ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Πρόγραμμα Μεταπτυχιακών Σπουδών

«ΔΙΚΑΙΟ ΚΑΙ ΤΕΧΝΟΛΟΓΙΕΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ»

Ακαδημαϊκό έτος 2024-2025

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ
του Σπυρίδωνος Τρουγκάκου, Α.Μ.:ΜΔΙ2354

ΨΗΦΙΑΚΗ ΕΓΚΛΗΜΑΤΟΛΟΓΙΑ ΣΤΟ ΝΕΦΟΣ – ΝΕΟΤΕΡΕΣ ΕΞΕΛΙΞΕΙΣ
LATEST DEVELOPMENTS IN CLOUD FORENSICS

Επιβλέπων:

Καθηγητής Στέφανος Γκρίτζαλης

Πειραιάς, Μάϊος 2025

[Η σελίδα αυτή είναι σκόπιμα λευκή.]

Πρόλογος και ευχαριστίες

Η παρούσα διπλωματική εργασία εκπονήθηκε στο πλαίσιο του μεταπτυχιακού προγράμματος σπουδών "Δίκαιο και Τεχνολογίες Πληροφορικής και Επικοινωνιών" του Πανεπιστημίου Πειραιά. Η ολοκλήρωσή της δεν θα ήταν εφικτή χωρίς την ανεκτίμητη καθοδήγηση και υποστήριξη του καθηγητή μου, Στέφανου Γκρίτζαλη. Η συμβολή του ξεπέρασε τα όρια της απλής επιτήρησης της διπλωματικής εργασίας και ήταν καθοριστική σε όλα τα στάδια της εκπαιδευτικής διαδικασίας, από την αρχή μέχρι την ολοκλήρωσή της, στο πλαίσιο του προγράμματος σπουδών.

Για την καθοδήγηση του, την πολύτιμη έμπνευση που μου προσέφερε, καθώς και για την παρακίνηση να ξεπεράσω τα όρια της "κανονικότητας", οφείλω ένα βαθύ ευχαριστώ.

ΤΡΟΥΓΚΑΚΟΥ ΣΠΥΡΙΔΩΝΟΣ
Τμήμα Ψηφιακών Συστημάτων
ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

[Η σελίδα αυτή είναι σκόπιμα λευκή.]

Πίνακας Περιεχομένων

Ακρωνύμια

AWS	Amazon Web Services
IaaS	Infrastructure as a Service
PaaS	Platform as a Service
SaaS	Software as a Service
GDPR	General Data Protection Regulation
ISO	International Organization for Standardization
NIST	National Institute of Standards and Technology
IoT	Internet of Things
DDoS	Distributed Denial of Service
RBAC	Role-Based Access Control
ABAC	Attribute-Based Access Control
ELK	Elasticsearch, Logstash, Kibana
CFLOG	Cloud Forensic Logging
FRM	Forensic Readiness Model
SLAs	Service Level Agreements
HIPAA	Health Insurance Portability and Accountability Act
ACPO	Association of Chief Police Officers
FRF	Forensic Readiness Framework
CLOUD Act	Clarifying Lawful Overseas Use of Data Act
CFeS	Cloud Forensic-enabled Services
DFRWS	Digital Forensics Research Workshop
CSA CCM	Cloud Security Alliance Cloud Controls Matrix
DFS	Distributed File System

Περίληψη

Η παρούσα μεταπτυχιακή εργασία εξετάζει το συνεχώς εξελισσόμενο πεδίο της εγκληματολογικής διερεύνησης στο υπολογιστικό νέφος (cloud forensics), στο πλαίσιο της ψηφιακής εγκληματολογίας.

Καθώς το cloud computing καθίσταται θεμέλιο της σύγχρονης ψηφιακής υποδομής, αναδύονται νέες προκλήσεις που απαιτούν τροποποιήσεις των υφιστάμενων παραδοσιακών μεθοδολογιών .

Η έρευνα αναλύει τις τεχνικές, νομικές και οργανωτικές διαστάσεις της εγκληματολογικής έρευνας σε περιβάλλοντα cloud. Εξετάζει ζητήματα όπως η πολυμίσθωση, η διασπορά των δεδομένων, η συνεργασία με παρόχους και η δικαιοδοσία, συγκρίνοντάς τα με τα παραδοσιακά μοντέλα ψηφιακής εγκληματολογίας. Μέσα από μελέτες περιπτώσεων και αξιολόγηση υφιστάμενων εργαλείων, αναδεικνύεται η σημαντική έλλειψη στον τομέα ετοιμότητας και προτείνονται πλαίσια λύσεων που συνδυάζουν τόσο την τεχνική διάσταση όσο και την εναρμόνιση στα υφιστάμενα νομικά πλαίσια. Τονίζεται η ανάγκη προσαρμογής των μεθόδων εγκληματολογικής διερεύνησης ώστε να διασφαλίζεται η ακεραιότητα, η νομιμότητα, ενώ αναδεικνύεται και η συνεχόμενη εξέλιξή του περιβάλλοντος της ψηφιακής εγκληματολογίας στο νέφος.

Λέξεις Κλειδιά: ψηφιακή εγκληματολογία cloud, ψηφιακά αποδεικτικά στοιχεία, εγκληματολογική ετοιμότητα, ακεραιότητα δεδομένων, νομική συμμόρφωση, κυβερνοασφάλεια.

Abstract

This postgraduate dissertation examines the ever-evolving field of forensic investigation within cloud computing environments, in the broader context of digital forensics.

As cloud computing is becoming a cornerstone of modern digital infrastructure, new challenges have emerged that demand modifications to existing traditional methodologies.

The research analyzes the technical, legal, and organizational dimensions of conducting forensic investigations in cloud environments. It explores issues such as multitenancy, data dispersion, provider cooperation, and jurisdiction, comparing them with traditional digital forensic models. Through case studies and the evaluation of existing tools, it highlights the significant lack of readiness in the field and proposes solution frameworks that combine both technical approaches and harmonization with current legal standards. The study emphasizes the necessity of adapting forensic investigation methods to ensure data integrity and legal compliance, while also underlining the continuous evolution of the cloud forensics landscape.

Keywords: cloud forensics, digital evidence, forensic readiness, data integrity, legal compliance, cybersecurity.

1 ΕΙΣΑΓΩΓΗ

1.1 Τεχνολογικές εξελίξεις στο ψηφιακό περιβάλλον

Είναι πλέον αυτονόητο πως το σύγχρονο ψηφιακό περιβάλλον έχει υποστεί μια σειρά από αλλαγές που έχουν μεταβάλει την ίδια του την υπόσταση. Κατά τη διάρκεια των τελευταίων ετών, πραγματοποιήθηκε η μετάβαση στο πλαίσιο των υπηρεσιών υποδομών από τη λογική μιας απλής δομής, την οποία διαχειρίζεται ένας πάροχος υπηρεσιών, σε μια κεντρικά διαχειριζομένη υποδομή που αποτελεί τη ραχοκοκαλιά του συνόλου των υπηρεσιών που απολαμβάνει το κοινό.

Το ίδιο το cloud έχει εξελιχθεί από μια υπηρεσία που παλαιότερα θεωρούνταν ενδιαφέρουσα αλλά ενδεχομένως άγνωστο πεδίο, σε μια υπηρεσία που πλέον θεωρείται αυτονόητη λύση. Φυσικά, το συνεχώς μειούμενο κόστος αρχικής επένδυσης και λειτουργίας έπαιξε σημαντικό ρόλο σε αυτή τη μετάβαση, αλλά καθοριστική υπήρξε και η συμβολή των τεχνολογικών εξελίξεων, που οδήγησαν σε μια στροφή προς την ευκολία χρήσης.

Κάθε νέα τεχνολογική εξέλιξη δημιουργεί ευκαιρίες τόσο για το κοινό όσο και για όσους επιδιώκουν να τις αξιοποιήσουν, και το cloud δεν αποτελεί εξαίρεση. Αυτή η εξέλιξη, καθώς και οι τρόποι τεκμηρίωσης πιθανών συμβάντων, είναι το αντικείμενο που θα επιχειρηθεί να καταγραφεί και να αναλυθεί.

Εν τέλει, στόχος είναι η τεκμηρίωση προβλημάτων και η δημιουργία ενός ξεκάθαρου πλάνου δράσης και αντιμετώπισης ζητημάτων στην ψηφιακή εγκληματολογία, στο περιβάλλον του cloud.

1.1.1 Ρόλος της ψηφιακής εγκληματολογίας στο σύγχρονο ψηφιακό περιβάλλον.

Αυτόματα τίθεται το ερώτημα: Είναι πραγματικά τόσο σημαντική η ψηφιακή εγκληματολογία και, αν ναι, ποια είναι τα σημάδια που το αποδεικνύουν; Απλά η εξέλιξη της τεχνολογίας και η αντίστοιχη χρήση της από το ευρύ κοινό, δεν μπορεί να αποτελεί απόδειξη γι' αυτό. Η αλήθεια θα πρέπει να αναζητηθεί στη φύση της ίδιας της ψηφιακής

εγκληματολογίας, το έργο που επιτελείται καθώς και στα ερωτήματα που προκύπτουν από αυτή.

Η ψηφιακή εγκληματολογία είναι θεμελιώδους σημασίας, καθώς ασχολείται με την ανάλυση ψηφιακών ιχνών σε εγκληματικές ενέργειες. Η αύξηση της εγκληματικότητας στον ψηφιακό χώρο, κάτι που είναι αναμενόμενο, την καθιστά ιδιαίτερα σημαντική, καθώς αποτελεί αναπόσπαστο κομμάτι της αντιμετώπισης των απειλών.

Η διαδικασία της ψηφιακής εγκληματολογίας περιλαμβάνει υποθέσεις που αφορούν τόσο τον πραγματικό όσο και τον ψηφιακό κόσμο. Αυτό σημαίνει ότι ο στόχος της δεν είναι απλώς η μελέτη ψηφιακών επιθέσεων, αλλά μπορεί να συνεισφέρει σε υποθέσεις που διαθέτουν τόσο ψηφιακή διάσταση όσο και φυσική υπόσταση. Έτσι όπως οι υπολογιστές κάθε μορφής έχουν ενσωματωθεί στην καθημερινότητά μας και παίζουν ουσιαστικό ρόλο σε κάθε μας δραστηριότητα, έτσι και η ψηφιακή εγκληματολογία ακολουθεί αυτή την πορεία. Υποθέσεις αστικού και ποινικού δικαίου μπορεί να απαιτούν στοιχεία που εμπίπτουν στον τομέα της ψηφιακής εγκληματολογίας, γεγονός που καθιστά το εύρος και την ποικιλία των υποθέσεων τεράστια. (Kävrestad, et al., 2024)

Επιπλέον, δεν θα πρέπει να παραλειφθεί πως συντελούνται σημαντικές αλλαγές και στον τομέα των προσωπικών δεδομένων. Αυτό έχει ως αποτέλεσμα την ανάγκη θέσπισης κανόνων, και φυσικά, με την ύπαρξη κανόνων, υπάρχει και η πιθανότητα παραβίασης τους. Και σε αυτό το πλαίσιο, η ψηφιακή εγκληματολογία βρίσκει ουσιαστικό πεδίο εφαρμογής. (Kävrestad, et al., 2024)

Τέλος, έχει ενδιαφέρον να επισημανθεί πως ένα αξιόλογο κριτήριο σημαντικότητας της ψηφιακής εγκληματολογίας στο cloud, είναι η τάση για έρευνα στον χώρο. Είναι πολύ ενδιαφέρον να παρατηρήσει κανείς ότι όχι μόνο μεταβάλλεται το πλήθος των μελετών στο αντικείμενο, αλλά αλλάζει και ο προσανατολισμός τους. Έτσι, ενώ στις αρχές της δεκαετίας του 2010 ο κύριος στόχος ήταν η διατήρηση και η προστασία των ίδιων των δεδομένων, προς το τέλος της ίδιας δεκαετίας οι στόχοι γίνονται πλέον πολυδιάστατοι. Περιλαμβάνουν τη μελέτη τρόπων αντιμετώπισης προβλημάτων, τον ορισμό διαδικασιών και την υλοποίηση των βέλτιστων πρακτικών. (Purnaye & Kulkarni, 2022)

1.1.2 Αναγκαιότητα έρευνας

Μπορεί εύκολα να γίνει αποδεκτό ότι υπάρχουν εξελίξεις, αλλά δεν είναι αυτονόητο ότι υπάρχει και ανάγκη για έρευνα και λύσεις στον τομέα, τουλάχιστον μια ανάγκη ικανή να δημιουργήσει την τάση προς ερευνά. Ποιος ορίζει το πρόβλημα και ποιος καθορίζει την ανάγκη για λύση; Και, εν τέλει, πόσο εύκολο είναι η έρευνα να είναι ουσιαστική, με πρακτική εφαρμογή, και όχι απλώς ακαδημαϊκού επιπέδου;

Το αρχικό κίνητρο είναι συχνά ο παράγοντας της σημασίας των αποτελεσμάτων, σε συνδυασμό με το έργο ή κόστος που απαιτείται για την εξαγωγή τους. Όταν αναφερόμαστε σε αποτελέσματα, εννοούμε το πλήθος των πιθανών περιπτώσεων που απαιτούν έρευνα σε ένα περιστατικό και το πόσο δύσκολο είναι να επιτευχθεί ο προσδοκώμενος στόχος. Αυτοί οι δύο παράγοντες λειτουργούν συνεργατικά, και καθώς αυξάνονται και οι δύο, δημιουργείται η ανάγκη για βελτίωση.

Η αύξηση της πολυπλοκότητας των συστημάτων, σε συνδυασμό με την ποικιλομορφία τους, δείχνει ότι πλέον η συλλογή ψηφιακών πειστηρίων γίνεται ολοένα και πιο δύσκολη. Επιπλέον, εμφανίζονται νέες μορφές ψηφιακού εγκλήματος, οι οποίες απαιτούν αντίστοιχα νέες μεθόδους αντιμετώπισης και έρευνας (SentinelOne, 2025). Τέλος, δεν θα πρέπει να παραβλέψουμε και τις αλλαγές στο νομικό και ρυθμιστικό πλαίσιο, οι οποίες επηρεάζουν την ευκολία λήψης δεδομένων.

Αυτοί οι παράγοντες, από μόνοι τους, αρκούν για να στοιχειοθετήσουν την ανάγκη για περαιτέρω έρευνα. Πέρα όμως από αυτούς, δεν μπορούμε να αγνοήσουμε και τα εγγενή προβλήματα του τομέα. Με την πάροδο του χρόνου, αποκαλύπτονται οι αδυναμίες των συστημάτων, γεγονός που μας προτρέπει στη μελέτη και τον εκ νέου σχεδιασμό λύσεων. Αυτές οι αδυναμίες αφορούν τόσο τον τεχνικό τομέα – και ιδιαίτερα τη φύση και την αποθήκευση των δεδομένων – όσο και τον οργανωτικό τομέα, δηλαδή τον ορισμό συνολικών λύσεων για την υλοποίηση μιας ακολουθίας ανάκτησης στοιχείων. (QA.com, 2023)

Ιδιαίτερο ενδιαφέρον παρουσιάζουν και οι τάσεις στην έρευνα. Οι τάσεις αυτές μπορούν να αποκαλύψουν τις αιτίες που έχουν οδηγήσει στην αυξημένη ερευνητική δραστηριότητα..

Γενικά, η κατεύθυνση είναι προς την αναζήτηση των ιδιαίτερων χαρακτηριστικών του αντικειμένου και των προβλημάτων που αυτό φέρνει. Παρατηρούμε έρευνες πάνω στη μεταβλητότητα των δεδομένων, τη δυσκολία τήρησης αρχείων καταγραφής, τις υλοποιήσεις σε εικονικά περιβάλλοντα (virtual environments) και περιβάλλοντα πολλαπλής μίσθωσης (multitenancy). (Ziv, 2024) (Purnaye & Kulkarni, 2022). Επιπλέον, δίνεται έμφαση στην ταχύτητα και στην προτυποποίηση των διαδικασιών. Αυτές οι τάσεις μπορούν από μόνες τους να αποκαλύψουν μελλοντικές αδυναμίες και ανάγκες, συμβάλλοντας έτσι στην ανατροφοδότηση της αλυσίδας της έρευνας.

Τέλος, ένας επιπλέον παράγοντας που δεν πρέπει να παραλειφθεί είναι η διάκριση ανάμεσα στην παραδοσιακή πλέον ψηφιακή εγκληματολογία και στη μετάβαση σε cloud περιβάλλοντα. Αυτή η διαφορά από μόνη της προσθέτει μια επιπλέον διάσταση στην ανάγκη μελέτης του τομέα.

1.2 Στόχοι ανάλυσης

Στην παρούσα ανάλυση, η έρευνα επικεντρώνεται σε συγκεκριμένες διαστάσεις, που άπτονται της πραγματικής χρήσης των εργαλείων και των ζητημάτων που εγείρονται. Θα γίνει προσπάθεια να προσδιοριστούν τα βασικά δομικά προβλήματα του χώρου, με σκοπό την προσέγγιση των διαφόρων τρόπων πιθανής αντιμετώπισής τους.

Πιο συγκεκριμένα, θα γίνει προσπάθεια να παρουσιαστούν οι βασικές αρχές και οι εξελίξεις στον χώρο, να αναλυθούν οι τεχνικές, νομικές και οργανωτικές προκλήσεις που αναδύονται, να προταθούν μεθοδολογίες που μπορούν να αντιμετωπίσουν αυτές τις προκλήσεις και τέλος, να διερευνηθούν τα μελλοντικά ζητήματα που ενδέχεται να προκύψουν.

Συμπερασματικά, όλα τα παραπάνω θα αξιολογηθούν ως προς την πρακτική τους αξία και τη δυνατότητα εφαρμογής τους στο πεδίο, προκειμένου να ενισχυθεί η αποτελεσματικότητα της διαδικασίας απονομής δικαιοσύνης.

1.2.1 Εύρος μελέτης και Προσδοκόμενα αποτελέσματα

Πρωταρχικός στόχος της παρούσας μελέτης είναι ο σαφής προσδιορισμός των πεδίων που αποτελούν τις σημαντικότερες περιοχές προς διερεύνηση. Έχει ήδη καταστεί σαφές ότι η ανάλυση επικεντρώνεται στα προβλήματα που ανακύπτουν τόσο στο παρόν όσο και στο μέλλον. Η επίτευξη αυτού του στόχου προϋποθέτει τη διερεύνηση τριών βασικών κατηγοριών προβλημάτων, καθώς και των πιθανών λύσεων που έχουν προταθεί ή βρίσκονται υπό ανάπτυξη.

Στο πλαίσιο αυτό, θα πραγματοποιηθεί μια σε βάθος διερεύνηση των τεχνικών ζητημάτων που προκύπτουν από τη φύση του μέσου, με έμφαση στη διαδικασία αποθήκευσης και διατήρησης των δεδομένων, η οποία αποτελεί θεμελιώδες στοιχείο της συνολικής διαδικασίας.

Σε τεχνικό επίπεδο, θα επιχειρηθεί, επίσης, η αξιολόγηση των κατηγοριών εργαλείων και τεχνικών που υφίστανται στην παρούσα φάση, ενώ παράλληλα θα εξεταστεί το ζήτημα της αξιοπιστίας και της διατήρησης των αποδεικτικών στοιχείων. Αυτό κρίνεται ιδιαίτερα σημαντικό, καθώς το τελικό προϊόν της διαδικασίας αποτελεί στοιχείο προς αξιοποίηση, το οποίο οφείλει να χαρακτηρίζεται από υψηλό βαθμό εγκυρότητας και αξιοπιστίας.

Σε δεύτερο επίπεδο, η ανάλυση επικεντρώνεται στις νομικές διαστάσεις που ανακύπτουν από τη χρήση του μέσου. Στο πλαίσιο αυτό, θα εξεταστούν οι πρόσφατες εξελίξεις στον τομέα της προστασίας προσωπικών δεδομένων και ο αντίκτυπός τους στις διαδικασίες. Έτσι, θα πραγματοποιηθεί μια εισαγωγική προσέγγιση στο ζήτημα της δικαιοδοσίας, της τοποθεσίας των δεδομένων και της συνεργασίας μεταξύ νομικών, κρατικών και εμπορικών οντοτήτων, προκειμένου να διαμορφωθεί μια πιο γενική εικόνα του νομοθετικού πλαισίου που διέπει τον τομέα.

Τέλος, ο τρίτος σημαντικός πυλώνας της μελέτης αφορά το οργανωτικό πλαίσιο. Πέρα από τις τεχνικές και νομικές πτυχές, θεωρείται αναγκαία η εξέταση των διαδικασιών που οφείλουν να προσαρμόζονται στις διαρκείς εξελίξεις του πεδίου. Θα παρουσιαστούν οι

υφιστάμενες διαδικασίες και θα καταστεί σαφές το τελικό προσδοκώμενο αποτέλεσμα της συνολικής μελέτης.

Στο πλαίσιο αυτό, μέσω των προτάσεων για διαδικασίες ασφαλείας, ετοιμότητας και ανταπόκρισης, θα διαφανεί με μεγαλύτερη σαφήνεια τόσο το ερευνητικό μέλλον του πεδίου όσο και τα προβλήματα που θα κληθούν να αντιμετωπίσουν οι αρμόδιοι φορείς. Θα καταστεί σαφές πως υπάρχει η ανάγκη για μια ενιαία προσέγγιση, που θα υπερβαίνει την αποσπασματική αντιμετώπιση των επιμέρους ζητημάτων.

Είναι αυτονόητο ότι ο στόχος δεν είναι να δοθεί μία και μοναδική λύση που θα επιλύει κάθε πρόβλημα στον χώρο, αλλά να πραγματοποιηθεί μια κριτική αποτίμηση των υφιστάμενων τάσεων και λύσεων, προκειμένου να διαμορφωθεί μια σαφέστερη κατεύθυνση για τις ορθές επιλογές του μέλλοντος.

Οι επιλογές αυτές κινούνται στους εξής άξονες:

1. Σωστός ορισμός του συστήματος και των περιορισμών του βάσει τεχνικών και νομικών παραμέτρων – Καθορισμός αναγκών των διωκτικών αρχών.
2. Σχεδιασμός συστήματος με ενσωματωμένη ετοιμότητα για τη διαχείριση κρίσιμων περιστατικών.
3. Ορισμός διαδικασίας αντιμετώπισης συμβάντος (αναγνώριση και αξιολόγηση υφιστάμενων διαδικασιών).
4. Αναγνώριση και ανάλυση προβλημάτων που προκύπτουν από την εξέλιξη των τεχνολογικών και νομικών παραμέτρων

1.3 Σπουδαιότητα Cloud Forensics στη Δικαιοσύνη

Μια μελέτη, και πολύ περισσότερο ένα επιστημονικό πεδίο, αποκτά ιδιαίτερη σημασία όταν αναφέρεται σε απτά αποτελέσματα που επηρεάζουν την καθημερινή ζωή. Αναφερθήκαμε ήδη στην αναγκαιότητα της έρευνας που εξετάζει το κατά πόσο ο τομέας απαιτεί βελτίωση. Ωστόσο, θα πρέπει επίσης να γίνει αναφορά στη χρησιμότητα των αποτελεσμάτων της

ψηφιακής εγκληματολογίας, και συγκεκριμένα στον τομέα του cloud. Το μέσο επίτευξης των αποτελεσμάτων είναι η ψηφιακή απόδειξη.

Η έννοια της ψηφιακής απόδειξης στο cloud έχει θεμελιώδη σημασία ως αφετηρία κάθε διαδικασίας τεκμηρίωσης γεγονότων. Αναγνωρίζοντας ότι για πολλές δεκαετίες ο νομικός τομέας αντιμετώπιζε σημαντικές δυσκολίες στην προσαρμογή του στις τεχνολογικές εξελίξεις, γίνεται προφανές ότι η σύνδεση αυτών των δύο πεδίων παρουσιάζει ιδιαίτερο ενδιαφέρον και δεν θα είχε επιτευχθεί αν δεν υπήρχε ουσιαστική ανάγκη. Αυτή η ανάγκη προκύπτει από τη σημασία και την ισχύ των ψηφιακών αποδείξεων. (Narasimhan, 2024). Για αυτές τις αποδείξεις είναι απαραίτητο στα πλαίσια ενός διαρκώς μεταβαλλόμενου ψηφιακού κόσμου, να διασφαλιστούν μια σειρά από κρίσιμα χαρακτηριστικά (Peterson & Shenoi, 2023):

Διατήρηση της ακεραιότητας των αποδεικτικών στοιχείων. Η ακεραιότητα πρέπει να περιλαμβάνει τη διάσταση της αυθεντικότητας, της μη τροποποίησης και της αξιοπιστίας ως προς τη διαδικασία συλλογής.

Ιχνηλάτηση εγκληματικών δραστηριοτήτων. Η δημιουργία και χρήση των μεταδεδομένων ιχνηλάτησης που προκύπτουν από τα συστήματα, με σκοπό τη δημιουργία νέων αποδείξεων. Αυτές οι νέες αποδείξεις οφείλουν να πληρούν τα παραπάνω κριτήρια εγκυρότητας και αξιοπιστίας.

Διασφάλιση της διαφάνειας και τήρησης της νομιμότητας. Ιδιαίτερη προσοχή απαιτείται στον ορισμό της νομιμότητας, η οποία διαφέρει ανάλογα με τη γεωγραφική περιοχή και ως προς το αντικείμενο της έρευνας.

Για τον λόγο αυτό, είναι ζωτικής σημασίας να εξεταστούν τα διαφορετικά νομικά πλαίσια και η δικαιοδοσία. Δεν αρκεί μόνο να γνωρίζουμε σε ποιον ανήκουν τα δεδομένα και πού είναι αποθηκευμένα, αλλά και με ποιον τρόπο μεταφέρονται από έναν φορέα σε έναν άλλο. Εξίσου σημαντική είναι η διερεύνηση του πλαισίου διεθνούς συνεργασίας μεταξύ κρατών ή ομοσπονδιών για τη μετακίνηση αποδεικτικών στοιχείων.

Όλα τα παραπάνω καταδεικνύουν ότι οι ψηφιακές αποδείξεις διαφέρουν σημαντικά από την παραδοσιακή αντίληψη περί αποδεικτικών στοιχείων, καθιστώντας την ψηφιακή

εγκληματολογία ένα ιδιαίτερα σημαντικό επιστημονικό πεδίο ακόμα και αν η μόνη της αξία θα ήταν να παράγει δεδομένα.

Ωστόσο, η σημασία των ψηφιακών αποδείξεων δεν επηρεάζεται μόνο από τα τεχνικά θέματα, η τα θέματα νομιμότητας. Υφίσταται και μια παράμετρος ευκολίας δημιουργίας της απόδειξης. Ιδιαίτερο ενδιαφέρον παρουσιάζει η μελέτη του ρόλου του ίδιου του παρόχου cloud υπηρεσιών. Ο πάροχος καλείται να παρέχει πρόσβαση σε δεδομένα, τα οποία σε ορισμένες περιπτώσεις ενδέχεται να αντιβαίνουν στα επιχειρηματικά του συμφέροντα. Παρ' όλα αυτά, το νομικό πλαίσιο οφείλει να είναι επαρκώς προετοιμασμένο ώστε να διασφαλίζει ότι, η ψηφιακή απόδειξη μπορεί να μεταφερθεί στον αρμόδιο παραλήπτη με την απαιτούμενη ισχύ και εγκυρότητα. (Willson, 2013)

Τέλος, με την αυξανόμενη επικράτηση συσκευών IoT(Internet of things) (Statista, 2025), ο όγκος των παραγόμενων δεδομένων συνεχώς αυξάνει, καθιστώντας σαφές ότι οι ψηφιακές αποδείξεις τείνουν να αντικαταστήσουν τις φυσικές αποδείξεις σε πολλές περιπτώσεις. Αυτό από μόνο του αποτελεί τη μεγαλύτερη απόδειξη της σημασίας τους, επιβεβαιώνοντας την ανάγκη περαιτέρω μελέτης και ανάπτυξης λύσεων στον τομέα της ψηφιακής εγκληματολογίας.

2 Βασικές έννοιες και ιστορικά στοιχεία

Πρώτο βήμα στη μελέτη είναι ο ξεκάθαρος ορισμός των αντικειμένων και τομέων με τα οποία ασχολούμαστε. Θα ξεκινήσουμε αυτούς τους ορισμούς από την επεξήγηση του ίδιου του cloud computing και των παραμέτρων του, καθώς αυτό δημιουργεί ιδιαίτερες συνθήκες και απαιτήσεις στον τομέα της ψηφιακής εγκληματολογίας. Στη συνέχεια, θα παρουσιαστούν τα χαρακτηριστικά της παραδοσιακής ψηφιακής εγκληματολογίας και θα αναλυθούν οι αλλαγές που επιφέρει ή απαιτεί η μετάβασή της στο υπολογιστικό νέφος.

2.1 Βασικές έννοιες

2.1.1 Cloud Computing: Αρχές και υποδομές

Όταν γίνεται αναφορά στο cloud, εννοείται μια δομή συνδεδεμένων υποδομών που τοποθετούνται σε έναν απομακρυσμένο χώρο (data center) και μπορούν να προσφέρουν υπηρεσίες τόσο στον ίδιο τον ιδιοκτήτη τους όσο και ως αγαθό προς πώληση ή ενοικίαση (Microsoft, 2025) . Ο όρος του cloud computing επεκτείνει αυτή τη λογική στην παροχή υπηρεσιών που χρησιμοποιεί τις προαναφερθείσες υποδομές. Ουσιαστικά δίνεται η δυνατότητα σε χρήστες να απολαμβάνουν υπηρεσίες δίχως την ανάγκη της φυσικής εγκατάστασης που υπήρχε στο παρελθόν.

Η έννοια του cloud computing εμφανίζεται στη βιβλιογραφία από τη δεκαετία του 1960 και συνδέεται άμεσα με την ιστορία του Internet. Ο J.C.R. Licklider είχε τη βασική ιδέα της δημιουργίας ενός δικτύου υπολογιστών που θα υλοποιούσε τον διαμοιρασμό δεδομένων και προγραμμάτων και το ονόμαζε *Intergalactic Computer Network*. (HASSAN, 2023) (Apogee, 2024). Παράλληλα, ο καθηγητής John McCarthy είχε περιγράψει ένα μοντέλο υπηρεσιών βασισμένο στον διαμοιρασμό πόρων, το οποίο παρουσίαζε ομοιότητες με τη λογική του cloud computing. (ECPI, 2024).

Ωστόσο, τα παραπάνω δεν αποτέλεσαν το cloud computing που γνωρίζουμε σήμερα, καθώς απαιτήθηκαν πολλές τεχνολογικές και οικονομικές εξελίξεις προκειμένου να φτάσουμε στη σύγχρονη μορφή του. Τη δεκαετία του 1990, οι εξελίξεις άρχισαν να πλησιάζουν περισσότερο

προς το σημερινό μοντέλο, αλλά και πάλι χρειάστηκαν μερικά χρόνια μέχρι να αναπτυχθούν υπηρεσίες που θα υλοποιούσαν το πραγματικό cloud computing. Η ιστορία του cloud computing πέρασε από πολλά ενδιάμεσα στάδια, αλλά αυτό που έχει ιδιαίτερη σημασία είναι η παρούσα φάση και το μοντέλο που επικρατεί σήμερα. Η σημερινή μορφή του cloud computing ξεκίνησε να διαμορφώνεται τη δεκαετία του 2000 με την εμφάνιση υπηρεσιών όπως το Amazon Web Services (AWS), το Google Cloud και το Microsoft Azure (Apogee, 2024). Τα κύρια χαρακτηριστικά που καθορίζουν μια υπηρεσία cloud είναι τα ακόλουθα:

- On demand self service – Αυτοματοποιημένη παροχή υπηρεσιών κατόπιν ζήτησης
- Rapid elasticity – Δυναμική και ταχεία επεκτασιμότητα πόρων
- Location independence – Ανεξαρτησία φυσικής τοποθεσίας υποδομών
- Data replication – Αναπαραγωγή δεδομένων σε πολλαπλές τοποθεσίες/κόμβους

Είναι σχεδόν προφανές ότι το μεγάλο πλεονέκτημα των υπηρεσιών cloud είναι πως μειώνει ουσιαστικά το κόστος εγκατάστασης, συντήρησης αλλά και το κόστος απαιτούμενης γνώσης εν γένει για τις προσφερόμενες υπηρεσίες (Alshabibi, et al., 2024). Ο πελάτης έχει άμεσα διαθέσιμο ένα νέο σύστημα, ενημερωμένο και αυτομάτως μεταβαλλόμενο, ανάλογα με τις ανάγκες του. Φυσικά, το κόστος που εξοικονομεί, μετακυλίεται στις ίδιες τις υπηρεσίες, αλλά σε πολλές περιπτώσεις η εφαρμογή οικονομιών κλίμακας δίνει όφελος σε όλα τα μέρη.

Οι υπηρεσίες που προσφέρονται έρχονται σε διαφορετικά μοντέλα και οι διαφορετικές προδιαγραφές χρήσης έχουν ενδιαφέρον γιατί μεταφράζονται και σε διαφορετικούς κινδύνους. Έτσι έχουμε τα μοντέλα (IBM, 2021):

Infrastructure as a Service (IaaS) – Παροχή δομών αποθήκευσης δεδομένων αλλά και υπολογιστικούς πόρους προς χρήση (π.χ. AWS, Microsoft Azure VMs).

Platform as a Service (PaaS) – Παροχή υποδομών ανάπτυξης εφαρμογών (Azure App Services).

Software as a Service (SaaS) – Παροχή καθαρά εφαρμογών, συνήθως web (παραδείγματα: Google Drive, Microsoft 365).

Τα πιο σημαντικά από τα χαρακτηριστικά που έχουν τα παραπάνω είναι η μεταβλητότητα των δεδομένων, και η τοποθεσία αποθήκευσης τους. Η μεταβλητότητα κάνει πιο δύσκολη

τη λήψη μιας σαφούς εικόνας των δεδομένων σε μια χρονική στιγμή, ενώ η τοποθεσία αποθήκευσης δυσκολεύει την ανάκτηση αλλά και τον ορισμό της δικαιοδοσίας σε περιπτώσεις νομικών υποθέσεων. Επιπλέον, μια σειρά δεδομένων ενδέχεται να μην είναι προσβάσιμα, είτε λόγω της φύσης τους, είτε της κεντρικής διαχείρισης που απαιτούν (π.χ. αρχεία καταγραφής σε SaaS).

2.1.2 Ψηφιακή εγκληματολογία γενικά και Ψηφιακή εγκληματολογία στο cloud

Οι υπηρεσίες cloud έχουν φέρει αναγκαστικά επεκτάσεις στον τομέα της ψηφιακής εγκληματολογίας όπως είχε οριστεί στο παρελθόν. Η ψηφιακή εγκληματολογία είναι ένα επιστημονικό πεδίο, κλάδος της παραδοσιακής εγκληματολογίας, που ασχολείται με την επεξεργασία ψηφιακών αποδείξεων (Badman, 2024). Η επεξεργασία ξεκινάει από την ίδια τη συλλογή των αποδείξεων, την ανάλυσή τους και την παρουσίαση σε αποδεκτή μορφή. Εναλλακτικά, ορισμός της ψηφιακής εγκληματολογίας θα μπορούσε να είναι η διαδικασία της ανάλυσης και παρουσίασης ψηφιακών δεδομένων σε μια μορφή που να είναι νομικά αποδεκτή. Χρησιμοποιείται σε αναγνώριση και πρόληψη εγκλημάτων, και στην επίλυση διαφορών που αναφέρονται σε δεδομένα που αποθηκεύονται ψηφιακά. (Kävrestad, et al., 2024) (Malik, et al., 2024). Πολύ σημαντική προδιαγραφή είναι αυτές οι ψηφιακές αποδείξεις αλλά και οι διαδικασίες να ακολουθούν σε ιδιότητες τις φυσικές αποδείξεις, πάνω στις οποίες άλλωστε μοντελοποιήθηκαν αρχικά. Θα πρέπει να διέπονται από τις παρακάτω αρχές (TrueScreen, 2025) (Stoykova, 2021):

- **Αυθεντικότητα** – Η απόδειξη είναι γνήσια
- **Ακεραιότητα** – Η απόδειξη δεν έχει υποστεί τροποποίηση ή αλλοίωση
- **Αξιοπιστία** – Η συλλογή των δεδομένων γίνεται με τρόπο και από πηγή που θεωρείται έμπιστη και έγκυρη
- **Πληρότητα** – Περιέχονται όλες οι απαραίτητες πληροφορίες
- **Αποδοχή** – Οι αποδείξεις ακολουθούν τα νομικά πρότυπα που επιτρέπουν την αποδοχή της στα δικαστήρια (Διατήρηση της αλυσίδας φύλαξης)
- **Επαναληψιμότητα** – Οι αποδείξεις θα πρέπει να είναι δυνατόν να αναπαραχθούν και να επαληθευθούν.

Φυσικά, μια απόδειξη θα πρέπει να έχει και τη σωστή συσχέτιση με την υπόθεση, όπως επίσης και την απαραίτητη αντοχή στον χρόνο, όσον αφορά την αποθήκευσή της.

Στον χώρο του cloud computing, η ψηφιακή εγκληματολογία δεν αλλάζει στόχους αλλά αλλάζει μέσα και περιπτώσεις χρήσης. Έτσι και εδώ ο στόχος είναι η παροχή εν τέλει ψηφιακών αποδείξεων, αλλά αυτό γίνεται σε ένα διαφορετικό περιβάλλον που προσφέρει ένα πιο διευρυμένο σύνολο εργαλείων και αναφέρεται σε υποθέσεις διαφορετικού χαρακτήρα.

Η ψηφιακή εγκληματολογία στο cloud αναγκαστικά ακολουθεί τις διαστάσεις των μορφών cloud που αναφέρθηκαν, έτσι ανά διαφορετική χρήση προκύπτουν και διαφορετικά ζητήματα προς διερεύνηση και επίλυση (Purnaye & Kulkarni, 2022).

Όπως είναι αναμενόμενο, τα πρώτα χρόνια της ύπαρξης των διάφορων μορφών cloud δεν είχε γίνει ξεκάθαρη η ανάγκη ορισμού ενός ξεχωριστού πλαισίου αντιμετώπισης των συμβάντων. Ήταν αρκετό το να χρησιμοποιούνται οι γενικές τεχνικές ψηφιακής εγκληματολογίας, οι οποίες και εν τέλει έκαναν εμφανή τα ζητήματα που θα προέκυπταν.

Έφτασε το 2011 για να οριστεί μια διαδικασία από το National Institute of Standards and Technology (Martin Herman, 2024). Σύμφωνα με το Ινστιτούτο, η πρότυπη διαδικασία ψηφιακής εγκληματολογίας στο cloud περιλαμβάνει τα βήματα: **Αναγνώριση → Διατήρηση → Ανάλυση → Παρουσίαση**, ενώ άρχισαν να εμφανίζονται και τα πρώτα

εργαλεία που είχαν δημιουργηθεί αποκλειστικά για αυτήν την κατηγορία χρήσης. Εργαλεία όπως το FTK και X-Ways.

Πιο ουσιαστική και αυστηρή οριοθέτηση έγινε το 2016, λόγω κυρίως μιας σειράς επιθέσεων που έφεραν στο προσκήνιο ακόμα περισσότερο τις ιδιαιτερότητες του τομέα αυτού (Cloud Security Alliance, 2017). Το μοντέλο της διαδικασίας φαίνεται να εμπλουτίζεται και να φτάνει τα 8 βήματα/προϋποθέσεις που περιλαμβάνουν λεπτομέρειες τόσο σε σχέση με το νομικό κομμάτι και τη τήρηση της αλυσίδας αποδείξεων, όσο και τη σωστή διαχείριση των δεδομένων.

Συνοπτικά, οι προϋποθέσεις είναι οι ακόλουθες (Sardinas, 2020)

- Εξουσιοδότηση έρευνας. Απαιτείται νομική εξουσιοδότηση για τη διεξαγωγή έρευνας και/ή κατάσχεσης δεδομένων.
- Αλυσίδα επιτήρησης (Chain of custody). Σε νομικά πλαίσια, απαιτείται χρονολογική τεκμηρίωση της πρόσβασης και του χειρισμού των αποδεικτικών στοιχείων, ώστε να αποφεύγονται ισχυρισμοί περί αλλοίωσης ή κακής διαχείρισης των αποδείξεων.
- Λειτουργία δημιουργίας εικόνας (imaging) και κατακερματισμού (hashing). Όταν εντοπίζονται αντικείμενα που περιέχουν πιθανές ψηφιακές αποδείξεις, κάθε ένα

από αυτά πρέπει να αντιγράφεται προσεκτικά και στη συνέχεια να υποβάλλεται σε κατακερματισμό (hashing) για την επαλήθευση της ακεραιότητας του αντιγράφου.

- Επικυρωμένα εργαλεία. Όποτε είναι δυνατόν, τα εργαλεία που χρησιμοποιούνται στην εγκληματολογική ανάλυση πρέπει να είναι επικυρωμένα για να διασφαλίζεται η αξιοπιστία και η ορθότητά τους.
- Ανάλυση. Η εγκληματολογική ανάλυση περιλαμβάνει την εφαρμογή ανακριτικών και αναλυτικών τεχνικών για την εξέταση, ανάλυση και ερμηνεία των αποδεικτικών στοιχείων που έχουν συλλεχθεί.
- Επαναληψιμότητα και αναπαραγωγιμότητα (διασφάλιση ποιότητας). Οι διαδικασίες και τα συμπεράσματα της εγκληματολογικής ανάλυσης πρέπει να είναι επαναλήψιμα και αναπαραγώγιμα από τον ίδιο ή άλλους εγκληματολόγους.
- Τεκμηρίωση. Ο εγκληματολόγος πρέπει να καταγράφει τη διαδικασία ανάλυσης και τα συμπεράσματά του, ώστε να είναι διαθέσιμα για χρήση από άλλους.
- Παρουσίαση. Στις περισσότερες περιπτώσεις, ο εγκληματολόγος θα πρέπει να παρουσιάσει τα ευρήματα και τα συμπεράσματά του σε δικαστήριο ή σε άλλο κοινό.

Εν τέλει, εν έτει 2024, η αντίστοιχη έκθεση του NIST (NIST, 2024) προσεγγίζει το θέμα από τη σκοπιά της δημιουργίας ενός αρχιτεκτονικού μοντέλου, το οποίο μπορεί να αναγνωρίσει όλα αυτά τα ζητήματα που μπορούν να προκύψουν ήδη από τη δημιουργία της υποδομής. Το μοντέλο απευθύνεται τόσο σε σχεδιαστές υποδομών cloud, όσο και σε εγκληματολόγους ερευνητές, αλλά και τελικά και στους καταναλωτές, χρήστες υπηρεσιών cloud.

Συμπερασματικά, η διαδικασία μπορεί να θεωρηθεί ότι ακολουθεί το βασικό διάγραμμα που είναι έγκυρο και μέχρι σήμερα, και περιλαμβάνει τα 4 βασικά βήματα (Malik, et al., 2024), παρ' όλα αυτά, έμφαση δίνεται στην ποιότητα της εκτέλεσης των βημάτων και στην αντιμετώπιση των ζητημάτων που προκύπτουν με διάφορες τεχνικές ή μεθοδολογίες. Σε μια πολύ γενική θεώρηση, τα προβλήματα που προκύπτουν έχουν σχέση με μια σειρά από σημαντικά βήματα της διαδικασίας:

- Αναγνώριση του συμβάντος και αντίστοιχα των ζητούμενων αποδείξεων
- Ανάκτηση αποδείξεων – Χρήση των κατάλληλων εργαλείων για να προσπελαστούν οι ευμετάβλητες πηγές
- Ανάλυση των αποδείξεων
- Μηχανισμοί διατήρησης της πιστότητας των αποδείξεων
- Παρουσίαση των αποδείξεων

Σε όλα αυτά προστίθεται πάντα και το ζήτημα της τήρησης των νομικών πλαισίων που διέπουν τον κάθε χώρο, και υπεισέρχεται σε πολλά βήματα της διαδικασίας.

2.2 Σύγκριση ψηφιακής εγκληματολογίας και εγκληματολογίας στο cloud

2.2.1 Διαφορές μεταξύ παραδοσιακής και cloud εγκληματολογίας

Οι δύο διαφορετικές μορφές της ψηφιακής εγκληματολογίας δεν απέχουν φυσικά πολύ μεταξύ τους. Οι τρεις βασικές διαφορές έχουν να κάνουν με την ίδια τη φύση του cloud.

Τα δεδομένα βρίσκονται αποθηκευμένα τόσο σε διαφορετικό σημείο όσο και με διαφορετικό τρόπο. Η πρόσβαση σε αυτά δεν είναι πάντα εφικτή, καθώς ενδέχεται η πληροφορία να είναι κατακερματισμένη σε πολλά σημεία, ενώ συχνά λόγω του φαινομένου της πολυμίσθωσης, δεδομένα διαφορετικών χρηστών ή υποθέσεων βρίσκονται στην ίδια υποδομή. Επιπλέον, το περιβάλλον γενικά είναι δυναμικό και πόροι που έχουν ανατεθεί είναι εικονικοί και ενδέχεται να πάψουν να υπάρχουν. Στην παραδοσιακή αρχιτεκτονική βρισκόμαστε ένα βήμα πιο κοντά στους φυσικούς πόρους, και με πολύ μικρό βαθμό κατακερματισμού, συνήθως στο ίδιο σύστημα.

Ο ρόλος του παρόχου είναι πολυσύνθετος. Μπορεί να βοηθήσει με τις πολιτικές διατήρησης δεδομένων, αλλά και μπορεί να δυσχεράνει το έργο των ανακριτικών αρχών, καθώς οι τυπικές και νομικές του υποχρεώσεις μπορεί εν τέλει να είναι διαφορετικές. Επίσης, διαδραματίζει σημαντικό ρόλο και στη διατήρηση της αλυσίδας φύλαξης και θα πρέπει να μπορεί να τεκμηριώσει αυτός, και συχνά μόνο αυτός, τη σωστή φύλαξη των αποδείξεων. Τέλος, αυτός είναι και ο ιδιοκτήτης των πόρων, οπότε μπορεί να παίξει σημαντικό ρόλο στη λήψη δεδομένων ή εγκρίσεων. Στην παραδοσιακή αρχιτεκτονική, ιδιοκτήτης των πόρων

μπορεί να είναι και ο πάροχος αλλά και ο ίδιος ο χρήστης, κάτι που κάνει την απόδοση ευθυνών ή τη λήψη εγκρίσεων κατά τι πιο εύκολη.

Το νομικό πλαίσιο έρχεται στην εγκληματολογία στο cloud να αντιμετωπίσει τη νομοθεσία διαφορετικών τοποθεσιών. Ενδέχεται να υπάρχει μη ξεκάθαρη τοποθεσία δεδομένων και συνήθως η άμεση γνώση περιορίζεται σε επίπεδο υποδομών ανά ήπειρο, χωρίς να είναι εντελώς ξεκάθαρο πού βρίσκονται.

Στην ψηφιακή εγκληματολογία στο cloud, σημαντική διαφοροποίηση έρχεται με τις τεχνικές διαχείρισης αποδεικτικών στοιχείων. Κάποιες νέες τεχνικές ή διαδικασίες έρχονται σταδιακά στο προσκήνιο

• **Live Forensics** – Εξαγωγή δεδομένων από ενεργά cloud instances. (Kävrestad, et al., 2024). Σε αυτή την περίπτωση ενδέχεται να χρειαστεί ανάκτηση δεδομένων ακόμα και από στοιχεία μνήμης ή από ενεργές δικτυακές συνδέσεις, αλλά χωρίς να σταματήσει η λειτουργία της υποδομής. Αυτό φυσικά δεν είναι πάντα εφικτό, διότι ενδέχεται το νομικό ή ιδιοκτησιακό πλαίσιο να το αποτρέπει. Σε κάθε περίπτωση, εργαλεία όπως το Google Cloud Forensic API και AWS Systems Manager διευκολύνουν τη διαδικασία αυτή.

• **Network Forensics in the Cloud** – Στόχος στην παρούσα τεχνική είναι η ανάλυση των δικτυακών δεδομένων, που μπορεί να περιλαμβάνουν τόσο την κίνηση μεταξύ υποδομής και πελάτη, αλλά και τις ενδεχόμενες επιθέσεις σε δικτυακό επίπεδο. Δυσκολίες εδώ εντοπίζονται τόσο στην πολυμίσθωση και τον δυσδιάκριτο ορισμό και αντιστοίχιση της δικτυακής κίνησης σε κάθε τμήμα υπηρεσίας, όσο και στην ίδια τη φύση της επικοινωνίας που στις περισσότερες περιπτώσεις έρχεται σε κρυπτογραφημένο κανάλι.

Συνηθέστερα εργαλεία τα Google Cloud Packet Mirroring και Azure Network Watcher, ενώ ακόμα και παραδοσιακά εργαλεία όπως το Wireshark μπορεί να χρησιμοποιηθούν, αλλά προϋποθέτουν την εξαγωγή των αρχείων καταγραφής δικτύου. (Kävrestad, et al., 2024)

• **Cloud Log Analysis** – Ανάλυση από τους ίδιους τους παρόχους με σκοπό τον έλεγχο πρόσβασης και παρακολούθηση κακόβουλων ενεργειών. Συνηθέστερα εργαλεία: AWS CloudTrail, Google Cloud Logging, αλλά και ενδεχομένως ο συνδυασμός ELK (Elasticsearch, Logstash, Kibana), που διευκολύνει την ανάλυση των αρχείων καταγραφής, προσφέροντας

δυνατότητες αποθήκευσης, φιλτραρίσματος, οπτικοποίησης και αναζήτησης των δεδομένων, σε πραγματικό ή σχεδόν πραγματικό χρόνο (Pichan, 2022) (Casino, et al., 2022).

2.3 Εξελίξεις και αναγκαιότητα έρευνας.

Τα σημαντικότερα ζητήματα σύμφωνα με τους (Manoj & Bhaskari, 2016) και (Malik, et al., 2024) που εγείρονται μπορούν να κατηγοριοποιηθούν σε μερικές μεγάλες κατηγορίες:

1. *Προβλήματα αρχιτεκτονικής συστημάτων*. Πολυμίσθωση συστημάτων, κατακερματισμός δεδομένων.
2. *Προβλήματα συλλογής δεδομένων*. Διατήρηση ακεραιότητας και μεταδεδομένων τοποθεσίας. Αδυναμία εργαλείων, μέγεθος δεδομένων, περιορισμοί εύρους ζώνης. Αδυναμία φυσικής πρόσβασης στα συστήματα.
3. *Ανάλυση δεδομένων*. Χρονικές συσχετίσεις, ανάλυση αρχείων καταγραφής, μεταδεδομένων.
4. *Παρουσίαση δεδομένων*. Τήρηση νομικών διαδικασιών και τήρηση αρχείων καταγραφής
5. Αντιμετώπιση αντιδικανικών τεχνικών.
6. *Πιστότητα των παρόχων* και αντιμετώπιση συμβάντων από αυτούς. Διατήρηση ποιότητας πληροφορίας σε αυτή την αντιμετώπιση. Διατήρηση σκηνής εγκλήματος
7. *Διαχείριση διαφορετικών ρόλων*. Διάκριση μεταξύ ιδιοκτητών δεδομένων και διαχειριστών, διαχείριση πρόσβασης των παραπάνω.
8. *Νομικά ζητήματα*. Δικαιοδοσία, συμβόλαια και συμφωνίες επιπέδου ποιότητας υπηρεσίας, διεθνής συνεργασία, θέματα προσωπικών δεδομένων
9. Προτυποποίηση διαδικασιών και μεθόδων
10. *Εκπαίδευση* στα διάφορα εμπλεκόμενα μέλη. Εκπαίδευση σε θέματα ασφάλειας αλλά και εκπαίδευση στους ερευνητές.

Τα παραπάνω δίνουν και μια εικόνα της τάσης για μελέτη. Όπως είναι αναμενόμενο, η επίλυση κάποιων από τα ζητήματα αυτά επαφίεται σε επαγγελματίες του χώρου, και οι τάσεις φαίνονται και από το πλήθος των μελετών που προσανατολίζονται σε αυτά. Έτσι, σύμφωνα με τους (Casino, et al., 2022), σημαντική είναι η τάση τόσο της αντιμετώπισης των ζητημάτων συνολικά, αλλά και σε ένα επίπεδο παραπάνω, της δημιουργίας

διαφορετικών λύσεων. Η προσέγγιση που έχει ενδιαφέρον είναι η δημιουργία ενός πλαισίου που θα εξαλείφει κάποια από τα προβλήματα εν τη γενέσει τους. Αυτό που προκρίνεται είναι η ετοιμότητα σε σχέση με την ανταπόκριση. Έτσι, φαίνεται να είναι πιο αποδοτικό ένα σύστημα να είναι έτοιμο για κάθε επίθεση και να μπορεί να ανταπεξέλθει ήδη σε όλες τις απαιτήσεις παροχής δεδομένων, μεταδεδομένων και αρχείων καταγραφής. Αυτή η διαδικασία ονομάζεται **Cloud Forensics Readiness** και θα αποτελέσει αντικείμενο μελέτης και στο παρόν κείμενο. (Ahmed Alenezi, 2019)

Πέρα όμως από το πλαίσιο που θα περιγραφεί στην παρούσα μελέτη, υπάρχουν ακόμα περισσότερες τεχνολογικές εξελίξεις που ωθούν και την έρευνα σε συγκεκριμένα μονοπάτια. Κάποια από τα πολύ ενδιαφέροντα είναι και τα:

• **Χρήση blockchain για την ασφαλή αποθήκευση εγκληματολογικών στοιχείων.** Εξασφάλιση της ακεραιότητας δεδομένων με χρήση της ιδιότητας της μη αυθαίρετης τροποποίησης που προσφέρει η τεχνολογία αυτή.

• **Blockchain Forensics.** Επίσης στον ίδιο τομέα αναγνωρίζεται και η ανάγκη έρευνας πάνω σε εγκληματικά συμβάντα στα ίδια τα blockchain δίκτυα. Μια ιδιαίτερα δύσκολη πρακτική λόγω της κρυπτογράφησης αλλά και του αποκεντρωμένου χαρακτήρα αυτών των συστημάτων (Atlam Hany, 2024)

• **AI-powered Cloud Forensics.** Αυτοματοποιημένη εγκληματολογική ανάλυση με τεχνητή νοημοσύνη. Δημιουργία μοντέλων μηχανικής μάθησης που θα αναγνωρίζουν αυτόματα τα προβλήματα, αλλά και περαιτέρω χρήση AI assistants για τη διευκόλυνση χρηστών. Σε αυτό το περιβάλλον υπεισέρχονται φυσικά όλες οι δυσκολίες που φέρνει η τεχνητή νοημοσύνη, από τη μεροληψία των αλγορίθμων μέχρι και το διαρκώς μεταβαλλόμενο νομικό πλαίσιο. (Weir & Aßmuth, 2024), (Nelufule, et al., 2024), (Alashjaee, 2024)

• **Edge Forensics.** Επέκταση των ερευνών σε *edge computing* περιβάλλοντα. Αυτό σημαίνει μια επικέντρωση σε μικροσυσκευές IoT ή ακόμα και συσκευές κινητές. Πολύ σημαντικό ζήτημα εδώ είναι και το πού βρίσκονται τα δεδομένα αλλά επίσης και οι δυνατότητες που

πραγματικά έχουν αυτές οι μικροσυσκευές, τόσο σε επεξεργασία όσο και σε καταγραφή δεδομένων. (Prakash, et al., 2021)

3 Cloud Forensics. Η παρούσα κατάσταση και οι προκλήσεις

3.1 Παρούσα κατάσταση

Η ανάπτυξή του κλάδου της ψηφιακής εγκληματολογίας στο cloud ακολουθεί τις τεχνολογικές εξελίξεις, αλλά τροφοδοτείται κυρίως από την ύπαρξη προβλημάτων – νέων ή παλαιότερων – τα οποία δεν μπορούν να αντιμετωπιστούν επαρκώς με τις υπάρχουσες μεθόδους. Οι εξελίξεις αυτές γίνονται εμφανείς τόσο από την πληθώρα εργαλείων που είναι πλέον διαθέσιμα και αντιμετωπίζουν τις σύνθετες καταστάσεις ανάκτησης αποδεικτικών στοιχείων, όσο και από την αύξηση των επιθέσεων, οι οποίες γίνονται ολοένα και πιο σοβαρές και τεχνικά εξεζητημένες.

Όσον αφορά τα εργαλεία, έχει ενδιαφέρον να παρατεθεί μια λίστα λογισμικού που εστιάζει αποκλειστικά στην εγκληματολογική ανάλυση cloud περιβαλλόντων (Yodha, 2023) (Magnet Forensics, 2025; Malik, et al., 2024).

Κάποια από τα βασικά εργαλεία είναι τα εξής:

- Magnet Axiom Cloud – Προσφέρει τη συλλογή δεδομένων από cloud περιβάλλοντα, υποστηρίζοντας τις πιο διαδεδομένες πλατφόρμες.
- Volatility – Εργαλείο για την ανάλυση μνήμης σε εικονικές μηχανές που βρίσκονται σε cloud περιβάλλοντα.
- Cellebrite UFED Analyzer – Εξειδικεύεται στη συλλογή δεδομένων, εστιάζοντας κυρίως σε social media και email υπηρεσίες.
- Mandiant Cloudlens – Εργαλείο παρακολούθησης που μπορεί να αναγνωρίσει επιθέσεις και ύποπτες δραστηριότητες στο cloud.
- AccessData Cloud Extractor – Υλοποιεί την εξαγωγή πληροφοριών, τη διατήρησή τους, καθώς και τη δημιουργία αντιγράφων δεδομένων για συγκεκριμένους χρήστες.
- Oxygen Forensics Cloud Extractor – Γενικό εργαλείο εξαγωγής δεδομένων από cloud περιβάλλοντα.
- Azure Security Center – Το εργαλείο της Microsoft που υλοποιεί την προστασία δεδομένων και την αντιμετώπιση απειλών στο Azure Cloud.

Είναι σαφές ότι θα μπορούσε να παρατεθεί μια πολύ εκτενέστερη λίστα εργαλείων, ωστόσο αυτό δεν θα οδηγούσε σε κάποιο άλλο συμπέρασμα πέρα από τον κατακερματισμό του χώρου, αλλά και την ύπαρξη πολλών εργαλείων από τους ίδιους τους παρόχους. Μια

συγκριτική προσέγγιση των εργαλείων που προσφέρουν οι ίδιοι οι πάροχοι θα αποτελέσει και αντικείμενο ερευνάς, στα πλαίσια των προτάσεων.

Πώς διαμορφώνεται, όμως, η κατάσταση από την πλευρά των επιθέσεων; Η αύξηση του όγκου των επιθέσεων οφείλεται, εν μέρει, στο γεγονός ότι το cloud αποτελεί πλέον έναν προνομιακό στόχο. Όσο περισσότεροι χρήστες και επιχειρήσεις μεταβαίνουν σε cloud υποδομές, τόσο περισσότεροι επιτιθέμενοι στρέφουν την προσοχή τους προς αυτές.

Μερικές από τις πολύ γνωστές επιθέσεις είναι οι παρακάτω:

- Microsoft Databases Cloud Breach – Επίθεση σε βάσεις δεδομένων της Microsoft στο cloud, με αποτέλεσμα την έκθεση δεδομένων 250 εκατομμυρίων χρηστών (Team, 2025).
- LastPass Data Breach – Οι επιτιθέμενοι εκμεταλλεύτηκαν τον οικιακό υπολογιστή ενός DevOps engineer της εταιρείας, εκθέτοντας στοιχεία για 25 εκατομμύρια χρήστες, συμπεριλαμβανομένων μυστικών φράσεων (vault credentials). Το κόστος της επίθεσης υπολογίζεται στα 35 εκατομμύρια δολάρια, καθώς αρκετοί χρήστες έχασαν κρυπτονομίσματα (Kapko, 2023).
- Volkswagen Data Breach – Επίθεση σε σύστημα αναζήτησης κειμένου, που είχε ως αποτέλεσμα την έκθεση των δεδομένων 3,3 εκατομμυρίων χρηστών. Το κόστος της επίθεσης υπολογίζεται στα 5 εκατομμύρια δολάρια. (Malik, et al., 2024)

Σύμφωνα με την έκθεση του ExpertInsights, το 45% των επιθέσεων που συμβαίνουν έχουν ως βάση τους το cloud, ενώ το 80% των επιχειρήσεων που έχουν υποδομές σε cloud έχουν δεχτεί κάποια επίθεση. Σημειώνοντας πως όλο και περισσότερες επιχειρήσεις πλέον καταφεύγουν στο cloud για τις υποδομές τους (72%), είναι προφανές ότι η συχνότητα των επιθέσεων αυξάνεται ραγδαία (Harris, 2025). Έτσι πολύ χαρακτηριστικά με βάση την έκθεση των Cybersecurity Insiders για το 2024, 61%των επιχειρήσεων έχουν κάποιο περιστατικό ασφαλείας σε σχέση με το cloud, και ένα επιπλέον 23% απαντά πως δεν είχαν ξεκάθαρη απάντηση, είτε από αδυναμία είτε από άρνηση αποκάλυψης πληροφορίας. (Cybersecurity Insiders, 2024). Επιπλέον, το πλήθος των αρχείων που εκτίθενται αυξάνει και αυτό με τις επιθέσεις. Για το 2023, υπολογίζεται πως 8 εκατομμύρια αρχεία βρέθηκαν εκτεθειμένα σε επιθέσεις (Edgedelta, 2024). Στον τομέα της σοβαρότητας των επιθέσεων, είναι

χαρακτηριστικό πως το μέσο κόστος μιας επίθεσης έχει αυξηθεί ραγδαία. Πλέον, για το 2024, υπολογίζεται σε 4,88 εκατομμύρια δολάρια, αυξημένο κατά 20% σε σχέση με την προηγούμενη τετραετία, ενώ αντίστοιχα σημαντικά αυξάνονται και οι επιπτώσεις στην αξιοπιστία των επιχειρήσεων. Το τελευταίο είναι ιδιαίτερα σημαντικό, καθώς συνδέεται με οικονομικά στοιχεία μιας επιχείρησης, μέσω της διαπραγμάτευσης της μετοχής της. (Gratton, 2025).

Τα παραπάνω παραδείγματα και στατιστικά στοιχεία δημιουργούν το πλαίσιο αναγκαιότητας για την ανάλυση των ζητημάτων εγκληματολογικής αντιμετώπισης επιθέσεων στο cloud. Η μελέτη αυτή δεν εστιάζει στην εξέταση του γιατί τα συστήματα παραμένουν εκτεθειμένα, καθώς αυτό αποτελεί αντικείμενο διαφορετικής έρευνας. Αντίθετα, επικεντρώνεται στον τρόπο αντίδρασης μετά από μια επίθεση, και ειδικότερα στη συλλογή αποδεικτικών στοιχείων για τη νομική αντιμετώπιση των κυβερνοεπιθέσεων.

Είναι σημαντικό επίσης να γίνει σαφές ότι ο στόχος δεν είναι η κατασκευή ενός "απόλυτα ασφαλούς" συστήματος, αλλά η διαμόρφωση ενός συνόλου διαδικασιών που θα είναι διαθέσιμες όταν μια επίθεση ασφαλείας καταστεί αναπόφευκτη. Εδώ αξίζει να αναφερθεί και μια σύντομη διαδικασία ή μεθοδολογία αντιμετώπισης συμβάντος.

Τα βήματα που πρέπει να γίνουν είναι τα παρακάτω (Malik, et al., 2024):

- Απομόνωση πόρων που έχουν επηρεαστεί.
- Ενημέρωση ομάδων ανταπόκρισης.
- Συλλογή στοιχείων.
- Διατήρηση αυτών των στοιχείων με τρόπο που εξασφαλίζει την αλυσίδα απόδειξης.
- Ανάλυση σε εγκληματολογικό επίπεδο, ώστε να αξιολογηθεί το εύρος του ζητήματος
- Αποκατάσταση ή περιορισμός προβλήματος.
- Νομική αντιμετώπιση και υλοποίηση κανονιστικών υποχρεώσεων.
- Ενημέρωση για τα αποτελέσματα όλων των εμπλεκόμενων μερών.

Αυτή η διαδικασία φαίνεται ότι καλύπτει τα ζητήματα, αλλά είναι πολύ γενική στη μορφή της και θα πρέπει να εμπλουτιστεί με ενημερωμένες τεχνικές. Επίσης, στις προτεινόμενες διαδικασίες θα πρέπει να συνυπολογιστεί η ύπαρξη ψηφιακών αντί-εγκληματολογικών τεχνικών (anti-forensic techniques) (Horton, 2024). Ουσιαστικά, θα πρέπει να εξεταστεί ο

τρόπος με τον οποίο οι επιτιθέμενοι μπορούν να δυσχεράνουν το έργο της εγκληματολογικής ανάλυσης, προκειμένου να καθυστερήσουν ή ακόμα και να αποτρέψουν τη συλλογή αποδεικτικών στοιχείων.

Για να προταθεί ένα αξιοποιήσιμο μοντέλο, το πρώτο βήμα είναι η περιγραφή των σημαντικότερων προκλήσεων που επηρεάζουν τον χώρο. Όπως έχει ήδη αναφερθεί, η παρούσα μελέτη θα κινηθεί σε τρία διαφορετικά πλαίσια: (Martin Herman, 2024) (Manoj & Bhaskari, 2016) (Purnaye & Kulkarni, 2022) (Egho-Promise, et al., 2024).

- Τεχνικές προκλήσεις
- Νομικές προκλήσεις
- Οργανωτικά ζητήματα που απαιτούν επίλυση

Αυτές οι διαστάσεις θα αναλυθούν με στόχο τη διαμόρφωση ενός ολοκληρωμένου πλαισίου αντιμετώπισης των προκλήσεων που αντιμετωπίζει η ψηφιακή εγκληματολογία στο cloud.

3.2 Τεχνικές προκλήσεις

Οι τεχνικές προκλήσεις που αξίζουν αναφοράς μπορούν να κατηγοριοποιηθούν σε τρεις μεγάλους πυλώνες: (Manoj & Bhaskari, 2016).

- Προκλήσεις που οφείλονται στη φύση της διαδικασίας αποθήκευσης των δεδομένων. Αυτές περιλαμβάνουν ζητήματα σχετικά με την ακεραιότητα, την αξιοπιστία και την ασφάλεια κατά την αποθήκευση των πληροφοριών σε cloud περιβάλλοντα, αλλά και

τον διαχωρισμό τους σε πολυδιαμοιραζόμενα περιβάλλοντα (περιβάλλοντα πολυμίσθωσης).

- Προκλήσεις που σχετίζονται με τη φύση των ίδιων των δεδομένων. Η πολυπλοκότητα και η ευμεταβλητότητα των δεδομένων αποτελούν καθοριστικούς παράγοντες που επηρεάζουν τη διαδικασία ανάλυσής τους.
- Προκλήσεις που αφορούν την ύπαρξη αντιδικανικών τεχνικών. Πρόκειται για τεχνικές που χρησιμοποιούνται σκόπιμα για να δυσχεράνουν ή να εμποδίσουν τη διαδικασία ψηφιακής εγκληματολογικής έρευνας.

3.2.1 Φύση δεδομένων, αποθήκευση και πρόσβαση

Ένα από τα πιο σημαντικά πλεονεκτήματα των δομών cloud είναι η αδιαφάνεια στην υλοποίηση των υποδομών(abstraction) (Cloud Native , 2022). Όταν αναφέρεται η αδιαφάνεια, δεν υπονοείται φυσικά κάποια δόλια απόκρυψη των υλοποιήσεων που ο χρήστης δεν μπορεί να δει. Τουναντίον, αναφερόμαστε στην προσπάθεια απλοποίησης της εμπειρίας χρήστη, αλώστε μικρή αξία θα είχε η γνώση των δομών αποθήκευσης δεδομένων. Αυτή η αδιαφάνεια έχει υπάρξει πολύ σημαντικός παράγοντας στην ανάπτυξη των cloud υπηρεσιών, αλλά αποτελεί και σημαντικό ζήτημα στην αναζήτηση δεδομένων σε περίπτωση εγκληματολογικής έρευνας.

Ποιος είναι ο τρόπος αποθήκευσης δεδομένων; Τα δεδομένα, αρχικά σε πολύ χαμηλό επίπεδο, αποθηκεύονται σε φυσικούς δίσκους, και συνήθως σε συστοιχίες φυσικών δίσκων, χρησιμοποιώντας διάφορες τεχνικές που εξασφαλίζουν την εγκυρότητα και ασφάλεια των δεδομένων. Έτσι, μπορούμε να έχουμε δεκάδες σκληρούς δίσκους, οι οποίοι δημιουργούν αντίγραφα των δεδομένων μεταξύ τους, όμως σε ανώτερο επίπεδο αποκρύπτεται αυτή η πολυπλοκότητα και η διαδικασία.

Και σε αυτές τις υποδομές μπορούμε να ξεχωρίσουμε διαφορετικές μορφές αποθήκευσης δεδομένων. Έτσι, υπάρχει το Direct Attached Storage (DAS), Network Attached Storage (NAS) και Storage Area Network (SAN). Η κάθε διαφορετική διάταξη χρησιμοποιείται για διαφορετικούς σκοπούς. Έτσι, τα DAS θεωρούνται άμεσα συνδεδεμένα με servers. Είναι μια υποδομή που δεν δίνει την καλύτερη εκμετάλλευση πόρων, και έτσι δεν είναι η πιο χρήσιμη

στο cloud περιβάλλον. Στα Storage Area Networks (SAN), ουσιαστικά υλοποιείται η δομή που περιεγράφηκε, και έτσι μια συλλογή από συστοιχίες δίσκων δημιουργεί ένα δίκτυο μαζί με υποδομές servers που έχουν πρόσβαση σε αυτές. Στα Network Attached Storage (NAS), τα συστήματα αρχείων θεωρούνται εξωτερικά, και η σύνδεση γίνεται σε επίπεδο αρχείων. Η υποδομή NAS δεν είναι η πρωταρχική που επιλέγεται για την υλοποίηση μιας cloud υποδομής, μπορεί εντούτοις να αποτελέσει βοηθητική υποδομή εξωτερικών αρχείων, που και αυτά υπόκεινται στη διαδικασία εγκληματολογικής ανάλυσης. (Castagna, 2024).

Τέλος, σε επίπεδο υπηρεσίας, δίνονται περισσότερες επιλογές όσον αφορά το είδος των δεδομένων που αποθηκεύονται. Τα δεδομένά μπορούν να είναι στις παρακάτω μορφές.

Αποθήκευση με τη μορφή blob ή object (Google cloud , 2024), δηλαδή δίνεται η δυνατότητα κατά βούληση αποθήκευσης σε έναν προκαθορισμένο χώρο, και χρησιμοποιείται για την αποθήκευση μεγάλου όγκου μη δομημένων αρχείων. Μπορεί αυτά να είναι αρχεία βίντεο, εικόνας, ήχου, κειμένου. Σε αυτή τη δομή δεν προσφέρεται μια δομή ανάκτησης και συσχέτισης των δεδομένων, και αποτελεί την πιο οικονομική λύση. Έτσι, ουσιαστικά ο πελάτης είναι υπεύθυνος για τη χρήση και διάρθρωση των δεδομένων. (Vivek, 2022).

Αποθήκευση σε δομή αρχείων (file storage). Συνήθως υποστηρίζουν τα πρωτόκολλα NFS και SMB, και είναι μια συνήθης επιλογή όταν απαιτείται ο διαμοιρασμός αρχείων. Κάθε πάροχος υλοποιεί το πρωτόκολλο με τον δικό του τρόπο, αλλά η πρόσβαση είναι δυνατή σε επίπεδο αρχείου.

Εναλλακτικά, υπάρχει η δυνατότητα χρήσης δομών αποθήκευσης που διατηρούν κάποια δομή (π.χ. Table Storage). Εδώ, το πλεονέκτημα είναι αυτή ακριβώς η συσχέτιση των δεδομένων, που μπορεί να δώσει και την αποδοτική χρήση τους.

Τέλος, υπάρχουν και οι δομές αποθήκευσης block. Σε αυτή την περίπτωση, τα δεδομένα κατακερματίζονται σε μικρότερα κομμάτια (blocks) και το κάθε ένα αποθηκεύεται κρατώντας μια μοναδική διεύθυνση. Ο τρόπος αυτός παρέχει ευελιξία και ταχύτητα, αλλά όπως και σε άλλες δομές, υλοποιείται διαφορετικά από κάθε πάροχο. Αυτό σημαίνει

πρακτικά ότι σε χαμηλότερο επίπεδο, τα δεδομένα δεν είναι ίδια και συγκρίσιμα μεταξύ των παρόχων.

Σε επίπεδο συστήματος αρχείων(file system). Χρησιμοποιούνται κατανεμημένα συστήματα διαχείρισης αρχείων, στα οποία δίνεται η δυνατότητα αποθήκευσης και διαχείρισης της ποσότητας των δεδομένων, χρησιμοποιώντας τις συστοιχίες δίσκων και δη των SAN, που προαναφέρθηκαν, χωρίς όμως ο τελικός χρήστης να έχει εικόνα της υλοποίησης και εν τέλει της τοποθεσίας αποθήκευσης των αρχείων του. (Arel, 2022). Κάθε πάροχος υλοποιεί αυτό το σύστημα με τον δικό του τρόπο. Η Amazon, σε χαμηλότερο επίπεδο, χρησιμοποιεί κατανεμημένο NFSv4.1 για την αποθήκευση αρχείων, ενώ για την αποθήκευση αντικειμένων χρησιμοποιεί κυρίως τα συστήματα ext4 ή NTFS. Για την αποθήκευση μπλοκ, χρησιμοποιούνται διάφορα συστήματα, όπως ext4, XFS, NTFS και FAT32. Σε ακόμη χαμηλότερο επίπεδο, η Amazon αξιοποιεί μια τροποποιημένη έκδοση του HDFS (Hadoop Distributed File System). Αντίστοιχα, οι επιλογές του Azure περιλαμβάνουν NTFS και HDFS για τα αντικείμενα, και SMB και NTFS για τα αρχεία. Από την πλευρά της, η Google χρησιμοποιεί τις δικές της επιλογές, με κύρια τεχνολογία το Colossus, ένα σύστημα αρχείων που βασίζεται στο Google File System (GFS). (Google, 2021)

Όλα τα παραπάνω καταδεικνύουν, πέρα από την πολυπλοκότητα και την ποικιλία των επιλογών, την αδυναμία του τελικού χρήστη ή, εν τέλει, του ερευνητή να γνωρίζει πού βρίσκονται τα δεδομένα και πως ακριβώς είναι αποθηκευμένα. Ένα αρχείο ήχου και ένα κείμενο μπορεί να αποθηκεύονται σε διαφορετικού είδους δομές, που ενδεχομένως καταλήγουν σε διαφορετικές υποδομές αποθήκευσης δεδομένων και, κατ' επέκταση, σε διαφορετικές συστοιχίες δίσκων και σε σπάνιες περιπτώσεις και σε διαφορετικές φυσικές τοποθεσίες και χώρες. Η αδυναμία αυτή δεν είναι φυσικά το μόνο ζήτημα. Η μη συγκρισιμότητα των διαφορετικών τρόπων υλοποίησης των δομών αποθήκευσης σημαίνει ότι απαιτούνται εξειδικευμένες λύσεις για κάθε πάροχο, ώστε να καταστεί δυνατή η ανάκτηση αρχείων και αποδείξεων.

Συμπερασματικά, όταν έρχεται η στιγμή της μελέτης, δεν είναι απαραίτητα αυτονόητο ποιος έχει τελικά πρόσβαση σε κάθε φυσική τοποθεσία και κάθε δομή, ενώ είναι ακόμα πιο σύνθετο να ανακτηθούν δεδομένα αλλά και να παρακολουθηθούν οι ενέργειες με στόχο την αναγνώριση πρόσβασης στα δεδομένα και σε ποιο επίπεδο έγιναν αυτές. Απαιτούνται

συνεπώς σύνθετα συστήματα διαχείρισης πρόσβασης (Identity & Access Management) σε επίπεδο χρηστών, και ακόμα πιο αυστηρές διαδικασίες σε επίπεδο υποδομής. Αυτό πρέπει να συνεπικουρείται και από την καταγραφή των ενεργειών που πραγματοποιούνται στα δεδομένα, αλλά και από τον συνεχόμενο έλεγχο για τη συμμόρφωση με κανονιστικά πλαίσια. Επιπλέον, η κρυπτογράφηση που γίνεται και πρέπει να γίνεται κατά την αποθήκευση και τη μεταφορά δεδομένων, δυσχεραίνει την εργασία αναγνώρισης της τροποποίησής τους. Πέρα από τα παραπάνω, υπάρχει ενδεχομένως και η διαδικασία της ανάκτησης δεδομένων. Υπάρχει η περίπτωση ανάγκης επαναφοράς αυτών που έχουν χαθεί ή καταστραφεί, και η στοιχειοθέτηση της παράβασης μέσω των ίδιων των δεδομένων. Τέλος, ένα από τα πιο σημαντικά στοιχεία είναι και η σωστή διατήρηση των μεταδεδομένων των αρχείων. Σε αυτά περιλαμβάνονται πληροφορίες όπως χρονικές σφραγίδες, αναγνωριστικά χρηστών που προσπελαύνουν έναν πόρο, στοιχεία ιδιοκτησίας, μεταβολές στην τοποθεσία ή στα δικαιώματα πρόσβασης, καθώς και κάθε άλλο δεδομένο που συνδράμει στην τεκμηρίωση της ύπαρξης και της διαχείρισης ενός ψηφιακού πόρου. (Pichan, 2022) (Prakash, et al., 2021) (Djalovic, 2025)

Τα εν λόγω μεταδεδομένα διαδραματίζουν καθοριστικό ρόλο στο πλαίσιο της ψηφιακής εγκληματολογικής διερεύνησης για πληθώρα λόγων, καθιστώντας τη διατήρησή τους απολύτως κρίσιμη. Συγκεκριμένα, μέσω της αξιοποίησης των μεταδεδομένων, είναι εφικτός ο εντοπισμός και η ταυτοποίηση χρηστών και συσκευών που έχουν αποκτήσει πρόσβαση σε συγκεκριμένους πόρους, η τεκμηρίωση της ακεραιότητας των δεδομένων, η αναγνώριση ενδεχομένως ύποπτης δραστηριότητας, καθώς και η ανασύσταση της χρονικής ακολουθίας των συμβάντων.

Σε νομικό επίπεδο, τα μεταδεδομένα θεωρούνται κρίσιμα για τη διασφάλιση της αποδεικτικής ισχύος ενός ψηφιακού πόρου, ενώ παράλληλα απαιτείται ιδιαίτερη μέριμνα κατά τη χρήση και την επεξεργασία τους, καθώς σε πολλές περιπτώσεις εμπίπτουν στην

κατηγορία των προσωπικών δεδομένων και υπόκεινται στη σχετική νομοθεσία περί προστασίας της ιδιωτικότητας. (CivicEye, 2025) (Montini, 2025)

Η συνεισφορά τους σε όλες τις προαναφερθείσες πτυχές καθιστά τα μεταδεδομένα αναπόσπαστο και απολύτως απαραίτητο στοιχείο της εγκληματολογικής διαδικασίας, επιβάλλοντας την ορθή, και τεκμηριωμένη διαχείρισή τους

Μετά από τα παραπάνω, ο ερευνητής έρχεται αντιμέτωπος με μια πολυεπίπεδη δομή που θα πρέπει να αντιμετωπιστεί στο σωστό πλαίσιο. Θα πρέπει να αναγνωριστούν οι τοποθεσίες των δεδομένων, και ενδεχομένως η απομακρυσμένη απόκτησή τους μέσω ενός ασφαλούς καναλιού.

Όλα τα παραπάνω δεν μπορούν να πραγματοποιηθούν αν ο πάροχος δεν έχει τις κατάλληλες δομές, και αν η τεχνική γνώση του ερευνητή δεν είναι επαρκής και ενημερωμένη. Επιπλέον, ο πάροχος θα πρέπει να έχει προνοήσει και για την αποθήκευση και διατήρηση των αρχείων καταγραφής, με σκοπό την εξασφάλιση της ύπαρξής τους σε περίπτωση καταστροφής. Μια ενδιαφέρουσα επιλογή είναι και η χρήση των στιγμιότυπων (forensic snapshots). Με αυτά τα ψηφιακά αντίγραφα ενός ολοκληρωμένου συστήματος, είναι δυνατή η μελέτη του συστήματος ακριβώς στη χρονική στιγμή λήψης του τελευταίου στιγμιότυπου που έχει ενδιαφέρον. Φυσικά, τα παραπάνω αποτελούν κοστοβόρες λύσεις, με το κόστος να μετακυλίεται στον πελάτη, και πολύ συχνά να αποφεύγονται τέτοιες λύσεις. (Kavanagh, 2021)

Σε όλα τα παραπάνω θα πρέπει να προσθέσουμε ιδιαίτερα και το πρόβλημα της ύπαρξης δεδομένων σε προσωρινές μνήμες. Τα πολυσύνθετα συστήματα απαιτούν τη χρήση σημαντικού όγκου δεδομένων, που βρίσκονται σε προσωρινές μνήμες και ενδεχομένως να χαθούν για πάντα μετά τη χρήση τους. Σε αυτές τις δομές ενδέχεται να περιλαμβάνονται στοιχεία ενεργών συνεδριών χρηστών, αποθηκευμένα διαπιστευτήρια, συνδέσεις, και άλλα. Στην ψηφιακή εγκληματολογία στο cloud, η διαδικασία ανάκτησης αυτών των δεδομένων είναι ιδιαίτερα δύσκολη, καθώς δεν προβλέπεται η τελική αποθήκευσή τους, ενώ σε φυσικό επίπεδο οι εικονικές μνήμες βρίσκονται σε μη γνωστές υποδομές. Συχνά, ο πάροχος μπορεί

να καταφύγει στη λύση του ελέγχου μηχανών σε λειτουργία, ενώ και το στιγμιότυπο μνήμης είναι κάτι που μπορεί να βοηθήσει.

3.2.2 Ετερογένεια δεδομένων – τυποποίηση δεδομένων

Στα παραπάνω έγινε προφανές ότι υπάρχει ανάγκη για την υποστήριξη του ίδιου του παρόχου στις διαδικασίες εγκληματολογικής μελέτης. Σε κάποιες περιπτώσεις όμως, μια υπόθεση δεν αφορά έναν μόνο πάροχο, αλλά πιθανώς μια συνεργασία δομών ή παρόχων. Σε αυτή την περίπτωση, προκύπτουν τα εξής ερωτήματα:

- Υπάρχει ένα κοινό πρότυπο διατήρησης αρχείων καταγραφής;
- Πώς συνδυάζονται τα αρχεία καταγραφής διαφορετικών ψηφιακών πηγών σε περίπτωση ανάγκης;

Είναι αλήθεια πως μέχρι στιγμής δεν έχει οριστεί ένα ενιαίο πρότυπο για τη διατήρηση αρχείων καταγραφής. Κάθε πάροχος χρησιμοποιεί το δικό του πρότυπο, και τελικά δεν υπάρχει ούτε καν ένα κοινό πρωτόκολλο επικοινωνίας και συνεργασίας μεταξύ παρόχων. Δεδομένα που εξάγονται από το CloudTrail (AWS) δεν μπορούν να συγκριθούν με τα αντίστοιχα από το Stackdriver (Google) ή το Azure Monitor. (Microsoft, 2025), (Aws, 2025)

Το πρόβλημα δεν περιορίζεται μόνο στα αρχεία καταγραφής, αλλά και στα ίδια τα δεδομένα προς μελέτη και ανάλυση. (Casino, et al., 2022). Η υλοποίηση του Blob Storage στη Microsoft είναι εντελώς διαφορετική σε φυσικό επίπεδο από την υλοποίηση μιας δομής Amazon S3 bucket (είτε Object Storage είτε Infrequent Access). Η σύγκριση των δεδομένων σε φυσικό επίπεδο δεν είναι εφικτή, και ο πάροχος πρέπει να αναλάβει τη νοηματοδότηση αυτών των δομών, ώστε να καταστεί δυνατή η ερμηνεία τους. Αντίστοιχες δυσκολίες εμφανίζονται και στην προτυποποίηση των υπολοίπων δομών, στα δεδομένα προσωρινής μνήμης και δεδομένα δικτύου. Όλα αυτά είναι διαθέσιμα σε διαφορετικές μορφές, κάτι που τελικά καθιστά ανέφικτη την προσπάθεια δημιουργίας ενός ενιαίου συστήματος συλλογής και ανάλυσης δεδομένων. (Purestorage, 2024), (DataScienceTest, 2023)

Η έλλειψη τυποποίησης δεν περιορίζεται μόνο στις δομές και τα πρότυπα, αλλά επεκτείνεται και στις πολιτικές. Δεν υπάρχει εγγύηση ότι τα αρχεία καταγραφής που ένας

πάροχος παρέχει για έλεγχο σε πραγματικό χρόνο, θα είναι αντίστοιχα διαθέσιμα και σε άλλους παρόχους, ενώ επιπλέον, σε πολλές περιπτώσεις, ενδέχεται να απαιτείται εξαγωγή και ανάλυση σε δεύτερο χρόνο, κάτι που περιορίζει σημαντικά τη δυνατότητα σύγκρισης των ενεργειών σε πραγματικό χρόνο.

Χαρακτηριστικά, εξετάζοντας τις προεπιλεγμένες πολιτικές των τριών βασικών παρόχων, διαπιστώνονται σημαντικές διαφοροποιήσεις. Στην περίπτωση της AWS, η Amazon υιοθετεί ως προεπιλογή τη διατήρηση των αρχείων καταγραφής επ' αόριστόν, εκτός εάν ο χρήστης ορίσει διαφορετική πολιτική. Παρέχεται η δυνατότητα διαμόρφωσης πολιτικών διατήρησης ανά κατηγορία αρχείων καταγραφής, ενώ η ίδια η εταιρεία προτείνει τη διατήρηση τους για τουλάχιστον 3 έως 12 μήνες για σκοπούς άμεσης ανάλυσης, και έως 7 έτη για λόγους συμμόρφωσης με κανονιστικά πλαίσια (AWS, 2025).

Στην περίπτωση της Azure, η πολιτική διατήρησης εμφανίζεται μεν πιο απλή, αλλά ενέχει αυξημένους κινδύνους. Η προεπιλεγμένη ρύθμιση προβλέπει τη διατήρηση των αρχείων καταγραφής για μόλις 30 ημέρες. Ωστόσο, παρέχεται η δυνατότητα επέκτασης της περιόδου διατήρησης, η οποία μπορεί να κυμαίνεται από 2 έως και 12 έτη, αναλόγως των απαιτήσεων του οργανισμού και του επιπέδου συμμόρφωσης με κανονιστικά ή επιχειρησιακά πρότυπα (Microsoft, 2024).

Στην περίπτωση της Google Cloud Platform (GCP), η πολιτική διατήρησης παρουσιάζει μεγαλύτερη ευελιξία, διαφοροποιούμενη ανάλογα με τον τύπο των αρχείων καταγραφής. Τα απολύτως απαραίτητα αρχεία (*Required logs*) διατηρούνται υποχρεωτικά για 400 ημέρες χωρίς δυνατότητα τροποποίησης, ενώ τα υπόλοιπα αρχεία (*Default και user-defined log buckets*) διαθέτουν προεπιλεγμένη πολιτική διατήρησης 30 ημερών. Παρ' όλα αυτά, ο χρήστης μπορεί να ρυθμίσει την περίοδο διατήρησης εντός εύρους από 1 έως 3.650 ημέρες (δηλαδή έως και 10 έτη), επιτρέποντας έτσι την προσαρμογή των πολιτικών ανάλογα με τις ανάγκες συμμόρφωσης ή ασφάλειας του οργανισμού. Αξίζει, βεβαίως, να σημειωθεί ότι τα αρχεία καταγραφής αποτελούν και αυτά έναν πόρο προς εκμετάλλευση για τους παρόχους υπηρεσιών cloud, καθώς η διατήρηση, η αποθήκευση και η επεξεργασία τους συνδέονται άμεσα με το μοντέλο τιμολόγησης. Συνεπώς, η διατήρηση και χρήση τους για αναλύσεις ενδέχεται να επιφέρει σημαντικό οικονομικό κόστος για τον πελάτη, γεγονός που συχνά

επηρεάζει τις επιλογές του ως προς την πολιτική καταγραφής και αποθήκευσης (Astrafy, 2024).

Σημαντικό ζήτημα αποτελεί, συνεπώς, και η υποχρέωση διατήρησης αρχείων καταγραφής, όπως αυτή διαμορφώνεται από το εκάστοτε νομοθετικό πλαίσιο. Ο Γενικός Κανονισμός για την Προστασία Δεδομένων (ΓΚΠΔ) δεν ορίζει συγκεκριμένη χρονική διάρκεια διατήρησης των αρχείων καταγραφής, αλλά επισημαίνει την αναγκαιότητα ύπαρξής τους στο πλαίσιο της αρχής της λογοδοσίας και της δυνατότητας ιχνηλασιμότητας. Αντιθέτως, στις Ηνωμένες Πολιτείες, σε τομείς όπως ο χρηματοοικονομικός έλεγχος (π.χ. κανονισμός SOX), προβλέπεται η υποχρεωτική διατήρηση αρχείων για τουλάχιστον επτά έτη, γεγονός που εξηγεί και ορισμένες αυστηρότερες προεπιλεγμένες πολιτικές από παρόχους υπηρεσιών cloud.

Σε κάθε περίπτωση, είναι σαφές ότι δεν υφίσταται ενιαία ή ομοιογενής αντιμετώπιση αναφορικά με τη διάρκεια ζωής των αρχείων καταγραφής. Ως εκ τούτου, ο ερευνητής καλείται να διαχειριστεί ένα απροσδιόριστο και συχνά κατακερματισμένο τοπίο, το οποίο μπορεί να περιλαμβάνει είτε τεράστιο όγκο δεδομένων που απαιτεί ομαδοποίηση και ομογενοποίηση, είτε – αντίθετα – μη επαρκή στοιχεία, ικανά να περιορίσουν την εγκληματολογική του ανάλυση και τα αναμενόμενα αποτελέσματα (Londa, 2022) (Microsoft, 2024), (Google, 2025).

3.2.3 Πολυμίσθωση

Γίνεται ήδη εμφανές πως τα ίδια τα εγγενή χαρακτηριστικά του cloud, που αποτελούν το συγκριτικό του πλεονέκτημα, ταυτόχρονα συνιστούν και μεγάλο μειονέκτημα όταν αναφερόμαστε στην ψηφιακή εγκληματολογία. Ένα από αυτά τα χαρακτηριστικά είναι και η δυνατότητα πολυμίσθωσης των υποδομών (ή ενδεχομένως η πολυμισθωτική αρχιτεκτονική). (Kävrestad, et al., 2024), (Pichan, 2022).

Από πολύ νωρίς, οι πάροχοι θεώρησαν ως ιδιαίτερα προσοδοφόρο το να μοιράζουν υποδομές και φυσικούς πόρους μεταξύ χρηστών, προσφέροντας ένα φαινομενικά απομονωμένο περιβάλλον στο επίπεδο των υπηρεσιών. Φαινομενικά, διότι σε φυσικό επίπεδο αυτή η

απομόνωση είναι μάλλον αμφισβητούμενη. Έτσι, με βάση το παραπάνω, οι πάροχοι μπορούσαν να προσφέρουν φθηνές υπηρεσίες, αλλά ταυτόχρονα να παρέχουν και προϊόντα ανώτερου επιπέδου. Δημιουργήθηκε, λοιπόν η διάκριση μεταξύ αυτού αυτό που ονομάζεται Single-tenant Software as a Service (SaaS) και Multi-tenant SaaS (Brook, 2018). Στην περίπτωση του single-tenant, ο πελάτης έχει σε αποκλειστική χρήση τους πόρους μέχρι το φυσικό επίπεδο, είτε την εφαρμογή που έχει εγκατασταθεί αποκλειστικά για αυτόν. Στην αντίθετη περίπτωση, στον πελάτη παρέχεται μια υπηρεσία στην οποία είτε μοιράζεται την εφαρμογή που έχει ζητήσει, είτε μοιράζεται πόρους (Infrastructure as a Service - IaaS). (Prakash, et al., 2021).

Το πιο χαρακτηριστικό παράδειγμα είναι τα εικονικά μηχανήματα (virtual machines), τα οποία τελικά βρίσκονται στον ίδιο εξυπηρετητή. Αντίστοιχα, το ίδιο συμβαίνει και με διατάξεις αποθήκευσης δεδομένων, ενώ το σχήμα μεταφέρεται σε ακόμη πιο σύνθετες υποδομές containers, όπου υπάρχει ένα επιπλέον επίπεδο αφαίρεσης και απομάκρυνσης από το φυσικό επίπεδο. Τελικά, όπως και στην περίπτωση των υποδομών δεδομένων, υπάρχει μια αδιαφάνεια σε σχέση με τη πραγματική τοποθεσία των υποδομών, αλλά και την επίδραση που μπορεί να έχει η πολυπλοκότητα αυτών των συστημάτων.

Όσον αφορά την ψηφιακή εγκληματολογία, το πρώτο πρόβλημα που αναγνωρίζεται είναι η ιδιοκτησία των δεδομένων. Κάθε πελάτης (tenant) κατέχει ένα μικρό ποσοστό χρήσης ενός δίσκου, και είναι αμφίβολο αν η εγκληματολογική ανάλυση μπορεί να περιοριστεί μόνο σε αυτό το κομμάτι χωρίς να περιλαμβάνει την απόδοση δικαιωμάτων πρόσβασης σε γειτονικά στοιχεία του φυσικού δίσκου, τα οποία δεν ανήκουν στον χρήστη ή στο σύστημα αναφοράς. Αυτό, πέρα από τη δυσκολία στη μελέτη, εγείρει και το πρόβλημα της μόλυνσης των δεδομένων. Όπως και στην κλασική εγκληματολογία, υπάρχει η απαίτηση για τη μη ανάμειξη δεδομένων που μπορεί να επηρεάσουν το τελικό αποτέλεσμα. (Flores, 2023) (Mathew, 2024). Η έννοια της μόλυνσης δεδομένων αναφέρεται ουσιαστικά στη μη εξουσιοδοτημένη πρόσβαση σε δεδομένα άλλων ενοικιαστών σε περιβάλλοντα πολυμίσθωσης, είτε ως αποτέλεσμα σκόπιμων ενεργειών είτε λόγω τεχνικών σφαλμάτων ή παραλείψεων. Τέτοια περιστατικά μπορούν να προκύψουν εξαιτίας λανθασμένων ρυθμίσεων δικαιωμάτων πρόσβασης, κακόβουλων ενεργειών χρηστών ή ανεπαρκούς διαχείρισης των μηχανισμών ελέγχου πρόσβασης. Σε όλες τις περιπτώσεις, το αποτέλεσμα είναι η ακούσια ή εσκεμμένη αποκάλυψη δεδομένων που δεν ανήκουν στον

εξουσιοδοτημένο χρήστη ή διαχειριστή της υπηρεσίας, γεγονός που επιβαρύνει σημαντικά την εγκληματολογική διερεύνηση, καθώς προϋποθέτει την πρόσβαση και ανάλυση δεδομένων που αφορούν πολλαπλούς και ανεξάρτητους πελάτες.

Τα παραπάνω δημιουργούν ένα επιπλέον κίνητρο στους παρόχους να αποτρέψουν την πρόσβαση στο φυσικό μέσο, εφόσον βέβαια η ισχύουσα νομοθεσία τους το επιτρέπει.

Βεβαίως, έχουν καταγραφεί περιπτώσεις άρνησης πρόσβασης σε δεδομένα από παρόχους υπηρεσιών cloud, για διάφορους λόγους. Ένα χαρακτηριστικό παράδειγμα είναι η υπόθεση του San Bernardino, κατά την οποία οι αμερικανικές αρχές αιτήθηκαν πρόσβαση στα δεδομένα iCloud ενός υπόπτου. Η Apple αρνήθηκε να παρέχει πρόσβαση, επικαλούμενη την υποχρέωσή της για προστασία της ιδιωτικότητας και τη διατήρηση της ασφάλειας των δεδομένων των χρηστών.

Αντίστοιχα, στην υπόθεση που είναι γνωστή ως Microsoft Ireland Case, η Microsoft αρνήθηκε να παραδώσει δεδομένα που φυλάσσονταν σε διακομιστή στην Ιρλανδία, με το επιχείρημα ότι το αίτημα των αμερικανικών αρχών δεν είχε δικαιοδοσία επί των δεδομένων που βρίσκονταν σε φυσική τοποθεσία εκτός ΗΠΑ. Το ζήτημα της γεωγραφικής τοποθεσίας των δεδομένων αποτελεί ένα κρίσιμο και διαρκώς επανεμφανιζόμενο πρόβλημα, το οποίο θα αναλυθεί εκτενέστερα στη συνέχεια. (Daskal, 2018)

Συνοπτικά, η άγνοια της φυσικής θέσης ενός εικονικού δίσκου δυσχεραίνει τη συμμόρφωση με την νομοθεσία, ενώ ακόμα και όταν η τοποθεσία είναι γνωστή, ο εκάστοτε πάροχος μπορεί να αρνηθεί την παροχή πρόσβασης, επικαλούμενος θέματα εθνικής κυριαρχίας, ιδιωτικότητας ή προστασίας υποδομών (OnTrack, 2022).

Συμπερασματικά, η πληρότητα και η ποιότητα των δεδομένων που περιλαμβάνονται στα αρχεία καταγραφής τα οποία παρέχει ο πάροχος cloud, αποτελεί καθοριστικό παράγοντα για την επιτυχία μίας εγκληματολογικής έρευνας. Σε περιβάλλοντα πολυμίσθωσης, τα αρχεία καταγραφής ενδέχεται είτε να περιλαμβάνουν πληροφορίες που αφορούν ένα ευρύτερο σύνολο πελατών — δημιουργώντας προβλήματα ιδιωτικότητας και νομικής

συμμόρφωσης — είτε, αντίθετα, να μην περιέχουν επαρκή ή εστιασμένα δεδομένα που να επιτρέπουν την εξαγωγή ασφαλών συμπερασμάτων για έναν συγκεκριμένο πελάτη.

Ακόμη και αν τα δεδομένα έχουν διατηρηθεί τεχνικά από τον πάροχο, η πολιτική πρόσβασης ή η υποχρέωση προστασίας των υπόλοιπων tenants ενδέχεται να απαγορεύει τη διάθεσή τους στον ερευνητή. Σε κάθε περίπτωση, η μελέτη και αξιοποίηση των αρχείων καταγραφής καθίσταται ιδιαίτερα δύσκολη — και σε ορισμένες περιπτώσεις ανέφικτη — με αποτέλεσμα να καθίσταται αδύνατη η ταυτοποίηση του δράστη ή η πλήρης τεκμηρίωση του περιστατικού. (Keyun Ruan, 2011).

Στα διαμοιραζόμενα συστήματα, τόσο σε επίπεδο υποδομών όσο και σε επίπεδο υπηρεσιών, αν δεν απαντηθεί το βασικό ερώτημα της ιδιοκτησίας των δεδομένων και της υποχρεωτικής πολιτικής των παρόχων, η εγκληματολογική ανάλυση καθίσταται ιδιαίτερα επίπονη.

3.2.4 Εργαλεία και λογισμικό

Χτίζοντας με βάση τα παραπάνω, έρχεται στην επιφάνεια και η δυσκολία που ενδεχομένως να συναντήσει ο ερευνητής στην συλλογή αποδείξεων, αλλά δεν καλύπτεται από τα εργαλεία του χώρου. Πολύ συνοπτικά, μπορούμε να κατηγοριοποιήσουμε τα εργαλεία σε τρεις μεγάλες κατηγορίες (Malik, et al., 2024):

- Εργαλεία που χρησιμοποιούνται για την εξαγωγή δεδομένων
- Εργαλεία ανάλυσης δεδομένων
- Εργαλεία για τη δημιουργία αναφορών

Στο πρώτο επίπεδο, την εξαγωγή δεδομένων, τα προβλήματα που προαναφέρθηκαν δεν καλύπτονται από ένα ή μια ομάδα εργαλείων. Υπάρχει απουσία προτυποποίησης και συνήθως τα εργαλεία που δημιουργούνται αναφέρονται σε έναν ή το πολύ δύο από τους μεγάλους παρόχους, με αποτέλεσμα ο ερευνητής να χρειάζεται να έχει υπόψιν του τουλάχιστον μια συλλογή λύσεων. Στο δεύτερο επίπεδο, στα εργαλεία ανάλυσης, υπάρχει ενδεχομένως η ανάγκη μετατροπής των δεδομένων σε μια κοινή εμφάνιση, ώστε να υπάρχει συμβατότητα. Ακόμα και αν αυτό το πρόβλημα έχει ξεπεραστεί, πάντα θα υπάρχει το ζήτημα της εξειδίκευσης. Ακόμη και αν το ζήτημα της πρόσβασης στα δεδομένα έχει σε

κάποιο βαθμό αντιμετωπιστεί, παραμένει η πρόκληση της εξειδίκευσης των εργαλείων που χρησιμοποιούνται στην εγκληματολογική έρευνα. Υπάρχουν εργαλεία που εστιάζουν κυρίως στη δημιουργία στιγμιότυπων δεδομένων, καθώς και άλλα που στοχεύουν στην ανάλυση των ήδη αποκτηθέντων δεδομένων.

Χαρακτηριστικά, εργαλεία όπως το Google Cloud Persistent Disk Snapshots, το AWS Snapshot Utility και η Azure Disk Snapshot λειτουργικότητα εξειδικεύονται στη λήψη στιγμιότυπων (snapshots), με στόχο τη διατήρηση της κατάστασης ενός συστήματος σε συγκεκριμένη χρονική στιγμή. Αντίθετα, εργαλεία όπως το Autopsy, το Magnet AXIOM και το Cellebrite UFED επικεντρώνονται στην ανάλυση δεδομένων που έχουν ήδη εξαχθεί, παρέχοντας δυνατότητες εξερεύνησης αρχείων, και ουσιαστικά εγκληματολογικής έρευνας.

Έχει ιδιαίτερο ενδιαφέρον επίσης να γίνει και μια προσέγγιση των εργαλείων που προσφέρουν οι πάροχοι και να διαπιστωθεί και σε αυτό το πλαίσιο η εξειδίκευση. Αρχικά και

εκεί θα γίνει η κατηγοριοποίηση με βάση το αντικείμενο χρήσης και έτσι αναγνωρίσουμε τις ακόλουθες κατηγορίες

- Εργαλεία παρακολούθησης και καταγραφής
    - AWS – CloudTrail : Παρακολούθηση και καταγραφή δραστηριότητας σε όλη την υποδομή cloud της Amazon. (AWS, 2025)
    - AWS – CloudWatch logs – Συλλογή και Παρακολούθηση αρχείων καταγραφής. (AWS, 2024)
    - Azure Monitor – Παρακολούθηση της απόδοσης των διαφόρων υπηρεσιών
    - Azure AD logs – Παρακολούθηση του Azure Active Directory. (Microsoft, 2025)
    - Google Cloud – Audit logs – Καταγραφή ενεργειών χρηστών και διαφόρων αιτημάτων (Google, 2024)
    - Cloud logging – Συνδυασμός των αρχείων καταγραφής από τις διάφορες πήγες του Google Cloud (Google, 2024)
    - Λοιπά - IBM cloud monitoring, Alibaba ActionTrail, etc.
- Εργαλεία αναγνώρισης απειλών
    - AWS GuardDuty – Ανίχνευση απειλών με χρήση μηχανικής μάθησης
    - Azure Sentinel – Ανίχνευση επιθέσεων και προληπτική αντιμετώπιση απειλών.
    - Google Cloud Security Operations – Αποθήκευση και ανάλυση δεδομένων για αναγνώριση και αντιμετώπιση απειλών. (Google, 2024)
    - IBM Cloud Qradar – Παρακολούθηση δικτύου (IBM, 2025)
- Εργαλεία για προστασία δεδομένων
    - AWS Macie – Αναγνώριση και προστασία ευαίσθητων δεδομένων με μηχανική μάθηση. (AWS, 2025)
    - Azure information protection – Κατηγοριοποίηση και προστασία δεδομένων
    - Google Cloud data loss prevention – Κατηγοριοποίηση ευαίσθητων δεδομένων για την αποτροπή διαρροής τους. (Google, 2024)
- Εργαλεία για την αντιμετώπιση περιστατικών
    - AWS Security Hub – Το βασικό εργαλείο για την κεντρική αντιμετώπιση περιστατικών
    - Azure Sentinel

- Google Cloud – Security Command center

- Εργαλεία διαχείρισης πρόσβασης και ρόλων
  - AWS – Identity and Access management – Ελέγχει την πρόσβαση σε πόρους
  - Azure – Active directory – Διαχείριση χρηστών και ρόλων
  - Google Cloud – Identity and Access management – Ελέγχει την πρόσβαση σε πόρους

Τα ανωτέρω συνιστούν ενδεικτικά παραδείγματα εργαλείων που προσφέρονται από τους παρόχους υπηρεσιών. Ορισμένα εξ αυτών λειτουργούν προληπτικά, ενώ άλλα αξιοποιούνται κυρίως για την απόκριση σε επιθέσεις και την εν συνεχεία ανάλυση του περιστατικού. Καθίσταται σαφές ότι ο τελικός χρήστης εξαρτάται σε μεγάλο βαθμό από την επιλογή παρόχου, γεγονός που ενδέχεται να οδηγήσει στο φαινόμενο του τεχνολογικού εγκλωβισμού. Το αποτέλεσμα είναι, συχνά, μια μονομερής εξειδίκευση, η οποία δυσχεραίνει την διαχείριση των περιστατικών. Επιπλέον, διαμορφώνεται ένα καθεστώς αβεβαιότητας ή και ασάφειας ως προς τα πρότυπα που ενδέχεται να εφαρμόζονται. Η προβληματική των προτύπων αποτελεί μια σημαντική πρόκληση και έχει πέρα από τον τεχνολογικό εγκλωβισμό, και το αποτέλεσμα της αδυναμίας συγκερασμού πληροφορίας Έτσι, δεδομένου ότι τα στοιχεία μπορεί να είναι διασπαρμένα σε πολλά συστήματα, ενδεχομένως να χρειάζονται πολλαπλά εργαλεία για την εξαγωγή και ανάλυση των δεδομένων. (Prakash, et al., 2021). Επιπλέον, πολλά από τα εργαλεία έχουν δημιουργηθεί αρχικά για μη-cloud υποδομές και δεν είναι κατάλληλα στοχευμένη η λειτουργία τους. Αυτό το ζήτημα διορθώνεται, όμως ο κατακερματισμός του χώρου παραμένει.

3.2.5 Αντι-δικανικές τεχνικές

Στις τεχνικές προκλήσεις των συστημάτων που μελετώνται, έρχονται να προστεθούν και τεχνικές προκλήσεις που δημιουργούνται από τις εξελίξεις των επιτιθέμενων. Είναι γνωστό πως πολύ συχνά το έγκλημα προηγείται σε μεθόδους, και δεν θα μπορούσε να είναι εξαίρεση και ο χώρος του ψηφιακού εγκλήματος. Αυτό που παρουσιάζει ιδιαίτερο ενδιαφέρον στην ψηφιακή εγκληματολογία στο cloud είναι οι τεχνικές που αναπτύσσουν οι επιτιθέμενοι για να κρύψουν ή να αλλοιώσουν τα πιθανά αποδεικτικά στοιχεία. Αυτές

ονομάζονται αντιδικανικές τεχνικές, και οι σημαντικότερες είναι οι ακόλουθες: (Satvik Gurjar, 2023), (HackTheBox, 2023).

1. **Αλλοίωση ή καταστροφή στοιχείων.** Ο επιτιθέμενος, με την έξοδό του, καταστρέφει τόσο τα στοιχεία που χρησιμοποίησε, όσο και τα γειτονικά, με στόχο να αποκρύψει το σημείο της επίθεσής του αν αυτή είναι στοχευμένη, καθώς και να αποκρύψει ίχνη που μπορεί να έχει αφήσει. Επιπλέον, μπορεί η καταστροφή αυτή να επεκταθεί και σε αρχεία καταγραφής, κάτι που θα αποτρέψει την ανάλυση σε ακόμα πιο χαμηλό επίπεδο.
2. **Κρυπτογράφηση αποτυπωμάτων.** Στην περίπτωση αυτή, ο επιτιθέμενος κρυπτογραφεί με τρόπο μη αναστρέψιμο τα πιθανά ίχνη του, με αποτέλεσμα, ενώ είναι εμφανές ότι έχει υπάρξει επίθεση, να μην είναι εφικτό να διαβαστούν τα ίχνη.
3. **Παραπλανητικά στοιχεία.** Σε πολλές περιπτώσεις, χρησιμοποιείται ο συνδυασμός των παραπάνω, αλλά δημιουργούνται και ψευδή στοιχεία για να ωθήσουν τις έρευνες σε λάθος κατεύθυνση. Τα ψευδή στοιχεία αυτά μπορούν να οδηγήσουν την έρευνα σε σημεία που επιλέγει ο επιτιθέμενος, τα οποία ουσιαστικά δεν έχουν καμία αξία.
4. **Χρήση ειδικών περιβαλλόντων** (sandbox) ώστε να μπορούν να αποκρύψουν το σημείο εκκίνησης της επίθεσης.
5. **Παραποίηση και χρονική παραποίηση μεταδεδομένων.** Ο επιτιθέμενος τροποποιεί τα μεταδεδομένα των αρχείων που έχει υποκλέψει, και ιδιαίτερα αυτά που έχουν χρονοσήμανση, ώστε να μπορέσει να δημιουργήσει μια λανθασμένη χρονική αλληλουχία γεγονότων.
6. **Εγκατάσταση rootkits**. Ειδικό λογισμικό που δύναται να αποκρύψει την ύπαρξη κακόβουλων προγραμμάτων.
7. **Στεγανογραφία**. Εισαγωγή μηνυμάτων σε εικόνες και χρήση τους ως μέθοδο επικοινωνίας.

Η παραπάνω λίστα δεν είναι εξαντλητική, αλλά δίνει μια εικόνα του πώς ο επιτιθέμενος μπορεί να προστατευτεί απέναντι στην ανάλυση (Shadawck, 2022).

Είναι αυτονόητο πως, δεδομένης μιας επίθεσης, το σύστημα μπορεί να βρεθεί σε μια κατάσταση μη αναστρέψιμη, και εδώ είναι που αρχίζει να παρουσιάζεται πιο ξεκάθαρα και η ανάγκη της πρόληψης. Και όπως έχει σημειωθεί νωρίτερα, δεν γίνεται αναφορά στην

πρόληψη απέναντι στην επίθεση, αλλά στην πρόληψη με σκοπό την αναγνώριση του προβλήματος και του επιτιθέμενου, παροχή δεδομένων και εν τέλει επίλυση του προβλήματος.

3.3 Νομικές προκλήσεις

Μελετώντας μια νέα υπόθεση, ένας ερευνητής έχει να απαντήσει μια σειρά από ερωτήματα, τα οποία θα καθορίσουν τις ενέργειες που θα ακολουθήσουν. Οι βασικές αυτές ερωτήσεις είναι:

- Ποιος είναι αυτός που μπορεί να συλλέξει τα δεδομένα; Είναι διαθέσιμα στον ίδιο τον ερευνητή;
- Ποια είναι η δικαιοδοσία που ισχύει;
- Υπάρχει η δυνατότητα για την υποχρέωση παροχής δεδομένων;
- Ποια είναι τα εργαλεία στη διάθεση του ερευνητή;
- Ποιες είναι οι διαδικασίες για τη χρήση και διαφύλαξη των αποδείξεων, ώστε αυτές να γίνονται αποδεκτές στα δικαστήρια;

Αυτές οι ερωτήσεις αποκαλύπτουν άμεσα ότι ένα από τα βασικά ζητήματα της διαδικασίας αφορά το νομικό κομμάτι και τη συμμόρφωση με νομοθεσίες και κανόνες. Η συμμόρφωση αυτή αφορά όλους τους εμπλεκόμενους φορείς. Από την πλευρά του, ο καθένας μπορεί να δημιουργήσει προβλήματα που θα καθυστερήσουν ή και θα ακυρώσουν τη διαδικασία. Είναι αναγκαίο να γίνει μια προσπάθεια τόσο ορισμού του προβλήματος όσο και της αντιμετώπισής του. (Willson, 2013) (Allahrakha, 2024).

Στα νομικά ζητήματα, αναγνωρίζουμε τις ακόλουθες διακριτές περιπτώσεις προβλημάτων.

3.3.1 Δικαιοδοσίες – Συμμόρφωση με διεθνείς κανονισμούς

Το ζήτημα της δικαιοδοσίας είναι ιδιαίτερα πολύπλοκο γενικά, πόσο μάλλον στον τομέα του cloud. Στην παραδοσιακή ψηφιακή εγκληματολογία, η αναγνώριση της τοποθεσίας των δεδομένων ήταν σχετικά εφικτή, καθώς δεν υπήρχε η έννοια των κατανεμημένων συστημάτων. Έτσι σε περίπτωση επιλογής δικαιοδοσίας με βάση την τοποθεσία των

δεδομένων, οι κανόνες μπορούσαν να εφαρμοστούν χωρίς πρόβλημα καθώς η τοποθεσία ήταν μια και γνωστή. Στην ψηφιακή εγκληματολογία στο cloud, τα δεδομένα μπορεί να είναι διαμοιρασμένα σε πολλαπλές τοποθεσίες, ενώ δεν υπάρχει καμία διασφάλιση ότι ο πάροχος δεν θα μετακινήσει τα δεδομένα κατά βούληση. Έτσι, δεν μπορεί να υπάρχει διασφάλιση ότι τα δεδομένα δεν βρίσκονται ταυτόχρονα σε διαφορετικές χώρες, οι οποίες, εκ των πραγμάτων, διέπονται από διαφορετικούς κανόνες σχετικά με τη λήψη, συντήρηση και αρμοδιότητα στην έρευνα τους.

Για την προσέγγιση αυτού του ζητήματος έχουν αναπτυχθεί μια σειρά από θεωρίες σχετικά με τη δικαιοδοσία, που έχουν ιδιαίτερη αξία περνώντας σε cloud υποδομές. (Karagiannis & Vergidis, 2021).

1. **Τοποθεσία διάπραξης του εγκλήματος**. Σύμφωνα με τη θεωρία αυτή, η αρμοδιότητα ανήκει στη χώρα στην οποία διαπράχθηκε το έγκλημα, κάτι που ήδη έχει δημιουργήσει ζητήματα όπως αναφέρθηκε, σε σχέση με την ολότητα των δεδομένων στην συγκεκριμένη τοποθεσία. Αντικείμενο είναι η αναζήτηση της τοποθεσίας του data center όπου βρίσκονται τα δεδομένα, χωρίς αυτό να σημαίνει ότι αναφερόμαστε σε μια αποκλειστική τοποθεσία. Υπάρχουν σοβαρές πιθανότητες να συζητάμε για πολλά data center, με αποτέλεσμα να αναγνωρίζεται δικαιοδοσία σε όλες τις εμπλεκόμενες τοποθεσίες.
2. **Τοποθεσία του μέσου διάπραξης του εγκλήματος**. Βάσει αυτής της θεωρίας, η σημαντικότητα έγκειται στην τεχνική υποδομή που χρησιμοποιήθηκε για τη διάπραξη του εγκλήματος. Επομένως, αν χρησιμοποιήθηκε μια υποδομή cloud στην Ευρώπη, τότε η δικαιοδοσία για την έρευνα μπορεί να αποδοθεί στις Ευρωπαϊκές αρχές, με ό,τι συνέπειες μπορεί να έχει αυτό για τις εισαγγελικές παραγγελίες σχετικά με τα δεδομένα. Εδώ είναι προφανές ότι παραβλέπεται η τοποθεσία των δεδομένων, κάτι που κατά τη διάρκεια της έρευνας μπορεί πράγματι να αποτελέσει ζήτημα και εν τέλει εμπόδιο. Το ζητούμενο είναι η τοποθεσία ευθύνης του ίδιου του παρόχου cloud μέσω των υποδομών του οποίου, επιτυγχάνεται η διάπραξη του εγκλήματος.
3. **Θεωρία σχετικά με το προϊόν του εγκλήματος**. Ουσιαστικά το ερώτημα αφορά πάλι τα δεδομένα, αλλά αυτή τη φορά εξετάζεται σε ποια περιοχή έχουν δημιουργηθεί τα αποτελέσματα της ενέργειας του δράστη. Στις περισσότερες

περιπτώσεις, αυτό συμπίπτει με την τοποθεσία του δράστη, όμως δεν υπάρχει πλήρης αντιστοιχία, καθώς οι δράστες μπορεί να μεταφέρουν το προϊόν του εγκλήματος σε διαφορετικές τοποθεσίες. Έτσι, το πιο σημαντικό ερώτημα είναι πώς θα ασκηθεί δίωξη σε ένα άτομο για έγκλημα με προϊόν εγκλήματος σε διαφορετική χώρα ή ήπειρο.

4. **Η τελευταία θεωρία αφορά την ίδια την εθνικότητα του δράστη**. Δεν λαμβάνει υπόψη την τοποθεσία του εγκλήματος και των δεδομένων, αλλά ούτε και το αν έχει έρθει σε επαφή με αυτά ο δράστης, και με ποιο τρόπο ορίζεται η επαφή. Γενικά, θα λέγαμε ότι αποτελεί μια μάλλον αδύναμη προσέγγιση σε σχέση με την απόδειξη υπευθυνότητας του δράστη.

Οι τέσσερις αυτές θεωρίες παρουσιάζουν αδυναμίες, τις οποίες μπορούν να εκμεταλλευτούν οι επιτιθέμενοι. Οι επιτιθέμενοι μπορεί να επιλέξουν να κάνουν μια επίθεση από Ευρωπαϊκά συστήματα, τα οποία είναι γνωστό ότι θα παρέχουν δεδομένα στην έρευνα με μεγαλύτερη δυσκολία. Μπορεί, δηλαδή, να εκμεταλλευτούν την αδυναμία συνεργασίας των φορέων και

την μη ύπαρξη πολλαπλών διακρατικών συμφωνιών που δυσχεραίνουν τη δημιουργία ενός κοινού κανόνα παγκοσμίως.

Ο τρόπος με τον οποίο επιτρέπεται η απαγορεύεται η παροχή δεδομένων ανά περιοχή βασίζεται σε διαφορετικούς κανόνες (EU, 2016), (FedRAMP.gov, 2024) (Cooperation, 2022), (Iso.org, 2012). Οι κυριότεροι κανόνες που ισχύουν σε σχέση με τα δεδομένα είναι οι εξής:

- GDPR (General Data Protection Regulation) - Διέπει γεωγραφικά την Ευρωπαϊκή Ένωση και ρυθμίζει την προστασία των προσωπικών δεδομένων. Παρέχει κανόνες για τον έλεγχο πρόσβασης στα δεδομένα.
- Cloud Act (Clarifying Lawful Overseas Use of Data Act) - Διέπει τις αρχές των ΗΠΑ και δίνει τη δυνατότητα για απαίτηση δεδομένων από παρόχους, ακόμα και αν αυτά βρίσκονται εκτός των ΗΠΑ.
- ISO/IEC 27037 - Ένα διεθνές πρότυπο για τη συλλογή και διατήρηση ψηφιακών αποδείξεων. Είναι πρότυπο χωρίς νομική δέσμευση.
- FedRAMP (Federal Risk and Authorization Management Program) - Κανονισμός που θεωρείται προαπαιτούμενος για συνεργασία με ομοσπονδιακές υπηρεσίες στις ΗΠΑ. Ορίζει μια σειρά απαιτήσεων ασφαλείας.

Οι κανόνες αυτοί ενδέχεται να δημιουργήσουν συγκρούσεις, όπως για παράδειγμα η σύγκρουση μεταξύ GDPR και Cloud Act. Με βάση τον δεύτερο κανονισμό, σε μια έρευνα υπάρχει η δυνατότητα να ζητηθούν δεδομένα που βρίσκονται σε Ευρωπαϊκούς παρόχους από Αμερικανικές αρχές. Εντούτοις, ο Γενικός Κανονισμός Προστασίας Δεδομένων μπορεί να απαγορεύσει την παροχή τους. Σε μια πραγματική τέτοια περίπτωση, το δικαστήριο επέβαλε την παροχή των δεδομένων, παρά τις αντιρρήσεις της ΕΕ.

3.3.2 Προκλήσεις απορρήτου και ασφάλειας - Αποθήκευση δεδομένων

Επιπλέον, ένα σημαντικό ζήτημα που ανακύπτει είναι η ιδιοκτησία των δεδομένων, η αποθήκευσή τους και η διατήρησή τους. Οι νόμοι που διέπουν την προστασία των δεδομένων

έχουν μεγάλη σημασία και συχνά έρχονται σε αντίθεση με τις ανάγκες μιας εγκληματολογικής έρευνας.

Τα δεδομένα κατατάσσονται σε διάφορες κατηγορίες, με κάθε κατηγορία να αντιμετωπίζεται διαφορετικά ως προς τη σπουδαιότητά της. Για παράδειγμα, σύμφωνα με τον Γενικό Κανονισμό Προστασίας Δεδομένων (ΓΚΠΔ) (European Parliament, 2016), απαιτείται η διαγραφή δεδομένων όταν αυτά δεν είναι απαραίτητα, ενώ σύμφωνα με τον νόμο HIPAA, τα ιατρικά δεδομένα πρέπει να διατηρούνται τουλάχιστον για 6 χρόνια. Πέρα από τα δεδομένα καθαυτά, επανερχόμαστε στο θέμα της διατήρησης των δεδομένων ελέγχου, όπως τα αρχεία καταγραφής. Στον τομέα αυτό, δεν υπάρχει σαφές πλαίσιο για την υποχρέωση διατήρησης, με αποτέλεσμα να υπάρχει περιθώριο ερμηνείας των κανονισμών. (Health and Human services, 2003)

Επιπλέον, υπάρχει ασάφεια σχετικά με την ιδιοκτησία των δεδομένων (Flores, 2023). Σε περιβάλλον cloud, ο πάροχος αναφέρει συνήθως ότι δεν είναι ο ιδιοκτήτης των δεδομένων, αλλά παρέχει μόνο την υπηρεσία αποθήκευσης. Παράλληλα, σε υπηρεσίες cloud, οι χρήστες συχνά δεν κατεβάζουν ποτέ τοπικά τα δεδομένα τους και αυτά παραμένουν μόνο σε προσωρινή μνήμη. Γενικά, μπορούμε να συμπεράνουμε ότι, εφόσον τα δεδομένα έχουν γίνει προσβάσιμα, τότε θεωρείται ότι αυτά αποτελούν και κατοχή των δεδομένων, κάτι που ενδέχεται νομικά να αποδειχθεί μη έγκυρο. Επομένως, υπάρχει ανάγκη για έναν διαφορετικό ορισμό της κατοχής των δεδομένων σε σχέση με τα παραδοσιακά ψηφιακά δεδομένα. Η Ευρωπαϊκή Ένωση έχει προτείνει την έννοια τριών επιπέδων για τα δεδομένα: Ανάγνωση, κατοχή και επεξεργασία. Μόνο η επεξεργασία δηλώνει την πραγματική ενέργεια πάνω στα δεδομένα και μπορεί να συνιστά ποινικό αδίκημα. (Flores, 2023)

3.3.3 Νομικές ευθύνες παρόχων cloud υπηρεσιών

Η ιδιοκτησία των δεδομένων, η ύπαρξη διεθνών κανονισμών και οι προαναφερθείσες τοποθεσίες, αναδεικνύουν επίσης το ζήτημα της ευθύνης που ενδέχεται να έχουν οι πάροχοι cloud υπηρεσιών, καθώς αυτοί αποτελούν ουσιαστικά τους κατόχους της φυσικής μορφής της πληροφορίας. Σε γενικές γραμμές, οι πάροχοι έχουν υποχρεώσεις που συνδέονται με τα

αυτονόητα: συμμόρφωση με διεθνείς κανονισμούς και διασφάλιση της ακεραιότητας των δεδομένων, διατηρώντας παράλληλα το απόρρητο αυτών. (Karagiannis & Vergidis, 2021).

Στον τομέα της παροχής δεδομένων, συχνά ο πάροχος βρίσκεται σε ένα κρίσιμο σημείο, όπου πρέπει να λάβει μια απόφαση. Δεδομένης μιας επίσημης αίτησης, ο πάροχος πρέπει να διασφαλίσει ότι δεν παραβιάζεται η νομοθεσία προστασίας προσωπικών δεδομένων. Σε περιπτώσεις άρνησης του παρόχου, το ζήτημα περνά στη δικαστική διαμάχη, η οποία μπορεί να οδηγήσει σε απόφαση, η οποία έρχεται πολύ συχνά αφού τα δεδομένα έχουν καταστραφεί. (Casino, et al., 2022)

Όσον αφορά την ακεραιότητα των δεδομένων, αν και οι πάροχοι οφείλουν να διατηρούν τα δεδομένα, υπάρχει αβεβαιότητα σχετικά με τις ενέργειες που γίνονται στα αρχεία καταγραφής. Σε πολλές περιπτώσεις, τα δεδομένα αυτά μπορεί να διαγραφούν σύμφωνα με την πολιτική της εταιρείας, η οποία δεν έρχεται σε αντίθεση με κάποιο συγκεκριμένο νομικό πλαίσιο (Google, 2025). Είναι ενδιαφέρον να εξετάσουμε εάν είναι σαφές από την αρχή ποια δικαιώματα και υποχρεώσεις έχουν οι πάροχοι σχετικά με την τήρηση αρχείων καταγραφής, τη διατήρηση δεδομένων, τον ορισμό υπευθύνων και τη συνεργασία με τις αρχές. Επίσης, σε αυτή την περίπτωση δεν υπάρχει κάποια διακρατική σύμβαση που να ορίζει όλα τα παραπάνω, με αποτέλεσμα οι πάροχοι να δεσμεύονται μόνο από τους δικούς τους όρους παροχής υπηρεσιών, οι οποίοι ενδέχεται να διαφέρουν ανάλογα με την περίπτωση.

Μετά τα παραπάνω, αξίζει να αναφερθεί πως μια σημαντική προσπάθεια να τεθεί ένα συνολικό πλαίσιο για την αντιμετώπιση του εγκλήματος στον κυβερνοχώρο πραγματοποιήθηκε μέσω της σύμβασης της Βουδαπέστης (Lawspot, 2001). Η συνθήκη αυτή ακολούθησε τις πρωτοβουλίες των G8 για τον ορισμό διεθνών προτύπων σχετικά με την πρόσβαση σε δεδομένα άλλων χωρών.

Σύμφωνα με τις G8, προτάθηκαν τρεις βασικές αρχές:

- Πρόσβαση σε δεδομένα αποθηκευμένα σε πληροφοριακά συστήματα. Κάθε κράτος θα πρέπει να εξασφαλίζει την άμεση διατήρηση δεδομένων, ειδικά αυτών που

διέπονται από κανονισμούς σύντομης διατήρησης ή είναι ευάλωτα σε τροποποίηση ή αλλοίωση.

- Επιτάχυνση αμοιβαίας νομικής συνδρομής. Όταν υπάρξει ένα επίσημο αίτημα για πρόσβαση, αναζήτηση, αντιγραφή κλπ. δεδομένων, το κράτος οφείλει να εκτελέσει το αίτημα άμεσα.
- Διασυνοριακή πρόσβαση σε δεδομένα χωρίς την απαίτηση νομικής βοήθειας. Ένα κράτος δεν χρειάζεται να ζητήσει εξουσιοδότηση από άλλο κράτος όταν ενεργεί σύμφωνα με τη δική του εθνική νομοθεσία για την πρόσβαση σε δημόσια δεδομένα ή για την πρόσβαση σε δεδομένα που βρίσκονται σε υπολογιστή σε άλλο κράτος, εφόσον έχει τη συγκατάθεση του ατόμου που έχει τη νόμιμη εξουσιοδότηση να παραχωρήσει αυτά τα δεδομένα.

Οι παραπάνω αρχές φαίνονται γενικές, προσπαθούν να αντιμετωπίσουν τον πυρήνα του προβλήματος, παρέχοντας γρήγορη και άμεση πρόσβαση στα δεδομένα χωρίς να δημιουργούνται νομικά εμπόδια.

Η σύμβαση της Βουδαπέστης προσπαθεί να θέσει τις βάσεις για την εναρμόνιση των εθνικών νομοθεσιών, την ενίσχυση των τεχνικών διερεύνησης και τη βελτίωση της διεθνούς συνεργασίας. Ωστόσο, δεν είναι μια καθολικά δεσμευτική συνθήκη, καθώς απαιτεί την υπογραφή από τα κράτη μέλη του Συμβουλίου της Ευρώπης και τρίτες χώρες, καθώς και την επικύρωσή της από τις εθνικές νομοθεσίες. Τα κράτη επίσης έχουν τη δυνατότητα να αποδεχτούν ή να υλοποιήσουν μερικώς τις απαιτήσεις. Σύμφωνα με το περιεχόμενο της συνθήκης, στο άρθρο 32Β προβλέπεται η δυνατότητα σε ένα κράτος να λάβει δεδομένα που βρίσκονται σε άλλο κράτος με τη συγκατάθεση του ατόμου που έχει τη νόμιμη εξουσία να αποκαλύψει τα δεδομένα. Στα άρθρα 16 και 29 ορίζονται οι υποχρεώσεις για τη διατήρηση δεδομένων που είναι απαραίτητα για ποινικές έρευνες, ακόμα κι αν αυτά βρίσκονται σε άλλο κράτος. Επιπλέον, καθορίζονται τα σχήματα διεθνούς συνεργασίας, είτε με τη συγκατάθεση, είτε χωρίς αυτή αλλά με νομικά διαπιστευτήρια, είτε χωρίς συγκατάθεση αλλά μέσω παρόχων cloud.

Από το 2011 που τέθηκε σε εφαρμογή η σύμβαση, έχουν σημειωθεί σημαντικές αλλαγές, και είναι σαφές ότι απαιτούνται τροποποιήσεις. Ωστόσο, οι πιο σημαντικές αλλαγές θα πρέπει

να αφορούν τη διεύρυνση της αποδοχής της, συμπεριλαμβανομένων των κρατών που θεωρούν ότι αυτή αντιτίθεται στην κυριαρχία τους (όπως η Ρωσία και η Κίνα).

3.3.4 Ακεραιότητα της αποδεικτικής αλυσίδας

Ένα επίσης πολύ σημαντικό πρόβλημα που συναντάται κατά τη διαδικασία συγκέντρωσης αποδεικτικών στοιχείων στον τομέα της εγκληματολογίας, είναι η διατήρηση της ακεραιότητας της αποδεικτικής αλυσίδας (Chain of Custody) (NIST Glossary, 2024). Συνοπτικά, η διατήρηση της αποδεικτικής αλυσίδας αναφέρεται στο σύνολο των βημάτων που σχηματίζουν τη διαδικασία μέσω της οποίας ένα ψηφιακό αποδεικτικό στοιχείο συλλέγεται, μεταφέρεται, αναλύεται και παρουσιάζεται, διατηρώντας παράλληλα την ακεραιότητά του ως αποδεικτικό στοιχείο. Για να διασφαλιστεί η ακεραιότητά του, θα πρέπει να πληρούνται μια σειρά από προϋποθέσεις (Obbayi, 2019):

Πρώτον, πρέπει να υπάρχουν στοιχεία λήψης ή απόκτησης του αποδεικτικού στοιχείου. *Δεύτερον*, απαιτείται η γνωστοποίηση του τρόπου λήψης του στοιχείου. *Τρίτον*, απαιτείται η γνωστοποίηση της διαδικασίας αποθήκευσης του αποδεικτικού στοιχείου, καθώς και του ποιος έχει πρόσβαση στο αποθετήριο των στοιχείων αυτών.

Με αυτά τα βήματα διασφαλίζεται ότι ένα αποδεικτικό στοιχείο παραμένει αυθεντικό, δεν έχει παραποιηθεί, και υπάρχει πλήρης καταγραφή του ποιος έχει αλληλοεπιδράσει με αυτό. Αυτό από μόνο του αποτελεί ένα ζήτημα που επιφέρει σημαντικές δυσκολίες. Ακόμα και αν ο στόχος περιορίζεται στα ψηφιακά δεδομένα, η διατήρηση των παραπάνω προϋποθέσεων είναι εξαιρετικά δύσκολη, ειδικά όταν το σύνολο των διαχειριστών δεν είναι επαρκώς εκπαιδευμένο. Στο περιβάλλον του cloud, η κατάσταση είναι ακόμα πιο δύσκολη λόγω της πολυπλοκότητας των υποδομών και του πλήθους των ατόμων που μπορεί να έχουν ή να μην έχουν δικαιώματα πρόσβασης σε αυτούς τους πόρους. (Hall, 2024)

Στα δύο διακριτά είδη δεδομένων που μελετάμε, οι απαιτήσεις είναι ελαφρώς διαφοροποιημένες μεταξύ τους. Στα αρχεία καταγραφής, επιθυμητό είναι να υπάρχει αμετάβλητη αποθήκευση από τη στιγμή της έναρξης της έρευνας (ή του σημείου αναγνώρισης του ζητήματος), καθώς αυτά μεταβάλλονται συνεχώς. Θα πρέπει με την αποθήκευσή τους να διατηρηθούν και οι κατάλληλες χρονοσημάνσεις πρέπει να τεκμηριωθεί και ο τρόπος συλλογής τους. Καταγραφή της τοποθεσίας τους και των

συστημάτων που ενεπλάκησαν στην αποθήκευσή τους, ενώ συνήθως απαιτείται και η διαδικασία hashing που τεκμηριώνει τη μη τροποποίηση.. (Suleman, 2025)

Ομοίως, για τα ίδια τα δεδομένα οι απαιτήσεις ξεκινούν από την πλήρη λήψη αντιγράφου του αρχείου, καθώς και τη διαδικασία hashing, που θα πρέπει να συγκριθεί με το αποτέλεσμα πριν την επίθεση, αν υπάρχει. Φυσικά, απαιτείται η τεκμηρίωση της διαδικασίας συλλογής, ενώ πολύ σημαντική είναι και η σωστή αποθήκευση αυτού του αντιγράφου, σε ασφαλή και μη τροποποιήσιμη δομή (EclipseForensics, 2024).

Οι διαδικασίες παροχής και μελέτης αυτών των δεδομένων θα πρέπει πάντα να λαμβάνουν υπόψη την ανάγκη ύπαρξης του μη τροποποιήσιμου πηγαίου αρχείου ως σημείου αναφοράς και διατήρησης (CII, 2021). Το ζήτημα αυτό δεν είναι καθαρά τεχνικό ή νομικό, καθώς απαιτεί συνδυασμένες λύσεις. Το νομικό πλαίσιο και οι κανονισμοί θα πρέπει να επιβάλλουν τη σωστή διατήρηση των στοιχείων, και τα εργαλεία ανάκτησης και μελέτης θα πρέπει να υποστηρίζουν αυτή την απαίτηση για ακεραιότητα. Και οι τρεις κανονισμοί προστασίας δεδομένων που αναφέρθηκαν περιλαμβάνουν προβλέψεις για τα δεδομένα, αλλά δεν είναι ξεκάθαρο πώς τα θεωρούν ως αποδεικτικά στοιχεία.

Πιο συγκεκριμένα, ο κανονισμός ISO/IEC 27037 (Iso.org, 2012), παρέχει κανόνες για τη διατήρηση αποδεικτικών στοιχείων, το Cloud Act (U.S. Department of Justice, 2018) προβλέπει ότι τα δεδομένα που προκύπτουν δεν πρέπει να έχουν υποστεί τροποποίηση, ενώ ο GDPR εστιάζει κυρίως στη διασφάλιση της ιδιωτικότητας και δεν προβλέπει τη διατήρηση των αποδεικτικών στοιχείων. Επιπλέον, η έλλειψη κανονισμών για τη χρονική διατήρηση των αρχείων δημιουργεί επίσης ζητήματα. Συνολικά, η κατεύθυνση του ISO/IEC 27037 φαίνεται να είναι ορθή· ωστόσο, η εφαρμογή του στο περιβάλλον του cloud παραμένει μέχρι στιγμής προβληματική, καθώς οι βασικές αρχές του προτύπου δεν συμβαδίζουν με τη φύση της υπηρεσίας. Ο κύριος λόγος αυτής της προβληματικής εφαρμογής σχετίζεται πρωτίστως με τη δυναμική φύση των δεδομένων. Δευτερευόντως, η απουσία φυσικής πρόσβασης στις υποδομές, καθώς και οι ελλιπείς υποχρεώσεις των ίδιων των παρόχων, καθιστούν τον κανονισμό αδύναμο. Η τεκμηρίωση της απόκτησης, η δημιουργία πιστών (bit for bit)

αντιγράφων, αλλά και η έλλειψη πιστοποιημένων εργαλείων θέτουν συχνά το αποτέλεσμα μιας έρευνας εν αμφιβόλω.

3.3.5 Ηθικά διλήμματα και διαφάνεια στη χρήση δεδομένων

Σε όλα τα παραπάνω ζητήματα, δεν θα πρέπει να παραλείψουμε να αναφερθούμε και στο ηθικό ζήτημα της χρήσης δεδομένων.

Στο πλαίσιο μιας εγκληματολογικής έρευνας, υπάρχει ένα σημείο στο οποίο ο ερευνητής καλείται να προσπελάσει δεδομένα που ενδέχεται να κατατάσσονται στα προσωπικά ή ευαίσθητα προσωπικά δεδομένα. Ποιο είναι το σημείο όπου η διαδικασία θα πρέπει να σταματήσει και ποιο είναι τελικά το πιο σημαντικό, η αναγνώριση του εγκλήματος ή η διασφάλιση της ιδιωτικότητας; Εγείρονται, λοιπόν, ηθικά ζητήματα καθώς και ζητήματα ισότητας μεταξύ των ατόμων (MS Nashua, 2025). Επιπλέον, η καταπάτηση των ηθικών ορίων, τα οποία θα πρέπει φυσικά να ορίζονται με βάση την ισχύουσα νομοθεσία, ενδέχεται να οδηγήσει και σε καταπάτηση των όρων της ορθής εγκληματολογικής έρευνας. Με άλλα λόγια, όπως και με τα φυσικά εγκληματολογικά στοιχεία, υπάρχει η πιθανότητα δημιουργίας παράνομων αποδεικτικών στοιχείων, κάτι που θα τα καθιστούσε αβέβαια και ανίσχυρα στα μάτια του δικαστηρίου. Το ζητούμενο, ωστόσο, δεν είναι να τεθεί ο ερευνητής μπροστά σε ένα τέτοιο δίλημμα, αλλά κυρίως η θέσπιση κανόνων για τη γκρίζα αυτή περιοχή, όπου δεν είναι ξεκαθαρισμένη η προτεραιότητα, και η δημιουργία διαδικασιών που θα διασφαλίσουν την ιδιωτικότητα, προσφέροντας παράλληλα τα δεδομένα που απαιτούνται για την έρευνα, τροποποιημένα ή ανωνυμοποιημένα κατάλληλα και με αποδεκτό τρόπο. (Aleke, 2025)

3.4 Οργανωτικές προκλήσεις

Υπάρχουν περιπτώσεις ζητημάτων στον τομέα της ψηφιακής εγκληματολογίας στο cloud, τα οποία δεν εντάσσονται σε καθαρά τεχνικές ή νομικές διαστάσεις. Αυτές οι περιπτώσεις κατατάσσονται στον οργανωτικό τομέα, και γίνεται μια προσπάθεια προσέγγισης των

δυσκολιών που προκύπτουν κατά την οργάνωση και εκτέλεση των διαδικασιών που απαιτούνται, οι οποίες παρουσιάζουν σημαντικά ζητήματα.

3.4.1 Έλλειψη τυποποιημένων διαδικασιών και πρωτοκόλλων

Είναι δεδομένο ότι κάθε πάροχος cloud, χρησιμοποιεί τις δικές του υποδομές, και οι τεχνικές επιλογές επηρεάζονται από μια σειρά παραμέτρων, οι οποίες σε καμία περίπτωση δεν στοχεύουν στην ομοιογένεια με άλλους παρόχους. Το πρώτο βασικό πρόβλημα που προκύπτει από την έλλειψη ασυμβατότητας μεταξύ διαφορετικών παρόχων είναι η τήρηση των αρχείων καταγραφής, όπως έχει ήδη αναφερθεί. Αυτή η ασυμβατότητα συνίσταται τόσο στη διαφορετική επιλογή πολιτικής για τα αρχεία αυτά, όσο και στο είδος τους και το περιεχόμενό τους. Στο πλαίσιο της πολιτικής, κάθε πάροχος τηρεί τα αρχεία αυτά, για όσο χρονικό διάστημα επιθυμεί ενώ επιλέγει ο ίδιος το εύρος των δεδομένων που καταγράφει, ακολουθώντας συνήθως την ελάχιστη τυπική υποχρέωση που επιβάλλει ο νόμος και δίνοντας έμφαση περισσότερο στις εσωτερικές ανάγκες του. Πολύ συχνά δίνεται η επιλογή για την διάρκεια ζωής δεδομένων στον χρήστη της υπηρεσίας και αυτό περιπλέκει ακόμα περισσότερο την διαδικασία. (Google, 2025), (AWS, 2025).

Σε δεύτερο επίπεδο, δεν είναι αυτονόητο ότι η παροχή πρόσβασης στα αρχεία καταγραφής διέπεται από τους ίδιους κανόνες και διαδικασίες. Πέρα από την νομική πλευρά, ο πάροχος μπορεί να έχει εσωτερικές δομές που επιτρέπουν ή αποτρέπουν την πρόσβαση. Κάθε πάροχος φυσικά ορίζει τις διαδικασίες του κατά βούληση και δεν υποχρεούται να ακολουθεί μια δεδομένη αλληλουχία βημάτων.

Τέλος, στο θέμα της ποιότητας των δεδομένων, η κατάσταση είναι επίσης περίπλοκη. Είναι αναμενόμενο, συνεπώς, σε περιπτώσεις ανάγκης συνδυασμού στοιχείων από διαφορετικούς παρόχους, να υπάρχει αδυναμία σύγκρισης των δεδομένων, δηλαδή απουσία ενός κοινού σημείου αναφοράς. Έτσι ενώ οι πάροχοι υποστηρίζουν μια πληθώρα διαφορετικών μορφών αρχείων καταγραφής, δεν συνεπάγεται ότι μπορεί να γίνει και σύγκριση μεταξύ τους, η ότι το περιεχόμενο της πληροφορίας είναι κοινό (AWS, 2025). Αυτό έχει ως αποτέλεσμα, πέρα από τη δυσκολία συγκερασμού των πληροφοριών, και την αδυναμία ορισμού ενός αυτόματου και κοινώς αποδεκτού πρότυπου συλλογής αρχείων καταγραφής, κάτι που θα ενοποιούσε τη διαδικασία έρευνας σε μεγάλο βαθμό. Κάποια

πρότυπα βέβαια υφίστανται, το ζήτημα όμως παραμένει ότι αυτά τα πρότυπα θα πρέπει να μετατραπούν σε κανονισμούς.

3.4.2 Μη ετοιμότητα για έρευνα

Τα παραπάνω οδηγούν σε ένα πολύ σημαντικό συμπέρασμα και ταυτόχρονα ζήτημα, τη μη ετοιμότητα για έρευνα. Αυτή η μη ετοιμότητα αναφέρεται κυρίως στους παρόχους, αλλά μπορεί να οριστεί συνολικά ως η αδυναμία του χώρου να ρυθμίσει τα ζητήματα του. Θα πρέπει, βέβαια, να γίνει ξεκάθαρο τι είναι αυτό που ορίζεται ως ετοιμότητα για έρευνα, ποιες είναι οι σημαντικές παράμετροι και ποιες οι προϋποθέσεις και τα επακόλουθα.

Ως ετοιμότητα, λοιπόν, ορίζεται σύμφωνα με τον (Tan, 2001), η κατάσταση των οργανισμών που φροντίζουν ώστε να έχουν εγκατεστημένες προληπτικές τεχνικές ή διαδικασίες ψηφιακής εγκληματολογίας. Ο στόχος είναι φυσικά η διευκόλυνση της συλλογής αποδείξεων για τον ερευνητή, η μείωση του συνολικού κόστους για τον πάροχο και η ταχύτητα υλοποίησης των διαδικασιών αυτών. Η παράμετρος του κόστους ειδικά έχει ιδιαίτερη σημασία, καθώς είναι ένα από τα κίνητρα που μπορούν να ενεργοποιήσουν έναν πάροχο και να τον ωθήσουν να ξεπεράσει το αρχικό κόστος εγκατάστασης, το οποίο πιθανώς δεν επιθυμεί να επωμιστεί.

Η αναγκαιότητα για ετοιμότητα ξεπερνά βέβαια την διευκόλυνση ή το απλό κόστος της διαδικασίας εγκληματολογικής έρευνας. Μια από τις κυριότερες αιτίες ανάγκης της είναι η μεταβλητότητα των συστημάτων που πραγματευόμαστε. Δεν μπορεί να υπάρχει 100% εξασφάλιση ότι το σύστημα που χρησιμοποιείται και από το οποίο θέλουμε να εξαγάγουμε δεδομένα ήταν σε πλήρη και κανονική λειτουργία τη δεδομένη στιγμή που είναι προς εξέταση. Συνεπώς, η ανάγκη είναι ξεκάθαρη. Θα πρέπει βέβαια να αναφερθούν και οι δυσκολίες που θα αντιμετωπίσει ένας οργανισμός στην πορεία υλοποίησης αυτών των τεχνικών. Εν συντομία, τα πιο σημαντικά ζητήματα είναι θέματα ασφάλειας, θέματα ύπαρξης δοκιμασμένων πρακτικών, οργανωτικά, επιχειρηματικά και, φυσικά, πάντα ο νομικός παράγοντας και η εγκυρότητα μιας διαδικασίας. (SisaInfosec, 2024).

Στο θέμα της ασφάλειας, κυρίως ενδιαφέρει το πώς θα προσεγγιστούν διαφορετικές υποδομές και πώς δεν θα υπάρχει διαρροή πληροφοριών ανάμεσα σε μη συσχετιζόμενα συστήματα. Στο θέμα των μη δοκιμασμένων πρακτικών, ουσιαστικά οι πάροχοι

αντιλαμβάνονται ότι έχουν να αντιμετωπίσουν έναν νέο τομέα, και πολύ συχνά εγείρονται βασικά ζητήματα ασφάλειας και κόστους που αποθαρρύνουν από τη δημιουργία δοκιμαστικών υποδομών.

Οι πάροχοι δεσμεύονται κυρίως απέναντι στους πελάτες τους, και είναι αναμενόμενο πως οτιδήποτε μπορεί να δημιουργήσει ζητήματα στην ομαλή λειτουργία εξετάζεται με μεγάλη προσοχή. Πρέπει κάθε δοκιμαστικό σύστημα να φροντίζει να μην παραβιάζει κάποια συμφωνία υπηρεσίας (SLA), αλλά και επιπλέον να μην δημιουργεί πιθανά νομικά ζητήματα. Ιδιαίτερα στο νομικό κομμάτι, ένα τέτοιο σύστημα θα πρέπει να σέβεται τοποθεσίες και δικαιοδοσίες.

Τέλος, υπάρχει φυσικά και το κόστος που τυπικά έρχεται με κάθε τέτοια τροποποίηση–δοκιμή των υποδομών. Βέβαια, το κόστος θεωρείται συχνά ασήμαντο σε σχέση με το όφελος, αρκεί βέβαια το όφελος να έχει οριστεί ξεκάθαρα.

Σε όλα τα παραπάνω προστίθεται και η ανάγκη ύπαρξης μιας αρχής που θα μπορεί ενδεχομένως να ορίσει πρότυπα για την ετοιμότητα ενός οργανισμού, είτε να επικυρώσει την ετοιμότητά του. Βασικό, λοιπόν, ερώτημα είναι ποιος ορίζει τις ανάγκες και τους παράγοντες ετοιμότητας, ποιος ορίζει το πότε ένας οργανισμός πληροί τις προδιαγραφές και πώς αυτή η διαδικασία είναι αποδεκτή από την νομική αρχή (Reggiani, 2016). Επιπλέον, έχει ιδιαίτερο ενδιαφέρον να γίνει διαχωρισμός της ετοιμότητας αυτής τόσο σε τεχνικές παραμέτρους όσο και σε παραμέτρους διαδικασιών.

Τέλος, θα πρέπει να απαντηθεί και το πολύ σημαντικό ερώτημα, πόσο αυτοματοποιημένη μπορεί να είναι μια τέτοια υποδομή. Βρισκόμενοι μέσα σε μια εποχή μοντέλων τεχνητής νοημοσύνης και ερχόμενοι από δεκαετίες αλγορίθμων και μηχανικής μάθησης, εύκολα μπορεί να υποθέσει ο ερευνητής ότι κάτι τέτοιο μπορεί να εφαρμοστεί και σε αυτή την περίπτωση σχετικά ικανοποιητικά. Τα νομικά ζητήματα, όμως, δεν μπορούν να βασιστούν σε ένα επίπεδο ποιότητας που μπορεί να θεωρηθεί αρκούντως ποιοτικό, αλλά θα πρέπει να είναι τουλάχιστον ίδιου επιπέδου με τα αποτελέσματα της διαδικασίας στην οποία

παρεμβαίνει ένα φυσικό πρόσωπο και θεωρείται πως επιβλέπεται από ανθρώπινο παράγοντα.

Πέρα από τις δυσκολίες που αναγνωρίζονται, η επιλογή της εγκληματολογικής ετοιμότητας φαίνεται να είναι από τα ζητήματα που θα απασχολήσουν ιδιαίτερα στο άμεσο μέλλον.

4 Προτάσεις και εργαλεία για αντιμετώπιση

Τα ανοιχτά ζητήματα που αναφέρονται δεν γίνεται να μην ωθήσουν σε μια σειρά προτάσεων και λύσεων. Οι προκλήσεις αναλύθηκαν με βάση μια υψηλού επιπέδου κατηγοριοποίηση και με την ίδια λογική θα παρουσιαστούν και οι λύσεις. Είναι αναμενόμενο πως πρωταρχικό σημείο είναι η αντιμετώπιση των τεχνικών ζητημάτων, καθώς ο πυρήνας του προβλήματος ξεκινά από την τεχνική διάσταση των πράγματων.

4.1 Τεχνικό επίπεδο

Σε τεχνικό επίπεδο, οι προτάσεις θα επικεντρωθούν στα εργαλεία που μπορεί να γίνουν διαθέσιμα στους ερευνητές, στις διαδικασίες και πρακτικές που θα πρέπει να ακολουθήσουν ενδεχομένως οι πάροχοι, και τέλος σε νέες αυτοματοποιημένες διαδικασίες που θα φέρουν καινοτόμες λύσεις σε υπάρχοντα προβλήματα. Πολλές από τις παραμέτρους που αναφέρθηκαν δεν θα αναλυθούν αυτοτελώς, καθώς μπορούν να ενσωματωθούν σε κάποια από τις προτάσεις που θα ακολουθήσουν.

4.1.1 Σύγχρονες τεχνικές και εργαλεία ανάλυσης δεδομένων στο cloud

Το ζήτημα της ύπαρξης τεχνικών και κατάλληλου λογισμικού για την ανάλυση δεδομένων μιας υπόθεσης στο cloud άπτεται τόσο του θέματος των ίδιων των εργαλείων που είναι ή θα έπρεπε να είναι διαθέσιμα, όσο και της μορφής των δεδομένων που μπορούν αυτά τα εργαλεία να χειριστούν. Επιπλέον αναφορά θα πρέπει να γίνει και στην ανάγκη για ακεραιότητα των δεδομένων, τόσο των αντικειμενικών (δεδομένα χρήστη) όσο και των συμπληρωματικών (δεδομένα καταγραφής). Επιπλέον εγείρονται και τα ζητήματα αντιδικανικών τεχνικών που χρίζουν αντιμετώπισης, καθώς και οι τυπικές τεχνικές υποχρεώσεις για τη διατήρηση της αποδεικτικής αλυσίδας. Τα δύο τελευταία ζητήματα θα μπορούν ενδεχομένως να αποτελέσουν κομμάτι της θεωρίας περί ετοιμότητας, συνεπώς θα δοθεί περισσότερη έμφαση στα εργαλεία που θα πρέπει να είναι διαθέσιμα τόσο για τον ερευνητή όσο και για τον πάροχο.

Ας δούμε τι υπάρχει αυτή τη στιγμή στο πεδίο των αξιόπιστων εργαλείων και που θα πρέπει να γίνουν αλλαγές. Μια βασική κατηγοριοποίηση των εργαλείων με βάση τη λειτουργία τους θα μπορούσε να θεωρηθεί αρχικά χρήσιμη. Η διάκριση θα μπορούσε να είναι ανάμεσα

σε εργαλεία που συλλέγουν δεδομένα, εργαλεία ανάλυσης και εργαλεία δημιουργίας αναφορών. Εντούτοις, τα πιο σημαντικά εργαλεία του χώρου προσπαθούν να καλύψουν και τις τρεις αυτές λειτουργίες, συνεπώς θα πρέπει να γίνει μια συνολική αξιολόγηση των εργαλείων αυτών.

Magnet AXIOM και Cellebrite θεωρούνται δύο πολύ συνηθισμένες επιλογές για τη συλλογή και ανάλυση ψηφιακών στοιχείων (Kävrestad, et al., 2024) (Magnet Forensics, 2025). Το Magnet AXIOM θεωρείται ένα πολυσύνθετο εργαλείο που μπορεί να εξάγει πληροφορία από διαφορετικές πηγές, να κάνει ανάλυση πάνω στην πληροφορία αυτή και να δημιουργήσει αναφορές που είναι και ένα από τα τελικά ζητούμενα. Το Cellebrite από την άλλη διαφημίζεται σαν τη βασική επιλογή για την εγκληματολογική έρευνα πάνω σε ψηφιακά δεδομένα, και ενώ παρουσιάζεται αρχικά σαν ένα εργαλείο ανάλυσης δεδομένων, εκτελεί το σύνολο των βημάτων της διαδικασίας, καθώς αποτελεί ένα σύνολο προϊόντων που καλύπτει κάθε ανάγκη και εξελίσσονται διαρκώς (Cellebrite, 2025).

Στο παρελθόν υπήρχε και η χρήση των οδηγιών του CFLOG framework (Pourvahab, 2019), το οποίο είχε τον ίδιο σκοπό, τη συλλογή των logs και την αποθήκευσή τους με συγκεκριμένο πρότυπο. Το τελευταίο μάλιστα ακολουθούσε τις ACPO guidelines (Association of Chief Police Officers, 2012) για τη διατήρηση των ψηφιακών αποδείξεων. Το συγκεκριμένο πρότυπο βέβαια έχει σχεδόν τεθεί σε αχρηστία καθώς οι εξελίξεις ώθησαν στη δημιουργία του Forensic Science Regulator's (FSR) Code of Practice. Αυτό κάνει το εργαλείο μάλλον να τίθεται γενικά υπό αμφισβήτηση. (Dodd, 2024). Στον τομέα της συλλογής των δεδομένων υπάρχει συχνά και η χρήση διαφόρων βοηθητικών εργαλείων που αναλαμβάνουν τον συνδυασμό

πληροφορίας από αρχεία καταγραφής, ιδιαίτερα όταν αυτά έχουν διαφορετικό τύπο. Κάποια από αυτά τα εργαλεία είναι και τα ακόλουθα:

- Logstash – Εργαλείο συλλογής και μετασχηματισμού logs. Συνήθως απαντάται ως τμήμα του ELK stack.
- Graylog – Εργαλείο διαχείρισης logs.
- Datadog – Εργαλείο παρακολούθησης υποδομών cloud και ανάλυσης logs.
- Papertrail – Εργαλείο διαχείρισης και αναζήτησης logs για cloud περιβάλλοντα.

Στον τομέα της Ανάλυσης των δεδομένων, πέρα από τα δύο εργαλεία που αναφέρθηκαν, υπάρχουν επιλογές ενσωματωμένες στους παρόχους, όπως τα AWS CloudTrail & AWS Detective, Azure Security Center, Google Cloud Operations Suite. Επίσης ενδιαφέρουσες επιλογές είναι εφαρμογές όπως το Datadog (Datadog, 2025) , που αναλαμβάνουν τη διατήρηση των δεδομένων καταγραφής, την ανάλυσή τους και τη δημιουργία μιας

τοποθεσίας όπου ο πελάτης μπορεί να κάνει ανάλυση των δεδομένων του και να αναγνωρίσει πιθανές απειλές.

Τέλος, για τη δημιουργία αναφορών δεν υπάρχει μεγάλη διαφοροποίηση. Magnet και Cellebrite μπορούν να δημιουργήσουν τις αναφορές που απαιτούνται, ενώ και τα εργαλεία που προσφέρουν οι πάροχοι έχουν αντίστοιχες λειτουργίες.

Άλλα εργαλεία που προσφέρουν περίπου το ίδιο σύνολο υπηρεσιών είναι και τα:

- Autopsy (με κατάλληλα add-ons για το cloud) (Autopsy, 2025)
- FTK Digital Forensics Solutions by Exterro (Exterro, 2025)
- X-Ways Forensics: Integrated Computer Forensics Software (X-Ways, 2015)

Επιπλέον στον χώρο χρησιμοποιούνται πολλά εργαλεία που διευκολύνουν μικρές διεργασίες:

- Εργαλεία ανάλυσης δικτυακής κίνησης
- Εργαλεία λήψης αντιγράφων δεδομένων από cloud
- Εργαλεία διαχείρισης logs
- Εργαλεία ανάλυσης και εκτίμησης απειλών

Τα παραπάνω οδηγούν σε δύο βασικά συμπεράσματα. Πρωτίστως, ο χώρος των εργαλείων είναι ιδιαίτερα κατακερματισμένος, με πολλές διαφοροποιήσεις σε τεχνικές επιλογές, και επιπλέον υπάρχει σοβαρό ερωτηματικό σε σχέση με την εναρμόνιση με κανόνες και πρότυπα. Η εναρμόνιση αυτή, φυσικά, θεωρείται απαραίτητη ώστε να διασφαλίζεται η αποδεικτική αλυσίδα. Έχει ενδιαφέρον να γίνει ξεκάθαρο το κατά πόσο αυτά τα εργαλεία

ακολουθούν κάποια πρότυπα του χώρου και αν ναι ποια από αυτά. Τα πιο σημαντικά πρότυπα που θα πρέπει να ελεγχθούν αν ακολουθούνται είναι τα ακόλουθα:

- ISO/IEC 27037:2012: Ορίζει πρακτικές για απόκτηση και διατήρηση ψηφιακών αποδείξεων, έτσι ώστε να είναι αποδεκτές από νομικής άποψης (Iso.org, 2012).
- ISO/IEC 27041:2012: Ορίζει κανόνες για μεθόδους διερεύνησης (Iso.org, 2012).
- ISO/IEC 27042:2012: Ορίζει πρακτικές για ανάλυση ψηφιακών αποδείξεων (Iso.org, 2012).
- NIST SP 800-86: Ορισμός ρόλων και διαδικασιών για συλλογή αποδείξεων και γενικά τη χρήση εργαλείων για την έρευνα σε cloud περιβάλλοντα. Γενικά ορίζει διαδικασίες αντιμετώπισης περιστατικών (NIST, 2006).
- NIST SP 800-92: Οδηγίες για τη σωστή συλλογή, αποθήκευση και ανάλυση αρχείων καταγραφής (NIST, 2006)
- CIS Benchmarks: Ένα σύνολο βέλτιστων πρακτικών σε σχέση με την ασφαλή ρύθμιση των υπηρεσιών cloud (CISecurity, 2024).
- CSA CCM (Cloud Controls Matrix): Οδηγίες για cloud περιβάλλοντα στον τομέα της ασφάλειας και ετοιμότητας για εγκληματολογική μελέτη (CSA, 2024)
- Digital Forensics Research Workshop (DFRWS) για πρότυπα cloud forensics (Pollitt, 2004).
- NIST SP 800-101 Rev.1 – Οδηγίες σε σχέση με διαδικασίες κινητών (NIST, 2014).
- Scientific Working Group on Digital Evidence best practices (Swgde, 2025)

Από τα εργαλεία που αναφέρθηκαν και μερικά επιπλέον, ενδιαφέρον έχει να αναγνωριστούν ποια ακολουθούν τις παραπάνω οδηγίες στο σύνολό τους ή μερικώς. Έτσι βλέπουμε ακολούθως:

Magnet AXIOM	Συμμορφώνεται με ISO 27037 και NIST 800-86
FTK	Συμβατό με ISO 27037, DFRWS
Cellebrite	Συμμορφώνεται με ISO 27037 και NIST 800-86 και NIST SP 800-101 Rev.1 καθώς και με DFRWS και SWGDE
AWS CloudTrail detective	Πλήρης συμμόρφωση με NIST SP 800-92, CIS Benchmarks, ISO 27001
Azure monitor & Microsoft purview	Συμμορφώνεται με ISO 27037 και NIST 800-86

Google cloud operations suite	Συμβατό με NIST και CSA
X-ways forensics	Δεν έχει κάποια επίσημη συμμόρφωση με πρότυπα
Autopsy	Χωρίς επίσημη πιστοποίηση
Oxygen Forensics	Χωρίς επίσημη πιστοποίηση

Εν τέλει, το μεγάλο πρόβλημα με τα εμπορικά εργαλεία ενδεχομένως να είναι πως δεν υπάρχει εύκολος τρόπος να κατευθύνουν οι αρχές την εξέλιξή τους προς μια συγκεκριμένη κατεύθυνση και με συγκεκριμένα χαρακτηριστικά. Το πρόβλημα είναι ακόμα μεγαλύτερο αν αναλογιστεί κανείς πως δεν υπάρχει μια κεντρική αρχή προτυποποίησης που να μπορεί να ασχοληθεί συγκεκριμένα με αυτό τον τομέα. Εξάλλου, τα πρότυπα συνήθως είναι κατευθυντήριες γραμμές και μη δεσμευτικά σε πολλές περιπτώσεις. Όπως στο παρελθόν σε διάφορα θέματα προτυποποίησης διάφοροι οργανισμοί προσπαθούσαν να επιβάλουν τις προτάσεις τους, έτσι και στην περίπτωση αυτή, οργανισμοί που προσπαθούν να επιλύσουν το ζήτημα, θα πρέπει να συνεπικουρηθούν από τη βοήθεια της Ευρωπαϊκής Ένωσης ή κάποιου άλλου κρατικού φορέα, όπως το NIST, με ικανότητα επιβολής αποφάσεων. Αναφέρεται η Ευρωπαϊκή Ένωση, κυρίως διότι οποιαδήποτε απόφασή της αναγκάζει σε εξελίξεις όλο τον υπόλοιπο κόσμο, όπως έχουμε δει στο παρελθόν σε μια πληθώρα θεμάτων από την τεχνητή νοημοσύνη μέχρι τα πολύ απλά τεχνικά θέματα προτύπων.

Έτσι, πρόταση για λύση θα μπορούσε να είναι η επίσημη προτυποποίηση για την προετοιμασία και αντιμετώπιση συμβάντων ασφάλειας σε περιβάλλοντα cloud. Αυτή την πρόταση θα μπορούσε να συνδυαστεί και με την ετοιμότητα που θα αναλυθεί ακολούθως. Επίσης, διαδικασίες που θα μπορούσαν να εξασφαλίσουν τη σωστή καταγραφή αρχείων, θα μπορούσαν να βελτιώσουν και να υπερκεράσουν τα ζητήματα που προκύπτουν. Άλλωστε βασικό στοιχείο για την έρευνα είναι τα αρχεία καταγραφής και η ποιότητα αυτών συμβάλλει ουσιαστικά —και μερικές φορές αρκετά περισσότερο— από την ίδια την ποιότητα των διαθέσιμων εφαρμογών.

Δεδομένου ότι μια συνεργασία μεταξύ Ε.Ε. και Η.Π.Α. θα ήταν πολύ δύσκολη, στο πλαίσιο των οργανισμών NIST και Ευρωπαϊκής Επιτροπής, η μόνη βιώσιμη πρόταση στην παρούσα

φάση θα μπορούσε να είναι η ενσωμάτωση των διαφόρων πρωτοβουλιών στα διεθνή πρότυπα ISO/IEC.

Μια πρόταση στον τομέα των εργαλείων που παρουσιάζει ενδιαφέρον έχει να κάνει με την βελτίωση της ανθεκτικότητας των δεδομένων, προτού χρειαστεί μια εγκληματολογική έρευνα. Η πρόταση αυτή περιλαμβάνει την χρήση τεχνολογίας blockchain (Pourvahab, 2019) για την αποθήκευση αρχείων καταγραφής ή γενικά αρχείων δεδομένων, έτσι ώστε να διασφαλίζονται οι πληροφορίες ενεργειών που εκτελούνται πάνω στα δεδομένα. Αυτό παρουσιάζεται ιδιαίτερα σημαντικό όταν η μελέτη αρχίζει να πραγματεύεται και το θέμα της αντιδικανικής τεχνικής που ενδέχεται να χρησιμοποιεί ένας επιτιθέμενος. Μέρος των διαδικασιών που χρησιμοποιούνται είναι και η κάλυψη των αποδείξεων, με τροποποιήσεις αρχείων καταγραφής. Δεδομένου πως η τεχνολογία blockchain δεν επιτρέπει την τροποποίηση χωρίς καταγραφή, και μόνο η απόπειρα δημιουργεί ίχνη και αποδεικτικά στοιχεία.

Η τεχνολογία αυτή μπορεί να επεκταθεί και σε χρήση για τα ίδια τα δεδομένα. Παράνομες τροποποιήσεις δεδομένων μπορούν να αναγνωριστούν και να αντιστραφούν, έχοντας μια ξεκάθαρη πορεία ιστορικού. Πιο συγκεκριμένα, όταν δημιουργείται ή τροποποιείται ένα αρχείο επίσημα, δημιουργείται το αρχείο hash, που θεωρείται ένα αρχείο επαλήθευσης. Αυτό το hash στη συνέχεια θα αποθηκευτεί στο δίκτυο blockchain και σε κάθε μελλοντική χρήση, κάθε ενδιαφερόμενος μπορεί να το συγκρίνει με αυτό το αρχείο επαλήθευσης. Μια μη έγκυρη τροποποίηση δεν θα έχει ενημερώσει το hash, με αποτέλεσμα την έγκαιρη αναγνώριση μιας απειλής, καθώς και τη διατήρηση του ιστορικού αλλαγών κάθε αρχείου. Τέτοιες προσπάθειες ήδη έχουν αρχίσει να εμφανίζονται (Pichan, 2022). Κάποιες εταιρείες, μάλιστα, προσφέρουν εμπορικά προϊόντα που παρέχουν αυτή την καταγραφή και ασφάλεια σε δεδομένα cloud, δίνοντας ουσιαστικά μια υπηρεσία παρακολούθησης κάθε ίχνους τροποποίησης. Πιο χαρακτηριστικά παραδείγματα είναι τα Guardtime KSI Blockchain και Tierion (Chain, 2024). Μια πιο ενδιαφέρουσα πρόταση είναι το EtrusChain, που προσφέρει κρυπτογράφηση DNA και χρήση blockchain. Έτσι, πέρα από την ιχνηλασιμότητα, ενισχύεται

και η ασφάλεια των ίδιων των δεδομένων έναντι μη εξουσιοδοτημένων τροποποιήσεων. (Yıldırım, 2023)

4.1.2 Αποθήκευση και διαχωρισμός δεδομένων (multitenancy)

Πέρα από τα ζητήματα της εγκληματολογικής έρευνας, είχαν προσεγγιστεί και τα ίδια ζητήματα της φύσης των δεδομένων καθώς και ο τρόπος αποθήκευσής τους.

Θεωρείται αυτονόητο πως δεν υπάρχει δυνατότητα για τροποποίηση του τρόπου αποθήκευσης δεδομένων σε χαμηλό επίπεδο. Κάθε πάροχος είναι φυσικά ελεύθερος να υλοποιήσει τον τρόπο αποθήκευσης και διαμοιρασμού των δεδομένων που επιθυμεί. Δεν θεωρείται ότι υπάρχει ιδιαίτερη δυνατότητα στη δημιουργία ενός κοινού προτύπου, παρ' όλα αυτά αξία φαίνεται να υπάρχει στον τρόπο με τον οποίο τα δεδομένα κατοικούν σε υποδομές.

Ουσιαστικά το σημαντικό ζήτημα που πρέπει να επιλυθεί είναι η πολυμίσθωση και ο τρόπος ουσιαστικά που τα δεδομένα διαφορετικών πελατών/οντοτήτων μπορεί να είναι πεπλεγμένα (Prakash, et al., 2021), . Μέχρι στιγμής θεωρείται επίσης αυτονόητο, πως η δημιουργία εικονικών μηχανών αλλά και containers είναι κάτι που προσφέρει σε μεγάλο βαθμό τον διαχωρισμό που είναι επιθυμητός. Πέρα από αυτό το επίπεδο όμως, προτείνεται και η κατάλληλη κρυπτογράφηση των δεδομένων. Η απομόνωση μέσω κρυπτογράφησης θα εξασφαλίσει πως τα όποια δεδομένα είναι αποθηκευμένα μπορούν να είναι προσπελάσιμα μόνο από τον κάτοχο του κλειδιού, που είναι και ο εγκεκριμένος πελάτης. Ακόμα και αν τα δεδομένα είναι στον ίδιο φυσικό πόρο με κάποια διαφορετικού πελάτη, μόνο ο νόμιμος κάτοχος του κλειδιού μπορεί να αποκρυπτογραφήσει και να αναγνώσει.

Η απομόνωση μέσω κρυπτογράφησης (CSA, 2025) μπορεί να θεωρηθεί βέβαια το δεύτερο βήμα στη διαδικασία απομόνωσης. Κύρια και πιο σημαντική ενέργεια θα μπορούσες να είναι ο ίδιος ο φυσικός διαχωρισμός των δεδομένων πελατών. Ο διαχωρισμός όμως αυτός είναι ξεκάθαρα προς την αντίθετη κατεύθυνση των εξελίξεων στον χώρο του cloud. Οι οικονομίες κλίμακας επιτυγχάνονται όταν μπορεί ένας πάροχος να χρησιμοποιήσει μια νέα υποδομή, με πολλούς τρόπους, ή πολλούς αποδέκτες. Έτσι, ο φυσικός διαχωρισμός θα πρέπει να αναζητηθεί σε άλλο επίπεδο. Ένα από τα επίπεδα αυτά είναι και ο διαχωρισμός σε επίπεδο υπηρεσίας. Ένα πολύ ξεκάθαρο παράδειγμα είναι οι υπηρεσίες βάσεων δεδομένων. Υπάρχει

η δυνατότητα συνύπαρξης δεδομένων στην ίδια βάση και διαχωρισμός σε διαφορετικές βάσεις. Φαίνεται αυτονόητο πως κάθε πελάτης θα έχει τη δική του βάση δεδομένων, αλλά αυτό δεν είναι τελικά αυτονόητο. Σε περιπτώσεις που προσφέρεται μια υπηρεσία SaaS, ενδέχεται, βάσει σχεδιασμού, τα δεδομένα των πελατών που χρησιμοποιούν την υπηρεσία να βρίσκονται σε μια ίδια υποδομή. Αυτός ο διαχωρισμός θα μπορούσε να είναι το πρώτο στάδιο. Η χρήση διαφορετικών βάσεων δεδομένων, που άλλωστε από κατασκευής είναι διακριτές, επιτυγχάνει μια απομόνωση, αλλά αυτή η χρήση διαφορετικών βάσεων θα πρέπει να ενορχηστρωθεί από τον ίδιο τον σχεδιαστή της υπηρεσίας. Αυτό είναι ένα πολύ ενδιαφέρον παράδειγμα βελτίωσης της ποιότητας και ανθεκτικότητας των υπηρεσιών που προσφέρονται, όχι μέσω ενεργειών του παρόχου ή κάποιου φορέα, αλλά από τον ίδιο τον σχεδιαστή της υπηρεσίας. Αντίστοιχη απομόνωση θα πρέπει να επιδιώκεται και από τους παρόχους, όταν σχεδιάζουν την εσωτερική υπηρεσία τους για τη δημιουργία και διαχείριση αρχείων καταγραφής. Αυτές οι δύο περιπτώσεις θα μπορούσαν ίσως να είναι από τα ελάχιστα δυνατά βήματα φυσικού διαχωρισμού δεδομένων. (CSA, 2025)

Τέλος, σημαντικό βήμα πρέπει να είναι και οι διαδικασίες ελέγχου πρόσβασης σε κάθε σύστημα. Υπάρχουν ήδη πολιτικές πρόσβασης που οφείλουν οι πάροχοι να ακολουθούν, αλλά ελέγχεται το κατά πόσο αυτό γίνεται σε σωστό βαθμό. Οι δύο πιο κλασικοί τρόποι ορισμού πολιτικής είναι: (Okta, 2024) (Permify, 2024)

- RBAC (Role-Based Access Control) – Έλεγχος Πρόσβασης Βασισμένος σε Ρόλους
  Με αυτή την πολιτική, κάθε χρήστης αναλαμβάνει έναν ή περισσότερους ρόλους, και κάθε ρόλος έχει συγκεκριμένες προσβάσεις. Θεωρείται ο πιο απλός και διαδεδομένος τρόπος, αλλά εν γένει θεωρείται πως μπορεί να βελτιωθεί, καθώς δεν παρέχει περιθώρια ευελιξίας σε σχέση με την ανάθεση ρόλων, ενώ και η ίδια η δημιουργία των κατάλληλων ρόλων συχνά πάσχει.
- ABAC (Attribute-Based Access Control) – Έλεγχος Πρόσβασης Βασισμένος σε Χαρακτηριστικά. Σε αυτή την πολιτική, η πρόσβαση δεν βασίζεται μόνο σε έναν ρόλο αλλά σε μια ομάδα χαρακτηριστικών που μπορεί να έχει ένας χρήστης. Έτσι συχνά και η τοποθεσία, η ώρα ή ακόμα και ο τίτλος μπορεί να καθορίσει ή όχι την πρόσβαση.

Η συγκεκριμένη πολιτική είναι σαφώς πιο ευέλικτη και σημαντικά πιο ακριβής στον ορισμό του ποιος έχει πρόσβαση σε τι.

Και με τις δύο πολιτικές, η ουσία βρίσκεται στο αδιαμφισβήτητο γεγονός ότι η διαχείριση της πρόσβασης είναι ακρογωνιαίος λίθος της ασφάλειας και, κατά συνέπεια, του διαχωρισμού των δεδομένων. Οι πιθανές βελτιώσεις θα μπορούσαν να κινηθούν σε πολλά πλαίσια.

Καταρχάς, στο Role-Based Access Control, το οποίο είναι το πιο αδύναμο από τα δύο σχήματα, θα είχε ενδιαφέρον ο συνδυασμός του με το Attribute-Based Access Control. Ο στόχος θα είναι μεγαλύτερη ευελιξία στην ανάθεση ρόλων, διατηρώντας, φυσικά, την ασφάλεια. Προτείνεται ένα σχήμα στο οποίο το RBAC ορίζει τα βασικά επίπεδα δικαιωμάτων, ενώ το ABAC επεμβαίνει στη λεπτομέρεια. Σε δεύτερο επίπεδο, ενδιαφέρον παρουσιάζει και μια πιθανή αυτοματοποίηση της ανάθεσης των ρόλων. Αντί της ανάθεσης από τον ανθρώπινο παράγοντα, προτείνεται η αυτόματη ανίχνευση και εξάλειψη του σημαντικότερου παράγοντα κινδύνου σε όλη αυτή την αλυσίδα. Η αυτοματοποίηση αυτή, η οποία παραπέμπει στις πιο πρόσφατες εξελίξεις της τεχνητής νοημοσύνης (Akuthota, 2025), θα μπορούσε να επεκταθεί και στο πλαίσιο του ελέγχου των πολιτικών πρόσβασης. Μετά την ανάθεση ρόλου σε ένα άτομο, να γίνεται έλεγχος και της ποιότητας των δικαιωμάτων.

Η αυτοματοποίηση που αναφέρεται μπορεί, προφανώς, να εφαρμοστεί και στον Έλεγχο Πρόσβασης Βασισμένο σε Χαρακτηριστικά (ABAC), αλλά δεν είναι το μόνο πλαίσιο βελτίωσης που αναγνωρίζεται. Σημαντική βελτίωση διαφαίνεται στην αναγνώριση των χαρακτηριστικών και στην επιλογή αυτών που πραγματικά παρέχουν τον κατάλληλο διαχωρισμό των ατόμων, στο πλαίσιο της ασφάλειας. Τέλος, πολύ ενδιαφέροντα αποτελέσματα δείχνουν να έχουν δύο ακόμα ερευνητικές κατευθύνσεις. Η Αρχιτεκτονική Μηδενικής Εμπιστοσύνης αλλάζει το υφιστάμενο σχήμα επαλήθευσης δικαιωμάτων και απαιτεί μια συνεχής επαλήθευση ταυτότητας. Τέλος, και σε αυτό το σημείο, θα πρέπει να αναφερθούν οι τεχνολογίες blockchain. Σε αυτή την περίπτωση, η εφαρμογή αφορά τη διασφάλιση της ακεραιότητας της ίδιας της πολιτικής και της διαχείρισής της και όχι στο επίπεδο του αποτελέσματος. Σε όλα τα παραπάνω, φυσικά, θα πρέπει να τεθεί και το θέμα

της εκπαίδευσης. Πολύ συχνά, ο αδύναμος κρίκος είναι ο άνθρωπος που παρακάμπτει όλες αυτές τις πολιτικές

4.1.3 Αυτοματοποίηση και τεχνητή νοημοσύνη στην ανάλυση ψηφιακών στοιχείων

Σε όλα τα παραπάνω γίνεται μια προσπάθεια παραδοσιακής προσέγγισης στην επίλυση των ζητημάτων, αναγνώριση προβλήματος και αντιμετώπιση με κλασικές μεθόδους. Εντούτοις ήδη έχουν γίνει αναφορές σε αυτοματοποιημένες διαδικασίες. Πράγματι, πλέον υπάρχει και μεγάλη δυνατότητα για χρήση, τουλάχιστον σε ερευνητικό επίπεδο, αυτοματοποιημένων τεχνικών για την επίλυση των τεχνικών ζητημάτων της εγκληματολογίας στο cloud. Τα σημαντικότερα ζητήματα που είναι η Ανάλυση Δεδομένων και Στοιχείων και Ανίχνευση Κακόβουλης Δραστηριότητας είναι ζητήματα που θα μπορούσαν να αποτελέσουν αντικείμενο μιας προσπάθειας με μηχανική μάθηση ή τεχνητή νοημοσύνη.

Ακόμα περισσότερο ενδιαφέρον θα έχει και το επόμενο βήμα που είναι η Βελτιστοποίηση και Ανάλυση Συστημάτων σε Πραγματικό Χρόνο. Και αυτό θα μπορούσε να προσεγγιστεί με Τεχνητή Νοημοσύνη (Hungwe & Venter, 2024), (Purnaye & Kulkarni, 2022) . Ποια είναι τα προαπαιτούμενα για να γίνει κάτι τέτοιο και πόσο δύσκολο ή κοστοβόρα διαδικασία μπορεί να είναι;

Τα επίπεδα που μπορεί να εφαρμοστεί μια αυτοματοποιημένη διαδικασία είναι τα ακόλουθα:

- **Ανάλυση δεδομένων.** Η αυτοματοποιημένη ανάλυση δεδομένων μπορεί να επιτευχθεί είτε με αλγόριθμους μηχανικής μάθησης που θα ενεργούν πάνω στα αρχεία καταγραφής και θα επιχειρεί να αναγνωρίσει μη κανονική συμπεριφορά (anomaly detection), (Chukwuemeka Nwachukwu, 2024) είτε με αντίστοιχους αλγορίθμους που θα ενεργούν πάνω στα ίδια τα δεδομένα των χρηστών και θα επιχειρούν να αναγνωρίσουν μη κανονικές ενέργειες και μη κανονική κατάσταση των δεδομένων. Για να επιτευχθεί ιδιαίτερα το δεύτερο επίπεδο, πρέπει να μπορεί να είναι εφικτή η αναγνώριση και κατηγοριοποίηση των δεδομένων αλλά και η αναγνώριση και η κατηγοριοποίηση των κινήσεων δικτύου. Επιπλέον, με τη χρήση

επεξεργασίας φυσικής γλώσσας (NLP), η πρώτη κατηγοριοποίηση μπορεί να γίνει πιο σωστή και με τη δυνατότητα για καλύτερη νοηματοδότηση.

- **Ανίχνευση εισβολών.** Τα ήδη υπάρχοντα συστήματα αναγνώρισης εισβολών μπορούν να βελτιωθούν και να εκπαιδευτούν με μεγαλύτερη ακρίβεια για την ανίχνευση (Sowmya T., 2023) . Η ανίχνευση φυσικά θα πρέπει να είναι το πρώτο βήμα στη διαδικασία, αλλά πολύ συχνά αν δεν υπάρχει ανίχνευση εγκαίρως, τα απαραίτητα στοιχεία ενδέχεται να έχουν καταστραφεί. Έτσι, η χρήση μηχανικής μάθησης θα μπορέσει να ανιχνεύσει εγκαίρως τις επιθέσεις αλλά και να αναγνωρίσει νέες κατηγορίες αυτών.
- **Ανάλυση συστημάτων σε πραγματικό χρόνο.** Αυτή η ανάλυση προφανώς αναφέρεται και στα συστήματα αναγνώρισης εισβολών αλλά και στα συστήματα ανάλυσης κίνησης δικτύου (Moffitt, 2024). Με τη χρήση αυτοματοποιημένων τεχνικών, Μηχανικής μάθησης, είναι προφανώς πιο εύκολο και λιγότερο κοστοβόρο να υλοποιηθεί αυτή η ανάλυση. Επόμενο βήμα της ανάλυσης σε πραγματικό χρόνο είναι η βελτιστοποίηση.

Παραδείγματα των παραπάνω ήδη βρίσκονται σε κάποιο πειραματικό στάδιο. Πιο συγκεκριμένα:

Συστήματα Ανίχνευσης Εισβολών (IDS) με AI/ML. Δοκιμαστική λειτουργία από το ίδρυμα DARPA με στόχο την αναγνώριση νέων τύπων επιθέσεων και κακόβουλης δραστηριότητας. (Sowmya T., 2023). Χρησιμοποιήθηκαν αλγόριθμοι Support Vector Machine και Random Forest με σκοπό την κατηγοριοποίηση της κίνησης στο δίκτυο. Πιο συγκεκριμένα, ο αλγόριθμος Support Vector Machine, αξιοποιώντας υπερεπίπεδα (hyperplanes), διαχωρίζει την κατηγορία της κίνησης μεταξύ κανονικής και κακόβουλης, παρουσιάζοντας ιδιαίτερα καλά αποτελέσματα ως προς την ακρίβεια των προβλέψεων. Ο αλγόριθμος Random Forest, από την άλλη πλευρά, δημιουργεί πολλαπλά δέντρα αποφάσεων και επιλέγει την τελική κατηγοριοποίηση βάσει της πλειοψηφίας των αποτελεσμάτων τους. Και αυτός ο αλγόριθμος επιδεικνύει υψηλή ακρίβεια, ενώ επιπλέον εμφανίζει βελτιωμένη συμπεριφορά ως προς τη μείωση των ψευδώς θετικών αποτελεσμάτων.

Τα αποτελέσματα της εφαρμογής αυτών των τεχνικών περιλάμβαναν την αναγνώριση νέων τύπων επιθέσεων. Συγκεκριμένα, εντοπίστηκαν επιθέσεις τύπου Slowloris (είδος επίθεσης DoS που χαρακτηρίζεται από εξαιρετικά χαμηλό ρυθμό αποστολής δεδομένων, με

σκοπό την εξάντληση των πόρων του διακομιστή) και Heartbleed, η οποία εκμεταλλεύεται ευπάθειες του πρωτοκόλλου SSL για να αποκτήσει πρόσβαση σε ευαίσθητες περιοχές μνήμης. Επιπλέον, αναγνωρίστηκαν επιθέσεις τύπου brute force σε διάφορες παραλλαγές.

Είναι πλέον σαφές ότι οι τεχνικές αυτές έχουν τη δυνατότητα να αναγνωρίζουν αποτελεσματικά κακόβουλες ενέργειες. Το ουσιαστικό ερώτημα που τίθεται είναι κατά πόσο μπορούν να εφαρμοστούν σε ευρεία κλίμακα και ποια είναι τα πιθανά προβλήματα που μπορεί να ανακύψουν. Το κυριότερο ζήτημα αφορά στους υπολογιστικούς πόρους που απαιτούνται για την εκτέλεση τέτοιων ενεργειών ανάλυσης και αναγνώρισης σε πραγματικό χρόνο. Επιπλέον, παρουσιάζεται δυσκολία στην τεκμηρίωση των αποτελεσμάτων, καθώς οι αλγόριθμοι μηχανικής μάθησης λειτουργούν με μη ντετερμινιστικό τρόπο, γεγονός που έρχεται σε αντίθεση με τις απαιτήσεις διαφάνειας των υπευθύνων ασφάλειας.

Τέλος, υπάρχει έντονος προβληματισμός σχετικά με το κατά πόσο τέτοια συστήματα μπορούν να ενσωματωθούν στις υπάρχουσες υποδομές χωρίς σημαντικές τεχνικές παρεμβάσεις. Ενδεχομένως, η χρήση αυτών των τεχνολογιών θα πρέπει να αντιμετωπίζεται ως μια λύση που προβλέπεται εξαρχής από τους σχεδιαστές υποδομών, ενσωματώνοντας το σχετικό κόστος και τις απαιτήσεις στο πλαίσιο της αρχικής επένδυσης.

Τέλος, ερευνητικό ενδιαφέρον υπάρχει και στον τομέα του IoT. Είναι εφικτή η αναγνώριση κακόβουλων συσκευών αλλά και ασυνήθιστες συμπεριφορές σε έγκυρες συσκευές. Ένα τέτοιο παράδειγμα είναι και το έργο *IoT Security and Forensics*. (Yang, 2020)

Στο έργο αυτό προτείνονται μια σειρά από εργαλεία τα οποία αναλαμβάνουν, αρχικά, τη συλλογή δεδομένων, την κατασκευή του βασικού μοντέλου αποδεκτής συμπεριφοράς και στη συνέχεια την ανάλυση των δεδομένων με σκοπό την ανίχνευση συμπεριφορών που αποκλίνουν από τον κανόνα. Τελικός στόχος του μοντέλου είναι η καταγραφή αυτών των ευρημάτων με τρόπο που να μπορεί να υποστηρίξει έγκυρα μια εγκληματολογική μελέτη. Η μεθοδολογία που ακολουθείται έχει σημαντικές ομοιότητες με εκείνη που εφαρμόζεται στην

ανίχνευση μέσω αλγορίθμων μηχανικής μάθησης σε περιβάλλον cloud. Η κύρια διαφοροποίηση αφορά το είδος και την ποσότητα των συλλεγόμενων δεδομένων.

Ιδιαίτερη αναφορά αξίζει να γίνει στο γεγονός ότι τα δεδομένα προέρχονται από συσκευές που βρίσκονται συχνά εντός οικιακού περιβάλλοντος, γεγονός που εγείρει ζητήματα συμμόρφωσης με τις νομοθεσίες περί προστασίας προσωπικών δεδομένων.

Όλες οι παραπάνω προσεγγίσεις βρίσκονται σήμερα κυρίως στο ερευνητικό πεδίο. Ωστόσο, οι τεχνολογικές εξελίξεις τις φέρνουν ολοένα και πιο κοντά στην πρακτική εφαρμογή, για έναν καθοριστικό λόγο: δεν απαιτείται απόλυτη ακρίβεια κατά το αρχικό στάδιο της μελέτης. Τα συστήματα αυτά μπορούν να λειτουργήσουν ως επικουρικοί μηχανισμοί, προσφέροντας ευελιξία τόσο ως προς την κλίμακα εφαρμογής όσο και ως προς τις ποιοτικές απαιτήσεις. Έτσι, δίνεται ουσιαστικά ο απαραίτητος χρόνος ώστε να ωριμάσουν οι μηχανισμοί ώστε να μπορούν να αναλάβουν πλήρως την συγκεκριμένη ευθύνη.

4.2 Τεχνοοργανωτικό επίπεδο

Οι τεχνολογικές προτάσεις που προηγήθηκαν βρίσκουν ένα σημείο δυσκολίας εφαρμογής στο επίπεδο αποδοχής τους από τους παρόχους αλλά και το σύνολο των εμπλεκομένων φορέων.
Γίνεται σταδιακά εμφανές πως η βέλτιστη προσέγγιση του ζητήματος αφορά, πέρα από τον τεχνικό τομέα, και τον οργανωτικό. Όταν αναφερόμαστε σε οργανωτικό, ουσιαστικά αναφερόμαστε σε διαδικασίες και πρακτικές που θα πρέπει να παγιωθούν ώστε η ροή της διαδικασίας εγκληματολογικής ανάλυσης να είναι επιτυχημένη, αποδοτική και με πλήρως αποδεκτά αποτελέσματα από τις νομικές αρχές.

Το πρώτο βήμα για τη βελτιστοποίηση της διαδικασίας είναι η αναγνώριση των διακριτών βημάτων της εγκληματολογικής διαδικασίας, βημάτων που είναι κοινώς αποδεκτά στον

χώρο και θεωρούνται βασικοί πυλώνες χωρίς να θεωρούνται ότι παραβλέπουν κάποιο σημαντικό στάδιο. Έτσι, λοιπόν, αναγνωρίζονται τα ακόλουθα βήματα (Infosec, 2019):

- **Αναγνώριση:** Γίνεται τεκμηρίωση της ύπαρξης ενός περιστατικού ασφάλειας και λαμβάνεται η απόφαση της ανάγκης για εγκληματολογική διερεύνηση.
- **Διατήρηση δεδομένων**: Διαδικασία διατήρησης των δεδομένων που έχουν υποστεί την επίθεση. Εξασφάλιση της μη τροποποίησής τους από την εγκληματολογική διαδικασία και διατήρηση μεταδεδομένων τους.
- **Συλλογή αποδείξεων:** Συλλογή των αποδεικτικών στοιχείων, που μπορεί να περιλαμβάνουν τόσο πηγαία δεδομένα όσο και αρχεία καταγραφής. Συνεργασία και με τους παρόχους ώστε να τηρηθεί η αλυσίδα της εγκυρότητας των στοιχείων.
- **Εξέταση και φιλτράρισμα αποδείξεων:** Οι αποδείξεις ομαδοποιούνται κατάλληλα, γίνονται οι απαραίτητες διαδικασίες εκτίμησης χρήσιμων και μη δεδομένων και εντοπισμός των τελικών αρχείων προς εξέταση.
- **Ανάλυση και εξαγωγή συμπερασμάτων:** Μελέτη των αποδεικτικών στοιχείων και εξαγωγή συμπερασμάτων.
- **Νομική προετοιμασία και παρουσίαση αποτελεσμάτων:** Δημιουργία εξαγόμενων αρχείων προς νομική χρήση και αρχείων αναφορών όπου χρειάζεται.
- **Εσωτερική ανατροφοδότηση:** Προαιρετική αξιολόγηση της διαδικασίας και εύρεση πιθανών σημείων βελτίωσης.

Σε ένα περιβάλλον cloud η διαδικασία αναπροσαρμόζεται λόγω της φύσης του μέσου, όμως τα βασικά βήματα δεν τροποποιούνται. Έτσι, για την αναγνώριση των περιστατικών μπορεί να απαιτηθεί η χρήση των ενσωματωμένων εργαλείων που παρέχει ο πάροχος. Για τη διατήρηση των στοιχείων είναι χρήσιμη η παρουσία κάποιων μη τροποποιήσιμων δομών αποθήκευσης, ενώ για τη συλλογή και την εξέταση επίσης χρειάζεται η συνεργασία με τον πάροχο και η χρήση των εργαλείων ή δεδομένων που παρέχει αυτός. Τέλος, για την εξαγωγή συμπερασμάτων και την παρουσίαση αυτών, πρέπει να δοθεί προσοχή στην τήρηση της

αλυσίδας ακεραιότητας, που βασίζεται φυσικά σε όλα τα δεδομένα που έχει προσφέρει ο πάροχος.

Σε κάποια από τα σημεία της διαδικασίας αυτής έχει τεθεί το ερώτημα αν υπάρχουν τα δεδομένα που απαιτούνται. Και εδώ είναι που υπεισέρχεται το κομμάτι της ετοιμότητας για την εγκληματολογική έρευνα, που αποτελεί σημαντικό ερευνητικό πεδίο για τον χώρο.

4.2.1 Τεχνολογίες και μοντέλα ετοιμότητας

Αρχικά θα πρέπει να είναι ξεκάθαρος ο ορισμός της εγκληματολογικής ετοιμότητας. Ποιος είναι ο υπεύθυνος και σε ποια τμήματα της διαδικασίας που έχει οριστεί αναφέρεται. Η ετοιμότητα για ψηφιακή εγκληματολογική έρευνα είναι η προετοιμασία ενός συστήματος έτσι ώστε να έχει τη δυνατότητα να υποστηρίξει μια εγκληματολογική έρευνα όταν αυτό θα απαιτηθεί. Ουσιαστικά, η προετοιμασία συνίσταται σε διαδικασίες και στρατηγικές που εξασφαλίζουν τόσο τη διατήρηση των αποδεικτικών στοιχείων, είτε αυτά είναι πηγαία δεδομένα είτε επιπλέον αρχεία καταγραφής, με τέτοιο τρόπο ώστε να είναι εφικτή η ανάλυσή τους και η χρήση ως αποδεικτικά στοιχεία, τηρώντας πάντα τόσο τις τεχνικές όσο και τις νομικές προδιαγραφές που απαιτεί η αποδεικτική αλυσίδα (Simou, et al., 2019) (Al-mugern, et al., 2024) . Η ετοιμότητα μπορεί να αναφέρεται σε πολλαπλά από τα στάδια της εγκληματολογικής διαδικασίας. Πιο συγκεκριμένα:

- **Στο στάδιο αναγνώρισης,** δημιουργούνται διαδικασίες αυτόματης αναγνώρισης και αναφοράς περιστατικών
- **Στο στάδιο διατήρησης**, εξασφαλίζεται η εκ προοιμίου διατήρηση των δεδομένων ανεξαρτήτως περιστατικών ασφάλειας
- **Στο στάδιο συλλογής,** και δεδομένης της διατήρησης των δεδομένων, θα πρέπει να υπάρχει η δυνατότητα αξιολόγησης σημαντικότητας των αρχείων καταγραφής, και

των επιπέδων πρόσβασης που πρέπει να υπάρχουν, καθώς και να διατηρείται πάντα η αλυσίδα φύλαξης αποδείξεων.

Τα υπόλοιπα στάδια της διαδικασίας εξαρτώνται εμμέσως από τα παραπάνω, όμως η ποιότητά τους είναι άμεσα συνδεδεμένη με την ποιότητα των δεδομένων των προηγούμενων βημάτων.

Στην ερευνητική διαδικασία έχουν προταθεί μια σειρά από μοντέλα ετοιμότητας, εκ των οποίων άλλα δίνουν περισσότερη έμφαση στην προετοιμασία των υπηρεσιών και άλλα στην προετοιμασία των συστημάτων υποδομής. Κοινά στοιχεία των μοντέλων θα αναδειχθούν με σκοπό την πρόταση ενός ελάχιστου κοινού προτύπου που θα είναι άμεσα εφαρμόσιμο.

Μοντέλο 1 (Venter, 2024):

Στο μοντέλο που προτείνεται από τους Koen και Venter, η βασική λειτουργία που εντοπίζεται ως ανάγκη είναι η παροχή της πληροφορίας από ένα στάδιο σε ένα άλλο όπως π.χ. από την υποδομή στις υπηρεσίες. Δεν γίνεται ξεκάθαρος προσδιορισμός των τεχνικών απαιτήσεων, καθώς αυτό δεν προσφέρει κάτι το ιδιαίτερο στο εννοιολογικό σχήμα που προτείνεται. Η παροχή της πληροφορίας βασίζεται σε μια σειρά από υπηρεσίες, κάτι που υποδηλώνει την ύπαρξη σε χαμηλό επίπεδο, μιας υποδομής συλλογής πληροφορίας και παροχής σε μια διεπαφή. Περαιτέρω ορίζονται τα διαφορετικά επίπεδα ελέγχου που οφείλουν να υπάρχουν έτσι ώστε αυτή η παροχή υπηρεσίας να προσφέρει μεν τα δεδομένα που απαιτούνται, να ακολουθεί δε, νομικούς και τεχνικούς κανόνες.

Η δομή που προτείνεται, βασίζεται σε μια εννοιολογική προσέγγιση τεσσάρων επιπέδων που αλληλεπιδρούν μεταξύ τους. Στο κύριο επίπεδο βρίσκεται μια ομοσπονδιακή δομή ελέγχου που καθορίζει όλους τους κανόνες και πολιτικές, και ενορχηστρώνει τη μεταφορά πληροφορίας, όσον αφορά το περιεχόμενο, αιτίες, διάρκεια και άλλες παραμέτρους χρήσης της πληροφορίας. Αυτή η ομοσπονδιακή δομή ελέγχου που ονομάζεται *policy engine* είναι απλά ένα σύνολο κανόνων που μπορεί να έχει και ιεραρχική δομή και να παίρνει δεδομένα από άλλες πολιτικές, και εν τέλει να εκφράζεται σε μια μορφή *mark up* γλώσσας. Σε δεύτερο επίπεδο βρίσκονται οι ενέργειες που είναι δυνατές να γίνουν. Έτσι αυτό περιλαμβάνει τις ίδιες τις αιτήσεις για δεδομένα και τη διαχείρισή τους, τη δημιουργία και διαχείριση ειδοποιήσεων, και τις διαδικασίες ανωνυμοποίησης των δεδομένων όπου αυτό χρειάζεται.

Σε τρίτο επίπεδο ορίζονται κανόνες σχετικά με την αποθήκευση, διατήρηση και κατάλληλη σήμανση των δεδομένων, ενώ επιπλέον γίνεται δυνατός και ο ορισμός της ανίχνευσης ενός γεγονότος. Ο ορισμός αυτός ουσιαστικά προσδιορίζει τα χαρακτηριστικά που έχει μια ειδοποίηση και το περιεχόμενο του ίδιου του γεγονότος. Τέλος, στο μοντέλο προστίθεται και η οριοθέτηση κανόνων για τη σωστή τήρηση της εγκληματολογικής διαδικασίας και τήρηση των νομικών στοιχείων (*chain of custody*, νομοθετικά πλαίσια, διαφάνεια και λογοδοσία).

Αυτοί οι κανόνες ενσωματώνονται σε κάθε ένα από τα επίπεδα που ορίζει το πλαίσιο. Έτσι, στο πλαίσιο του *policy engine* ορίζονται απαιτήσεις σχετικά με τη μοναδικότητα του αριθμού μιας υπόθεσης, ενώ γίνεται επίσης αναφορά στα δικαιώματα και τα προνόμια πάνω στα δεδομένων κρίσιμης σημασίας. Σε επόμενο επίπεδο, αυτό των ενεργειών, διασφαλίζεται η ακεραιότητα και η εμπιστευτικότητα που οφείλει να διέπει όλα τα αποδεικτικά στοιχεία. Στο τρίτο επίπεδο, το οποίο σχετίζεται με τους κανόνες διαφύλαξης των αποδεικτικών στοιχείων, ορίζονται οι νομικές απαιτήσεις και προσδιορίζεται η συμμόρφωση με αυτές. Τέλος, στο τέταρτο επίπεδο καθορίζεται με σαφήνεια η διαδικασία αποθήκευσης και η συμμόρφωση με τους διεθνείς κανονισμούς αναφορικά με τα δεδομένα και τον τρόπο αποθήκευσής τους.

Η αρχική μελέτη του μοντέλου είναι καθαρά θεωρητική και δεν έχει προκύψει κάποια πρακτική εφαρμογή. Όμως θεωρείται από τους συγγραφείς ότι αντιμετωπίζει τα πυρηνικά προβλήματα του χώρου.

Ένα διαφορετικό μοντέλο έχει οριστεί από την ομάδα των Σίμου, Καλονιάττη, Γκρίτζαλη και Κάτος. (Simou, et al., 2019):

Αυτό το μοντέλο επιχειρεί μια πιο πρακτική προσέγγιση της ετοιμότητας. Ορίζει τα σημεία που πρέπει να επέμβει ένας σχεδιαστής συστημάτων σε πραγματική βάση και δεν περιορίζεται απλά σε μια αναφορά της ανάγκης παροχής δεδομένων ή την ενορχήστρωση της διαμεταγωγής τους. Ουσιαστικά η προσέγγιση βασίζεται, όπως θα δούμε, στην πρακτική λογική της διατήρησης και παροχής πληροφορίας. Αυτό έχει ιδιαίτερη αξία, καθώς το

μοντέλο προσπαθεί να προσεγγίσει ένα μεγάλο μέρος των ζητημάτων που έχουν αναλυθεί και μπορεί να προσφέρει μια ουσιαστική διέξοδο προς τη συνολική βελτίωση στον χώρο.

Έτσι ξεκινά η μελέτη με τον ορισμό των ζητημάτων προς επίλυση έτσι ώστε ένα σύστημα να θεωρείται ότι διέπεται από την ετοιμότητα. Τα 7 βασικά ζητήματα τα οποία ονομάζονται και περιορισμοί ετοιμότητας, ακολουθούνται από έναν ορισμό καθώς και από τα διακριτά βήματα που μπορεί να τα προσδιορίζουν, από τα ζητήματα και δυσκολίες που έχουν, τα εμπλεκόμενα μέρη και τις πιθανές λύσεις. Εν τέλει, για κάθε έναν από αυτούς τους περιορισμούς προτείνεται και ένα σύνολο από ενέργειες που είναι και το τελικό ζητούμενο.

Στα πλαίσια της προσέγγισής μας είναι προτιμότερη η προσέγγιση κυρίως στις δυσκολίες και τις ενέργειες ώστε να επιτευχθεί η εγκληματολογική ετοιμότητα.

• Accountability – Λογοδοσία

Η υποχρέωση των παρόχων να προστατεύουν τα δεδομένα και να είναι υπεύθυνοι σε κάθε περίπτωση συμβάντος. Παρουσιάζει δυσκολίες τόσο σε ζητήματα πρόσβασης δεδομένων και συμμόρφωσης με συμβάσεις, αλλά και κανονισμούς. Οι ενέργειες που προτείνονται είναι:

- Εξασφάλιση τήρησης συμφωνιών
- Παροχή εξασφαλίσεων
- Παρακολούθηση των ενεργειών για προβλήματα και αστοχίες
- Παροχή ικανότητας αναγνώρισης υπευθύνων

• Transparency – Διαφάνεια

Η ικανότητα πλήρους πρόσβασης στα δεδομένα για τους εμπλεκόμενους και η διαθεσιμότητα για ανατροφοδότηση. Παρουσιάζει δυσκολίες, ιδιαίτερα στην παροχή αλλά και τη φύση των δεδομένων. Οι ενέργειες που προτείνονται είναι:

- Εξασφάλιση της ορατότητας όλων των δεδομένων και της τοποθεσίας αποθήκευσης
- Δημιουργία διαδικασιών και πολιτικών για την τήρηση των δεδομένων
- Δημιουργία ειδοποιήσεων για τις παραβιάσεις των πολιτικών

• Internal disciplinary procedures – Εσωτερικές διαδικασίες πειθαρχίας

Διαδικασίες για το εσωτερικό ενός παρόχου, σε περίπτωση παραβιάσεων. Παρουσιάζει δυσκολίες λόγω της αναφοράς σε προσωπικό και τις συμπεριφορές τους, που θα πρέπει να καθορίζονται από πολιτικές. Οι ενέργειες που προτείνονται είναι:

- Εφαρμογή πειθαρχικών πολιτικών
- Δημιουργία πολιτικών και δικαιωμάτων πρόσβασης
- Χρήση νομικών δεσμεύσεων που αναφέρονται στο προσωπικό

• Access rights (policies) – Δικαιώματα πρόσβασης (πολιτικές)

Τα δικαιώματα πρόσβασης του προσωπικού ενός παρόχου και ενδεχομένως των πελατών. Οι ενέργειες που προτείνονται είναι:

- Εξασφάλιση ελέγχου εγγραφής και επιβεβαίωσης των χρηστών
- Σωστός έλεγχος ταυτοποίησης και εξουσιοδοτήσεων
- Επιβολή ελέγχου πρόσβασης

• Isolation – Απομόνωση

Ο διαχωρισμός των δεδομένων. Ιδιαίτερα σημαντικός τόσο σε σταθερά όσο και ευμετάβλητα δεδομένα (μνήμης). Οι ενέργειες που προτείνονται είναι:

- Εξασφάλιση διαχωρισμού δικαιωμάτων και πρόσβασης χρηστών
- Αποτροπή μόλυνσης δεδομένων σε περίπτωση αστοχίας από άλλους χρήστες
- Εμπιστευτικότητα

• Legal matters – Νομικά θέματα

Η συμμόρφωση με τους τοπικούς και διεθνείς νόμους και η παροχή των δεδομένων με σωστό και συνεπή νομικά τρόπο. Οι ενέργειες που προτείνονται είναι:

- Ορισμός SLAs (Συμβάσεων επιπέδου υπηρεσιών)
- Καθορισμός δικαιοδοσίας
- Εκπαίδευση προσωπικού

• Traceability – Ιχνηλασιμότητα

Ικανότητα παρακολούθησης και καταγραφής των ενεργειών που πραγματοποιούνται πάνω στα δεδομένα και γνώση αυτών σε κάθε χρονική στιγμή. Οι ενέργειες που προτείνονται είναι:

- Παρακολούθηση δραστηριότητας χρηστών
- Παρακολούθηση αρχείων καταγραφής
- Σωστή αποθήκευση αρχείων καταγραφής
- Σύστημα αντιστοίχισης χρηστών με τα δεδομένα

Η ομάδα έρευνας έχει κατατάξει τις 7 αυτές προδιαγραφές σε μια σειρά από διαδικασίες που επάγεται η μία χρονικά της άλλης και έτσι δημιουργούν το πρώτο μοντέλο σχεδιασμού της ετοιμότητας ενός συστήματος.

- Πρώτο στάδιο ορίζονται οι προκαταρκτικές διαδικασίες που ουσιαστικά καθορίζουν τις εσωτερικές πολιτικές συμμόρφωσης.
- Σε δεύτερο στάδιο έρχονται οι οργανωτικές συμφωνίες που περιλαμβάνουν τα βασικά στοιχεία της λογοδοσίας, διαφάνειας και συμμόρφωσης με τους νομικούς κανόνες.
- Σε τρίτο στάδιο έρχονται οι τεχνικές διαδικασίες, που αναφέρονται σε επίπεδα πρόσβασης και απομόνωση δεδομένων και τέλος σε τέταρτο στάδιο πρέπει να έρθει η παρακολούθηση των συστημάτων και η εξασφάλιση της ιχνηλασιμότητας.

Και σε αυτό το μοντέλο η προσέγγιση αρχικά είναι οργανωτική και όχι τεχνική. Δεν δίνονται συγκεκριμένες τεχνικές λύσεις, παρ' όλα αυτά ο ορισμός των απαιτήσεων είναι τόσο πιο ξεκάθαρος που εύκολα μπορεί να οδηγήσει σε επιλογή των τεχνικών αυτών. Άλλωστε, πέρα από τις απαιτήσεις, η ομάδα των ερευνητών παρέχει και μια πιο συνεκτική μεθοδολογία που αναφέρεται σε όλα τα στάδια μελέτης, καθώς και σε ποιο σημείο πρέπει να αποφασίζονται

οι απαιτούμενες τεχνικές και οργανωτικές επιλογές, καθώς και σε ποιο στάδιο θα πρέπει να υλοποιούνται.

Αυτή η μεθοδολογία εμπλουτίστηκε αργότερα με τις κατάλληλες φάσεις για την ευθυγράμμιση με την πραγματική ανάγκη, δηλαδή την ίδια τη διαδικασία εγκληματολογικής έρευνας (Simou, et al., 2022). Έτσι, επιτεύχθηκε μια πιο άμεση αντιστοίχιση της θεωρίας με τον ερευνητικό στόχο, με αποτέλεσμα το εννοιολογικό μοντέλο να προσεγγίσει ουσιαστικότερα μια ρεαλιστική διαδικασία προετοιμασίας εγκληματολογικής έρευνας. Αυτό πραγματοποιήθηκε μέσα από δύο βασικές ενέργειες. Πρώτον, εισήχθη η διαδικασία *Investigation Process Alignment*, η οποία, μέσα από τις δύο φάσεις της, καθορίζει τις πιθανές λύσεις και στη συνέχεια επιβεβαιώνει τα αποτελέσματά της. Δεύτερον, εξετάστηκαν οι επτά περιορισμοί ετοιμότητας, στους οποίους αποδόθηκε αντιστοίχιση με τα στάδια της εγκληματολογικής διαδικασίας, ώστε το μοντέλο να αποκτήσει πιο απτές σχεδιαστικές απαιτήσεις και να καταστεί σαφέστερο το πότε πρέπει να λαμβάνονται αποφάσεις σχετικά με την ενίσχυση της εγκληματολογικής ετοιμότητας μιας υποδομής ή υπηρεσίας.

Τέλος, όλα τα παραπάνω δοκιμάστηκαν πειραματικά στο Πανεπιστήμιο Αιγαίου, σε υπηρεσίες οι οποίες επέτρεπαν την υλοποιησιμότητα του δοκιμαστικού έργου. Στόχος της δοκιμαστικής εφαρμογής ήταν να αξιολογηθεί το μοντέλο σε σχέση με τη δυνατότητα μεταφοράς σε πραγματικές συνθήκες αλλά και να αξιολογηθεί και το επίπεδο εγκληματολογικής ετοιμότητας που προσφέρει. Η πιο χαρακτηριστική υπηρεσία που επιλέχθηκε για εφαρμογή ήταν η υπηρεσία παροχής εικονικών μηχανών με βασικό πάροχο την Digital Ocean. Τα αποτελέσματα αξιολογήθηκαν τόσο σε σχέση με υλοποίηση των θεωρητικών 7 απαιτήσεων όσο και τη συμμόρφωση με τα βήματα της εγκληματολογικής διαδικασίας. Αξιολογήθηκαν τόσο οι ελλείψεις όσο και εν τέλει το συνολικό επίπεδο ετοιμότητας. Αποτέλεσμα ήταν η αναμενόμενη επιβεβαίωση της σημαντικότητας του μοντέλου τόσο όσον αφορά την εγκληματολογική του χρήση αλλά και της ικανότητάς του να αναδείξει σημεία που χρήζουν ενίσχυσης.

Επιπλέον, η πειραματική εφαρμογή έδειξε πως ο οικονομικός παράγοντας αλλά και η ευκολία στην εφαρμογή του δεν αποτελούν ανασταλτικό παράγοντα για την υιοθέτησή του. Δεν απαιτεί σημαντικές τεχνικές αλλαγές, ενώ μπορεί να εφαρμοστεί και σταδιακά,

υλοποιώντας αρχικά τους κρισιμότερους περιορισμούς και στη συνέχεια τους υπολοίπους. Τελικά γίνεται ξεκάθαρο πως η απόσταση μεταξύ θεωρητικού μοντέλου και πρακτικής εφαρμογής δεν είναι τόσο σημαντική.

Πέρα από τα μοντέλα που δείξαμε, υπάρχουν και άλλα που προτείνονται από διεθνείς οργανισμούς ή άλλες πρωτοβουλίες. Μερικά από αυτά είναι

Kent Forensic Readiness Model (FRM) (Wedad Alawad, 2021)

Ένα από τα πρώτα συστηματικά μοντέλα ετοιμότητας, με έμφαση:

- Στον καθορισμό πολιτικών για συλλογή αποδεικτικών στοιχείων
- Στη συντονισμένη ανταπόκριση των εσωτερικών ομάδων
- Στην ενημέρωση του προσωπικού και εκπαίδευσή του για τη διαχείριση περιστατικών

Tan & Rahman Forensic Readiness Framework (FRF) (Tan, 2001)

Εστιάζει περισσότερο στα τεχνικά και διαδικαστικά μέτρα. Περιλαμβάνει:

- Προληπτική καταγραφή δεδομένων
- Καθορισμό σημείων συλλογής
- Ανάθεση ρόλων και ευθυνών σε ομάδες IT & ασφάλειας
- Διασφάλιση της νομικής συμμόρφωσης των καταγραφών

Rowlingson Forensic Readiness Planning Process (Rowlingson, 2004)

Πολύ πρακτικό μοντέλο που προτείνει 10 συγκεκριμένα βήματα, μερικά από τα οποία είναι:

- Προσδιορισμός πιθανών περιστατικών
- Ανάλυση των αναμενόμενων αποδεικτικών στοιχείων
- Ανάπτυξη πολιτικής για την προετοιμασία και την αποθήκευση
- Εκτίμηση κόστους έναντι οφέλους της εγκληματολογικής ετοιμότητας

ISO/IEC 27043 – Incident Investigation Principles and Processes (Iso, 2015)

Ένα πιο γενικό πρότυπο, αλλά με εφαρμογή στην προετοιμασία:

- Τονίζει τη σημασία της προετοιμασίας και της ύπαρξης σχεδίου
- Εστιάζει στην τεκμηρίωση και στην ακεραιότητα των στοιχείων
- Χρησιμοποιείται συχνά ως βάση για ειδικότερα μοντέλα ετοιμότητας

Επιπλέον μοντέλα όπως το *NIST Model*, το *Cloud Incident Response Model* και το *Cloud Forensic Readiness Framework*, συμφωνούν σε κάποιες από τις παραμέτρους που είδαμε προηγουμένως και επισημαίνουν διαφορετικά στάδια σε διαφορετικά επίπεδα λεπτομέρειας, δεν αλλάζουν όμως το επίπεδο της κατανόησης που προσέφεραν τα δύο παραπάνω μοντέλα.

Στο τελικό ερώτημα, του ποια μεθοδολογία θεωρείται η σωστή, η απάντηση μπορεί να έρθει από τον συγκερασμό των πληροφοριών που έρχονται από πολλαπλές πηγές και τη δημιουργία ενός ελάχιστου κοινού συνόλου βημάτων για την επίτευξη της ετοιμότητας. Ένα γενικό μοντέλο ετοιμότητας θα μπορούσε να είναι το ακόλουθο, χωρίς αυτό να αναφέρεται σε συγκεκριμένη αλληλουχία βημάτων:

1. Καθορισμός Στρατηγικής και Πολιτικής Ετοιμότητας, προσδιορισμός και των συμβάντων
2. Σχεδίαση Εγκληματολογικά Έτοιμων Υπηρεσιών
3. Στρατηγική Διατήρησης Αποδεικτικών Στοιχείων
4. Αξιολόγηση Τεχνολογιών και Εργαλείων
5. Στρατηγική Κατάρτισης και Ετοιμότητας του Προσωπικού
6. Συμμόρφωση με Νομικές και Κανονιστικές Απαιτήσεις
7. Συνεχής Αξιολόγηση και Βελτίωση του Μοντέλου

4.3 Νομικό επίπεδο

Τελικό στάδιο προσέγγισης των ζητημάτων είναι αυτό της νομικής συμμόρφωσης ή της προσαρμογής των ίδιων των νομικών πλαισίων. Εκ προοιμίου θεωρούμε αυτονόητο πως τα νομικά ζητήματα είναι εξαιρετικά πολύπλοκα, καθώς απαιτείται συμφωνία πολλών

οργανισμών ή και κρατών. Σε κάθε περίπτωση θα γίνει μια απόπειρα προσδιορισμού της κατεύθυνσης της λύσης, ανεξάρτητα του πόσο εφικτή είναι.

4.3.1 Υποχρεώσεις παρόχων cloud υπηρεσιών

Οι πάροχοι θα πρέπει να μετέχουν στην πρωτοβουλία για την επίλυση σημαντικών παραμέτρων των προβλημάτων. Συγκεκριμένα, θα πρέπει να ξεκινήσουν από θέματα ακεραιότητας αποδεικτικών στοιχείων και τήρησης της αποδεικτικής αλυσίδας. Επιπλέον, θα πρέπει να κινηθούν προς την κατεύθυνση της διαφύλαξης της ιδιωτικότητας αλλά με παράλληλη συμμόρφωση με τις δικαστικές εντολές για παροχή δεδομένων. Τέλος, θα πρέπει να γίνει και προσπάθεια στο θέμα της εμπιστοσύνης στον ίδιο τον πάροχο και τις διαδικασίες του.

Για το θέμα της ακεραιότητας των δεδομένων, η προσέγγιση των παρόχων μπορεί να είναι τεχνική, αλλά απαιτείται και η τεκμηρίωση καθώς και η δημιουργία των προϋποθέσεων για εμπιστοσύνη στον πάροχο. Οι τεχνικές λύσεις μπορεί να ενισχυθούν από μηχανισμούς επικύρωσης από ανεξάρτητα τρίτα μέλη, ενώ η εμπιστοσύνη θα πρέπει να θεσπίζεται με έναν μηχανισμό τήρησης προέλευσης δεδομένων (*data provenance mechanism)*, ο οποίος θα μπορούσε επιπλέον να βοηθήσει και στην τήρηση της αποδεικτικής αλυσίδας. Το θέμα της εμπιστοσύνης στον πάροχο μπορεί να ενισχυθεί και εναλλακτικά με ένα εξωτερικό εργαλείο εκτίμησης εμπιστοσύνης. Ένα πιθανό τέτοιο εργαλείο, σύμφωνα με τους Mary-Jane Sule, Maozhen Li, Gareth Taylor, Clement Onimein, (Purnaye & Kulkarni, 2022) βασίζεται σε εκτίμηση ασαφούς λογικής (*fuzzy logic*) της εμπιστοσύνης στο σύνολο των επιπέδων. Τέλος, η εμπιστοσύνη μπορεί να ενισχυθεί ακόμα και με την τήρηση των SLAs και ενδεχομένως με την ύπαρξη ενός πλαισίου επιβεβαίωσης των συμφωνιών SLAs.

Στο θέμα της ιδιωτικότητας, ο πάροχος θα πρέπει να έχει σαν σημείο εκκίνησης τη συμμόρφωση με τους διεθνείς κανονισμούς για δεδομένα, όπως οι GDPR και CCPA (Purnaye & Kulkarni, 2022). Επιπλέον, η χρήση τεχνικών μεθόδων, όπως της κρυπτογράφησης των δεδομένων και της απομόνωσης που προαναφέρθηκαν, ενισχύουν πέρα από τη συμμόρφωση και την αποτελεσματικότητα του παρόχου.

4.3.2 Νομικό Πλαίσιο και Ζητήματα Συμμόρφωσης

Στο νομικό πλαίσιο, τα ζητήματα είναι αρκετά πιο ξεκάθαρα. Το βασικό πρόβλημα της πολυδικαιοδοσίας απαιτεί την υιοθέτηση ενός παγκόσμιου προτύπου που θα καθορίζει επαρκώς τόσο τη δικαιοδοσία όσο και τις διαδικασίες διεξαγωγής εγκληματολογικών ερευνών στο πλαίσιο διεθνούς συνεργασίας. Οι ποικίλες προτάσεις οφείλουν να συγχωνευθούν σε ένα ενιαίο σχήμα, το οποίο θα αντιμετωπίζει ζητήματα όπως η τοποθεσία του εγκλήματος, η αρμοδιότητα και η υποχρέωση κάθε εμπλεκόμενου φορέα για την παροχή αποδείξεων, καθώς και η νομική αποδοχή αυτών ανεξαρτήτως του υπεύθυνου οργανισμού.

Η πρόταση για την πολυδικαιοδοσία μπορεί να βασιστεί σε θεωρίες όπως αυτές που προαναφέρθηκαν σε σχέση με την τοποθεσία του συμβάντος, ή το μέσο είτε του αποτελέσματος (*Criminal Event*, *Criminal Instrument*, *Direct Consequence Theory)* (Karagiannis & Vergidis, 2021), με δυνατότητα υβριδικής εφαρμογής ή συνδυασμού τους. Στόχος είναι να αποτρέπεται ο δράστης από το να επιλέγει αυθαίρετα τη δικαιοδοσία προς όφελός του. Παραδείγματα από τις Ηνωμένες Πολιτείες, όπως η εφαρμογή της θεωρίας της εθνικότητας του επιτιθέμενου στην Καλιφόρνια, δείχνουν ότι σημασία αποδίδεται στην ιθαγένεια του δράστη ανεξαρτήτως της φυσικής τοποθεσίας των δεδομένων. Ωστόσο, αυτή η προσέγγιση

δεν επαρκεί από μόνη της και απαιτείται η συμβολή ενός διεθνούς συστήματος αμοιβαίας νομικής συνδρομής.

Αναφορικά με την ενίσχυση της αποδεικτικής εγκυρότητας στα δικαστήρια, έχουν προταθεί διάφορα πλαίσια (Alashjaee, 2024), (Purnaye & Kulkarni, 2022):

- **FoRCE Framework**: καθορίζει πώς η συλλογή και παρουσίαση αποδείξεων μπορεί να γίνει νομικά αποδεκτή.
- **CLASS Framework**: διασφαλίζει την αυθεντικότητα των αρχείων καταγραφής.
- **CURE Framework**: εστιάζει στην προστασία της ακεραιότητας και της χρονικής εγκυρότητας των δεδομένων.

Επιπλέον, οργανισμοί όπως ο ACPO (Association of Chief Police Officers, 2012) προτείνουν κατευθυντήριες αρχές καλής πρακτικής για τη διαχείριση των ψηφιακών αποδεικτικών στοιχείων:

- Αποφυγή οποιασδήποτε ενέργειας που μεταβάλλει τα δεδομένα.
- Περιορισμένη πρόσβαση σε εξειδικευμένο προσωπικό.
- Διατήρηση της αποδεικτικής αλυσίδας σε όλα τα στάδια επεξεργασίας.
- Απόδοση πλήρους νομικής και τεχνικής ευθύνης στον υπεύθυνο ερευνητή.

Συνολικά, το νομικό πλαίσιο επιτρέπει στους παρόχους να αναλάβουν πρωτοβουλίες, ωστόσο η βασική έλλειψη έγκειται στην απουσία διεθνούς προτυποποίησης, τόσο σε επίπεδο νομικού καθεστώτος όσο και διαδικασιών.

5 Μελέτες περίπτωσης και πιθανά μελλοντικά προβλήματα

5.1 Μελέτες περίπτωσης ψηφιακών εγκλημάτων cloud

Στην πορεία των ετών, έχουν σημειωθεί σημαντικές περιπτώσεις παραβιάσεων ασφαλείας, που έχουν γίνει γνωστές στο ευρύ κοινό. Ενδιαφέρον παρουσιάζει η παράθεση αυτών, κυρίως με σκοπό την αναγνώριση των βασικών προβληματισμών που δημιουργούνται. Είναι αναμενόμενο πως το σύνολο αυτών των παραβιάσεων θα αναδείξει και θα επιβεβαιώσει την θεωρητική προσέγγιση των προηγούμενων κεφαλαίων όσον αφορά τις βασικές δυσκολίες που παρουσιάζει η εγκληματολογική έρευνα στο cloud, αλλά και την πιθανή εγκυρότητα των κατευθύνσεων προς επίλυση που έχουν αναφερθεί.

5.1.1 Παραβίαση Sony PlayStation Network

Το 2011 η Sony δέχθηκε μία επίθεση στο δίκτυο του PlayStation (Arthur, 2011). Η βασική επίθεση ήταν τύπου DDOS, με σκοπό τόσο να αποτρέψει χρήστες από την πρόσβαση στις υπηρεσίες, να αποδιοργανώσει τις υπηρεσίες με σκοπό να εκμεταλλευτεί ευπάθειες στους servers της εταιρείας, αλλά και να αποκρύψει τις δραστηριότητες των επιτιθέμενων. Η επίθεση αυτή δεν θεωρείται ακριβώς επίθεση σε cloud υποδομή, όμως παρουσιάζει πολλά κοινά στοιχεία γιατί καθώς το δίκτυο PSN βασιζόταν σε αντίστοιχες τεχνολογίες, που οδήγησαν σε αντίστοιχα προβλήματα με αυτά που μελετώνται.

Η επίθεση είχε σαν αποτέλεσμα να εκτεθούν 77 εκατομμύρια λογαριασμοί του δικτύου PSN,. Αυτό, πέρα από το υπολογιζόμενο κόστος των 170 εκατομμυρίων δολαρίων, είχε και ένα εξαιρετικά σημαντικό κόστος στο προφίλ της εταιρείας. Τα αποτελέσματα της εγκληματολογικής έρευνας δεν είναι ευρέως γνωστά, καθώς υπάρχουν υποψίες ότι συγκεκριμένες ομάδες βρίσκονταν πίσω από την επίθεση, και είναι αμφίβολο αν

πραγματικά υπήρχαν τα κατάλληλα στοιχεία για την στοιχειοθέτηση μιας υπόθεσης. Βασικές δυσκολίες στην εγκληματολογική έρευνα ήταν:

- Ελλιπή στοιχεία καταγραφής από το ίδιο το δίκτυο του PSN. Οι ενέργειες των χρηστών δεν καταγράφονταν σε πραγματικό χρόνο και δεν ήταν ξεκάθαρο τι γινόταν την ώρα της επίθεσης.
- Οι επιτιθέμενοι χρησιμοποίησαν αντιδικανικές τεχνικές για να αποκρύψουν τόσο την πηγή της επίθεσης όσο και πιθανά ίχνη. Σε συνδυασμό με την μη ύπαρξη τεχνικών από την εταιρεία για σωστή διαφύλαξη των όποιων αρχείων καταγραφής, αυτό έκανε την έρευνα ακόμα δυσκολότερη.
- Ο όγκος των δεδομένων προς μελέτη για την εξακρίβωση των ενεργειών ήταν εν τέλει πολύ μεγάλος. Σε αυτό συνέτεινε η μη τήρηση σωστών αρχείων καταγραφής, αφού οι ερευνητές θα έπρεπε να μελετήσουν τα ίδια τα δεδομένα για την εξακρίβωση της παραβίασης.

Θα πρέπει επίσης να αναφερθεί πως η διαρροή των προσωπικών δεδομένων των χρηστών έφερε στο προσκήνιο και ελλείψεις στην απαραίτητη προστασία τους, σύμφωνα με τον GDPR, κάτι που άφησε την εταιρεία εκτεθειμένη σε αγωγές και ελέγχους από ρυθμιστικές αρχές, ενώ και η απόδοση της εταιρείας στην προστασία των δεδομένων πιστωτικών καρτών τέθηκε στο μικροσκόπιο. Έτσι το κόστος για την εταιρεία ήταν πολλαπλάσια μεγαλύτερο εν τέλει στην πορεία του χρόνου.

5.1.2 Η παραβίαση του Dropbox

Το 2012 σημειώθηκε μια σημαντική παραβίαση ασφαλείας στο Dropbox (BBC, 2016). Οι επιτιθέμενοι χρησιμοποίησαν στοιχεία πρόσβασης χρηστών που είχαν διαρρεύσει από άλλες παραβιάσεις και απέκτησαν πρόσβαση σε λογαριασμούς μέσω credential stuffing. Ουσιαστικά, η εταιρεία βρέθηκε εκτεθειμένη, καθώς οι επιτιθέμενοι εκμεταλλεύτηκαν κάποια κενά ασφαλείας, κυρίως στην απουσία πιστοποίησης δύο παραγόντων, αλλά και την κακή πολιτική της διαχείρισης των κωδικών πρόσβασης. Επιπλέον, η απουσία επιτήρησης

και ανίχνευσης της κακόβουλης δραστηριότητας άφησε το σύστημα εκτεθειμένο. Τα βασικά προβλήματα της εγκληματολογικής έρευνας ήταν:

- Δυσκολία αναγνώρισης της επίθεσης. Η μη καταγραφή και η χρήση νόμιμων στοιχείων έκανε δύσκολη την αναγνώριση ότι υπήρχε επίθεση, αλλά και τη συλλογή στοιχείων στη συνέχεια.
- Η φύση του τρόπου αποθήκευσης των δεδομένων στο cloud δυσκόλεψε στην αποκατάσταση των δεδομένων, αλλά και την μελέτη αυτών για την παροχή αποδεικτικών στοιχείων.
- Μη ξεκάθαρη νομική προσέγγιση του θέματος και δικαιοδοσία. Εν τέλει, νομικά δεν υπήρχε κάποιο αποτέλεσμα ούτε απέναντι στους επιτιθέμενους, ούτε και σε σχέση με τις ευθύνες της ίδιας της εταιρείας. Το θολό τοπίο της δικαιοδοσίας για υποθέσεις που αφορούσαν χρήστες παγκοσμίως δεν έφτασε να δοκιμαστεί

5.1.3 Η παραβίαση του AWS της Uber

Το 2016 η Uber δέχθηκε και αυτή μια επίθεση στις υποδομές της που χρησιμοποιούσαν το Amazon Web Services (AWS) (Uber, 2017). Και σε αυτή την περίπτωση οι επιτιθέμενοι χρησιμοποίησαν κλεμμένα διαπιστευτήρια για να αποκτήσουν πρόσβαση σε λογαριασμούς χρηστών. Αυτή τη φορά τα κλεμμένα διαπιστευτήρια ανήκαν στην ίδια την Uber, η οποία είχε προβεί σε πολύ κακή διαχείριση τους, αποθηκεύοντας τα στο GitHub. Η επίθεση επηρέασε εν τέλει 57 εκατομμύρια χρήστες που συμπεριλάμβαναν πελάτες αλλά και οδηγούς, ενώ η ίδια η εταιρεία ανακοίνωσε ότι πλήρωσε ένα ποσό της τάξης των 100,000 δολαρίων στους επιτιθέμενους για να διαγράψουν τα στοιχεία.

Βασικό ζήτημα στην επίθεση ήταν η δυσκολία στην ανίχνευσή της. Ουσιαστικά, η μη ύπαρξη κατάλληλου συστήματος ανίχνευσης της ύποπτης δραστηριότητας έθεσε την εταιρεία σε ακόμα πιο δύσκολη θέση, καθώς δεν ήταν πλέον σε θέση να αποκαταστήσει τη ζημιά ή να συλλέξει τα κατάλληλα στοιχεία. Επιπλέον, τέθηκε και το θέμα της διαφάνειας της έρευνας, και της τήρησης των όποιων διαδικασιών. Το δεδομένο του συμβιβασμού της εταιρείας θέτει εν αμφιβόλω την σωστή παροχή πληροφοριών στους ερευνητές, αλλά και την ουσιαστική έγκαιρη έναρξη της έρευνας. Εν τέλει, και η ίδια η εταιρεία θα πρέπει να ελέγχεται σε σχέση

με την τήρηση των υποχρεώσεών της. Η επίθεση είχε σαν στόχο τα συστήματα της Uber στο AWS και αυτό αύξησε την πολυπλοκότητα, ενώ τέθηκαν και ζητήματα άλλων πιθανών επηρεαζόμενων από την επίθεση. Όσον αφορά τα θέματα δικαιοδοσίας, και πάλι αν και δεν υπήρξε κάποια νομική απόφαση, το θέμα της δικαιοδοσίας ήταν μη ξεκάθαρο.

5.1.4 Η επίθεση στο AWS S3 Bucket της Verizon

Η παραβίαση αυτή συνέβη το 2017 και αφορούσε ένα δημόσιο σύνολο δεδομένων της εταιρείας, το οποίο περιείχε ευαίσθητα δεδομένα και δεν είχε προστατευτεί κατάλληλα (Bacon, 2017). Η επίθεση αυτή παρουσιάζει ενδιαφέρον διότι δεν χρειάστηκε καμία ιδιαίτερη τεχνική από τους επιτιθέμενους. Τα δεδομένα ήταν απλώς εκεί και εύκολα διαθέσιμα, κάνοντας το περιστατικό να μην μοιάζει καν με επίθεση. Αυτό φυσικά είχε ως αποτέλεσμα τη μεγάλη καθυστέρηση στην αναγνώριση της παραβίασης. Επιπλέον, έθεσε και το θέμα της ευαλωτότητας των υπηρεσιών, ανεξαρτήτως των ενεργειών του ίδιου του παρόχου της υπηρεσίας. Ο πάροχος μπορεί να είχε ακόμα και υπηρεσίες ετοιμότητας, αλλά η σχεδόν νόμιμη χρήση των δεδομένων κατέστησε όλες αυτές τις διαδικασίες αναποτελεσματικές.

5.1.5 Παραβίασης δεδομένων της Capital One, μέσω AWS (2019)

Ένα από τα μεγαλύτερα περιστατικά ασφάλειας συνέβη μέσω των υποδομών Amazon Web Services (AWS) που χρησιμοποιούσε η Capital One (Khan, 2022). Η έκθεση βασίστηκε σε ευπάθεια ενός συστήματος της AWS, αλλά κατέστη δυνατή λόγω κακών ρυθμίσεων ασφαλείας από τους χρήστες της υπηρεσίας. Εντυπωσιακό ήταν ότι η επίθεση διήρκεσε 4 μήνες και αποτέλεσμα της ήταν η διαρροή δεδομένων εκατομμυρίων χρηστών της Capital One, συμπεριλαμβανομένων και οικονομικών στοιχείων. Η επίθεση έγινε τελικά γνωστή από ένα εξωτερικό άτομο και όχι από την ίδια την εταιρεία. Και πάλι είναι εμφανής η δυσκολία στην αναγνώριση της επίθεσης, καθώς οι μήνες που πέρασαν έθεσαν όλο και περισσότερα δεδομένα σε κίνδυνο, αλλά και τα πιθανά στοιχεία. Η έρευνα επίσης καθυστέρησε λόγω των ελλιπών αρχείων καταγραφής που παρείχε το AWS, ενώ πέρα από τα ίδια τα στοιχεία, ο επιτιθέμενος χρησιμοποίησε και τεχνικές απόκρυψης των ιχνών του. Στο συγκεκριμένο παράδειγμα έγινε για άλλη μια φορά ξεκάθαρη η ανάγκη για ετοιμότητα τόσο στην ανίχνευση όσο και στην παροχή δεδομένων κατά την έρευνα.

Σε νομικό επίπεδο, είχε ενδιαφέρον το πώς εκτεθειμένοι βρέθηκαν τόσο οι επιτιθέμενοι (που τελικά ταυτοποιήθηκε ως η Paige Thompson) όσο και η Capital One, αλλά και η ίδια η AWS. Ο κάθε εμπλεκόμενος είχε ένα συγκεκριμένο κομμάτι ευθύνης, με τελικό κόστος αρκετά εκατομμύρια δολάρια

5.1.6 Επίθεση σε IoT συσκευές της Verkada (AWS) (2020)

Το 2020 συνέβη και επίθεση σε πλατφόρμα IoT. Η εταιρεία Verkada χρησιμοποιούσε την AWS για την αποθήκευση δεδομένων, και ιδιαίτερα δεδομένων από κάμερες ασφαλείας σε δημόσιους οργανισμούς. Οι επιτιθέμενοι εκμεταλλεύτηκαν κενά ασφαλείας της πλατφόρμας, χρησιμοποιώντας διαπιστευτήρια που είχαν διαρρεύσει σε άλλη χρονική στιγμή και απέκτησαν πρόσβαση στο σύστημα, εκμεταλλευόμενοι ουσιαστικά και τον ελλιπή έλεγχο πρόσβασης του cloud προς αυτές τις συσκευές (Hulme, 2025).

Από τις βασικότερες δυσκολίες της έρευνας αποτέλεσε ο κατακερματισμός των δεδομένων, χαρακτηριστικό άλλωστε όλων των IoT εφαρμογών. Διαφορετικές δικαιοδοσίες για τα δεδομένα αυτά έκαναν ακόμα πιο δύσκολη τη λήψη στοιχείων και αποδεικτικών για την έρευνα σε κάθε περιοχή. Ο όγκος των δεδομένων ήταν σημαντικά μεγάλος, με αποτέλεσμα τη δυσκολία στην ανάλυσή τους αλλά και την αποκατάστασή τους εν τέλει

5.1.7 Επίθεση στο Microsoft Azure (2021)

Το 2021 καταγράφηκε μια σημαντική επίθεση που αφορούσε την πλατφόρμα Microsoft Azure. Συγκεκριμένα, οι επιτιθέμενοι εκμεταλλεύτηκαν αδυναμίες στο Active Directory, καταφέρνοντας να αποκτήσουν πρόσβαση σε υποδομές και λογαριασμούς, χωρίς την έγκριση των ιδιοκτητών τους (Lakshmanan, 2021). Και σε αυτή την περίπτωση, παρατηρήθηκε καθυστέρηση στην αναγνώριση του συμβάντος από την εταιρεία, ενώ οι επιτιθέμενοι χρησιμοποίησαν επίσης αντιδικανικές τεχνικές για να συγκαλύψουν τα ίχνη τους. Κατά τη διάρκεια της έρευνας, τα ζητήματα που αφορούσαν τη φύση των δεδομένων, αλλά και την τοποθεσία αποθήκευσής τους, δυσχέραναν σημαντικά το έργο των ερευνητών.

Επιπλέον, το ζήτημα της δικαιοδοσίας, σε σχέση με δεδομένα και υπηρεσίες που βρίσκονταν κατανεμημένα σε διάφορες περιοχές, παρουσίαζε και πάλι σημαντικές προκλήσεις.

Αυτό το περιστατικό, καθώς και τα προηγούμενα, αναδεικνύουν σταθερά τα ίδια καίρια ζητήματα, ενώ παράλληλα υπογραμμίζουν την ανάγκη για σαφή ορισμό των πιο σημαντικών εξ αυτών. Στις προτεινόμενες λύσεις, συχνά επανέρχεται το ζήτημα του κόστους, και μια κατηγοριοποίηση βάσει των προτεραιοτήτων των αναγκών θα μπορούσε να καταστήσει τις προσπάθειες βελτίωσης πιο εφικτές και οικονομικά βιώσιμες.

5.2 Μελλοντικά προβλήματα

Πέρα από τα υφιστάμενα προβλήματα, όμως, οι επιστημονικοί ερευνητές πρέπει πάντα να κοιτάζουν και προς το μέλλον. Ιδιαίτερα σε ένα περιβάλλον που εξελίσσεται συνεχώς, η έρευνα οφείλει να παραμένει ένα βήμα μπροστά. Συνεπώς, είναι απαραίτητο να διατυπωθεί μια εικόνα για το τι φέρνει το μέλλον και πώς ενδεχομένως νέες προκλήσεις θα ανακύψουν στον τομέα της εγκληματολογικής έρευνας στο cloud.

Υπάρχουν δύο τρόποι προσέγγισης του ζητήματος. Αρχικά, οι τεχνικές εξελίξεις που ήδη συντελούνται και επηρεάζουν τον χώρο, θα ενταχθούν στα υπάρχοντα προβλήματα και θα αποτελέσουν αντικείμενο έρευνας για το άμεσο μέλλον. Σε δεύτερο επίπεδο, θα προσεγγιστούν και οι μελλοντικές εξελίξεις που δεν έχουν ακόμα αρχίσει να δείχνουν ξεκάθαρα τις επιπτώσεις τους στον χώρο. Σε πρώτο επίπεδο, τα βασικότερα ζητήματα είναι:

Αύξηση πολυπλοκότητας συστημάτων και ένταση πολυμίσθωσης.

Νέες τεχνολογίες έρχονται να κάνουν ακόμα πιο εύκολη την πολυμίσθωση των συστημάτων και τον διαχωρισμό τους σε μικρότερα τμήματα ή αντικείμενα. Τα συστήματα γίνονται περισσότερο πολύπλοκα, κάτι που δυσχεραίνει το έργο της αναγνώρισης τόσο των περιστατικών όσο και του διαχωρισμού των στοιχείων που απαιτούνται. Παρατηρείται εντατικοποίηση της χρήσης τεχνολογιών Containers και αρχιτεκτονικών microservices, έτσι γίνεται όλο και μικρότερη η ελάχιστη μονάδα μίσθωσης για έναν πελάτη. Δημιουργώντας μια πολύ μικρότερη ελάχιστη ποσότητα υπηρεσίας, επιτυγχάνεται η ευελιξία, αυτονομία και η δυνατότητα κλιμάκωσης των υποδομών, εντούτοις εντείνεται η ύπαρξη πεπλεγμένων κατανεμημένων υποδομών που, σε περίπτωση ενός περιστατικού, θα πρέπει να

απομονωθούν και στο επίπεδο έρευνας. Μελετώντας την αγορά του cloud computing, είναι δύσκολο να εξαχθεί η πληροφορία της ακριβούς χρήσης τέτοιων τεχνολογιών, όμως ο συνδυασμός της αύξησης χρήσης του cloud και ένα ενδεικτικό της αύξησης της χρήσης μιας εκ των τεχνολογιών αυτών (Docker) κατά 45% σε σχέση με την προηγούμενη χρονιά, δίνει μια εποπτική εικόνα του μέλλοντος (Waters, 2024).

Κρυπτογράφηση δεδομένων

Η τάση για όλο και περισσότερη κρυπτογράφηση δεδομένων των πελατών εντείνει την αδυναμία αποκρυπτογράφησης και παροχής των δεδομένων όταν αυτά χρειάζονται. Το πρόβλημα εντείνεται, διότι η αυτόματη κρυπτογράφηση και αποκρυπτογράφηση κατά την εγγραφή και ανάγνωση αντιστοίχως, αλλά και η μη τήρηση κλειδιών αποκρυπτογράφησης από τον ίδιο τον πάροχο, αποτελεί θεμελιώδες στοιχείο της παρεχόμενης υπηρεσίας και η άρνηση του πελάτη να συνεργαστεί όταν δεν το επιθυμεί, δημιουργεί νέα προσχώματα. Επιπλέον, η κρυπτογράφηση των δεδομένων ακόμα και κατά τη μεταφορά τους (Encryption in transit) (AWS, 2025) δυσχεραίνει και τις διαδικασίες εγκληματολογικής ετοιμότητας πραγματικού χρόνου. Τέλος, η κρυπτογράφηση δημιουργεί ένα ακόμα επίπεδο δυσκολίας στην ανασυγκρότηση και μελέτη μεγάλου όγκου δεδομένων, καθιστώντας έτσι τους χρόνους έρευνας απαγορευτικούς.

Δυναμικότητα δεδομένων

Παρατηρείται όλο και μεγαλύτερη ανάγκη για δεδομένα άμεσης πρόσβασης που απαιτούν την αποθήκευσή τους σε γρήγορες μνήμες αλλά προσωρινής φύσης. Επιλέγονται έτσι σε πολλές εφαρμογές in-memory βάσεις δεδομένων και προσωρινές δομές αποθήκευσης. Επιπλέον, συστήματα που απαιτούν ανάλυση ή χρήση δεδομένων σε πραγματικό χρόνο (Apache Spark) έχουν ως απαίτηση τέτοιες μνήμες. Το αποτέλεσμα της εντατικοποίησης της χρήσης αυτής είναι μια νέα κατηγορία δεδομένων, μια κατηγορία που έχει δυσκολία τόσο στη συλλογή και ανάκτηση των ιδίων των στοιχείων, συχνά δεν έχει συνεπή καταγραφή ενεργειών και εν τέλει δημιουργεί υψηλό βαθμό πολυπλοκότητας στην ανάλυση. (IEEE, 2014)

Σε δεύτερο επίπεδο ζητήματα που θα έχουν μεγάλη σημασία στο μέλλον είναι τα ακόλουθα:

Serverless computing

Το επόμενο στάδιο αφαίρεσης μετά τις τεχνολογίες containers και microservices είναι το serverless computing. Σε αυτή την τεχνολογία εξαλείφεται εντελώς για τον χρήστη η ανάγκη ύπαρξης οποιασδήποτε υποδομής (εικονικές μηχανές) και οι εφαρμογές εκτελούνται σχεδόν αυτόνομα (CloudFlare, 2025). Αυτή βέβαια είναι η εικόνα του πελάτη. Οι πόροι αυτοματοποιούνται και κλιμακώνονται δυναμικά, αλλά χωρίς την απαίτηση διαχείρισης από τον ίδιο τον χρήστη. Το βάρος της δημιουργίας και διαχείρισης όλων αυτών των υπηρεσιών πέφτει στον πάροχο και ουσιαστικά μεταφέρεται ένα επίπεδο της πολυπλοκότητας περισσότερο προς την υποδομή, κάτι που επιφέρει σημαντική αύξηση της γενικής πολυπλοκότητας των διαμοιραζόμενων πόρων. Σε ένα τέτοιο περιβάλλον, η εφαρμογή εκτελείται σε ένα απομονωμένο περιβάλλον με προσωρινή μνήμη και ελλιπή καταγραφή ενεργειών. Επιπλέον, συνηθίζεται μετά το τέλος της εκτέλεσης οποιασδήποτε εφαρμογής, να γίνεται και εκκαθάριση των δεδομένων. Αυτά τα δεδομένα, αν δεν διαγραφούν και υπάρχει η απαίτηση διατήρησής τους, και πάλι θα είναι σε μεγάλο βαθμό κατακερματισμένα και δύσκολο να απομονωθούν. Αυτό έχει ως συνέπεια την καθυστέρηση στην εγκληματολογική έρευνα, ενώ συχνά θα έχει και την άρνηση του παρόχου για συνεργασία, καθώς επιφέρει σημαντικό κόστος. Η παρακολούθηση μιας τέτοιας υποδομής σε πραγματικό χρόνο, και αυτή επιφέρει κόστος, που συχνά εξαφανίζει τα οικονομικά οφέλη της προσωρινής φύσης του όλου υπολογιστικού μοντέλου, δημιουργώντας έτσι και μια σύγκρουση συμφερόντων.

Αυτή η σύγκρουση ενδεχομένως να είναι και το σημαντικότερο ζήτημα εν τέλει. Ο πάροχος δεν θα θέλει να επενδύσει στην παρακολούθηση μιας δομής που είναι σχεδιασμένη να υφίσταται μόνο προσωρινά. Ουσιαστικά, η απαίτηση της εγκληματολογικής έρευνας θα πρέπει να μετασχηματίσει σε ένα βαθμό την ίδια την φύση της υπηρεσίας.

Edge computing και IOT

Οι εξελίξεις δεν περιορίζονται μόνο σε τεχνολογίες που αφορούν υποδομές και υπηρεσίες cloud, αλλά και σε τεχνολογίες που χρησιμοποιούν το cloud σαν ένα κομμάτι της αλυσίδας των υπηρεσιών. Μία από αυτές τις περιπτώσεις είναι οι τεχνολογίες IoT και Edge Computing

(Mazur, 2025). Ορίζουμε ως Internet of Things, ένα σύνολο συνδεδεμένων εφαρμογών που χρησιμοποιούν μία μεγάλη ποσότητα μικρών φυσικών συσκευών που συνήθως έχουν λειτουργίες όπως αυτοματοποίηση διαδικασιών και εν τέλει παράγουν και διαμοιράζονται δεδομένα (Ibm, 2023). Ως Edge Computing αναφερόμαστε σε υποδομές που αναλαμβάνουν την επεξεργασία δεδομένων στην απομακρυσμένη άκρη του δικτύου, δηλαδή στην ίδια τη συσκευή (Aws, 2025). Έτσι μειώνονται καθυστερήσεις που οφείλονται σε δικτυακές υποδομές, ενώ ενισχύεται η ασφάλεια και η ιδιωτικότητα. Το Edge Computing συναντάται κατά κόρον σε εφαρμογές IoT και γι' αυτό αναφέρονται συνδυαστικά στην μελέτη αυτή. Παρά τους παραπάνω ορισμούς, πρέπει να γίνει ξεκάθαρο ότι εν τέλει πολλά από τα δεδομένα, πρωτογενή αλλά και δευτερογενή, θα πρέπει να βρεθούν στο cloud. Στην περίπτωση των πρωτογενών δεδομένων, μιλάμε για έναν τεράστιο όγκο πληροφορίας που, όπως έχουμε δει σε προηγούμενες περιπτώσεις, επιβαρύνει τη διαδικασία εγκληματολογικής έρευνας σε πολλά επίπεδα. Αυτός ο όγκος δεδομένων, σε συνδυασμό με την πολυποικιλότητά του, δημιουργεί το πιο σημαντικό πρόβλημα, όμως οι δυσκολίες δεν περιορίζονται σε αυτό. Σε περιπτώσεις edge computing, πολύ συχνά τα δεδομένα δεν έχουν φτάσει στο cloud, και σε μία περίπτωση επίθεσης δεν υπάρχει καν εξασφάλιση ότι τα δεδομένα υπήρχαν σε κάποια υποδομή πέρα από την τοπική συσκευή. Επιπλέον, δεν υπάρχει όριο στην τοποθεσία των συσκευών, δημιουργώντας έτσι μια διαφορετική, αλλά επίσης σημαντική παράμετρο του προβλήματος της δικαιοδοσίας.

Τέλος, στις περιπτώσεις IoT, οι πολλές διαφορετικές δυνατότητες σχεδιασμού δικτύων και εφαρμογών, αλλά και η δυνατότητα επαναπροσδιορισμού κατά τη διάρκεια της λειτουργίας τους, δημιουργούν μία ασαφή σχέση με προτεινόμενες πρακτικές και οδηγίες. Πολύ απλά, ο κάθε πάροχος υπηρεσιών IoT δεν δεσμεύεται από κάποιο φορέα για το σχεδιασμό του και δεν υποχρεούται ούτε σε εγκληματολογική ετοιμότητα. Εισέρχεται έτσι ένας επιπλέον κόμβος που μπορεί να είναι σημείο αποτυχίας της εγκληματολογικής διαδικασίας.

Blockchain forensics

Η τεχνολογία blockchain είχε αναφερθεί σαν μία προτεινόμενη λύση για τη δημιουργία αρχείων καταγραφής που δεν μπορούν να τροποποιηθούν. Υπάρχουν όμως και άλλες χρήσεις της τεχνολογίας αυτής που συχνά, και όλο και περισσότερο, υπεισέρχονται σε θέματα εγκληματολογικής ανάλυσης, και τα εγγενή χαρακτηριστικά της τεχνολογίας,

μετατρέπονται, από εργαλείο σε εμπόδιο στη μελέτη (Science, 2024). Συναλλαγές μέσω blockchain δικτύων δεν επιτρέπουν την ταυτοποίηση των εμπλεκομένων και αυτό μπορεί να θέσει μία έρευνα σε πλήρη αδράνεια. Ιδιαίτερα όταν αναφερόμαστε σε οικονομικές συναλλαγές, το πρόβλημα εντείνεται, καθώς έχουν αναπτυχθεί τεχνολογίες όπως οι cryptocurrency tumblers που αναμιγνύουν νόμιμες με παράνομες δραστηριότητες με σκοπό την απόκρυψη των τελευταίων. Επίσης, η μη δυνατότητα τροποποίησης δεδομένων ισχύει και για τη μελέτη αυτών, καθιστώντας τα πιο δύσκολα στην επεξεργασία και ανάκτηση σε περίπτωση κάποιας κακόβουλης ενέργειας. Φυσικά, και σε αυτή την περίπτωση εντείνεται το ζήτημα της δικαιοδοσίας. Το συγκεκριμένο ζήτημα δεν έχει λυθεί μέχρι στιγμής, αλλά κάθε νέα δραστηριότητα ή υπηρεσία ή εφαρμογή καθιστά την ανάγκη ορισμού κανόνων επιτακτική.

Τεχνητή νοημοσύνη

Στον τομέα της τεχνητής νοημοσύνης, αυτό που έρχεται να αντιμετωπίσει ο ερευνητής είναι το πρόβλημα του μαύρου κουτιού. Η πολυπλοκότητα των αλγορίθμων, αλλά και ο τρόπος εκπαίδευσης με την συνεχιζόμενη παροχή δεδομένων, κάνει σχεδόν αδύνατη την εξαγωγή συμπερασμάτων σχετικά με την εγκυρότητα των αποτελεσμάτων. Αυτό έχει διπλή σημασία, καθώς αν η τεχνητή νοημοσύνη είναι εργαλείο έρευνας, δεν είναι ξεκάθαρο πώς χτίζεται η εμπιστοσύνη και η αποδοχή από τη νομική αρχή, ενώ αν είναι αντικείμενο προς μελέτη, δεν είναι ξεκάθαρο πώς δίνεται η δυνατότητα πρόσβασης σε όλη αυτή την ποσότητα δεδομένων. Και στις δύο περιπτώσεις, η αδιαφάνεια των αλγορίθμων ενισχύει την αβεβαιότητα των αποτελεσμάτων.

Όλα τα παραπάνω αποτελούν μελλοντικά, αλλά ισως και σύγχρονα πλέον, προβλήματα. Η έρευνα και η εξέλιξη της τεχνολογίας προχωρούν παράλληλα και έτσι αναμένεται και η συγκεκριμένη έρευνα για την αντιμετώπιση ζητημάτων.

6 Σύνοψη ευρημάτων – Συμπέρασμα

Η σύντομη περιήγηση στα προβλήματα και τις πιθανές λύσεις που υπάρχουν στον χώρο της ψηφιακής εγκληματολογίας στο cloud θα πρέπει να έχει ως τελευταίο σταθμό και μια ανασκόπηση ή ίσως και ενδοσκόπηση. Βασικά ερωτήματα που τέθηκαν θα πρέπει ίσως να απαντηθούν, ή ακόμα νέες ερωτήσεις θα πρέπει να γίνουν ξεκάθαρες. Στην εκκίνηση της μελέτης στόχος ήταν η ανάδειξη των ζητημάτων και η πρόταση λύσεων. Παραμένει αυτός ο στόχος επίκαιρος ή έχει αντικατασταθεί από πιο σύνθετες απαιτήσεις; Αν ναι, ποια είναι τα ζητήματα του χώρου που θα πρέπει να θεωρηθούν αναγκαία προς άμεση επίλυση; Ποιες από τις προτεινόμενες λύσεις είναι απολύτως αναγκαίες, ή ακόμα και εφικτές; Εν τέλει, ποιο θα είναι το τοπίο σε μερικά χρόνια;

Ο αρχικός στόχος θεωρείται ότι έχει καλυφθεί, και επιπλέον παρέχεται η δυνατότητα μιας πιο ουσιαστικής εστίασης στα προβλήματα που μελετήθηκαν, καθώς και στο κατά πόσο μια λύση είναι άμεσα εφικτή. Συνοψίζοντας, τα πιο βασικά ζητήματα αφορούν την επίλυση του τεχνικοοργανωτικού ζητήματος, το οποίο θα ήταν σκόπιμο να συμπεριλάβει πολλές δύσκολες τεχνικές προκλήσεις, καθώς και την επίλυση του νομικού ζητήματος. Ωστόσο, το πιο δύσκολο ίσως σημείο είναι η προσέγγιση των προβλημάτων που δεν έχουν ακόμα πλήρως σχηματιστεί. Αυτή η ματιά στο μέλλον, καθώς και η μελέτη των αναδυόμενων τεχνολογιών, θα πρέπει να αποτελεί τόσο συμπέρασμα όσο και σημείο εκκίνησης για μια νέα μελέτη.

Τα σημεία που θα ήταν χρήσιμο να κρατηθούν ως συμπέρασμα, στους διακριτούς τομείς, είναι τα εξής:

6.1 Πρακτικές ετοιμότητας και συνεργασίας

Στην πορεία της μελέτης, εξετάστηκαν μια σειρά από προβλήματα τεχνικής φύσης, για τα οποία ενδεχομένως να μην υπάρχει τεχνική λύση, τουλάχιστον εφικτή αυτή τη στιγμή. Μια τεχνική λύση αυτών των ζητημάτων έρχεται να παρατηρήσει αδυναμίες μιας διαδικασίας και να διορθώσει τα συμπτώματα. Μια πιο ολοκληρωμένη λύση είναι να

αντιμετωπιστεί η αδυναμία της διαδικασίας στη ρίζα της, και δεν υπάρχει καλύτερο σημείο εκκίνησης από τη δημιουργία πλαισίου εγκληματολογικής ετοιμότητας.

Αυτό το πλαίσιο προφανώς δεν είναι απλό στην δημιουργία του, καθώς είναι ακόμα δύσκολο να οριστεί και ο στόχος αλλά και το εύρος, πόσο μάλλον οι διαδικασίες που το υλοποιούν. Οι προσπάθειες που έχουν γίνει και παρουσιάστηκαν, κινούνται προς τη σωστή κατεύθυνση, αφήνουν όμως, και ίσως ηθελημένα, πολλά περιθώρια ερμηνείας, υλοποίησης και εξέλιξης. Σε αυτό που συμφωνούν όμως είναι πως πρέπει να τηρούνται μια σειρά από βασικές προϋποθέσεις, ανεξαρτήτως του τρόπου υλοποίησης. Ακρογωνιαίος λίθος είναι η παροχή δεδομένων για ανάλυση. Τα δεδομένα θα πρέπει να είναι πλήρως διαθέσιμα και να εξασφαλίζεται η μη τροποποίησή τους και η απώλειά τους. Η παροχή αυτών των δεδομένων θα πρέπει να βασίζεται σε αυτοματοποιημένες διαδικασίες που τηρούν τους απαραίτητους νομικούς κανόνες, αλλά ταυτόχρονα διασφαλίζουν και την αλυσίδα εγγύησης των αποδείξεων. Ένα μοντέλο ετοιμότητας θα πρέπει επίσης να λαμβάνει υπόψη την ανάγκη για ευελιξία για τις μελλοντικές αλλαγές που θα εμφανιστούν στον χώρο, αλλά επίσης και τις ανάγκες για πλήρη κατάρτιση των εμπλεκόμενων μερών. Εν τέλει, ένα μοντέλο ετοιμότητας θα πρέπει να είναι εντελώς διαφανές και να μην έχει καμία επίπτωση στην ποιότητα των υπηρεσιών που προσφέρονται.

6.2 Παγκόσμια Πρότυπα και Διακρατική Συνεργασία

Στον νομικό τομέα, η κατάσταση είναι ακόμα πιο ξεκαθαρισμένη όσον αφορά βέβαια τις ανάγκες. Το νομικό πλαίσιο αδυνατεί να καλύψει ακόμα και βασικά αιτήματα και το σημείο εκκίνησης θα πρέπει να είναι η οριοθέτηση του ζητήματος της δικαιοδοσίας. Οι διάφορες προτάσεις για επιλογή της δικαιοδοσίας, είτε με την τοποθεσία του εγκλήματος, είτε με την τοποθεσία του δράστη, είτε ακόμα και του προϊόντος του εγκλήματος, δείχνουν ότι πάντα θα παρουσιάζουν ζήτημα αν δεν επιτευχθεί μια διακρατική δικαιοδοσία που θα παρακάμπτει το πρόβλημα των πολλαπλών τοποθεσιών αποθήκευσης. Επιπλέον απαιτείται και η εύρεση του σημείου ισορροπίας ανάμεσα στην προστασία της ιδιωτικότητας αλλά και της παροχής δεδομένων από τους παρόχους προς τις αρχές. Σε αυτό το ζήτημα πολύ μεγάλη σημασία έχει και να είναι ξεκάθαρες οι υποχρεώσεις των παρόχων, έτσι ώστε να μην χρησιμοποιείται η ασάφεια ως επιχείρημα για μη παροχή βοήθειας. Σε επόμενο

επίπεδο θα είναι εξαιρετικά χρήσιμο να θεσπιστούν και κανόνες σχετικά με τη νομική εγκυρότητα των αποδεικτικών στοιχείων. Ιδιαίτερα σε ένα περιβάλλον που οι διαδικασίες μελέτης των δεδομένων απαιτούν αλληλουχία βημάτων, πρέπει να υπάρχει ένα συνεκτικό και αυστηρό πλαίσιο ορισμού του τι επιτρέπεται ώστε να μην δημιουργούνται προσκόμματα λόγω κακής χρήσης της τεχνολογίας. Τέλος, σημαντικό θα είναι να καρποφορήσει η συζήτηση για τις νέες νομικές απαιτήσεις που φέρνει στο προσκήνιο κάθε νέα τεχνολογία. Η αντιμετώπιση των υποδομών cloud με νομοθετήματα σχεδιασμένα για τεχνολογικές υποδομές παλαιότερης γενιάς είναι αντίστοιχη με την αντιμετώπιση κλασικών εγκληματολογικών ζητημάτων με νομοθεσίες πολλών δεκαετιών πίσω. Οι εξελίξεις στην τεχνολογία απαιτούν ταχύτατες προσαρμογές στη νομική επιστήμη. Σε όλα αυτά θα πρέπει να προστεθεί και η εκπαίδευση σε όλα τα εμπλεκόμενα μέρη, κάτι που πολύ συχνά παραβλέπεται.

6.3 Αντί επιλόγου

Η επισήμανση της συνεχούς εξέλιξης των τεχνολογιών στον τομέα του cloud και της ψηφιακής εγκληματολογίας είναι πολύ σημαντική, καθώς οι νέες τεχνολογίες δημιουργούν νέες προκλήσεις και ανοίγουν αχαρτογράφητα νερά για τους επαγγελματίες του χώρου. Σήμερα αναγνωρίζουμε ως αναδυόμενη τεχνολογία την τεχνητή νοημοσύνη, το Serverless Computing, το Internet of Things και το blockchain, όμως αυτές οι τεχνολογίες απασχολούν την επικαιρότητα ήδη για δεκαετίες. Τι γίνεται όμως όταν έρθουμε αντιμέτωποι με πραγματικά καινοτόμα ζητήματα;

Οι τεχνολογίες όπως το Edge Computing σε 5G, το Quantum Computing, υποδομές Multi-cloud, το Confidential Computing, το EdgeAI και άλλες όπως το Federated AI learning και η Zero Trust Cloud Security προσθέτουν νέες διαστάσεις στην ψηφιακή εγκληματολογία, καθιστώντας την ανάγκη για νέες μεθόδους ανάλυσης και στρατηγικές ακόμα πιο επιτακτική.

Η δημιουργία ενός υβριδικού μοντέλου μελέτης που να ενσωματώνει τόσο τις τεχνολογικές όσο και τις νομικές πτυχές είναι μια καίρια ανάγκη για το μέλλον. Ένα τέτοιο μοντέλο θα μπορούσε να γεφυρώσει το χάσμα μεταξύ των δύο κόσμων, εξασφαλίζοντας ότι οι νομικοί

επιστήμονες έχουν τη γνώση για να κατανοήσουν τις νέες τεχνολογίες και οι τεχνολόγοι να κατανοήσουν τις νομικές πτυχές των καινοτόμων τεχνολογιών.

Η έμφαση σε μια δημιουργία ερωτημάτων, παρά σε συγκεκριμένα αποτελέσματα είναι μια προσέγγιση μάλλον μονόδρομος, καθώς ανοίγει το πεδίο για συνεχιζόμενη έρευνα και μελέτη. Σε έναν ταχέως εξελισσόμενο τομέα, η έρευνα και η ανοιχτότητα σε νέα ερωτήματα είναι συχνά πιο σημαντικές από τις βραχυπρόθεσμες λύσεις, διότι οδηγούν στην πρόοδο και στην κατανόηση των συνεπειών που ενδέχεται να προκύψουν στο μέλλον.

7 Πηγές και Αναφορές

Ahmed Alenezi, H. F. A. G. B. W., 2019. Experts reviews of a cloud forensic readiness framework for organizations. *Journal of cloud computing.*

Akuthota, A., 2025. Role-Based Access Control (RBAC) in Modern Cloud Security Governance: An In-depth Analysis. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, Τόμος 11, pp. 3297-3311.

Alashjaee, A., 2024. *Toward a Conflict Resolution Protocol for*, s.l.: s.n.

Aleke, N. &. T. M., 2025. Legal and Ethical Challenges in Digital Forensics Investigations.

Allahrakha, N., 2024. *Demystifying the Network and Cloud Forensics Legal, Ethical, and Practical Considerations.* s.l.:s.n.

Al-mugern, R., Othman, S. H., Al-Dhaqm, A. & Ali, A., 2024. *A Cloud Forensics Framework to Identify, Gather, and Analyze Cloud Computing Incidents.* s.l.:Engineering, Technology & Applied Science Research.

Alshabibi, M. M., Bu dookhi, A. K. & Hafizur Rahman, M. M., 2024. *Forensic Investigation, Challenges, and Issues of Cloud Data: A Systematic Literature Review.* s.l.:Multidisciplinary Digital Publishing Institute (MDPI).

Apogee, 2024. *The birth of the cloud.* [Ηλεκτρονικό] Available at: https://apogeecorp.com/insights/the-birth-of-the-cloud/

Arel, R., 2022. *Distributed File System.* [Ηλεκτρονικό].

Arthur, B. Q. a. C., 2011. *PlayStation Network hackers access data of 77 million users.* [Ηλεκτρονικό] Available at: https://www.theguardian.com/technology/2011/apr/26/playstation-network-hackers-data

Association of Chief Police Officers, 2012. *ACPO Good Practice Guide ACPO Good Practice Guide*, s.l.: s.n.

Astrafy, 2024. *Google Cloud logging: Complete guide on usage and pricing optimization.* [Ηλεκτρονικό] Available at: https://astrafy.io/the-hub/blog/technical/google-cloud-logging-complete-guide-on-usage-and-pricing-optimization

Atlam Hany, E. N. ,. A. M. L. H., 2024. Blockchain Forensics: A Systematic Literature Review of Techniques, Applications, Challenges, and Future Directions. *Electronics 2024.*

Autopsy, 2025. *Autopsy.* [Ηλεκτρονικό] Available at: https://www.autopsy.com/

AWS, 2024. *What is Amazon CloudWatch Logs?.* [Ηλεκτρονικό] Available at: https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/WhatIsCloudWatchLogs.html

AWS, 2025. *Amazon CloudWatch Logs policies.* [Ηλεκτρονικό] Available at: https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/WhatIsCloudWatchLogs.html

AWS, 2025. *Amazon Macie Documentation.* [Ηλεκτρονικό] Available at: https://docs.aws.amazon.com/macie/

AWS, 2025. *Centralized Logging with OpenSearch.* [Ηλεκτρονικό] Available at: https://docs.aws.amazon.com/solutions/latest/centralized-logging-with-opensearch/supported-log-formats-and-log-sources.html

AWS, 2025. *Cloudtrail/.* [Ηλεκτρονικό] Available at: https://docs.aws.amazon.com/cloudtrail/

AWS, 2025. *Encrypting Data-at-Rest and Data-in-Transit.* [Ηλεκτρονικό] Available at: https://docs.aws.amazon.com/whitepapers/latest/logical-separation/encrypting-data-at-rest-and--in-transit.html

AWS, 2025. *Identify appropriate log retention.* [Ηλεκτρονικό] Available at: https://docs.aws.amazon.com/security-ir/latest/userguide/identify-appropriate-log-retention.html

Aws, 2025. *Supported log formats and log sources.* [Ηλεκτρονικό] Available at: https://docs.aws.amazon.com/solutions/latest/centralized-logging-with-opensearch/supported-log-formats-and-log-sources.html

Aws, 2025. *What is edge computing?.* [Ηλεκτρονικό] Available at: https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-edge-computing

Bacon, M., 2017. *AWS S3 bucket leak exposes millions of Verizon customers' data.* [Ηλεκτρονικό] Available at: https://www.techtarget.com/searchsecurity/news/450422709/Misconfigured-AWS-S3-bucket-exposes-millions-of-Verizon-customers-data

Badman, A., 2024. *IBM Digital Forensics.* [Ηλεκτρονικό] Available at: https://www.ibm.com/think/topics/digital-forensics

BBC, 2016. *Dropbox hack 'affected 68 million users'.* [Ηλεκτρονικό] Available at: https://www.bbc.com/news/technology-37232635

Brook, C., 2018. *SaaS: Single Tenant vs Multi-Tenant.* [Ηλεκτρονικό] Available at: https://www.digitalguardian.com/blog/saas-single-tenant-vs-multi-tenant-whats-difference

Casino, F. και συν., 2022. *Research Trends, Challenges, and Emerging Topics in Digital Forensics: A Review of Reviews.* s.l.:Institute of Electrical and Electronics Engineers Inc..

Castagna, R., 2024. *SAN vs. NAS vs. DAS: Key differences and best use cases.* [Ηλεκτρονικό].

Cellebrite, 2025. *Cellebrite.* [Ηλεκτρονικό] Available at: https://cellebrite.com/en/home/

Chain, 2024. *How to Strengthen Your Cloud Security with Blockchain Technology.* [Ηλεκτρονικό] Available at: https://medium.com/%40chaincom/how-to-strengthen-your-cloud-security-with-blockchain-technology-fff4bd4438c5

Chukwuemeka Nwachukwu, K. D.-T. C. A.-U., 2024. AI-driven anomaly detection in cloud computing environments. *International Journal of Science and Research Archive,* p. 692–710.

CII, 2021. *General Principles for Digital Evidence,* s.l.: s.n.

CISecurity, 2024. *CIS Benchmarks List.* [Ηλεκτρονικό] Available at: https://www.cisecurity.org/cis-benchmarks

CivicEye, 2025. *The Power of Metadata.* [Ηλεκτρονικό] Available at: https://www.civiceye.com/metadata-in-digital-evidence-corroboration/

Cloud Native , 2022. *Cloud Native Glossary - Abstraction.* [Ηλεκτρονικό] Available at: https://glossary.cncf.io/abstraction/

Cloud Security Alliance, 2017. *Cloud Security Alliance Releases Updates to 'The Treacherous 12: Cloud Computing Top Threats in 2016'.* [Ηλεκτρονικό] Available at: https://cloudsecurityalliance.org/press-releases/2017/10/20/cloud-security-alliance-releases-updates-treacherous-12-cloud-computing-top-threats-2016

CloudFlare, 2025. *Why use serverless computing? | Pros and cons of serverless.* [Ηλεκτρονικό] Available at: https://www.cloudflare.com/learning/serverless/why-use-serverless/

Cooperation, E. U. A. f. C. J., 2022. *The CLOUD act.* [Ηλεκτρονικό] Available at: https://www.eurojust.europa.eu/publication/cloud-act

CSA, 2024. *Cloud Controls Matrix.* [Ηλεκτρονικό] Available at: https://cloudsecurityalliance.org/research/cloud-controls-matrix

CSA, 2025. *CSA Security Guidance for Critical Areas of Focus in Cloud Computing.* [Ηλεκτρονικό] Available at: https://cloudsecurityalliance.org/research/guidance/

Cybersecurity Insiders, 2024. *Cloud Security*, s.l.: s.n.

Daskal, J., 2018. *Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0.* [Ηλεκτρονικό] Available at: https://www.stanfordlawreview.org/online/microsoft-ireland-cloud-act-international-lawmaking-2-0/

Datadog, 2025. *Datadog Platform.* [Ηλεκτρονικό] Available at: https://www.datadoghq.com/

DataScienceTest, 2023. *Understanding Google Cloud Platform Buckets: Their Purpose and Functionality.* [Ηλεκτρονικό]
Available at: https://datascientest.com/en/understanding-google-cloud-platform-buckets-their-purpose-and-functionality

Djalovic, N., 2025. *What Is Metadata? Types of Metadata and Its Role in Compliance and Investigations.* [Ηλεκτρονικό]
Available at: https://jatheon.com/blog/what-is-metadata

Dodd, A., 2024. *R.I.P. - ACPO Guidelines and Hello to the FSR Code of Practice.* [Ηλεκτρονικό] Available at: https://www.linkedin.com/pulse/rip-acpo-guidelines-hello-fsr-code-practice-andrew-dodd-msc-fciis-styhe/

EclipseForensics, 2024. *Understanding the Chain of Custody.* [Ηλεκτρονικό] Available at: https://eclipseforensics.com/the-chain-of-custody-maintaining-evidence-integrity-in-digital-forensics

ECPI, 2024. *A brief history of cloud computing.* [Ηλεκτρονικό] Available at: https://www.ecpi.edu/blog/a-brief-history-of-cloud-computing#:~:text=The%20Time%2DSharing%20Theory,upwards%20of%20several%20million%20dollars

Egho-Promise, E., Idahosa, S., Asante, G. & Okungbowa, A., 2024. *Digital Forensic Investigation Standards in Cloud Computing.* s.l.:Science Publications (SCIPUB).

EU, 2016. *General Data Protection Regulation*, https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng: s.n.

European Parliament, 2016. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data*, https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng: s.n.

Exterro, 2025. *FTK Forensic Toolkit.* [Ηλεκτρονικό] Available at: https://www.exterro.com/digital-forensics-software/forensic-toolkit

FedRAMP.gov, 2024. *FedRAMP.* [Ηλεκτρονικό] Available at: https://www.gsa.gov/technology/government-it-initiatives/fedramp

Flores, N., 2023. *Who Owns the Information Stored in the Cloud?.* [Ηλεκτρονικό] Available at: https://verpex.com/blog/cloud-hosting/who-owns-the-information-stored-in-the-cloud

Flores, N., 2023. *Who Owns the Information Stored in the Cloud?.* [Ηλεκτρονικό] Available at: https://verpex.com/blog/cloud-hosting/who-owns-the-information-stored-in-the-cloud

Google cloud , 2024. *What is Cloud Storage.* [Ηλεκτρονικό] Available at: https://cloud.google.com/learn/what-is-cloud-storage?hl=en#:~:text=wherever%20they%20reside.-,Types%20of%20Cloud%20Storage,-Cloud%20Storage%20comes

Google, 2021. *Colossus under the hood.* [Ηλεκτρονικό] Available at: https://cloud.google.com/blog/products/storage-data-transfer/a-peek-behind-colossus-googles-file-system

Google, 2024. *Cloud Audit logs overview.* [Ηλεκτρονικό] Available at: https://cloud.google.com/logging/docs/audit

Google, 2024. *Cloud Data Loss Prevention.* [Ηλεκτρονικό] Available at: https://cloud.google.com/security/products/dlp?hl=en

Google, 2024. *Cloud Logging documentation.* [Ηλεκτρονικό] Available at: https://cloud.google.com/logging/docs

Google, 2024. *Google Security Operations.* [Ηλεκτρονικό] Available at: https://cloud.google.com/chronicle/docs

Google, 2025. *Audit logging.* [Ηλεκτρονικό] Available at: https://developers.google.com/workspace/cloud-search/docs/guides/audit-logging-manual

Google, 2025. *Google cloud quotas and limits.* [Ηλεκτρονικό] Available at: https://cloud.google.com/logging/quotas

Gratton, P., 2025. *10 Ways Cybercrime Impacts Business.* [Ηλεκτρονικό] Available at: https://www.investopedia.com/financial-edge/0112/3-ways-cyber-crime-impacts-business.aspx

HackTheBox, 2023. *5 anti-forensics techniques to trick investigators.* [Ηλεκτρονικό] Available at: https://www.hackthebox.com/blog/anti-forensics-techniques

Hall, C., 2024. *The Challenges of Chain of Custody in the Cloud.* [Ηλεκτρονικό] Available at: https://www.cadosecurity.com/blog/chain-of-custody-in-the-cloud

Harris, C., 2025. *50 Cloud Security Stats You Should Know In 2025.* [Ηλεκτρονικό] Available at: https://expertinsights.com/cloud-infrastructure/50-cloud-security-stats-you-should-know

HASSAN, M., 2023. *J. C. R. Licklider and the Birth of Cloud Computing: How His Vision Changed the World.* [Ηλεκτρονικό]

Available at: https://www.linkedin.com/pulse/j-c-r-licklider-birth-cloud-computing-how-his-vision-changed-a/

Health and Human services, 2003. *Summary of the HIPAA Privacy Rule.* [Ηλεκτρονικό] Available at: https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html

Horton, V., 2024. *Anti-Forensics: What it is, Examples and How to Defend Against it.* [Ηλεκτρονικό] Available at: https://www.itgovernance.eu/blog/en/anti-forensics-what-it-is-examples-and-how-to-defend-against-it

Hulme, G., 2025. *Verkada Surveillance Hack, Breach Highlights IoT Risks.* [Ηλεκτρονικό] Available at: https://securityboulevard.com/2021/03/verkada-surveillance-hack-breach-highlights-iot-risks/

Hungwe, T. & Venter, H., 2024. *An AI Model for Digital Forensic Readiness in the Cloud Using Secure Access Service Edge,* s.l.: s.n.

IBM, 2021. *What are Iaas, Paas and Saas?.* [Ηλεκτρονικό] Available at: https://www.ibm.com/think/topics/iaas-paas-saas

Ibm, 2023. *What is the IoT?.* [Ηλεκτρονικό] Available at: https://www.ibm.com/think/topics/internet-of-things

IEEE, 2014. Impact of memory intensive applications on performance of cloud virtual machine. *Recent Advances in Engineering and Computational Sciences (RAECS).*

Infosec, 2019. *Computer forensics: Network forensics analysis and examination steps.* [Ηλεκτρονικό] Available at: https://www.infosecinstitute.com/resources/digital-forensics/computer-forensics-network-forensics-analysis-examination-steps

Iorga, M. και συν., 2024. *NIST cloud computing forensic reference architecture,* s.l.: s.n.

Iso.org, 2012. *ISO/IEC 27037:2012.* [Ηλεκτρονικό] Available at: https://www.iso.org/standard/44381.html

Iso, 2015. *ISO/IEC 27043:2015 - Security techniques — Incident investigation principles and processes,* s.l.: s.n.

Kapko, M., 2023. *LastPass breach timeline:.* [Ηλεκτρονικό] Available at: https://www.cybersecuritydive.com/news/lastpass-cyberattack-timeline/643958/

Karagiannis, C. & Vergidis, K., 2021. *Digital evidence and cloud forensics: Contemporary legal challenges and the power of disposal.* s.l.:MDPI AG.

Kavanagh, S., 2021. *Forensic investigation environment strategies in the AWS Cloud.* [Ηλεκτρονικό] Available at: https://aws.amazon.com/blogs/security/forensic-investigation-environment-strategies-in-the-aws-cloud

Kävrestad, J., Birath, M. & Clarke, N., 2024. *Fundamentals of Digital Forensics.* Cham: Springer International Publishing.

Keyun Ruan, J. C. T. K. ,. M. C., 2011. Cloud Forensics. Στο: *IFIP Advances in Information and Communication Technology.* s.l.:s.n., pp. 35-46.

Khan, S., 2022. A Systematic Analysis of the Capital One Data Breach: Critical Lessons Learned. *ACM Transactions on Privacy and Security.*

Lakshmanan, R., 2021. *New Azure AD Bug Lets Hackers Brute-Force Passwords Without Getting Caught.* [Ηλεκτρονικό]
Available at: https://thehackernews.com/2021/09/new-azure-ad-bug-lets-hackers-brute.html

Lawspot, 2001. *Σύμβαση της Βουδαπέστης για το έγκλημα στον Κυβερνοχώρο.* [Ηλεκτρονικό] Available at: https://www.lawspot.gr/nomikes-plirofories/nomothesia/n-4411-2016/symvasi-tis-voydapestis-gia-egklima-ston-kyvernohoro-0

Londa, P., 2022. *AWS CloudWatch: Set Retention Periods for Log Groups.* [Ηλεκτρονικό] Available at: https://www.blinkops.com/blog/cloudwatch-retention

Magnet Forensics, 2025. *Magnet Axiom.* [Ηλεκτρονικό] Available at: https://www.magnetforensics.com/products/magnet-axiom/

Malik, A. W. και συν., 2024. *Cloud Digital Forensics: Beyond Tools, Techniques, and Challenges.* s.l.:Multidisciplinary Digital Publishing Institute (MDPI).

Manoj, S. K. A. & Bhaskari, D. L., 2016. *Cloud Forensics-A Framework for Investigating Cyber Attacks in Cloud Environment.* s.l.:Elsevier B.V..

Martin Herman, M. H., 2024. *Martin Herman Michaela Iorga Ahsen Michael Salim Robert H. Jackson Mark R. Hurst Ross A. Leo Anand Kumar Mishra Nancy M. Landreville Yien Wang,* s.l.: s.n.

Mathew, A., 2024. *https://www.isaca.org/resources/news-and-trends/industry-news/2024/cloud-data-sovereignty-governance-and-risk-implications-of-cross-border-cloud-storage.* [Ηλεκτρονικό] Available at: https://www.isaca.org/resources/news-and-trends/industry-news/2024/cloud-data-sovereignty-governance-and-risk-implications-of-cross-border-cloud-storage

Mazur, B., 2025. *Edge computing in IoT: A game-changer for product performance.* [Ηλεκτρονικό] Available at: https://www.ignitec.com/insights/edge-computing-in-iot-a-game-changer-for-product-performance/

Microsoft, 2024. *Manage data retention in a Log Analytics workspace.* [Ηλεκτρονικό] Available at: https://learn.microsoft.com/en-us/azure/azure-monitor/logs/data-retention-configure

Microsoft, 2024. *Manage data retention in a Log Analytics workspace.* [Ηλεκτρονικό] Available at: https://learn.microsoft.com/en-us/azure/azure-monitor/logs/data-retention-configure

Microsoft, 2025. *Azure monitor.* [Ηλεκτρονικό] Available at: https://learn.microsoft.com/en-us/azure/azure-monitor/

Microsoft, 2025. *Azure Monitor Logs overview.* [Ηλεκτρονικό] Available at: https://learn.microsoft.com/en-us/azure/azure-monitor/logs/data-platform-logs

Microsoft, 2025. *What is the cloud.* [Ηλεκτρονικό] Available at: https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-the-cloud [Πρόσβαση 2025].

Moffitt, J., 2024. *Real-Time Anomaly Detection.* [Ηλεκτρονικό] Available at: https://www.tinybird.co/blog-posts/real-time-anomaly-detection

Montini, H., 2025. *Why is metadata important for digital forensic.* [Ηλεκτρονικό] Available at: https://www.provendata.com/blog/what-is-metadata-forensics

MS Nashua, 2025. Ethical Considerations in Digital Forensic. *IJIRMPS,* 13(1).

Narasimhan, P., 2024. Ensuring the Integrity of Digital Evidence: The Role of the Chain of Custody in Digital Forensics. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, pp. 2438-2450.

Nelufule, N., Masango, M. & Singano, T., 2024. *The Future of Digital Forensic Investigations: Keeping the Pace with Technological Advancements.* s.l.:Institute of Electrical and Electronics Engineers Inc..

NIST Glossary, 2024. *NIST Glossary - Chain of custody.* [Ηλεκτρονικό] Available at: https://csrc.nist.gov/glossary/term/chain_of_custody

NIST, 2006. *NIST SP 800-86 Guide to Integrating Forensic Techniques into Incident Response,* s.l.: s.n.

NIST, 2006. *NIST SP 800-92 Guide to Computer Security Log Management,* s.l.: s.n.

NIST, 2014. *NIST SP 800-101 Rev.1 - Guidelines on Mobile Device Forensics,* s.l.: s.n.

NIST, 2024. *NIST Cloud Computing Forensic Reference Architecture,* s.l.: s.n.

Obbayi, L., 2019. *Computer forensics: Chain of custody.* [Ηλεκτρονικό] Available at: https://www.infosecinstitute.com/resources/digital-forensics/computer-forensics-chain-custody/

Okta, 2024. *RBAC vs. ABAC: Definitions & When to Use.* [Ηλεκτρονικό] Available at: https://www.okta.com/identity-101/role-based-access-control-vs-attribute-based-access-control/#:~:text=The%20main%20difference%20between%20RBAC,%2C%20action%20types%2C%20and%20more.

OnTrack, 2022. *Where on earth is cloud data actually located.* [Ηλεκτρονικό] Available at: https://www.ontrack.com/en-ca/blog/where-on-earth-is-cloud-data-actually-stored

Permify, 2024. *ABAC vs RBAC: Exploring Strengths and Weaknesses.* [Ηλεκτρονικό] Available at: https://permify.co/post/abac-vs-rbac/

Peterson, G. & Shenoi, S., 2023. *Advances in Digital Forensics XIX*. 1 επιμ. s.l.:Springer Cham.

Pichan, A. A., 2022. *Digital Forensics Investigation Frameworks for Cloud Computing and Internet of Things,* s.l.: s.n.

Pollitt, M., 2004. *A Framework for Digital Forensic Science,* s.l.: s.n.

Pourvahab, M., 2019. Digital forensics Architecture for Evidense collection and provenance preservation in IaaS Cloud Environment using SDN and Blockchain technology. *IEEEAccess*, Τόμος 7.

Prakash, V. και συν., 2021. *Cloud and edge computing-based computer forensics: Challenges and open problems.* s.l.:MDPI AG.

Purestorage, 2024. *Blob Storage vs. File Storage.* [Ηλεκτρονικό] Available at: https://blog.purestorage.com/purely-educational/blob-storage-vs-file-storage/

Purnaye, P. & Kulkarni, V., 2022. *A Comprehensive Study of Cloud Forensics.* s.l.:Springer Science and Business Media B.V..

QA.com, 2023. *Disadvantages of cloud computing explained.* [Ηλεκτρονικό] Available at: https://www.qa.com/resources/blog/disadvantages-of-cloud-computing/

Reggiani, M., 2016. *A brief introduction to Forensic Readiness.* [Ηλεκτρονικό] Available at: https://www.infosecinstitute.com/resources/digital-forensics/a-brief-introduction-to-forensic-readiness/

Rowlingson, R., 2004. A Ten Step Process for Forensic Readiness. *International Journal of Digital Evidence* .

Sardinas, M. H. M. I. A. M. S. R. H. J. M. R. H. R. L. R. L. N. M. L. A. K. M. Y. W. R., 2020. *NIST Cloud Computing Forensic Science Challenges,* s.l.: s.n.

Satvik Gurjar, D. N. A. S., 2023. Anti-Forensic Techniques and Its Impact on Digital Forensic. *International Research Journal of Engineering and Technology (IRJET)* .

Science, M., 2024. *What is Blockchain Forensics? An In-Depth Guide.* [Ηλεκτρονικό] Available at: https://www.merklescience.com/blog/what-is-blockchain-forensics-an-in-depth-guide

SentinelOne, 2025. *17 Security Risks of Cloud Computing in 2025.* [Ηλεκτρονικό] Available at: https://www.sentinelone.com/cybersecurity-101/cloud-security/security-risks-of-cloud-computing/

Shadawck, 2022. *Awesome-anti-forensic.* [Ηλεκτρονικό] Available at: https://github.com/shadawck/awesome-anti-forensic

Simou, S., Kalloniatis, C., Gritzalis, S. & Katos, V., 2019. *A framework for designing cloud forensic-enabled services (CFeS).* s.l.:Springer London.

Simou, S. και συν., 2022. *Revised forensic framework validation and cloud forensic readiness.* s.l.:Inderscience Publishers.

SisaInfosec, 2024. *Forensic Readiness: A Crucial Element of Cybersecurity.* [Ηλεκτρονικό] Available at: https://www.sisainfosec.com/blogs/forensic-readiness-a-crucial-element-of-cybersecurity/

Sowmya T., M. A. E., 2023. A comprehensive review of AI based intrusion detection system. *Measurement: Sensors,* p. 100827.

Statista, 2025. *Internet of Things (IoT) total annual revenue worldwide from 2020 to 2033.* [Ηλεκτρονικό] Available at: https://www.statista.com/statistics/1194709/iot-revenue-worldwide/

Stoykova, R., 2021. Digital evidence: Unaddressed threats to fairness and the presumption of innocence. *Computer Law & Security Review,* Τόμος 42, p. 105575.

Suleman, S., 2025. *Chain of Custody for Digital Evidence: Importance, Best Practices, and How to Maintain It.* [Ηλεκτρονικό] Available at: https://vidizmo.ai/blog/chain-of-custody-for-digital-evidence

Swgde, 2025. *Swgde Documents published complete listing/.* [Ηλεκτρονικό] Available at: https://www.swgde.org/documents/published-complete-listing/

Tan, J., 2001. *Forensic Readiness.* s.l.:s.n.

Team, S., 2025. *Microsoft Data Breaches: Timeline & Security Lessons.* [Ηλεκτρονικό] Available at: https://www.strongdm.com/what-is/microsoft-data-breaches

TrueScreen, 2025. *Digital evidence and its admissibility:.* [Ηλεκτρονικό] Available at: https://truescreen.io/admissibility-of-digital-evidence/

U.S. Department of Justice, 2018. *CLOUD Act Resources,* s.l.: s.n.

Uber, N., 2017. *2016 Data Security Incident.* [Ηλεκτρονικό] Available at: https://www.uber.com/en-BG/newsroom/2016-data-incident/

Venter, R. K. a. H., 2024. *A Federated Distributed Digital Forensic Readiness Model for the Cloud.* s.l., s.n.

Vivek, V., 2022. *CLOUD STORAGE ARCHITECTURE.* [Ηλεκτρονικό] Available at: https://medium.com/%40vikashvivek/cloud-storage-architecture-d98bea3645b9

Waters, J., 2024. *Docker's 2024 State of Application Development Report Highlights Key Trends for Developers.* [Ηλεκτρονικό] Available at: https://adtmag.com/Articles/2024/06/12/Docker-2024-State-of-AppDev-Report.aspx

Wedad Alawad, a. A. B., 2021. Forensic-Enabled Security as a Service. *ISC Int'l Journal of Information Security*, pp. 49-57.

Weir, G. R. S. & Aßmuth, A., 2024. *Strategies for Intrusion Monitoring in Cloud Services.* s.l.:s.n.

Willson, D., 2013. *Expert Reference Series of White Papers - Legal Issues of Cloud Forensics*, s.l.: s.n.

X-Ways, 2015. *X-Ways Forensics: Integrated Computer Forensics Software.* [Ηλεκτρονικό] Available at: https://www.x-ways.net/forensics/

Yang, W. a. J. M. N. a. S. L. F. a. W. S., 2020. *Security and Forensics in the Internet of Things: Research Advances and Challenges.* Sydney, NSW, Australia, s.n.

Yıldırım, O., 2023. EtrusChain:File Storage with DNA and.

Yodha, C., 2023. *Top 10 Best cloud Forensics Tool.* [Ηλεκτρονικό] Available at: https://www.cyberyodha.org/2023/01/top-10-best-cloud-forensics-tool.html

Ziv, G. B., 2024. *Emerging Trends and Technologies in Digital Forensics Investigations.* [Ηλεκτρονικό] Available at: https://www.cognyte.com/blog/digital-forensics-investigations/

Edgedelta, 2024. *Top Cloud Security Statistics in 2025.* [Ηλεκτρονικό] Available at: https://edgedelta.com/company/blog/cloud-security-statistics

IBM, 2025. *QRadar on Cloud overview.* [Ηλεκτρονικό] Available at: https://www.ibm.com/docs/en/qradar-on-cloud?topic=started-qradar-cloud-overview