234 – Ασφάλεια & Ιδιωτικότητα στο Διαδίκτυο του Μέλλοντος

ΑΣΦΑΛΕΙΑ ΣΤΟ ΥΠΟΛΟΓΙΣΤΙΚΟ ΝΕΦΟΣ

Κυριάκος Κρητικός
Αναπλ. Καθηγητής
Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων

Περίγραμμα – Θέματα Ασφάλειας

- Θεμελιώσεις
- Παράγοντες Επίδρασης στην Ασφάλεια
- Πράκτορες Απειλών
- Απειλές στην Ασφάλεια του Νέφους
- Επιπρόσθετα Θέματα Ασφάλειας
- Μηχανισμοί & Τεχνικές Ασφάλειας

Ασφάλεια

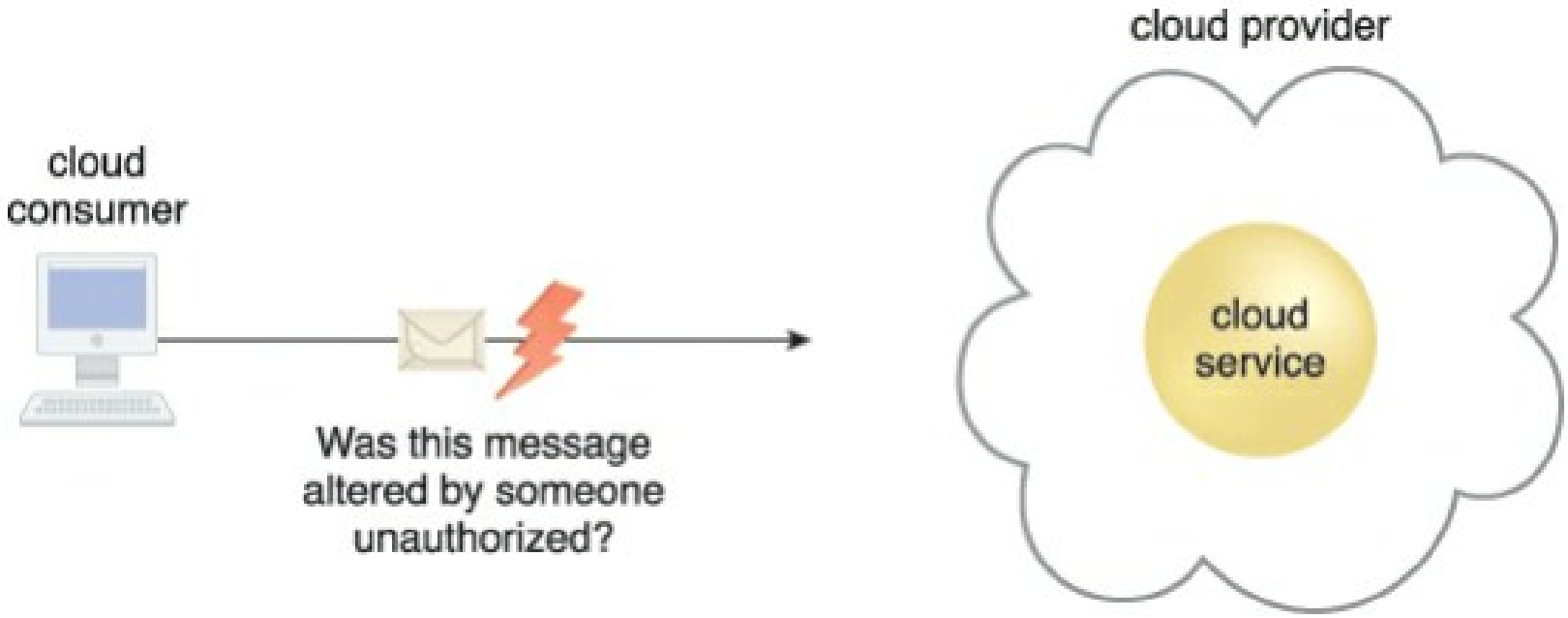
- Βασικό θέμα και στόχος σε ένα νέφος είναι η προστασία όλων των πόρων που φιλοξενούνται και προσφέρονται
- Πόροι μπορεί να είναι:
  - Αρχεία, δεδομένα, βάσεις
  - Λογισμικό, υπηρεσίες
  - Εικονικοί πόροι (π.χ., εικονικοί εξυπηρετητές, εικονικές συσκευές αποθήκευσης)
  - Φυσικοί πόροι (π.χ., φυσικοί εξυπηρετητές, φυσικές συσκευές αποθήκευσης)

Βασικές Αρχές – Εμπιστευτικότητα (Confidentiality)

- Πρόσβαση σε πόρο μόνο από εξουσιοδοτημένα μέρη
- Είδη πόρων προς προστασία:
  - Υπολογιστικοί πόροι
  - Διαβατικά δεδομένα
  - Δεδομένα αποθηκευμένα σε χώρους αποθήκευσης

Βασικές Αρχές – Ακεραιότητα (Integrity)

- Μη τροποποίηση πόρου από μη εξουσιοδοτημένο μέρος
- Σημαντικό ζήτημα για δεδομένα:
  - Τα δεδομένα παράδοσης από έναν καταναλωτή συμφωνούν με αυτά που λήφθηκαν από την αντίστοιχη υπηρεσία
- Για δεδομένα, η ακεραιότητα επεκτείνεται ως προς πως
  - τα δεδομένα αποθηκεύονται
  - γίνεται η επεξεργασία σε αυτά
  - επαναφέρονται από υπηρεσίες και άλλα είδη πόρων στο ΥΝ


cloud provider
cloud consumer
cloud service
Was this message altered by someone unauthorized?

Πηγή: [1]

Βασικές Αρχές – Αυθεντικότητα (Authenticity)

- Παροχή πόρου από μια εξουσιοδοτημένη πηγή
- Περιλαμβάνει την μη αποκήρυξη (non-repudiation) που είναι η αδυναμία ενός μέρους να αρνηθεί ή να αμφισβητήσει την αυθεντικότητα μιας αλληλεπίδρασης
- Πολύ χρήσιμη στην διενέργεια συναλλαγών που έχουν εμπορικό & οικονομικό αντίκτυπο
  - Παράδειγμα:
    - Ένας χρήστης δεν μπορεί να προσπελάσει ένα αρχείο μη αποκήρυξης, μετά την έκδοση μιας απόδειξης, χωρίς να παράγει μια εγγραφή για αυτή την πρόσβαση

Βασικές Αρχές – Διαθεσιμότητα

- Δυνατότητα πρόσβασης σε και χρήσης ενός πόρου μέσα σε συγκεκριμένο χρονικό διάστημα
- Η διαθεσιμότητα υπηρεσιών νέφους μπορεί να διαμοιράζεται ως προς την ευθύνη της μεταξύ του παρόχου νέφους και του φορέα νέφους
- Αν η λύση νέφους επεκτείνεται σε καταναλωτές νέφους (π.χ., είναι πάροχοι της λύσης αυτής), τότε η ευθύνη διαμοιράζεται και σε αυτούς

Βασικοί Όροι – Απειλή (Threat)

- Δυνητική παραβίαση της ασφάλειας με στόχο την ιδιωτικότητα και πρόκληση βλάβης
  - Οι απειλές μπορεί να προκαλούνται χειρωνακτικά ή αυτόματα για την εκμετάλλευση συγκεκριμένων αδυναμιών/τρωτοτήτων
  - Η πραγματοποίηση απειλής οδηγεί στην διενέργεια μιας επίθεσης

Βασικοί Όροι – Τρωτότητα (Vulnerability)

- Αδυναμία που μπορεί να τύχει εκμετάλλευσης
- Λόγοι αδυναμίας:
  - Ανεπαρκή αρχιτεκτονική ασφάλειας
  - Αδυναμίες πολιτικών ασφάλειας
  - Προστασία με ανεπαρκείς ελέγχους/μηχανισμούς ασφάλειας
  - Απενεργοποίηση ελέγχων/μηχανισμών ασφάλειας από προγενέστερη επίθεση
  - Χρήση μηχανισμών ασφάλειας ή συστατικών μερών με συγκεκριμένες τρωτότητες σε ένα σύστημα
- Συγκεκριμένοι λόγοι τρωτότητας πόρων ΤΠ:
  - Ανεπάρκεια συγκρότησης
  - Σφάλματα χρηστών
  - Ελαττώματα υλικού / υλικολογισμικού
  - Σφάλματα λογισμικού

Βασικοί Όροι – Κίνδυνος (Risk)

- Πιθανότητα απώλειας ή βλάβης που μπορεί να προκύψει από την εκτέλεση μιας δραστηριότητας
- Κίνδυνος συνήθως μετριέται/αποτιμάται από το επίπεδο της απειλής του & τον αριθμό των πιθανών ή γνωστών τρωτοτήτων
- Δύο μετρικές που μπορούν να χρησιμοποιηθούν για την αποτίμηση του κινδύνου:
  - Πιθανότητα μια απειλή να εκμεταλλευτεί τρωτότητες που βρίσκονται μέσα στον πόρο ΤΠ
  - Η προσδοκία της απώλειας όταν ο πόρος ΤΠ εκτεθεί σε κίνδυνο

Βασικοί Όροι – Έλεγχοι Ασφάλειας (Security Controls)

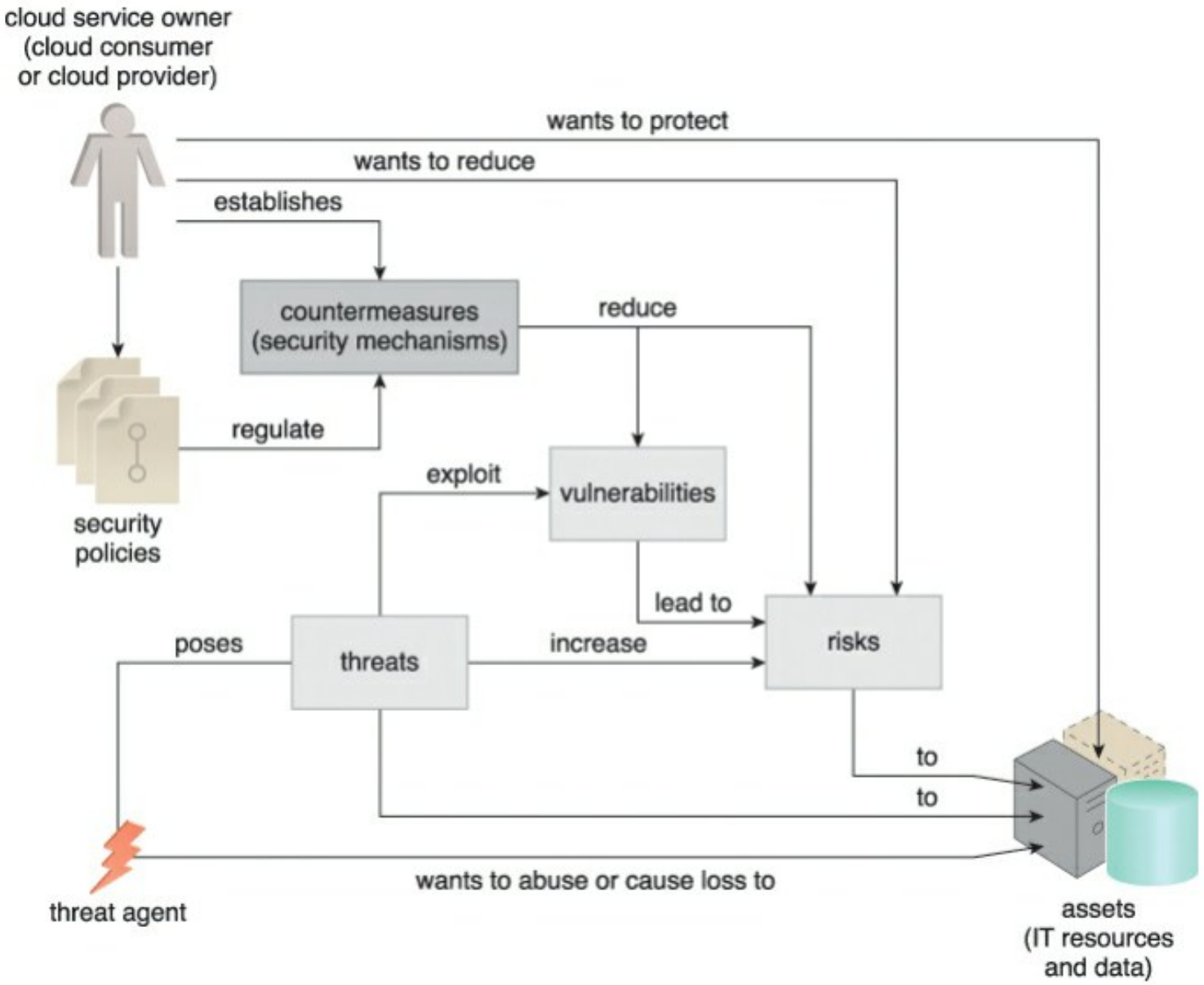
- Αντίμετρα για την αποτροπή απειλών ασφάλειας ή την απόκριση σε αυτές για την μείωση ή την εξάλειψη του αντίστοιχου κινδύνου
  - Λεπτομέρειες για την χρήση των αντιμέτρων ασφάλειας τίθενται στις πολιτικές ασφάλειας

Βασικοί Όροι – Μηχανισμοί Ασφάλειας (Security Mechanisms)

- Αντίμετρα ως συστατικά ενός αμυντικού πλαισίου για την προστασία πόρων ΤΠ, υπηρεσιών και πληροφοριών

Βασικοί Όροι – Πολιτικές Ασφάλειας (Security Policies)

- Ένα σύνολο κανόνων, ρυθμίσεων και πρακτικών που προσδιορίζουν πως πρέπει να υλοποιηθεί ένα σύστημα, μια υπηρεσία ή ένα σχέδιο ασφάλειας για την μέγιστη προστασία των ευαίσθητων και κρίσιμων πόρων ΤΠ
  - Ουσιαστικά καθορίζουν πως οι κανόνες, ρυθμίσεις και πρακτικές υλοποιούνται και επιβάλλονται/εφαρμόζονται
    - Παράδειγμα: καθορισμός της χρήσης και τοποθέτησης ενός ελέγχου ή μηχανισμού ασφαλείας


cloud service owner
(cloud consumer
or cloud provider)
wants to protect
wants to reduce
establishes
countermeasures
(security mechanisms)
reduce
regulate
security
policies
exploit
vulnerabilities
lead to
poses
threats
increase
risks
to
to
wants to abuse or cause loss to
threat agent
assets
(IT resources
and data)

Πηγή: [1]

Παράγοντες Επίδρασης στην Ασφάλεια

- Υπάρχουν 3 παράγοντες που επιδρούν στην ασφάλεια του νέφους:
  - Διαμοιρασμός ευθύνης
    - Ανάλογα με τα είδη των υπηρεσιών που έχουν επιλεγεί από τον καταναλωτή νέφους, οι ευθύνες ασφάλειας θα διαμοιραστούν μεταξύ του παρόχου και του καταναλωτή
    - Αυτός ο διαμοιρασμός θα πρέπει να συμφωνηθεί και αποτυπωθεί σε ένα SLA
    - Θα πρέπει επίσης να είναι δίκαιος
    - Αλλά η ασφάλεια των δεδομένων βρίσκεται σχεδόν υπό τον πλήρη έλεγχο των χρηστών
  - Μοντέλο ανάπτυξης
    - Σε ένα δημόσιο νέφος, οι πόροι διαμοιράζονται μέσω εικονικοποίησης με βάση το μοντέλο της πολλαπλής μίσθωσης
      - Οπότε ο πάροχος θα πρέπει να εξασφαλίσει την λογική απομόνωση των πελατών
    - Αντιθέτως, σε ένα ιδιωτικό νέφος, ο πελάτης είναι ένας οπότε είναι πιο εύκολη η εγκαθίδρυση συμμόρφωσης ασφάλειας και κανονιστικών πολιτικών

Παράγοντες Επίδρασης στην Ασφάλεια

- Υπάρχουν 3 παράγοντες που επιδρούν στην ασφάλεια του νέφους (συνέχεια):
  - Δυναμική τροφοδοσία & τοποθεσία πόρων
    - Οι πόροι που τροφοδοτούνται σε έναν χρήστη μπορεί να αλλάξουν δυναμικά (πχ. προσθήκη επιπλέον ή αφαίρεση υπαρχόντων)
    - Η τοποθεσία και κατανομή των πόρων αλλάζει επίσης ανάλογα με τις ανάγκες των χρηστών
      - Οι αλλαγές στην τοποθεσία μπορεί να επιδράσουν σε θέματα ασφάλειας ειδικότερα διότι οι πολιτικές και νόμοι για ασφάλεια και ιδιωτικότητα σε διαφορετικές χώρες ή περιοχές ποικίλλει

Πράκτορες Απειλών (Threat Agents)

- Οντότητα που παριστά μια απειλή διότι είναι σε θέση πραγματοποίησης μιας επίθεσης
- Οι απειλές μπορεί να είναι είτε εσωτερικές στο νέφος είτε εξωτερικές
- Οι εκμεταλλεύοντες αυτών μπορεί να είναι άνθρωποι ή προγράμματα λογισμικού
- Υπάρχουν διάφορα είδη πρακτόρων απειλών

Ανώνυμος Επιτιθέμενος (Anonymous Attacker)

- Ένας μη εμπιστευμένος καταναλωτής υπηρεσίας νέφους που δεν έχει καμία άδεια/δικαίωμα στο νέφος
  - Τυπικά, είναι ένα εξωτερικό πρόγραμμα που πραγματοποιεί δικτυακές επιθέσεις μέσω δημόσιων δικτύων
- Αν έχει ανεπαρκείς ή περιορισμένες πληροφορίες για τις πολιτικές & άμυνες ασφάλειας του νέφους, τότε μπορεί να εμποδιστεί η δυνατότητά του για αποτελεσματικές επιθέσεις

Ανώνυμος Επιτιθέμενος

- Συχνά καταφεύγει σε ενέργειες όπως παράκαμψη λογαριασμών χρηστών ή κλοπή διαπιστευτήριων χρηστών, ενώ καταφεύγει σε μεθόδους που διασφαλίζουν την ανωνυμία ή απαιτούν σημαντικούς πόρους για την δίωξή του

Κακόβουλος Πράκτορας Υπηρεσίας (Malicious Service Agent)

- Μπορεί να αιχμαλωτίσει και να προωθήσει την κίνηση δικτύου που ρέει μέσα σε ένα νέφος
- Υλοποιείται ως πράκτορας υπηρεσίας ή ως πρόγραμμα προσποιούμενο ότι είναι πράκτορας υπηρεσίας που διαθέτει λογική έκθεσης ή κακόβουλη λογική
- Μπορεί να υλοποιηθεί και ως εξωτερικό πρόγραμμα που μπορεί να αιχμαλωτίσει εξ αποστάσεως και πιθανώς να αλλοιώσει περιεχόμενα μηνυμάτων
- Οπότε, εν γένει, μπορεί να πραγματοποιήσει επιθέσεις ενδιάμεσου (man-in-the-middle attacks)

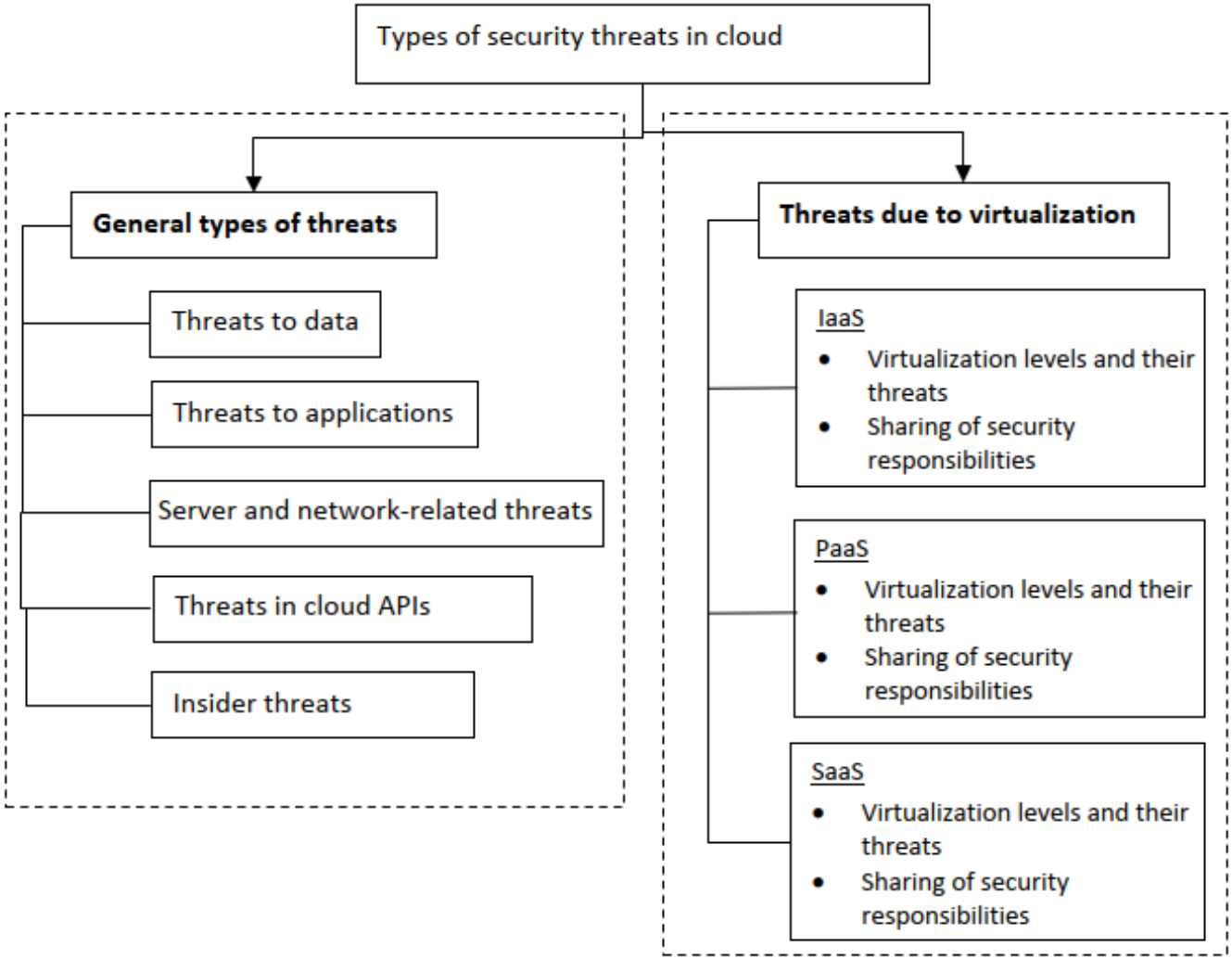
Εμπιστευμένος Επιτιθέμενος (Trusted Attacker)

- Μοιράζεται πόρους ΤΠ μαζί με καταναλωτές νέφους στο ίδιο περιβάλλον νέφους
- Προσπαθεί να εκμεταλλευθεί νόμιμα διαπιστευτήρια για να στοχεύσει πάροχους νέφους και μισθωτές νέφους (με τους οποίους μοιράζεται τους πόρους)
- Εκκινεί τις επιθέσεις του μέσα από τα όρια εμπιστοσύνης του νέφους μέσω της εκμετάλλευσης νόμιμων διαπιστευτήριων ή της οικειοποίησης ευαίσθητων ή εμπιστευτικών πληροφοριών
- Μπορεί να χρησιμοποιεί τους πόρους ΥΝ για διενέργεια μεγάλης ποικιλίας από επιθέσεις όπως παρενόχληση λογαριασμών email ή επιθέσεις (distributed) denial of service ((κατανεμημένης) άρνησης υπηρεσίας)

Κακόβουλος Εσωτερικός Χρήστης (Malicious Insider)

- Ανθρώπινοι πράκτορες απειλών που δρουν για λογαριασμό ή σε σχέση με τον πάροχο του νέφους
- Τρέχοντες ή πρώην εργαζόμενοι ή συνεργαζόμενα τρίτα μέρη που έχουν πρόσβαση στις εγκαταστάσεις του παρόχου νέφους
- Έχουν πολλές δυνατότητες καταστροφών λόγω των πιθανών προνομίων διαχείρισης ως προς την πρόσβαση σε πόρους ΤΠ που μπορεί να έχουν (που να είναι ήδη σε χρήση από τους καταναλωτές νέφους)

Είδη Απειλών στο Νέφος



Πηγή: [2]

Γενικά Είδη Απειλών - Απειλές σε Δεδομένα

- 4 είδη απειλών:
  - Παραβίαση δεδομένων (data breach)
    - Κατάσταση ή συμβάν όπου η εμπιστευτικότητα της ιδιωτικής πληροφορίας ενός ατόμου (πχ. οικονομικές πληροφορίες ή εγγραφές υγείας) φανερώνονται σε μη εξουσιοδοτημένα άτομα
  - Απώλεια δεδομένων (data loss)
    - Μπορεί να συμβεί οποιαδήποτε στιγμή για διάφορους λόγους όπως φυσικές καταστροφές, αποτυχία εξυπηρετητών, ανθρώπινα λάθη και λάθη δικτύου
    - Μετά την διακοπή υπηρεσίας (νέφους), ο καταναλωτής μπορεί να χάσει τα δεδομένα του εφόσον ο πάροχος τα διαγράφει αυτόματα

Γενικά Είδη Απειλών - Απειλές σε Δεδομένα

- 4 είδη απειλών (συνέχεια):
  - Κλείδωμα δεδομένων (data lock-in)
    - Αναφέρεται στην κατάσταση όπου οι καταναλωτές νέφους κλειδώνονται σε έναν πάροχο λόγω χρήσης ιδιόκτητων τεχνολογιών, διεπαφών και νομικών συμβολαίων
    - Δεν είναι βέβαιο τι θα συμβεί στα δεδομένα κατά την μετανάστευση σε άλλο πάροχο
      - Τα δεδομένα μπορεί να τροποποιηθούν για λόγους συμβατότητας
        - Αυτό μπορεί να έχει αρνητική επίδραση στην ακεραιότητα δεδομένων
  - Διαφυγή δεδομένων (data remanence)
    - Αναφέρεται στην διατήρηση των δεδομένων ακόμη και μετά από μια διαγραφή
      - Πχ. τα δεδομένα υπό διαγραφή μπορεί απλώς να σημειώνονται και όχι να διαγράφονται πραγματικά
    - Το φαινόμενο αυτό μπορεί να οδηγήσει τόσο σε εσκεμμένη ή ακούσια αποκάλυψη ευαίσθητης πληροφορίας σε μη εξουσιοδοτημένα άτομα

Γενικά Είδη Απειλών – Απειλές σε Εφαρμογές

- Υπάρχουν 4 απειλές
  - Έκχυση κακόβουλου λογισμικού (malware injection)
    - Αναφέρεται στο γεγονός έκχυσης κακόβουλου λογισμικού σε μια εφαρμογή από έναν επιτιθέμενο, ο οποίος εκμεταλλεύεται τις τρωτότητες της εφαρμογής
      - Η εκτέλεση του κακόβουλου λογισμικού θα οδηγήσει σε ανεπιθύμητες ενέργειες, η επίδραση των οποίων μπορεί να ποικίλλει
    - Να τονιστεί πως ένας επιτιθέμενος μπορεί να εκχύσει μια κακόβουλη εικόνα εικονικής μηχανής ή υπηρεσία σε ένα σύστημα νέφους
  - Επιλογές πίσω πόρτας & αποσφαλμάτωσης (backdoor & debug options)
    - Αποτελούν κοινές πρακτικές ανάπτυξης των προγραμματιστών για λόγους αποσφαλμάτωσης
    - Αν κώδικας πίσω πόρτας παραμείνει σε μια εφαρμογή σε περιβάλλον παραγωγής, τότε μπορεί να ανιχνευθεί και να γίνει εκμεταλλεύσιμος από επιτιθέμενους

Γενικά Είδη Απειλών – Απειλές σε Εφαρμογές

- Υπάρχουν 4 απειλές (συνέχεια)
  - Κρυφά πεδία σε φόρμες ιστού (hidden fields in web forms)
    - Κρυφά πεδία φόρμας σε κώδικα HTML που περιέχουν μεταβλητές κατάστασης στις οποίες καταχωρείται κρίσιμη πληροφορία όπως κωδικοί
      - Αυτά μπορεί να γίνουν ορατά όταν οπτικοποιείται ο πηγαίος κώδικας μιας ιστοσελίδας
      - Οπότε ένας επιτιθέμενος μπορεί είτε να προσπελάσει κρίσιμη πληροφορία ή να αλλάξει το περιεχόμενό της
  - Κακή διαμόρφωση εφαρμογών (application misconfiguration)
    - Αν οι εφαρμογές διαμορφωθούν με λιγότερο ασφαλείς ρυθμίσεις, είναι δυνατή η εκμετάλλευσή των αντίστοιχων κενών από επιτιθέμενους
      - Πχ. ένας εξυπηρετητής ιστού (web server) μπορεί να έχει διαμορφωθεί ώστε να επιτρέπει στην πλοήγηση και πρόσβαση σε διάφορα ευρετήρια, δεδομένα και πόρους του συστήματος
      - Πχ. προκαθορισμένες εφαρμογές και υπηρεσίες web container που είναι ευάλωτες όσον αφορά την ασφάλεια

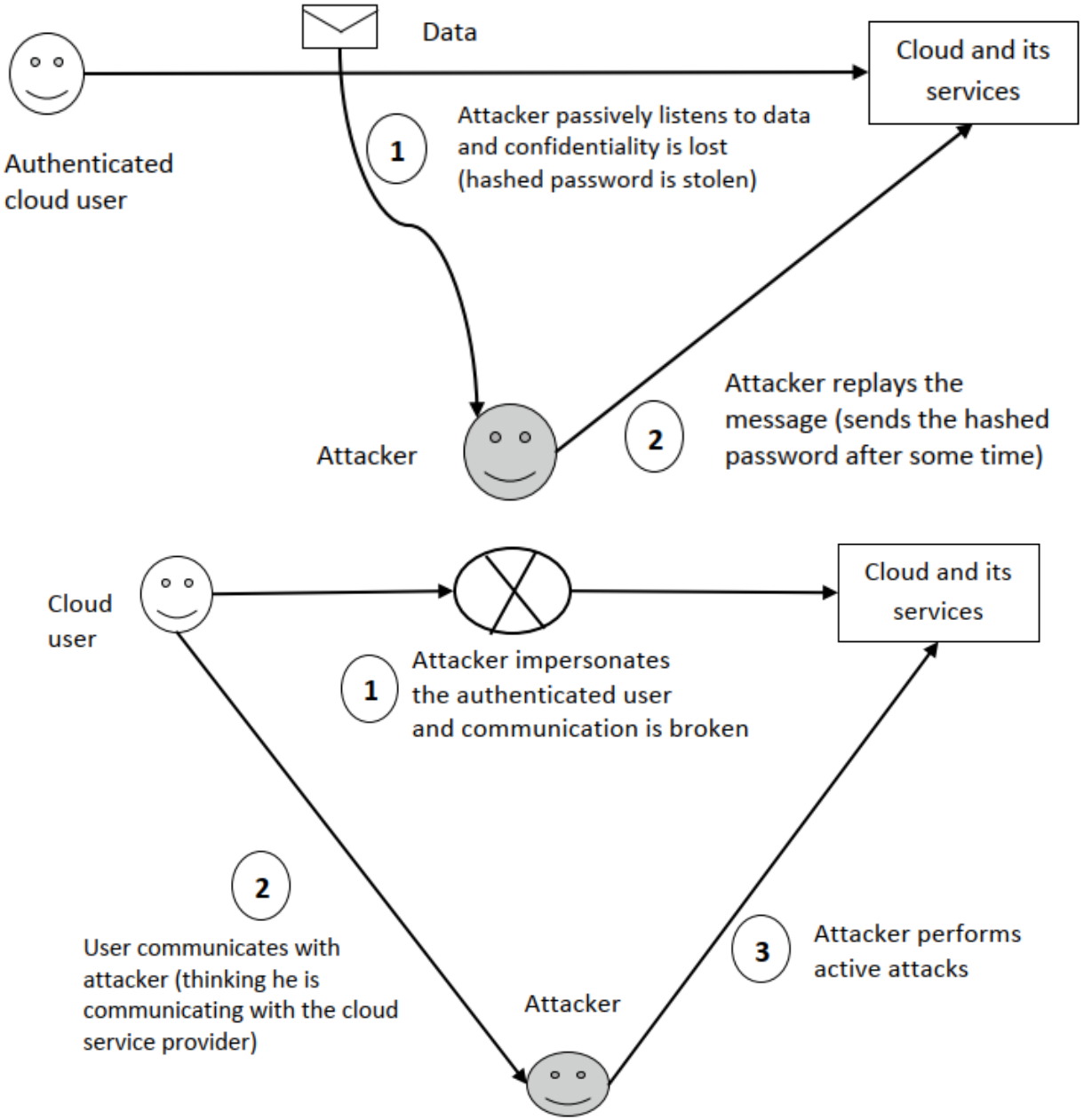
Γενικά Είδη Απειλών – Απειλές σε Εξυπηρετητές & Δίκτυο

- Μπορεί να είναι παθητικές ή ενεργές και χωρίζονται σε:
  - Υποκλοπή της κυκλοφορίας (traffic eavesdropping)
    - Παθητική υποκλοπή δεδομένων από τον επιτιθέμενο / ενδιάμεσο που οδηγεί σε παραβίαση εμπιστευτικότητας δεδομένων
  - Επίθεση επανάληψης (replay attack)
    - Ο επιτιθέμενος μπορεί να υποκλέψει ένα μήνυμα και να επαναλάβει την αποστολή του μηνύματος στον παραλήπτη, ο οποίος υποθέτει πως το μήνυμα έρχεται από τον αρχικό/γνήσιο αποστολέα

Γενικά Είδη Απειλών – Απειλές σε Εξυπηρετητές & Δίκτυο

- Μπορεί να είναι παθητικές ή ενεργές και χωρίζονται σε (συνέχεια):
  - Επίθεση ενδιάμεσου (man-in-the-middle attack)
    - Ο επιτιθέμενος μπαίνει ανάμεσα στον καταναλωτή και τον πάροχο/υπηρεσία νέφους
    - Μπορεί παθητικά να υποκλέψει πληροφορία ή μπορεί να πλαστογραφήσει τον καταναλωτή ώστε να εκτελέσει ενεργές επιθέσεις
    - Μπορεί επίσης να πλαστογραφείται ο πάροχος/υπηρεσίας έτσι ώστε ο καταναλωτής να ξεγελαστεί να επικοινωνεί με τον επιτιθέμενο κι όχι με τον πάροχο/υπηρεσία
  - Επιθέσεις έκχυσης κακόβουλου λογισμικού (malware injection attack)
    - Ο επιτιθέμενος εισάγει μια κακόβουλη υπηρεσία ή κώδικα στις υπηρεσίες που παρέχονται από τον αντίστοιχο πάροχο εκμεταλλευόμενος τρωτότητες στο λογισμικό του νέφους
      - Το κακόβουλο λογισμικό αντιστοιχεί σε ενεργό περιεχόμενο όπως ιούς ή σκουλήκια
      - Το αυξανόμενο πλήθος στον αριθμό των κινητών συσκευών και κοινωνικών μέσων που χρησιμοποιούνται έχει οδηγήσει σε αύξηση της δημιουργίας κακόβουλων λογισμικών
      - Διαφορετικά είδη κακόβουλου λογισμικού στοχεύουν σε διαφορετικούς πόρους της υποδομής νέφους όπως εξυπηρετητές, συσκευές αποθήκευσης δεδομένων και δικτυακές συσκευές

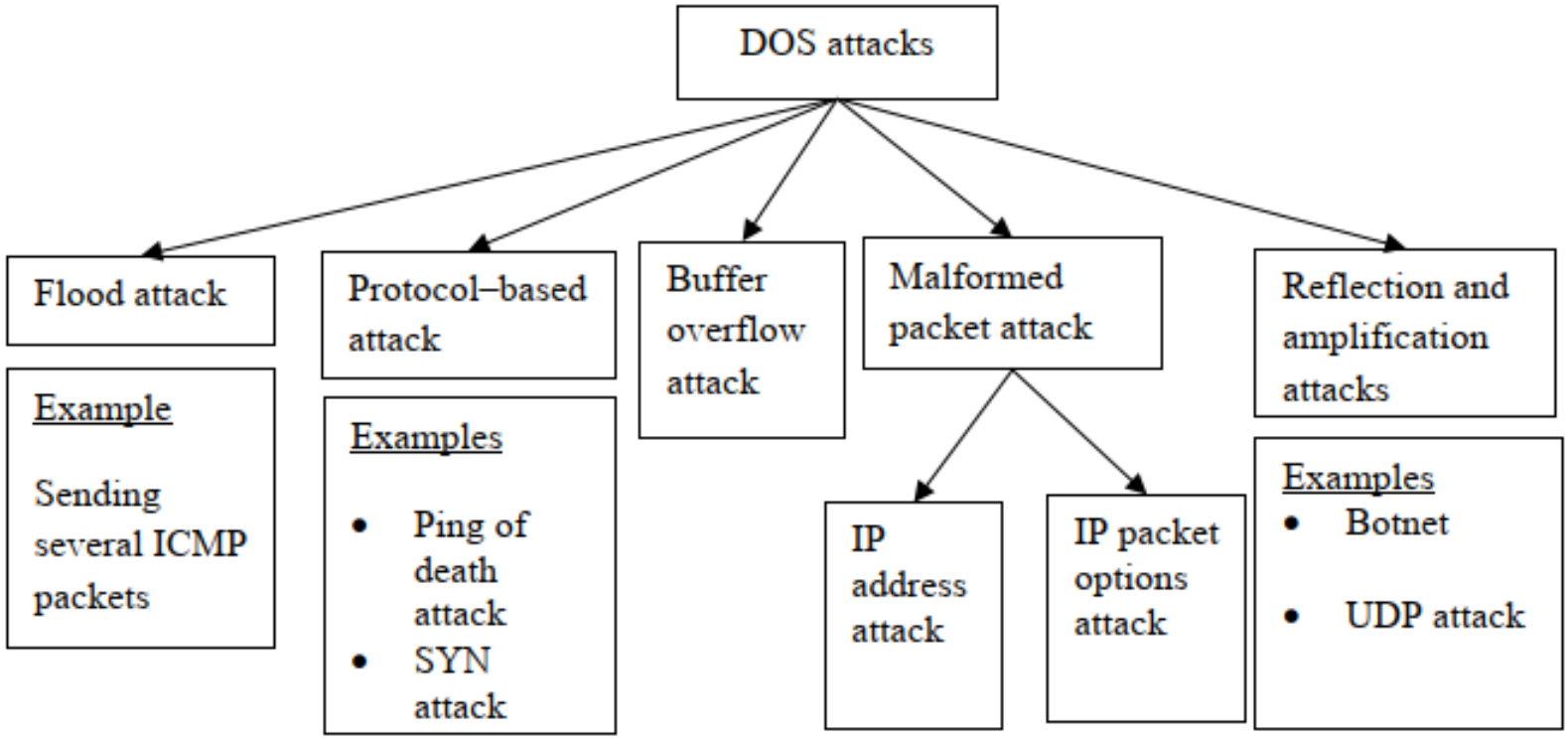
Πηγή: [2]


Data
Cloud and its services
Authenticated cloud user
1
Attacker passively listens to data and confidentiality is lost (hashed password is stolen)
Attacker
2
Attacker replays the message (sends the hashed password after some time)
Cloud user
Cloud and its services
1
Attacker impersonates the authenticated user and communication is broken
2
User communicates with attacker (thinking he is communicating with the cloud service provider)
Attacker
3
Attacker performs active attacks

Γενικά Είδη Απειλών – Απειλές σε Εξυπηρετητές & Δίκτυο

- Πειρατεία συνόδων (session hijacking)
  - Ο επιτιθέμενος ψάχνει σε ένα δίκτυο με υψηλή κίνηση για χρήστες που χρησιμοποιούν λιγότερο ασφαλή πρωτόκολλα και παρεμβάλλεται ώστε να υποκλέψει την ταυτότητα συνόδου τους και να τους πλαστογραφήσει με την βοήθεια εργαλείων λογισμικού για υποκλοπή πακέτων και σάρωση θυρών
- Άρνηση υπηρεσίας (denial-of-service)
  - Στοχεύει στην διακοπή των υπηρεσιών προς νόμιμους χρήστες από έναν εξυπηρετητή νέφους είτε για συγκεκριμένο χρονικό διάστημα ή και για πάντα
  - Ο επιτιθέμενος προσπαθεί να καταναλώσει το διαθέσιμο εύρος ζώνης δικτύου και να επιτεθεί στον εξυπηρετητή πλημμυρίζοντάς τον με ψευδή δεδομένα ή αιτήσεις ώστε ο εξυπηρετητής και οι υποκείμενοι πόροι του να κατακλυστούν
  - Μπορεί να πάρει απλή ή κατανεμημένη μορφή
    - Απλή μορφή: οι επιθέσεις πραγματοποιούνται μόνο από πια πηγή
    - Κατανεμημένη μορφή: οι επιθέσεις πραγματοποιούνται από ένα δίκτυο από ξενιστές (πχ. δίκτυο από υπολογιστές ζόμπι)

Είδη Επιθέσεων Άρνησης Υπηρεσίας



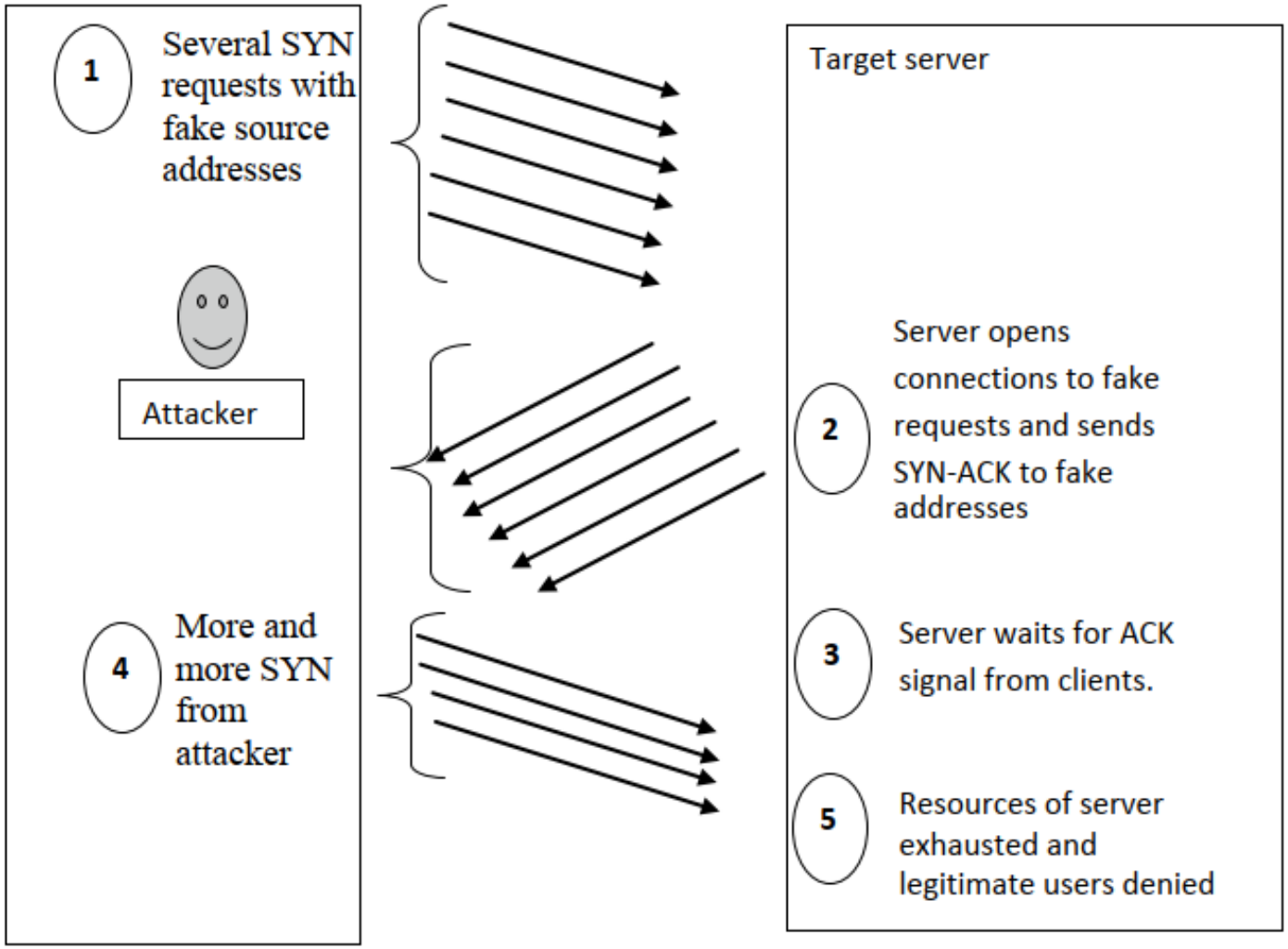
Πηγή: [2]

Είδη Επιθέσεων Άρνησης Υπηρεσίας

- Επίθεση πλημμυρίσματος (flooding attack)
  - Ο επιτιθέμενος πλαστογραφεί έναν νόμιμο χρήστη και αποκτά πρόσβαση στο νέφος ως ταυτοποιημένος χρήστης
  - Έπειτα, δημιουργεί μεγάλες ψευδείς αιτήσεις ICMP (Internet Control Message Protocol) και τις στέλνει σε εξυπηρετητές νέφους
  - Οι εξυπηρετητές θα προσπαθήσουν να επικυρώσουν την αυθεντικότητα των ψευδών αιτήσεων αντί να εξυπηρετήσουν τους νόμιμους χρήστες

Είδη Επιθέσεων Άρνησης Υπηρεσίας

- Επίθεση βασιζόμενη στο πρωτόκολλο (protocol-based attack)
  - Επίθεση ping of death
    - Σύμφωνα με το πρωτόκολλο IP το μέγεθος ενός ping/IP πακέτου με το ωφέλιμό του φορτίο είναι 65535 bytes αλλά συνήθως το μέγεθος των ping πακέτων που στέλνονται είναι αρκετά μικρότερο
      - Τα περισσότερα ΛΣ δεν γνωρίζουν πως να χειριστούν μεγάλα ping πακέτα οπότε είτε κρασάρουν ή επανεκκινούνται
  - Επίθεση SYN
    - Αφορά αδυναμία της διαδικασίας χειραψίας του TCP πρωτοκόλλου
      - Ο επιτιθέμενος στέλνει ένα μεγάλο αριθμό από SYN αιτήσεις με πλαστές διευθύνσεις πηγής
      - Σε κάθε αίτηση, ο εξυπηρετητής αναγκάζεται να ανοίξει σύνδεση με την πλαστή διεύθυνση, να στείλει μια απάντηση SYN-ACK και έπειτα να αναμένει πίσω μια απάντηση ACK από τον υποτιθέμενο πελάτη (πράγμα που δεν συμβαίνει)
      - Οπότε, η ουρά TCP του εξυπηρετητή θα γεμίσει και δεν θα μπορεί πια να εξυπηρετήσει πραγματικούς πελάτες
      - Επίσης, οι ανοικτές συνδέσεις καταναλώνουν πόρους κάνοντας τον εξυπηρετητή πολύ αργό


1
Several SYN requests with fake source addresses
Attacker
4
More and more SYN from attacker
Target server
2
Server opens connections to fake requests and sends SYN-ACK to fake addresses
3
Server waits for ACK signal from clients.
5
Resources of server exhausted and legitimate users denied

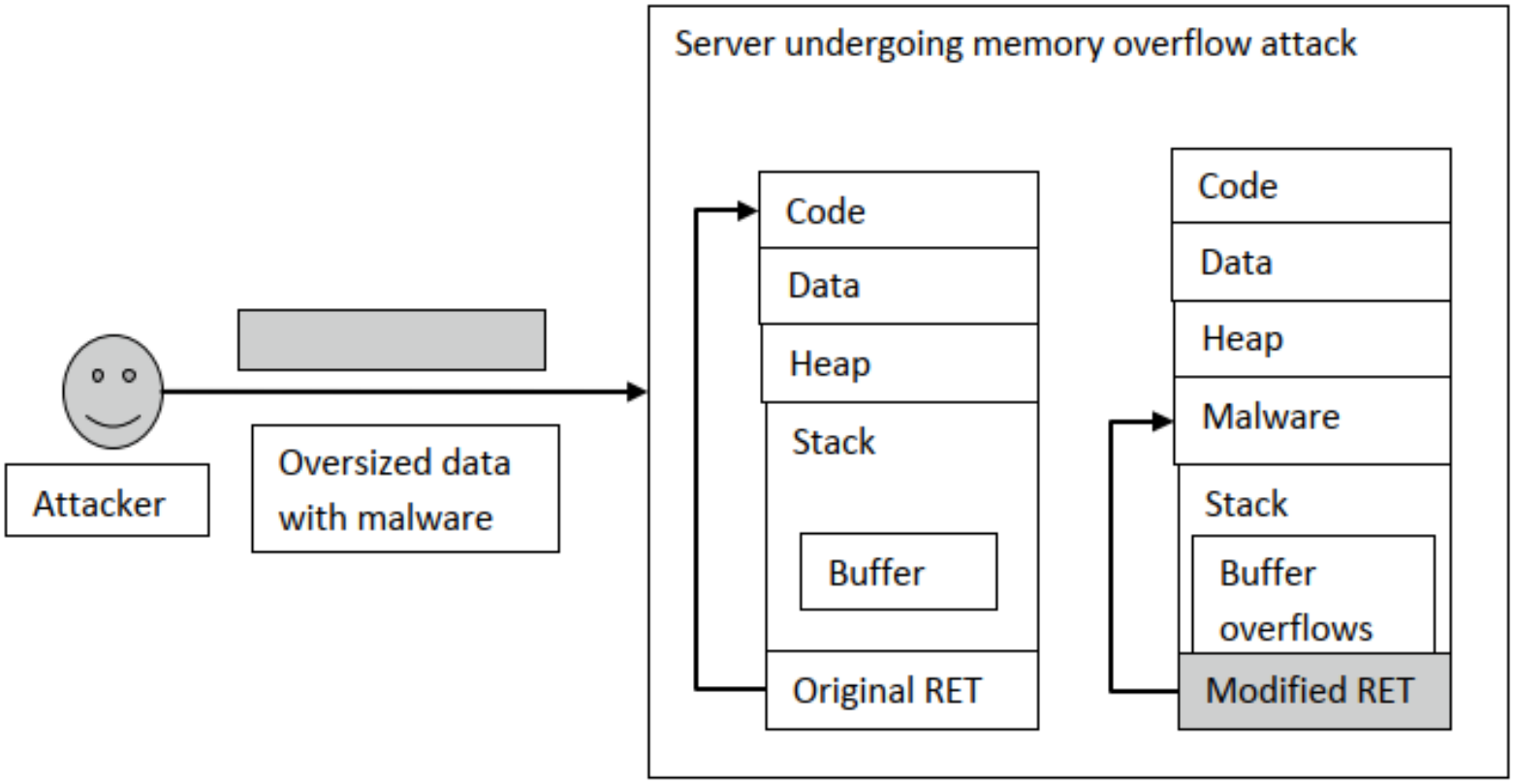
Πηγή: [2]

Είδη Επιθέσεων Άρνησης Υπηρεσίας

- Υπερχείλιση αποταμιευτή (buffer overflow)
  - Ο επιτιθέμενος στέλνει ψευδή δεδομένα με περισσότερο μέγεθος σε σχέση με αυτό του αποταμιευτή, επαναγράφοντας με αυτό τον τρόπο τα πραγματικά δεδομένα
  - Μπορεί να επαναγραφούν και δεδομένα στην κύρια μνήμη πέρα από τα όρια του αποταμιευτή, οδηγώντας σε λανθάνουσα συμπεριφορά προγραμμάτων, συμπεριλαμβανομένου λαθών πρόσβασης στη μνήμη, λανθασμένων αποτελεσμάτων και κρασαρισμάτων

Είδη Επιθέσεων Άρνησης Υπηρεσίας

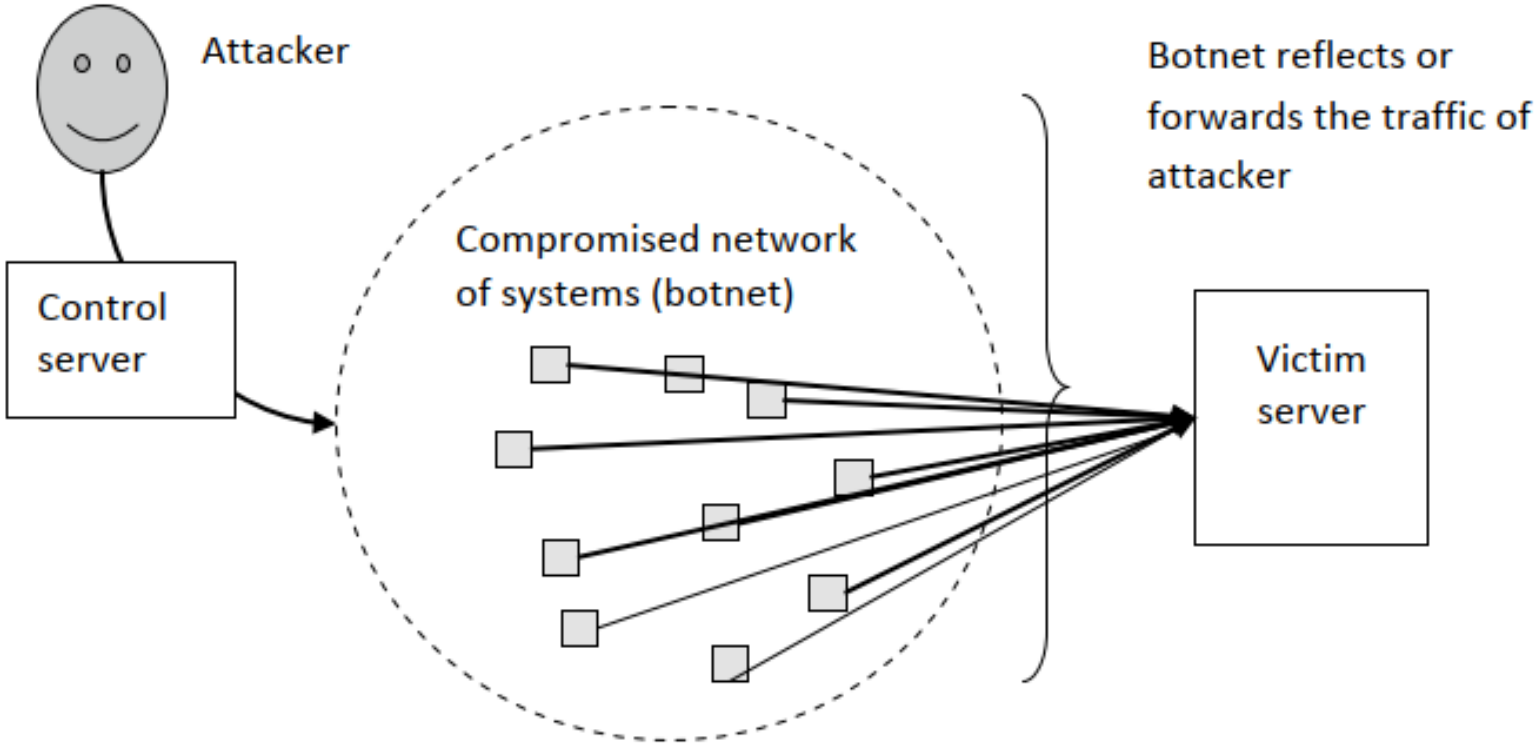
- Δύσμορφα Πακέτα (malformed packet)
  - Ο επιτιθέμενος αποστέλλει πακέτα με λανθασμένη μορφοποίηση στον εξυπηρετητή
    - Υπάρχουν 2 είδη επιθέσεων που μπορούν να συμβούν μέσω IP πακέτων
      - Επίθεση διεύθυνσης IP
        - Χρήση ίδιας διεύθυνσης πηγής και προορισμού. Ο εξυπηρετητής δεν γνωρίζει τι να κάνει με το κακόβουλο πακέτο και μπορεί να κρασάρει
      - Επίθεση επιλογής
        - Ο επιτιθέμενος συμπληρώνει όλες τις επιλογές του IP πακέτου
        - Οπότε, παίρνει πολύ περισσότερο χρόνο η επεξεργασία του πακέτου από τον εξυπηρετητή
        - Αν σταλούν πολλά δύσμορφα πακέτα, τότε ο εξυπηρετητής δεν μπορεί να καταναλώσει χρόνο για την εξυπηρέτηση πραγματικών, εύμορφων πακέτων


Server undergoing memory overflow attack
Code
Data
Heap
Stack
Buffer
Original RET
Code
Data
Heap
Malware
Stack
Buffer overflows
Modified RET
Attacker
Oversized data with malware

Πηγή: [2]

Είδη Επιθέσεων Άρνησης Υπηρεσίας

- Επίθεση ανάκλασης (reflection attack)
  - Ο επιτιθέμενος χρησιμοποιεί πολλά ενδιάμεσα συστήματα (ένα botnet) για να επιτεθεί σε έναν εξυπηρετητή
  - Το δίκτυο των ενδιάμεσων συστημάτων διαμορφώνεται ώστε να ανακλά ή να προωθεί ψευδείς αιτήσεις στον εξυπηρετητή
    - Μπορεί επίσης να χρησιμοποιηθεί ένα κυμαινόμενο εύρος από IP διευθύνσεις ώστε και το ίδιο το δίκτυο να παραμείνει μη ανιχνεύσιμο
- Επίθεση ενίσχυσης (amplification attack)
  - Παρόμοια με την επίθεση ανάκλασης αλλά πιο αφόρητη
  - Ο επιτιθέμενος χρησιμοποιεί πρωτόκολλα όπως το NTP (Network Time Protocol) που μπορεί να περιλαμβάνουν επερωτήσεις που μπορεί να οδηγούν σε πολύ μεγάλες απαντήσεις
    - Πχ. η επερώτηση MON_GETLIST αφορά τις διευθύνσεις με τις οποίες έχει επικοινωνήσει ο εξυπηρετητής
    - Η απάντηση σε μια τέτοια επερώτηση είναι μεγάλη διότι μπορεί να περιλαμβάνει τις διευθύνσεις μέχρι 600 μηχανημάτων
  - Οπότε, αποστέλλει ένα μεγάλο πλήθος από τέτοιες επερωτήσεις για να κατακλύσει τους πόρους των αντίστοιχων εξυπηρετητών (στο νέφος)


Attacker
Botnet reflects or
forwards the traffic of
attacker
Compromised network
of systems (botnet)
Control
server
Victim
server

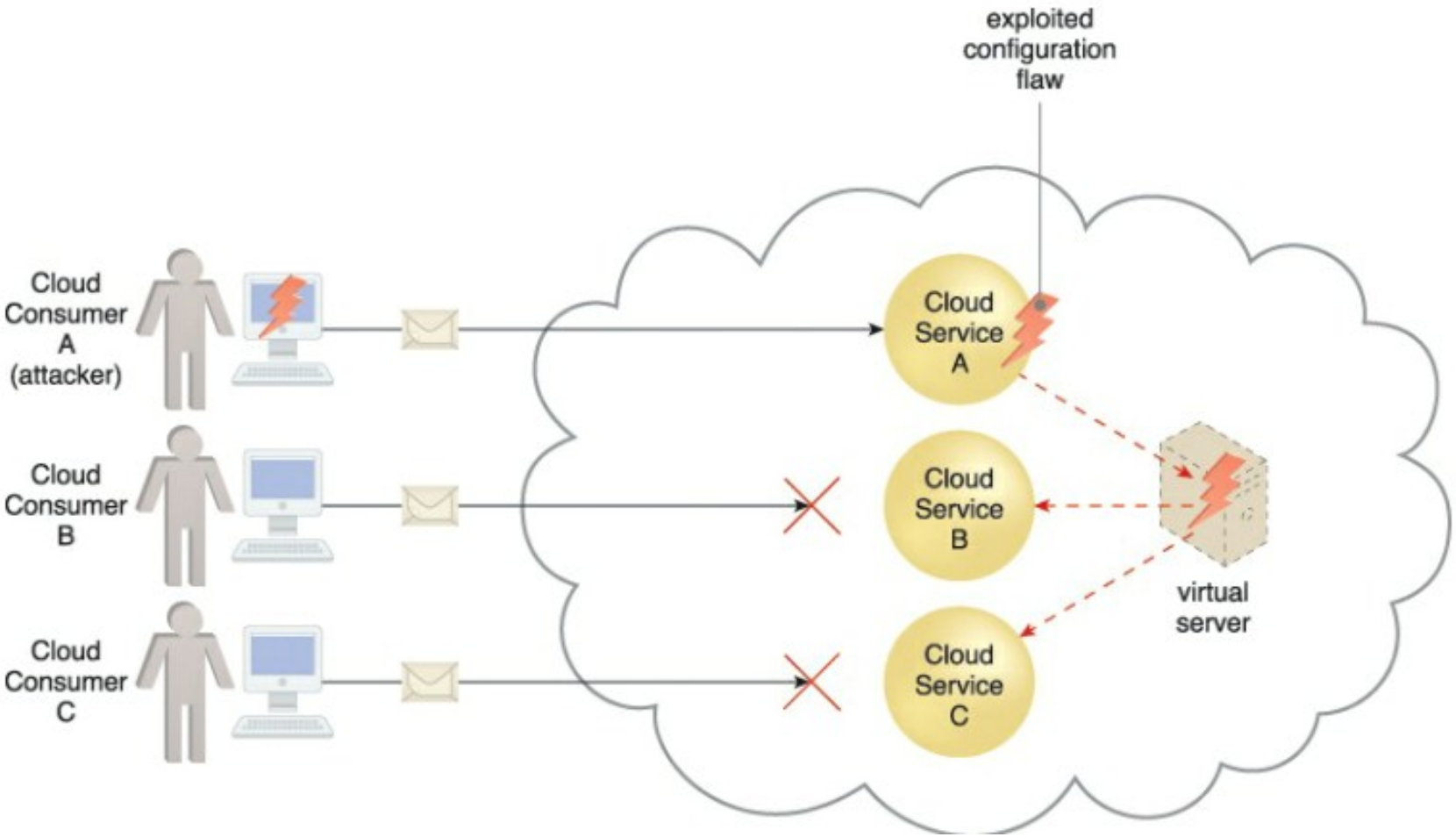
Πηγή: [2]

Γενικά Είδη Απειλών

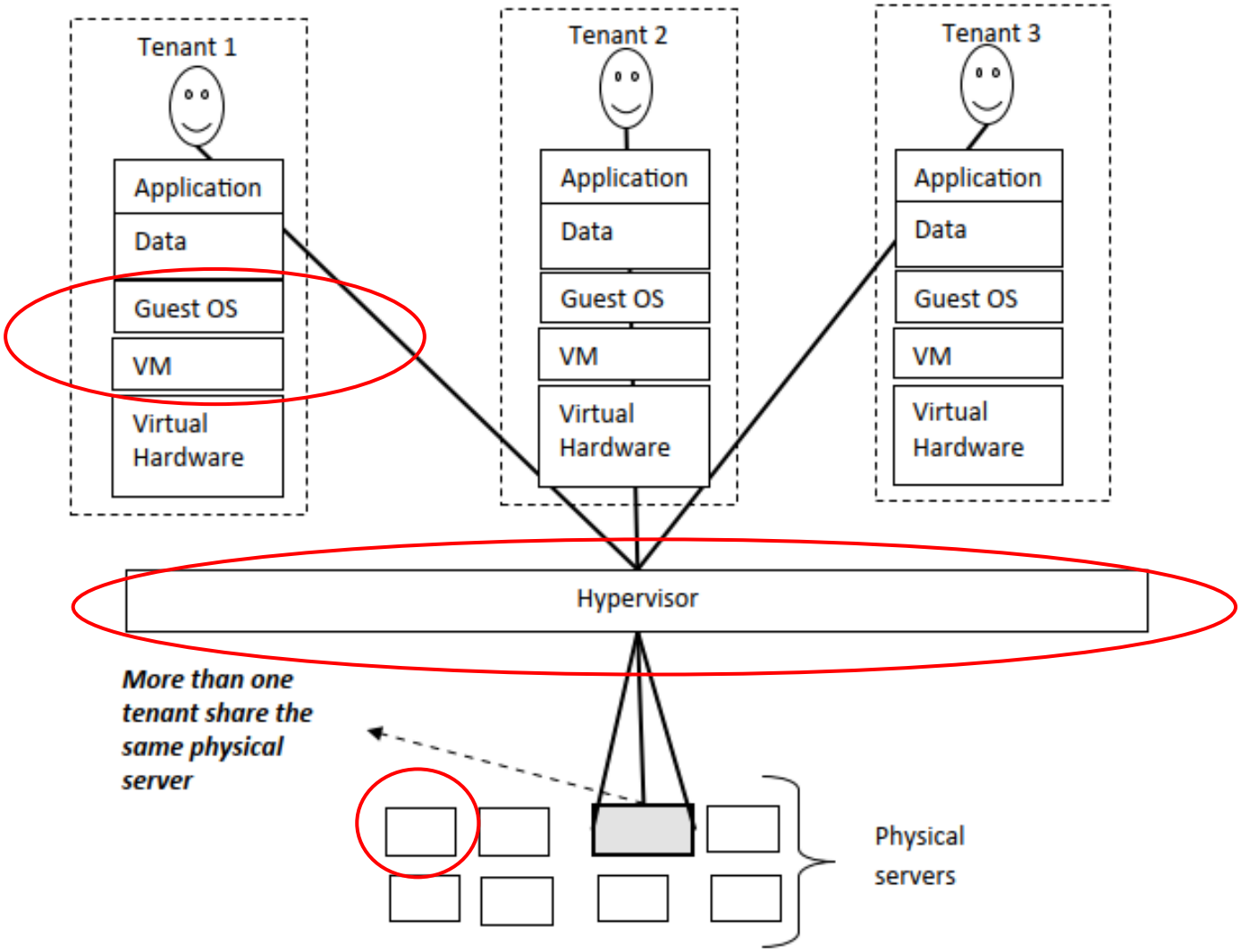
- Τρωτότητες σε APIs & Διεπαφές Νεφών
  - Οι υπηρεσίες νέφους συνήθως προσφέρονται μέσω ενός API ή διεπαφής
  - Οπότε, οποιαδήποτε τρωτότητα αφορά ένα τέτοιο API/διεπαφή μπορεί να έχει αντίκτυπο στην ασφάλεια των υποκείμενων πόρων και υπηρεσιών
    - Πχ. λάθος προσδιορισμός κανόνων πρόσβασης, μη χρήση κρυπτογράφησης, κλπ.
- Εσωτερικές Απειλές
  - Απειλή που τίθεται από ένα εξουσιοδοτημένο άτομο, το οποίο κακομεταχειρίζεται τα δικαιώματά του
  - Μπορεί να οδηγήσει σε μεγαλύτερο αντίκτυπο διότι ένα τέτοιο άτομο έχει περισσότερα δικαιώματα από έναν εξωτερικό επιτιθέμενο
  - Το άτομο αυτό μπορεί να εργάζεται για τον πάροχο ή για μια επιχείρηση που χρησιμοποιεί τις υπηρεσίες που προσφέρονται από το νέφος

Ελαττωματικές Υλοποιήσεις

- Η ακεραιότητα, εμπιστευτικότητα και διαθεσιμότητα των πόρων ΤΠ ενός νέφους (τόσο των φυσικών πόρων ΤΠ του πάροχου όσο και των εικονικών πόρων ΤΠ των καταναλωτών που φιλοξενούνται από τους φυσικούς) μπορεί να επηρεαστεί αρνητικά από τρωτότητες που εισάγονται λόγω ανεπαρκούς σχεδίασης, υλοποίησης ή συγκρότησης υπηρεσιών νέφους
- Παράδειγμα:
  - Λανθασμένα υλοποιημένη υπηρεσία νέφους οδηγεί σε κατάρρευση του εικονικού εξυπηρετητή που την φιλοξενεί
    - Αυτό έχει επίπτωση και στα άλλα στιγμιότυπα ή υπηρεσίες νέφους που φιλοξενούνται από τον ίδιο εξυπηρετητή


exploited
configuration
flaw
Cloud
Consumer
A
(attacker)
Cloud
Consumer
B
Cloud
Consumer
C
Cloud
Service
A
Cloud
Service
B
Cloud
Service
C
virtual
server

Πηγή: [1]


Tenant 1
Application
Data
Guest OS
VM
Virtual Hardware
Tenant 2
Application
Data
Guest OS
VM
Virtual Hardware
Tenant 3
Application
Data
Guest OS
VM
Virtual Hardware
Hypervisor
More than one tenant share the same physical server
Physical servers

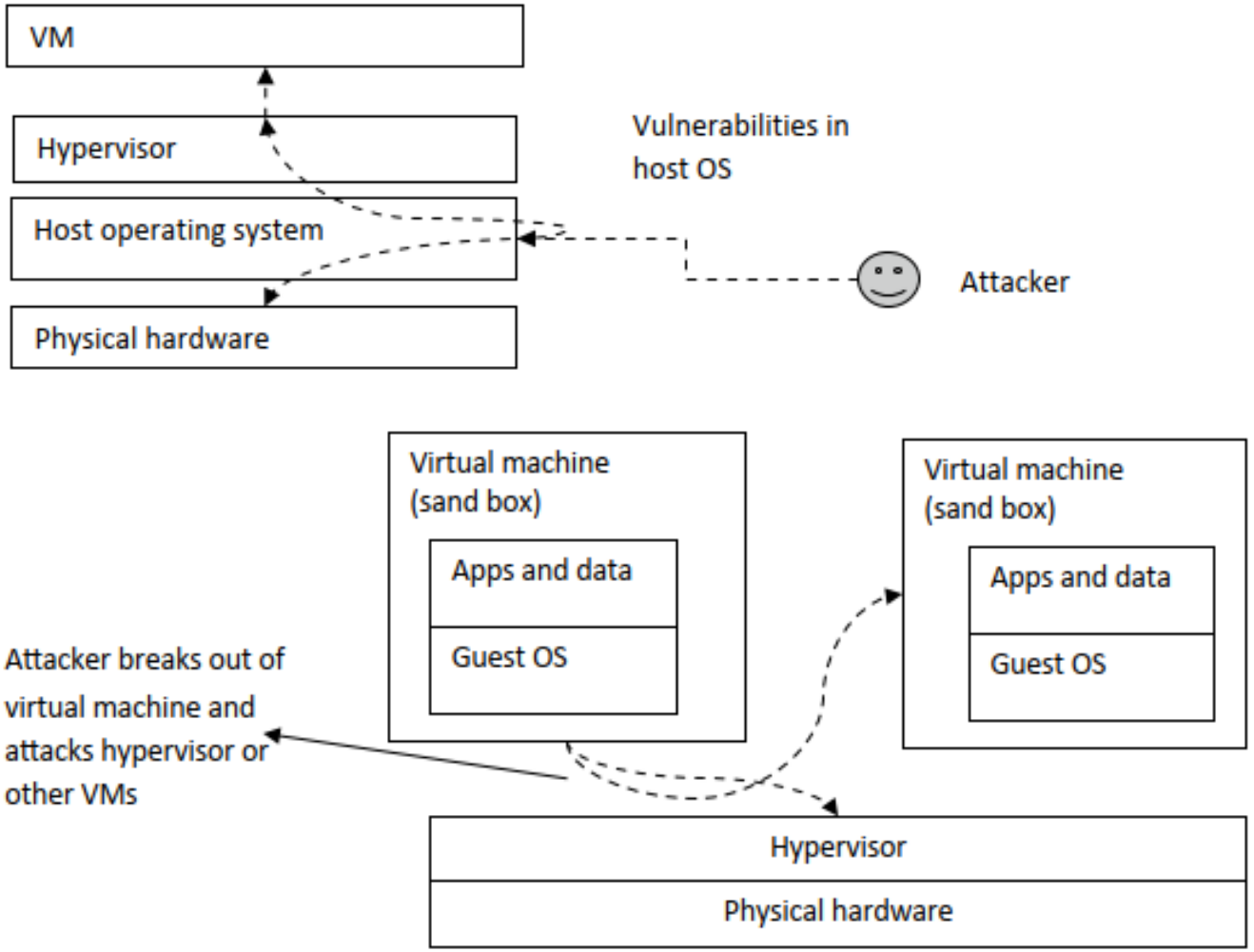
Πηγή: [2]

Απειλές λόγω Εικονικοποίησης στο Επίπεδο IaaS

- Επίθεση στον hypervisor μέσω του ΛΣ φιλοξενίας
  - Η εικονικοποίηση μπορεί να πραγματοποιείται στο ΛΣ φιλοξενίας
  - Οπότε, είναι δυνατό ένας επιτιθέμενος να εκμεταλλευτεί τρωτότητες αυτού του ΛΣ ώστε να επιτεθεί στον hypervisor και στις εικονικές μηχανές πάνω από αυτόν

Απειλές λόγω Εικονικοποίησης στο Επίπεδο IaaS

- Επίθεση απόδρασης εικονικής μηχανής (VM escape attack)
  - Μια εικονική μηχανή είναι ένα απομονωμένο υπολογιστικό περιβάλλον που προσφέρεται στους καταναλωτές ώστε να μπορούν να διατάσσουν το φιλοξενούμενο ΛΣ και άλλα είδη λογισμικού πάνω από αυτό χωρίς να διαταράσσεται αυτό το περιβάλλον
  - Σε αυτό το είδος επίθεσης, ο επιτιθέμενος μπορεί να τρέξει κακόβουλο κώδικα στην εικονική μηχανή που επιτρέπει στο φιλοξενούμενο ΛΣ της να εκμεταλλευτεί τρωτότητες της εικονικής μηχανής ώστε να αλληλεπιδράσει άμεσα με τον υποκείμενο hypervisor ή με άλλες εικονικές μηχανές που διαμοιράζονται το ίδιο υλικό


VM
Hypervisor
Host operating system
Physical hardware
Vulnerabilities in host OS
Attacker
Virtual machine (sand box)
Apps and data
Guest OS
Virtual machine (sand box)
Apps and data
Guest OS
Attacker breaks out of virtual machine and attacks hypervisor or other VMs
Hypervisor
Physical hardware

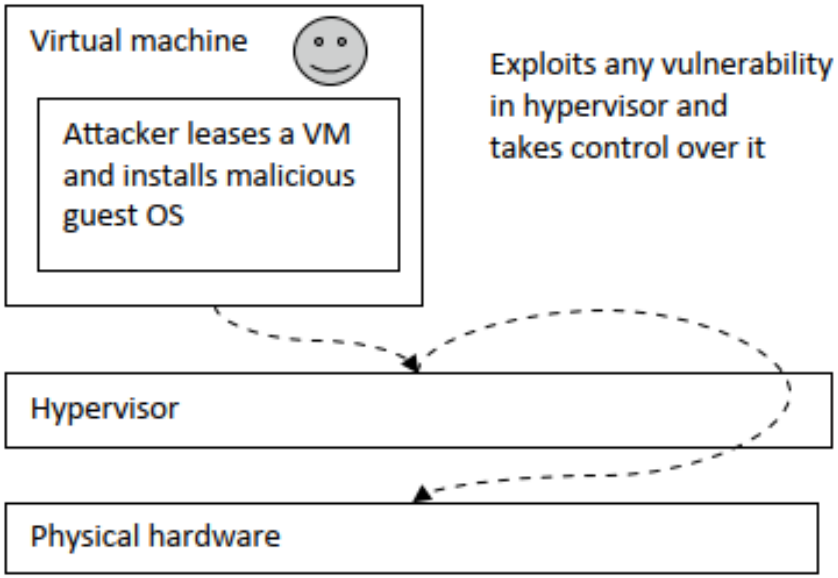
Πηγή: [2]

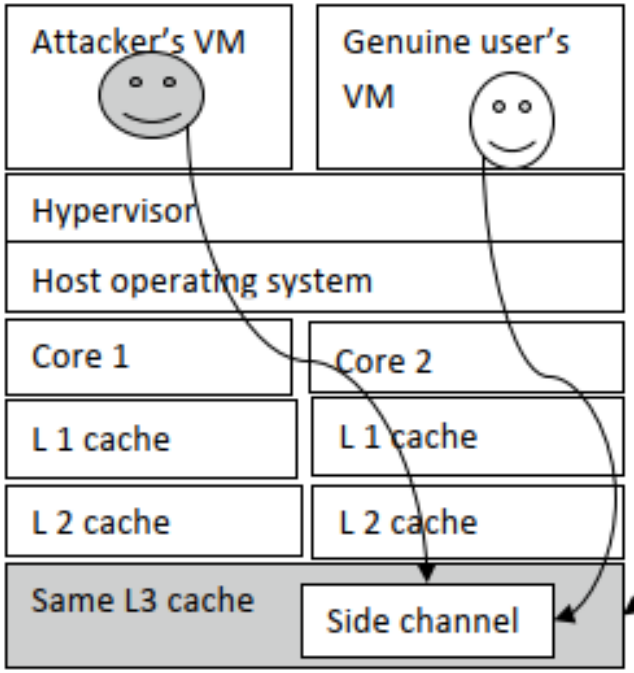
Απειλές Λόγω Εικονικοποίησης στο Επίπεδο IaaS

- Επίθεση Πειρατείας (hyperjacking attack)
  - Ο επιτιθέμενος δανείζεται μια εικονική μηχανή ώστε να εγκαταστήσει ένα κακόβουλο ΛΣ, το οποίο εκμεταλλεύεται τρωτότητες του υποκείμενου hypervisor
    - Μπορεί να αλλάξει τον πηγαίο κώδικα του hypervisor ώστε να πάρει τον έλεγχο της μνήμης και των δεδομένων άλλων (φιλοξενούμενων) εικονικών μηχανών

Απειλές Λόγω Εικονικοποίησης στο Επίπεδο IaaS

- Επίθεση πλευρικού καναλιού (cache-based side channel virtual machine attack)
  - Κάθε ΚΜΕ σε μια αρχιτεκτονική υλικού πολλαπλών ΚΜΕ έχει ξεχωριστή κρυφή μνήμη μόνο για 2 επίπεδα (L1 & L2). Όμως, η κρυφή μνήμη για το τρίτο επίπεδο (L3) είναι κοινή για περισσότερες από μια ΚΜΕ
  - Αυτό το γεγονός μπορεί να γίνει εκμεταλλεύσιμο από έναν επιτιθέμενο
    - Λόγω ανεπαρκούς λογικής απομόνωσης στο επίπεδο L3, είναι δυνατή η έκθεση δεδομένων και πληροφορίας από την εικονική μηχανή με την οποία συνφιλοξενείται η εικονική μηχανή του επιτιθέμενου
      - Αυτό πραγματοποιείται μέσω μια επίθεσης πλευρικού καναλιού





Both attacker and genuine user share the same L3 cache. They are co-residents of the same physical core. Attacker creates side channel and tries to track secret

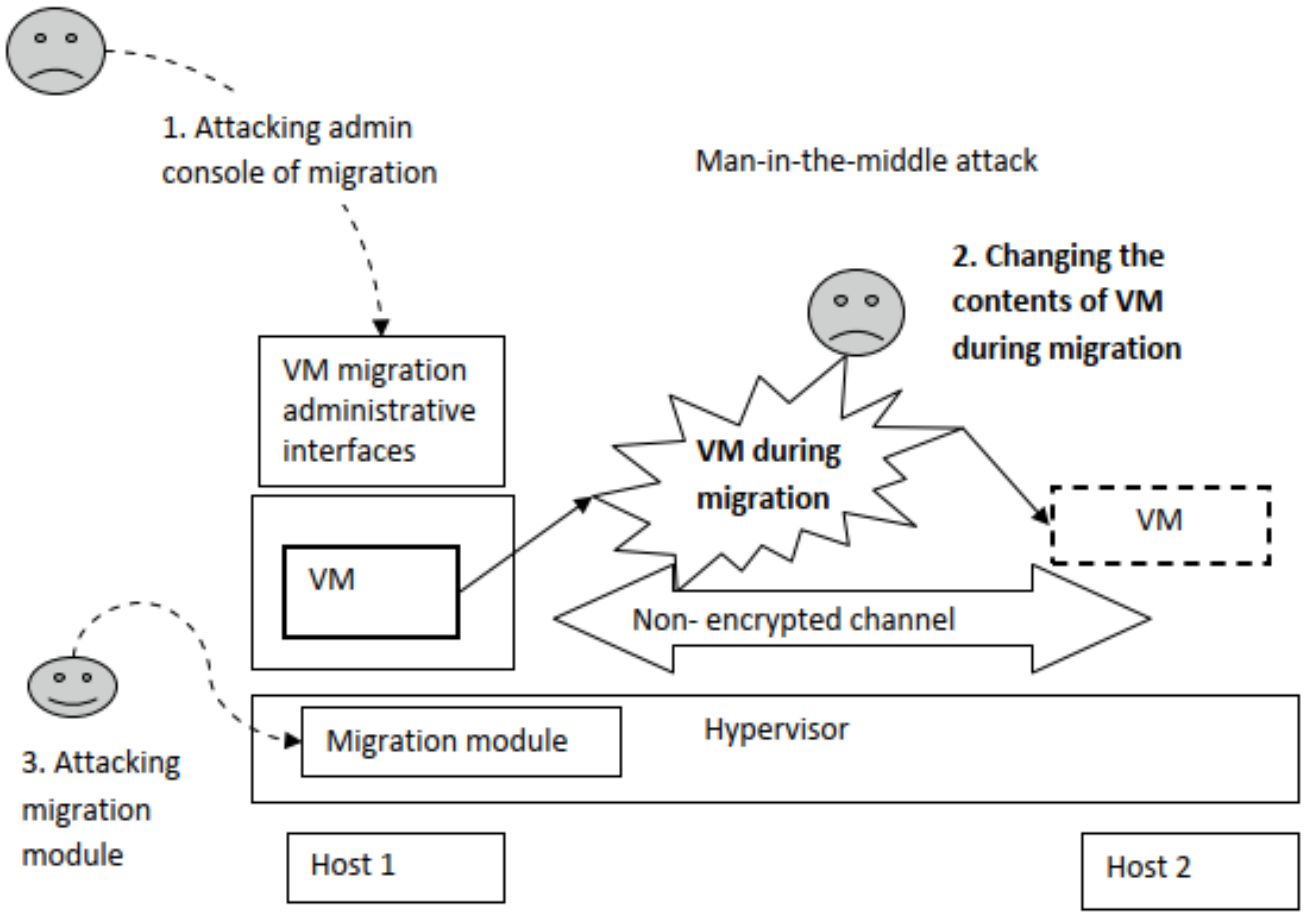
Πηγή: [2]

Απειλές Λόγω Εικονικοποίησης στο Επίπεδο IaaS

- Επίθεση μετανάστευσης εικονικής μηχανής (VM migration attack)
  - Μια εικονική μηχανή είναι απλώς ένα σύνολο από αρχεία αποθηκευμένα σε έναν ξενιστή. Μπορεί να καταναλώσει διάφορα είδη πόρων
  - Η μετανάστευση εικονικών μηχανών αναφέρεται στην διαδικασία μετακίνησης μιας εικονικής μηχανής (δηλ. των αρχείων της) και της κατάστασης των πόρων της από έναν φυσικό ξενιστή σε έναν άλλο
    - Μπορεί να πραγματοποιηθεί για διάφορους λόγους: εξισορρόπηση φορτίου, διαθεσιμότητα, αξιοπιστία, διαχείριση ενέργειας, διατήρηση και ανάνηψη από αποτυχία ξενιστή
    - Η μετανάστευση πραγματοποιείται με την βοήθεια της ενότητας μετανάστευσης (migration module)
    - Μπορεί να πραγματοποιηθεί με 2 τρόπους
      - Ψυχρή μετανάστευση (cold migration)
        - Οι εφαρμογές που εκτελούνται στο φιλοξενούμενο ΛΣ παύονται πριν την μετανάστευση και ανακινούνται μετά από αυτήν
        - Οδηγούν σε υψηλό χρόνο αργίας (downtime)
      - Ζωντανή μετανάστευση (live migration)
        - Η εκτέλεση των εφαρμογών δεν παύεται

Απειλές Λόγω Εικονικοποίησης στο Επίπεδο IaaS

- Επίθεση μετανάστευσης εικονικής μηχανής (VM migration attack) (συνέχεια)
  - Από την μεριά της ασφάλειας, υπάρχουν 3 περιοχές σχετικές με την μετανάστευση εικονικών μηχανών που μπορούν να υποστούν επίθεση
    - Οι διεπαφές κονσόλας διοίκησης, τα περιεχόμενα ή δεδομένα της εικονικής μηχανής & η ενότητα μετανάστευσης


1. Attacking admin console of migration
Man-in-the-middle attack
2. Changing the contents of VM during migration
VM migration administrative interfaces
VM
VM during migration
VM
Non- encrypted channel
3. Attacking migration module
Migration module
Hypervisor
Host 1
Host 2

Πηγή: [2]

Επιθέσεις Μετανάστευσης

- Επίθεση στην διεπαφή κονσόλας διοίκησης (administrative console interface attack)
  - Η μετανάστευση εικονικών μηχανών είναι υπό τον έλεγχο του διαχειριστή (όταν πραγματοποιείται χειρωνακτικά)
    - Αυτός πρέπει να πραγματοποιήσει ορισμένες ενέργειες μέσω της κονσόλας διοίκησης όπως προετοιμασία για την μετανάστευση, εγκαθίδρυση των απαραίτητων πόρων στους ξενιστές πηγής και προορισμού, μεταφορά των καταστάσεων της διαδικασίας και της μνήμης, την δημιουργία νέας εικονικής μηχανής, την ενεργοποίησή της και την διαγραφή της αντίστοιχης εικονικής μηχανής στον πηγαίο ξενιστή
  - Συνεπώς, οποιοδήποτε είδος τρωτότητας στην κονσόλα διοίκησης μπορεί να οδηγήσει σε διάφορες επιθέσεις και αντίστοιχες ανεπιθύμητες ενέργειες:
    - Ανεπιθύμητη μετανάστευση (εκκινούμενη από τον επιτιθέμενο) με πιθανό στόχο που θα μπορούσε να προσδιοριστεί από τον επιτιθέμενο
    - Άρνησης υπηρεσίας (δημιουργία πολλαπλών εικονικών μηχανών και υπερφόρτωση του ΛΣ φιλοξενίας)

Επιθέσεις Μετανάστευσης

- Επίθεση στην κατάσταση εικονικής μηχανής κατά την μετανάστευση
  - Ο επιτιθέμενος μπορεί να διενεργήσει παθητικές και ενεργές επιθέσεις στην κατάσταση όσον αφορά την ΚΜΕ, την κύρια μνήμη και το δίκτυο κατά την μετανάστευση μιας εικονικής μηχανής όταν χρησιμοποιείται ένα μη κρυπτογραφημένο κανάλι
    - Κατά τις παθητικές επιθέσεις μπορεί να αντλήσει πληροφορία, όπως δεδομένα εφαρμογής, μηνύματα, διαπιστευτήρια και tokens ασφάλειας
    - Κατά τις ενεργητικές επιθέσεις, μπορεί να αλλάξει την κατάσταση της εφαρμογής, των διαδικασιών και της κύριας μνήμης

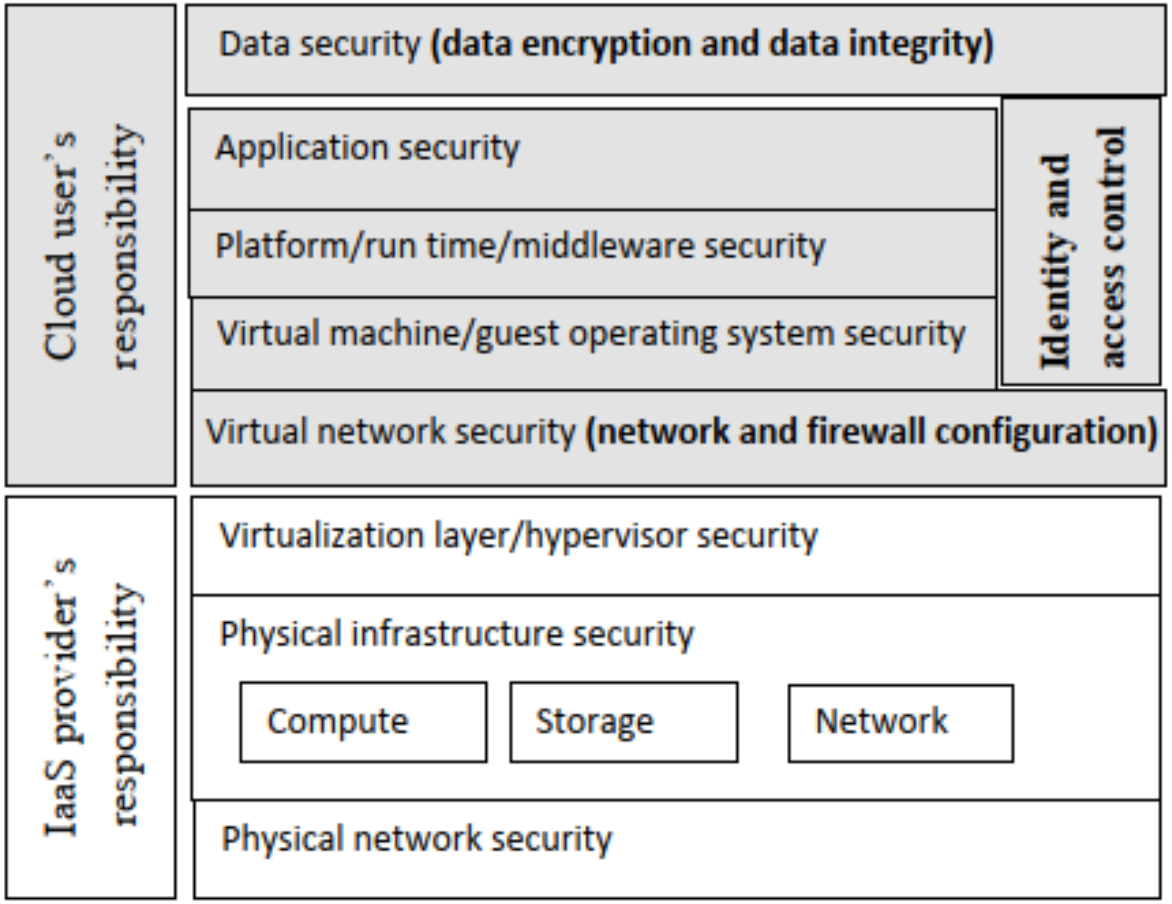
Επιθέσεις Μετανάστευσης

- Επίθεση στην ενότητα μετανάστευσης
  - Ο στόχος είναι η μετέπειτα επίθεση στον hypervisor ώστε να αναληφθεί ο έλεγχός του και άρα και των εικονικών μηχανών που αυτός διαχειρίζεται

Απειλές Λόγω Εικονικοποίησης στο Επίπεδο IaaS

- Επίθεση στην φιλοξενούμενη εικόνα (guest image attack)
  - Η δημιουργία πολλών εικόνων φιλοξενούμενων ΛΣ και η αποθήκευσή τους στον δίσκο όχι μόνο καταναλώνει πόρους αποθήκευσης αλλά δημιουργεί το ρίσκο επίθεσης ως προς την πρόσβαση αυτών των δεδομένων με μη εξουσιοδοτημένο τρόπο
  - Ο επιτιθέμενος μπορεί να αντλήσει πληροφορία για το σημείο ελέγχου εικονικής μηχανής (VM checkpoint), δηλαδή ενός checkpoint για το περιεχόμενο φυσικής μνήμης της εικονικής μηχανής
    - Αυτό μπορεί να οδηγήσει στην έκθεση εμπιστευτικών δεδομένων
    - Οπότε θα πρέπει να περιορίζεται αισθητά η δημιουργία εικόνων φιλοξενούμενων ΛΣ

Συν-ευθυνότητες στο Επίπεδο IaaS



Πηγή: [2]

Μέτρα Πρόληψης Επιθέσεων στην Εικονικοποίηση στο Επίπεδο IaaS

- Οι επιθέσεις στην εικονικοποίηση οφείλονται στην απουσία φυσικής απομόνωσης σε σχέση με την λογική απομόνωση που έχει ήδη επιτευχθεί
- Οπότε θα πρέπει να ληφθούν μέτρα προς αυτή την κατεύθυνση:
  - Η φυσική υποδομή νέφους θα πρέπει να διατηρηθεί ασφαλής από εσωτερικές επιθέσεις
    - Θα πρέπει να εξασφαλιστεί πως δωμάτια εξυπηρετητών, οι εξυπηρετητές, οι συσκευές αποθήκευσης και δικτύωσης και άλλα είδη φυσικών υποδομών είναι ασφαλή
    - Θα πρέπει να ληφθεί υπόψη η συμπεριφορά των εσωτερικών χρηστών λόγω της πιθανής χρήσης κοινωνικής μηχανικής (social engineering) από τους επιτιθέμενους

Μέτρα Πρόληψης Επιθέσεων στην Εικονικοποίηση στο Επίπεδο IaaS

- Οπότε θα πρέπει να ληφθούν μέτρα προς αυτή την κατεύθυνση (συνέχεια):
  - Περιορισμός με αυστηρά δικαιώματα της κονσόλας hypervisor
  - Διατήρηση της ακεραιότητας κώδικα του hypervisor με την βοήθεια εργαλείων όπως το HyperSage
  - Σκλήρυνση του hypervisor
    - Διαδικασία αφαίρεσης μη υποχρεωτικού ή επιθυμητού λογισμικού από τον hypervisor στην συγκεκριμένη περίπτωση

Μέτρα Πρόληψης Επιθέσεων στην Εικονικοποίηση στο Επίπεδο IaaS

- Οπότε θα πρέπει να ληφθούν μέτρα προς αυτή την κατεύθυνση (συνέχεια):
  - Η επικοινωνία μεταξύ του hypervisor και των εικονικών μηχανών θα πρέπει να διαμορφωθεί κατάλληλα
  - Ο hypervisor θα πρέπει να ανανεωθεί με patches ενάντια στις τρέχουσες απειλές και πιθανά σφάλματα (bugs)
  - Εγκατάσταση μηχανισμών τειχών προστασίας (firewalls) και συστημάτων πρόληψης εισβολών (intrusion prevention systems) για την πρόληψη επιθέσεων δικτύου

Μέτρα Πρόληψης Επιθέσεων στην Εικονικοποίηση στο Επίπεδο IaaS

- Οπότε θα πρέπει να ληφθούν μέτρα προς αυτή την κατεύθυνση (συνέχεια):
  - Τα φιλοξενούμενα ΛΣ και οι εικονικές μηχανές θα πρέπει να εξοπλισθούν με εργαλεία ασφάλειας όπως αντι-ιικά καθώς και να σκληρυνθούν
  - Τα αρχεία φιλοξενούμενων ΛΣ πρέπει να σαρωθούν για την ανίχνευση ιών, σκουληκιών, κακόβουλου λογισμικού εν γένει
  - Τα δεδομένα μιας εικονικής μηχανής όταν αυτή μεταναστεύσει σε άλλον ξενιστή θα πρέπει να διαγράφονται. Το ίδιο πρέπει να ισχύει και για τα αντίγραφα ασφαλείας των εικονικών μηχανών
  - Οι μη χρειαζούμενες εικόνες φιλοξενούμενων ΛΣ θα πρέπει επίσης να διαγράφονται

Απειλές Εικονικοποίησης & Άλλα Θέματα Ασφάλειας στο Επίπεδο PaaS

- Οι πάροχοι PaaS υπηρεσιών πρέπει να γνωρίζουν πως υπάρχουν επιπρόσθετοι περιορισμοί και επιπλέον απειλές ασφάλειας λόγω της χρήσης διαφόρων εικονικοποιημένων συστατικών μερών σε περιβάλλοντα PaaS
  - Οπότε θα πρέπει να διατηρηθεί η ακεραιότητα του περιβάλλοντος ανάπτυξης και διάταξης καθώς και των σχετικών εφαρμογών
- Απειλές ασφάλειας στο επίπεδο αυτό
  - Ετερογενής πόροι και κακή διαμόρφωση εφαρμογών
    - Η ετερογένεια των διαφορετικών πόρων υλικού και λογισμικού μπορεί να δημιουργήσει προβλήματα στην διαμόρφωση ρυθμίσεων ασφάλειας λόγω της ετερογένειας αυτών των ρυθμίσεων
    - Αν ο προγραμματιστής εφαρμογής διαμορφώσει λανθασμένα μια εφαρμογή με φτωχές ή λιγότερο ασφαλής ρυθμίσεις, τότε η διαμόρφωση αυτή είναι τρωτή ως προς επιθέσεις ασφάλειας

Απειλές Εικονικοποίησης & Άλλα Θέματα Ασφάλειας στο Επίπεδο PaaS

- Απειλές ασφάλειας στο επίπεδο αυτό (συνέχεια)
  - Μετανάστευση εφαρμογών και έλλειψη προτυποποίησης σε APIs πρόσβασης πόρων
    - Οι εφαρμογές μπορεί να μεταναστεύουν κατά μήκος ΛΣ και ξενιστών για διάφορους λόγους (απόδοση, διαθεσιμότητα, κλιμακωσιμότητα, κλπ.)
    - Επειδή οι πόροι είναι ετερογενής και διαφορετικοί ως προς την φύση τους, η πρόσβαση σε αυτούς δεν είναι ομοιόμορφη
      - Η πρόσβαση πραγματοποιείται μέσω APIs
      - Η ανομοιομορφία των APIs πρόσβασης μπορεί να οδηγήσει σε υποχρησιμοποίηση πόρων ή στο σταμάτημά τους
    - Η έλλειψη προτυποποίησης επίσης οδηγεί σε μη κατάλληλες ρυθμίσεις ασφάλειας στα συστήματα
      - Πχ. η ίδια ρύθμιση μπορεί να κάνει ένα σύστημα πιο ασφαλές και να εισάγει τρωτότητα σε ένα άλλο
      - Επομένως, η μετανάστευση εφαρμογών κατά μήκος διαφορετικών πόρων ανοίγει νέους δρόμους για απειλές ασφάλειας

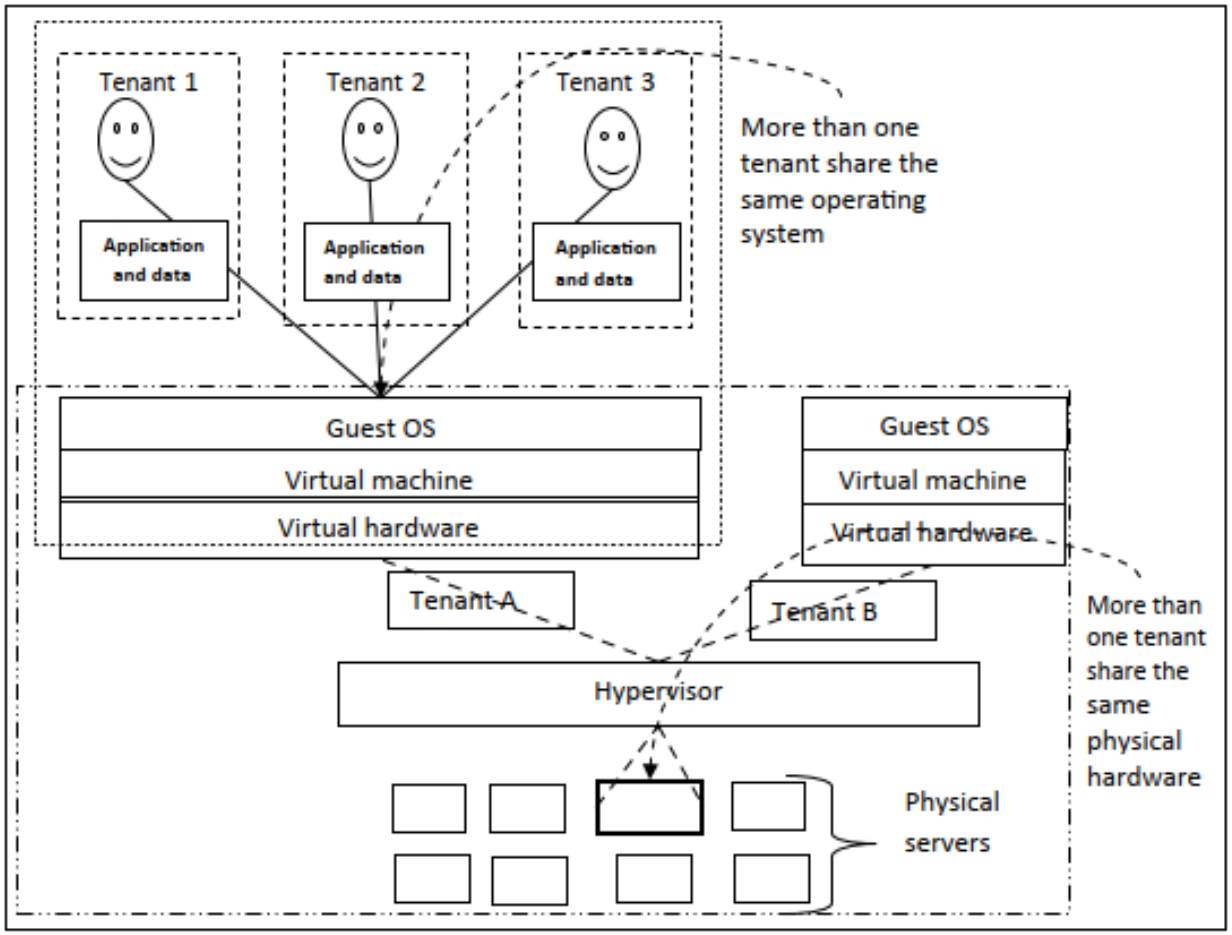
Απειλές Εικονικοποίησης & Άλλα Θέματα Ασφάλειας στο Επίπεδο PaaS

- Απειλές ασφάλειας στο επίπεδο αυτό (συνέχεια)
  - Εικονικοποίηση & πολλαπλή μίσθωση
    - Επειδή μια υπηρεσία PaaS χρησιμοποιεί περισσότερο την εικονικοποίηση, εφαρμόζονται 2 επίπεδα απομόνωσης
      - Απομόνωση στο επίπεδο του hypervisor
      - Απομόνωση στο επίπεδο της εφαρμογής για το διαμοιρασμό του ίδιου φιλοξενούμενου ΛΣ από πολλαπλές εφαρμογές
      - Ουσιαστικά, μια εφαρμογή μπορεί να διαταχθεί κατά μήκος πολλαπλών συστημάτων
      - Σε κάθε περίπτωση, η περαιτέρω εικονικοποίηση μπορεί να οδηγήσει σε περισσότερες τρωτότητες
      - Οπότε, είναι αναγκαία η χρήση επιπρόσθετων μηχανισμών ασφάλειας
  - Τρωτότητες στις εφαρμογές χρηστών
    - Οι τρωτότητες σε εφαρμογές χρηστών όπως κώδικας πίσω πόρτας και κρυφά πεδία φορμών μπορεί να δημιουργήσουν απειλές ασφάλειας από άλλους χρήστες και επιτιθέμενους
    - Θα πρέπει να χρησιμοποιηθεί ασφαλής προγραμματισμός και μηχανισμοί ασφάλειας για την μείωση των απειλών

Απειλές Εικονικοποίησης & Άλλα Θέματα Ασφάλειας στο Επίπεδο PaaS

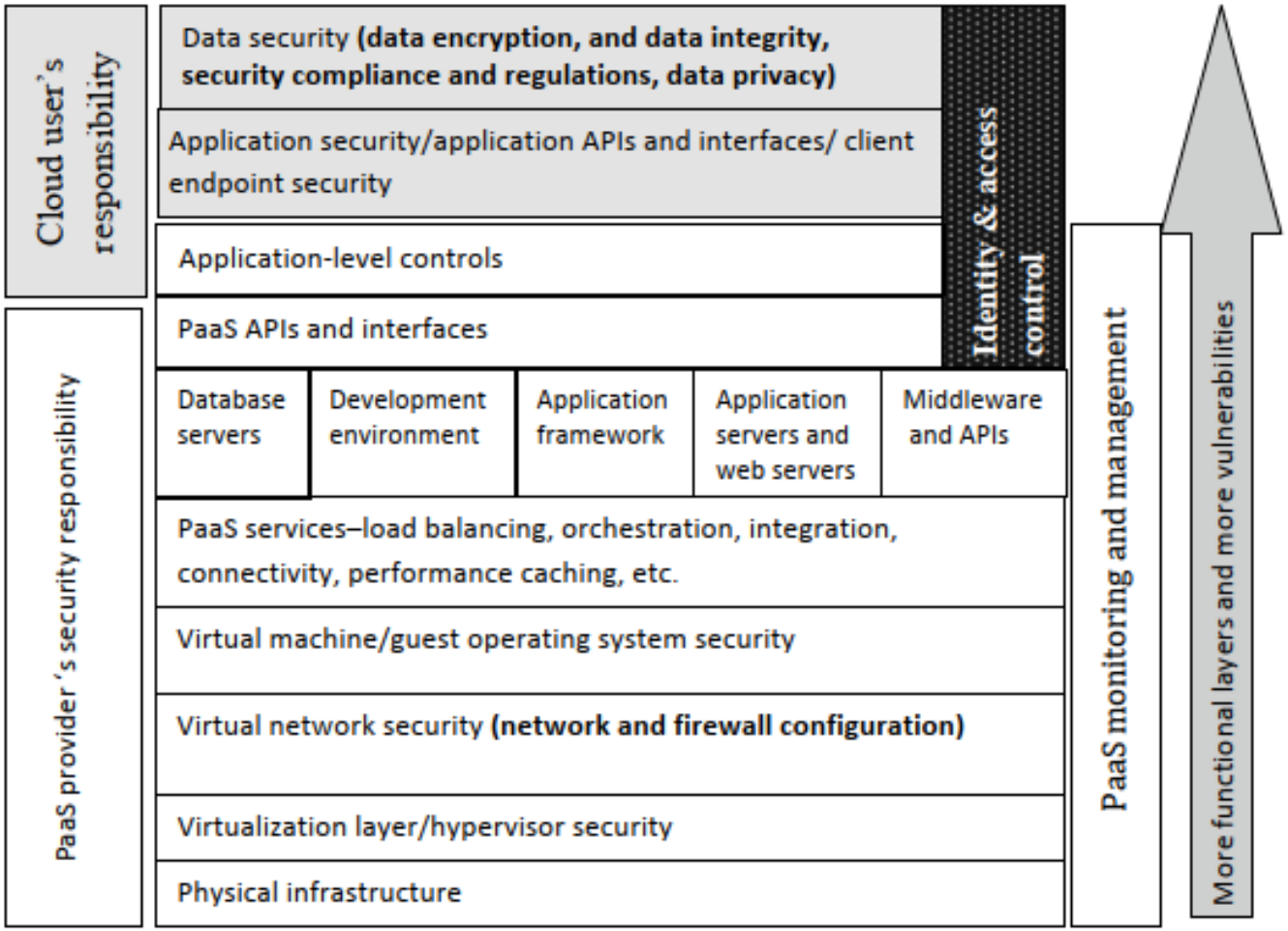
- Απειλές ασφάλειας στο επίπεδο αυτό (συνέχεια)
  - Τρωτότητες στα λειτουργικά επίπεδα του PaaS και διαμοιρασμένες υπευθυνότητες ασφάλειας
    - Ένα PaaS δεν έχει μόνο διαφορετικά λειτουργικά συστήματα αλλά παρέχει και διαφορετικές υπηρεσίες όπως εξισορρόπησης φορτίου, ενορχήστρωσης, ενοποίησης, διασύνδεσης και κρυφής μνήμης
    - Επίσης, μπορεί να έχει ένα κύριο στρώμα διαχείρισης και ένα στρώμα ασφάλειας
      - Το στρώμα διαχείρισης είναι υπεύθυνο για την τροφοδοσία, παρακολούθηση και διαχείριση πόρων
      - Το στρώμα ασφάλειας είναι υπεύθυνο για την διαχείριση απειλών και επιθέσεων ασφάλειας οπότε θα πρέπει να προστατεύσει όλα τα (λειτουργικά) επίπεδα PaaS από επιθέσεις σε φιλοξενούμενα ΛΣ, εικονικοποίηση, άρνησης υπηρεσίας, ενδιάμεσου, API, εργαλείων ανάπτυξης και διάταξης τρίτων μερών, βάσεων δεδομένων, πλαισίων εφαρμογών και μεσισμικού

Απομόνωση στο Επίπεδο Εφαρμογής



Πηγή: [2]

Συν-ευθυνότητες στο Επίπεδο PaaS



Πηγή: [2]

Μέτρα Πρόληψης Επιθέσεων στο Επίπεδο PaaS

- Προσφορά από τους παρόχους PaaS πρότυπων τρόπων πρόσβασης σε πόρους
  - Αυτό μειώνει θέματα διαλειτουργικότητας και ασφάλειας
- Υλοποίηση κρυπτογράφησης, αυστηρής αυθεντικοποίησης, εξουσιοδότησης και ανιχνευσιμότητας (traceability)
- Σκλήρυνση πλατφόρμων, εργαλείων, πλαισίων και APIs

Μέτρα Πρόληψης Επιθέσεων στο Επίπεδο PaaS

- Ανίχνευση και αποθήκευση γεγονότων και δραστηριοτήτων
- Προστασία εικονικών μηχανών και εργαλείων λογισμικού με αντι-ιικά εργαλεία
- Εφαρμογή τελευταίων patches σε όλα τα εργαλεία
- Όλη η ασφάλεια περιμέτρου και τελικών σημείων πρέπει να είναι στενή ώστε η επιφάνεια επιθέσεων στο νέφος να διατηρηθεί ελαχιστοποιημένη

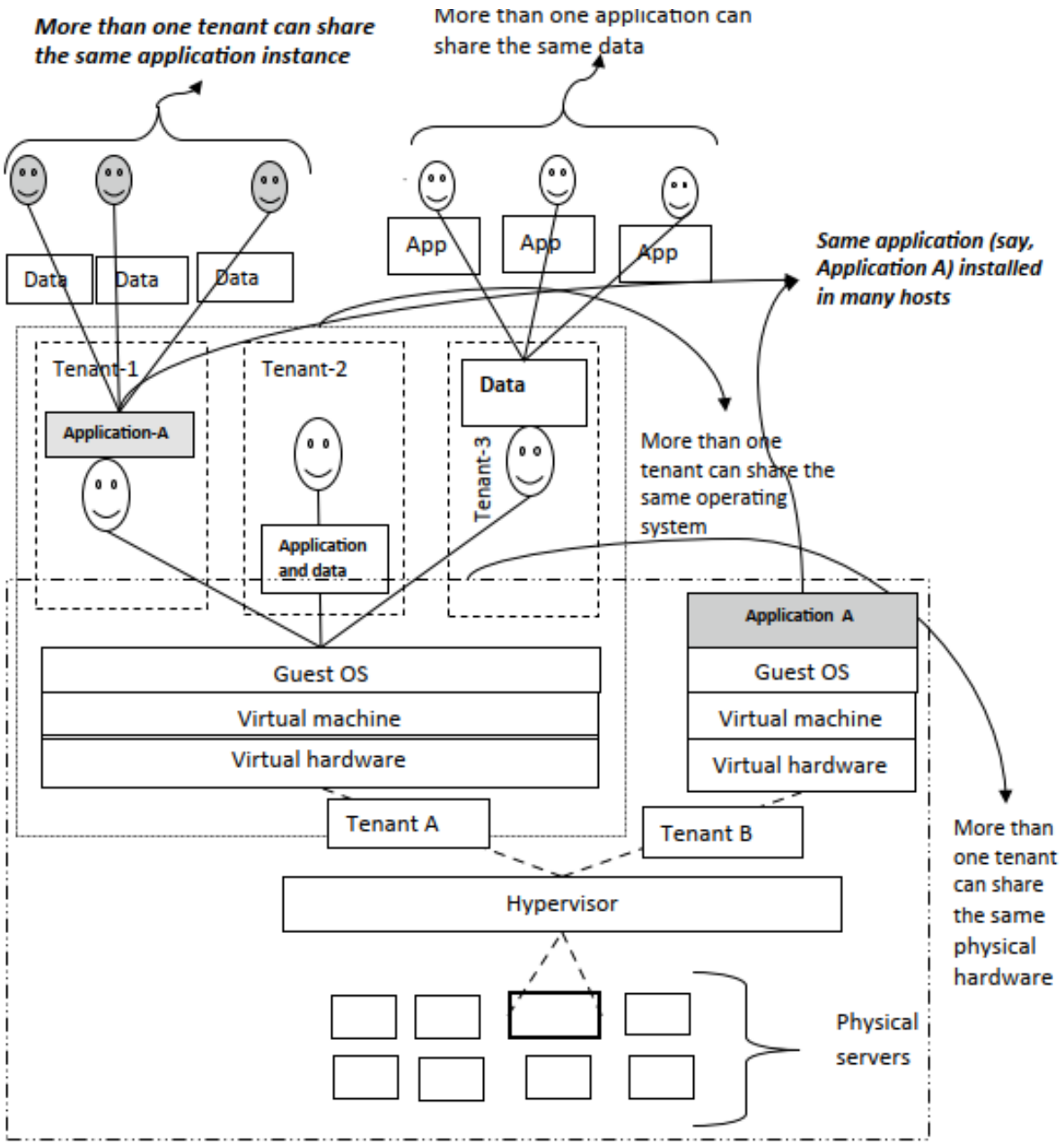
Απειλές Εικονικοποίησης & Άλλα Θέματα Ασφάλειας στο Επίπεδο SaaS

- Οι πάροχοι υπηρεσιών SaaS μπορεί έμμεσα να εφαρμόζουν την εικονικοποίηση σε διαφορετικά επίπεδα
  - Απομόνωση σε επίπεδο hypervisor
  - Απομόνωση σε επίπεδο εφαρμογής όσον αφορά το φιλοξενούμενο ΛΣ
  - Απομόνωση σε επίπεδο εφαρμογής όσον αφορά το σύνολο δεδομένων
  - Απομόνωση σε επίπεδο δεδομένων ώστε το ίδιο στιγμιότυπο εφαρμογής να διαμοιράζεται παραπάνω από ένα σύνολα δεδομένων
  - Διάταξη ενός στιγμιότυπου της εφαρμογής σε πολλαπλά στιγμιότυπα εικονικών μηχανών με βάση απαιτήσεις απόδοσης, κλιμακωσιμότητας & διαθεσιμότητας

Απειλές Εικονικοποίησης & Άλλα Θέματα Ασφάλειας στο Επίπεδο SaaS

- Οι εφαρμογές SaaS προσπελαύνονται μέσω φυλλομετρητών και διεπαφών υπηρεσιών ιστού
  - Οπότε, μπορεί να δεχθούν επιθέσεις που μπορεί να αφορούν τον φυλλομετρητή, την XML και τις υπηρεσίες ιστού

Πηγή: [2]


More than one tenant can share the same application instance
More than one application can share the same data
Data
Data
Data
App
App
App
Same application (say, Application A) installed in many hosts
Tenant-1
Application-A
Tenant-2
Application and data
Tenant-3
Data
More than one tenant can share the same operating system
Application A
Guest OS
Virtual machine
Virtual hardware
Guest OS
Virtual machine
Virtual hardware
Tenant A
Tenant B
Hypervisor
Physical servers
More than one tenant can share the same physical hardware

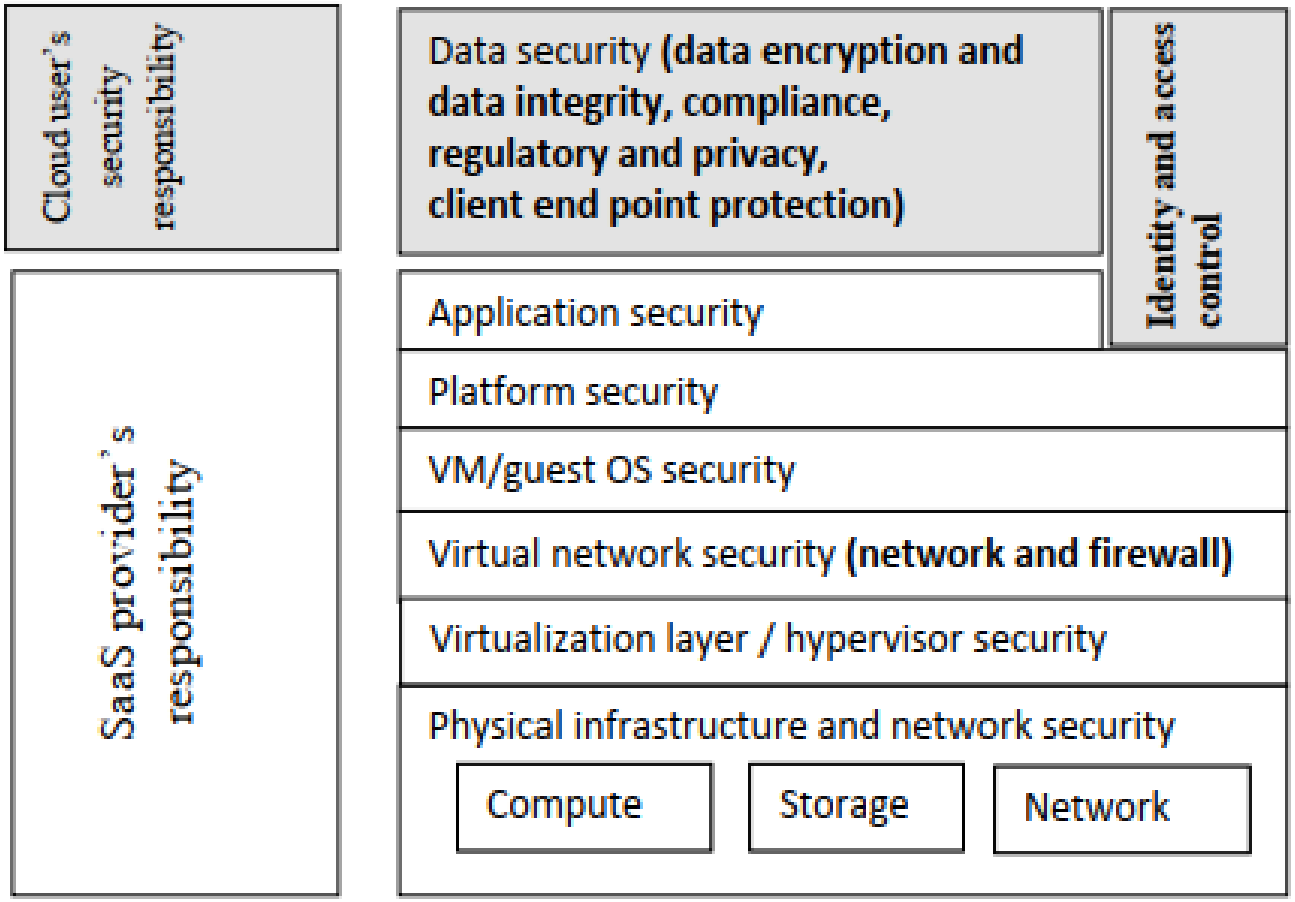
Απειλές Εικονικοποίησης & Άλλα Θέματα Ασφάλειας στο Επίπεδο SaaS

- Απειλές
  - Μη προβλεψιμότητα και σταθερότητα
    - Αν και ένας πάροχος SaaS μπορεί να προσφέρει εφαρμογές υψηλής ποιότητας, δεν είναι σίγουρο ότι δεν θα σταματήσει να λειτουργεί. Οπότε εγείρονται θέμα όπως μετανάστευση (σε άλλο πάροχο παρόμοιας υπηρεσίας SaaS) και απώλεια δεδομένων (που αφορούν έναν χρήστη)
  - Αδιαφάνεια
    - Δεν είναι σίγουρο τι ακριβώς κάνει ένας πάροχος ώστε να διατηρεί τα δεδομένων των πελατών του ασφαλή λόγω έλλειψης διαφάνειας από την μεριά του (όσον αφορά τους μηχανισμούς και πρωτόκολλα ασφάλειας που εφαρμόζει)
  - Αβεβαιότητα στην τοποθεσία δεδομένων
    - Δεν αποκαλύπτεται η τοποθεσία της υποδομής που χρησιμοποιείται για τις προσφερόμενες εφαρμογές (όπου υπάρχει περίπτωση πολλαπλά κέντρα δεδομένων γεωγραφικά κατανεμημένα να γίνονται εκμεταλλεύσιμα)

Απειλές Εικονικοποίησης & Άλλα Θέματα Ασφάλειας στο Επίπεδο SaaS

- Απειλές
  - Έλλειψη απευθείας ελέγχου στα δεδομένα χρηστών
    - Συνήθως, ο έλεγχος που προσφέρεται στους χρήστες για τα δεδομένα τους μπορεί να είναι έμμεσος ή περιορισμένος
    - Επίσης, μερικοί πάροχοι μπορεί να επιβάλλουν στον χρήστη την εφαρμογή κατάλληλης ασφάλειας ως προς τα δεδομένα του (διαμοιρασμένη υπευθυνότητα)
  - Μη συμμόρφωση με μοντέρνα πρότυπα ασφάλειας
    - Μπορεί να μην εφαρμόζονται πρότυπα ασφάλειας ή να είναι απαρχαιωμένα (outdated)
    - Επίσης, μπορεί οι χρήστες να υπογράφουν μακροπρόθεσμες συμφωνίες, το οποίο μπορεί να μεγεθύνει το πρόβλημα (αν τα δεδομένα είναι ασφαλή τώρα μπορεί να μην είναι σε 2-3 χρόνια από τώρα αν ο πάροχος δεν ενημερώνει τα πρότυπα ασφάλειας που εφαρμόζει)

Συν-ευθυνότητες στο Επίπεδο SaaS



Πηγή: [2]

Διαχείριση Ασφάλειας Νέφους

- Περιλαμβάνει περιοχές όπως
  - Διοίκηση νέφους
  - Πολιτικές ασφάλειας
  - Συμβόλαια υπηρεσιών
  - SLAs
  - Διαχείριση ρίσκου

Διοίκηση Νέφους (Cloud Administration)

- Σύνολο από διαδικασίες, πολιτικές, τεχνολογίες και υπηρεσίες που επιδρούν στον τρόπο που οι λύσεις νέφους ενός οργανισμού διοικούνται και ελέγχονται
- Είναι αναγκαία για μια επιχείρηση ώστε να διατηρήσει τον έλεγχο σε αυξανόμενα πολύπλοκα και ενοποιημένα συστήματα, υπηρεσίες και περιβάλλοντα ανθρώπινων πόρων
- Υπάρχουν πολλά μοντέλα διοίκησης νέφους που όλα ακολουθούν την ίδια βασική αρχή
  - Εφαρμογή σωστών πολιτικών και συμμόρφωση ως προς ώριμες διαδικασίες κατά την χρήση τεχνολογιών και υπηρεσιών νέφους

Συστατικά Μέρη Διοίκησης Νέφους

- Εκπαίδευση δύναμης εργασίας (workforce education)
  - Πολλές παραβιάσεις ασφάλειας και επιθέσεις οφείλονται σε αμέλεια όσον αφορά την εσωτερική δύναμη εργασίας ενός οργανισμού
    - Αυτές οι παραβιάσεις οφείλονται σε πράξεις που είτε έπρεπε να είχαν γίνει ή απέτυχαν να εκτελεστούν από την δύναμη εργασίας
    - Οπότε, οι εσωτερικοί χρήστες πρέπει να εκπαιδευτούν ως προς τους κινδύνους συγκεκριμένων ενεργειών και στην σωστή χρήση και εκτέλεση των μέτρων ασφάλειας
- Διαχείριση ταυτότητας και πρόσβασης (identity & access management)
  - Είναι από τους πιο αποτελεσματικούς τρόπους παρακολούθησης των ατόμων που έχουν πρόσβαση σε ευαίσθητα συστήματα και δεδομένα
  - Προλαμβάνει και τουλάχιστον περιορίζει παραβιάσεις και επιθέσεις από εσωτερικούς πόρους
  - Θα πρέπει να συνδυάζεται με μια λύση καταχώρησης δεδομένων που να επιτρέπει στους διαχειριστές να γνωρίζουν ποιος έκανε τι, πότε και που και πως όλες οι αλλαγές καταγράφονται κατάλληλα

Διαχείριση Ταυτότητας & Πρόσβασης (Identity & Access Management - IAM)

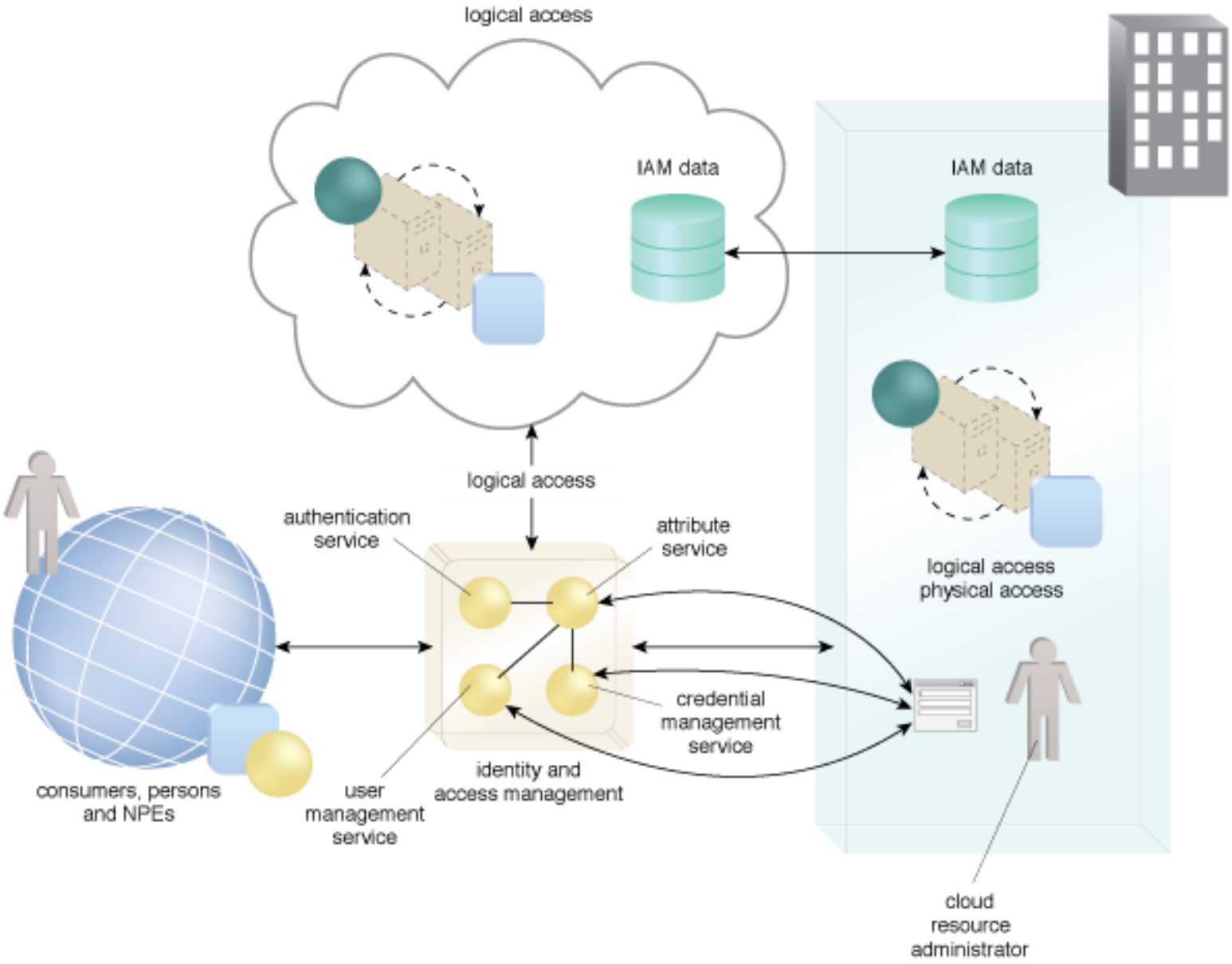
- Περιλαμβάνει συστατικά και πολιτικές που είναι απαραίτητες για τον έλεγχο και την παρακολούθηση των ταυτοτήτων των χρηστών και των προνομίων πρόσβασης τους ως προς πόρους ΤΠ, περιβάλλοντα & συστήματα
- Τα κύρια συστατικά ενός IAM συστήματος είναι:
  - Πιστοποίηση αυθεντικότητας (Authentication)
    - Η συνηθέστερη μορφή διαπιστευτηρίου πιστοποίησης αυθεντικότητας χρηστών εξακολουθεί να είναι το ζεύγος όνομα χρήστη-κωδικός πρόσβασης. Όμως, το IAM μπορεί να υποστηρίζει επίσης τη χρήση ψηφιακών υπογραφών, ψηφιακών πιστοποιητικών, βιομετρικού υλικού (π.χ. δαχτυλικά αποτυπώματα), εξειδικευμένου λογισμικού (π.χ. αναγνώστης φωνής) και κλειδώματος λογαριασμών χρηστών σε καταχωρημένες διευθύνσεις IP ή MAC

Διαχείριση Ταυτότητας & Πρόσβασης

- Τα κύρια συστατικά ενός συστήματος IAM είναι (συνέχεια):
  - Εξουσιοδότηση (Authorization)
    - Ορίζει τις σωστές λεπτομέρειες για έλεγχο πρόσβασης και επιβλέπει τις σχέσεις ανάμεσα σε ταυτότητες, δικαιώματα ελέγχου πρόσβασης και διαθεσιμότητας πόρων
  - Διαχείριση Χρηστών (User Management)
    - είναι υπεύθυνο για την δημιουργία νέων ταυτοτήτων χρηστών και ομάδων πρόσβασης, την επανάθεση κωδικών πρόσβασης, τον ορισμό πολιτικών κωδικού πρόσβασης και διαχείρισης προνομίων
  - Διαχείριση Διαπιστευτηρίων (Credential Management)
    - Περιλαμβάνει διαδικασίες και πρακτικές για την διαχείριση και προστασία των διαπιστευτηρίων (πχ. ασφαλής αποθήκευση, εναλλαγή, τροφοδοσία/ανάκληση, παρακολούθηση)

Διαχείριση Ταυτότητας & Πρόσβασης

- Χρησιμοποιείται κυρίως για την αντιμετώπιση των απειλών ανεπαρκούς εξουσιοδότησης, άρνησης υπηρεσίας & αλληλοκάλυψης ορίων εμπιστοσύνης


logical access
IAM data
IAM data
logical access
logical access
physical access
authentication
service
attribute
service
credential
management
service
identity and
access management
consumers, persons
and NPEs
user
management
service
cloud
resource
administrator

Πηγή: [1]

Μοναδική Διαδικασία Αναγνώρισης (Single Sign-On - SSO)

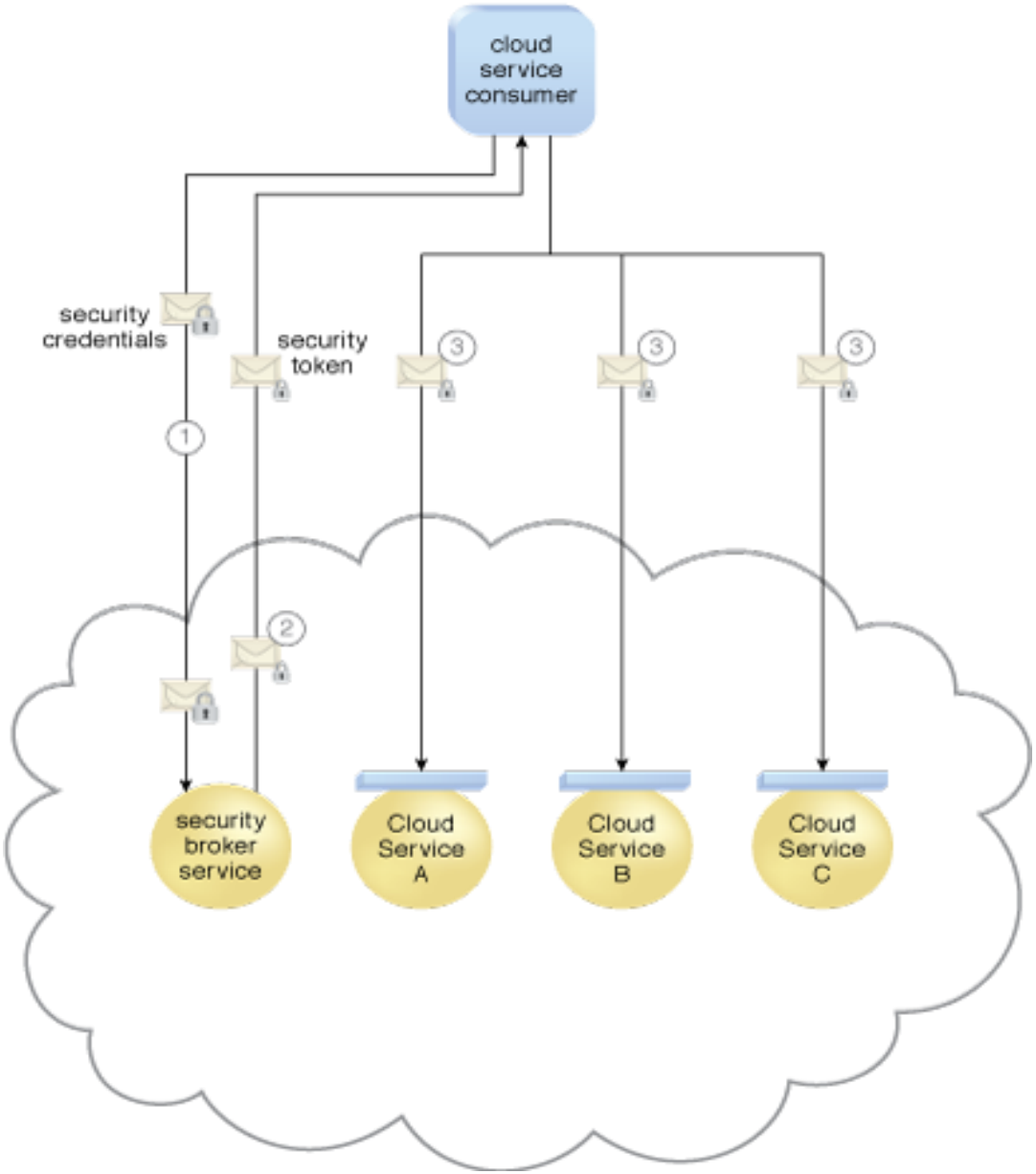
- Αρκετοί καταναλωτές χρησιμοποιούν πολλαπλές υπηρεσίες νέφους που μπορεί να προσφέρονται από διαφορετικούς πάροχους
- Παραδοσιακά, για την ταυτοποίησή τους, απαιτείται η διάδοση των πληροφοριών πιστοποίησης της αυθεντικότητας & εξουσιοδότησης που τους αφορούν ανάμεσα σε όλες αυτές τις υπηρεσίες νέφους
- Το πρόβλημα αυτό λύνεται με τη χρήση ενός μεσίτη ασφάλειας (security broker)

Μοναδική Διαδικασία Αναγνώρισης

- Ο μεσίτης ασφάλειας εγκαθιδρύει ένα περιβάλλον ασφάλειας που παραμένει σε ισχύ καθώς ο καταναλωτής προσπελαύνει άλλες υπηρεσίες νέφους
  - Οπότε, ο καταναλωτής δεν χρειάζεται να πιστοποιεί τον εαυτό του σε κάθε υπηρεσία νέφους

Μοναδική Διαδικασία Αναγνώρισης

- Ο μηχανισμός SSO επιτρέπει ανεξάρτητες υπηρεσίες νέφους και πόρους ΤΠ να παράγουν και να διακινούν διαπιστευτήρια πιστοποίησης αυθεντικότητας & εξουσιοδότησης
  - Τα διαπιστευτήρια αυτά που παρέχονται μόνο αρχικά από τον καταναλωτή παραμένουν έγκυρα καθόλη τη διάρκεια της συνόδου εργασίας καθώς οι πληροφορίες του περιβάλλοντος ασφαλείας διαμοιράζονται
- Ο μηχανισμός SSO δεν αντιμετωπίζει ευθέως καμία από τις απειλές ασφάλειας στο νέφος
  - Απλώς εμπλουτίζει τη δυνατότητα χρήσης περιβαλλόντων ΥΝ για πρόσβαση και διαχείριση κατανεμημένων πόρων ΤΠ και λύσεων
  - Επιπλέον, αναβαθμίζει την εμπειρία του καταναλωτή όσον αφορά την πρόσβαση & χρήση των υπηρεσιών νέφους


cloud service consumer
security credentials
security token
1
2
3
3
3
security broker service
Cloud Service A
Cloud Service B
Cloud Service C

Πηγή: [1]

Συστατικά Μέρη Διοίκησης Νέφους

- Διαχείριση κινδύνων και γεγονότων (risk & event management)
  - Όλες οι επιχειρήσεις αντιμετωπίζουν την αβεβαιότητα καθώς και γεγονότα που δημιουργούνται από ανθρώπους ή με φυσικό τρόπο
  - Αυτές θα πρέπει να ακολουθούν καλά εγκαθιδρυμένες διαδικασίες για τον προσδιορισμό του πως μπορούν να ανιχνεύσουν, διαχειριστούν και να περιορίσουν την αβεβαιότητα και να απαντήσουν τάχιστα σε αναμενόμενα και μη γεγονότα ώστε να ελαχιστοποιήσουν την αρνητική επίδραση στην επιχείρηση
- Έλεγχος συμμόρφωσης (conformance checking)
  - Θα πρέπει να πραγματοποιείται ανεξάρτητα και θα πρέπει να σχεδιάζεται ρωμαλέα ώστε να ανακλά καλές πρακτικές, απαραίτητους πόρους και καλά ελεγμένα πρωτόκολλα και πρότυπα
  - Η χρήση εργαλείων ελέγχου για την αποτίμηση και οπτικοποίηση των τρωτοτήτων του οργανισμού είναι επιβεβλημένη

Διαχείριση Κινδύνου

- Οι καταναλωτές θα πρέπει να εκτελέσουν μια μεθοδική αποτίμηση κινδύνου όταν υιοθετείται το ΥΝ
- Η διαχείριση κινδύνου είναι μια κυκλικά εκτελούμενη διαδικασία
  - Χρησιμοποιείται για να βελτιώσει το επίπεδο ασφάλειας σε έναν οργανισμό
  - Αποτελείται από ένα σύνολο δραστηριοτήτων για την αποτίμηση, έλεγχο και τον χειρισμό των κινδύνων

Διαχείριση Κινδύνου

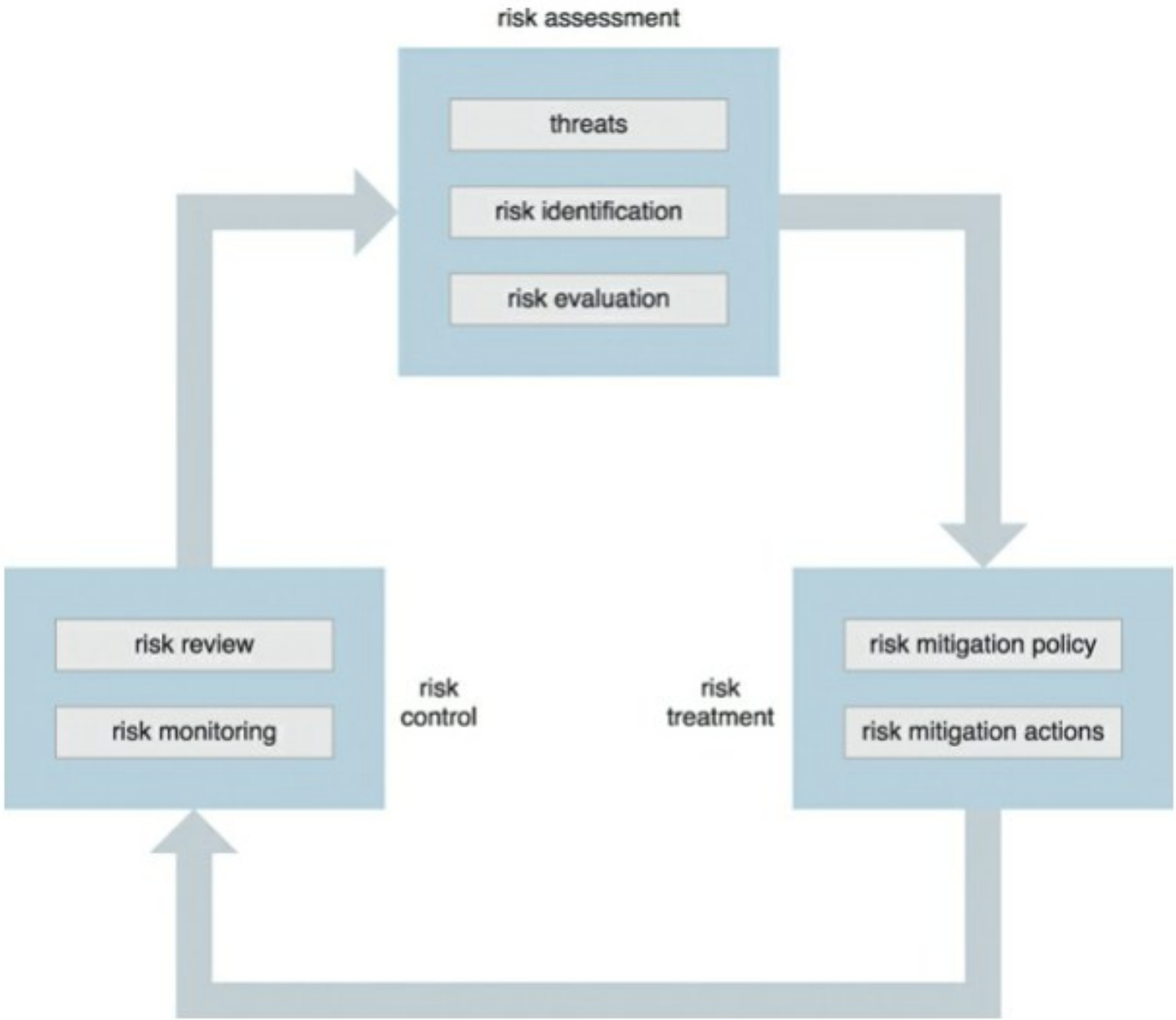
- Αποτίμηση Κινδύνου (risk assessment):
  - Ανάλυση περιβάλλοντος νέφους για την αναγνώριση πιθανών τρωτοτήτων και ατελειών που μπορούν να γίνουν εκμεταλλεύσιμες από απειλές
    - Οπότε, μπορεί να γίνει και αναγνώριση και τεκμηρίωση διάφορων απειλών ασφάλειας νέφους που μπορεί να οφείλονται σε διάφορα είδη πρακτόρων απειλών
  - Απαιτεί τη χρήση στατιστικών παρεχόμενων από τον πάροχο νέφους όσον αφορά προηγούμενες επιθέσεις που πραγματοποιήθηκαν στο νέφος του
  - Οι αναγνωρισμένοι κίνδυνοι ποσοτικοποιούνται και αναλύονται σύμφωνα με την πιθανότητα εμφάνισής τους και το βαθμό επίπτωσής τους καθώς και σε σχέση με το πώς σχεδιάζει ο καταναλωτής νέφους να χρησιμοποιήσει πόρους του ΥΝ

Διαχείριση Κινδύνου

- Χειρισμός Κινδύνου (risk treatment):
  - Σχεδίαση πολιτικών και σχεδίων μετριασμού του κινδύνου (risk mitigation policies & plans)
  - Ανάλογα με τις αντίστοιχες πολιτικές & σχέδια, ορισμένοι κίνδυνοι μπορούν να εξαλειφθούν, άλλοι να μετριαστούν και άλλοι να τύχουν χειρισμού μέσω εξωτερικής ανάθεσης ή και ενσωμάτωσης σε προϋπολογισμούς για ασφάλιστρα και λειτουργικές απώλειες (οπότε ο πάροχος του νέφους αναλαμβάνει την ευθύνη σε αυτή την περίπτωση)

Διαχείριση Κινδύνου

- Έλεγχος Κινδύνου (risk control):
  - Επιτελείται η διαδικασία παρακολούθησης του κινδύνου που αποτελείται από 3 βήματα:
    - Εντοπισμός σχετικών συμβάντων
    - Επισκόπηση των συμβάντων για τον καθορισμό της αποτελεσματικότητας των προηγούμενων αποτιμήσεων και χειρισμών
    - Αναγνώριση πιθανών αναγκών για προσαρμογή της πολιτικής/σχεδίου ασφάλειας
  - Η διαδικασία μπορεί να εκτελεστεί εξολοκλήρου από το πάροχο ή από κοινού με τον καταναλωτή νέφους


risk assessment
threats
risk identification
risk evaluation
risk review
risk monitoring
risk control
risk treatment
risk mitigation policy
risk mitigation actions

Πηγή: [1]

Πολιτικές Ασφάλειας

- Μια πολιτική ασφάλειας (security policy) νέφους είναι ένα έγγραφο που δηλώνει πως μια επιχείρηση σχεδιάζει να προστατεύσει τις λύσεις νέφους και τα περιουσιακά στοιχεία του
- Είναι ένα ζωντανό έγγραφο που συνέχεια ανανεώνεται διότι η τεχνολογία και οι επιχειρησιακές απαιτήσεις αλλάζουν
- Η κατασκευή πολιτικών ασφάλειας νέφους είναι ένα κρίσιμο βήμα πριν την μετανάστευση στο νέφος ώστε να μεγιστοποιηθούν τα οφέλη και να ασφαλιστούν τα δεδομένα (εν γένει τα περουσιακά στοιχεία)

Πολιτικές Ασφάλειας

- Η ανάπτυξη καλής πολιτικής ασφάλειας απαιτεί συλλογισμό ως προς τις σωστές ερωτήσεις και αντίστοιχες απαντήσεις που θα πρέπει να δοθούν για την μετακίνηση των περιουσιακών στοιχείων της επιχείρησης στο νέφος, την επιλογή του κατάλληλου παρόχου και την κατανόηση των οργανωσιακών αναγκών και κουλτούρων
- Οι πιο σημαντικές ερωτήσεις που θα πρέπει να απαντηθούν περιλαμβάνουν:
  - Τις υπάρχουσες πολιτικές που πρέπει να εφαρμοστούν στο νέφος, τις καλές πρακτικές που θα πρέπει να ακολουθηθούν, τι θα πρέπει να μεταφερθεί στο νέφος, την στρατηγική εξόδου, τι θα πρέπει να διαπραγματευθεί και να μπει στις συμφωνίες με τους παρόχους, πως θα εγκαθιδρυθούν και θα αναπτυχθούν οι εφαρμογές στο νέφος, που θα μεταφερθούν ακριβώς οι εφαρμογές και τα δεδομένα

Απαιτήσεις Συμβολαίων & Γλώσσες

- Ένα συμβόλαιο νέφους (cloud contract) είναι ένα τυπικό συμβόλαιο μεταξύ του παρόχου και του πελάτη
- Πριν μπει σε ένα συμβόλαιο, η επιχείρηση θα πρέπει να αποτιμήσει τις δικές τις πρακτικές, ανάγκες και περιορισμούς ώστε να εντοπίσει νομικά εμπόδια και απαιτήσεις συμμόρφωσης που σχετίζονται με μια προτεινόμενη λύση νέφους
- Επιπλέον, θα πρέπει να εξασκήσει την δέουσα επιμέλεια (due diligence) ως προς τον προτεινόμενο πάροχο ώστε να προσδιορίσει πότε η αντίστοιχη προσφορά θα επιτρέψει την επιχείρηση να ικανοποιήσει την συνεχή υποχρέωσή της να προστατεύσει τα περιουσιακά στοιχεία της

Απαιτήσεις Συμβολαίων & Γλώσσες

- Ανάλογα με την φύση των προσφερόμενων υπηρεσιών, το συμβόλαιο μπορεί να πάρει την μορφή μιας συμφωνίας click-wrap που δεν είναι διαπραγματεύσιμη ή τα δύο μέρη μπορεί να διαπραγματευτούν ένα πιο κατάλληλο έγγραφο που να ταιριάζει με την εξειδικευμένη κατάσταση
  - Σε μια συμφωνία click-wrap όλα είναι στατικώς ορισμένα εκ των προτέρων
    - Οπότε, ο πελάτης θα πρέπει να ισορροπήσει τους κινδύνους λόγω της μη εξάσκησης διαπραγμάτευσης ως προς τα πραγματικά οφέλη, την οικονομική μείωση κόστους και την ευκολία χρήσης που υπόσχεται ο πάροχος
  - Σε μια διαπραγμάτευση, θα πρέπει να εξασφαλιστεί πως το συμβόλαιο θα καλύπτει τις ανάγκες και υποχρεώσεις και των 2 μερών κατά την διάρκεια της ισχύς του συμβολαίου και κατά τον τερματισμό του

Απαιτήσεις Συμβολαίων & Γλώσσες

- Η γλώσσα περιγραφής συμβολαίου θα πρέπει να καλύψει τουλάχιστον τις εξής περιοχές:
  - Μοντέλο χρέωσης
  - Δεδομένα (πελάτη)
    - Τρόποι ανάκτησης κατ'απαίτηση
    - Καταστροφή δεδομένων/εγγραφών κατ'απαίτηση
    - Επιστροφή/ανάκτηση δεδομένων κατά τον τερματισμό
    - Υποχρεώσεις πάροχου σε περιστατικά ασφάλειας
  - Έλεγχοι (audits)
    - Τι ακριβώς έλεγχοι και από ποιον μπορούν να πραγματοποιηθούν

Απαιτήσεις Συμβολαίων & Γλώσσες

- Η γλώσσα περιγραφής συμβολαίου θα πρέπει να καλύψει τουλάχιστον τις εξής περιοχές (συνέχεια):
  - SLA (Service-Level Agreement)
  - Επιχειρησιακή συνέχεια / ανάνηψη από καταστροφές (business continuity / disaster recovery)
    - Ελάχιστες απαιτήσεις και ποινές μη συμμόρφωσης
  - Τερματισμός (Termination)
    - Όροι και συνθήκες τερματισμού

SLAs

- Σημαντικός τρόπος εξασφάλισης πως ο πάροχος επιτυγχάνει το επίπεδο υπηρεσίας που απαιτείται από τον πελάτη
- Θα πρέπει να προσδιορίζει
  - Παραμέτρους επιπέδου υπηρεσίας
  - Ελάχιστα επίπεδα (ποιότητας υπηρεσίας)
  - Ποινές για μη συμμόρφωση ως προς τις υποχρεώσεις
- Διαφοροποιούνται ανάλογα με το μοντέλο παράδοσης
- Θα πρέπει να είναι επιβλητά (enforceable)

SLAs

- Πριν την αποτίμηση οποιουδήποτε SLA, οι πελάτες θα πρέπει να αναπτύξουν μια ισχυρή επιχειρησιακή περίπτωση και στρατηγική για τις λύσεις νέφους τους
  - Θα πρέπει να προσδιοριστούν οι υπηρεσίες που θα διαταχθούν στο νέφος καθώς και η σημαντικότητά τους για την επιχείρηση
  - Είναι σημαντικός κι ο έλεγχος στις συνθήκες τερματισμού των συμβολαίων των τρέχοντων υπηρεσιών που φιλοξενούνται
  - Μόνο όταν ολοκληρωθεί η στρατηγική ανάλυση θα μπορεί μια επιχείρηση να αποτιμήσει και να συγκρίνει SLAs από διαφορετικούς πάροχους

SLAs

- Τα ακόλουθα βήματα πρέπει να εκτελεστούν για την αποτίμηση των SLAs ώστε να μπορεί να γίνει η σχετική σύγκριση ή η διαπραγμάτευση των όρων με έναν πάροχο
  - Κατανόηση ρόλων και υπευθυνοτήτων
  - Αποτίμηση των πολιτικών επιπέδου επιχείρησης
  - Κατανόηση διαφορών μοντέλων παράδοσης και ανάπτυξης
  - Προσδιορισμός κριτικών στόχων απόδοσης
  - Αποτίμηση απαιτήσεων ασφάλειας και ιδιωτικότητας
  - Ετοιμασία για την διαχείριση σφαλμάτων υπηρεσιών
  - Κατανόηση του πλάνου ανάνηψης από καταστροφές
  - Ορισμός μιας αποτελεσματικής διαδικασίας διαχείρισης
  - Κατανόηση διαδικασίας τερματισμού/εξόδου

Μηχανισμοί & Τεχνικές Ασφάλειας

- Ασφάλεια δικτύου (network security)
  - Η ασφάλεια δικτύου αντιμετωπίζει κινδύνους που σχετίζονται με την χρήση και πρόσβαση σε επιχειρησιακά δίκτυα (corporate networks)
  - Ενσωματώνει την προστασία δεδομένων καθώς διασχίζουν τα δίκτυα (συμπ. του διαδικτύου), την προστασία συστημάτων και δεδομένων από επιθέσεις βασισμένες στο δίκτυο και την προστασία των συστατικών των δικτύων των ίδιων
  - Εν γένει όλα τα σημεία εισόδου και εξόδου σε ένα περιβάλλον νέφους πρέπει να ελέγχουν την κίνηση και να καταγράφουν τις δραστηριότητες δικτύου σε συγκεκριμένες χρονικές περιόδους

Μηχανισμοί Ασφάλειας Δικτύου

- Ελέγχου πρόσβασης δικτύου (Network access control)
  - Μπορούν να υλοποιηθούν σε φυσικές, συγκλίνουσες και εικονικές συσκευές
- Περιμετρικού τείχους προστασίας (Perimeter firewall control)
  - Πρώτο επίπεδο άμυνας που παρέχει έλεγχο σε πραγματικό χρόνο για τα πρωτόκολλα και την ανίχνευση γνωστών επιθέσεων
- Τειχών προστασίας υπο-επιπέδων (Sub-tier firewall control)
  - Παρέχουν ένα ξεχωριστό όριο ασφάλειας στο στρώμα εικονικοποίησης του νέφους για να προστατεύσουν τις εικονικές μηχανές και επίπεδα δικτύου μέσω του δικτύου του νέφους
- Λίστες ελέγχου πρόσβασης (Access control lists)
  - Παρέχουν ένα στρώμα βασικού ελέγχου ασφάλειας για να υποστηρίξουν την προστασία των εικονικών μηχανών από τυπικές απειλές επιπέδου 2, όπως η σάρωση (scanning) και το πλημμύρισμα (flooding)

Μηχανισμοί Ασφάλειας Δικτύου

- Επιθεώρησης περιεχομένου & ελέγχου (Content inspection & control)
  - Εδώ εντάσσονται διάφορες τεχνολογίες προστασίας του δικτύου, των επιχειρησιακών συστημάτων και δεδομένων τόσο από εξωτερικές επιθέσεις όσο και από εσωτερικές κλοπές δεδομένων
  - Περιλαμβάνουν την ανίχνευση και αποτροπή εισβολών (intrusion detection & prevention), την αποτροπή απώλειας δεδομένων (data loss prevention) και τους εξυπηρετητές πληρεξούσιου (proxy servers)
- Προστασίας από (κατανεμημένη) άρνηση υπηρεσίας (DDoS protection/prevention)
  - Επιθέσεις κατανεμημένης άρνησης υπηρεσίας μπορούν να αντιμετωπισθούν στη ραχοκοκαλιά (backbone) ή σε άλλα δίκτυα ενός παρόχου νέφους που έχουν περισσότερο εύρος ζώνης (bandwidth) σε σχέση με το άθροισμα όλης της κίνησης επιθέσεων
  - Μόλις προσδιοριστεί μια συνθήκη επίθεσης, οντότητες παρακολούθησης εκκινούν την αναδρομολόγηση της ύποπτης κίνησης μέσω ενός συστατικού που επιχειρεί να φιλτράρει την κίνηση επίθεσης ενώ επιτρέπει νόμιμα πακέτα να περάσουν

Μηχανισμοί & Τεχνικές Ασφάλειας

- Ασφάλεια και Ιδιωτικότητα Δεδομένων
  - 3 θέματα θα πρέπει να αντιμετωπισθούν: διαθεσιμότητα, κρυπτογράφηση και προστασία δεδομένων
  - Θα πρέπει να αποτιμηθεί εκ των προτέρων ποια είναι η αξία των δεδομένων και ποιος είναι ο απαιτούμενος βαθμός προστασίας τους
    - Οπότε, θα πρέπει να προσδιοριστεί το επίπεδο ιδιωτικότητας που απαιτείται
    - Υπάρχουν 5 συμβουλές για την ιδιωτικότητα ως προς αυτή την κατεύθυνση
      - Αποφυγή αποθήκευσης ευαίσθητης πληροφορίας στο νέφος εκτός και αν μπορούν να εφαρμοστούν κατάλληλες λύσεις ασφάλειας
      - Επιθεώρηση του συμβολαίου ώστε να αποτιμηθεί ο τρόπος που λειτουργεί η αποθήκευση νέφους ενός παρόχου και τι είδος αποθήκευσης θα πρέπει να επιλεγεί
      - Χρήση αυστηρών κωδικών
      - Χρήση κρυπτογραφημένων υπηρεσιών νέφους
        - Υπάρχουν υπηρεσίες νέφους που προσφέρουν τοπική κρυπτογράφηση και αποκρυπτογράφηση αρχείων επιπρόσθετα της αποθήκευσης και της δημιουργίας αντιγράφων

Μηχανισμοί & Τεχνικές Ασφάλειας

- Ασφάλεια Εφαρμογών
  - Η ασφάλεια εφαρμογών (application security) θα πρέπει να εξασφαλίζεται από τον ιδιοκτήτη/προγραμματιστή τους χωρίς οποιαδήποτε προϋπόθεση για το περιβάλλον νέφους που θα τις φιλοξενήσει
  - Η ανάπτυξη εφαρμογών σε ένα τέτοιο περιβάλλον είναι διαφορετική σε σχέση με ένα παραδοσιακό στις ακόλουθες περιοχές
    - Ο έλεγχος για την φυσική ασφάλεια (physical security) είναι αισθητά μειωμένος σε σενάρια δημόσιου νέφους
    - Πιθανή ασυμβατότητα μεταξύ παρόχων όταν υπηρεσίες μεταναστεύουν από τον έναν πάροχο στον άλλο
    - Θα πρέπει να ληφθεί υπόψη η προστασία δεδομένων δια μέσου του κύκλου ζωής. Αυτό περιλαμβάνει την μεταφορά, επεξεργασία και αποθήκευση των δεδομένων

Μηχανισμοί & Τεχνικές Ασφάλειας

- Ασφάλεια Εφαρμογών
  - Η ανάπτυξη εφαρμογών σε ένα τέτοιο περιβάλλον είναι διαφορετική σε σχέση με ένα παραδοσιακό στις ακόλουθες περιοχές (συνέχεια)
    - Οι συνδυασμοί υπηρεσιών ιστού σε ένα περιβάλλον νέφους μπορεί πιθανώς να δημιουργήσουν τρωτότητες ασφάλειας
    - Η προστασία από σφάλματα για τα δεδομένα και την ασφάλεια τους στο νέφος θα πρέπει να γίνει πιο λεπτομερής και να στρωματοποιηθεί
    - Η εξασφάλιση συμμόρφωσης με σχετικούς βιομηχανικούς και κυβερνητικούς κανονισμούς είναι τυπικά πιο δύσκολη
  - Οπότε, δημιουργείται η ανάγκη για αυστηρές πρακτικές που πρέπει να ακολουθηθούν για την ανάπτυξη ή μετανάστευση εφαρμογών στο νέφος
    - Οι ουσιώδης καλύτερες πρακτικές ασφάλειας περιλαμβάνουν έναν κύκλο ζωής ανάπτυξης ασφαλούς λογισμικού (Secure Software Development Life Cycle - SSDLC), αποτελεσματικά προγράμματα εξασφάλισης ασφάλειας εφαρμογών και αξιόπιστους μηχανισμούς παρακολούθησης εφαρμογών

Κύκλος Ζωής Ανάπτυξης Ασφαλών Εφαρμογών

- Οι οργανισμοί πρέπει να εξασφαλίσουν πως οι καλύτερες πρακτικές για ασφάλεια εφαρμογών, διαχείριση ταυτοτήτων, διαχείριση δεδομένων και ιδιωτικότητα είναι ενσωματωμένες στα προγράμματα ανάπτυξής και κατά μήκος όλου του κύκλου ζωής των εφαρμογών
- Για την υλοποίηση ενός τέτοιου κύκλου ζωής, οι οργανισμοί είτε θα πρέπει να χρησιμοποιήσουν τις δικές τους καλές πρακτικές (διαδικασίες, εργαλεία & τεχνολογίες) ή να υιοθετήσουν μοντέλα ωριμότητας όπως
  - Building Security in Maturity Model
  - Software Assurance Maturity Model
  - Systems Security Engineering Capability Maturity Model

Αρχιτεκτονική Ασφάλειας Εφαρμογών

- Οι παραδοσιακές επιχειρησιακές εφαρμογές μπορούν να προστατευθούν από παραδοσιακούς μηχανισμούς ασφάλειας edge (edge security controls) όπως τείχη προστασίας, ανίχνευση εισβολών και πληρεξούσια
- Σε ένα περιβάλλον νέφους, όμως, όλοι αυτοί οι μηχανισμοί είναι ανεπαρκής διότι οι εφαρμογές εκτελούνται σε μη έμπιστα δίκτυα
  - Οι εφαρμογές μπορεί να βρίσκονται με άλλους μισθωτές του ίδιου παρόχου και μπορεί να προσπελαστούν από οπουδήποτε και μέσω οποιασδήποτε συσκευής

Αρχιτεκτονική Ασφάλειας Εφαρμογών

- Αυτό αλλάζει την ίδια την φύση των απαιτήσεων ασφάλειας για εφαρμογές νέφους
- Η αποτελεσματική ασφάλεια εφαρμογών στο νέφος πρέπει να περιλαμβάνει τα ακόλουθα συστατικά
  - Αυθεντικοποίηση (Authentication)
    - Όσον αφορά την εγκαθίδρυση / επικύρωση των ταυτοτήτων
    - Πραγματοποιείται σε 2 φάσεις
      - Αποσαφήνισης της ταυτότητας & επικύρωσης των διαπιστευτηρίων που έχουν παραδοθεί ήδη από τον χρήστη
    - Αυτό το είδος ταυτοποίησης βασίζεται σε αναγνωριστικά συσκευής, τον πάροχο υπηρεσιών διαδικτύου (ISP), ευρετική (heuristic) πληροφορία κα.
    - Μια εφαρμογή νέφους δεν πρέπει μόνο να αυθεντικοποιεί κατά την αρχική σύνδεση αλλά να επιχειρεί αυθεντικοποίηση βασιζόμενη στους κινδύνους (risk-based authentication) με βάση τις δοσοληψίες που πραγματοποιούνται μέσα στην εφαρμογή

Αρχιτεκτονική Ασφάλειας Εφαρμογών

- Η αποτελεσματική ασφάλεια εφαρμογών στο νέφος πρέπει να περιλαμβάνει τα ακόλουθα συστατικά (συνέχεια)
  - Εξουσιοδότηση (Authorization)
    - Υπάρχουν διάφορα μοντέλα εξουσιοδότησης όπως βασιζόμενα σε ρόλους, σε κανόνες, σε ιδιότητες, & σε ισχυρισμούς (πχ. RBAC, ABAC)
    - Μια επιχείρηση πρέπει να σχεδιάσει τον τρόπο που οι χρήστες θα αυθεντικοποιούνται απρόσκοπτα κατά μήκος όλων των εφαρμογών της και που τα προφίλ χρηστών (όπως συσχετίσεις με ομάδες, δικαιώματα και ρόλους) διαμοιράζονται για εκλεπτυσμένο έλεγχο πρόσβασης
    - Οι επιχειρήσεις θα πρέπει να χρησιμοποιούν ανοικτά πρότυπα, όπως SAML, OAuth ή XACML

Αρχιτεκτονική Ασφάλειας Εφαρμογών

- Η αποτελεσματική ασφάλεια εφαρμογών στο νέφος πρέπει να περιλαμβάνει τα ακόλουθα συστατικά (συνέχεια)
  - Διοίκηση (Management)
    - Θα πρέπει να διοικούνται τόσο οι χρήστες όσο και οι πολιτικές πρόσβασης για τις επιχειρησιακές εφαρμογές
    - Η αποτελεσματική διοίκηση δεν παρέχει μόνο κατάλληλη χρονικά πρόσβαση στους χρήστες αλλά και ανάκλαση της πρόσβασης όταν οι χρήστες φεύγουν από την εφαρμογή καθώς και την κατάλληλη διαχείριση της πρόσβασης όταν οι χρήστες μετακινούνται σε έναν νέο ρόλο
    - Η διοίκηση επίσης διαχειρίζεται τα διαπιστευτήρια εφαρμογών και υπηρεσιών νέφους, τις πολιτικές πρόσβασης για αυτές και τις προνομιούχες ταυτότητές τους

Παρακολούθηση Εφαρμογών Νέφους

- Η παρακολούθηση εφαρμογών βασιζόμενων στο νέφος ποικίλει σε σχέση με τον τύπο του νέφους
- Θα πρέπει να καλύψει τα ακόλουθα
  - Παρακολούθηση καταγραφών (Log monitoring)
    - Η αποθήκευση καταγραφών είναι μόνο το πρώτο βήμα για την συμμόρφωση. Θα πρέπει να υπάρχει κατανόηση για τις διαφορετικές εγγραφές ενώ θα πρέπει να παρακολουθούνται τα περιεχόμενα για την ύπαρξη γεγονότων που απαιτούν αντίδραση
      - Συνεπώς, θα πρέπει να υπάρχει μια διαδικασία που θα ανιχνεύει και θα απαντά στις εγγραφές τέτοιου είδους
  - Παρακολούθηση απόδοσης (Performance monitoring)
    - Μια σημαντική αλλαγή στην απόδοση μιας εφαρμογής μπορεί να είναι σύμπτωμα της χρήσης περαιτέρω πόρων από αυτούς που θα έπρεπε να δικαιούται ένας πελάτης ή κακόβουλης δραστηριότητας ως προς την εφαρμογή που παρακολουθείται είτε για άλλες εφαρμογές στην διαμοιραζόμενη υποδομή

Παρακολούθηση Εφαρμογών Νέφους

- Θα πρέπει να καλύψει τα ακόλουθα (συνέχεια)
  - Παρακολούθηση για κακόβουλη χρήση (Monitoring for malicious use)
    - Θα πρέπει να γίνει κατανοητό τι θα συμβεί αν ένας κακόβουλος χρήστης αποκτήσει πρόσβαση στην εφαρμογή ή χρησιμοποιήσει δικαιώματα που δεν έχει
    - Οι καταχωρήσεις θα πρέπει να καταγράφουν προσπάθειες εισόδου (login)
    - Αν μια εφαρμογή αντιμετωπίσει σημαντική αύξηση στο φόρτο κίνησης, θα πρέπει να επικυρωθεί αν οφείλεται σε έναν συναγερμό που έχει δημιουργηθεί από άλλες εφαρμογές στο περιβάλλον νέφους
  - Παρακολούθηση παραβιάσεων πολιτικής (Monitoring for policy violations)
    - Θα πρέπει να παρακολουθείται και καταγράφεται πως μια απόφαση πολιτικής έχει παρθεί έτσι ώστε να αποφευχθούν τα τυπικά προβλήματα παρακολούθησης λανθασμένων θετικών και η υπερφόρτωση συμβάντων μέσω μιας τέτοιας προσέγγισης παρακολούθησης που οδηγείται από τις πολιτικές

Παρακολούθηση Εφαρμογών Νέφους

- Για μια εφαρμογή βασισμένη σε IaaS υπηρεσίες, η παρακολούθησή της είναι σχεδόν κανονική
  - Ο πελάτης θα πρέπει να παρακολουθεί θέματα με την διαμοιραζόμενη υποδομή ή την απόπειρα μη εξουσιοδοτημένης πρόσβασης από έναν κακόβουλο συνμισθωτή
- Η παρακολούθηση εφαρμογών βασισμένων σε PaaS απαιτεί επιπρόσθετη εργασία
  - Αν δεν προσφέρεται κάποια δυνατότητα παρακολούθησης της εφαρμογής που έχει διαταχθεί από τον PaaS πάροχο, ο πελάτης θα πρέπει είτε να γράψει επιπρόσθετη λογική εφαρμογής για την παρακολούθηση ή να στείλει καταχωρήσεις σε ένα απομακρυσμένο σύστημα παρακολούθησης
- Επειδή οι εφαρμογές SaaS παρέχουν την λιγότερη ευελιξία, η παρακολούθηση της ασφάλειας είναι η περισσότερο δύσκολη

Μηχανισμοί & Τεχνικές Ασφάλειας

- Έλεγχος Ασφάλειας (Security Auditing)
  - Εξασφαλίζει πως οι λύσεις νέφους των οργανισμών λειτουργούν με αναμενόμενο τρόπο
  - Μπορεί να πραγματοποιηθεί είτε εσωτερικά από ομάδες ΤΠΕ ή επιχειρησιακές είτε εξωτερικά από υπηρεσίες τρίτων μερών
  - Το είδος της πληροφορίας που παρέχεται από τον πάροχο είναι ανεξάρτητο από το μοντέλο παράδοσης

Μηχανισμοί & Τεχνικές Ασφάλειας

- Έλεγχος Ασφάλειας (Security Auditing)
  - Η πρόσβαση σε πληροφορίες ελέγχου και διασφάλισης (assurance) είναι ευθύνη κυρίως του παρόχου σε λύσεις SaaS αλλά είναι διαμοιραζόμενη στις περιπτώσεις των άλλων μοντέλων παράδοσης. Εξαρτάται επίσης από την λειτουργικότητα που παρέχει ο πάροχος
    - Σε υπηρεσίες IaaS υπάρχουν περισσότερες ευκαιρίες για εγκαθίδρυση, διαμόρφωση και εγκατάσταση προγραμμάτων στις εικονικές μηχανές, όπως προγράμματα παρακολούθησης
    - Σε υπηρεσίες PaaS οι πελάτες θέτουν απαιτήσεις για τις διευκολύνσεις καταχώρησης (logging facilities) όσον αφορά τα δικά τους προγράμματα
    - Σε υπηρεσίες SaaS οι πελάτες εξαρτώνται από τις καταχωρήσεις και τις λειτουργίες παρακολούθησης των παρόχων

Έλεγχος Ασφάλειας

- Εν γένει, η ακόλουθη πληροφορία πρέπει να παρέχεται από έναν πάροχο για λόγους ελέγχου ασφάλειας
  - Γραπτή τεκμηρίωση για διαδικασίες, πρότυπα και πολιτικές
  - Τυπικές διαμορφώσεις και τεκμηρίωση για την τρέχουσα διαμόρφωση των συστημάτων πελατών
  - Συνεχής πληροφορία καταγραφής και παρακολούθησης
- Ανεξάρτητα από την λύση που ακολουθείται, ο πάροχος θα πρέπει να μπορεί να καταγράφει την φυσική ασφάλεια, τις υποκείμενες πολιτικές, τις διαδικασίες και τις διαμορφώσεις ώστε να ικανοποιεί την αποτίμηση ρίσκου των πελατών του ενώ θα πρέπει να συμμορφώνεται με κανονιστικές απαιτήσεις

Μηχανισμοί & Τεχνικές Ασφάλειας

- Αποτιμήσεις (Assessments)
  - Οι βασιζόμενες στο νέφος αποτιμήσεις ασφάλειας παρέχουν την απαραίτητη πληροφορία για μια έξυπνη και βασισμένη στο ρίσκο διαδικασία λήψης αποφάσεων ενώ ελαφρώνει το προσωπικό ΤΠΕ από το λειτουργικό φόρτο της διαχείρισης της υποδομής εργαλείων αποτίμησης
  - Οι οργανισμοί θα πρέπει να εγκαθιδρύσουν πολιτικές & διαδικασίες καθώς και να υλοποιήσουν μηχανισμούς ελέγχου για να εξασφαλίσουν την εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα της πληροφορίας και της τεχνολογίας πληροφοριών από την οποία οι κριτικές επιχειρησιακές διαδικασίες εξαρτώνται

Αποτιμήσεις

- Περιλαμβάνει κυρίως σάρωση για τρωτότητες και συμμόρφωση
  - Οι αποτιμήσεις τρωτοτήτων δικτύου και συστήματος προσπαθούν να ανιχνεύσουν τρωτότητες με την χρήση τεχνικών σάρωσης IP συνδυαζόμενα με την λεπτομερή κατανόηση των τρωτοτήτων
    - Περιλαμβάνουν τον προσδιορισμό των συστημάτων και των σχετικών τρωτοτήτων τους καθώς και πληροφορία για την πιθανή επίδρασή τους στο δίκτυο ή στην επιχείρηση
  - Η σάρωση συμμόρφωσης επιχειρεί να επικυρώσει την κατάσταση συμμόρφωσης των συσκευών σε λύσεις νέφους
    - Οι αποτιμήσεις συμμόρφωσης για εξυπηρετητές επιτρέπουν την ανακάλυψη των διαμορφώσεών τους καθώς και την σύγκριση των αποτελεσμάτων σε σχέση με καλές πρακτικές της βιομηχανίας και οποιοδήποτε ιδιόκτητο πρότυπο διαμόρφωσης

Αποτιμήσεις

- Οι σημαντικές επιχειρησιακές διαδικασίες και τα περιουσιακά στοιχεία που τις εκτελούν πρέπει να προσδιοριστούν πριν την εκκίνηση των αποτιμήσεων
- Όλα τα μέρη θα πρέπει να συμφωνήσουν και να τεκμηριώσουν κανόνες εμπλοκής που θα χρησιμοποιηθούν κατά την αποτίμηση όπως εξαιρέσεις περιουσιακών στοιχείων, χρονικά παράθυρα, επίπεδα επιθέσεων, τεχνικές κοινωνικής μηχανικής κα.
- Οι αποτιμήσεις είναι ασφαλής προς εκτέλεση ακόμη και σε παραγωγικά συστήματα αλλά ο πάροχος θα πρέπει να κατέχει μηχανισμούς για να σταματήσει μια αποτίμηση οποτεδήποτε αν κάτι συμβεί που είναι καταστροφικό (πχ. ως προς έναν εξυπηρετητή) ή αποδιοργωνατικό για τις σημαντικές επιχειρησιακές διαδικασίες

Αποτιμήσεις

- Είναι σημαντική η κατανόηση των εργαλείων αποτίμησης που θα χρησιμοποιηθούν
  - Οι ομάδες αποτίμησης θα πρέπει να συνεργαστούν με τον πάροχο ώστε να επιτελέσουν δοκιμές με βάση καλές πρακτικές
  - Αν ο πάροχος δεν προσφέρει μια τέτοια υπηρεσία, θα πρέπει να κατανοηθούν οι περιορισμοί επιτέλεσης τέτοιων δράσεων σε φιλοξενούμενα περιβάλλοντα νέφους
  - Η εμβέλεια και οι περιορισμοί μπορεί να ποικίλουν με βάση σε ποιο μοντέλο παράδοσης μια εφαρμογή νέφους ταιριάζει
- Τα δεδομένα που παράγονται από υπηρεσίες αποτίμησης είναι ευαίσθητα ως προς την φύση και πρέπει να προστατεύονται κατάλληλα
  - Οι υπηρεσίες θα πρέπει να εξασφαλίζουν την εμπιστευτικότητα των δεδομένων και να επιβεβαιώνουν πως μόνο εξουσιοδοτημένα μέρη μπορούν να τα προσπελάσουν
  - Τόσο ο πάροχος όσο και ο πελάτης θα πρέπει να υπογράψουν κατάλληλη συμφωνία μη έκθεσης (nondisclosure agreement – NDA)
    - Αυτή θα πρέπει να περιορίζει την έκθεση της πληροφορίας που λαμβάνεται είτε κατά την προετοιμασία της αποτίμησης ή που είναι απόρροια της εκτέλεσής της μόνο σε αυτούς που έχουν τις κατάλληλες αρμοδιότητες (και για την εκμετάλλευσή της)
    - Τα δεδομένα θα πρέπει να προστατεύονται σε όλες τις φάσεις (δημιουργία, αποθήκευση, μεταφορά, επεξεργασία και διαγραφή)

Δοκιμή Διείσδυσης (Penetration Testing)

- Είναι μια μεθοδολογία δοκιμής ασφάλειας που επιτρέπει την αποτίμηση του σθένους της ασφάλειας συστήματος προσομοιώνοντας μια επίθεση από μια κακόβουλη πηγή
- Η διαδικασία δοκιμής περιλαμβάνει την ενεργή ανάλυση του συστήματος νέφους για οποιαδήποτε πιθανή τρωτότητα που μπορεί να προέρχεται από φτωχή ή ακατάλληλη διαμόρφωση συστήματος, γνωστά σφάλματα λογισμικού ή υλικού ή λειτουργικές αδυναμίες σε διαδικασίες ή τεχνικά αντίμετρα
  - Η ανάλυση επιτελείται από την θέση ενός δυνητικού επιτιθέμενου και μπορεί να περιλαμβάνει την ενεργή εκμετάλλευση τρωτοτήτων ασφάλειας

Δοκιμή Διείσδυσης (Penetration Testing)

- Εν γένει, η δοκιμή διείσδυσης περιλαμβάνει 3 κύριες φάσεις: ετοιμασία, εκτέλεση και παραγωγή αναφορών
- Το μοντέλο παράδοσης έχει σημαντική επίδραση στην δοκιμή διείσδυσης και στην απόφαση αν μια τέτοια δοκιμή είναι δυνατή
  - Εν γένει, οι υπηρεσίες IaaS & PaaS πιθανώς να επιτρέπουν την δοκιμή διείσδυσης
  - Όμως, οι πάροχοι SaaS πιθανώς δεν επιτρέπουν μια τέτοια δοκιμή από τους πελάτες τους όσον αφορά τις εφαρμογές και υποδομή τους. Εξαιρούνται τα τρίτα μέρη που εκτελούν δοκιμές διείσδυσης εκ μέρους του παρόχου SaaS για συμμόρφωση ή ακολούθηση καλών πρακτικών

Δοκιμή Διείσδυσης

- Κατά την διενέργεια αποτιμήσεων δοκιμών διεισδύσεων για ένα περιβάλλον νέφους, θα πρέπει να δοθεί δέουσα προσοχή στο χαρακτηριστικό της πολλαπλής μίσθωσης και την πιθανή αναστάτωση/διατάραξη άλλων συστημάτων του οργανισμού
- Οι οργανισμοί μπορεί να μην μπορούν να επιτελέσουν μια εσωτερική δοκιμή διείσδυσης από άκρο σε άκρο για ένα πάροχο και μπορεί να πρέπει να βασιστούν σε μια επιβεβαίωση πως μια τέτοια δοκιμή έχει εκτελεστεί (επιτυχώς)
- Θα πρέπει να κατανοήσουν ποιο είδος δοκιμής επιτρέπεται να επιτελέσουν πριν επιλέξουν τις πρωτοβουλίες ασφάλειας ενός παρόχου

Μηχανισμοί & Τεχνικές Ασφάλειας

- Ανίχνευση Εισβολών Νέφους & Απάντηση σε Συμβάντα (Cloud Intrusion Detection & Incident Response)
  - Ο σκοπός της ανίχνευσης εισβολών είναι η παρακολούθηση του επιχειρησιακού περιβάλλοντος σε σημεία κλειδιά για την αποκάλυψη κακόβουλης δραστηριότητας που στοχεύει σε υποβάθμιση, αποδιοργάνωση, μόλυνση ή την αποβολή δεδομένων, εφαρμογών και των συστημάτων που τα φιλοξενούν
  - Ο σκοπός της απάντησης σε συμβάντα είναι να λάβει δράσεις για την αποφυγή των σημαντικών επιδράσεων, το μπλοκάρισμα της μόλυνσης και την συνέχιση της επιχειρησιακής λειτουργίας κατά την διάρκεια μιας ανιχνευμένης επίθεσης
  - Μια εξεζητημένη υπηρεσία ανίχνευσης εισβολών συνδυάζει την ανίχνευση και την απάντηση, την δομή διαχείρισης για έλεγχο και αναφορές, και διεπαφές με την υπόλοιπη αρχιτεκτονική ασφάλειας ώστε να υπάρξει μια πιο ολιστική όψη και καλύτερη αποκάλυψη της κακόβουλης ή ανώμαλης δραστηριότητας

Τεχνικές και Στρατηγικές Ανίχνευσης Εισβολών

- Οι μηχανισμοί ανίχνευσης εισβολών εφαρμόζονται σε ευκαιριακές διασυνδέσεις (opportunistic interconnections) ή διαμοιραζόμενα σημεία (shared points), όπου προστατευόμενη και ξένη κίνηση διασχίζει σχετικά μονοπάτια
  - όρια διοίκησης δικτύου (network management boundaries), διεπαφές δικτύου τελικών συστημάτων (end system network interfaces), ξενιστές μέσα σε εικονικοποιημένα container όρια ή άμεσα μέσα σε φιλοξενούμενα περιβάλλοντα

Τεχνικές και Στρατηγικές Ανίχνευσης Εισβολών

- Υπάρχουν 2 είδη τεχνικών ανίχνευσης εισβολών
  - Βασισμένη στο δίκτυο
    - Αναζητά δυαδικά μοτίβα ή μοτίβα συμπεριφοράς και ανώμαλη δραστηριότητα στην κίνηση δικτύου
    - Οι σχετικές τεχνικές εφαρμόζουν στρατηγικές για ανίχνευση με βάση υπογραφές, ευριστική συμπεριφορά (behaviour heuristics), και συσχετίσεις μοτίβων κίνησης (traffic pattern correlations)
      - Εν γένει βασίζονται σε κάποια μορφή βαθιάς μελέτης πακέτων (deep packet inspection) που αφορά την ικανότητα της συσκευής ή του λογισμικού ανίχνευσης να κατανοεί τις διάφορες κεφαλίδες και συστατικά των πακέτων
    - Τα συστήματα ανίχνευσης τοποθετούνται σε σημεία εισόδου και εξόδου στο δίκτυο για να επεξεργάζονται όλη την δυνατή κίνηση
      - Μπορούν να διαταχθούν με τη χρήση υπάρχοντος εξοπλισμού δικτύου, εξειδικευμένων συσκευών και διεπαφών ή λογισμικού που εκτελείται σε ένα ξενιστή

Τεχνικές και Στρατηγικές Ανίχνευσης Εισβολών

- Υπάρχουν 2 είδη τεχνικών ανίχνευσης εισβολών (συνέχεια)
  - Βασισμένη σε γεγονότα
    - Αναζήτηση για δραστηριότητες ή γεγονότα σε συστατικά στα στρώματα συστήματος/υποδομής, εικονικοποίησης και εφαρμογών
    - Οι τεχνικές που βασίζονται σε γεγονότα χρησιμοποιούν την πρόσβαση ή αναφορές σε γεγονότα και διαμορφώσεις για να προσδιορίσουν πιθανή δραστηριότητα που οδηγεί ή είναι αποτέλεσμα μιας κακόβουλης επίθεσης, υποβάθμισης, αποβολής κλπ.
    - Τα γεγονότα ανιχνεύονται μέσω της ανάλυσης των κεντρικά αναφερόμενων καταχωρήσεων ή από λογισμικό που εκτελείται απευθείας στο σύστημα στο στρώμα εικονικοποίησης για συγκεκριμένες συμπεριφορές που υποδηλώνουν πιθανή εισβολή:
      - Παραβιάσεις σε πολιτικές
      - Αλλαγές στην διαμόρφωση
      - Αλλαγές στο φόρτο εργασίας
      - Ξένες διαδικασίες και κλήσεις συστήματος
      - Αλλαγές στην ακεραιότητα του ΛΣ και του συστήματος αρχείων

Τεχνικές και Στρατηγικές Ανίχνευσης Εισβολών

- Η ανίχνευση εισβολών σε ένα περιβάλλον νέφους μπορεί να είναι περισσότερο επίπονη ανάλογα με τους διαθέσιμους πόρους στο νέφος και το επίπεδο διαχείρισης ή ελέγχου των συσκευών, υπηρεσιών ή διαμορφώσεων που απαιτούνται
- Τα SLAs μπορούν να ορίσουν τις περιοχές που θα πρέπει να παρακολουθηθούν & να προσδιορίσουν τα επίπεδα υπηρεσίας και ποιότητας καθώς και τον τρόπο προσθήκης και διαχείρισης κανόνων
  - Η ασφαλής διαχείριση, θέση μεταφοράς, κατάτμηση και ανάλυση της συλλεγμένης πληροφορίας πρέπει να οριστεί σε οποιοδήποτε είδος συμβολαίου με τον πάροχο
- Οποιαδήποτε συσκευή ανίχνευσης τρωτοτήτων θα πρέπει να είναι ικανή να διαχειρίζεται την κίνηση που αναμένεται να την διαπεράσει ώστε να είναι αποτελεσματική

Ανίχνευση Εισβολών

- Τα συστήματα ανίχνευσης εισβολών (intrusion detection systems – IDSs) είναι ένα ουσιώδες συστατικό των μέτρων άμυνας για την προστασία υπολογιστικών συστημάτων και δικτύων από κακό και κατάχρηση
  - Συνεπώς, είναι κρίσιμη η εφαρμογή τους σε περιβάλλοντα νέφους
  - Σε ένα περιβάλλον νέφους, η ανίχνευση που βασίζεται σε γεγονότα απαιτεί ορατότητα σε περισσότερα στρώματα στο σύστημα
    - Εφόσον μιλάμε για ένα περιβάλλον πολλαπλής μίσθωσης, εισάγονται επιπρόσθετες πολυπλοκότητες, όπως APIs, αλληλεπιδράσεις φιλοξενούμενων διαδικασιών και το επίπεδο διαχείρισης
    - Οπότε, ορισμένα γεγονότα ή έλεγχοι μπορεί να περιλαμβάνουν
      - Γεγονότα στρώματος εικονικοποίησης
      - Παρακολούθησης αποθετηρίου εικόνων εικονικών μηχανών
      - Παρακολούθησης ακεραιότητας
      - Αλληλεπίδρασης μεταξύ ανεξάρτητων φόρτων εργασίας (workloads) κα.

Ανίχνευση Εισβολών

- Για την διαχείριση της προστασίας ξενιστών, εφαρμογών και δεδομένων, μια υπηρεσία ανίχνευσης πρέπει να ελέγχει ή να έχει ορατότητα σε σημεία ενδιαφέροντος, να έχει δυνατότητες συσχέτισης πληροφοριών και γεγονότων και να παρέχει την υποδομή επικοινωνίας μέσα και μεταξύ συστατικών των υπηρεσιών εντός της επιχείρησης καθώς και πίσω στο περιβάλλον
  - Για την παροχή αυτής της ικανότητας από το νέφος απαιτούνται διοικητικές σχέσεις, ενισχυμένα δικαιώματα χρηστών και πρόσβαση σε δοσοληψίες από άκρο σε άκρο μεταξύ φιλοξενούμενων στοιχείων και του κεντρικού ελέγχου

Απάντηση σε Συμβάντα

- Η φύση της απάντησης επηρεάζεται από την μετακίνηση των υπηρεσιών στο νέφος
  - Ο πελάτης θα πρέπει να κατανοήσει τι πρέπει να κάνει ώστε να επιτρέψει την αποτελεσματική και αποδοτική διαχείριση των συμβάντων ασφαλείας στο νέφος
  - Με βάση τη πιθανότητα ότι η πληροφορία καταχώρησης μπορεί να μην είναι άμεσα διαθέσιμη στον πελάτη, η απάντηση σε συμβάντα θα πρέπει να λάβει υπόψη το είδος της υπηρεσίας προς χρήση και να δημιουργήσει ένα SLA ασφάλειας ώστε να προσδιορίσει επακριβώς τις υπευθυνότητες του παρόχου
  - Αν χρησιμοποιείται IaaS, ο πάροχος είναι υπεύθυνος για τις καταχωρήσεις που αφορούν την υποδομή. Οπότε, οι πελάτες θα έχουν πρόσβαση στις καταχωρήσεις των εικονικών μηχανών τους και των IDS κατά τη διάρκεια ενός συμβάντος

Απάντηση σε Συμβάντα

- Η φύση της απάντησης επηρεάζεται από την μετακίνηση των υπηρεσιών στο νέφος (συνέχεια)
  - Αν χρησιμοποιείται PaaS, η ομάδα απάντησης συμβάντων θα έχει πρόσβαση σε καταχωρήσεις εφαρμογής αλλά ο πάροχος θα διατηρεί ακόμη τις καταχωρήσεις εξυπηρετητών
    - Ο πελάτης έχει περισσότερες ευκαιρίες για την άντληση πληροφορίας καταχώρησης από ένα πάροχο PaaS επικοινωνώντας σε αυτόν τι εκκινεί ένα γεγονός (πχ. αποτυχημένες απόπειρες ταυτοποίησης)
  - Αν χρησιμοποιείται SaaS, η ομάδα απάντησης του παρόχου θα απαντά εσωτερικά σε γεγονότα μέσω της ικανότητας διαχείρισης γεγονότων και συμβάντων, εργαλείων ανίχνευσης εισβολών και άλλων εργαλείων διαχείρισης καταχωρήσεων
    - Οπότε, ο πελάτης δεν έχει καμία ευθύνη
  - Εν γένει, η χρήση υπηρεσιών PaaS & SaaS διευκολύνουν την απάντηση διότι το βάρος παραμένει στον πάροχο
    - Επίσης, συμβάντα που απαιτούν την ανάκτηση μια εικόνας ή στιγμιοτύπου εικονικής μηχανής για λόγους εγκληματολογικούς (forensics) διευκολύνονται ως προς την απάντησή τους διότι το εικονικοποιημένο περιβάλλον έχει σχεδιαστεί για την αντιγραφή ή κλωνοποίηση εικόνων

Μηχανισμοί & Τεχνικές Ασφάλειας

- Επιχειρησιακή Συνέχεια & Σχεδιασμός Ανάνηψης από Καταστροφές (Cloud Business Continuity & Disaster Recovery Planning)
  - Οι περισσότερες προσπάθειες είναι παρόμοιες με αυτές για παραδοσιακά περιβάλλοντα σε σχέση με τι απαιτείται και ποια θα πρέπει να είναι η σχετική προετοιμασία για έναν οργανισμό
  - Τα σημαντικά οφέλη χρήσης μια αξιόπιστης και υψηλά διαθέσιμης υπηρεσίας BC/DR (Business Continuity/Disaster Recovery) περιλαμβάνουν
    - Ασφαλή δημιουργία αντιγράφων
      - Ο πάροχος θα φιλοξενήσει όλα τα αναπαραγωγημένα συστήματα στο νέφος ώστε να είναι διαθέσιμα για λόγους ανάνηψης από καταστροφές
    - Κλιμακώσιμη υποδομή
      - Κύριο χαρακτηριστικό ενός νέφους που εξασφαλίζει πως τα συστήματα BC/DR θα κλιμακωθούν κατ'απαίτηση

Μηχανισμοί & Τεχνικές Ασφάλειας

- Επιχειρησιακή Συνέχεια & Σχεδιασμός Ανάνηψης από Καταστροφές (Cloud Business Continuity & Disaster Recovery Planning)
  - Τα σημαντικά οφέλη χρήσης μια αξιόπιστης και υψηλά διαθέσιμης υπηρεσίας BC/DR (Business Continuity/Disaster Recovery) περιλαμβάνουν (σύνέχεια)
    - Χρέωση ανάλογα με την χρήση
      - Οι πελάτες πληρώνουν μόνο για την πραγματική χρήση της υπηρεσίας. Αυτό μεταφράζεται σε χαμηλότερα κόστη υπηρεσίας κατά την κανονική λειτουργία, όταν η ελάχιστη χωρητικότητα και απόδοση απαιτούνται για την αποθήκευση και αναπαραγωγή των συστημάτων και δεδομένων από την λύση BC/DR
      - Όταν γεγονότα απαιτούν μια απάντηση BC/DR, απαιτούμενες υπηρεσίες υποστήριξης εκτελούνται για να ικανοποιήσουν την σχετική ανάγκη
    - Μειωμένη εξειδίκευση σε BC/DR
      - Τόσο για εξειδίκευση αλλά και προσπάθεια από τον πελάτη
      - Ο πάροχος μπορεί να κλιμακώσει την χωρητικότητα, τις δημόσιες εγγραφές καθώς και να καθοδηγήσει για την εφαρμογή καλών πρακτικών BC/DR
        - Αυτό είναι ιδιαίτερα αληθές σε ένα περιβάλλον νέφους όπου ο πάροχος προσφέρει διευκολύνσεις αυτόματης απάντησης σε σφάλματα προστατεύοντας τα συστήματά και την υποδομή

Επιχειρησιακή Συνέχεια & Σχεδιασμός Ανάνηψης από Καταστροφές

- Υπάρχουν διάφοροι επιχειρησιακοί οδηγοί κατά τον σχεδιασμό, εκτέλεση και δοκιμή λύσεων BC/DR
  - Ο σωστός συνδυασμός τους θα επηρεάσει την επιχειρησιακή στρατηγική BC/DR
  - Θέματα που πρέπει να ληφθούν υπόψιν:
    - Ποια είναι η αξία των επιχειρησιακών δεδομένων και πόσο κοστίζει η αντικατάσταση τους αν χαθούν ή κλαπούν; Ποια δεδομένα θα μεταφερθούν στο νέφος;
    - Πόσο αποτελεσματική είναι η σχεδίαση BC/DR του παρόχου; Μπορεί να παρέχει όλους τους απαραίτητους πόρους για BC/DR
    - Πως πραγματοποιείται η δοκιμή ανάνηψης από καταστροφές; Την υποστηρίζει ο πάροχος;
    - Πως προσπελαύνονται οι υπηρεσίες ανάνηψης από καταστροφές;

Επιχειρησιακή Συνέχεια & Σχεδιασμός Ανάνηψης από Καταστροφές

- Εκτός από τα λογικά συστατικά μέρη της BC/DR πρέπει να ληφθούν υπόψη φυσικές τοποθεσίες όπως εναλλακτικά μέρη λειτουργίας & γεωγραφικά κατανεμημένα κέντρα δεδομένων, η επιβιωσιμότητα του δικτύου και η ενσωμάτωση οικοσυστημάτων τρίτων μερών στην σχεδίαση και δοκιμή
- Οι απαιτήσεις προστασίας δεδομένων μπορεί να περιορίσουν τα δεδομένα που αντιστοιχούν σε πληροφορία προσωπικού προσδιορισμού (personally identifiable information)
  - Η προσεκτική επιλογή του παρόχου και η ξεκάθαρη κατανόηση της τοποθεσίας των κέντρων δεδομένων του μαζί με τις πολιτικές μετακίνησης δεδομένων του μπορούν να μετριάσουν αυτό τον κίνδυνο

Βασιζόμενες στο Νέφος Ομάδες Ασφάλειας (Cloud-Based Security Groups)

- Η προστασία δεδομένων αυξάνεται όταν τίθενται φραγμοί ανάμεσα σε πόρους ΤΠ
- Αυτό μπορεί να επιτευχθεί μέσω διαδικασίας τμηματοποίησης πόρων νέφους (resource segmentation):
  - δημιουργεί ξεχωριστά φυσικά & εικονικά περιβάλλοντα ΤΠ για διαφορετικούς χρήστες & ομάδες χρηστών
    - Παράδειγμα: το ΔΕΠ ενός οργανισμού μπορεί να διαμεριστεί σύμφωνα με συγκεκριμένες απαιτήσεις ασφάλειας δικτύου. Ένα μέρος θα αντιστοιχεί σε ένα δίκτυο με ανθεκτικό τείχος προστασίας για την πρόσβαση στο διαδίκτυο. Ενώ το άλλο μέρος θα αναπτυχθεί εσωτερικά χωρίς τείχος προστασίας διότι θα αντιστοιχεί σε εσωτερικούς χρήστες που δεν έχουν πρόσβαση στο διαδίκτυο

Βασιζόμενες στο Νέφος Ομάδες Ασφάλειας

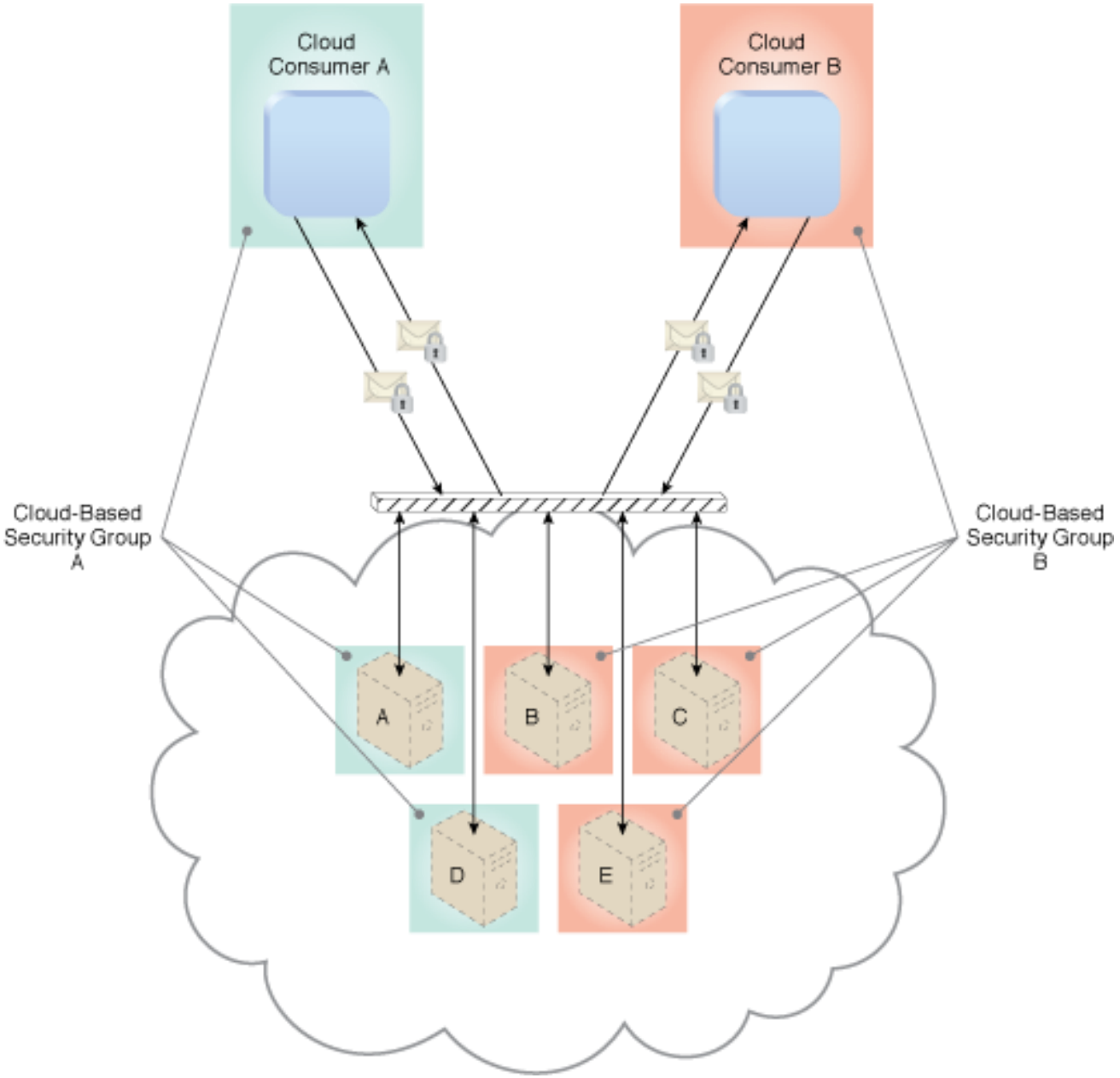
- Η τμηματοποίηση καταρχάς διευκολύνει την εικονικοποίηση των φυσικών πόρων
  - Όμως, πρέπει να βελτιστοποιείται σε περιβάλλοντα δημόσιου νέφους όπου τα όρια εμπιστοσύνης μεταξύ διαφορετικών καταναλωτών επικαλύπτονται
- Η τμηματοποίηση πόρων δημιουργεί μηχανισμούς βασιζόμενους στο νέφος ομάδας ασφάλειας που καθορίζονται από πολιτικές ασφάλειας
  - Συνέπειες:
    - τα δίκτυα τμηματοποιούνται σε λογικές βασιζόμενες στο νέφος ομάδες που δημιουργούν περιμέτρους λογικών δεδομένων
    - Κάθε πόρος ΤΠ τοποθετείται σε τουλάχιστον μια λογική ομάδα
    - Σε κάθε λογική ομάδα ασφάλειας εκχωρούνται κανόνες που καθορίζουν την επικοινωνία μεταξύ των διαφορετικών ομάδων

Βασιζόμενες στο Νέφος Ομάδες Ασφάλειας

- Είναι πιθανό διαφορετικοί εικονικοί εξυπηρετητές που τρέχουν πάνω από τον ίδιο φυσικό να αντιστοιχιστούν σε διαφορετικές λογικές ομάδες
  - Επιπλέον, μπορεί να διαχωριστούν περαιτέρω σε δημόσιες-ιδιωτικές ομάδες, σε ομάδες ανάπτυξης-παραγωγής ή με βάση οποιοδήποτε άλλο χαρακτηριστικό που συγκροτείται από τον διαχειριστή του (είδους) πόρου

Βασιζόμενες στο Νέφος Ομάδες Ασφάλειας

- Οι ομάδες ασφάλειας απεικονίζουν περιοχές στις οποίες μπορούν να εφαρμοστούν διαφορετικά μέτρα ασφάλειας
- Η σωστή διαμόρφωση και χρήση μέτρων ασφάλειας στις ομάδες μπορεί να βοηθήσει στον περιορισμό της μη εξουσιοδοτημένης πρόσβασης σε περίπτωση παραβίασης ασφάλειας
- Ο μηχανισμός αυτός μπορεί να χρησιμοποιηθεί στην αντιμετώπιση των απειλών άρνησης υπηρεσίας, ανεπαρκούς εξουσιοδότησης & αλληλοκάλυψης ορίων εμπιστοσύνης ενώ σχετίζεται στενά με τον μηχανισμό περιμέτρου λογικού δικτύου


Cloud
Consumer A
Cloud
Consumer B
Cloud-Based
Security Group
A
Cloud-Based
Security Group
B
A
B
C
D
E

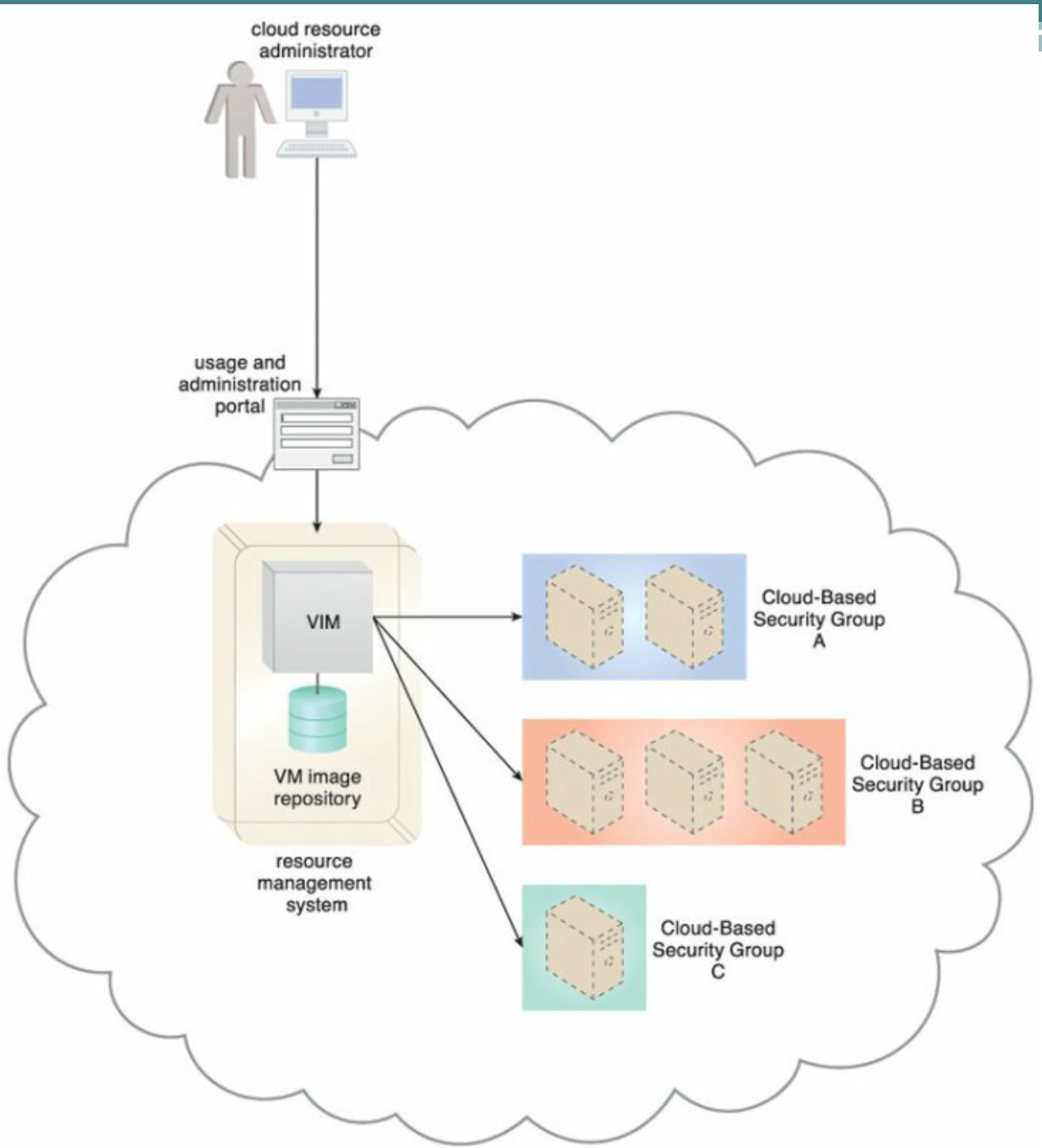
Πηγή: [1]

Παράδειγμα Μελέτης - DTGOV

- Η DTGOV έχει γίνει πάροχος νέφους αλλά εφόσον έχει πελάτες στο δημόσιο τομέα, θα πρέπει να αντιμετωπίσει κατάλληλα θέματα ασφάλειας ειδικότερα όσον αφορά την πρόσβαση στα δεδομένα αυτών των πελατών
- Για αυτό το λόγο, καλείται μια ομάδα ειδικών ασφάλειας, οι οποίοι προτείνουν τον ορισμό ομάδων ασφάλειας καθώς και την χρήση μηχανισμών ψηφιακής υπογραφής & PKI

Παράδειγμα Μελέτης - DGOV

- Οι πολιτικές ασφάλειας κατατάσσονται σε επίπεδα τμηματοποίησης πόρων πριν να υλοποιηθούν στο αντίστοιχο διαδικτυακό σύστημα διαχείρισης
- Για την ικανοποίηση των απαιτήσεων ασφάλειας που πηγάζουν επίσης από SLAs, η DTGOV αντιστοιχεί την κατανομή πόρων ΤΠ στα επίπεδα τμηματοποίησης των λογικών ομάδων ασφάλειας (που έχουν τις δικές τους πολιτικές ασφάλειας) για την εγγύηση των επιπέδων απομόνωσης και ελέγχου των πόρων ΤΠ
- Το νέο αυτό χαρακτηριστικό (των διαφορετικών επιπέδων ασφάλειας) διαδίδεται στους πελάτες της DTGOV που έχουν την ευχέρεια να το χρησιμοποιήσουν με μια επιπλέον χρέωση


cloud resource administrator
usage and administration portal
VIM
VM image repository
resource management system
Cloud-Based Security Group A
Cloud-Based Security Group B
Cloud-Based Security Group C

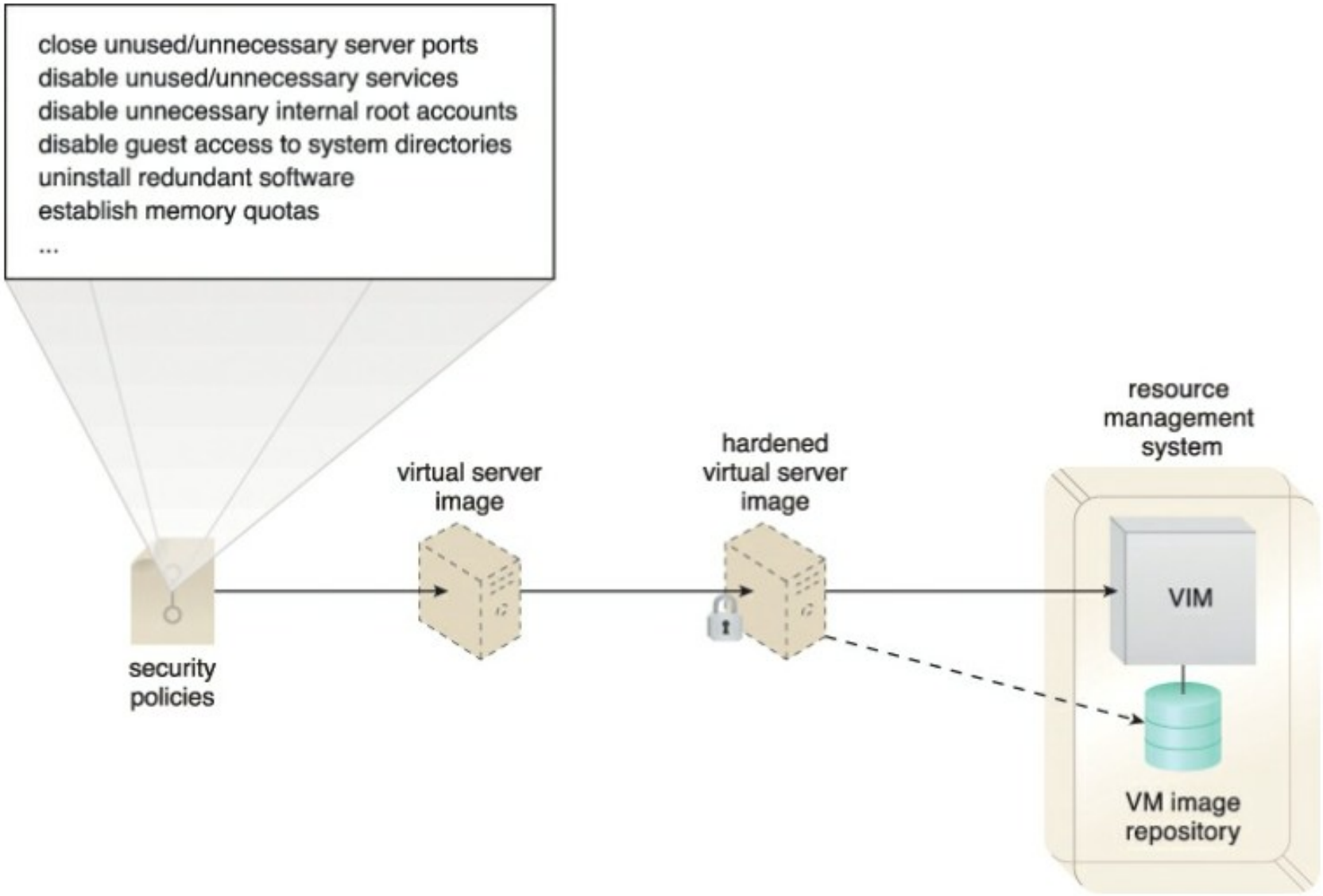
Πηγή: [1]

Σκλήρυνση Εικόνων Εικονικών Εξυπηρετητών (Virtual Server Image Hardening)

- Η εικόνα ενός εικονικού εξυπηρετητή αποτελεί ένα πρότυπο συγκρότησης
- Σκλήρυνση είναι η διαδικασία απογύμνωσης ενός συστήματος από μη χρήσιμο λογισμικό για τον περιορισμό των πιθανών τρωτοτήτων
  - Επιπλέον, μπορεί να περιλαμβάνει το κλείσιμο μη χρησιμοποιούμενων θυρών εξυπηρετητή καθώς και την απενεργοποίηση μη χρησιμοποιούμενων υπηρεσιών, εσωτερικών ριζικών λογαριασμών και της πρόσβασης επισκεπτών
  - Τέλος, μπορεί να περιλαμβάνει την ανανέωση εκδόσεων λογισμικού (ειδικότερα στο λειτουργικό σύστημα) για την διόρθωση κενών ασφάλειας και σφαλμάτων

Σκλήρυνση Εικόνων Εικονικών Εξυπηρετητών

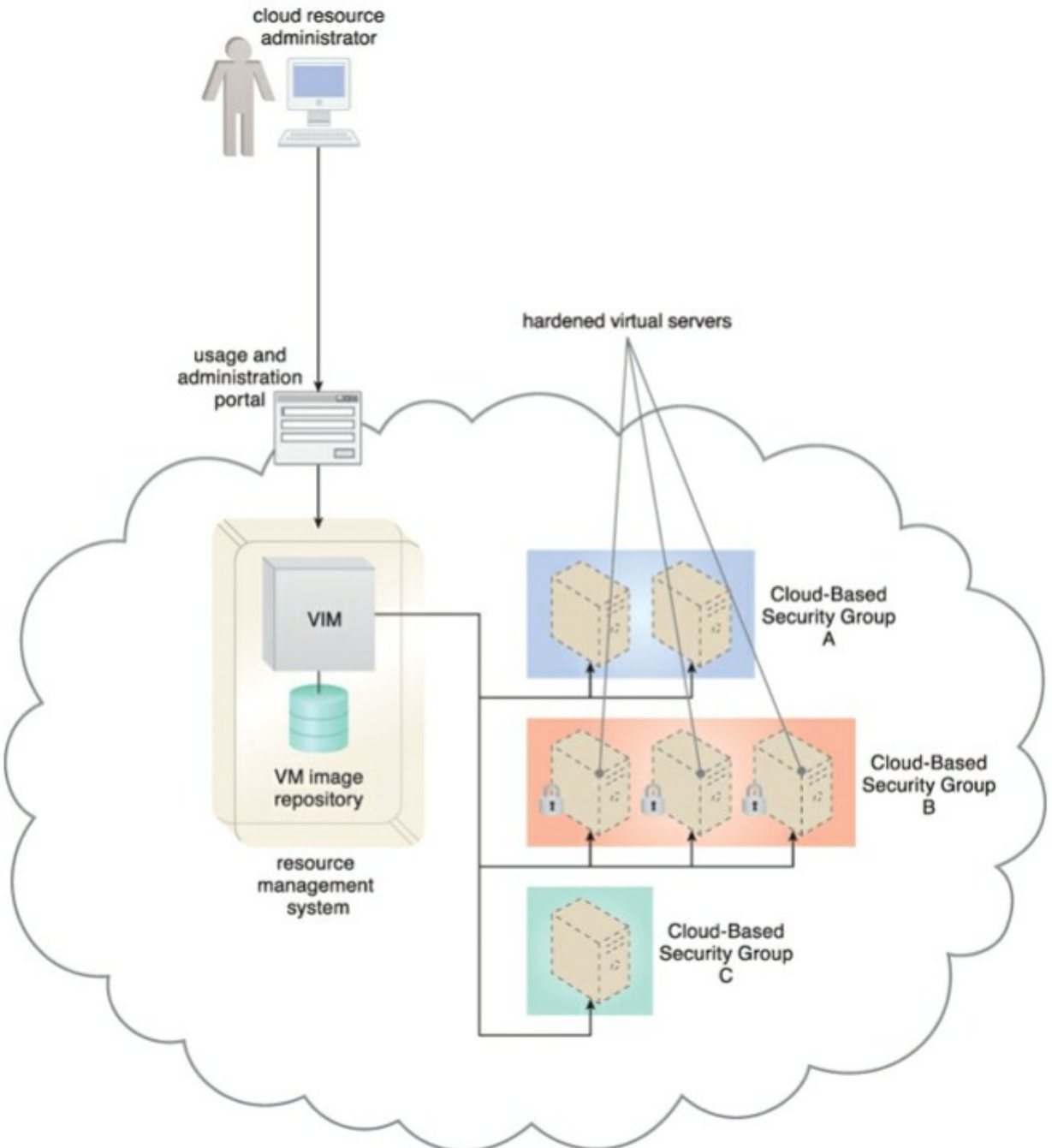
- Το αποτέλεσμα της εφαρμογής της διαδικασίας σκλήρυνσης είναι μια εικόνα εικονικού εξυπηρετητή που είναι σκληρυμένη και άρα πιο ασφαλής
  - Συνεπώς, έχουμε τη δημιουργία εικονικών εξυπηρετητών που είναι περισσότερο ασφαλείς μέσω της χρήσης σκληρυμένων προτύπων εικόνων
- Οι σκληρυμένες εικόνες εξυπηρετητών μας επιτρέπουν να αντιμετωπίσουμε απειλές όπως άρνησης υπηρεσίας, ανεπαρκούς εξουσιοδότησης και αλληλοκάλυψης ορίων εμπιστοσύνης


close unused/unnecessary server ports
disable unused/unnecessary services
disable unnecessary internal root accounts
disable guest access to system directories
uninstall redundant software
establish memory quotas
...
security policies
virtual server image
hardened virtual server image
resource management system
VIM
VM image repository

Πηγή: [1]

Παράδειγμα Μελέτης - DTGOV

- Η DTGOV προσφέρει την επιλογή σκλήρυνσης εικονικών εξυπηρετητών μέσα σε μια δεδομένη ομάδα
  - Η κάθε σκλήρυνση εξυπηρετητή χρεώνεται έξτρα αλλά γλυτώνει τους καταναλωτές από το να επιχειρήσουν την διαδικασία σκλήρυνσης οι ίδιοι


cloud resource administrator
hardened virtual servers
usage and administration portal
VIM
VM image repository
resource management system
Cloud-Based Security Group A
Cloud-Based Security Group B
Cloud-Based Security Group C

Πηγή: [1]

Πηγές / Βιβλιογραφία

1. Thomas Erl, Zaigham Mahmood, Ricardo Puttini. Cloud Computing: Concepts Technology & Architecture, Pearson, 2013
2. Chellammal Surianarayanan & Pethuru Raj Chelliah. Essentials of Cloud Computing. Springer International Publishing, 2019
3. San Murugesan, Irena Bojanova. Encyclopedia of Cloud Computing. John Wiley & Sons, Ltd. 2016