2023-05

þÿ ¥ À ¿ » ¿ ³ ¹ Ã Ä ¹ º Ì ½ - Æ ¿ Â : ‘ ½ ± Ã º Ì

þÿ ‘ À µ ¹ » - Â º ± ¹ £ Ä Á ± Ä · ³ ¹ º - Â ’ µ » Ä ¯

þÿ » ± Ä ¬ Á ¿ Â , ± ½ ± ³ ¹ Î Ä · Â

þÿ œ µ Ä ± À Ä Å Ç ¹ ± º Ì Ã Ä ± » · Á ¿ Æ ¿ Á ¹ ± º ¬ £ Å Ã Ä ® ¼ ± Ä ± º ± ¹ ¨ · Æ ¹ ± º ® š ± ¹ ½ ¿ Ä ¿ ¼ ¯ ± ,
þÿ º ± ¹ • À ¹ Ã Ä ® ¼ · Â ¥ À ¿ » ¿ ³ ¹ Ã Ä Î ½ , ± ½ µ À ¹ Ã Ä ® ¼ ¹ ¿ • µ ¬ À ¿ » ¹ Â ¬ Æ ¿ Å

ΣΧΟΛΗ Distance Information Systems and Digital Innovation

Υπολογιστικό νέφος : Ανασκόπηση, Απειλές και Στρατηγικές Βελτίωσης

ΠΑΝΑΓΙΩΤΗΣ ΠΛΑΤΑΡΟΣ

ΜΑΙΟΣ/2023

ΣΧΟΛΗ Πληροφοριακά Συστήματα και τη Ψηφιακή Καινοτομία

Υπολογιστικό νέφος : Ανασκόπηση, Απειλές και Στρατηγικές Βελτίωσης

Διπλωματική Εργασία η οποία υποβλήθηκε προς απόκτηση Μεταπτυχιακού τίτλου σπουδών στα Πληροφοριακά Συστήματα και τη Ψηφιακή Καινοτομία στο Πανεπιστήμιο Νεάπολις

ΠΑΝΑΓΙΩΤΗΣ ΠΛΑΤΑΡΟΣ

ΜΑΙΟΣ/2023

Περιεχόμενα

Ονοματεπώνυμο Φοιτητή/Φοιτήτριας: Παναγιώτης Πλατάρος

Τίτλος Διπλωματικής Εργασίας: Υπολογιστικό νέφος : Ανασκόπηση, Απειλές και Στρατηγικές Βελτίωσης

Η παρούσα Διπλωματική Εργασία εκπονήθηκε στο πλαίσιο των σπουδών για την απόκτηση εξ αποστάσεως μεταπτυχιακού τίτλου στο Πανεπιστήμιο Νεάπολις και εγκρίθηκε στις [ημερομηνία έγκρισης] από τα μέλη της Εξεταστικής Επιτροπής.

Εξεταστική Επιτροπή: Πρώτος επιβλέπων (Πανεπιστήμιο Νεάπολις Πάφος)

[ονοματεπώνυμο, βαθμίδα, υπογραφή] Μέλος Εξεταστικής Επιτροπής:

[ονοματεπώνυμο, βαθμίδα, υπογραφή] Μέλος Εξεταστικής Επιτροπής:

[ονοματεπώνυμο, βαθμίδα, υπογραφή]

Ή ΥΠΕΥΘΥΝΗ ΔΗΛΩΣΗ Ο Παναγιώτης Πλατάρος , γνωρίζοντας τις συνέπειες της λογοκλοπής, δηλώνω υπεύθυνα ότι η παρούσα εργασία με τίτλο «Υπολογιστικό νέφος : Ανασκόπηση, Απειλές και Στρατηγικές Βελτίωσης», αποτελεί προϊόν αυστηρά προσωπικής εργασίας και όλες οι πηγές που έχω χρησιμοποιήσει, έχουν δηλωθεί κατάλληλα στις βιβλιογραφικές παραπομπές και αναφορές. Τα σημεία όπου έχω χρησιμοποιήσει ιδέες, κείμενο ή/και πηγές άλλων συγγραφέων, αναφέρονται ευδιάκριτα στο κείμενο με την κατάλληλη παραπομπή και η σχετική αναφορά περιλαμβάνεται στο τμήμα των βιβλιογραφικών αναφορών με πλήρη περιγραφή.

Ο/Η Δηλών /σα

Παναγιώτης Πλατάρος

Περίληψη

Το υπολογιστικό νέφος είναι ένα σύνολο πόρων και υπηρεσιών που προσφέρονται μέσω του Διαδικτύου. Οι υπηρεσίες νέφους παρέχονται από κέντρα δεδομένων που βρίσκονται σε όλο τον κόσμο. Το υπολογιστικό νέφος διευκολύνει τους καταναλωτές του παρέχοντας εικονικούς πόρους μέσω του διαδικτύου. . Η ραγδαία ανάπτυξη στον τομέα του "cloud computing" αυξάνει επίσης τις σοβαρές ανησυχίες για την ασφάλεια. Η ασφάλεια παρέμεινε ένα σταθερό ζήτημα για τα ανοικτά συστήματα και το διαδίκτυο, όταν μιλάμε για ασφάλεια το σύννεφο υποφέρει πραγματικά. Η έλλειψη ασφάλειας είναι το μοναδικό εμπόδιο στην ευρεία υιοθέτηση του cloud computing. Το υπολογιστικό νέφος περιβάλλεται από πολλά ζητήματα ασφάλειας, όπως η διασφάλιση των δεδομένων και η εξέταση της χρήσης του νέφους από τους προμηθευτές υπολογιστικού νέφους. Η παρούσα μελέτη αποσκοπεί στον εντοπισμό των πιο ευάλωτων απειλών ασφαλείας στο υπολογιστικό νέφος, γεγονός που θα επιτρέψει τόσο στους τελικούς χρήστες όσο και στους προμηθευτές να γνωρίζουν τις βασικές απειλές ασφαλείας που σχετίζονται με το υπολογιστικό νέφος. Η εργασία επίσης θα παρουσίαση ένα σημαντικό εργαλείο για την εξάλειψη των κινδύνων αυτών. Τα συστήματα ανίχνευσης εισβολών (IDS) αποτελούν έναν απαραίτητο μηχανισμό άμυνας. Δυστυχώς, η ικανότητά τους υπολείπεται της αντίστοιχης των επιτιθέμενων. Αυτό μας παρακινεί να βελτιώσουμε την κατανόηση των βαθύτερων αιτιών των ψευδώς αρνητικών αποτελεσμάτων τους. Στο έγγραφο αυτό κάνουμε ένα πρώτο βήμα προς τον τελικό στόχο ώστε να αντλήσουμε χρήσιμες γνώσεις και αρχές που μπορούν να καθοδηγήσουν το σχεδιασμό των IDS επόμενης γενιάς. Συγκεκριμένα, προτείνουμε μια μεθοδολογία για την ανάλυση των βαθύτερων αιτιών των ψευδώς αρνητικών IDS και διεξάγουμε μια μελέτη περίπτωσης με βάση το Snort και ένα σύνολο δεδομένων πραγματικού κόσμου από κυβερνοεπιθέσεις. Η μελέτη περίπτωσης μας επιτρέπει να αντλήσουμε χρήσιμες πληροφορίες.

Λέξεις κλειδιά: IDS, Snort , προκλήσεις για την ασφάλεια του νέφους, μοντέλα ασφάλειας του νέφους, Υιοθέτηση νέφους

Κεφάλαιο 1 : Εισαγωγή

Παρόλο που το υπολογιστικό νέφος, ως μοντέλο, δεν είναι καινούργιο, οι οργανισμοί το εφαρμόζουν όλο και περισσότερο λόγω της μεγάλης κλίμακας υπολογισμών και αποθήκευσης δεδομένων, της ευέλικτης επεκτασιμότητας, της σχετικής αξιοπιστίας και της οικονομίας κόστους των υπηρεσιών. Ωστόσο, παρά την ταχεία υιοθέτησή του σε ορισμένους τομείς και τομείς, είναι προφανές από έρευνες και στατιστικά στοιχεία, ότι οι απειλές που σχετίζονται με την ασφάλεια αποτελούν το πιο αξιοσημείωτο εμπόδιο για την ευρεία υιοθέτησή του. Επομένως ο καθένας θέτει το ερώτημα, είναι οι πληροφορίες του ασφαλείς; Γι' αυτό υπάρχουν Τα συστήματα ανίχνευσης εισβολών (IDS) είναι ένα απαραίτητο εργαλείο άμυνας. Ωστόσο, πρόσφατες μελέτες δείχνουν ότι έχουν σημειώσει σημαντικές απώλειες στην αποτελεσματικότητα της ανίχνευσης . Ενώ μπορεί να είναι διαισθητικό να υποθέσουμε ότι οι επιτιθέμενοι έχουν ξεγελάσει τους προγραμματιστές IDS σε αυτό το παιχνίδι της γάτας με το ποντίκι. Γι' αυτό πρέπει να προσδιορίσουμε με ακρίβεια τις αιτίες αυτής της μειούμενης αποτελεσματικότητας. Είναι σημαντικό, λοιπόν, να αναζητήσουμε προσεγγίσεις για να καταστήσουμε τα IDS τόσο χρήσιμα όσο το δυνατόν περισσότερο. Αυτό μας παρακινεί να διερευνήσουμε τα βαθύτερα αίτια των των ψευδώς αρνητικών αποτελεσμάτων ανίχνευσης εισβολών με τη χρήση σύγχρονων επιθέσεων στον κυβερνοχώρο με σύνολα δεδομένων με γνωστή βασική αλήθεια.

1.1 Ερωτήματα της έρευνας

Συνεπώς, το κύρια ερωτήματα της έρευνας διαμορφώνονται ως εξής:

1. Ποιοι κίνδυνοι ασφαλείας και ποιες λύσεις παρουσιάζονται στη βιβλιογραφία σχετικά με τη ασφάλεια cloud computing ;

2. Ποια είναι τα προβλήματα ασφάλειας που δεν έχουν αντιμετωπιστεί;

3. Πως τα συστήματα IDS μπορούν να δώσουν λύση στο πρόβλημα;

1.2 Μέθοδος

Για τη μελέτη τη συγκεκριμένης έρευνας επικεντρωθήκαμε σε λέξεις-κλειδιά αναζήτησης, ηλεκτρονικές πηγές, εργαλείο διαχείρισης αναφορών και διαδικασία αναζήτησης. Απαιτείται να εντοπιστεί και να αναλυθεί η πρόσφατη βιβλιογραφία, οι έρευνες και οι μελέτες που έχουν δημοσιευθεί πάνω στο συγκεκριμένο ζήτημα. Θα πάρουμε λέξεις-κλειδιά από τη σχετική βιβλιογραφία για θέματα ασφάλειας υπολογιστικού νέφους. Εμείς παρουσιάζουμε τις λέξεις-κλειδιά αναζήτησης στα ακόλουθα. "προκλήσεις για την ασφάλεια του νέφους". Τέλος μέσω της μελέτης περίπτωσης παρουσιάζονται οι συνεισφορές μιας εργασίας που προτείνει μια μεθοδολογία για τον εντοπισμό και την ανάλυση ψευδώς αρνητικών αποτελεσμάτων σε συστήματα ανίχνευσης εισβολών (IDS).

1.3 Δομή

Στο κεφάλαιο της εισαγωγής, έγινε αναφορά στο χώρο έρευνας της μεταπτυχιακή διατριβής , αναφέραμε τις ελλείψεις που υπάρχουν στην βιβλιογραφία, καθορίσαμε το στόχο της εργασίας και τέλος τη μεθοδολογία που ακολουθήσαμε για την εκπόνηση της.

Στο δεύτερο κεφάλαιο περιγράφεται το υπολογιστικό νέφος. Πιο συγκεκριμένα αναλύουμε: τον ορισμό του υπολογιστικού νέφους, τα χαρακτηριστικά του , τα μοντέλα υπολογιστικού νέφους (Software as a service (SaaS), Platform as a Service (PaaS), και Infrastructure as a Service (IaaS)). Τέλος αναλύουμε τα 4 μοντέλα ανάπτυξης (δημόσιο, το ιδιωτικό, το κοινοτικό και το υβριδικό).

Στο τρίτο κεφάλαιο γένεται αναφορά στις απειλές που μπορεί να αντιμετωπίσουμε κατά την υιοθέτηση του υπολογιστικού νέφους. Παρουσιάζονται τρόποι επιθέσεων που γίνονται στο υπολογιστικό νέφος και πως οι χάκερ παραβιάζουν το σύστημα. Μάσα σε όλα αυτά καταλήγουμε στο συμπέρασμα ότι και το υπολογιστικό νέφος έχει και αυτό θέματα ασφαλείας και τρωτά σημεία .

Στο τέταρτο κεφάλαιο παρουσιάζονται μερικές από τις πολιτικές ασφαλείας που εφαρμόζονται για την εξάλειψη των απειλών και των κινδύνων που παρουσιάζονται στο υπολογιστικό νέφος. Συνοπτικά αναφέρονται μερικά μέτρα αντιμετώπισης.

Στο πέμπτο κεφάλαιο παρουσιάζεται η υιοθέτηση του υπολογιστικού νέφους από του οργανισμούς . συγκεκριμένα περιγράφουμε το πως γίνεται η υιοθέτηση ανάλογα με το μέγεθος του οργανισμού . Τι προβλήματα μπορεί να προκύψουν κατά τη διαδικασία της υιοθέτησης, ενώ στο τέλος παρουσιάζονται τα 10 βασικά οφέλη της υιοθέτησης του Cloud για τις επιχειρήσεις.

Στο έκτο κεφάλαιο παρουσιάζεται μια μελέτη περίπτωσης που χρησιμοποιεί το σύστημα ανίχνευσης εισβολών Snort αποδεικνύει τη χρησιμότητα της μεθοδολογίας, αποκαλύπτοντας ζητήματα με τα σύνολα κανόνων του Snort, τις ειδοποιήσεις, τις αρχές σχεδιασμού και την επιθεώρηση του ωφέλιμου φορτίου. Τα ευρήματα αυτά υποδηλώνουν την ανάγκη για πολλαπλά σύνολα κανόνων και βελτιώσεις στις πληροφορίες ειδοποιήσεων και στην τήρηση των κανόνων για την ενίσχυση της αποτελεσματικότητας των IDS.

Κεφάλαιο 2 : Βιβλιογραφική Ανασκόπηση

2.1 Υπολογιστικό νέφος

2.1.1 Τί είναι το υπολογιστικό νέφος ;

Το υπολογιστικό νέφος είναι ένα μοντέλο που επιτρέπει την πανταχού παρούσα, βολική, δικτυακή πρόσβαση κατά παραγγελία σε μια κοινόχρηστη δεξαμενή διαμορφώσιμων υπολογιστικών πόρων (π.χ. δίκτυα, διακομιστές, αποθήκευση, εφαρμογές και υπηρεσίες), οι οποίοι μπορούν να παρέχονται και να απελευθερώνονται γρήγορα με ελάχιστη προσπάθεια διαχείρισης ή αλληλεπίδρασης με τον πάροχο υπηρεσιών. Το μοντέλο του υπολογιστικού νέφους αποτελείται από πέντε βασικά χαρακτηριστικά, τρία μοντέλα υπηρεσιών και τέσσερα μοντέλα ανάπτυξης. (Peter Mell, 2011)

Το Cloud Computing έχει αναδειχθεί ως μια σημαντική τεχνική στον τομέα των εφαρμογών πληροφορικής και της τεχνολογίας πληροφοριών. Περιλαμβάνει υπηρεσίες για την αποθήκευση, την επεξεργασία και τη μετάδοση δεδομένων μέσω κοινόχρηστων πόρων, μέσω του διαδικτύου. Οι πόροι που χρησιμοποιούνται για αυτές τις υπηρεσίες μπορεί να είναι μετρήσιμες και οι πελάτες μπορούν να χρεώνονται για τους πόρους που χρησιμοποιούν. (Bhowmik, 2017)

Το υπολογιστικό νέφος είναι μια πολύπλευρη έννοια που περιλαμβάνει διάφορες τεχνολογίες και μοντέλα ανάπτυξης. Ο όρος "σύννεφο" υποδηλώνει μια αφηρημένη οντότητα όπου οι πόροι είναι διαθέσιμοι κατά παραγγελία μέσω μιας σύνδεσης δικτύου και όχι τοπικά παρεχόμενοι. Αυτή η αφαίρεση επιτρέπει μεγαλύτερη ευελιξία, επεκτασιμότητα και εξοικονόμηση κόστους σε σύγκριση με τις παραδοσιακές προσεγγίσεις. (Attaran, 2017) Παρά τις ανησυχίες σχετικά με την ασφάλεια και την προστασία της ιδιωτικής ζωής, το υπολογιστικό νέφος έχει γίνει όλο και πιο δημοφιλές τα τελευταία χρόνια, με πολλές επιχειρήσεις και ιδιώτες να βασίζονται σε λύσεις που βασίζονται στο νέφος για τις υπολογιστικές τους ανάγκες.

Το υπολογιστικό νέφος είναι μία από τις πιο μετασχηματιστικές τεχνολογίες που εμφανίστηκαν τα τελευταία χρόνια. Διευκόλυνε την απομακρυσμένη πρόσβαση σε δεδομένα και εφαρμογές, δίνοντας τη δυνατότητα σε ιδιώτες και επιχειρήσεις να έχουν μεγαλύτερη ευελιξία και αποτελεσματικότητα. Ένα από τα βασικά πλεονεκτήματα της τεχνολογίας υπολογιστικού νέφους είναι ότι επιτρέπει στους οργανισμούς να παρακολουθούν το εξωτερικό περιβάλλον λειτουργίας τους μέσω συνδέσεων μεταξύ

προμηθευτών, διανομέων και πελατών μέσω μιας κεντρικής τοποθεσίας. Αυτό σημαίνει ότι οι οργανισμοί μπορούν να συνεργάζονται ευκολότερα με εταίρους και ενδιαφερόμενους φορείς σε διαφορετικές τοποθεσίες χωρίς να περιορίζονται από γεωγραφικά όρια. (Attaran, 2017) Επιπλέον, το υπολογιστικό νέφος μπορεί να συμβάλει στη μείωση του κόστους που συνδέεται με τη συντήρηση του υλικού, καθώς οι χρήστες δεν χρειάζεται πλέον να βασίζονται σε φυσικούς διακομιστές για αποθήκευση ή επεξεργαστική ισχύ. Με αυτά τα οφέλη κατά νου, είναι σαφές γιατί τόσες πολλές εταιρείες υιοθετούν λύσεις που βασίζονται στο cloud ως μέρος των στρατηγικών ψηφιακού μετασχηματισμού τους. Η εκρηκτικότητα αυτής της παραγράφου προέρχεται από τη χρήση τόσο μεγάλων προτάσεων με πολύπλοκες γλωσσικές δομές όσο και μικρότερων φράσεων όπως "μεγαλύτερη ευελιξία", οι οποίες διευκολύνουν τους αναγνώστες να κατανοήσουν σύνθετες έννοιες. Η αμηχανία προέρχεται από τον συνδυασμό τεχνικών όρων όπως "απομακρυσμένοι διακομιστές", "εφαρμογές", "συνδέσεις" και "κεντρική τοποθεσία". Αυτοί οι όροι απαιτούν την προσοχή των αναγνωστών, καθώς μπορεί να μην είναι εξοικειωμένοι με αυτούς, αλλά είναι απαραίτητοι για να τους βοηθήσουν να κατανοήσουν τι συνεπάγεται το Cloud Computing.

2.1.2 Μοντέλα υπολογιστικού νέφους

Σύμφωνα με τους διαφορετικούς τύπους υπηρεσιών που προσφέρονται, το cloud computing μπορεί να θεωρηθεί ότι αποτελείται από τρία επίπεδα: Software as a service (SaaS), Platform as a Service (PaaS), και Infrastructure as a Service (IaaS). Η υποδομή ως υπηρεσία (IaaS) είναι το χαμηλότερο επίπεδο που παρέχει βασική υπηρεσία υποστήριξης υποδομής. Το στρώμα πλατφόρμας ως υπηρεσίας (PaaS) είναι το μεσαίο στρώμα, το οποίο προσφέρει υπηρεσίες προσανατολισμένες στην πλατφόρμα, εκτός από την παροχή του περιβάλλοντος για τη φιλοξενία των χρηστών εφαρμογών του χρήστη. Το λογισμικό ως υπηρεσία (SaaS) είναι το ανώτερο στρώμα το οποίο διαθέτει μια πλήρη εφαρμογή που προσφέρεται ως υπηρεσία κατά παραγγελία (Mohammed, 2021).

Τα τρία μοντέλα περιγράφονται ως εξής:

Software-as-a-Service (SaaS): Το SaaS μπορεί να περιγραφεί ως μια διαδικασία με την οποία ο πάροχος υπηρεσιών εφαρμογών (ASP) παρέχει διάφορες εφαρμογές λογισμικού μέσω του Διαδικτύου. Αυτό κάνει τον πελάτη να απαλλαγεί από την εγκατάσταση και λειτουργίας της εφαρμογής στον υπολογιστή του και εξαλείφει επίσης το τεράστιο φορτίο της συντήρησης του λογισμικού, συνεχούς λειτουργίας, διασφάλισης και υποστήριξης . Ο πάροχος SaaS αναλαμβάνει διαφημιστικά την ευθύνη για την ανάπτυξη και τη διαχείριση της υποδομής IT (διακομιστές, λογισμικό λειτουργικού συστήματος, βάσεις δεδομένων, χώρος στο κέντρο δεδομένων, δίκτυο πρόσβαση, ισχύς και ψύξη κ.λπ.) και των διαδικασιών (διορθώσεις/αναβαθμίσεις υποδομής, διορθώσεις/αναβαθμίσεις εφαρμογών, αντίγραφα ασφαλείας, κ.λπ.) που απαιτούνται για τη λειτουργία και τη διαχείριση της πλήρους λύσης. Το SaaS διαθέτει μια πλήρη εφαρμογή που προσφέρεται ως υπηρεσία κατά παραγγελία. Στο SaaS, υπάρχει ο μηχανισμός συνοχής Divided Cloud και Convergence, σύμφωνα με τον οποίο κάθε στοιχείο δεδομένων έχει είτε το "κλείδωμα ανάγνωσης" είτε το "κλείδωμα εγγραφής" . Δύο τύποι διακομιστών χρησιμοποιούνται από το SaaS: ο κύριος Consistence Server (MCS) και ο Domain Consistence Server (DCS). Η συνοχή της κρυφής μνήμης επιτυγχάνεται με τη συνεργασία μεταξύ MCS και DCS . Στον SaaS, εάν ο MCS υποστεί βλάβη ή παραβιαστεί, ο έλεγχος του περιβάλλον νέφους χάνεται. Ως εκ τούτου, η διασφάλιση του MCS έχει μεγάλη σημασία. Παραδείγματα SaaS περιλαμβάνουν: Google Apps, Salesforce.com. (Baharuddin, 2021)

Platform as a Service (PaaS): Είναι η παροχή μιας υπολογιστικής πλατφόρμας και μιας στοίβας λύσεων ως υπηρεσία χωρίς λήψη ή εγκατάσταση λογισμικού για προγραμματιστές, διαχειριστές πληροφορικής ή τελικούς χρήστες. Παρέχει μια υποδομή με υψηλό επίπεδο ολοκλήρωσης για την υλοποίηση και τη δοκιμή εφαρμογών νέφους. Ο χρήστης δεν διαχειρίζεται την υποδομή (συμπεριλαμβανομένου του δικτύου, των διακομιστών, των λειτουργικών συστημάτων και της αποθήκευσης), αλλά ελέγχει τις εφαρμογές που αναπτύσσονται και ενδεχομένως, τις διαμορφώσεις τους. Παραδείγματα PaaS : Force.com, Google App Engine και Microsoft Azure. (Parast, 2022)

Infrastructure as a Service (IaaS): αναφέρεται στον διαμοιρασμό πόρων υλικού για την εκτέλεση υπηρεσιών με τη χρήση της τεχνολογίας Virtualization. Ο κύριος στόχος της είναι να καταστήσει πόρους όπως οι διακομιστές, δίκτυο και αποθήκευση, πιο εύκολα προσβάσιμα από εφαρμογές και λειτουργικά συστήματα. Έτσι, προσφέρει βασικές υπηρεσίες υποδομής κατά παραγγελία και χρησιμοποιεί διεπαφή προγραμματισμού εφαρμογών (API) για αλληλεπιδράσεις με hosts, μεταγωγείς και δρομολογητές, καθώς και τη δυνατότητα προσθήκης νέου εξοπλισμού με απλό και διαφανή τρόπο. Γενικά, ο χρήστης δεν διαχειρίζεται το υποκείμενο υλικό στην υποδομή νέφους, αλλά ελέγχει τα λειτουργικά συστήματα, την αποθήκευση και τις εφαρμογές που αναπτύσσονται. Ο πάροχος υπηρεσιών κατέχει τον εξοπλισμό και είναι υπεύθυνος για τη στέγαση, τη λειτουργία και τη συντήρησή του. Ο πελάτης συνήθως πληρώνει ανά χρήση. Παραδείγματα IaaS περιλαμβάνουν τα Amazon Elastic Cloud Computing (EC2), Amazon S3, GoGrid.

2.1.3 Μοντέλα ανάπτυξης υπολογιστικού νέφους

Οι υπηρεσίες νέφους μπορούν να οργανωθούν ή να αναπτυχθούν με διάφορους τρόπους. Η επιλογή ανάπτυξης εξαρτάται από τις απαιτήσεις του οργανισμού-καταναλωτή. Το μοντέλο ανάπτυξης περιγράφει τη χρησιμότητα ενός νέφους και προσδιορίζει επίσης τα όρια πρόσβασής του. Το μοντέλο υποδεικνύει επίσης τη σχετική θέση του νέφους σε σχέση με τη θέση του οργανισμού-καταναλωτή. Το NIST σαν ορισμό αναφέρει τέσσερα κοινά μοντέλα ανάπτυξης, όπως το δημόσιο, το ιδιωτικό, το κοινοτικό και το υβριδικό.

Δημόσιο υπολογιστικό νέφος (Public cloud): Το μοντέλο ανάπτυξης του δημόσιου νέφους παρέχει το ευρύτερο φάσμα πρόσβασης στους καταναλωτές μεταξύ όλων των εφαρμογών νέφους. Οποιοσδήποτε εγγράφεται σε αυτό αποκτά ανοικτή πρόσβαση σε αυτή τη δυνατότητα νέφους. Το καταναλωτής μπορεί να είναι είτε ένας μεμονωμένος χρήστης είτε μια ομάδα ανθρώπων που εκπροσωπούν κάποιον οργανισμό ή μια επιχείρηση. Το δημόσιο νέφος αναφέρεται επίσης ως εξωτερικό νέφος, καθώς από άποψη φυσικής θέσης παραμένει εξωτερικό ή εκτός εγκαταστάσεων και οι καταναλωτές μπορούν στη συνέχεια να έχουν απομακρυσμένη πρόσβαση στην υπηρεσία. Ένα δημόσιο νέφος φιλοξενείται και διαχειρίζεται από ορισμένους προμηθευτές υπολογιστών οι οποίοι δημιουργούν κέντρα δεδομένων για την παροχή της υπηρεσίας

στους καταναλωτές. Οι καταναλωτές στο πλαίσιο αυτού του μοντέλου ανάπτυξης νέφους είναι εντελώς απαλλαγμένοι από οποιαδήποτε διαχείριση υποδομών και ζητήματα που σχετίζονται με τη διαχείριση του συστήματος. Αλλά, ταυτόχρονα, οι ίδιοι (οι καταναλωτές) θα έχουν χαμηλό βαθμό ελέγχου επί των cloud. Τα Amazon Web Services, Google Cloud, Microsoft Azure και Salesforce.com είναι μερικά από τα τα δημοφιλή δημόσια νέφη. (Yang, Wenyam, 2017)

Η ανάπτυξη του δημόσιου νέφους προωθεί την πολυενοικίαση στον υψηλότερο βαθμό. Ο ίδιος φυσικός υπολογιστικός πόρος μπορεί να διαμοιραστεί μεταξύ πολλών μη συνδεδεμένων καταναλωτών. Αυτό παρέχει σημαντικά πλεονεκτήματα, καθώς καθίσταται δυνατή η εξυπηρέτηση μεγάλου αριθμού χρηστών από έναν ενιαίο πάροχο νέφους . Όταν ένας μεγάλος αριθμός καταναλωτών διασκορπισμένων σε όλο τον κόσμο μοιράζεται πόρους από το κέντρο δεδομένων ενός και μόνο προμηθευτή, αυτό αυξάνει αυτόματα τα ποσοστά χρήσης των πόρων και μειώνει το κόστος παροχής υπηρεσιών του προμηθευτή. Συνεπώς, για τους καταναλωτές, το βασικό όφελος από τη χρήση δημόσιου νέφους είναι το οικονομικό του πλεονέκτημα. Οι πάροχοι δημόσιου νέφους από την άλλη πλευρά, εκμεταλλεύονται το μέγεθος των λειτουργίων. Όντας μεγάλοι σε όγκο και επιχειρήσεις, μπορούν να αντέξουν οικονομικά την τελευταία λέξη της τεχνολογίας και εξειδικευμένους ανθρώπους. Αυτό εξασφαλίζει καλύτερη ποιότητα υπηρεσιών. Μέσω αυτού του μοντέλου, οι καταναλωτές μπορούν να έχουν πρόσβαση σε δυνητικά ανώτερες υπηρεσίες με χαμηλότερο κόστος. Δεδομένου ότι οι διαφορετικοί καταναλωτές (από διαφορετικές μέρη του κόσμου) έχουν μεταβλητές απαιτήσεις φόρτου εργασίας κατά τη διάρκεια μιας ημέρας, εβδομάδας, μήνα ή του έτους, ένας πάροχος νέφους μπορεί πάντα να υποστηρίζει αποτελεσματικά τα φορτία κατά τη διάρκεια της υψηλής ζήτησης (η οποία είναι συνήθως αυξάνεται από ένα τμήμα των καταναλωτών του, σε κάθε συγκεκριμένη χρονική στιγμή).

Ιδιωτικό υπολογιστικό νέφος (Private cloud): Η ανάπτυξη του ιδιωτικού νέφους δεν παρέχει ανοικτή πρόσβαση σε όλους. Είναι κυρίως για οργανωτική χρήση και η πρόσβαση σε μια ιδιωτική εγκατάσταση νέφους είναι περιορισμένη για το ευρύ κοινό. Το ιδιωτικό νέφος επίσης αναφέρεται και ως εσωτερικό νέφος, δεδομένου ότι είναι κατασκευασμένο για την εξυπηρέτηση εσωτερικών σκοπών των οργανισμών. Ενώ τα δημόσια νέφη είναι εξίσου χρήσιμα τόσο για μεμονωμένους χρήστες όσο και για οργανισμούς, το ιδιωτικό νέφος εξυπηρετεί γενικά τους σκοπούς μόνο των οργανισμών. Για συστήματα υψηλής ασφάλειας και κρίσιμα συστήματα, όπως συστήματα αμυντικών

οργανισμών, το ιδιωτικό νέφος είναι η προτεινόμενη προσέγγιση. Ενώ ένα δημόσιο νέφος δεν μπορεί να βρίσκεται φυσικά στη θέση οποιουδήποτε καταναλωτή (φυσικό όριο), τα ιδιωτικά νέφη μπορούν να βρίσκονται είτε εντός των εγκαταστάσεων του οργανισμού του καταναλωτή (on-premises) είτε εκτός (off-premises) σε οποιαδήποτε ουδέτερη τοποθεσία. Τα on-premises ιδιωτικά νέφη διαμένουν φυσικά κάτω από του ίδιου του καταναλωτικού οργανισμού, καθώς και εντός των ορίων του δικτύου. Εκτός εγκαταστάσεων private clouds διαμένουν εκτός των ορίων του δικτύου του οργανισμού, αλλά παραμένουν κάτω από το έλεγχο ή την εποπτεία του οργανισμού-καταναλωτή. Ένα ιδιωτικό νέφος μπορεί να δημιουργηθεί και να διαχειριστεί από τον ίδιο τον οργανισμό-καταναλωτή ή (ο καταναλωτής) μπορεί να αναθέσει την ευθύνη σε κάποιον άλλο προμηθευτή υπολογιστών. Μια σημαντική διαφορά του ιδιωτικού νέφους με το δημόσιο νέφος είναι ότι κάθε ιδιωτικό νέφος μοιράζεται τη σχέση ένα προς ένα με τον καταναλωτή, ενώ το δημόσιο νέφος διατηρεί τη σχέση ένα προς πολλά. Αυτό απεικονίζει ότι οι πόροι ενός ιδιωτικού νέφους παραμένουν αφιερωμένοι για έναν οργανισμό-καταναλωτή μόνο και δεν μπορούν να μοιραστούν με άλλους. Έτσι, τα χαρακτηριστικά της πολλαπλής μίσθωσης (όπου οι μισθωτές είναι εξωτερικές άσχετες οντότητες) δεν ισχύουν στο ιδιωτικό νέφος, όπως συμβαίνει στο δημόσιο νέφος. Όμως, μια τέτοια απομόνωση εξασφαλίζει την ιδιωτικότητα και δημιουργεί ένα πιο ασφαλές υπολογιστικό περιβάλλον. Ωστόσο, αυτό δεν σημαίνει απαραίτητα ότι το δημόσιο νέφος δεν είναι αρκετά ασφαλές. Το άλλο σημείο διαφοροποίησης προκύπτει σχετικά με τη δυνατότητα του καταναλωτή να ελέγχει το νέφος. Οι καταναλωτές δεν έχουν κανέναν έλεγχο σε ένα περιβάλλον δημόσιου νέφους. Αλλά με το ιδιωτικό νέφος, οι καταναλωτές μπορούν να επωφεληθούν από τα περισσότερα, από τα πλεονεκτήματα του υπολογιστικού νέφους και μπορούν ακόμα να κρατήσουν τον έλεγχο του περιβάλλοντος. Για τους καταναλωτές, το κόστος χρήσης του ιδιωτικού νέφους είναι υψηλότερο από το δημόσιο νέφος, καθώς οι πόροι παραμένουν αφιερωμένοι για έναν συγκεκριμένο οργανισμό εδώ.

Υπολογιστικό νέφος κοινότητας (Community cloud): Το μοντέλο ανάπτυξης του κοινοτικού νέφους επιτρέπει την πρόσβαση σε έναν αριθμό οργανισμών ή καταναλωτών που ανήκουν σε μια κοινότητα και το μοντέλο είναι κατασκευασμένο για να εξυπηρετεί κάποια κοινά και συγκεκριμένο σκοπό. Είναι για τη χρήση κάποιας κοινότητας ανθρώπων ή οργανισμών που μοιράζονται κοινά ανησυχίες όσον αφορά τις επιχειρηματικές λειτουργίες, τις απαιτήσεις ασφαλείας κ.λπ. Το μοντέλο αυτό επιτρέπει την κοινή χρήση υποδομών και πόρων μεταξύ πολλαπλών καταναλωτών που ανήκουν

σε μία κοινότητα και έτσι γίνεται φθηνότερο σε σύγκριση με ένα ιδιωτικό νέφος. (Mukundha, C. and Vidyamadhuri, K., 2017) Η ανάπτυξη του κοινοτικού νέφους μπορεί να είναι εντός ή εκτός εγκαταστάσεων. Φυσικά μπορεί να βρίσκεται στις εγκαταστάσεις οποιουδήποτε μέλους της κοινότητας ή μπορεί να βρίσκεται σε κάποια εξωτερική τοποθεσία. Όπως το ιδιωτικό νέφος, αυτό το νέφος μπορεί επίσης να διοικείται από κάποιον ή κάποιους συμμετέχοντες οργανισμούς (της κοινότητας) ή μπορεί να ανατεθεί σε κάποιον εξωτερικό προμηθευτή υπολογιστών. Αυτή η ανάπτυξη νέφους μπορεί να χαρακτηριστεί ως μια γενικευμένη μορφή ιδιωτικού νέφους. Ενώ ένα ιδιωτικό νέφος είναι προσβάσιμο μόνο σε έναν καταναλωτή, ένα κοινοτικό νέφος χρησιμοποιείται από πολλούς καταναλωτές μιας κοινότητας. Έτσι, αυτό το μοντέλο ανάπτυξης υποστηρίζει την πολυμισθικότητα, αν και όχι στο ίδιο βαθμό όπως το δημόσιο νέφος που επιτρέπει πολλαπλούς μισθωτές που δεν σχετίζονται μεταξύ τους. Έτσι, η μίσθωση του κοινοτικού νέφους βρίσκεται μεταξύ του ιδιωτικού και του δημόσιου νέφους. Ο στόχος της ανάπτυξης του κοινοτικού νέφους είναι να παρέχει τα οφέλη του δημόσιου νέφους, όπως η πολλαπλή μίσθωση, η χρέωση ανά χρήση κ.λπ. στους καταναλωτές του, μαζί με πρόσθετο επίπεδο ιδιωτικότητας και ασφάλειας όπως το ιδιωτικό νέφος. Ένα γνωστό παράδειγμα κοινοτικού νέφους είναι ορισμένες υπηρεσίες που δρομολογήθηκαν από την κυβέρνηση μιας χώρας με σκοπό την παροχή υπηρεσιών νέφους σε εθνικές υπηρεσίες. Οι οργανισμοί είναι καταναλωτές σε αυτή την περίπτωση που ανήκουν σε μια ενιαία κοινότητα (η κυβέρνηση).

Υβριδικό υπολογιστικό νέφος (Hybrid cloud): Ένα υβριδικό νέφος δημιουργείται γενικά συνδυάζοντας ιδιωτική ή κοινοτική ανάπτυξη με την ανάπτυξη δημόσιου νέφους μαζί. Αυτό το μοντέλο ανάπτυξης βοηθά τις επιχειρήσεις να επωφεληθούν του ιδιωτικού ή κοινοτικού νέφους αποθηκεύοντας κρίσιμες εφαρμογές και δεδομένα. Την ίδια στιγμή, παρέχει το όφελος κόστους διατηρώντας τα κοινά δεδομένα και τις εφαρμογές στο δημόσιο νέφος. Στην πράξη, το υβριδικό νέφος μπορεί να σχηματιστεί συνδυάζοντας δύο στοιχεία από ένα σύνολο πέντε διαφορετικών αναπτύξεων νέφους, όπως το ιδιωτικό νέφος στις εγκαταστάσεις, το ιδιωτικό νέφος εκτός των εγκαταστάσεων, το κοινοτικό νέφος εντός των εγκαταστάσεων, το κοινοτικό νέφος εκτός των εγκαταστάσεων και το δημόσιο νέφος, όπου μία από τις τέσσερις πρώτες αναπτύξεις συνδυάζεται με την τελευταία (δημόσιο νέφος).

2.1.4 Χαρακτηριστικά υπολογιστικού νέφους

Το μοντέλο υπολογιστικού νέφους του NIST περιλαμβάνει πέντε βασικά χαρακτηριστικά ή απαιτήσεις, τα οποία διαφοροποιούν το μοντέλο νέφους από την παραδοσιακή υπολογιστική προσέγγιση. Αυτά τα χαρακτηριστικά εν συντομία είναι:

On-demand self-service: Είναι το πιο ελκυστικό χαρακτηριστικό που αρέσει στους χρήστες σε αυτό το σύστημα υπολογιστικού μοντέλου. Το χαρακτηριστικό της υπηρεσίας κατά παραγγελία αναφέρεται στη δυνατότητα που δίνει τη δυνατότητα στους χρήστες να καταναλώνουν την υπολογιστική εγκατάσταση όσο χρειάζονται ανά πάσα στιγμή. Όντας αυτοεξυπηρετούμενο, το υπολογιστικό νέφος μπορεί να οργανώσει την κατά παραγγελία διευκόλυνση για τους χρήστες χωρίς να χρειάζεται ανθρώπινη παρέμβαση από την πλευρά του προμηθευτή. Ο ίδιος ο χρήστης μπορεί να ζητήσει υπηρεσίες νέφους όπως χρειάζεται μέσω κάποιας διεπαφής (γενικά μέσω διαδικτυακών φορμών) και οι πόροι καθίστανται διαθέσιμοι εντός δευτερολέπτων. Αυτό το χαρακτηριστικό είναι γνωστό ως αυτοεξυπηρέτηση. Η διεπαφή αυτοεξυπηρέτησης πρέπει να είναι φιλική προς τον χρήστη για να είναι αποτελεσματική και ελκυστική.

Resource pooling: Η πληροφορική απαιτεί πόρους όπως επεξεργαστή, μνήμη, αποθηκευτικό χώρο και δίκτυο. Το υπολογιστικό νέφος οργανώνει αυτούς τους πόρους για τους χρήστες στο από την πλευρα του προμηθευτή. Οι χρήστες μπορούν να έχουν πρόσβαση και να χρησιμοποιούν αυτούς τους πόρους για να ικανοποιήσουν τις υπολογιστικές τους ανάγκες όπως και όταν απαιτείται. Σε αντίθεση με το παραδοσιακή υπολογιστική προσέγγιση όπου κάθε επιχείρηση ή χρήστης διαθέτει τους δικούς του φυσικούς υπολογιστικούς πόρους. Οι δεξαμενές πόρων πρέπει να είναι αρκετά μεγάλες, ευέλικτες και ικανές να υποστηρίζουν πολλούς χρήστες ταυτόχρονα χωρίς καμία αποτυχία.

Broad network access: Το υπολογιστικό νέφος παρέχει οικονομικό πλεονέκτημα στους χρήστες, καθώς απελευθερώνει από την ταλαιπωρία της δημιουργίας ακριβών εσωτερικών κέντρων δεδομένων. Αντίθετα, η υπηρεσία νέφους που αναπτύσσεται και εγκαθίσταται στον πάροχο έχει απομακρυσμένη πρόσβαση από τους χρήστες μέσω του δικτύου. Για να εξυπηρετηθεί αυτός ο σκοπός, πρέπει να υπάρχει ισχυρή υποδομή δικτύου για αβίαστη και γρήγορη παράδοση των υπηρεσιών πληροφορικής. Έτσι, η επικοινωνία υψηλού εύρους ζώνης που κατανέμονται στην περιοχή παροχής υπηρεσιών

είναι τα βασικά χαρακτηριστικά του υπολογιστικού νέφους, ώστε οι χρήστες μπορούν να έχουν πρόσβαση στην πληροφορική από οποιαδήποτε τοποθεσία και ανά πάσα στιγμή.

Rapid elasticity: Παροχή επαρκούς και συχνά μεταβαλλόμενης ζήτησης πόρων για μεγάλο αριθμό χρηστών αποτελεί μείζον τεχνικό πρόβλημα στο υπολογιστικό νέφος. Ο πάροχος δεν γνωρίζει πότε και πόσο θα καταναλώσουν οι χρήστες τους πόρους πριν από την πραγματική ζήτηση. Αλλά ο μηχανισμός θα πρέπει να είναι τέτοιος ώστε ο απαιτούμενος όγκος πόρων να μπορεί να οργανωθεί κατά την στιγμή της ζήτησης από τους χρήστες. Το υπολογιστικό περιβάλλον πρέπει να δημιουργεί την εντύπωση απεριόριστου αποθετηρίου πόρων στους χρήστες, και θα πρέπει να μπορούν να καταναλώνουν οποιονδήποτε όγκο πόρων ανά πάσα στιγμή. Και πάλι, όταν ένας χρήστης δεν χρησιμοποιεί πλέον τους πόρους, αυτοί πρέπει να ληφθούν πίσω αμέσως, ώστε να μην υπάρχει σπατάλη πολύτιμων πόρων μέσω της αδρανούς κατοχής. Από την άποψη των χρηστών, το σύστημα πρέπει να είναι αρκετά ελαστικό. Θα πρέπει να μπορεί να αναπτύσσεται και να συρρικνώνεται ανάλογα με τις απαιτήσεις. Η ταχεία ελαστικότητα αναφέρεται σε αυτή την ικανότητα του νέφους όπου ένα υπολογιστικό σύστημα μπορεί να επεκταθεί ή να μειωθεί γρήγορα σύμφωνα με τους πραγματικούς πόρους απαίτηση κατά την εκτέλεση.

Measured service: Καθώς οι χρήστες χρησιμοποιούν υπηρεσίες υπολογιστών που παρέχονται από τον προμηθευτή νέφους, πρέπει να πληρώνουν γι' αυτό. Στο μοντέλο υπολογιστικού νέφους, η πληρωμή αυτή καθορίζεται με τη μέτρηση των χρήσεων των υπολογιστικών πόρων από έναν χρήστη. Ως εκ τούτου, ο πάροχος πρέπει να χρησιμοποιεί κάποιο μηχανισμό για τη μέτρηση την πραγματική κατανάλωση από κάθε μεμονωμένο χρήστη ή οργανισμό. Αυτό σημαίνει ότι η χρήση των συγκεντρωμένων πόρων πρέπει να υπολογίζεται και να δηλώνεται (ή να χρεώνεται) σε κάθε χρήστη με βάση ένα σύστημα μέτρησης. Γενικά αυτό γίνεται με βάση κάποια γνωστή μετρική, όπως η ποσότητα της επεξεργαστικής ισχύος που καταναλώνεται, η χρήση του όγκου αποθήκευσης, το εύρος ζώνης δικτύου που χρησιμοποιείται, ο αριθμός των δικτυακών συναλλαγών κ.λπ. Κάθε χρήστης τιμολογείται μόνο με βάση την πραγματική κατανάλωση των πόρων του νέφους ή για τους πόρους που του/της έχουν παραχωρηθεί.

2.2 Απειλές ασφάλειας, κίνδυνοι και τρωτά σημεία

Εισαγωγη

Δεν υπάρχει αμφιβολία ότι η ευκολία και το χαμηλό κόστος των υπηρεσιών υπολογιστικού νέφους έχουν αλλάξει την καθημερινότητά μας, ωστόσο, τα ζητήματα ασφάλειας που σχετίζονται με το υπολογιστικό νέφος μας κάνουν να ευάλωτους σε εγκλήματα στον κυβερνοχώρο που συμβαίνουν καθημερινά. Οι χάκερς χρησιμοποιούν διάφορες τεχνικές για να αποκτήσουν πρόσβαση σε νέφη χωρίς νόμιμη άδεια ή να διαταράξουν τις υπηρεσίες στα νέφη προκειμένου να επιτύχουν συγκεκριμένους στόχους. Οι χάκερς θα μπορούσαν να ξεγελάσουν ένα νέφος ώστε να αντιμετωπίσουν την παράνομη δραστηριότητά τους ως έγκυρη περίπτωση, επομένως, αποκτώντας μη εξουσιοδοτημένη πρόσβαση στις πληροφορίες που είναι αποθηκευμένες στο νέφος.

Μόλις εντοπιστεί η ακριβής τοποθεσία των δεδομένων, οι χάκερς κλέβουν ιδιωτικές και ευαίσθητες πληροφορίες για εγκληματικές δραστηριότητες. Σύμφωνα με την DataLossDB, υπήρξαν 1.047 περιστατικά παραβίασης δεδομένων τους πρώτους εννέα μήνες του 2012, σε σύγκριση με 1.041 περιστατικά κατά τη διάρκεια ολόκληρου του 2011 (DataLossDB Open Security Foundation, 2015).

Η Epsilon και η Stratfor ήταν δύο θύματα παραβίασης δεδομένων. Στο ατύχημα διαρροής δεδομένων, η Epsilon διέρρευσε εκατομμύρια ονόματα και διευθύνσεις ηλεκτρονικού ταχυδρομείου από τις βάσεις δεδομένων των πελατών της. Στην Stratfor 75.000 αριθμοί καρτών και 860.000 ονόματα χρηστών και κωδικοί πρόσβασης εκλάπησαν (Sophos Security Threat Report , 2012). Οι χάκερ θα μπορούσαν επίσης να επωφεληθούν από τη μαζική υπολογιστική ισχύ των υπολογιστικών νεφών για να εξαπολύσουν επιθέσεις σε χρήστες που βρίσκονται στα ίδια ή διαφορετικά δίκτυα. Για παράδειγμα, οι χάκερ νοίκιασαν έναν διακομιστή μέσω της υπηρεσίας EC2 της Amazon και πραγματοποίησαν επίθεση στο δίκτυο PlayStation της Sony (Amazon.com Server Said to Have Been Used in Sony Attack, 2011). Ως εκ τούτου, η καλή κατανόηση των απειλών ασφαλείας του νέφους είναι απαραίτητη προκειμένου να παρέχονται ασφαλέστερες υπηρεσίες στους χρήστες του νέφους.

Τα τρία μοντέλα υπηρεσιών νέφους (SaaS, PaaS και IaaS) όχι μόνο παρέχουν διαφορετικούς τύπους υπηρεσιών σε χρήστες, αλλά και αποκαλύπτουν θέματα ασφάλειας πληροφοριών και κινδύνους των συστημάτων υπολογιστικού νέφους.

Πρώτον, οι χάκερ ενδέχεται να κάνουν κατάχρηση της δυναμικής υπολογιστικής ικανότητας που παρέχουν τα νέφη, διεξάγοντας παράνομες δραστηριότητες. Το IaaS βρίσκεται στο κατώτατο στρώμα, το οποίο παρέχει άμεσα τις ισχυρότερη λειτουργικότητα ολόκληρου του νέφους. Μεγιστοποιεί την επεκτασιμότητα για τους χρήστες ώστε να προσαρμόζουν ένα "ρεαλιστικό" περιβάλλον που περιλαμβάνει εικονικές μηχανές που λειτουργούν με διαφορετικά λειτουργικά συστήματα. Οι χάκερς θα μπορούσαν να νοικιάσουν τις εικονικές μηχανές, να αναλύσουν τις διαμορφώσεις τους, να βρουν τις τρωτά σημεία και να επιτεθούν στις εικονικές μηχανές άλλων πελατών εντός του ίδιου νέφους. (Anita, 2017) Το IaaS επίσης επιτρέπει στους χάκερς να εκτελούν επιθέσεις, π.χ. brute-forcing cracking, που χρειάζονται υψηλή υπολογιστική ισχύ. Δεδομένου ότι το IaaS υποστηρίζει πολλαπλές εικονικές μηχανές, παρέχει μια ιδανική πλατφόρμα για τους χάκερς να εξαπολύσουν επιθέσεις (π.χ. κατανεμημένες επιθέσεις άρνησης παροχής υπηρεσιών (DDoS)) που απαιτούν μεγάλο αριθμό επιθέσεων.

Δεύτερον, η απώλεια δεδομένων είναι ένας σημαντικός κίνδυνος ασφάλειας των μοντέλων νέφους. Στα μοντέλα νέφους SaaS, οι εταιρείες χρησιμοποιούν εφαρμογές για την επεξεργασία επιχειρηματικών δεδομένων και αποθηκεύουν τα δεδομένα των πελατών στα κέντρα δεδομένων. (Anita, 2017) Στα μοντέλα νέφους PaaS, οι προγραμματιστές χρησιμοποιούν δεδομένα για να ελέγχουν την ακεραιότητα του λογισμικού κατά τη διάρκεια του συστήματος κύκλου ζωής της ανάπτυξης (SDLC). Στα μοντέλα νέφους IaaS, οι χρήστες δημιουργούν νέες μονάδες σε εικονικά μηχανές και αποθηκεύουν δεδομένα σε αυτούς τους δίσκους. Ωστόσο, τα δεδομένα και στα τρία μοντέλα cloud μπορεί να υπάρχει πρόσβαση σε αυτά από μη εξουσιοδοτημένους εσωτερικούς υπαλλήλους, καθώς και από εξωτερικούς χάκερ. Οι εσωτερικοί υπάλληλοι είναι σε θέση να αποκτήσουν πρόσβαση στα δεδομένα σκόπιμα ή κατά λάθος. Οι εξωτερικοί χάκερ αποκτούν πρόσβαση σε βάσεις δεδομένων σε περιβάλλοντα νέφους χρησιμοποιώντας μια σειρά από τεχνικές παραβίασης, όπως η σύνοδος και υποκλοπή καναλιών δικτύου. (Alhenaki, 2019)

Τρίτον, οι παραδοσιακές στρατηγικές επίθεσης στο δίκτυο μπορούν να εφαρμοστούν για να παρενοχλήσουν τρία στρώματα του νέφους συστημάτων. Για παράδειγμα, οι επιθέσεις στο πρόγραμμα περιήγησης ιστού χρησιμοποιούνται για την εκμετάλλευση του ελέγχου ταυτότητας, της εξουσιοδότησης, και λογιστικές ευπάθειες των συστημάτων νέφους. Κακόβουλα προγράμματα (π.χ. ιός και Trojan) μπορούν να να μεταφορτωθούν σε συστήματα νέφους και να προκαλέσουν ζημιά (Zaki, 2011). Κακόβουλες λειτουργίες (π.χ. metadata spoofing attacks) μπορούν να ενσωματωθούν σε μια κανονική εντολή, να μεταβιβαστούν στα νέφη και να εκτελεστούν ως έγκυρες περιπτώσεις (K. Zunnurhain and S. Vrbsky, 2010). Στο IaaS, o hypervisor (π.χ. VMware vSphere και Xen) που διεξάγει διαχειριστικές λειτουργίες των εικονικών στιγμιοτύπων μπορεί να παραβιαστεί από επίθεση μηδενικής ημέρας (W. A. Jansen, 2011).

Είναι απαραίτητο να εντοπιστούν οι πιθανές απειλές του νέφους, προκειμένου να εφαρμοστεί καλύτερη ασφάλεια. μηχανισμών για την προστασία των περιβάλλοντος υπολογιστικού νέφους. Στη συνέχεια, θα αναλύσουμε τις απειλές ασφάλειας που παρουσιάζονται στα νέφη από τρεις οπτικές γωνίες: καταχρηστική χρήση υπολογιστικών πόρων του νέφους , παραβιάσεις δεδομένων και επιθέσεις ασφάλειας νέφους. Πρόσφατες πραγματικές συνθήκες επιθέσεων στο νέφος συμπεριλήφθηκαν για να καταδείξουν τις τεχνικές που χρησιμοποιούν οι χάκερς για την εκμετάλλευση των τρωτών σημείων των συστημάτων νέφους.

2.2.1 Καταχρηστική χρήση υπολογιστικών πόρων Cloud:

Στο παρελθόν, οι χάκερς χρησιμοποιούσαν πολλούς υπολογιστές ή ένα botnet για να παράγουν ένα μεγάλο ποσό υπολογιστικής ισχύος προκειμένου να πραγματοποιήσουν κυβερνοεπιθέσεις σε συστήματα υπολογιστών. Αυτή η διαδικασία είναι περίπλοκη και μπορεί να διαρκέσει μήνες για να ολοκληρωθεί. Σήμερα, μια ισχυρή υπολογιστική υποδομή, που περιλαμβάνει τόσο συστατικά λογισμικού και υλικού, θα μπορούσε εύκολα να δημιουργηθεί χρησιμοποιώντας μια απλή διαδικασία εγγραφής σε έναν πάροχο υπηρεσιών υπολογιστικού νέφους. (Masood, 2020) Εκμεταλλευόμενοι την ισχύουσα υπολογιστική ισχύ των δικτύων νέφους, οι χάκερ μπορούν να εξαπολύσουν επιθέσεις σε πολύ σύντομο χρονικό διάστημα. Για παράδειγμα, brute force attack και επιθέσεις DoS μπορούν να εξαπολυθούν κάνοντας κατάχρηση της ισχύος του υπολογιστικού νέφους.

Η brute force attack είναι μια τεχνική που χρησιμοποιείται για την παραβίαση κωδικών πρόσβασης. Η επιτυχία αυτής της επίθεσης σε μεγάλο βαθμό εξαρτάται από τις ισχυρές υπολογιστικές δυνατότητες, επειδή απαιτούνται χιλιάδες πιθανοί κωδικοί πρόσβασης για να αποσταλούν στο λογαριασμό ενός χρήστη-στόχου μέχρι να βρεθεί ο σωστός για πρόσβαση. Του υπολογιστικό νέφος παρέχει μια τέλεια πλατφόρμα για τους χάκερς ώστε να εξαπολύσουν αυτού του είδους την επίθεση. Ο Thomas Roth, ένας Γερμανός ερευνητής, παρουσίασε μια επίθεση ωμής βίας στο Black Hat Technical SecurityConference (T. Roth, 2011). Κατάφερε να σπάσει ένα δίκτυο που προστατεύεται με WPA-PSK νοικιάζοντας έναν διακομιστή από τον EC2 της Amazon. Σε περίπου 20 λεπτά, ο Roth έριξε 400.000 κωδικούς πρόσβασης ανά δευτερόλεπτο στο σύστημα και το κόστος χρήσης της υπηρεσίας EC2 ήταν μόλις 28 λεπτά ανά λεπτό.

Οι επιθέσεις DoS επιχειρούν να διαταράξουν έναν κεντρικό υπολογιστή ή έναν πόρο δικτύου προκειμένου να κάνουν τους νόμιμους χρήστες να μην μπορούν να έχουν πρόσβαση στην υπηρεσία υπολογιστή. Παρουσιάζονται σε διάφορες μορφές και στοχεύουν σε διάφορες υπηρεσίες. Γενικά, κατηγοριοποιούνται σε τρεις βασικούς τύπους: κατανάλωση σπάνιων, περιορισμένων ή μη ανανεώσιμων πόρων, καταστροφή ή αλλοίωση των στοιχείων του δικτύου (CERT Coordination Center, Denial of Service, 2023). Μεταξύ αυτών, η πλημμύρα είναι η πιο συνηθισμένος τρόπος με τον οποίο οι χάκερς καταρρακώνουν το σύστημα του θύματος με τη χρήση ενός συντριπτικού αριθμού ψεύτικων αιτημάτων- ως εκ τούτου, οι υπηρεσίες προς τους νόμιμους χρήστες μπλοκάρονται. Όταν η επίθεση πλημμύρας εφαρμόζεται σε υπηρεσίες νέφους, δύο τύποι DoS θα μπορούσαν να συμβούν σε συστήματα υπολογιστικού νέφους: άμεσο DoS και έμμεσο DoS (M. Jensen, J. Schwenk, N. Gruschka, and L. L. Iacono, 2009). Όταν ένας διακομιστής νέφους λαμβάνει μεγάλο όγκο πλημμυρισμένων αιτημάτων, τότε θα παρέχει περισσότερους υπολογιστικούς πόρους για να αντιμετωπίσει τα κακόβουλα αιτήματα. Τέλος, ο διακομιστής εξαντλεί την πλήρη ικανότητά του και εμφανίζεται ένα άμεσο DoS σε όλα τα αιτήματα από νόμιμους χρήστες. Επιπλέον, η επίθεση πλημμύρας θα μπορούσε ενδεχομένως να προκαλέσει έμμεσο DoS σε άλλους διακομιστές στο ίδιο νέφος, όταν οι διακομιστές μοιράζονται το φόρτο εργασίας του διακομιστή-θύματος, με αποτέλεσμα την πλήρη έλλειψη διαθεσιμότητας σε όλες τις υπηρεσίες.

Οι υπηρεσίες υπολογιστικού νέφους μπορούν να χρησιμοποιηθούν για την αποστολή μεγάλου όγκου πακέτων στα δίκτυα των εταιρειών. Για παράδειγμα, δύο σύμβουλοι ασφαλείας, ο Bryan και ο Anderson, ξεκίνησαν cloud-based επιθέσεις DoS σε έναν από

τους πελάτες τους, προκειμένου να ελέγξουν τη συνδεσιμότητά του με τη βοήθεια της υπηρεσίας της Amazon EC2 της Amazon (Thunder in the Cloud: $6 Cloud-Based Denial-of-Service Attack, 2010). Ξοδεύοντας μόνο 6 δολάρια για να νοικιάσουν εικονικούς διακομιστές στο EC2, χρησιμοποίησαν ένα αυτοσχέδιο πρόγραμμα "Thunder Clap" για να κατακλύσουν με επιτυχία τον διακομιστή του πελάτη τους και να κάνουν την εταιρεία μη διαθέσιμη στο διαδίκτυο. Ένα άλλο παράδειγμα επίθεσης DoS συζητήθηκε απο έναν δανέζικο προγραμματιστή, Jesper Nøhr (DDoS Attack Rains Down on Amazon Cloud, 2009). Σύμφωνα με την αναφορά του, το Bitbucket, μια διαδικτυακή υπηρεσία φιλοξενίας εταιρεία παροχής υπηρεσιών που φιλοξενείται από την Amazon, δέχθηκε επίθεση από μαζικής κλίμακας επιθέσεις DDoS που χρησιμοποιήθηκαν από δύο τεχνικές πλημμύρας: μια πλημμύρα πακέτων UDP και μια πλημμύρα αιτήσεων σύνδεσης TCP SYN. Οι επιθέσεις προκάλεσαν τη μη διαθεσιμότητα της εταιρείας και, ως εκ τούτου, πολλοί προγραμματιστές έχασαν την πρόσβαση στην έργα που φιλοξενούνται στο Bitbucket.

2.2.2 Παραβίαση δεδομένων

Κακόβουλος εισβολέας

Οι απειλές για την ασφάλεια μπορεί να προέρχονται τόσο από το εξωτερικό όσο και από το εσωτερικό των οργανισμών. Σύμφωνα με την έκθεση του 2011 CyberSecurity Watch Survey που διεξήχθη σε 607 επιχειρήσεις, κυβερνητικά στελέχη, επαγγελματίες και συμβούλους, το 21% των επιθέσεων στον κυβερνοχώρο προκλήθηκαν από εσωτερικούς χρήστες. Το 33% των ερωτηθέντων πίστευαν ότι οι επιθέσεις εκ των έσω ήταν πιο δαπανηρές και επιζήμιες για τους οργανισμούς (CERT Coordination Center at Carnegie Mellon University., 2011). Οι πιο συνηθισμένες επιθέσεις εκ των έσω ήταν η μη εξουσιοδοτημένη πρόσβαση και χρήση εταιρικών πληροφοριών (63%), η ακούσια έκθεση ιδιωτικών ή ευαίσθητων δεδομένων (57%), ο ιός, κακόβουλοι κώδικες (37%) και κλοπή πνευματικής ιδιοκτησίας (32%). Τα τρωτά σημεία του cloud computing σε κακόβουλους εσωτερικούς χρήστες είναι: ασαφείς ρόλοι και ευθύνες, μη εφαρμογή της αρχής της ανάγκης γνώσης, ευπάθειες AAA, ευπαθή λειτουργικά συστήματα, ανεπαρκείς διαδικασίες φυσικής ασφάλειας, αδυναμία επεξεργασίας δεδομένων

κρυπτογραφημένης μορφής, ευπάθειες εφαρμογών ή ανεπαρκής διαχείριση επιδιορθώσεων (Hogben, 2016).

Ενώ η μετακίνηση δεδομένων και εφαρμογών σε περιβάλλοντα υπολογιστικού νέφους μπορεί να επεκτείνει τις επιχειρήσεις, η κακόβουλη δολιοφθορά των ευαίσθητων πληροφοριακών πόρων ενός οργανισμού θα μπορούσε να θέσει σε κίνδυνο την ολόκληρη τη λειτουργία του οργανισμού-θύματος. Υπάρχουν τρεις τύποι εσωτερικών απειλών που σχετίζονται με το νέφος: οι αθέμιτος διαχειριστής, οι εσωτερικοί χρήστες που εκμεταλλεύονται τα τρωτά σημεία του cloud και οι εσωτερικοί χρήστες που χρησιμοποιούν το νέφος για τη διεξαγωγή κακόβουλης δραστηριότητας (CERT, 2012). Ο απατεώνας διαχειριστής έχει το προνόμιο να κλέβει μη προστατευμένα αρχεία, με επίθεση brute-force σε κωδικούς πρόσβασης και να κατεβάζει δεδομένα πελατών από το θύμα οργανισμό. Οι εσωτερικοί χρήστες που εκμεταλλεύονται τις ευπάθειες του cloud προσπαθούν να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση σε εμπιστευτικά δεδομένα σε έναν οργανισμό- θα μπορούσαν να βγάλουν μια περιουσία πουλώντας τις ευαίσθητες πληροφορίες, ή να χρησιμοποιήσουν τις πληροφορίες για τις μελλοντικές τους επιχειρήσεις. Οι εσωτερικοί χρήστες που χρησιμοποιούν το νέφος για να διεξάγουν κακόβουλη δραστηριότητα πραγματοποιούν επιθέσεις κατά της υποδομής ΤΠ του δικού τους εργοδότη. Δεδομένου ότι οι insiders είναι εξοικειωμένοι με τις λειτουργίες ΤΠ των δικών τους εταιρειών, οι επιθέσεις είναι γενικά δύσκολο να εντοπιστούν με τη χρήση εγκληματολογικής ανάλυσης.

Ηλεκτρονική κλοπή στον κυβερνοχώρο

Οι υπηρεσίες υπολογιστικού νέφους παρέχουν στους χρήστες ισχυρές δυνατότητες επεξεργασίας και μαζικές ποσότητες αποθηκευτικού χώρου. Με το ανέξοδο κόστος τους, οι εταιρείες θα μπορούσαν να μεταφέρουν την επιχείρησή τους σε νέφη, ώστε να μην χρειάζεται να αγοράζουν δικούς τους διακομιστές για να αποθηκεύουν τις πληροφορίες των πελατών και να διαχειρίζονται την κίνηση από τους πελάτες και τους επισκέπτες. Για παράδειγμα, το Netflix μισθώνει υπολογιστικό χώρο από Amazon Web Services (AWS) για να παρέχει συνδρομητική υπηρεσία για την παρακολούθηση τηλεοπτικών επεισοδίων και ταινιών. Το Dropbox προσφέρει στους πελάτες της υπηρεσία αποθήκευσης στο νέφος για την αποθήκευση δεδομένων terabytes. Οι υπηρεσίες cloudbased γίνονται πλέον μέρος της καθημερινότητάς μας. Εν τω μεταξύ, τα ευαίσθητα

δεδομένα που είναι αποθηκευμένα σε υπολογιστικά νέφη γίνονται ελκυστικός στόχος για διαδικτυακές κλοπές στον κυβερνοχώρο. Σύμφωνα με την ανάλυση της παραβιάσεων δεδομένων 209 παγκόσμιων εταιρειών το 2011, το 37% των περιπτώσεων παραβίασης δεδομένων αφορούσε κακόβουλες επιθέσεις. Το μέσο κόστος ανά παραβιασμένο αρχείο ανέρχεται σε 222 δολάρια (Symantec, 2012). Ο διαδικτυακός λιανοπωλητής Zappos (που ανήκει στον πάροχο cloud Amazon) έπεσε θύμα διαδικτυακής κλοπής στον κυβερνοχώρο (2012 Has Delivered Her First Giant Data Breach, January, 2012). Σχεδόν 24 εκατομμύρια λογαριασμοί πελατών ενδέχεται να έχουν παραβιαστεί κατά την παραβίαση. Οι εκτεθειμένες πληροφορίες περιλαμβάνουν ονόματα, διευθύνσεις ηλεκτρονικού ταχυδρομείου, διευθύνσεις χρέωσης και αποστολής, αριθμούς τηλεφώνου, τα τέσσερα τελευταία ψηφία των αριθμών πιστωτικών καρτών, καθώς και κρυπτογραφημένες εκδόσεις των κωδικών πρόσβασης των λογαριασμών.

Η κλοπή δεδομένων που είναι αποθηκευμένη, σε νέφη θα μπορούσε να συμβεί στους ιστότοπους κοινωνικής δικτύωσης. Κοινωνική δικτύωση όπως το Twitter, το MySpace και το Facebook, έχουν προσελκύσει ανθρώπους που τους χρησιμοποιούν για να αλληλεπιδρούν με τους φίλους τους στην καθημερινή τους ζωή. Η USA Today διαπίστωσε ότι το 35 τοις εκατό των ενηλίκων χρηστών του Διαδικτύου έχουν ένα προφίλ σε τουλάχιστον έναν ιστότοπο κοινωνικής δικτύωσης (A Few Wrinkles Are Etching Facebook, Other Social Sites, USA Today, 2011). Αυτά τα δίκτυα παρέχουν μια πλατφόρμα για τους χρήστες να μοιράζονται πληροφορίες με άλλους, π.χ. προσωπικό προφίλ (φύλο, ημερομηνία γέννησης, ηλεκτρονικό ταχυδρομείο, τηλέφωνο και εκπαίδευση) και ψηφιακά μέσα (μουσική, φωτογραφίες και βίντεο). Ωστόσο, αυτά τα προσωπικά δεδομένα μπορούν ενδεχομένως να παραβιαστούν από διαδικτυακούς κλέφτες στον κυβερνοχώρο, αν βρουν τρόπο να αποκτήσουν πρόσβαση στα σύννεφα. Για παράδειγμα, Το LinkedIn, ο μεγαλύτερος δικτυακός τόπος επαγγελματικής δικτύωσης στον κόσμο που διαθέτει 175 εκατομμύρια χρήστες, ανέφερε ότι η βάση δεδομένων των κωδικών πρόσβασης παραβιάστηκε (LinkedIn Blog, 2012). Περίπου 6,5 εκατομμύρια κατακερματισμένοι κωδικοί πρόσβασης εκλάπησαν και δημοσιεύτηκαν σε ένα ρωσικό διαδικτυακό φόρουμ. Περισσότεροι από 200.000 από αυτούς τους κωδικούς πρόσβασης έχουν σπάσει.

Οι διαδικτυακοί κλέφτες θα μπορούσαν να χρησιμοποιήσουν τους κλεμμένους κωδικούς πρόσβασης για να αποκτήσουν πρόσβαση στους λογαριασμούς των χρηστών, καθώς και για να εξαπολύουν κακόβουλες επιθέσεις στους χρήστες. Η Dropbox επιβεβαίωσε ότι οι χρήστες της υπέστησαν spam επίθεση (Dropbox, 2012). Τα ονόματα χρηστών και οι κωδικοί πρόσβασης που είχαν κλαπεί από άλλους ιστότοπους χρησιμοποιήθηκαν για να συνδεθούν στους χρήστες του Dropbox. Επιπλέον, ένας κλεμμένος κωδικός πρόσβασης χρησιμοποιήθηκε για την πρόσβαση σε ένα Dropbox υπαλλήλου που περιείχε ένα έγγραφο έργου με διευθύνσεις ηλεκτρονικού ταχυδρομείου χρηστών. Στη συνέχεια, ο χάκερ έστειλε μηνύματα spam σχετικά με διαδικτυακά καζίνο και ιστότοπους τυχερών παιχνιδιών σε άλλους χρήστες

Οι διαδικτυακοί κλέφτες στον κυβερνοχώρο θα μπορούσαν επίσης να επωφεληθούν από την υπολογιστική ισχύ που προσφέρει το νέφος, παρόχους υπηρεσιών υπολογιστών για να εξαπολύσουν επιθέσεις. Η υπηρεσία υπολογιστικού νέφους EC2 της Amazon χρησιμοποιήθηκε από χάκερς για να παραβιάσουν ιδιωτικές πληροφορίες. Με την εγγραφή στην υπηρεσία EC2 της Amazon με ψεύτικε ςπληροφορίες, οι χάκερ νοίκιασαν έναν εικονικό διακομιστή και εξαπέλυσαν επίθεση για να κλέψουν τα δεδομένα των πελατών από PlayStation Network της Sony (Amazon.com Server Said to Have Been Used in Sony Attack, 2011). Οι χάκερς δεν διέρρηξαν τους διακομιστές της Amazon κατά τη διάρκεια του περιστατικού, ωστόσο οι προσωπικοί λογαριασμοί περισσότερων από 100 εκατομμυρίων χρηστών του Sony PlayStation Network συνδρομητών παραβιάστηκαν.

2.2.3 Επιθέσεις ασφάλειας cloud

Επίθεση εισβολής κακόβουλου λογισμικού

Οι εφαρμογές που βασίζονται στον ιστό παρέχουν δυναμικές ιστοσελίδες για την πρόσβαση των χρηστών του Διαδικτύου στην εφαρμογή διακομιστές μέσω ενός προγράμματος περιήγησης στο διαδίκτυο. Οι εφαρμογές μπορεί να είναι τόσο απλές όσο ένα σύστημα ηλεκτρονικού ταχυδρομείου ή τόσο πολύπλοκες όπως ένα ηλεκτρονικό τραπεζικό σύστημα. Μελέτη έχει δείξει ότι οι διακομιστές είναι ευάλωτοι σε επιθέσεις μέσω διαδικτύου (Symantec White Paper, 2011). Σύμφωνα με μια έκθεση της Symantec, ο αριθμός των επιθέσεων μέσω διαδικτύου το 2011 αυξήθηκε κατά 36% με πάνω από 4.500 νέες επιθέσεις κάθε μέρα (Symantec Internet Security Threat Report, 2011). Οι επιθέσεις περιελάμβαναν cross site scripting, ελαττώματα έγχυσης, διαρροή πληροφοριών και ακατάλληλο χειρισμό σφαλμάτων, σπασμένη αυθεντικοποίηση και διαχείριση συνόδου, αποτυχία περιορισμού της πρόσβασης σε διεύθυνση URL, ακατάλληλη επικύρωση δεδομένων, μη ασφαλείς επικοινωνίες και κακόβουλη εκτέλεση αρχείων (Mudholkar, 2012). Η επίθεση έγχυσης κακόβουλου λογισμικού είναι μια κατηγορία επιθέσεων που βασίζονται στον ιστό, κατά την οποία οι χάκερ εκμεταλλεύονται ευπάθειες μιας εφαρμογής ιστού και ενσωματώνουν κακόβουλους κώδικες σε αυτήν που αλλάζουν την πορεία της κανονικής εκτέλεσή της. Όπως και οι διαδικτυακές εφαρμογές, τα συστήματα νέφους είναι επίσης ευάλωτα σε επιθέσεις εισβολής κακόβουλου λογισμικού. Οι χάκερς δημιουργούν μια κακόβουλη εφαρμογή, ένα κακόβουλο πρόγραμμα και μια εικονική μηχανή και τα εγχέουν στα μοντέλα υπηρεσιών νέφους-στόχου SaaS, PaaS και IaaS, αντίστοιχα. Μόλις η εισβολή ολοκληρωθεί, η κακόβουλη μονάδα εκτελείται ως μία από τις έγκυρες περιπτώσεις που εκτελούνται, στη συνέχεια, ο χάκερ μπορεί να κάνει ό,τι επιθυμεί, όπως υποκλοπές, χειραγώγηση δεδομένων και κλοπή δεδομένων. Μεταξύ όλων των επιθέσεων έγχυσης κακόβουλου λογισμικού, η επίθεση έγχυσης SQL και η επίθεση cross-site scripting είναι οι δύο πιο συνηθισμένες μορφές (Dhore, 2012). Η επίθεση έγχυσης SQL αυξήθηκε κατά 69% το δεύτερο τρίμηνο του 2012 σε σύγκριση με το πρώτο τρίμηνο, σύμφωνα με έκθεση του παρόχου ασφαλούς cloud host FireHost (Web Application Attack Report For The Second Quarter of 2012, 2012). Η FireHost δήλωσε ότι μεταξύ Απριλίου και Ιουνίου, μπλόκαρε σχεδόν μισό εκατομμύριο επιθέσεις SQLi.

Οι παρεμβάσεις SQL στοχεύουν σε SQL διακομιστές που εκτελούν ευάλωτες εφαρμογές βάσεων δεδομένων. Οι χάκερ εκμεταλλεύονται τις ευπάθειες των διακομιστών ιστού και εισάγουν έναν κακόβουλο κώδικα προκειμένου να παρακάμψουν τη σύνδεση και να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση σε backend βάσεις δεδομένων. Εάν επιτύχουν, οι χάκερ μπορούν να χειραγωγήσουν τα περιεχόμενα των των βάσεων δεδομένων, να ανακτήσουν εμπιστευτικά δεδομένα, να εκτελέσουν εξ αποστάσεως εντολές του συστήματος ή ακόμη και να πάρουν τον έλεγχο του διακομιστή ιστού για περαιτέρω εγκληματικές δραστηριότητες. Το PlayStation της Sony έπεσε θύμα επίθεσης SQL injection. Το blog της SophosLabs ανέφερε ότι μια επίθεση SQL injection χρησιμοποιήθηκε με επιτυχία για την τοποθέτηση μη εξουσιοδοτημένου κώδικα σε 209 σελίδες που προωθούν τα παιχνίδια του PlayStation,

"SingStar Pop" και "God of War" (Infection, 2008). Οι επιθέσεις SQL injection μπορούν να εξαπολυθούν από ένα botnet. Το Asprox botnet χρησιμοποίησε χίλια bots που ήταν εξοπλισμένα με ένα SQL injection kit για να εκτοξεύσουν μια SQL injection (N. Provos, 2018). Τα bots έστειλαν πρώτα κωδικοποιημένα ερωτήματα SQL που περιείχαν το ωφέλιμο φορτίο εκμετάλλευσης σε Google για την αναζήτηση διακομιστών ιστού που εκτελούν ASP.net. Στη συνέχεια, τα bots ξεκίνησαν μια SQL injection επίθεση κατά των δικτυακών τόπων που επέστρεφαν τα ερωτήματα αυτά. Συνολικά, περίπου 6 εκατομμύρια διευθύνσεις URL που ανήκαν σε 153.000 διαφορετικές τοποθεσίες web ήταν θύματα επίθεσης SQL injection από το Asprox botnet. Μια διαδικτυακή εφαρμογή SaaS λιανικής πώλησης που επιτρέπει σε πολλούς λιανοπωλητές να φιλοξενούν τα προϊόντα τους και να τα πωλούν μέσω SaaS. Η διαδικασία εκμετάλλευσης της ευπάθειας και της πρόσβασης σε backend βάση δεδομένων εξηγήθηκε λεπτομερώς. Οι επιθέσεις cross-site scripting (XSS) θεωρούνται μία από τις πιο κακόβουλες και επικίνδυνες τύποι επιθέσεων από την FireHost. Το 27% των επιθέσεων ιστού, επιθέσεις cross-site scripting, πραγματοποιήθηκαν με επιτυχία εμποδίστηκαν επιτυχώς από το να προκαλέσουν ζημιά στις διαδικτυακές εφαρμογές και τις βάσεις δεδομένων των πελατών της FireHost κατά τη διάρκεια του 2ου τριμήνου του 2012. (Web Application Attack Report For The Second Quarter of 2012, 2012) Οι χάκερς εισάγουν κακόβουλα σενάρια, όπως JavaScript, VBScript, ActiveX, HTML και Flash, σε μια ευάλωτη δυναμική ιστοσελίδα για να εκτελέσουν τα σενάρια στο πρόγραμμα περιήγησης ιστού του θύματος. Στη συνέχεια η επίθεση θα μπορούσε να πραγματοποιήσει παράνομες δραστηριότητες (π.χ. να εκτελέσει κακόβουλο κώδικα στο μηχανή του θύματος και να κλέψει το cookie συνεδρίας που χρησιμοποιείται για εξουσιοδότηση) για πρόσβαση στο

λογαριασμό του θύματος ή να εξαπατήσει το θύμα κάνοντας κλικ σε έναν κακόβουλο σύνδεσμο. Ερευνητές στη Γερμανία έχουν δημιουργήσει με επιτυχία μια επίθεση XSS κατά της πλατφόρμας υπολογιστικού νέφους Amazon AWS. Η ευπάθεια στο κατάστημα της Amazon επέτρεψε στην ομάδα να καταλάβει μια σύνοδο AWS και να αποκτήσει πρόσβαση σε όλα τα δεδομένα των πελατών. Τα δεδομένα περιλαμβάνουν δεδομένα ελέγχου ταυτότητας, tokens, ακόμη και κωδικούς πρόσβασης απλού κειμένου.

Wrapping Επίθεση

Όταν ένας πελάτης ζητά υπηρεσίες σε έναν διακομιστή ιστού μέσω ενός προγράμματος περιήγησης ιστού, η υπηρεσία αλληλεπιδρά με τη χρήση μηνυμάτων SOAP (Simple Object Access Protocol) που μεταδίδονται μέσω HTTP πρωτόκολλο με μορφή XML (Extensible Markup Language). Προκειμένου να διασφαλιστεί η εμπιστευτικότητα και η ακεραιότητα των δεδομένων των μηνυμάτων SOAP κατά τη διαμετακόμιση μεταξύ πελατών και διακομιστών, ένα σύστημα ασφαλείας μηχανισμός, WS-Security (Web Services Security), για υπηρεσίες ιστού. (Modak, 2021) Χρησιμοποιεί ψηφιακή υπογραφή για την υπογραφή του μηνύματος και τεχνική κρυπτογράφησης για την κρυπτογράφηση του περιεχομένου του μηνύματος. Με τον τρόπο αυτό ο πελάτης πιστοποιείται και ο διακομιστής μπορεί να επικυρώσει ότι το μήνυμα δεν έχει αλλοιωθεί κατά τη διάρκεια της μετάδοσης.

Οι επιθέσεις περιτύλιξης χρησιμοποιούν την περιτύλιξη υπογραφής XML (ή την επανεγγραφή XML) για να εκμεταλλευτούν μια αδυναμία όταν διακομιστές ιστού επικυρώνουν υπογεγραμμένες αιτήσεις (Yang, 2020). Η επίθεση γίνεται κατά τη διάρκεια της μετάφρασης του SOAP μηνυμάτων μεταξύ ενός νόμιμου χρήστη και του διακομιστή ιστού. Με την αντιγραφή του λογαριασμού του χρήστη και των κωδικό πρόσβασης στην περίοδο σύνδεσης, ο χάκερ ενσωματώνει ένα ψεύτικο στοιχείο (το wrapper) στο μήνυμα δομή, μετακινεί το αρχικό σώμα του μηνύματος κάτω από το περιτύλιγμα, αντικαθιστά το περιεχόμενο του μηνύματος με κακόβουλο κώδικα, και στη συνέχεια στέλνει το μήνυμα στο διακομιστή. Δεδομένου ότι το αρχικό σώμα εξακολουθεί να είναι έγκυρο, ο διακομιστής θα εξαπατηθεί ώστε να εξουσιοδοτήσει το μήνυμα που στην πραγματικότητα έχει αλλοιωθεί. Ως αποτέλεσμα, ο χάκερ είναι σε

θέση να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε προστατευόμενους πόρους και να διεκπεραιώσει τις προβλεπόμενες λειτουργίες.

Δεδομένου ότι οι χρήστες του υπολογιστικού νέφους συνήθως ζητούν υπηρεσίες από τους παρόχους υπηρεσιών υπολογιστικού νέφους μέσω ενός web browser, οι επιθέσεις περιτύλιξης μπορούν να προκαλέσουν ζημιά και στα συστήματα νέφους. Το EC2 της Amazon ανακαλύφθηκε ότι είναι ευάλωτο σε επιθέσεις wrapping το 2008 (Iacono, 2009). Η έρευνα έδειξε ότι το EC2 είχε αδυναμία στον μηχανισμό επικύρωσης της ασφάλειας του μηνύματος SOAP. Ένα υπογεγραμμένο αίτημα SOAP ενός νόμιμου χρήστη μπορεί να υποκλαπεί και να τροποποιηθεί. Ως αποτέλεσμα, οι χάκερ θα μπορούσαν να λάβουν μη εξουσιοδοτημένες ενέργειες στους λογαριασμούς των θυμάτων στα σύννεφα. Χρησιμοποιώντας την τεχνική περιτύλιξης της υπογραφής XML, οι ερευνητές παρουσίασαν επίσης μια επίθεση αεροπειρατείας λογαριασμού που εκμεταλλευόταν ευπάθεια στο Amazon AWS (Researchers Demo Cloud Security Issue With Amazon AWS Attack, 2011) . Τροποποιώντας εξουσιοδοτημένα ψηφιακά υπογεγραμμένα μηνύματα SOAP, οι ερευνητές ήταν σε θέση να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση στο λογαριασμό ενός πελάτη, να διαγράψουν και να δημιουργήσουν νέες εικόνες στο EC2 instance του πελάτη και να εκτελέσουν άλλες διαχειριστικές εργασίες.

2.3 Μέτρα αντιμετώπισης

Μια υποδομή υπολογιστικού νέφους περιλαμβάνει έναν πάροχο υπηρεσιών υπολογιστικού νέφους, ο οποίος παρέχει υπολογιστικές πόρους σε τελικούς χρήστες του νέφους που καταναλώνουν τους πόρους αυτούς. Προκειμένου να διασφαλιστεί η καλύτερη ποιότητα των υπηρεσιών, οι πάροχοι είναι υπεύθυνοι για τη διασφάλιση της ασφάλειας του περιβάλλοντος νέφους. Αυτό μπορεί να είναι με τον καθορισμό αυστηρών πολιτικών ασφαλείας και με την εφαρμογή προηγμένων τεχνολογιών ασφαλείας.

2.3.1 Ενίσχυση της πολιτικής ασφαλείας

Με μια έγκυρη πιστωτική κάρτα, οποιοσδήποτε μπορεί να εγγραφεί για να χρησιμοποιήσει τους πόρους που προσφέρονται από την υπηρεσία cloud- παρόχους υπηρεσιών cloud. Αυτό κάνει τους χάκερ να εκμεταλλεύονται την ισχυρή υπολογιστική ισχύ των υπολογιστικών νεφών για να να διεξάγουν κακόβουλες δραστηριότητες, όπως spam και επιθέσεις σε άλλα υπολογιστικά συστήματα. Με τον μετριασμό αυτής της συμπεριφοράς κατάχρησης που προκαλείται από αδύναμα συστήματα εγγραφής, στις απάτες με πιστωτικές κάρτες θα μπορούσε να εφαρμοστεί παρακολούθηση και αποκλεισμός των δημόσιων μαύρων λιστών (A. Tripathi and A. Mishra, 2011). Επίσης, η εφαρμογή πολιτικών ασφαλείας μπορεί να μειώσει τον κίνδυνο καταχρηστικής χρήσης της υπολογιστικής ισχύος του νέφους (Zaki, 2011). Οι καλά καθιερωμένοι κανόνες και κανονισμοί μπορούν να βοηθήσουν τους διαχειριστές δικτύων να διαχειρίζονται τα νέφη περισσότερο αποτελεσματικά. Για παράδειγμα, η Amazon έχει ορίσει μια σαφή πολιτική χρηστών και απομονώνει (ή και τερματίζει) τυχόν παραβατικές περιπτώσεις κάθε φορά που λαμβάνει καταγγελία για spam ή κακόβουλο λογισμικό που έρχεται μέσω του Amazon EC2.

2.3.2 Διαχείριση πρόσβασης

Τα δεδομένα των τελικών χρηστών που είναι αποθηκευμένα στο νέφος είναι ευαίσθητα και ιδιωτικά και οι μηχανισμοί ελέγχου πρόσβασης θα μπορούσαν να εφαρμοστούν για να διασφαλιστεί ότι μόνο εξουσιοδοτημένοι χρήστες μπορούν να έχουν πρόσβαση στα δεδομένα τους. Δεν είναι μόνο το φυσικά συστήματα υπολογιστών (όπου αποθηκεύονται τα δεδομένα) πρέπει να παρακολουθούνται συνεχώς, η πρόσβαση της κυκλοφορίας στα δεδομένα θα πρέπει να περιορίζεται με τεχνικές ασφαλείας. Τείχη προστασίας και εισβολές ανίχνευσης είναι κοινά εργαλεία που χρησιμοποιούνται για τον περιορισμό της πρόσβασης από μη αξιόπιστους πόρους και για την παρακολούθηση κακόβουλων δραστηριοτήτων. Επιπλέον, τα πρότυπα ελέγχου ταυτότητας, τα πρότυπα σήμανσης ισχυρισμών ασφαλείας (Security Assertion Markup) Language (SAML) και eXtensible Access Control Markup Language (XACML), μπορούν να χρησιμοποιηθούν για να τον έλεγχο της πρόσβασης σε εφαρμογές και δεδομένα νέφους. Η SAML επικεντρώνεται στα μέσα μεταφοράς αποφάσεων ελέγχου ταυτότητας και εξουσιοδότησης μεταξύ συνεργαζόμενων οντοτήτων, ενώ η XACML εστιάζει στο μηχανισμό για την εξαγωγή αποφάσεων εξουσιοδότησης (Grance, 2018).

2.3.3 Προστασία δεδομένων

Οι παραβιάσεις δεδομένων που προκαλούνται από εσωτερικούς χρήστες μπορεί να είναι είτε τυχαίες είτε σκόπιμες. Δεδομένου ότι είναι δύσκολο να εντοπισμός της συμπεριφοράς των εσωτερικών προσώπων, είναι προτιμότερο να εφαρμόζονται κατάλληλα εργαλεία ασφαλείας για την αντιμετώπιση των εσωτερικών απειλών. Τα εργαλεία αυτά περιλαμβάνουν: συστήματα πρόληψης απώλειας δεδομένων, ανίχνευση ανώμαλων προτύπων συμπεριφοράς, εργαλεία διατήρησης μορφής και κρυπτογράφησης, προφίλ συμπεριφοράς χρήστη, τεχνολογία παραπλάνησης και τεχνολογίες ελέγχου ταυτότητας και εξουσιοδότησης. (Alotaibi, 2021) Αυτά τα εργαλεία παρέχουν λειτουργίες όπως ανίχνευση σε πραγματικό χρόνο στην παρακολούθηση της κυκλοφορίας, καταγραφή διαδρομών ελέγχου για μελλοντική εγκληματολογία και παγίδευση κακόβουλης δραστηριότητας σε έγγραφα δόλωμα.

2.3.4 Εφαρμογή τεχνικών ασφαλείας

Η επίθεση με κακόβουλο λογισμικό έχει γίνει μια σημαντική ανησυχία για την ασφάλεια των συστημάτων υπολογιστικού νέφους. Μπορεί να αποτραπεί με τη χρήση της αρχιτεκτονικής του συστήματος File Allocation Table (FAT) (Vrbsky, 2015). Από τον FAT πίνακα, η περίπτωση (κώδικας ή εφαρμογή) που πρόκειται να εκτελέσει ένας πελάτης μπορεί να αναγνωριστεί στο εκ των προτέρων. Συγκρίνοντας την περίπτωση με προηγούμενες που είχαν ήδη εκτελεστεί από το μηχάνημα του πελάτη, μπορεί επομένως να προσδιοριστεί η εγκυρότητα και η ακεραιότητα της νέας περίπτωσης. Ένας άλλος τρόπος αποτροπής επιθέσεων έγχυσης κακόβουλου λογισμικού είναι η αποθήκευση μιας τιμής κατακερματισμού στην αρχική υπηρεσία του αρχείου εικόνας της υπηρεσίας . Πραγματοποιώντας έναν έλεγχο ακεραιότητας μεταξύ της αρχικής και της νέας υπηρεσίας εικόνων, μπορούν να εντοπιστούν κακόβουλες περιπτώσεις.

Για τις επιθέσεις αναδίπλωσης υπογραφής XML σε υπηρεσίες ιστού, έχουν εφαρμοστεί διάφορες τεχνικές για να διορθώσουν την ευπάθεια που εντοπίζεται σε τεχνολογίες που βασίζονται στην XML. Για παράδειγμα, το XML Schema Η τεχνική Hardening χρησιμοποιείται για την ενίσχυση των δηλώσεων XML Schema . Ένα υποσύνολο του XPath, που ονομάζεται FastXPath, προτείνεται για να αντιστέκεται στα κακόβουλα στοιχεία που εισάγουν οι επιτιθέμενοι στις δομή του μηνύματος SOAP (S. Gajek, 2019).

2.4 Υιοθέτηση και επιτυχία του Cloud Computing σε έναν οργανισμό

2.4.1 Υιοθέτηση του Cloud Computing για τις επιχειρήσεις

Τα τελευταία χρόνια, η τεχνολογία νέφους έχει γίνει αναπόφευκτη πτυχή κάθε οργανισμού και τομέα. Λειτουργώντας ως καταλύτης για την ανάπτυξη. Ή προσέγγιση του νέφους έχει φέρει πλήρη επανάσταση στον τρόπο με τον οποίο οι επιχειρήσεις λειτουργούν.

2.4.2 Τι είναι η υιοθέτηση του Cloud;

Η υιοθέτηση του νέφους αναφέρεται στη μετάβαση ή την εφαρμογή του υπολογιστικού νέφους σε έναν οργανισμό. Αυτό μπορεί να περιλαμβάνει τη μετάβαση από την επιτόπια υποδομή στο σύννεφο ή τη χρήση του σύννεφου επιπλέον της επιτόπιας υποδομής. Μερικά παραδείγματα του τρόπου με τον οποίο οι οργανισμοί μπορούν να υιοθετήσουν το cloud computing (Michael, 2022)

Οι προμηθευτές υπολογιστικού νέφους αυξάνουν το εύρος και τον αριθμό των υπηρεσιών που παρέχουν μέσω του νέφους και τα δημοφιλή περιβάλλοντα δημόσιου νέφους, όπως το Microsoft Azure, το Amazon Web Services και το Google Cloud Platform, γίνονται πιο δημοφιλή από ποτέ.

Ανεξάρτητα από το μέγεθός τους, οι περισσότεροι οργανισμοί σήμερα έχουν υιοθετήσει το νέφος σε κάποια μορφή. Αν και η στρατηγική υιοθέτησης του cloud χρησιμοποιείται κυρίως από τις επιχειρήσεις για να βελτιώσουν την επεκτασιμότητα των δυνατοτήτων των βάσεων δεδομένων που βασίζονται στο Διαδίκτυο, μειώνοντας παράλληλα τον κίνδυνο και το κόστος, υπάρχουν και πολλά άλλα οφέλη αυτής της τεχνολογίας.

2.4.3 Εταιρείες διαφόρων μεγεθών μπορούν να επωφεληθούν από αυτή την τεχνολογική επανάσταση

Μεγάλες εταιρείες και επιχειρήσεις: Εταιρικά περιβάλλοντα απαιτούν τις μεγαλύτερες επενδύσεις IT. Η υιοθέτηση του επιχειρηματικού cloud οδηγεί σε σημαντική εξοικονόμηση πόρων, καθώς βελτιώνει την αποδοτικότητα, εξαλείφει την ανάγκη για μεγάλο προσωπικό ασφαλείας και συντήρησης και μειώνει το κόστος του χώρου για τους διακομιστές. (Ahmad, 2015)

Μικρές και μεσαίου μεγέθους εταιρείες: Η αύξηση του προσωπικού, του πελατολογίου και των έργων συχνά απαιτεί από τους μικρούς και μεσαίους οργανισμούς να αναπτύξουν γρήγορα την υποδομή IT τους. Η ενασχόληση με το cloud computing επιτρέπει την αποτελεσματική και οικονομικά αποδοτική επεκτασιμότητα που διαρκεί λεπτά αντί για ημέρες.

Επιχειρηματίες και νεοσύστατες επιχειρήσεις: Η επιλογή του νέφους αντί μιας ακριβής υποδομής IT μειώνει το κόστος εκκίνησης και τις αρχικές επενδύσεις σε λογισμικό. Οι πωλητές λογισμικού ως υπηρεσία (SaaS) προσφέρουν πλέον συνήθως ένα συνδρομητικό μοντέλο με μηνιαία χρέωση. (Habjan, 2017)

2.4.4 Πώς λειτουργεί η υιοθέτηση του Cloud;

Προκειμένου να πραγματοποιήσουν τη μετάβαση στο νέφος, οι οργανισμοί πρέπει να έχουν κατά νου μερικά κρίσιμα βήματα. Σε αυτά περιλαμβάνονται:

Αξιολόγηση: Τα στελέχη και οι υπεύθυνοι για τη λήψη αποφάσεων στον τομέα της πληροφορικής πρέπει να αξιολογήσουν τις ευκαιρίες και τις προκλήσεις της εφαρμογής μιας στρατηγικής υπολογιστικού νέφους στην αγορά τους. Εκτός από την έρευνα δημοφιλών προμηθευτών στον κλάδο τους, οι επικεφαλής των επιχειρήσεων και οι τεχνολογικές τους ομάδες θα πρέπει να συλλέξουν στοιχεία σχετικά με τις προκλήσεις και τις επιτυχίες των προηγούμενων υιοθετών στον χώρο τους. (Eckhardt, 2014)

Σχεδιασμός: Μόλις οι οργανισμοί κάνουν την έρευνά τους, πρέπει να σχεδιάσουν τη συγκεκριμένη στρατηγική τους για το cloud. Οι ηγέτες της πληροφορικής θα πρέπει να επιλέξουν πλατφόρμες και υπηρεσίες που είναι γνωστές στον κλάδο τους και που

κυκλοφορούν γρήγορα στην αγορά. Θα πρέπει επίσης να αποφασίσουν μεταξύ δημόσιου, ιδιωτικού ή υβριδικού νέφους.

Υιοθέτηση: Κατά τη φάση της υιοθέτησης, οι ηγέτες ΤΠ θα πρέπει να αναπτύξουν στρατηγικές μετριασμού των κινδύνων. Θα πρέπει επίσης να έχουν μια εξειδικευμένη κατανόηση των διακομιστών, του λογισμικού και των αποθηκών δεδομένων τους για τη μελλοντική επανάληψη και την επεκτασιμότητα της στρατηγικής τους.

Βελτιστοποίηση: Με τακτικές συναντήσεις με την εκτελεστική τους ομάδα, τα τμήματα πληροφορικής μπορούν να συζητήσουν τα διδάγματα που αποκόμισαν από τη στρατηγική τους για το υπολογιστικό νέφος και να δημιουργήσουν νέες και βελτιωμένες λύσεις για περαιτέρω διαδικασίες και εργασίες.

Ενώ οι οργανισμοί όλων των μεγεθών θα πρέπει να ακολουθήσουν τα τρία πρώτα βήματα της αρχικής υιοθέτησης, θα πρέπει επίσης να συνεχίσουν να βελτιστοποιούν τη στρατηγική τους για το υπολογιστικό νέφος με την πάροδο του χρόνου. (T. Oliveira, 2015)

2.4.5 Πτυχές ασφαλείας της υιοθέτησης του Cloud

Οι επιχειρήσεις που μεταβαίνουν στο νέφος έχουν φυσικά ανησυχίες σχετικά με την ασφάλεια των ευαίσθητων δεδομένων της εταιρείας και των πελατών. Για να διασφαλιστεί ότι οι πληροφορίες δεν θα χαθούν ή δεν θα εκτεθούν μέσω παραβιάσεων δεδομένων ή πειρατείας λογαριασμών, είναι απαραίτητες οι ακόλουθες εκτιμήσεις σχετικά με την ασφάλεια του νέφους: (T. Dillon, 2010)

Χρήση ασφαλών διεπαφών και API: Οι επιχειρήσεις θα πρέπει να φροντίζουν να διασφαλίζουν ότι οι διεπαφές χρήστη (UI) του λογισμικού και οι διεπαφές προγραμματισμού εφαρμογών (API) είναι ενημερωμένες - και ασφαλείς. Η συνεπής διαχείριση και παρακολούθηση αξιόπιστων εργαλείων θα βοηθήσει στην προστασία από κακόβουλες και απρόβλεπτες παραβιάσεις και σφάλματα.

Αποτρέψτε τα τρωτά σημεία του συστήματος: Τα σφάλματα του προγράμματος επιτρέπουν στους χάκερ να αναλάβουν τον έλεγχο των συστημάτων cloud ή να κλέψουν δεδομένα. Η παρακολούθηση των ενημερώσεων του συστήματος και ο γρήγορος εντοπισμός των ευπαθειών μπορεί να βοηθήσει στην εξάλειψη αυτού του κινδύνου.

Δημιουργία προγράμματος κατάρτισης και σχέδια αντιμετώπισης καταστροφών: Οι φυσικές καταστροφές, η τυχαία διαγραφή και η ανεπαρκής επιμέλεια κατά την υιοθέτηση

τεχνολογιών cloud μπορεί να οδηγήσουν σε απώλεια δεδομένων και κακόβουλες επιθέσεις. Οι εταιρείες όλων των μεγεθών θα πρέπει να δημιουργήσουν έναν οδικό χάρτη υπολογιστικού νέφους και ένα πρόγραμμα εκπαίδευσης των εργαζομένων για τον μετριασμό αυτών των ζητημάτων. (Oliveira, 2014)

2.4.6 Ποιες είναι οι προκλήσεις της υιοθέτησης του Cloud

Ενώ τα θέματα ασφάλειας βρίσκονται στην πρώτη γραμμή των ανησυχιών για την υιοθέτηση του νέφους, υπάρχουν και άλλες προκλήσεις που εμφανίζονται. Αυτές περιλαμβάνουν:

Εκπαίδευση του προσωπικού: Οι σημερινές επιχειρήσεις περιλαμβάνουν υπαλλήλους διαφόρων ηλικιών και τεχνικών δεξιοτήτων. Μαζί με την εκπαίδευση σε θέματα ασφάλειας, οι οργανισμοί θα πρέπει να συνεχίσουν να εκπαιδεύουν τις ομάδες σε διάφορα τμήματα σχετικά με τον τρόπο χρήσης του cloud και την ελαχιστοποίηση των καθημερινών λειτουργικών προκλήσεων. (Chen, 2012)

Βελτίωση των διαδικασιών: Οι εταιρείες πρέπει να γίνουν έμπειρες στη χρήση διαφόρων ολοκληρωμένων υπηρεσιών, ειδικά σε ένα υβριδικό περιβάλλον cloud. Το IT θα πρέπει να είναι προετοιμασμένο να μετακινεί δεδομένα σε διαφορετικούς παρόχους υπηρεσιών για να προσαρμόζεται στη ζήτηση και να βελτιστοποιεί τις διαδικασίες.

Παρόλο που υπάρχουν πολλά οφέλη από την υιοθέτηση του νέφους, συμπεριλαμβανομένων των αποδοτικότερων επιχειρηματικών λειτουργιών και της εξοικονόμησης κόστους, κάθε εταιρεία που δραστηριοποιείται στο νέφος θα πρέπει να εξετάζει προσεκτικά τους παρόχους υπηρεσιών, τις ανησυχίες για την ασφάλεια και τις συνεχείς προκλήσεις των διαδικασιών, προκειμένου να δημιουργήσει μια αποτελεσματική και ασφαλή εμπειρία για την ομάδα και τους πελάτες της. Οι Nearshore Plus Services της iTexico επιτρέπουν στον οργανισμό να συνεργαστεί με ειδικούς στο cloud computing και να καινοτομήσει καλύτερα, μειώνοντας παράλληλα τον κίνδυνο και το κόστος που απαιτείται για την υλοποίηση της στρατηγικής για το νέφος στην αγορά. (G. Feuerlicht, 2015)

2.4.7 Ποιος χρειάζεται την υιοθέτηση του Cloud - και γιατί;

Μια ποικιλία κλάδων επωφελείται από την υιοθέτηση του νέφους, όπως η υγειονομική περίθαλψη, το μάρκετινγκ και η διαφήμιση, το λιανικό εμπόριο, η χρηματοδότηση και η εκπαίδευση. Τα οφέλη περιλαμβάνουν:

Υγειονομική περίθαλψη: Με αφορμή την ψηφιακή και κοινωνική συμπεριφορά των καταναλωτών και την ανάγκη για ασφαλή και προσβάσιμα ηλεκτρονικά αρχεία υγείας (EHR), τα νοσοκομεία, οι κλινικές και άλλοι ιατρικοί οργανισμοί χρησιμοποιούν το υπολογιστικό νέφος για την αποθήκευση εγγράφων, το μάρκετινγκ και τους ανθρώπινους πόρους. (Repschlaeger, 2013)

Μάρκετινγκ και διαφήμιση: Σε έναν κλάδο που εξαρτάται από τα μέσα κοινωνικής δικτύωσης, καθώς και από τη γρήγορη δημιουργία και δημοσίευση περιεχομένου σχετικού με τους πελάτες, οι οργανισμοί χρησιμοποιούν στρατηγικές υιοθέτησης υβριδικού cloud για να μεταφέρουν κρίσιμα μηνύματα πελατών στο τοπικό και παγκόσμιο κοινό τους.

Λιανικό εμπόριο: Μια επιτυχημένη στρατηγική ηλεκτρονικού εμπορίου απαιτεί μια υγιή στρατηγική για το Διαδίκτυο. Με τη βοήθεια της υιοθέτησης του cloud, το λιανικό εμπόριο που βασίζεται στο Internet είναι σε θέση να προωθήσει αποτελεσματικά την αγορά στους πελάτες και να αποθηκεύσει τα δεδομένα των προϊόντων του με λιγότερα χρήματα.

Χρηματοοικονομικά: Η αποτελεσματική διαχείριση δαπανών, οι ανθρώπινοι πόροι και οι επικοινωνίες με τους πελάτες είναι τρεις από τις σημαντικότερες επιχειρηματικές ανάγκες των σημερινών οικονομικών οργανισμών. Για τους λόγους αυτούς, τα χρηματοπιστωτικά ιδρύματα τοποθετούν πλέον τις πλατφόρμες ηλεκτρονικού ταχυδρομείου και τα εργαλεία μάρκετινγκ στο cloud.

Εκπαίδευση: Οι εκπαιδευτικές ευκαιρίες που βασίζονται στο διαδίκτυο είναι σήμερα πιο δημοφιλείς από ποτέ. Το νέφος επιτρέπει στα πανεπιστήμια, τα ιδιωτικά ιδρύματα και τα δημόσια σχολεία K-12 να παρέχουν online συστήματα μάθησης, εργασίας και βαθμολόγησης. (Lin, 2012)

Πρόσθετες βιομηχανίες που επωφελούνται από την υιοθέτηση του νέφους περιλαμβάνουν τις κατασκευές, τα ακίνητα και τους μη κερδοσκοπικούς οργανισμούς.

2.4.8 10 βασικά οφέλη της υιοθέτησης του Cloud για τις επιχειρήσεις

1. Βελτιωμένη εξυπηρέτηση πελατών

Η εξυπηρέτηση πελατών διαδραματίζει κρίσιμο ρόλο στη διασφάλιση της επιτυχίας κάθε επιχείρησης. Η προσφορά εξαιρετικής εμπειρίας πελατών μπορεί να αποτελέσει έναν παράγοντα αλλαγής παιχνιδιού που μπορεί να σας δώσει ένα σαφές ανταγωνιστικό πλεονέκτημα. (Vairagkar, 2023)

Η υιοθέτηση της τεχνολογίας και των λύσεων cloud μπορεί να συμβάλει καθοριστικά στην επίτευξη αυτού του στόχου, καθώς επιτρέπει στους πελάτες να παραμένουν σε επαφή με την εταιρεία σας. Οι περισσότερες από τις εταιρείες που βασίζονται στο cloud επιλύουν προληπτικά τα ερωτήματα υποστήριξης πελατών και διαθέτουν επίσης SLAs για το χρόνο διαθεσιμότητας, ώστε να διασφαλίζουν τη διαθεσιμότητα του συστήματος όποτε υπάρχει ανάγκη.

Επιπλέον, επιτρέπουν στους πελάτες να συνδέονται εύκολα με το προσωπικό για να επιλύσουν τα ερωτήματά τους ή να δώσουν ανατροφοδότηση άμεσα. Αυτού του είδους η επικοινωνία σε πραγματικό χρόνο μπορεί να βοηθήσει να προσελκύσουμε και να δεσμεύσουμε τους πελάτες με την επιχείρησή μας.

2.Αποδοτικότητα κόστους

Οι λύσεις επί τόπου είναι συχνά αρκετά ακριβές, με διάφορα κόστη να αθροίζονται. Αυτά περιλαμβάνουν το απαραίτητο υλικό και το κόστος υλοποίησης μαζί με το κόστος που σχετίζεται με τη συνεχή διαχείριση και ενημέρωση που απαιτείται από το εσωτερικό προσωπικό.

Η μετάβαση στο cloud, αντίθετα, παρέχει στους οργανισμούς τα πλεονεκτήματα της εξάλειψης του υψηλού κόστους υλικού και εγκατάστασης, καθώς τους επιτρέπει να επιλέξουν ένα μοντέλο με βάση τη συνδρομή που ταιριάζει στον προϋπολογισμό τους.

Επιπλέον, οι περισσότερες λύσεις cloud παρέχουν στις επιχειρήσεις τη δυνατότητα να πληρώνουν ακριβώς γι' αυτό που χρειάζονται, αντί να πληρώνουν για ανεπιθύμητες ή αχρησιμοποίητες υπηρεσίες.

3. Ταχύτεροι κύκλοι υλοποίησης

Οι περισσότεροι οργανισμοί με λογισμικό επί τόπου αγωνίζονται με τον υψηλότερο χρόνο μεταξύ της απόφασης για την υλοποίηση του προϊόντος και της στιγμής που ο χρήστης αρχίζει να το χρησιμοποιεί.

Όμως, με τις λύσεις cloud, οι επιχειρήσεις απολαμβάνουν το πλεονέκτημα ενός γρήγορου κύκλου υλοποίησης, όπου τα προϊόντα συνήθως τίθενται σε λειτουργία μέσα σε εβδομάδες αντί για μήνες.

Επιπλέον, η τεχνολογία cloud βελτιώνει τη συνεργασία μεταξύ των ομάδων, καθώς επιτρέπει στις ομάδες να έχουν εύκολη πρόσβαση, να επεξεργάζονται και να μοιράζονται έγγραφα και δεδομένα από οπουδήποτε και ανά πάσα στιγμή. Αυτό οδηγεί σε αυξημένη παραγωγικότητα και αποδοτικότητα και παρέχει ενημερώσεις σε πραγματικό χρόνο μέσω εφαρμογών ροής εργασιών και κοινής χρήσης αρχείων που βασίζονται στο cloud.

4. Προωθεί την επεκτασιμότητα

Με την πάροδο του χρόνου, κάθε επιχείρηση βιώνει αλλαγές στην οργανωτική της δομή, καθώς είτε επεκτείνεται, είτε περιορίζεται, είτε υφίσταται εποχικές επιχειρηματικές αλλαγές. Οι λύσεις cloud μπορούν να φιλοξενήσουν απρόσκοπτα τέτοιες αλλαγές και να ανταποκριθούν επαρκώς σε αυτές. Μόλις μεταβείτε στο cloud, δεν χρειάζεται να αλλάζετε συνεχώς λογισμικό κάθε φορά που αυξάνετε ή μειώνετε την κλίμακα. Αυτό προάγει την επεκτασιμότητα της επιχείρησης και επιτρέπει στην εταιρεία να αναπτύσσεται σύμφωνα με τις συγκεκριμένες ανάγκες της.

5. Αναβαθμίσεις & συντήρηση

Η αντιμετώπιση των διακοπών λειτουργίας για αναβαθμίσεις και δαπανηρή συντήρηση είναι ένα κοινό πρόβλημα που αντιμετωπίζουν οι οργανισμοί με το λογισμικό on-premise. Επιπλέον, οι αναβαθμίσεις είναι συχνά μακρινές και λιγότερες σε αριθμό με τα on-premise προϊόντα, αυξάνοντας έτσι τον κίνδυνο το λογισμικό να καταστεί παρωχημένο. Με το cloud, δεν υπάρχει τέτοιος κίνδυνος. Οι αναβαθμίσεις και η συντήρηση στην περίπτωση του νέφους είναι απρόσκοπτες και συχνές. Οι πελάτες που χρησιμοποιούν λογισμικό βασισμένο στο cloud απολαμβάνουν πάντα το πλεονέκτημα ότι βρίσκονται στην τελευταία έκδοση.

6. Καλύτερη ασφάλεια

Οι υπηρεσίες cloud είναι γνωστό ότι αποθηκεύουν πληροφορίες σε διακομιστές και υλικό που δεν ελέγχονται από την επιχείρηση. Αυτοί οι εξωτερικοί διακομιστές προσφέρουν αυστηρά μέτρα ασφαλείας για την αποτροπή οποιασδήποτε μορφής παραβίασης δεδομένων. Ως εκ τούτου, το σύννεφο είναι γενικά πιο ασφαλές σε σύγκριση με την υποδομή στις εγκαταστάσεις. Η μετάβαση σε μια λύση cloud διασφαλίζει ότι κανένα από τα εμπιστευτικά δεδομένα δεν είναι ευάλωτο σε χάκερ ή σε όσους δεν είναι εξουσιοδοτημένοι και το σώζει από τις συνήθεις απειλές ασφαλείας.

7. Καλύτερος έλεγχος εγγράφων

Σε κάθε οργανισμό όπου οι εργαζόμενοι παράγουν και ανταλλάσσουν μεγάλο όγκο πληροφοριών εντός του κύκλου παραγωγής, υπάρχει αυξημένη ανάγκη για σωστή τεκμηρίωση. Αυτό γενικά δημιουργεί πολλά αντικρουόμενα αρχεία σε πολλαπλές μορφές και τίτλους. Όμως με το cloud, οι εργαζόμενοι μπορούν να στέλνουν αρχεία σε ένα κεντρικό σημείο όπου όλοι μπορούν να έχουν πρόσβαση σε αυτά. Επιπλέον, με τις εφαρμογές και την υποδομή σας να φιλοξενούνται στο cloud, τοποθετείτε τον εαυτό σας σε ένα οικοσύστημα όπου υπάρχει συνεχής καινοτομία. Αρκετές τεχνολογικές εξελίξεις φροντίζονται και υλοποιούνται από τον συνεργάτη σας στο cloud.

8. Δίνει πολλαπλές επιλογές

Το cloud computing προσφέρει στις επιχειρήσεις πλήθος εφαρμογών στο πλαίσιο μιας από τις παρακάτω υπηρεσίες:

Λογισμικό ως υπηρεσία (SaaS)

Πλατφόρμα ως υπηρεσία (PaaS)

Υποδομή ως υπηρεσία (IaaS)

Οι πελάτες έχουν επίσης τη δυνατότητα να δημιουργήσουν πρόσβαση σε ιδιωτικό, δημόσιο ή υβριδικό δίκτυο. Εκτός από αυτές τις ατελείωτες δυνατότητες, το cloud computing προσφέρει επίσης στις επιχειρήσεις το πλεονέκτημα της προσαρμογής σε κάθε είδους επιχειρηματική αλλαγή.

9. Φιλικό προς το περιβάλλον

Τα πλεονεκτήματα των λύσεων cloud δεν περιορίζονται μόνο στην επιχειρηματική πλευρά. Η τεχνολογία προσφέρει επίσης αρκετά περιβαλλοντικά οφέλη. Η υιοθέτηση της τεχνολογίας cloud σας επιτρέπει να μειώσετε το αποτύπωμα άνθρακα, καθώς μπορείτε εύκολα να αυξάνετε και να μειώνετε την κλίμακα ανάλογα με τις συγκεκριμένες απαιτήσεις της επιχείρησής σας. Σας δίνει το πλεονέκτημα να χρησιμοποιείτε μόνο τους πόρους που χρειάζεστε και να γλιτώνετε από το να αφήνετε υπερμεγέθη αποτυπώματα.

10. Αποκατάσταση από καταστροφές

Ανεξάρτητα από το μέγεθός τους, οι επιχειρήσεις δαπανούν συχνά ένα τεράστιο μέρος των χρημάτων τους για την αποκατάσταση καταστροφών. Το cloud computing μπορεί να βοηθήσει τους οργανισμούς, ιδίως τις μικρές επιχειρήσεις, να εξοικονομήσουν χρόνο και πόρους, να αποφύγουν υψηλές επενδύσεις και να επωφεληθούν από την τεχνογνωσία τρίτων. (Vairagkar, 2023)

Για να κλείσουμε

Το υπολογιστικό νέφος είναι ένας εξαιρετικός τρόπος για τις επιχειρήσεις να βελτιώσουν και να ενισχύσουν τη συνολική παραγωγικότητά τους και να περιηγηθούν αποτελεσματικά στο ταχέως εξελισσόμενο επιχειρηματικό περιβάλλον. Όμως, όταν πρόκειται για την υιοθέτηση λύσεων cloud, μία από τις πιο κρίσιμες πτυχές για τη διασφάλιση των βέλτιστων οφελών της τεχνολογίας είναι η επιτυχής στρατηγική υλοποίησης. Αυτό καθιστά πολύ σημαντικό για τους οργανισμούς να αφιερώνουν άφθονο χρόνο στον σχεδιασμό της στρατηγικής μετάβασης στο νέφος και να την παρακολουθούν σε κάθε στάδιο.

Κεφάλαιο 3 : Μεθοδολογία έρευνας

3.1 Σχετική εργασία

Τα συστήματα ανίχνευσης εισβολών (IDS) χρησιμοποιούν δύο κύριες προσεγγίσεις για τον εντοπισμό επιθέσεων στον κυβερνοχώρο: ανίχνευση βάσει υπογραφής και ανίχνευση ανωμαλίας με χρήση μηχανικής μάθησης. (Axelsson, 2000). Οι ανιχνευτές που βασίζονται σε υπογραφές χρησιμοποιούνται ευρέως για γνωστές επιθέσεις, αλλά περιορίζονται από την εξάρτησή τους από τη γνώση των ειδικών και την αδυναμία τους να ανιχνεύσουν επιθέσεις 0 ημερών (0-day attacks) (J. Song, 2008). Η ανίχνευση ανωμαλιών στοχεύει να ξεπεράσει αυτούς τους περιορισμούς, αλλά αντιμετωπίζει προκλήσεις όσον αφορά την παραγωγή αξιόπιστων αποτελεσμάτων, γεγονός που οδηγεί σε περιορισμένη ανάπτυξη. (J. Gao, 2006) Πρόσφατα η εστίαση έχει μετατοπιστεί από τις απόψεις που βασίζονται σε πακέτα στις απόψεις που βασίζονται σε ροές για τη μέτρηση της αποτελεσματικότητας των IDS. (N. Lu, 2012) Η παρούσα εργασία αποσκοπεί στη συστηματική κατανόηση και ανάλυση των βαθύτερων αιτιών των ψευδώς αρνητικών αποτελεσμάτων στην ανίχνευση εισβολών, με στόχο την καθοδήγηση του σχεδιασμού των IDS επόμενης γενιάς.

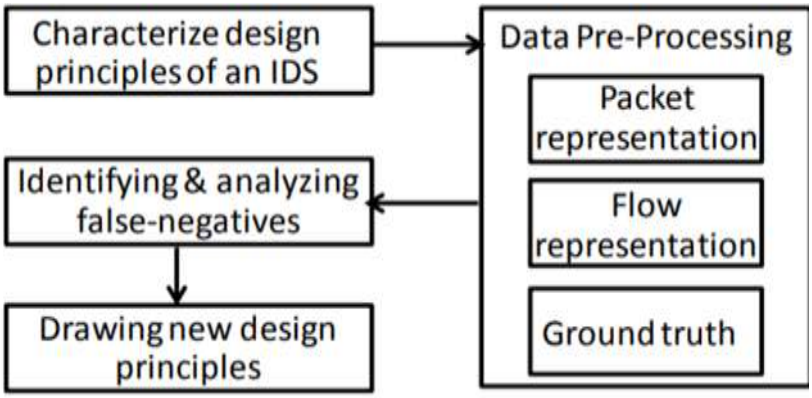
3.2 Περιεχόμενο μελέτης περίπτωσης

Περιγράφει τη μεθοδολογία για την ανάλυση των βαθύτερων αιτιών των ψευδώς αρνητικών αποτελεσμάτων της ανίχνευσης εισβολών. Στη συνέχεια παρουσιάζεται η μελέτη περίπτωσής μας και συζητούνται οι περιορισμοί της παρούσας μελέτης.

3.3 Μεθοδολογία ανάλυσης αιτιών

Προτείνουμε μια προσέγγιση με βάση τα δεδομένα για τον εντοπισμό και την ανάλυση ψευδώς αρνητικών περιπτώσεων σε συστήματα ανίχνευσης εισβολών (IDS). Η μεθοδολογία αποτελείται από τέσσερα βήματα: (ii) προεπεξεργασία δεδομένων με γνωστή βασική αλήθεια, iii) εντοπισμός και ανάλυση ψευδώς αρνητικών αποτελεσμάτων και iv) εξαγωγή νέων αρχών για την καθοδήγηση μελλοντικών σχεδίων IDS. Η προσέγγιση αυτή αποσκοπεί στη βελτίωση της απόδοσης των IDS και στη μείωση των ψευδώς αρνητικών περιστατικών.

Τα βήματα αυτά επισημαίνονται στο Σχήμα και αναλύονται παρακάτω.



Εικόνα 1-Παρουσίαση της μεθοδολογίας ανάλυσης αιτιών

3.3.1 Χαρακτηρισμός αρχών σχεδιασμού ενός IDS

Είναι ζωτικής σημασίας να κατανοήσουμε τις αρχές σχεδιασμού και τους στόχους ενός συστήματος ανίχνευσης εισβολών (IDS) για τον ακριβή εντοπισμό ψευδώς αρνητικών περιπτώσεων. Η κατανόηση των ειδών αποτυχιών που ευθυγραμμίζονται με τους στόχους του IDS βοηθά στη διαφοροποίηση μεταξύ αληθινών και ψευδώς αρνητικών αποτελεσμάτων. Για παράδειγμα, ενώ ένα IDS που στοχεύει σε κακόβουλες δραστηριότητες μπορεί να χαρακτηρίσει μια σάρωση ping ως κακόβουλη, ένας ανιχνευτής ανωμαλιών μπορεί να τη θεωρήσει φυσιολογική λόγω τακτικής παρόμοιας κίνησης.

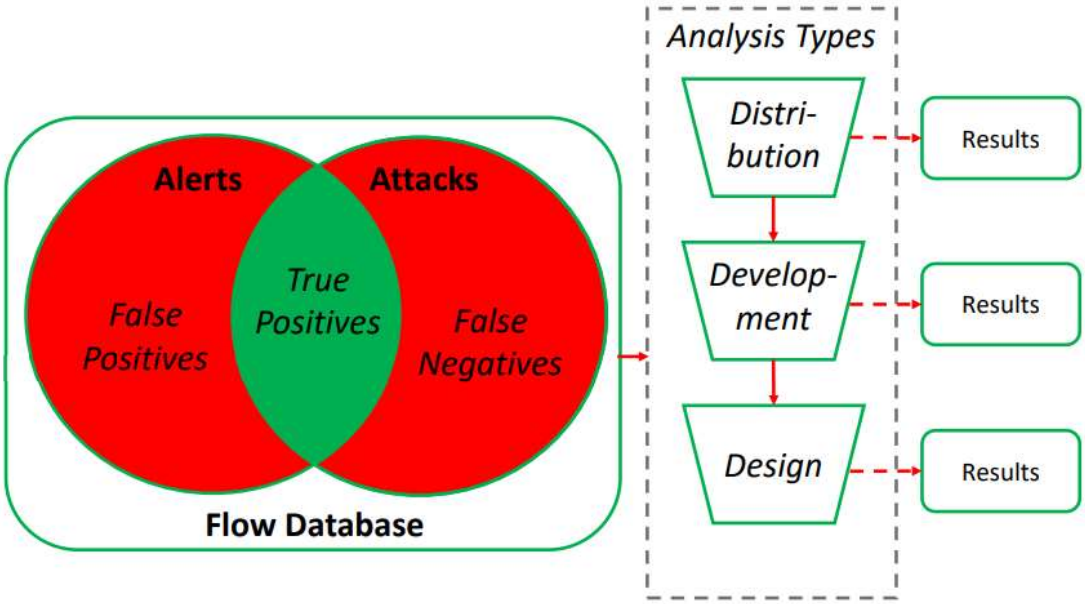
3.3.2 Προεπεξεργασία δεδομένων

Στην ενότητα αυτή προτείνεται η δημιουργία δύο βάσεων δεδομένων από ένα δεδομένο σύνολο δεδομένων δικτυακών επιθέσεων: μια βάση δεδομένων με βάση τη ροή και μια βάση δεδομένων με βάση τα πακέτα. Αυτό είναι σημαντικό για τη σύγκριση των νεότερων IDS που βασίζονται στη ροή με τα παλαιότερα συστήματα που βασίζονται σε πακέτα. (Pras, 2011) Μια ροή δικτύου ορίζεται από μια 5-σύζευξη, η οποία περιλαμβάνει διευθύνσεις IP πηγής και προορισμού, αριθμούς θύρας πηγής και προορισμού και πρωτόκολλο.

Η προτεινόμενη μέθοδος περιλαμβάνει την αντιστοίχιση κάθε πακέτου στην αντίστοιχη ροή του με βάση την 5-σύζευξη και τις χρονοσφραγίδες. Μπορούν να δημιουργηθούν ετικέτες βασικής αλήθειας σε επίπεδο πακέτου ή ροής χρησιμοποιώντας αυτή την αντιστοίχιση πακέτου-ροής τόσο για δεδομένη βασική αλήθεια όσο και για ειδοποιήσεις που δημιουργούνται από IDS. Επιπλέον, το IDS πρέπει να ρυθμιστεί ώστε να ταιριάζει με την αρχική αρχιτεκτονική του δικτύου για την επεξεργασία των καταγεγραμμένων αρχείων PCAP.

3.3.3 Προσδιορισμός και ανάλυση ψευδώς αρνητικών περιπτώσεων

Περιγράφει μια διαδικασία δύο βημάτων για τον εντοπισμό ψευδώς αρνητικών περιπτώσεων σε προεπεξεργασμένα δεδομένα κίνησης δικτύου. Πρώτον, η βασική αλήθεια ταυτίζεται με τα πειραματικά αποτελέσματα χρησιμοποιώντας την αντιστοίχιση μεταξύ πακέτων και ροών, επιτρέποντας τον εντοπισμό των σωστά εντοπισμένων επιθέσεων. (Paxson, 2010) Για παράδειγμα, το ερώτημα flows.find({Tag:Attack,Alert:True}), θα επέστρεφε όλες τις κακόβουλες ροές που οδήγησαν σωστά σε ειδοποιήσεις IDS.



Εικόνα 2-Διαδικασία ανάλυσης. Έξοδος απο τα ερωτήματα της βάσης δεδομένων ροής, εξετάζονται σύμφωνα με τον κύκλο ζωής ανάπτυξης IDS, αλλά και αντίστροφα

Δεύτερον, αναλύεται ο σχεδιασμός του IDS, εστιάζοντας σε ατέλειες στο σύστημα διανομής, στη διαδικασία ανάπτυξης και στον σχεδιασμό του κινητήρα. Αυτές οι εντοπισμένες ατέλειες συντίθενται στη συνέχεια σε αποτελέσματα.

3.3.4 Αντλώντας νέες αρχές

Εξετάζει πώς οι γνώσεις που αποκτώνται από την ανάλυση των ψευδώς αρνητικών αποτελεσμάτων μπορούν να καθοδηγήσουν την ανάπτυξη μελλοντικών συστημάτων

ανίχνευσης εισβολών (IDS). Αυτές οι γνώσεις μπορούν να συμπληρώσουν ή να αντικαταστήσουν τις υπάρχουσες αρχές σχεδιασμού, βελτιώνοντας τελικά την απόδοση των IDS.

Κεφάλαιο 4 Μελέτη Περίπτωσης

Αυτή η ενότητα εξετάζει μια μελέτη περίπτωσης σχετικά με την εφαρμογή της προτεινόμενης μεθοδολογίας για τον εντοπισμό ψευδώς αρνητικών αποτελεσμάτων και την ανάλυση των βαθύτερων αιτιών τους στο Snort, ένα δημοφιλές IDS ανοικτού κώδικα που βασίζεται σε υπογραφές. Η μελέτη χρησιμοποιεί τα σύνολα κανόνων που είναι διαθέσιμα από το Snort κατά την εγκατάσταση χωρίς καμία τροποποίηση.

4.1 Χαρακτηρισμός των αρχών σχεδιασμού του Snort

Αυτή η ενότητα εξετάζει τις αρχές σχεδιασμού του Snort για τη δημιουργία κανόνων που εξετάζουν την κυκλοφορία του δικτύου. (system., 2018)

Οι πέντε βασικές αρχές είναι οι εξής:.

1. Αντιστοίχιση περιεχομένου: Για να επιτύχουν υψηλή απόδοση, οι κανόνες πρέπει να αντιστοιχούν σε συγκεκριμένα bytestrings για να αποκλείουν γρήγορα την κίνηση που δεν ταιριάζει.

2. Σύλληψη ευπαθειών, όχι εκμεταλλεύσεων: Οι κανόνες θα πρέπει να στοχεύουν σε ευπάθειες και όχι σε συγκεκριμένα exploits, ώστε να αποτρέπεται η παράκαμψη μέσω τροποποιημένου κώδικα exploits.

3. Λαμβάνοντας υπόψη τις παραξενιές του πρωτοκόλλου: Οι κανόνες θα πρέπει να λαμβάνουν υπόψη τις παραλλαγές του πρωτοκόλλου (π.χ. κωδικοποιήσεις χαρακτήρων μεταβλητού μήκους) για να αποτρέπεται η αποφυγή μέσω μικρών τροποποιήσεων του πρωτοκόλλου.

4. Έλεγχος διακριτών τιμών πριν από τις αναδρομικές: Η ιεράρχηση διακριτών τιμών μπορεί να βελτιώσει την απόδοση, αποκλείοντας γρήγορα τη μη κακόβουλη κυκλοφορία.

5. Βελτιστοποίηση για κωδικοποιήσεις μεταβλητού μήκους: Η απόδοση μπορεί να βελτιωθεί με την παράκαμψη μη σχετικών δεδομένων μεταβλητού μήκους για την ταχύτερη εύρεση σχετικών πεδίων.

Η ενότητα τονίζει ότι οι αρχές (ii) και (iii) είναι ιδιαίτερα σημαντικές, καθώς η μη τήρησή τους μπορεί να οδηγήσει σε ψευδώς αρνητικά αποτελέσματα λόγω κακού σχεδιασμού κανόνων και όχι λόγω κακής εφαρμογής των κανόνων.

4.2 Προεπεξεργασία δεδομένων

Εξετάζουμε ένα σύνολο δεδομένων από το Κέντρο Αριστείας για την Ασφάλεια Πληροφοριών (ISCX) του Πανεπιστημίου του New Brunswick, το οποίο (A. Shiravi, 2012)χρησιμοποιείται για την αξιολόγηση συστημάτων ανίχνευσης εισβολών (IDS).

Αυτό το σύνολο δεδομένων επιλέχθηκε λόγω των καλά τεκμηριωμένων και ποικίλων σεναρίων επίθεσης που περιέχει, και περιέχει μικτή κακόβουλη και καλοήθη κυκλοφορία από μια ρεαλιστική αρχιτεκτονική δικτύου. Πιο συγκεκριμένα, το σύνολο δεδομένων περιέχει καλοήθη κυκλοφορία που παράγεται από ορισμένα στατιστικά μοντέλα πραγματικής κυκλοφορίας, καθώς και χειροκίνητες επιθέσεις. Επιλέγουμε αυτό το σύνολο δεδομένων επειδή περιλαμβάνει καλά τεκμηριωμένα και ποικίλα σενάρια επιθέσεων και έχει γίνει αποδεκτό από την ερευνητική κοινότητα για την αξιολόγηση IDS. Εξετάστηκαν και άλλα σύνολα δεδομένων, αλλά αυτά είναι πιο περιορισμένα επειδή δεν περιγράφουν ποιες επιθέσεις υπάρχουν τα δεδομένα, τα δεδομένα πρέπει να καθαριστούν λόγω της παρουσίας ευαίσθητων πληροφοριών, ή δεν περιλαμβάνουν πλήρη πακέτα συλλήψεις πακέτων. Χρησιμοποιούμε την ενότητα MongoDB της Python, pymongo, για να να διαχειριστούμε μια βάση δεδομένων για πακέτα και μια βάση δεδομένων για ροές.

Το σύνολο δεδομένων περιλαμβάνει εννέα διαφορετικές επιθέσεις, οι οποίες κατηγοριοποιούνται σε τρεις ομάδες με βάση τους στόχους των IDS:

Επιθέσεις ευπάθειας-μελέτης: Οι επιθέσεις αυτές ρητά στοχεύουν σε ευπάθειες λογισμικού (A. Shiravi, 2012)

1 . Vulnerability-leveraging attacks: Αυτές οι επιθέσεις στοχεύουν σε ευπάθειες λογισμικού. (Adobe printf buffer overflow, SMB stack overflow, SQL injection, Slowloris DoS attack)

2 . Auxiliary attacks: Αυτές οι συμπεριφορές δεν είναι εγγενώς κακόβουλες, αλλά συχνά αξιοποιούνται από τους επιτιθέμενους.(Reverse shell, Nmap scan, IRC command & control)

3 . Brute force attacks: Οι επιθέσεις αυτές δεν στοχεύουν σε συγκεκριμένα ευπάθειες λογισμικού, αλλά ελπίζουν να κατακλύσουν το στόχο με τον όγκο των επιθέσεων.(DDoS (Distributed Denial-of-Service) attack, SSH brute force login attempts)

Η αξιολόγηση επικεντρώνεται στις επιθέσεις της κατηγορίας (I), καθώς ο πρωταρχικός στόχος του Snort είναι ο εντοπισμός κακόβουλων χρήσεων.

Οι επιθέσεις της κατηγορίας (II) δεν είναι εγγενώς κακόβουλες και οι επιθέσεις της κατηγορίας (III) δεν στοχεύουν σε ευπάθειες λογισμικού- συνεπώς, δεν θεωρούνται πρωταρχικές ανησυχίες για τις αρχές σχεδιασμού του Snort. (Reiher, 2014)

Η διαχείριση του συνόλου δεδομένων γίνεται με τη χρήση της μονάδας MongoDB της Python, pymongo, για πακέτα και ροές.

4.3 Προσδιορισμός και ανάλυση ψευδώς αρνητικών αποτελεσμάτων

Τώρα αναλύουμε τέσσερις περιπτώσεις ψευδώς αρνητικών αποτελεσμάτων που παρουσιάστηκαν κατά τη χρήση του Snort για την ανάλυση του προαναφερθέντος συνόλου δεδομένων. Σε κάθε περίπτωση, περιγράφουμε την επίθεση, αναλύουμε τη βασική αιτία του ψευδώς αρνητικού αποτελέσματος και αντλούμε κάποιες πληροφορίες.

1 . Μια περίπτωση επίθεσης υπερχείλισης του buffer του Adobe printf

Η επίθεση:

Η επίθεση αυτή εκτελείται με την αποστολή ενός κακόβουλου αρχείου PDF στο σύστημα ηλεκτρονικού ταχυδρομείου των χρηστών-στόχων ως συνημμένο, το οποίο είναι μια ευρέως χρησιμοποιούμενη επίθεση κοινωνικής μηχανικής τακτικής. Στην περίπτωση που περιγράφεται στο σύνολο δεδομένων, ένα κακόβουλο PDF αποστέλλεται στον χρήστη του οποίου ο σταθμός εργασίας διαθέτει διεύθυνση IP 192.168.1.105. Ο σταθμός εργασίας χρησιμοποιεί το πρωτόκολλο ηλεκτρονικού ταχυδρομείου POP μέσω της θύρας 110 για να ανακτήσει το μήνυμα ηλεκτρονικού ταχυδρομείου από τον διακομιστή ηλεκτρονικού ταχυδρομείου (192.168.5.122) (A. Shiravi, 2012). Συγκρίνοντας αυτό με τη βασική αλήθεια, διαπιστώνουμε ότι αυτή η αλληλεπίδραση δεν χαρακτηρίζεται ως κακόβουλη στη βάση της αλήθειας του συνόλου δεδομένων, ενώ θα έπρεπε να είναι. Από την άλλη πλευρά, το Snort παράγει διάφορες ειδοποιήσεις που αντιστοιχούν στην κυκλοφορία. Σε αυτές περιλαμβάνονται δύο μοναδικές υπογραφές: "[139:1:1] (spp_sdf) SDF Combination Alert" (υποδεικνύοντας την παρουσία ευαίσθητων δεδομένων, όπως διευθύνσεις ηλεκτρονικού ταχυδρομείου) εμφανίζεται δύο φορές, και "[129:12:1] Διαδοχικά μικρά TCP τμήματα που υπερβαίνουν το όριο" εμφανίζεται 8 φορές. (υποδεικνύοντας μια ανωμαλία που εντοπίστηκε από τον επεξεργαστή stream5 του Snort).

Ωστόσο, δεν θεωρείται κακόβουλο για τα τμήματα TCP να είναι ασυνήθιστα μικρά, ακόμη και σε σχετικά μεγάλη ποσότητα. Ούτε αυτές οι ειδοποιήσεις δεν υποδηλώνουν την παρουσία επίθεσης υπερχείλισης ρυθμιστικού διαφράγματος, υποδεικνύοντας ένα ψευδώς αρνητικό αποτέλεσμα.

Ανάλυση αιτιών:

Οι ειδοποιήσεις του Snort δεν περιγράφουν, ούτε καν υπονοούν την παρουσία επίθεσης υπερχείλισης ρυθμιστικού διαφράγματος, Αντίθετα, αυτές οι ειδοποιήσεις δίνουν αόριστες πληροφορίες από τον προεπεξεργαστή ευαίσθητων δεδομένων (αρχικά το "Φίλτρο ευαίσθητων δεδομένων" ή SDF) και μικρά τμήματα TCP (τα οποία δεν έχουν σημασιολογική αξία για τους ανθρώπινους υπερασπιστές). Περαιτέρω διερεύνηση σε ένα εναλλακτικό σύνολο κανόνων (Emerging Threats (server, 2019)) αποκαλύπτει ότι αυτή η επίθεση είναι ανιχνεύσιμη από IDS που βασίζονται σε υπογραφές. Ο κανόνας είναι

διαθέσιμος ως "2800385 - ETPRO WEB_CLIENT Adobe Reader και Acrobat util.printf Stack Buffer Overflow". Δεδομένου ότι αυτό δεν περιλαμβάνεται στον προεπιλεγμένο κανόνα του Snort (σύνολο κανόνων), συμπεραίνουμε ότι δεν θεωρήθηκε σημαντικό για την γενική χρήση. Δεύτερον, το γεγονός ότι η επίθεση περιγράφει το σύνολο δεδομένων (A. Shiravi, 2012), αλλά δεν επισημαίνεται στο σύνολο δεδομένων, εγείρει ανησυχίες για την αξιοπιστία της βασικής αλήθειας στο πλαίσιο του συνόλου δεδομένων. Από αυτές τις παρατηρήσεις, αντλούμε δύο συμπεράσματα:

Συμπέρασμα 1: Πρέπει να εξεταστούν εναλλακτικά σύνολα κανόνων επειδή οι προγραμματιστές δεν μπορούν να υιοθετήσουν κανόνες που έχουν σχεδιαστεί από άλλους για δικό τους προεπιλεγμένο σύνολο.

Συμπέρασμα 2: Οι ειδοποιήσεις πρέπει να παρέχουν σημαντικές πληροφορίες που επιτρέπει στους υπερασπιστές να κατανοήσουν τη φύση μιας ειδοποίησης διότι δεν αρκεί η απλή αναφορά των συναγερμών, χωρίς να παρουσιάζονται χρήσιμες ή αυτονόητες πληροφορίες.

2 . Μια περίπτωση επίθεσης υπερχείλισης στοίβας SMB

Η επίθεση

Στην επίθεση υπερχείλισης στοίβας SMB, ένα κακόβουλο διαμορφωμένο πακέτο αποστέλλεται στο διακομιστή SMB. Το πακέτο υπερχειλίζει έναν απομονωτή στοίβας στον στόχο, επιτρέποντας σε έναν εισβολέα να εκτελέσει αυθαίρετο κώδικα. Σε αυτή την περίπτωση, ο επιτιθέμενος χρησιμοποιεί την ευπάθεια που είναι γνωστή ως MS08-067 κατά

του κεντρικού υπολογιστή στο 192.168.2.113. Χρησιμοποιώντας τη βάση δεδομένων ροής μας, έχουμε πρόσβαση στη σχετική κίνηση που χαρακτηρίζεται ως κακόβουλη. Συγκρίνοντας αυτό με το Snort, δεν βρίσκουμε καμία ειδοποίηση. Εξετάζοντας τους υπάρχον Snort κανόνες, βρίσκουμε εκπληκτικά αρκετούς κανόνες σχεδιασμένους για την ανίχνευση (και επισημαίνονται ρητά για το MS 08-067). Δυστυχώς, κανένας από αυτούς τους κανόνες δεν ενεργοποιήθηκε από την επίθεση στα δεδομένα. Ως εκ τούτου, αυτό αποτελεί ψευδώς αρνητικό αποτέλεσμα του IDS.

Ανάλυση αιτιών

Αυτό το ψευδώς αρνητικό προκαλεί ιδιαίτερη έκπληξη επειδή η υπερχείλιση στοίβας SMB που χρησιμοποιήθηκε σε αυτή την περίπτωση (δηλαδή η εκμετάλλευση της ευπάθειας MS08-067) είναι εξαιρετικά γνωστή στην κοινότητα και είναι καλά τεκμηριωμένη. Το γεγονός ότι το Snort δεν ανιχνεύει αυτή την επίθεση με την προεπιλεγμένη διαμόρφωση του συνόλου κανόνων είναι απροσδόκητο. Με τον ίδιο τρόπο, εξετάζουμε ένα άλλο IDS (συγκεκριμένα το Suricata (engine, 2018)). για να δούμε αν αυτό το πρόβλημα αφορά μόνο το Snort. Αφού ακολουθήσουμε την ίδια διαδικασία επεξεργασίας με πριν (χρησιμοποιώντας την προεπιλεγμένη ρύθμιση του Suricata, διαμόρφωση και το σύνολο κανόνων), το Suricata παρήγαγε πράγματι μια ειδοποίηση που αντιστοιχεί στην επίθεση. Συγκεκριμένα, η Suricata παρήγαγε ειδοποιήσεις ως "[1:2008705:5] ET NETBIOS Microsoft Windows NETAPI Stack Overflow Inbound - MS08-067 (15)". Δεδομένου ότι αυτή η ειδοποίηση περιγράφει με ακρίβεια την επίθεση, συμπεριλαμβανομένης της ευπάθειας στην οποία στόχευε, θεωρείται επαρκής για λόγους ανίχνευσης. Σημειώνοντας την διαφορά μεταξύ του αποτελέσματος του Snort και του Suricata, αντλούμε:

Συμπέρασμα 3: Ακόμη και εντός μιας κατηγορίας IDS (π.χ. ανοικτού κώδικα, ανιχνευτές κατάχρησης), διαφορετικά προϊόντα έχουν διαφορετικές ανίχνευτικές ικανότητες. Συνεπώς, είναι σημαντικό να δοκιμάζεται το καθένα ξεχωριστά, αντί να αντιμετωπίζεται μια κατηγορία IDS ως το άθροισμα κάθε προϊόντος.

3. Μια περίπτωση επίθεσης SQL injection:

α) Η επίθεση: Σε μια επίθεση SQL, ο αντίπαλος υποβάλλει

ένα ερώτημα με ειδικούς χαρακτήρες για να διαφύγει από την μη σαρωμένη είσοδο πεδίου. Οι συνήθεις εκδοχές της επίθεσης περιλαμβάνουν εισαγωγικά, αποσιωπητικά και άλλους ειδικούς χαρακτήρες. Εδώ, η επίθεση είναι εναντίον του διακομιστή ιστού που φιλοξενείται στη διεύθυνση 192.168.5.123. Εμείς συγκρίνουμε τη βασική αλήθεια με τις ειδοποιήσεις στη βάση δεδομένων ροής. Από τις 62 περιπτώσεις που χαρακτηρίστηκαν ως κακόβουλες, το Snort δημιούργησε ειδοποιήσεις μόνο για 4. Συγκεκριμένα, φέρουν την ένδειξη "[129:12:1] Διαδοχικά μικρά τμήματα TCP που υπερβαίνουν το όριο". Αυτή η ειδοποίηση δεν είναι αντιπροσωπευτική της επίθεσης οπότε το θεωρούμε ψευδώς αρνητικό.

Ανάλυση αιτιών:

Ορισμένες ειδοποιήσεις Snort έχουν γράφτηκαν σε προσπάθειες να ανιχνεύσουν αυτή την επίθεση, αλλά δεν ενεργοποιήθηκαν σε αυτή την περίπτωση. Ένα παράδειγμα είναι το "[1:19439:8] SQL 1 = 1 - πιθανή απόπειρα έγχυσης sql". Αυτός ο κανόνας αναζητά τη συμβολοσειρά "1=1" στο πακέτο, η οποία χρησιμοποιείται συνήθως μετά την αποφυγή της συμβολοσειράς εισόδου. Ωστόσο, αυτή η συμβολοσειρά είναι συγκεκριμένη για την υλοποίηση του exploit και όχι για την ίδια την ευπάθεια. Ως εκ τούτου, είναι σαφές ότι δεν ακολουθούσε τις οδηγίες της αρχής σχεδιασμού του Snort, (ii) να συλλαμβάνει ευπάθειες και όχι εκμεταλλεύσεις.

Μετά από αυτή την παρατήρηση, εξάγουμε την ακόλουθη διαπίστωση:

Συμπέρασμα 4 : Οι κανόνες IDS πρέπει να ακολουθούν τις αρχές που έχουν θεσπιστεί που καθοδηγούν την ανάπτυξή τους. Ως πρώτη γραμμή άμυνας, αυτό είναι ιδιαίτερα σημαντικό για τα IDS ανοικτού κώδικα, επειδή οι επιτιθέμενοι μπορούν να αναλύσουν τους κανόνες τους όταν προσπαθούν να τους παρακάμψουν χωρίς δοκιμή και σφάλμα εναντίον ζωντανών συστημάτων.

4 .Μια περίπτωση επίθεσης Slowloris DoS:

Η επίθεση

Η τελευταία επίθεση που εξετάζουμε είναι η εγκατάσταση και η εκτέλεση του λογισμικού Slowloris DoS. Σε αυτή την επίθεση, ένας επιτιθέμενος εγκαθιστά πολυάριθμες συνδέσεις σε έναν στόχο διακομιστή, μέχρι να γεμίσει κάθε υποδοχή που είναι διαθέσιμη στον στόχο, εμποδίζοντάς τον να δέχεται νέες συνδέσεις από κανονικούς χρήστες.Το Slowloris είναι το όνομα ενός κοινού λογισμικού που χρησιμοποιείται για μια τέτοια επίθεση. Σε αυτήν την περίπτωση, οι επιτιθέμενοι χρησιμοποιούν αρκετά από τους προηγούμενα παραβιασμένα θύματα τους για να ενισχύσουν την αποτελεσματικότητα της επίθεσης, στοχεύοντας τον διακομιστή ιστού στη διεύθυνση 192.168.5.122. Σύμφωνα με τις ετικέτες που περιλαμβάνονται στο σύνολο δεδομένων, τα θύματα που έχουν παραβιαστεί προκάλεσαν 1969 συνδέσεις στο στόχο κατά τη διάρκεια της επίθεσής τους. Σε αυτή την έκδοση του Slowloris, σημειώνουμε ότι τα πακέτα που αποστέλλονται δεν περιέχουν ωφέλιμα φορτία. Εξετάζοντας την έξοδο του Snort, παρατηρούμε βρίσκουμε αρκετές ειδοποιήσεις που δείχνουν τις επιθέσεις με την ένδειξη "[139:1:1] (spp_sdf) SDF Combination Alert". Όπως και με τις επίθεση Adobe printf, αυτή η ειδοποίηση δεν είναι αντιπροσωπευτική της πραγματικής επίθεσης σε εξέλιξη. Ως εκ τούτου, πρόκειται για άλλο ένα ψευδώς αρνητικό αποτέλεσμα.

Ανάλυση αιτιών:

Δεδομένου ότι το Snort δεν έχει κανόνες που έχουν σχεδιαστεί για την ανίχνευση επιθέσεων όπως η Slowloris, ψάχνουμε σε άλλους κανόνες που προτείνονται από την κοινότητα και θα μπορούσαν να είναι επαρκείς. Ένας σχετικός κανόνας, ο οποίος προτείνεται στο (GoodKingRene, 2019), βασίζεται σε ένα μοτίβο που εντοπίζεται από μια περίπτωση του Slowloris (συγκεκριμένα, εντοπίζει ότι η σύνδεση διατηρείται ζωντανή με επανειλημμένες στέλνοντας αυθαίρετες τιμές κεφαλίδας 'X-a: '). Δυστυχώς, έκδοση του Slowloris στα δεδομένα μας δεν παρουσιάζει το ίδιο μοτίβο, πράγμα που σημαίνει ότι ακόμη και αυτός ο κανόνας δεν θα έπιανε την επίθεση. Δεδομένου ότι αυτή η περίπτωση δεν χρησιμοποιεί ωφέλιμα φορτία μετά την αρχική σύνδεση, είναι σημαντικό να βρεθεί ένα άλλο μέσο για την ανίχνευση την επίθεση. Υπό το πρίσμα αυτό, αντλούμε την ακόλουθη διαπίστωση:

Συμπέρασμα 5 : Τα IDS που βασίζονται σε υπογραφές περιορίζονται από την εξάρτησή τους από την επιθεώρηση του ωφέλιμου φορτίου των πακέτων, επειδή ορισμένες επιθέσεις δεν χρησιμοποιούν ωφέλιμα φορτία.

Κεφάλαιο 5 Αποτελέσματα και Συζήτηση

5.1 Σχέδιο νέων αρχών

Στην παρούσα ενότητα παρουσιάζονται τρεις αρχές που θα καθοδηγήσουν το σχεδιασμό των μελλοντικών συστημάτων ανίχνευσης εισβολών (IDS).

Αρχή 1 (σαφείς προδιαγραφές):

Τονίζει την ανάγκη προσδιορισμού των δυνατοτήτων και των αδυναμιών ενός IDS όσον αφορά τους τύπους τρωτών σημείων ή επιθέσεων από τις οποίες αμύνεται, την είσοδο που απαιτεί και τις κατευθυντήριες αρχές του. Πιο συγκεκριμένα υπογραμμίζει τη σημασία των ειδοποιήσεων, ώστε να έχουν νόημα για τους υπερασπιστές. Προηγούμενη μελέτη (J. D. Mireles, 2016) έδειξε ότι η σημασία της κατανόησης της σημασιολογίας των ειδοποιήσεων, ή περισσότερο συγκεκριμένα της έννοιας των αφηγήσεων επίθεσης, αποτελεί σημαντική προσέγγιση για την κατανόηση των ειδοποιήσεων. Δηλαδή, η σημασιολογία της ειδοποίησης είναι σημαντική για την κατανόηση της κατάστασης απειλής και την ανταπόκριση στην επίθεση κυβερνοχώρου. Χωρίς ουσιαστική σημασιολογία συναγερμών, οι ανθρώπινοι χειριστές δεν θα είναι σε θέση να κατανοήσουν γρήγορα και να ανταποκριθούν στις επιθέσεις.

Υπό το πρίσμα αυτής της παρατήρησης, σημειώνουμε ότι πολλές επιθέσεις στοχεύουν σε γνωστές ευπάθειες, για τις οποίες υπάρχουν επιδιορθώσεις και συχνά δημοσιεύονται κατά τη στιγμή της αποκάλυψής τους. Μεγάλο μέρος των του χρόνου ανάλυσης για τέτοιες επιθέσεις θα μπορούσε να μειωθεί αν τα ευάλωτα συστήματα είχαν ήδη επιδιορθωθεί. Με άλλα λόγια, ένα σύστημα ανίχνευσης εισβολών που γνωρίζει το λογισμικό καταστάσεις/εκδόσεις που εκτελούνται σε ένα εταιρικό δίκτυο μπορεί να είναι σε θέση να

προβλέψει εάν μια επίθεση θα είναι επιτυχής. Αυτό μπορεί να παρέχει ένα μέσο για την απομάκρυνση των περιττών ειδοποιήσεων και τη μείωση των αλληλεπιδράσεων που απαιτείται μεταξύ των συστημάτων ανίχνευσης εισβολών και των ανθρώπινων χειριστών.

Αρχή 2 (IDS-defender interface):

Τα IDS πρέπει να παρέχουν ειδοποιήσεις κατανοητές από τον χρήστη. Μια προσέγγιση για την επίτευξη αυτού του στόχου είναι να γνωρίζουν τα IDS τις στάσεις της στοίβας λογισμικού (π.χ, την παρουσία ορισμένων ευπαθειών). Με αυτόν τον τρόπο, τα IDS μπορούν να επιτύχουν μεγαλύτερη ικανότητα να βοηθήσουν τους αμυνόμενους να κατανοήσουν και να ανταποκριθούν στις επιθέσεις στον κυβερνοχώρο.

Επίσης δεδομένου ότι τα συστήματα ανίχνευσης εισβολών συχνά παράγουν περισσότερες ειδοποιήσεις από ό,τι μπορεί να παρακολουθούν οι αμυνόμενοι, είναι σημαντικό να παρουσιάζονται οι πιο κρίσιμες ειδοποιήσεις. Για το σκοπό αυτό, προτείνουμε τον καθορισμό προτύπων με τα οποία μπορεί να ποσοτικοποιηθεί η έννοια του αντίκτυπου της εισβολής. Με το αυτή την έννοια, οι ειδοποιήσεις εισβολής μπορούν να αναφέρουν τη χειρότερη ή καλύτερη περίπτωση εκτιμήσεις επιπτώσεων για μια δεδομένη επίθεση.

Αρχή 3 (Ιεράρχηση συναγερμών):

Τα ίδια τα IDS θα πρέπει να δίνουν προτεραιότητα στις ειδοποιήσεις προς τους αμυνόμενους. Προσεγγίσεις για την επίτευξη μπορεί να περιλαμβάνουν ποσοτικοποίηση του αντίκτυπου της εισβολής ή περιγραφή αφηγήσεις επιθέσεων, όπως αναφέρθηκε παραπάνω. Αυτό θα επέτρεπε την ιεράρχηση της απόκρισης στις ειδοποιήσεις.

5.2 Συζήτηση

Η παρούσα μελέτη έχει τους ακόλουθους περιορισμούς, οι οποίοι εξυπηρετούν ως κίνητρα για μελλοντικές μελέτες. Πρώτον, η μεθοδολογία μας στοχεύει να συσχετίσει πακέτα με ροές για την τυποποίηση μιας σύγκρισης μεταξύ διαφόρων IDS. Αρκετά από τα πακέτα στο σύνολο δεδομένων που χρησιμοποιήθηκαν στη μελέτη περίπτωσης δεν αντιστοιχούσαν με μοναδικό τρόπο σε ροές, οπότε θεωρήθηκαν ότι ανήκουν σε όλες τις ροές που αντιστοιχούσαν την 5-σύζευξη, με την απαίτηση χρονοσφραγίδας χαλαρή.

Δεύτερον, η μελέτη περίπτωσης περιορίζεται στην ανάλυση Snort, ενός ανιχνευτή κακόβουλης χρήσης. Ως εκ τούτου, δεν περιλαμβάνει ανιχνευτές ανωμαλιών (π.χ. IBM QRadar (qradar:, 2019) και Flowmon ADS (confidently, 2019)), οι οποίοι ενδέχεται να μην αντιστοιχούν άμεσα στο Snort. Επιπλέον, η μελέτη μας επικεντρώνεται στο Snort και πιο συγκεκριμένα στο προεπιλεγμένο σύνολο κανόνων, πράγμα που σημαίνει ότι πιθανότατα μας ξέφυγαν καλύτερες ανιχνευτικές δυνατότητες άλλων δημοφιλών συνόλων κανόνων (όπως τα (engine, 2018) και (server, 2019)).

Τρίτον, το σύνολο δεδομένων που αναλύουμε έχει επίσης ορισμένους περιορισμούς. Κατά τη διάρκεια της ανάλυσης του συνόλου δεδομένων, παρατηρούμε τα εξής προβλήματα με τα δεδομένα. (i) Ορισμένες επιθέσεις οι οποίες περιγράφηκαν στο αρχικό έγγραφο που δημοσιεύει τα δεδομένα δεν εμφανίστηκαν να επισημαίνονται ως τέτοιες στο σύνολο δεδομένων. Αυτό καθιστούσε δύσκολη την να προσδιοριστεί επακριβώς ποιες προειδοποιήσεις θα πρέπει να θεωρηθούν σχετικές για ορισμένες επιθέσεις, όπως η επίθεση Adobe printf. (ii) Ορισμένες ροές επισημάνθηκαν ως κακόβουλες δύο φορές εντός του συνόλου δεδομένων. Αυτό θα μπορούσε να επηρεάσει τη μέτρηση των αληθώς θετικών αποτελεσμάτων. Η παρούσα εργασία δεν επηρεάζεται από αυτό το ζήτημα, αλλά εκείνες που μετρούν ποσοστό ανίχνευσης μπορεί να έχουν επηρεαστεί (π.χ. (E. Ficke, 2018)).

Τέταρτον, μεγάλο μέρος της μεθοδολογίας μας εξακολουθεί να λειτουργεί χειροκίνητα, οπότε η εφαρμογή της σε διάφορα IDS και σύνολα δεδομένων απαιτεί κάποιο χρόνο για τη διεξαγωγή των μεταβάσεων μεταξύ κάθε σταδίου, καθώς και για την τελική αναζήτηση της βάσης δεδομένων.

Κεφάλαιο 6 Συμπεράσματα

Εξηγήσαμε τη σημασία της κατανόησης της βασικής αίτιας των ψευδώς αρνητικών αποτελεσμάτων της ανίχνευσης εισβολής. Παρουσιάσαμε μια μεθοδολογία για το σκοπό αυτό και αναφέραμε μια μελέτη περίπτωσης σχετικά με την εφαρμογή της μεθοδολογίας για την ανάλυση των βαθύτερων αιτιών του Snort σε σχέση με ένα πραγματικό σύνολο δεδομένων κυβερνοεπιθέσεων. Αντλήσαμε χρήσιμες πληροφορίες από αυτή την προκαταρκτική μελέτη. Ελπίζουμε ότι αυτή η μελέτη θα εμπνεύσει πολλές μελλοντικές έρευνες για τον σχεδιασμό των συστημάτων ανίχνευσης εισβολών επόμενης γενιάς.

Βιβλιογραφία

2012 Has Delivered Her First Giant Data Breach, January. (2012). Ανάκτηση από http://www.infosecisland.com/blogview/19432-2012-Has-Delivered-Her-First-Giant-DataBreach.html

A Few Wrinkles Are Etching Facebook, Other Social Sites, USA Today. (2011). *A Few Wrinkles Are Etching Facebook, Other Social Sites, USA Today.* Ανάκτηση από http://www.usatoday.com/printedition/life/20090115/socialnetworking15_st.art.htm

A. Shiravi, H. S. (2012). *Toward developing a systematic approach to generate benchmark datasets for intrusion detection.* Computers & Security.

A. Tripathi and A. Mishra. (2011). *Cloud Computing Security Considerations Interface.* Xi'an, China: International Conference on Signal Processing, Communications and Computing.

Ahmad, T. &. (2015). *Cloud Computing Adoption Issues and Applications in Developing Countries: A Qualitative Approach.* Int. Arab. J. e Technol.

Alhenaki, L. A. (2019). *A survey on the security of cloud computing.* 2nd international conference on computer applications & information security (ICCAIS).

Alotaibi, A. F. (2021). *A comprehensive survey on security threats and countermeasures of cloud computing environment.* Turkish Journal of Computer and Mathematics Education.

Amazon.com Server Said to Have Been Used in Sony Attack. (2011). Ανάκτηση από http://www.bloomberg.com/news/2011-05-13/sony-network-said-to-have-been-invaded-by-hackersusing-amazon-com-server.html

Anita, R. B. (2017). *A survey on data breach challenges in cloud computing security: Issues and threats.* Kollam, India: International Conference on Circuit ,Power and Computing Technologies (ICCPCT). doi:10.1109/ICCPCT.2017.8074287

Attaran, M. (2017). *Cloud Computing Technology: Leveraging the Power of the Internet to Improve Business Performance.* CSUSB ScholarWorks. doi:https://doi.org/10.58729/1941-6679.1283

Axelsson, S. (2000). *Intrusion detection systems: A survey and taxonomy.* Technical report.

Baharuddin, A. D. (2021). Implementation of cloud computing system in learning system development in engineering. Στο *International Journal of Education in Mathematics, Science, and* (σσ. 728-740). Ismail Sahin. doi:https://doi.org/10.46328/ijemst.2114

Bhowmik, S. (2017). *Cloud Computing.* Cambridge: Cambridge University.

CERT. (2012). Insider Threats Related to Cloud Computing. CERT. Ανάκτηση από http://www.cert.org/

CERT Coordination Center at Carnegie Mellon University. (2011). CyberSecurity Watch Survey.

CERT Coordination Center, Denial of Service. (2023). *CERT Coordination Center, Denial of Service*. Ανάκτηση από http://www.packetstormsecurity.org/distributed/denial_of_service.htm

Chen, A. L.-C. (2012). *Cloud computing as an innovation.* International Journal of Information Management.

confidently, D. w. (2019). *Deal with security threats and operational issues confidently.* Ανάκτηση από https://www.flowmon.com/en/products/flowmon/anomaly-detection-system

DataLossDB Open Security Foundation. (2015). Ανάκτηση από http://datalossdb.org/statistics

DDoS Attack Rains Down on Amazon Cloud. (2009). DDoS Attack Rains Down on Amazon Cloud. Ανάκτηση από http://www.theregister.co.uk/2009/10/05/amazon_bitbucket_outage/

Dhore, A. S. (2012). *"CIDT: Detection of Malicious Code Injection Attacks on Web Application.* International Journal of Computer Applications.

Dropbox. (2012). *Yes, We Were Hacked.* Ανάκτηση από https://gigaom.com/cloud/dropbox-yes-we-were-hacked/

E. Ficke, K. M. (2018). *Characterizing the effectiveness of network-based intrusion detection systems,.* MILCOM.

Eckhardt, S. H. (2014). *Organizational cloud service adoption: a scientometric and content-based literature analysis.* Journal of Business Economics.

engine, “. —o. (2018). *“Suricata — open source ids / ips / nsm engine.* Ανάκτηση από ” https://suricata-ids.org/download/

G. Feuerlicht, L. B. (2015). *Cloud computing adoption: what are the issues?* System Integration.

GoodKingRene, D. T. (2019). *“Ids snort rule to catch slowloris.* Ανάκτηση από https://security.stackexchange.com/questions/174454/ids-snort-rule-to-catch-slow-loris

Grance, W. J. (2018). *Guidelines on Security and Privacy in Public Cloud Computing.* National Institute of Standards and Technology.

Habjan, K. B. (2017). *Cloud computing adoption business model factors: does enterprise size matter?* Engineering Economics.

Hogben, D. C. (2016). “Cloud Computing Benefits, Risks and Recommendations for Information Security. The European Network and Information Security Agency (ENISA).

Iacono, .. N. (2009). *Vulnerable Cloud: SOAP Message Security Validation Revisited.* Los Angeles: IEEE International Conference on Web Services.

Infection, V. t. (2008). *Visitors to Sony PlayStation Website at Risk of Malware Infection.* Ανάκτηση από https://www.sophos.com/en-us/press/press-releases/2008/07/playstation

J. D. Mireles, J. C. (2016). *Extracting attack narratives from traffic datasets.* n Proc. CyCon U.S.

J. Gao, G. H. (2006). *Anomaly detection of network traffic based on wavelet packet.*

J. Song, H. T. (2008). *A generalized feature extraction scheme to detect 0-day attacks via ids alerts.* International Symposium on Applications and the Internet.

K. Zunnurhain and S. Vrbsky. (2010). *“Security Attacks and Solutions in Clouds.* Indianapolis: 2nd IEEE International Conference on Cloud Computing Technology and Science.

Lin, A. &. (2012). *Cloud computing as an innovation: Percepetion, attitude, and adoption.* International journal of information management.

LinkedIn Blog. (2012). *An Update on LinkedIn Member Passwords Compromised,.* LinkedIn. Ανάκτηση από https://blog.linkedin.com/2012/06/06/linkedin-member-passwords-compromised

M. Jensen, J. Schwenk, N. Gruschka, and L. L. Iacono. (2009). *On Technical Security Issues in Cloud.* Bangalore.

Masood, A. L. (2020). *Security and privacy challenges in connected vehicular cloud computing.* IEEE Communications Surveys & Tutorials.

Michael, D. I. (2022). *Implementation of Enterprise Architecture in Cloud Computing Companies.* inkron: jurnal dan penelitian teknik informatika,.

Modak, S. M. (2021). *Vulnerability of Cloud: Analysis of XML Signature Wrapping Attack and Countermeasures.* Springer Singapore: In Proceedings of International Conference on Frontiers in Computing and Systems: COMSYS 2020.

Mohammed, C. M. (2021). *Sufficient comparison among cloud computing services: IaaS, PaaS, and SaaS.* A review. International Journal of Science and Business.

Mudholkar, P. P. (2012). *"Cloud Market Cogitation and Techniques to Averting SQL Injection for University Cloud.* " International Journal of Computer Technology and Applications.

Mukundha, C. and Vidyamadhuri, K. (2017). *Cloud Computing Models: A Survey", Advances in Computational Sciences and Technology.* Research India Publications. Ανάκτηση από https://www.ripublication.com/acst17/acstv10n5_09.pdf

N. Lu, S. M. (2012). *Integrated fuzzy gnp rule mining with distance-based classification for intrusion detection system.* IEEE SMC.

N. Provos, M. A. (2018). *"Cybercrime 2.0: When the Cloud Turns Dark.* ACM Communications.

Oliveira, T. T. (2014). *Assessing the determinants of cloud computing adoption: An analysis of the manufacturing and services sectors.* Information & management, .

Parast, F. K. (2022). *Cloud computing security: A survey of service-based models.* Computers & Security.

Paxson, R. S. (2010). *Outside the closed world:.* IEEE symposium on security and privacy.

Peter Mell, T. G. (2011). The NIST Definition of Cloud Computing. (Special Publication 800-145). Gaithersburg: National Institute of Standards and Technology. Ανάκτηση από https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf

Pras, A. S. (2011). *"Flow-based intrusion detection," in IFIP/IEEE.*

qradar:, ". (2019). *"Ibm qradar:.* Ανάκτηση από " https://www.ibm.com/security/security-intelligence/qradar

Reiher,]. J. (2014). *A taxonomy of ddos attack and ddos defense mechanisms.* ACM SIGCOMM Computer Communication.

Repschlaeger, J. E. (2013). *Cloud computing adoption: an empirical study of customer preferences among start-up companies.* Electronic markets.

Researchers Demo Cloud Security Issue With Amazon AWS Attack. (2011). *Researchers Demo Cloud Security Issue With Amazon AWS Attack.* Ανάκτηση από http://www.pcworld.idg.com.au/article/405419/researchers_demo_cloud_security_issue_amazon_aws_attack/

S. Gajek, M. J. (2019). *"Analysis of Signature Wrapping Attacks and Countermeasures.* Miami: International Conference on Web Services.

server, W. t. (2019). *Welcome to the emerging threats rule server.* Ανάκτηση από https://rules.emergingthreats.net/

Sophos Security Threat Report . (2012). Ανάκτηση από http://www.sophos.com/

Symantec. (2012). Data Breach Trends & Stats. Ανάκτηση από http://www.indefenseofdata.com/data-breach-trendsstats/

Symantec Internet Security Threat Report. (2011). *Symantec Internet Security Threat Report.*

Symantec White Paper. (2011). *Web Based Attacks.*

system., ". -n. (2018). *"Snort - network intrusion detection & prevention system.* Ανάκτηση από https://www.snort.org/downloads

T. Dillon, C. W. (2010). *Cloud computing: issues and challenges.* Perth, Australia: 4th IEEE International Conference on Advanced Information Networking and Applications.

T. Oliveira, M. T. (2015). *Assessing the determinants of cloud computing adoption: an analysis of the manufacturing and services sectors.* Information and Management.

T. Roth. (2011). *Breaking Encryptions Using GPU Accelerated Cloud Instances.* Black Hat Technical Security Conference.

Thunder in the Cloud: $6 Cloud-Based Denial-of-Service Attack. (2010). Thunder in the Cloud: $6 Cloud-Based Denial-of-Service Attack. Ανάκτηση από http://blogs.computerworld.com/16708/thunder_in_the_cloud_6_cloud_based_denial_of_service_att

Vairagkar, S. (2023). *10 Key Benefits of Adopting Cloud Computing for Businesses.* xurixdigital. Ανάκτηση από https://www.hurix.com/10-key-benefits-of-adopting-cloud-computing-for-businesses/

Vrbsky, K. Z. (2015). *Security Attacks and Solutions in Clouds.* Indianapolis: Conference on Cloud Computing Technology and Science.

W. A. Jansen. (2011). "Cloud Hooks: Security and Privacy Issues in Cloud Computing. Στο *"Cloud Hooks: Security and Privacy Issues in Cloud Computing* (σσ. pp. 1–10). Koloa, Hawaii.

Web Application Attack Report For The Second Quarter of 2012. (2012). *Web Application Attack Report For The Second Quarter of 2012.* Ανάκτηση από https://www.firehost.com/company/newsroom/web-application-attack-report-second-quarter-2012

Yang, S. J. (2020). *Design Issues of a Hybrid Wrapping Attack Protecting Scheme in Cloud Computing Environment.* In Advances in E-Business Engineering for Ubiquitous Computing: Proceedings of the 16th International Conference on e-Business Engineering (ICEBE 2019).

Yang, Wenyam. (2017). *A Brief Analysis of Development Situations and Trend of Cloud Computing.* Ανάκτηση από http://iopscience.iop.org/article/10.1088/1755-1315/100/1/012032/pdf

Zaki, D. J. (2011). "Security Issues in Cloud Computing and Countermeasures,. Στο *International Journal of Engineering Science and Technology* (σσ. pp. 2672-2676).