατεύσει τη φήμη και την εικόνα του έχει την ευελιξία να αποκρύψει το γεγονός με αποτέλεσμα να εκτίθεται ο χρήστης εν αγνοία του.
- Γι’ αυτό το λόγο θα πρέπει να παρακολουθείται η λειτουργία του παρόχου από τρίτο μέρος επιθεώρησης,
  - το οποίο θα έχει υποχρέωση να ενημερώνει τους χρήστες για αυτό το είδος συμβάντων.
- Θα πρέπει να χρησιμοποιούνται συστήματα τα οποία θα πραγματοποιούν
  - ανάλυση συμπεριφοράς(behavior analysis) και
  - ανάλυση γνώσης(knowledge analysis).

Κλιμακοθετησιμότητα

- Τα συστήματα ανάλυσης συμπεριφοράς
  - αναγνωρίζουν και καταγράφουν το προφίλ των ενεργειών και δραστηριοτήτων ενός χρήστη
  - με αποτέλεσμα σε περίπτωση απόκλισης από αυτό το προφίλ να αναγνωρίζεται ο χρήστης ως επιτιθέμενος και να λαμβάνονται τα κατάλληλα αντίμετρα.
- Με αυτή τη μέθοδο είναι δυνατή η αντιμετώπιση νέων τεχνικών επιθέσεις.

Κλιμακοθετησιμότητα

- Τα συστήματα ανάλυσης γνώσης χρησιμοποιούν ένα έμπειρο σύστημα για να περιγράψουν κακόβουλη συμπεριφορά μέσω ενός κανόνα.
- Πλεονέκτημα αυτής της μεθόδου αποτελεί το γεγονός πως είναι εφικτό να συνυπάρξουν ταυτόχρονα πολλοί κανόνες.
- Το συγκεκριμένο σύστημα καταγράφει μια σειρά από ενέργειες και χρησιμοποιεί τους κανόνες για να ανιχνεύσει κακόβουλη συμπεριφορά.
- Βέβαια, η δικτυακή κίνηση η οποία πραγματοποιείται στα εικονικά δίκτυα δεν είναι δυνατό να παρακολουθηθεί από τα παραπάνω συστήματα ώστε να ανιχνευθεί ύποπτη δραστηριότητα.

Κλιμακοθετησιμότητα

- Κρίνεται απαραίτητο να γίνει σύγκριση από τους παρόχους υπολογιστικού νέφους
  - ως προς τους κινδύνους που υπάρχουν όταν η δικτυακή κίνηση δε παρακολουθείται και
  - όταν η κίνηση εκτεθεί σε φυσικό επίπεδο

Κλιμακοθετησιμότητα

- Η κλιμακοθετησιμότητα μπορεί να διατηρηθεί
  - ενώ παράλληλα να τεθεί σε εφαρμογή ένα μοντέλο ανίχνευσης εισβολών το οποίο θα είναι κατανεμημένο,
  - όπως και η αρχιτεκτονική του υπολογιστικού νέφους σε περισσότερα σημεία τα οποία θα αλληλεπιδρούν.
- Το συγκεκριμένο μοντέλο ονομάζεται Grid Intrusion Detection Architecture.
- Σε αυτό η αρχιτεκτονική των τοπικών υποδικτύων είναι κατανεμημένη σε τρία στρώματα,
  - το στρώμα δρομολόγησης,
  - το στρώμα τείχους προστασίας
  - και το στρώμα διαμοιραζόμενου δικτύου.

Κλιμακοθετησιμότητα

- Το στρώμα δρομολόγησης θέτει ένα μεμονωμένο κανάλι μεταξύ του εικονικού δικτύου και της φυσικής διεπαφής.
- Το στρώμα τείχους προστασίας διαφυλάσσει τα εικονικά δίκτυα από επιθέσεις παραπλάνησης(spoofing).
- Το στρώμα διαμοιραζόμενου δικτύου
  - απομονώνει τα επιμέρους εικονικά δίκτυα,
  - ώστε να αποφεύγεται η επικοινωνία συστημάτων,
  - τα οποία δε πρέπει να αλληλεπιδρούν.

Κλιμακοθετησιμότητα

- Παρά το γεγονός πως προορίζεται για χρήση στην τεχνολογία grid,
  - το υπολογιστικό νέφος μπορεί να το υιοθετήσει,
  - αφού αποτελείται από χαρακτηριστικά της συγκεκριμένης τεχνολογίας.
- Τα συστήματα DCPortalsNg, SnortFlow και CyberGuarder είναι σε θέση να παρέχουν ικανοποιητικές δικλείδες ασφαλείας στα εικονικά δίκτυα.

Κλιμακοθετησιμότητα

- Το σύστημα DCPortalsNg
  - προσφέρει απομόνωση στα εικονικά δίκτυα κάνοντας χρήση της τεχνολογίας δικτύων καθορισμένων από το λογισμικό(SDN).
- Το SnortFlow
  - είναι ένα σύστημα αποτροπής εισβολών βασισμένο στα συστήματα Snort και OpenFlow.

Κλιμακοθετησιμότητα

- Σε αυτό η ύποπτη δραστηριότητα ανιχνεύεται και στην συνέχεια ειδοποιείται ένα υποσύστημα δημιουργίας κανόνων.
- Αφού δημιουργηθούν νέοι κανόνες αυτόματα το σύστημα επανεξετάζει τη δικτυακή κίνηση .

- Το σύστημα CyberGuarder
  - προσφέρει τρείς υπηρεσίες για τη διασφάλιση των εικονικών δικτύων,
    - την υπηρεσία ασφάλειας των εικονικών συστημάτων,
    - την υπηρεσία ασφάλειας των εικονικών δικτύων
    - και την υπηρεσία διαχείρισης των πολιτικών οι οποίες έχουν τεθεί σε εφαρμογή.

Κλιμακοθετησιμότητα

- Επιπρόσθετα, δε θα πρέπει να παραληφθούν τρωτά σημεία
  - τα οποία εισάγονται στην υποδομή του υπολογιστικού νέφους με την εφαρμογή της τεχνολογίας της εικονικοποίησης
  - πέραν της ελλιπούς απομόνωσης των εικονικών συστημάτων.
- Τρωτά σημεία αποτελούν
  - (α) η άρνηση παροχής υπηρεσιών στο σύστημα εικονικοποίησης,
  - (β) η χρήση rootkit και
  - (γ) η χρήση στιγμιότυπων(snapshots).

Κλιμακοθετησιμότητα

- Η επίθεση άρνησης παροχής υπηρεσιών στο σύστημα εικονικοποίησης πραγματοποιείται κυρίως σε υπηρεσίες τύπου IaaS
  - όπου οι χρήστες έχουν στη κατοχή τους εικονικά συστήματα με δυνατότητα διαχείρισης τους.
- Η συγκεκριμένη επίθεση έχει ως στόχο την εξάντληση των φυσικών πόρων του hardware στοιχείου,
  - οι οποίοι χρησιμοποιούνται από το σύστημα εικονικοποίησης για τη λειτουργία των φιλοξενούμενων εικονικών συστημάτων.

Κλιμακοθετησιμότητα

- Μέσω ενός εικονικού συστήματος ο επιτιθέμενος είναι σε θέση
  - να καταστήσει μη λειτουργικά τα υπόλοιπα εικονικά συστήματα τα οποία βρίσκονται εγκατεστημένα στο ίδιο στοιχείο hardware.
- Εκτός αυτού, η επίθεση άρνησης παροχής υπηρεσιών μπορεί να πραγματοποιηθεί
  - και διαμέσου μιας υπηρεσίας PaaS,
  - με κώδικα ο οποίος μέσω της πλατφόρμας εξαντλεί τους παρεχόμενους πόρους.
- Επίθεση στο σύστημα εικονικοποίησης μπορεί να πραγματοποιηθεί με χρήση rootkit.

Κλιμακοθετησιμότητα

- Το rootkit είναι
  - μια συλλογή από εργαλεία
  - τα οποία εγκαθίστανται σ’ έναν υπολογιστή και
  - επιτρέπουν στον επιτιθέμενο να αποκτήσει πρόσβαση σε επίπεδο διαχειριστή.
- Σε περίπτωση που ένα rootkit παραβιάσει το σύστημα εικονικοποίησης
  - τότε ο επιτιθέμενος αποκτά τον έλεγχο του στοιχείου του hardware.
- Rootkit το οποίο χρησιμοποιείται επί του παρόντος και αποτελεί απειλή για την υποδομή του υπολογιστικού νέφους είναι το Blue Pill.

Κλιμακοθετησιμότητα

- Το Blue Pill είναι κακόβουλο λογισμικό βασισμένο στην εικονικοποίηση το οποίο μπορεί να χρησιμοποιηθεί εναντίον οποιουδήποτε συστήματος
  - ανεξάρτητα από την αρχιτεκτονική του hardware ή του εγκατεστημένου λειτουργικού συστήματος.
- Αφού πραγματοποιηθεί η εγκατάστασή του, λειτουργεί ως σύστημα εικονικοποίησης μεταξύ του αρχικού λειτουργικού συστήματος ή του αρχικού συστήματος εικονικοποίησης και του hardware.

Κλιμακοθετησιμότητα

- Εφόσον λειτουργεί σε κατώτερο αφαιρετικό επίπεδο από το αρχικό σύστημα
  - είναι σε θέση να το ελέγχει και
  - κατά συνέπεια να ελέγχει τους πόρους τους οποίους διανέμει στα επιμέρους εικονικά συστήματα.
- Το συγκεκριμένο κακόβουλο λογισμικό είναι μη ανιχνεύσιμο από συστήματα όπως το Red Pill κυρίως
  - επειδή βασίζεται η λειτουργία του στη τεχνολογία AMD SVM.
- Η τεχνολογία AMD SVM
  - επιτρέπει τον έλεγχο καταχωρητών του επεξεργαστή, διακοπών και εντολών εισόδου/εξόδου
  - οι οποίες χρησιμοποιούνται στην επικοινωνία των εικονικών συστημάτων με το hardware.

Κλιμακοθετησιμότητα

- Το Blue Pill είναι Proof of Concept
  - έτσι για να πραγματοποιηθεί επιτυχής επίθεση είναι απαραίτητο ο επιτιθέμενος να έχει συγκεντρώσει πληροφορίες σχετικά
    - με το λειτουργικό σύστημα και
    - το σύστημα εικονικοποίησης το οποίο χρησιμοποιείται.
- Το Blue Pill όπως και το κακόβουλο λογισμικό SubVirt
  - μπορούν να χρησιμοποιηθούν για την εκμετάλλευση ενός συστήματος εικονικοποίησης
  - εφόσον πραγματοποιηθεί ανίχνευση της διαδικασίας εικονικοποίησης.

Κλιμακοθετησιμότητα

- Η ανίχνευση της διαδικασίας εικονικοποίησης πραγματοποιείται με εργαλεία όπως τα Nopill και VMDetect.
- Η χρήση της λειτουργίας των στιγμιότυπων στα εικονικά συστήματα χρησιμοποιείται
  - κυρίως από το διαχειριστή σε περίπτωση αποτυχίας για την επαναφορά ενός συστήματος σε κατάσταση λειτουργική.

Κλιμακοθετησιμότητα

- Ωστόσο, σε περίπτωση κατά την οποία εκτεθεί το σύστημα εικονικοποίησης,
  - ο επιτιθέμενος έχει τη δυνατότητα χρήσης παλαιότερων στιγμιότυπων.
- Έτσι, επαναφέροντας τα εικονικά συστήματα σε μια παρελθοντική κατάσταση,
  - αποφεύγεται η εφαρμογή νέων πολιτικών και λογισμικού ασφάλειας για τη προστασία πληροφοριών και δεδομένων τα οποία διαχειρίζονται.

Κλιμακοθετησιμότητα

- Το περιβάλλον εικονικοποίησης καθιστά δυνατή την ικανοποίηση της κλιμακοθετησιμότητας
  - εφόσον δυναμικά δημιουργεί εικονικά συστήματα για την υποστήριξη της παρεχόμενης υπηρεσίας.
- Τα εικονικά συστήματα δημιουργούνται αυτόματα με χρήση εικόνων (VM-images) από το περιβάλλον εικονικοποίησης.
- Οι εικόνες είναι κρίσιμης σημασίας αφού αποτελούν τη βάση για τη λειτουργία των επιμέρους συστατικών μιας υπηρεσίας.

Κλιμακοθετησιμότητα

- Επιπλέον, χρησιμοποιούνται από τους πελάτες στις υπηρεσίες IaaS για τη κατασκευή εικονικών συστημάτων.
- Οι εικόνες κατασκευάζονται
  - από τους εκδότες (publishers) και
  - κατατίθενται στο αποθετήριο (repository) του υπολογιστικού νέφους
    - από όπου διανέμονται για χρήση στους ανακτώντες (retrievers).
- Οι εκδότες είναι οι κατασκευαστές των εικόνων και μπορεί να είναι διαχειριστές του υπολογιστικού νέφους ή χρήστες μιας IaaS υπηρεσίας.

Κλιμακοθετησιμότητα

- Οι ανακτώντες είναι
  - χρήστες μια υπηρεσίας IaaS και
  - χρησιμοποιούν τις εικόνες για τη δημιουργία instances διακομιστών (servers).
- Ωστόσο, η εισαγωγή εικόνων στην υποδομή των παρόχων υπολογιστικού νέφους δημιουργεί ένα τρωτό σημείο.
- Το συγκεκριμένο τρωτό σημείο επιτρέπει στους επιτιθέμενους να χρησιμοποιούν τις εικόνες ως περιέκτη (container) δούρειων ίππων.

Κλιμακοθετησιμότητα

- Οι δούρειοι ίπποι είναι κακόβουλο λογισμικό,
  - το οποίο επιτελεί λειτουργίες έμμεσα τις οποίες δε θα ήταν δυνατό να τις επιτελέσει άμεσα ένας μη εξουσιοδοτημένος χρήστης.
- Προκειμένου, οι επιτιθέμενοι να κατασκευάσουν δούρειους ίππους
  - πρέπει να κατέχουν γνώση του λειτουργικού συστήματος και των εφαρμογών οι οποίες δραστηριοποιούνται σε αυτό
  - ώστε να παραμετροποιήσουν κατάλληλα τις εξαρτήσεις ως προς το λογισμικό του δούρειου ίππου οι οποίες είναι αναγκαίες για την επιτυχή επίθεση.

Κλιμακοθετησιμότητα

- Έτσι, γίνεται κατανοητό πως έχοντας την δυνατότητα οι επιτιθέμενοι να εισάγουν δικές τους εικόνες,
  - πλέον δεν υπάρχει ανάγκη για συλλογή πληροφοριών πριν την εκμετάλλευση ενός εικονικού συστήματος,
  - αφού ο δούρειος ίππος έχει παραμετροποιηθεί ήδη στην εικόνα.
- Απαραίτητος είναι ο συνεχής έλεγχος των εικόνων,
  - οι οποίες κατατίθενται στο αποθετήριο για την ανίχνευση κακόβουλου λογισμικού,
  - όπως επίσης και η αναγνώριση του τρόπου λειτουργίας τους σε απομονωμένο περιβάλλον
    - το οποίο δεν είναι διασυνδεδεμένο με την υποδομή του παρόχου.

Κλιμακοθετησιμότητα

- Οι πάροχοι υπολογιστικού νέφους για την αντιμετώπιση αυτού του τρωτού σημείου
  - πρέπει να χρησιμοποιούν συστήματα διαχείρισης και ανίχνευσης κακόβουλου λογισμικού στο σύνολο των εικονικών εικόνων
    - όπως είναι το σύστημα Mirage.
- Το συγκεκριμένο σύστημα
  - αναθέτει δικαιώματα πρόσβασης στους ανακτώντες και εκδότες των εικόνων
  - με στόχο τον έλεγχο ως προς τη χρήση τους.

Κλιμακοθετησιμότητα

- Διαθέτει σύστημα συντήρησης
  - για έλεγχο τήρησης των όρων λειτουργίας από τις εικόνες και την ανίχνευση κακόβουλου λογισμικού.
- Το σύστημα Mirage
  - διευκολύνει τη διαχείριση του αποθετηρίου στο σύνολό του από τους διαχειριστές,
  - εφαρμόζοντας φίλτρα για την επίτευξη των παραπάνω στόχων.
- Σε περίπτωση ανίχνευσης κακόβουλου λογισμικού ή τρωτών σημείων
  - το σύστημα “μπαλώνει”(patches) την εικόνα ενημερώνοντας για άλλες εικόνες οι οποίες συνδέονται με αυτήν,
  - όπως για παράδειγμα η αρχική εικόνα η οποία χρησιμοποιήθηκε για τη κατασκευή της και η οποία ενδέχεται να είναι τρωτή.

Κλιμακοθετησιμότητα

- Μπορεί να γίνει επιπρόσθετα χρήση του συστήματος EVDIC
  - το οποίο κρυπτογραφεί τις εικόνες πριν αποθηκευτούν και
  - τις αποκρυπτογραφεί για χρήση από το σύστημα εικονικοποίησης.
- Τέλος, το σύστημα ImageElves μπορεί να χρησιμοποιηθεί από τους παρόχους
  - για την εγκατάσταση των κατάλληλων ενημερώσεων στις εικόνες,
  - πολλές εκ των οποίων θα καλύπτουν τρωτά σημεία.

Ελαστικότητα

- Η ελαστικότητα είναι η ικανότητα των υπηρεσιών του υπολογιστικού νέφους
  - να προσαρμόζουν τους πόρους που χρησιμοποιούν στη κλίμακα του χρόνου,
  - σύμφωνα με το φόρτο εργασίας που τους ανατίθεται.
- Το Διεθνή Ινστιτούτο Προτύπων και Τεχνολογίας (NIST) ορίζει την ελαστικότητα
  - ως την ικανότητα που διαθέτουν οι πελάτες μιας υπηρεσίας να λαμβάνουν και να αποδεσμεύουν πόρους σύμφωνα με τις ανάγκες τους.

Ελαστικότητα

- Ιδανικά ο κάθε πελάτης μιας υπηρεσίας αντιλαμβάνεται
  - πως το πλήθος των διαθέσιμων πόρων
  - το οποίο του διατίθεται είναι πολύ μεγαλύτερο από αυτό που χρειάζεται.
- Μια υπηρεσία του υπολογιστικού νέφους αυτόματα προσαρμόζει τους πόρους της προκειμένου να ικανοποιεί την ικανότητα της ελαστικότητας.
- Αρκετά σημαντικό αποτελεί το γεγονός πως η κλιμακοθετησιμότητα παρουσιάζει αρκετές ομοιότητες με την ελαστικότητα.

Ελαστικότητα

- Ωστόσο, η κλιμακοθετησιμότητα αποτελεί στατική ιδιότητα των υπηρεσιών του υπολογιστικού νέφους
  - η οποία περιγράφει την ικανότητα κλιμάκωσης σε συγκεκριμένο βαθμό (χιλιάδες διακομιστές ή εκατομμύρια αιτήσεις ανά λεπτό).
- Η ελαστικότητα, όπως προκύπτει από τους παραπάνω ορισμούς,
  - είναι μια δυναμική ιδιότητα η οποία επιτρέπει την κλιμάκωση μιας υπηρεσίας σύμφωνα με τη ζήτηση.

Ελαστικότητα

- Η ελαστικότητα εφαρμόζεται με τρείς μεθόδους στην υποδομή του υπολογιστικού νέφους:
  - α) τη μέθοδο αντιγραφής(replication),
  - β) τη μέθοδο μετακίνησης(migration) και
  - γ) τη μέθοδο επανακαθορισμού μεγέθους(resizing).
- Η μέθοδος της αντιγραφής πραγματοποιείται
  - με πρόσθεση και αφαίρεση υποστάσεων (instances) μιας υπηρεσίας στο περιβάλλον των χρηστών.

Ελαστικότητα

- Η συγκεκριμένη μέθοδος
  - είναι η ευρέως γνωστή και
  - εφαρμόζεται στις υπηρεσίες υπολογιστικού νέφους της Amazon και της Google.
- Υποστηρίζει την ελαστικότητα
  - με τη παροχή μηχανισμών ισοστάθμισης του φόρτου εργασίας σε τομείς,
  - οι οποίοι αποτελούνται από αντίγραφα υποστάσεων μιας υπηρεσίας.

Ελαστικότητα

- Η μέθοδος επανακαθορισμού μεγέθους αποτελείται
  - από ενέργειες πρόσθεσης δεδομένων και δομών δεδομένων σε μια υπόσταση υπηρεσίας,
  - οι οποίες είναι διαθέσιμες σε ένα εικονικό σύστημα.
- Η μέθοδος μετακίνησης πραγματοποιείται
  - με τη μεταφορά ενός εικονικού συστήματος από ένα διακομιστή σε έναν άλλο.

Ελαστικότητα

- Οι πάροχοι υπολογιστικού νέφους προκειμένου να διανέμουν ελαστικές υπηρεσίες είναι αναγκαίο
  - να κατασκευάζουν την υποδομή τους με γνώμονα τη συγκεκριμένη ιδιότητα.
- Επιπλέον, η ελαστικότητα της υποδομής ενός παρόχου περιορίζεται από τη χωρητικότητα αυτής
  - και γι’ αυτό το λόγο οι πάροχοι πρέπει να ορίζουν το πλήθος των πόρων
  - το οποίο μπορεί να διατεθεί σε έναν χρήστη κάθε χρονική στιγμή και
  - συναρτήσει του οποίου θα εφαρμόζεται η ελαστικότητα.

Ελαστικότητα

- Η ελαστικότητα είναι άμεσα συνδεδεμένη με τη χρονική καθυστέρηση,
  - η οποία απαιτείται προκειμένου οι πόροι να βρεθούν σε θέση ετοιμότητας.
- Σε περίπτωση που η χρονική καθυστέρηση υπερβαίνει συγκεκριμένο όριο τότε επηρεάζεται
  - η αποδοτικότητα και η αποτελεσματικότητα της υπηρεσίας
  - με αποτέλεσμα ο μηχανισμός ελαστικότητας να μη είναι σε θέση να ανταπεξέλθει σε υψηλό φόρτο εργασίας
  - και να προκαλείται ζημία στην υπηρεσία.

Ελαστικότητα

- Ιδανικά, η ανίχνευση της ζήτησης μιας υπηρεσίας και η εφαρμογή της ελαστικότητας με προσαρμογή των πόρων θα πραγματοποιείται άμεσα.
- Η συγκεκριμένη ιδιότητα επηρεάζει
  - το κόστος,
  - τη ποιότητα
  - και τη διαχείριση των πόρων μιας υπηρεσίας κατά την διανομή της.

Ελαστικότητα

- Μια από τις περισσότερο διαδεδομένες μεθόδους εφαρμογής της ελαστικότητας στην υποδομή παρόχων υπολογιστικού νέφους είναι η μετακίνηση εικονικών συστημάτων.
- Κατά τη συγκεκριμένη μέθοδο,
  - ένα εικονικό σύστημα μεταφέρεται από ένα διακομιστή σε έναν άλλο μεταφέροντας
    - τον αποθηκευτικό του χώρο,
    - την κατάσταση της μνήμης του
    - και τις ρυθμίσεις σχετικά με την διαδικτυακή του πρόσβαση.

Ελαστικότητα

- Οι περισσότεροι πάροχοι υπηρεσιών υπολογιστικού νέφους επιλέγουν την δυναμική μετακίνηση εικονικών συστημάτων,
  - ώστε να ικανοποιούνται οι στόχοι οι οποίοι τίθενται από τη συμφωνία στάθμης υπηρεσίας.
- Η κύρια διαφορά της δυναμικής μετακίνησης από τη στατική είναι πως κατά την διαδικασία μετακίνησης ελέγχεται
  - ο φόρτος εργασίας
  - και οι πόροι οι οποίοι ανατίθονται στο εικονικό σύστημα έχουν ως στόχο
    - την ικανοποίηση των αναγκών που υπάρχουν τη συγκεκριμένη χρονική στιγμή.

Ελαστικότητα

- Κατά την εφαρμογή της μεθόδου τα περιεχόμενα ενός εικονικού συστήματος είναι
  - εκτεθειμένα στο δίκτυο
  - δημιουργώντας ένα διάνυσμα επίθεσης
  - το οποίο μπορεί να οδηγήσει σε παραβίαση του απόρρητου και της ακεραιότητας των δεδομένων.
- Κατά τη μετακίνηση ενός εικονικού συστήματος,
  - τα συστήματα εικονικοποίησης των διακομιστών επικοινωνούν μέσω του τοπικού δικτύου με μηνύματα
  - τα οποία περιέχουν λεπτομέρειες σχετικά με τη διαδικασία.

Ελαστικότητα

- Τα μηνύματα είναι διαμορφωμένα σε μορφότυπο(format) κειμένου,
  - έτσι ο επιτιθέμενος με πρόσβαση στο συγκεκριμένο δίκτυο έχει τη δυνατότητα τροποποίησης αυτών
  - με αποτέλεσμα τη μετακίνηση εικονικών συστημάτων και τη παρεμπόδιση της διαδικασίας κατά βούληση.
- Επιπλέον, ο επιτιθέμενος έχει τη δυνατότητα εκκίνησης της διαδικασίας μετακίνησης πολαπλών εικονικών συστημάτων προς συγκεκριμένο διακομιστή
  - με στόχο τη πρόκληση ζημιάς στη διαθεσιμότητα των υπηρεσιών οι οποίες διατίθενται από αυτόν.

Ελαστικότητα

- Κατά τη μετακίνηση εικονικών συστημάτων δημιουργούνται τρείς κλάσεις απειλών.
- Η πρώτη κλάση απειλών αφορά το επίπεδο ελέγχου.
  - Οι απειλές δημιουργούνται σε αυτό το επίπεδο λόγω της αποτυχία των μηχανισμών επικοινωνίας μεταξύ των εικονικών συστημάτων να επαληθεύσουν τη ταυτότητα όσων λαμβάνουν μέρος στη διαδικασία.

Ελαστικότητα

- Η δεύτερη κλάση απειλών αφορά το επίπεδο δεδομένων.
  - Οι απειλές οι οποίες δημιουργούνται σε αυτό το επίπεδο επηρεάζουν τη κατάσταση των εικονικών συστημάτων κατά τη μετακίνηση τους.
- Παθητικές επιθέσεις που λαμβάνουν μέρος σε αυτό το επίπεδο οδηγούν σε διαρροή πληροφοριών
  - οι οποίες διαχειρίζονται από τα εικονικά συστήματα και οι ενεργές επιθέσεις οδηγούν σε συμβιβασμό των φιλοξενούμενων λειτουργικών συστημάτων.

Ελαστικότητα

- Ο συμβιβασμός ενός λειτουργικού συστήματος έχει ως αποτέλεσμα
  - την μακροχρόνια έκθεση πληροφοριών και τον έλεγχο του συστήματος από τον επιτιθέμενο.
- Ο έλεγχος ενός συστήματος της υποδομής από έναν επιτιθέμενο μπορεί να οδηγήσει
  - σε αδυναμία ελέγχου περισσότερων συστημάτων και χαρτογράφηση της αρχιτεκτονικής της υποδομής η οποία χρησιμοποιείται.

Ελαστικότητα

- Με αυτόν το τρόπο ο επιτιθέμενος συγκεντρώνει πληροφορίες για τα συστήματα όπως
  - υπηρεσίες και θύρες οι οποίες χρησιμοποιούνται, τα υποδίκτυα
  - ορίζοντας το εύρος τους και τα ενεργά συστήματα και τέλος τους μηχανισμούς επικοινωνίας τους.
- Όλες οι πληροφορίες συγκεντρώνονται
  - ώστε ο επιτιθέμενος να αποκτήσει γνώση για διανύσματα επίθεσης τα οποία μπορεί να εκμεταλλευτεί.

Ελαστικότητα

- Η τρίτη κλάση απειλών αφορά το δομοστοιχείο μετακίνησης το οποίο χρησιμοποιείται από το σύστημα εικονικοποίησης.
  - Σε περίπτωση που ο επιτιθέμενος αποκτήσει τον έλεγχο ενός συστήματος εικονικοποίησης μέσω τρωτών σημείων του δομοστοιχείου μετακίνησης
    - τότε θα θέσει υπό τον έλεγχό του τα φιλοξενούμενα εικονικά συστήματα.
- Το διάνυσμα επίθεσης το οποίο εκμεταλλεύεται ο επιτιθέμενος είναι ο κώδικας ο οποίος υλοποιεί το δομοστοιχείο μετακίνησης.

Ελαστικότητα

- Ο συγκεκριμένος κώδικας είναι τρωτός σε επιθέσεις
  - οι οποίες στοχοποιούν τη στοίβα και τη σωρό
  - όπως είναι η επίθεση υπερχείλισης του ενδιάμεσου καταχωρητή.
- Η εκμετάλλευση του συγκεκριμένου κώδικά οδηγεί
  - στην εκμετάλλευση όλων των φιλοξενούμενων συστημάτων του συστήματος εικονικοποίησης
  - με ανεπανόρθωτες συνέπειες σε σύγκριση με την εκμετάλλευση ενός απλού προγράμματος ή υπηρεσίας του υπολογιστικού νέφους.

Ελαστικότητα

- Παράδειγμα αυτού του τύπου αποτελεί τρωτό σημείο στο δομοστοιχείο μετακίνησης των τελευταίων εκδόσεων τόσο στο σύστημα εικονικοποίησης Xen όσο και στο VMWare.
- Αυτά τα τρωτά σημεία δίνουν τη δυνατότητα στον επιτιθέμενο να αποκτήσει τον έλεγχο της μετακίνησης εικονικών συστημάτων
  - με επιθέσεις τύπου man-in-the-middle και να τροποποιήσουν το κώδικα
  - ο οποίος χρησιμοποιείται για την επαλήθευση της ταυτότητας των συστημάτων.

Ακεραιότητα

- Η ακεραιότητα των δεδομένων αποτελεί μια δυνατότητα των υπηρεσιών του υπολογιστικού νέφους,
  - η οποία επηρεάζεται σε μεγάλο βαθμό από τις απειλές οι οποίες έχουν παρουσιαστεί μέχρι στιγμής.
- Επιπρόσθετα, το απόρρητο και η ακεραιότητα των πληροφοριών οι οποίες διαχειρίζονται σε υποδομή υπολογιστικού νέφους τίθενται σε κίνδυνο
  - κυρίως λόγου του συνόλου των δραστών που έχει δυνατότητα πρόσβασης σε αυτές.

Ακεραιότητα

- Έτσι, κρίνεται απαραίτητο ο τελικός πελάτης
  - να συμφωνεί με τους στόχους οι οποίοι τίθενται στη συμφωνία στάθμης υπηρεσίας
  - και οι οποίοι ορίζουν τον τρόπο διαχείρισης και ελέγχου των δεδομένων στην υποδομή του παρόχου.
- Στους στόχους της συμφωνίας στάθμης υπηρεσίας ορίζονται οι δράστες και το έργο τους στην υποδομή
  - όπως επίσης και τα δικαιώματά τους επί των δεδομένων του παρόχου.

Ακεραιότητα

- Επιπλέον, προκειμένου να διασφαλιστεί η ακεραιότητα και το απόρρητο των δεδομένων
  - θα μπορούσε να προσαρμοστεί ένας μηχανισμός στην υποδομή του νέφους
  - ο οποίος θα ελέγχει τη συμπεριφορά των εικονικών συστημάτων και τις ενέργειες των δραστών με στόχο την ανίχνευση επιτιθέμενων.
- Ωστόσο, τα συστήματα τα οποία διαχειρίζονται τα δεδομένα δεν είναι αξιόπιστα,
  - εφόσον το λογισμικό σε αυτά μπορεί να τροποποιηθεί για να παρουσιάζουν ψευδή στοιχεία.

Ακεραιότητα

- Γι’ αυτό το λόγο αποφεύγεται η χρήση του συγκεκριμένου τύπου μηχανισμών.
- Οι πάροχοι εμπιστεύονται το hardware το οποίο βρίσκεται σε διαφορετικό αφαιρετικό επίπεδο από το λογισμικό και είναι πιο δύσκολο να εκμεταλλευτεί.
- Το hardware λειτουργεί ως σημείο αναφοράς του επιπέδου εμπιστοσύνης(root of trust)
  - που προσφέρεται στα δεδομένα εσωτερικά στην υποδομή του υπολογιστικού νέφους.

Ακεραιότητα

- Σύμφωνα με τον οργανισμό TCG (Trusted Computing Group),
  - οι πάροχοι θα μπορούσαν να ορίσουν το επίπεδο εμπιστοσύνης
  - τίθοντας σε εφαρμογή το δομοστοιχείο εμπιστοσύνης πλατφόρμας(TPM).
- Το συγκεκριμένο δομοστοιχείο αποτελεί διεθνή πρότυπο και βασίζεται στη λειτουργία ενός κρυπτο-επεξεργαστή
  - ο οποίος χρησιμοποιεί κλειδιά κρυπτογράφησης για την ασφάλεια του hardware και των στοιχείων που αλληλεπιδρούν με αυτό.

Ακεραιότητα

- Το TMP επεκτείνει τις δυνατότητες του hardware με λειτουργίες κρυπτογράφησης
  - επιτρέποντας παράλληλα στις εφαρμογές και στο λειτουργικό σύστημα να λειτουργήσουν απρόσκοπτα.
- Ο κρυπτο-επεξεργαστής παράγει κλειδιά κρυπτογράφησης και πραγματοποιεί ασύμμετρη κρυπτογράφηση των πληροφοριών και των δεδομένων που διαχειρίζεται.

Ακεραιότητα

- Η μνήμη χρησιμοποιείται από το κρυπτο-επεξεργαστή ως αποθηκευτικό μέσο για τα κλειδιά κρυπτογράφησης.
- Εκτός των παραπάνω, το TMP παρέχει απομόνωση των δεδομένων μεταξύ των χρηστών μιας υπηρεσίας
  - και εξασφαλίζει την ακεραιότητα του συστήματος εικονικοποίησης
  - όπως και των εικονικών συστημάτων.

Ακεραιότητα

- Βέβαια, για τον πλήρη έλεγχο της ακεραιότητας τόσο των δεδομένων
  - όσο και των συστημάτων, κρίνεται απαραίτητο να συνεργάζεται το δομοστοιχείο με τα APIs των εφαρμογών.
- Με αυτόν το τρόπο, τα APIs θα επαληθεύουν τους χρήστες
  - οι οποίοι αποκτούν πρόσβαση σε μια υπηρεσία
  - και θα ελέγχουν τα δικαιώματά τους, διευκολύνοντας το δομοστοιχείο στην ανίχνευση μη εγκεκριμένης συμπεριφοράς.

Ακεραιότητα

- Επιπλέον, τα APIs θα ελέγχουν τους πόρους
  - οι οποίοι διανέμονται στους τελικούς χρήστες
  - και απομονώνοντας με αυτόν το τρόπο τα δεδομένα των χρηστών εξασφαλίζοντας έτσι ακεραιότητα στο επίπεδο των δεδομένων.

Ακεραιότητα

- Η ακεραιότητα των δεδομένων αποτελεί μια δυνατότητα των υπηρεσιών του υπολογιστικού νέφους,
  - η οποία επηρεάζεται σε μεγάλο βαθμό από τις απειλές οι οποίες έχουν παρουσιαστεί μέχρι στιγμής.
- Επιπρόσθετα, το απόρρητο και η ακεραιότητα των πληροφοριών
  - οι οποίες διαχειρίζονται σε υποδομή υπολογιστικού νέφους τίθενται σε κίνδυνο
  - κυρίως λόγου του συνόλου των δραστών που έχει δυνατότητα πρόσβασης σε αυτές.

Ευχαριστώ