ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ

Πρόγραμμα Μεταπτυχιακών Σπουδών
Επιστήμη και Τεχνολογία της Πληροφορικής και των Υπολογιστών

Ειδίκευση Δικτύων Επικοινωνιών και Κατανεμημένων Συστημάτων

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Κυβερνοέγκλημα Σε Περιβάλλοντα Υπολογιστικού Νέφους Κρίσιμων Υποδομών

Ανάργυρος Βελέντζας
Α.Μ. 18027

Εισηγητής: Δημήτριος Καλλέργης, Λέκτορας

ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ

Πρόγραμμα Μεταπτυχιακών Σπουδών
Επιστήμη και Τεχνολογία της Πληροφορικής και των Υπολογιστών

Ειδίκευση Δικτύων Επικοινωνιών και Κατανεμημένων Συστημάτων

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Κυβερνοέγκλημα Σε Περιβάλλοντα Υπολογιστικού Νέφους Κρίσιμων Υποδομών

Ανάργυρος Βελέντζας
Α.Μ. 18027

Τριμελής εξεταστική επιτροπή

Digitally signed by Dimitrios Kallergis
Date: 2021.02.26 22:07:29 +02'00'

1. **<u>Επιβλέπων καθηγητής</u>: Δημήτριος Καλλέργης**, Λέκτορας Πανεπιστημίου Δυτικής Αττικής

2. **<u>Μέλος</u>: Αντώνης Μπόγρης**, Καθηγητής Πανεπιστημίου Δυτικής Αττικής

3. **<u>Μέλος</u>: Ιωάννα Καντζάβελου**, Επίκουρη Καθηγήτρια Πανεπιστημίου Δυτικής Αττικής

Αθήνα, Φεβρουάριος 2021

Δήλωση περί μη λογοκλοπής

Δηλώνω ότι είμαι ο συγγραφέας της παρούσας εργασίας με τίτλο:

«**Κυβερνοέγκλημα Σε Περιβάλλοντα Υπολογιστικού Νέφους Κρίσιμων Υποδομών**»

και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της, είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, οι όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε ακριβώς, είτε παραφρασμένες, αναφέρονται στο σύνολό τους, με πλήρη αναφορά στους συγγραφείς, τον εκδοτικό οίκο ή το περιοδικό, συμπεριλαμβανομένων και των πηγών που ενδεχομένως χρησιμοποιήθηκαν από το διαδίκτυο. Επίσης, βεβαιώνω ότι αυτή η εργασία έχει συγγραφεί από εμένα αποκλειστικά και αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο δικής μου, όσο και του Ιδρύματος.

Παράβαση της ανωτέρω ακαδημαϊκής μου ευθύνης αποτελεί ουσιώδη λόγο για την ανάκληση του πτυχίου μου.

Επιθυμώ την απαγόρευση πρόσβασης στο πλήρες κείμενο της εργασίας μου μέχρι 1.1.2026 και έπειτα από αίτηση μου στη Βιβλιοθήκη και έγκριση του επιβλέποντα καθηγητή.

Ο Δηλών

Ανάργυρος Βελέντζας

Αριθμός Μητρώου : 18027

Ημερομηνία : Φεβρουάριος 2021

Digitally signed by Dimitrios Kallergis
Date: 2021.02.26 22:03:14 +02'00'

Περίληψη

Η ψηφιακή εγκληματολογία (computer forensic science), είναι κλάδος της επιστήμης της πληροφορικής που ασχολείται με την αναγνώριση, διατήρηση, ανάλυση και παρουσίαση ψηφιακών αποδείξεων και τεκμηρίων, για εγκλήματα σε υπολογιστές ή ακόμη και σε κινητά τηλέφωνα. Ωστόσο, η εμφάνιση και αυξανομένη χρήση της υπολογιστικής νέφους σε σχέση με τις έως τώρα διαδεδομένες μορφές τεχνολογιών πληροφορικής και επικοινωνιών, επιφέρει σημαντικές διαφοροποιήσεις στην ψηφιακή εγκληματολογία. Οι διαφοροποιήσεις αυτές δημιουργούν νέες προκλήσεις στον τομέα της διερεύνησης του κυβερνοεγκλήματος. Ως εκ τούτου, μια νέα ερευνητική περιοχή αναδεικνύεται σε αυτόν τον τομέα, δηλαδή η εγκληματολογία υπολογιστικής νέφους (cloud forensics). Εντωμεταξύ, οι υποδομές ζωτικής σημασίας κρατών και οργανισμών κρατών, όπως - μεταξύ άλλων - η υγεία, η άμυνα και η οικονομία, επεκτείνονται όλο και πιο πολύ στην υπολογιστική νέφους. Τούτο καθιστά την ψηφιακή εγκληματολογία ένα σημαντικό εργαλείο για την καταπολέμηση του κυβερνοεγκλήματος και την περαιτέρω αξιοποίηση της υπολογιστικής νέφους από τις υποδομές αυτές.

Μέσα από την εξέταση επιστημονικών δημοσιεύσεων, τεχνικών κειμένων ελληνικής και ξένης βιβλιογραφίας και νομικών κειμένων κρατών και διεθνών οργανισμών, η μελέτη αυτή έρχεται να φωτίσει τις ιδιαίτερες πτυχές του κυβερνοεγκλήματος και της εγκληματολογίας στον χώρο της υπολογιστικής νέφους. Στις σελίδες που ακολουθούν επιχειρείται η κατάδειξη των πρακτικών που προάγουν την προστασία των υποδομών ζωτικής σημασίας και διευκολύνουν τη διεξαγωγή εγκληματολογικών ερευνών στο νέφος. Επιπλέον, η μελέτη αυτή παρουσιάζει προκλήσεις στο αντικείμενο αυτό, ανοιχτά ζητήματα και σημεία που απαιτούν περαιτέρω επεξεργασία από την επιστημονική κοινότητα και τους φορείς που συμμετέχουν σε αυτό το οικοσύστημα (όπως για παράδειγμα πάροχοι υπηρεσιών νέφους, πελάτες, νομοθέτες, διωκτικές αρχές και άλλοι).

Κλείνοντας, παρατίθενται συμπεράσματα ως προς την τρέχουσα κατάσταση και τους μελλοντικούς κινδύνους, καθώς επίσης και προτάσεις που θα μπορούσαν να οδηγήσουν σε βελτιώσεις, τόσο σε τεχνικό επίπεδο όσο και σε θεσμικό.

Abstract

Digital forensics (Computer forensic science) is a branch of digital technology that focuses on recognition, preservation, analysis and presentation of digital evidence for crimes that are committed through the use of computers or even mobile phones. However, the increasing rise in the use of cloud computing, in relation to the widespread forms of information technology, has brought significant changes to digital forensics. These changes create new challenges in the field of cybercrime investigation. Hence, a new area of research is emerging in this field, namely cloud forensics. Meanwhile, critical infrastructures of states and government agencies, such as, *inter alia*, health, defense and the economy, are increasingly expanding their use of cloud computing. This makes cloud forensics an important tool in the fight against cybercrime so that these infrastructures and government agencies can continue to utilize cloud computing safely and securely.

Through the examination of scientific publications, technical texts of Greek and foreign bibliography, legal texts of local governments and international organizations, this study aims to shed a light on numerous aspects of cybercrime and forensics in the field of cloud computing. In the research that follows, an attempt is made to demonstrate the practices that initially promote the protection of critical infrastructures and, in turn, help facilitate forensic investigations of the cloud. In addition, this study highlights issues that will require further research by the scientific community and stakeholders of this ecosystem, such as cloud service providers, customers, legislators, law enforcement agencies and several others.

Finally, this study presents conclusions regarding the current situation and the future risks, as well as proposals that could lead to improvements, both within a technical, as well as within a regulatory framework.

Ευχαριστίες

Θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή μου, κύριο Δημήτριο Καλλέργη, για την καθοδήγηση και την υποστήριξη κατά την εκπόνηση της παρούσας εργασίας.

Πίνακας Περιεχομένων

Κατάλογος Εικόνων

Κατάλογος Πινάκων

Κατάλογος συντομογραφιών

ADF	Access Data Forensic
APT	Advanced Peristent Threat
BIRR	Better Infrastructure Risk and Resilience
BlockSLaaS	Blockchain-assisted Secure Logging-as-a-Service
BMI	Protection of Critical Infrastructures - Baseline Protection Concept
CERT	Computer Emergency Response Team
CI	Critical Infrastruture
CIMS	Critical Infrastructure Modelling Simulation
CISA	Cybersecurity and Infrastructure Security Agency
CJIS	Criminal Justice Information Services
CLASS	Cloud Log Assuring Soundness and Secrecy
CMMC	Cybersecurity Maturity Model Certification
CoC	Chain of Custody
CSP	Cloud Service Provider
DEFT	Digital Evidence & Forensics Toolkit
DEM	Digital Evidence Management
DFaaS	Digital-Forensics-as-a-Service
GDPR	General Data Protection Regulation
HIPAA	Health Insurance Portability and Accountability Act
ICS	Industrial Control Systems
IDS	Intrusion Detection System
KMS	Key Management Service
LEIP	Law Enforcement Investigative Platform
MLAT	Mutual Legal Assistance Treaty
NSRAM	Network Security Risk Assessment Modelling
OECD	Organisation for Economic Co-operation and Development
POR	Proof of Retrievability
RVA	Risk and Vulnerability Analysis
SCADA	Supervisory Control and Data Acquisition
SLA	Service License Agreement
TPM	Trust Model Platform
ΥΖΣ	Υποδομές Ζωτικής Σημασίας

Κεφάλαιο 1 - Εισαγωγή

1.1 Πρόλογος

Η υπολογιστική νέφους (cloud computing) εμφανίστηκε για πρώτη φορά στα μέσα της δεκαετίας του 2000 και ως σήμερα καταλαμβάνει όλο και πιο πολύ χώρο στον κλάδο της πληροφορικής διεθνώς. Η εξέλιξη αυτή οφείλεται στα ιδιαίτερα χαρακτηριστικά της, που δίνουν λύση στις σύγχρονες ανάγκες επιχειρήσεων, κυβερνήσεων, επιστημονικών φορέων, ακόμα και απλών φυσικών προσώπων. Παράλληλα όμως με την ραγδαία εμπορική εξάπλωση της υπολογιστικής νέφους, αναπτύχθηκε αντιστοίχως και το έγκλημα στο οικοσύστημα αυτό.

Στην παρούσα εργασία διερευνάται η ψηφιακή εγκληματολογία για το κυβερνοέγκλημα στον χώρο της υπολογιστικής νέφους. Δίδεται ιδιαίτερη έμφαση στις υποδομές ζωτικής σημασίας που λειτουργούν στο νέφος ή συνεργάζονται με αυτό ή εξαρτώνται από αυτό.

Οι γεωγραφικές περιοχές που εξετάζονται είναι οι Ηνωμένες Πολιτείες Αμερικής (ΗΠΑ), η Ευρωπαϊκή Ένωση (ΕΕ) και η Ρωσία. Αντιστοίχως, οι υποδομές ζωτικής σημασίας που εξετάζονται για κάθε μια από τις τρεις αυτές περιοχές, είναι η άμυνα, η οικονομία και η υγεία.

Ειδικότερα τα τελευταία χρόνια, η προτίμηση στις υπηρεσίες υπολογιστικής νέφους έχει σχεδόν περάσει από το στάδιο της τάσης στο στάδιο της εμμονής. Τούτο όμως συμβαίνει με άγνοια και περιφρόνηση προς τον παράγοντα της εγκληματολογικής έρευνας στο νέφος, όπως θα καταδειχθεί στις σελίδες που ακολουθούν. Παρά τα βήματα που έχουν γίνει, εξακολουθούν να υπάρχουν σοβαρά ζητήματα στην εγκληματολογία στο νέφος. Για παράδειγμα, τα συμφωνητικά παροχής υπηρεσιών νέφους σπανίως περιέχουν ειδικές προβλέψεις για τις εγκληματολογικές έρευνες, οι ανά τον κόσμο διωκτικές αρχές συνήθως δεν έχουν αρκετά καλή συνεργασία για τον εντοπισμό και τη δίωξη κακοποιών κυβερνοεγκλήματος, το νομικό πλαίσιο είναι δαιδαλώδες προκαλώντας προβλήματα περί του εφαρμοστέου δικαίου, και πολλά άλλα. Όλα αυτά διαμορφώνουν ένα περιβάλλον που μοιάζει ιδανικό για τους κακοποιούς και εξαιρετικά δυσχερές για τις διωκτικές αρχές και τους ερευνητές εγκληματολογίας στο νέφος.

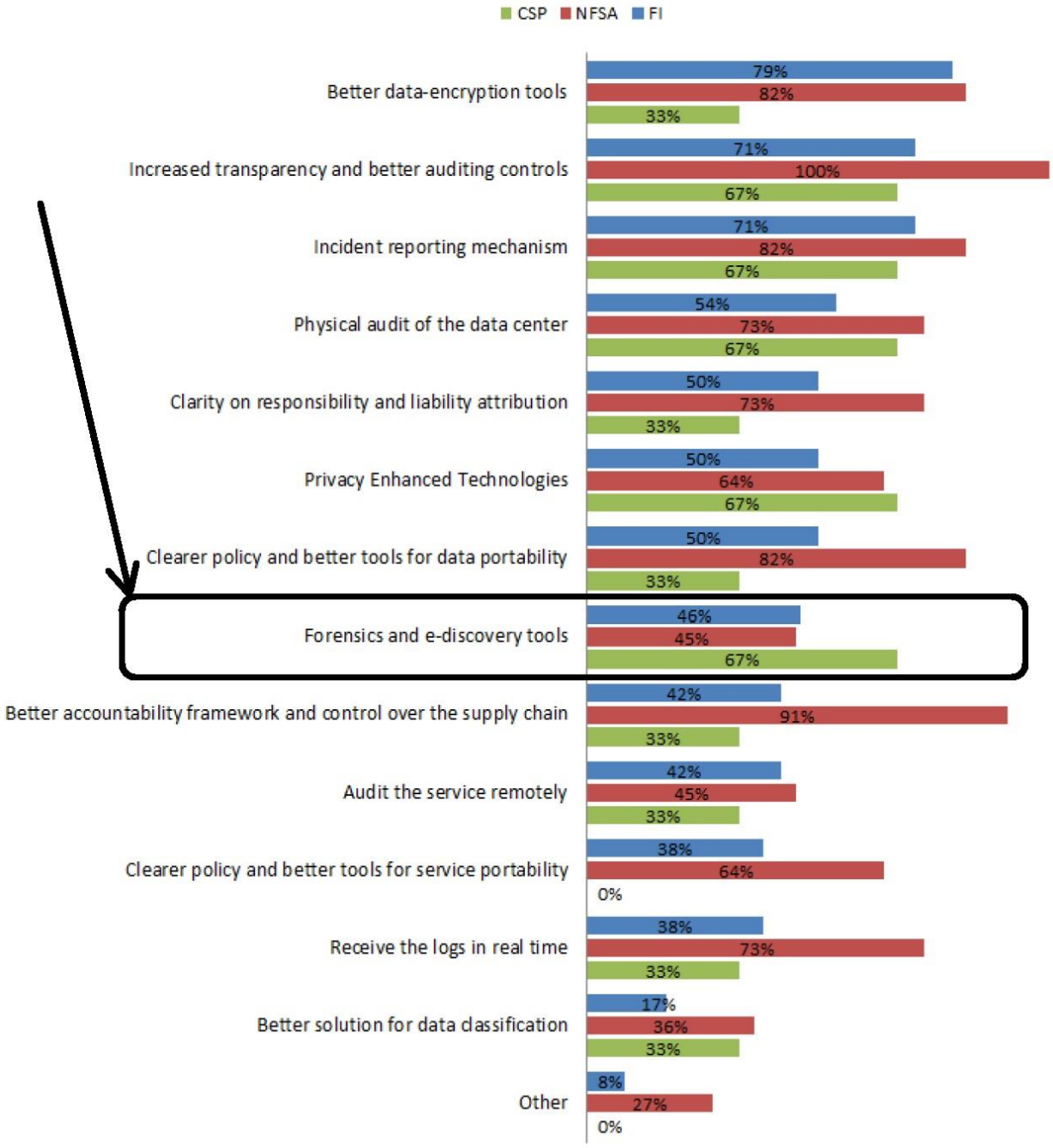
Τα ζητήματα αυτά, όσο δεν διευθετούνται, δημιουργούν σοβαρούς κινδύνους και στις υποδομές ζωτικής σημασίας που λειτουργούν στο νέφος (ή συνεργάζονται με αυτό ή εξαρτώνται από αυτό). Αυτές οι υποδομές έχουν συνήθως αυξημένες απαιτήσεις για την

προστασία τους και ενίοτε, βαριές επιπτώσεις σε περίπτωση ζημιάς ή δυσλειτουργίας. Συγκεκριμένα παραδείγματα που θα παρατεθούν, δείχνουν τι μπορεί να συμβεί όταν προκαλούνται κυβερνοεπιθέσεις σε υποδομές ζωτικής σημασίας που λειτουργούν στο νέφος και τι επιπτώσεις μπορεί να υπάρξουν για τη λειτουργία μιας ολόκληρης χώρας. Και όσον αφορά το σκέλος των εγκληματολογικών ερευνών, η πρόοδος που διαπιστώνεται, ιδίως στα θεσμικά ζητήματα, είναι μάλλον μικρή. Τούτο είναι κάτι που ίσως πρέπει να αλλάξει, ώστε να αποτραπούν χειρότερες εξελίξεις στον χώρο του κυβερνοεγκλήματος μελλοντικά.

Στο τέλος της μελέτης διεξάγεται γενική αποτίμηση της κατάστασης, παρουσιάζονται προκλήσεις και ανοιχτά ζητήματα σε αυτό το αντικείμενο, παρατίθενται προτάσεις για την επίλυση προβλημάτων που διαπιστώθηκαν και προτείνονται περιοχές για περαιτέρω διερεύνηση.

Η Εικόνα 1.1 είναι ενδεικτική της αδιαφορίας που επικρατεί προς το παρόν για τα ζητήματα εγκληματολογικών ερευνών στην υπολογιστική νέφους. Πρόκειται για ένα γράφημα του Ευρωπαϊκού Οργανισμού Κυβερνοασφάλειας [1] που απεικονίζει λειτουργίες κυβερνοασφάλειας, τις οποίες που επιθυμούν περισσότερο οι πελάτες υπολογιστικής νέφους και απαιτούν πιο συχνά από τους παρόχους (Cloud Service Providers / CSPs). Στην προκειμένη περίπτωση, οι πελάτες είναι χρηματοπιστωτικά ιδρύματα (Financial Institutes / FIs) στην Ευρωπαϊκή Ένωση. Από το γράφημα προκύπτει ότι, οι Εθνικές Αρχές Χρηματοπιστωτικής Εποπτείας (National Financial Supervisory Authorities / NFSAs) των κρατών μελών της ΕΕ – σημείωση: λόγου χάρη, για την Ελλάδα εποπτική αρχή των τραπεζών είναι η Τράπεζα της Ελλάδος - ενδιαφέρονται λιγότερο από τα ίδια τα χρηματοπιστωτικά ιδρύματα (FIs) για τα ζητήματα εγκληματολογικών ερευνών στην υπολογιστική νέφους. Ίσως οι μέχρι σήμερα εξελιχθείσες κυβερνοεπιθέσεις σε αυτόν τον κλάδο (οικονομία) και σε αυτόν τον χώρο (Ευρωπαϊκή Ένωση) δεν είχαν αρκετά βαριές επιπτώσεις, ώστε να αναζητηθούν μέχρι τέλους οι υπαίτιοι και να οδηγηθούν στη δικαιοσύνη.

Η παρούσα μελέτη φιλοδοξεί να συμβάλλει στην ανάδειξη της ψηφιακής εγκληματολογίας νέφους ως ένα αποτελεσματικό παράγοντα προστασίας και αποτροπής του κυβερνοεγκλήματος.



Εικόνα 1.1. Λειτουργίες κυβερνοασφάλειας νέφους που επιθυμούν περισσότερο φορείς χρηματοπιστωτικών υπηρεσιών στην Ευρωπαϊκή Ένωση [1]

1.2 Σκοπός και Αντικείμενο Μελέτης

Σκοπός αυτής της μελέτης είναι να παρουσιάσει και να συνοψίσει τις λύσεις που προτείνονται σε τεχνικό και θεσμικό επίπεδο για την έγκαιρη, αποτελεσματική και νομικά ορθή διεκπεραίωση των διαδικασιών ψηφιακής εγκληματολογίας, αλλά και το πώς οι λύσεις αυτές συνάδουν με το θεσμικό πλαίσιο και τις απαιτήσεις συγκεκριμένων γεωγραφικών περιοχών σε σχέση με την προστασία συγκεκριμένων υποδομών ζωτικής σημασίας. Συνάμα, επιδιώκεται η κατάδειξη α) εκείνων των πρακτικών που διευκολύνουν τη διεξαγωγή εγκληματολογικών ερευνών στο νέφος, β) των προκλήσεων αυτού του χώρου, και γ) όλων εκείνων των σημείων που απαιτούν περαιτέρω επεξεργασία από την επιστημονική κοινότητα και τους διάφορους φορείς συμμετοχής (πχ πάροχοι, πελάτες, διωκτικές αρχές).

Το αντικείμενο της μελέτης είναι η ανάλυση των ιδιαιτεροτήτων του κυβερνοεγκλήματος στον χώρο της υπολογιστικής νέφους ως προς το σκέλος της εγκληματολογίας. Όμως λόγω της ιδιαίτερης βαρύτητας που έχουν οι υποδομές ζωτικής σημασίας για την λειτουργία των κρατών και την εξασφάλιση της ομαλότητας στην καθημερινότητα των πολιτών ανά τον κόσμο, δίδεται έμφαση στο κυβερνοέγκλημα και στην εγκληματολογία που αφορά τις υποδομές ζωτικής σημασίας οι οποίες λειτουργούν στο νέφος ή συνεργάζονται με αυτό ή εξαρτώνται από αυτό.

1.3 Δομή Μεταπτυχιακής Εργασίας

Αυτή η μελέτη ασχολείται με τον κοινό τόπο τριών διαφορετικών επιστημονικών τομέων: α) την υπολογιστική νέφους (cloud), β) την εγκληματολογία (forensics), και γ) τις υποδομές ζωτικής σημασίας (critical infrastructures). Στα κεφάλαια που ακολουθούν διεξάγεται εξέταση καθενός από αυτούς τους τομείς και η σύνδεση μεταξύ τους.

- Στο **1ο κεφάλαιο** αναφέρονται το πλαίσιο και οι ερευνητικοί στόχοι της εργασίας.
- Στο **2ο κεφάλαιο** εξετάζεται το κυβερνοέγκλημα στο νέφος, με έμφαση στην ψηφιακή εγκληματολογία. Σε τούτο το κεφάλαιο καταδεικνύονται οι διαφορές ανάμεσα στην παραδοσιακή ψηφιακή εγκληματολογία και την εγκληματολογία νέφους, τα βήματα της ψηφιακής εγκληματολογίας και οι αντίστοιχες προσεγγίσεις για την εγκληματολογία νέφους, το λογισμικό και οι προτεινόμενες πρακτικές των μεγαλύτερων παγκοσμίως παρόχων υπολογιστικής νέφους.

- Στο **3ο κεφάλαιο** εξετάζονται οι υποδομές ζωτικής σημασίας και οι λεπτομέρειες της διεξαγωγής εγκληματολογικών ερευνών σε αυτές. Αρχικά αποδίδεται η έννοια του όρου «υποδομές ζωτικής σημασίας», στη συνέχεια παρουσιάζονται μέθοδοι προσδιορισμού της βαρύτητας της κάθε υποδομής και τέλος καταδεικνύεται το πώς οι μέθοδοι αυτοί συμβάλλουν στην προστασία των υποδομών αυτών, διευκολύνοντας παράλληλα και την διεξαγωγή εγκληματολογικών ερευνών.
- Το **4ο κεφάλαιο** εστιάζει στην εγκληματολογική έρευνα για υποδομές ζωτικής σημασίας που λειτουργούν στο νέφος ή συνεργάζονται με αυτό ή εξαρτώνται από αυτό. Αρχικά διερευνώνται περιπτώσεις χρήσης και βέλτιστες πρακτικές εγκληματολογικής έρευνας (πάντα για συστήματα που λειτουργούν στο νέφος) και κατόπιν διεξάγεται αξιολόγηση συστημάτων υποδομών ζωτικής σημασίας, από πλευράς υποστήριξης της εγκληματολογικής έρευνας.
- Στο **5ο κεφάλαιο** παρατίθενται περιπτώσεις επιθέσεων σε υποδομές ζωτικής σημασίας στο νέφος και αναλύονται, τόσο από πλευράς εγκληματολογίας όσο και από πλευράς επιπτώσεων που προκλήθηκαν. Από τα περιστατικά αυτά προκύπτουν ενδιαφέροντα συμπεράσματα αναφορικά με την τρέχουσα κατάσταση και τους μελλοντικούς κινδύνους.
- Στο **6ο κεφάλαιο** διεξάγεται διερεύνηση των δυνατοτήτων στο σκέλος της πρόληψης και της αντιμετώπισης (από πλευράς εγκληματολογικής έρευνας) των περιστατικών ασφαλείας στο νέφος. Οι δυνατότητες αυτές συνοψίζονται από τις επισημάνσεις προηγούμενων σημείων της μελέτης αλλά και από σχετική λίστα του Ευρωπαϊκού Οργανισμού Κυβερνοασφάλειας (ENISA).
- Στο **7ο κεφάλαιο** παρουσιάζονται οι προκλήσεις που ανακύπτουν από αυτή τη μελέτη καθώς επίσης και τα ανοιχτά ζητήματα.
- Στο **8ο κεφάλαιο** αναδεικνύονται τα συμπεράσματα που ανακύπτουν από τη μελέτη αυτή και παρατίθενται λίστες προτάσεων για την προαγωγή της κυβερνοασφάλειας στο νέφος –ιδίως για τα συστήματα υποδομών ζωτικής σημασίας– αλλά και τη διευκόλυνση της εγκληματολογικής έρευνας σε αυτό. Συγκεκριμένα παρατίθεται μια λίστα προτάσεων για τεχνικά ζητήματα και μια αντίστοιχη για θεσμικά ζητήματα.

Κεφάλαιο 2 - Κυβερνοέγκλημα και Ψηφιακή Εγκληματολογία στο νέφος

2.1 Μεθοδολογία

Πολλές επιστημονικές μελέτες έχουν ασχοληθεί με το ζήτημα της εγκληματολογίας στον χώρο της υπολογιστικής νέφους (cloud forensics), καταγράφοντας τις ιδιαίτερες προκλήσεις που αυτή παρουσιάζει, αλλά και τις διαφορές σε σχέση με την παραδοσιακή εγκληματολογία. Η μεθοδολογία που ακολουθείται στη συνέχεια της παρούσας μελέτης έχει ως ακολούθως:

- Προσδιορισμός της σύγχρονης μορφής του κυβερνοεγκλήματος και επισκόπηση λύσεων που προτείνονται για την αποτελεσματική διενέργεια εγκληματολογικών ερευνών.
- Διερεύνηση των γενικών αρχών της ψηφιακής Εγκληματολογίας (digital forensics), μέσα από την παρουσίαση επιστημονικών μελετών που συνοψίζουν τις ακολουθούμενες πρακτικές, την ανάδειξη των βασικών βημάτων εγκληματολογικής έρευνας και την προβολή περιοχών που χρειάζονται περαιτέρω έρευνα.
- Τέλος, αποπειράται μια ενδεικτική επισκόπηση του τρόπου με τον οποίο προσεγγίζουν την ψηφιακή εγκληματολογία οι πολύ μεγάλοι πάροχοι υπηρεσιών νέφους. Στο σημείο αυτό παρατίθενται οι λειτουργικές δυνατότητες που έχουν προβλέψει οι πάροχοι για τη διενέργεια εγκληματολογικών ερευνών εντός τους δικού τους νέφους αλλά και οι εφαρμογές εγκληματολογικής διερεύνησης που προσφέρουν στους πελάτες τους ως λογισμικό προς εκμίσθωση (Software-as-a-Service).

2.2 Κυβερνοέγκλημα και Εγκληματολογική Έρευνα

Η σύγχρονη μορφή του κυβερνοεγκλήματος δεν αφορά μόνο τη χρήση υπολογιστών αλλά και διαφόρων άλλων συσκευών που συνδέονται με το διαδίκτυο, συμπεριλαμβανομένων φυσικά των κινητών τηλεφώνων. Οι Asmita Roy, Sadip Midya, Koushik Majumder και Santanu Phadikar [2] παρουσιάζουν μια πρόταση για την καταπολέμηση του κυβερνοεγκλήματος στο χώρο του διαδικτύου και της κινητής τηλεφωνίας. Η πρότασή τους βασίζεται στην προσέγγιση Forensics-As-A-Service και, ως εκ τούτου, αποτελεί χρήσιμο παράδειγμα καταστολής του κυβερνοεγκλήματος μέσω της ψηφιακής εγκληματολογίας στον χώρο της υπολογιστικής νέφους. Οι Cheng-Ta Huang, Hung-Jui Ko, Zhi-Wei Zhuang,

Ping-Cheng Shih και Shiuh-Jeng WANG [3] μελετούν το κυβερνοέγκλημα, ειδικά στο πεδίο των υπηρεσιών παροχής αποθηκευτικού χώρου στο νέφος (cloud storage) και χρησιμοποιούν έξυπνες συσκευές με λειτουργικό σύστημα iOS για να επαναφέρουν ψηφιακά τεκμήρια που είχαν προηγουμένως διαγραφεί από τις εμπλεκόμενες συσκευές. Ειδικό ενδιαφέρον έχει η επισήμανση των παραπάνω ερευνητών ότι το πλήθος των εγκλημάτων στο χώρο του διαδικτύου μέσω της κινητής τηλεφωνίας είναι τέτοιος, που οι ανά τον κόσμο διωκτικές αρχές έχουν ήδη έρθει αντιμέτωπες με καθυστερούμενο απόθεμα υποθέσεων (backlog) με ισχυρό κίνδυνο το απόθεμα αυτό να αυξηθεί, αντί να μειωθεί στο μέλλον.

Σε μια άλλη μελέτη, αυτή των Áine MacDermott, Thar Baker και Qi Shi [4], η οποία αφορά το κυβερνοέγκλημα στον χώρο του Διαδικτύου των Αντικειμένων (Internet of Things / IoT), γίνεται χρήση συνδυασμού υπηρεσιών εγκληματολογίας του νέφους (cloud forensics) και λογισμικού εγκληματολογίας εγκατεστημένου τοπικά στις συσκευές IoT, για την αποτελεσματική διεξαγωγή ερευνών εγκληματολογίας και την αντιμετώπιση σχετικών προκλήσεων.

2.3 Ψηφιακή Εγκληματολογία

Μια μελέτη που επισημαίνει τον ολοένα και αυξανόμενο αριθμό υποθέσεων ψηφιακής εγκληματικότητας είναι εκείνη των Reza Montasari και Richard Hill [5]. Σε αυτή τη μελέτη παρουσιάζονται οι πιο δύσκολες τεχνικές προκλήσεις που πρέπει να αντιμετωπίσουν οι ανά τον κόσμο διωκτικές αρχές και οι οποίες έχουν να κάνουν – ανάμεσα σε άλλα - με τα ετερογενή περιβάλλοντα υλικού (hardware) και λογισμικού (software), την εμφάνιση ολοένα και καινούργιων συστημάτων διαχείρισης αρχείων (file systems), την τάση των κατασκευαστών έξυπνων κινητών τηλεφώνων (smartphones) να κρυπτογραφούν όλο και περισσότερες λειτουργίες των συσκευών, αλλά και την εμφάνιση ενός φαινομένου, που θα μπορούσε να ονομαστεί ως «Έγκλημα ως υπηρεσία» (Crime-as-a-Service), σύμφωνα με το οποίο, οι επιτιθέμενοι μπορούν να βρουν εύκολα στο νέφος τα εργαλεία εκείνα που χρειάζονται για να πραγματοποιήσουν τις επιθέσεις τους. Στη μελέτη αυτή προτείνονται συγκεκριμένες περιοχές για περαιτέρω ανάπτυξη, όπως η διασύνδεση των διωκτικών αρχών σε παγκόσμιο επίπεδο.

2.3.1 Η εγκληματολογία υπολογιστών και η εγκληματολογία τηλεπικοινωνιακών δικτύων

Σε έρευνα των Ray Hunt και Jill Slay [6] γίνεται αναφορά σε δυο έννοιες που αφορούν την ψηφιακή εγκληματολογία και δεν είναι ταυτόσημες: η εγκληματολογία υπολογιστών και η

εγκληματολογία τηλεπικοινωνιακών δικτύων. Ορισμένες από τις διαφορές αυτές, σύμφωνα με τη συγκεκριμένη μελέτη, είναι οι ακόλουθες:

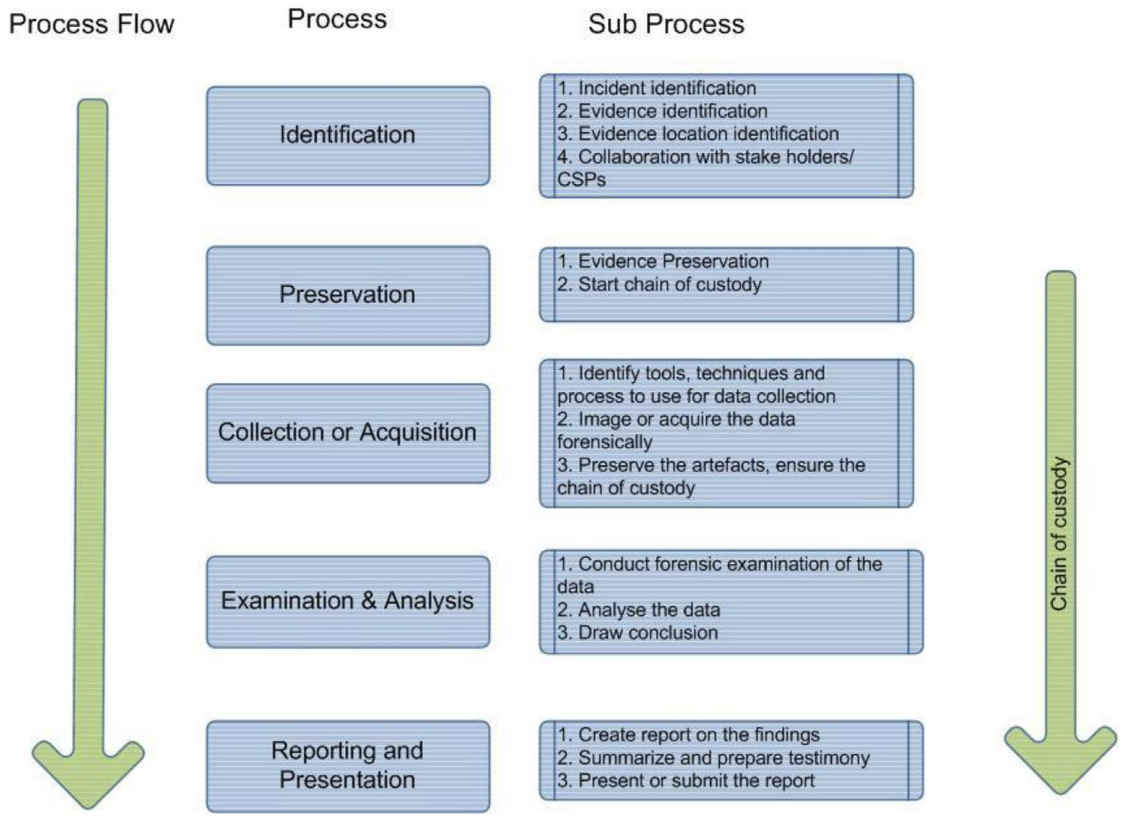
- Η εγκληματολογία υπολογιστών διεξάγεται κατά κανόνα από διωκτικές αρχές για την εξιχνίαση και τεκμηρίωση εγκληματικών ενεργειών, ενώ η εγκληματολογία τηλεπικοινωνιακών δικτύων αναπτύχθηκε για σκοπούς αυτόματης ανταπάντησης στις ενέργειες των hackers και αφορά κυρίως αρχιτεκτονικές και συσκευές δικτυακής ασφάλειας (πχ firewalls, κλπ).
- Στην εγκληματολογία υπολογιστών ο ερευνητής έχει συνήθως μεγαλύτερη τεχνική επάρκεια (στο αντικείμενο της εγκληματολογίας) από ό,τι ο επιτιθέμενος, ενώ στην εγκληματολογία τηλεπικοινωνιακών δικτύων ο ερευνητής και ο επιτιθέμενος έχουν συνήθως τις ίδιες τεχνικές δεξιότητες και χρησιμοποιούν τα ίδια ακριβώς εργαλεία.
- Στην εγκληματολογία υπολογιστών διεξάγεται διερεύνηση με τρόπο που καλείται να οδηγήσει στην εξιχνίαση μιας υπόθεσης και στην τεκμηρίωσή της ενώπιον των δικαστικών αρχών, ενώ στην εγκληματολογία τηλεπικοινωνιακών δικτύων δεν υπάρχει αντικείμενο προς έρευνα αλλά ανάγκη προστασίας των υποδομών.
- Τα εργαλεία είναι διαφορετικά: στη μεν εγκληματολογία υπολογιστών χρησιμοποιούνται εξειδικευμένες για τον σκοπό αυτό εφαρμογές, όπως το EnCase, το FTK και το DEFT (Digital Evidence & Forensics Toolkit), στη δε εγκληματολογία τηλεπικοινωνιακών δικτύων, τόσο ο ερευνητής όσο και ο επιτιθέμενος χρησιμοποιούν ευρείας χρήσης εφαρμογές, όπως για παράδειγμα το Wireshark, το TCPDump, το NetScanTools Pro, κλπ.
- Η εγκληματολογία υπολογιστών αφορά την κατάσχεση και τη διερεύνηση μη-προσωρινών αντικειμένων, όπως για παράδειγμα λέξεις-κλειδιά και αρχεία εικόνων (πχ jpeg), ενώ η εγκληματολογία τηλεπικοινωνιακών δικτύων έγκειται στην επεξεργασία προσωρινών πληροφοριών, οι οποίες μάλιστα για να συλλεχθούν, θα πρέπει να έχει προηγηθεί η αντίστοιχη μέριμνα (όπως για παράδειγμα η ενεργοποίηση μηχανισμών καταγραφής τηλεπικοινωνιακών πακέτων).

2.3.2 Τα βήματα της ψηφιακής εγκληματολογίας

Εκτεταμένη επισκόπηση του χώρου της ψηφιακής εγκληματολογίας διεξάγουν και οι Ameer Pichan, Mihai Lazarescu και Sie Teng Soh [7], οι οποίοι παραθέτουν αναλυτικά τα βήματα της έρευνας στην ψηφιακή εγκληματολογία, προβαίνοντας κατόπιν στην αντιπαραβολή των βημάτων αυτών με τις ειδικές προκλήσεις που αφορούν την εγκληματολογία υπολογιστικής

νέφους. Σύμφωνα με την μελέτη τους, τα βήματα της ψηφιακής εγκληματολογίας είναι τα ακόλουθα:

1. **Ταυτοποίηση (Identification)**. Αφορά την ταυτοποίηση του περιστατικού ασφάλειας, την ταυτοποίηση των εμπλεκόμενων τεκμηρίων, την ταυτοποίηση της θέσης στην οποία βρίσκονται αυτά τα τεκμήρια, τη συνεργασία με τους εμπλεκόμενους φορείς (εν προκειμένω τους παρόχους υπηρεσιών νέφους).
2. **Διατήρηση.** Αφορά τη μέριμνα για την διατήρηση των τεκμηρίων στην αρχική τους μορφή (δηλαδή τη μέριμνα για τη μη αλλοίωση των τεκμηρίων) και την έναρξη της καταγραφής της αλυσίδας των γεγονότων (Chain of Custody).
3. **Συλλογή ή Συγχώνευση.** Αφορά την ταυτοποίηση των εργαλείων, των τεχνικών και των διαδικασιών που θα χρησιμοποιηθούν κατά τη συλλογή των δεδομένων, τη καταγραφή του στιγμιότυπου στο οποίο βρίσκονται τα τεκμήρια και την προστασία των σημαντικών στοιχείων που συνθέτουν την αλυσίδα των γεγονότων.
4. **Διερεύνηση και Ανάλυση.** Αφορά τη διενέργεια της εγκληματολογικής έρευνας επί των συλλεχθέντων πληροφοριών, την ανάλυσή τους και τη διαμόρφωση συμπεράσματος.
5. **Αναφορά και Παρουσίαση.** Αφορά τη δημιουργία αναφοράς των ευρημάτων, τη σύνοψη και την προετοιμασία της μαρτυρικής κατάθεσης ενώπιον των ανακριτικών αρχών και την παρουσίαση (ή υποβολή) της αναφοράς στις αρμόδιες αρχές.



Εικόνα 2.1. Τα στάδια της Ψηφιακής Εγκληματολογίας [7]

Τόσο σε αυτή την μελέτη, όσο και σε πολλές άλλες, διαπιστώνεται συχνή επίκληση του Οδηγού Βέλτιστων Πρακτικών στην Ψηφιακή Εγκληματολογία της Ένωσης Αξιωματικών Αστυνομίας του Ηνωμένου Βασιλείου (ACPO)[1], αλλά και του -αντίστοιχου περιεχομένου- Οδηγού για την Ενσωμάτωση των Εγκληματολογικών Τεχνικών στην Αντιμετώπιση Περιστατικών του Αμερικανικού Εθνικού Οργανισμού Προτύπων και Τεχνολογίας (NIST) [8]. Επισημαίνεται ότι τα δυο τελευταία κείμενα αποτελούν τους πιο διαδεδομένους οδηγούς στο χώρο της ψηφιακής εγκληματολογίας.

2.3.3 Προτεινόμενες λύσεις στη διεξαγωγή ερευνών εγκληματολογίας στο νέφος

Στο επίπεδο των εφαρμογών και των συστημάτων, εξετάζονται δυο ολοκληρωμένες λύσεις λογισμικού διεξαγωγής εγκληματολογίας στο νέφος.

Η πρώτη λύση είναι το σύστημα των Shumian Yang, Lianhai Wang, Dawei Zhao, Guangqi Liu και Shuhui Zhang [9]. Αυτό αποτελείται από 3 μέρη: remote control side, server side και client side. Διεξάγει συλλογή στοιχείων και ανάλυση κατά τον παραδοσιακό τρόπο και έχει δοκιμαστεί σε Windows 10 (client) και Centos 7.0 (server). Είναι ένα σύγχρονο λογισμικό το οποίο παρουσιάζει καλά αποτελέσματα.

[1] Association of Chief Police Officers, 2012. ACPO Good Practice Guide for Digital Evidence

Η δεύτερη λύση είναι το σύστημα των Michael P . Vega, James Regan, Matteo Michelini και Jean - Francois Legault [10] για λογαριασμό του αμερικανικού χρηματοπιστωτικού ιδρύματος JP Morgan Chase Bank, N.A. Ένα μέρος αυτού του συστήματος αφορά την χρήση υποδομής IaaS για την λειτουργία εργαλείων και διεργασιών συλλογής στοιχείων, με τρόπο αποδοτικό και αξιόπιστο. Ένα άλλο μέρος αφορά την αναδρομική διερεύνηση στιγμιότυπων εικονικών μηχανών (VM instances), ακόμα και αν αυτά έχουν τερματιστεί από καιρό. Η προσέγγιση αυτή παρέχει σε οργανισμούς τη δυνατότητα να διεξάγουν εγκληματολογικές έρευνες τόσο για δημόσια όσο και για ιδιωτικά περιβάλλοντα.

2.3.4 Οι προσεγγίσεις των μεγάλων παρόχων νέφους στο ζήτημα της εγκληματολογικής έρευνας

Μεγάλο μέρος της εγκληματικής δραστηριότητας στο νέφος διεξάγεται μέσω των νεφοϋπολογιστικών υποδομών ή σε βάρος των υποδομών αυτών. Για τον λόγο αυτό, έχει εξαιρετικό ενδιαφέρον το πώς αυτοί οι μεγάλοι παίκτες αντιμετωπίζουν το ζήτημα της εγκληματολογίας. Στην ακόλουθη επισκόπηση, εξετάζεται το γενικό πλαίσιο ασφάλειας του κάθε παρόχου υπηρεσιών νέφους μέσα από έναν πίνακα. Ο πίνακας αυτός περιέχει ενδεικτικές πληροφορίες που προέρχονται από τους ιστότοπους των παρόχων και απευθύνονται στο ευρύ κοινό. Δεν περιλαμβάνονται πληροφορίες που παρέχονται από τις υποστηρικτικές τους υπηρεσίες στους επί πληρωμή πελάτες τους.

Πίνακας 2.1. Βασικές δυνατότητες για εγκληματολογική έρευνα που παρέχουν οι μεγάλοι πάροχοι νέφους

Α/Α	Όνομα Παρόχου	Εργαλεία για διεξαγωγή εγκληματο-λογικών ερευνών	Διασύνδεση με κρατικές υπηρεσίες / διωκτικές αρχές	Εργαλεία επιμέλειας αλυσίδας (Chain of Custody)	Εργαλεία διαχείρισης ανάλυσης logs	Πληροφορίες από τους παρόχους
1	Amazon Web Services (AWS)	-	Μόνο στις ΗΠΑ	-	AWS CloudTrail, AWS CloudWatch, AWS Config, Elastic Load Balancing, VPC Flow Logs	Προτεινόμενη μεθοδολογία εγκληματολογικής διερεύνησης: 1. Ενεργοποίησε AWS CloudTrail για όλους τους γεωγραφικούς τομείς. 2. Προστάτεψε τα logs. 3. Πάρε backup τακτικά & αποθήκευσέ τα αλλού. 4. Διάβασε αμέσως τις ειδοποιήσεις ασφάλειας της AWS. 5. Απομόνωσε τους πόρους που επηρεάζονται από το περιστατικό. 6. Περιόρισε την πρόσβαση μόνο στην ομάδα που διεξάγει τη διερεύνηση.
2	Microsoft Azure	-	Μόνο στις ΗΠΑ	Legal Hold	Autopsy (3rd party), ClearSkies™ SaaS NG SIEM (3rd party), Attivo Networks ThreatDefend Deception (3rd party), Avanan Office 365 Security (3rd party), LogSentinel (3rd party)	Προτεινόμενη μεθοδολογία εγκληματολογικής διερεύνησης: 1. Αντιγραφή του τεκμηρίου (σκληρός δίσκος ή εικονικός υπολογιστής) στο Azure Storage. 2. Ενεργοποίηση της υπηρεσίας Legal Hold. 3. Αποκρυπτογράφηση του σκληρού δίσκου ή/και το κλειδιού με το οποίο έγινε η κρυπτογράφηση. 4. Έρευνα των πληροφοριών και διεξαγωγή της ανάλυσης.
3	Google Cloud	-	-	-	Access Transparency (3rd party), Cloud Audit Logs	Διεξαγωγή εγκληματολογικής έρευνας από διάφορες ομάδες όπως: Εγκληματολογικής έρευνα (Forensics), Διαχείρισης περιστατικών νέφους (Cloud Incident Management), Μηχανικής προϊόντων (Product Engineering), Μηχανική αξιοπιστίας ιστοτόπων (Site reliability engineering), Ασφάλειας και ιδιωτικότητας στο νέφος (Cloud security and privacy), Παγκοσμίων ερευνών (Global investigations), Εντοπισμού σημάτων (Signals detection), Συμβουλευτικής σε θέματα ασφάλειας, ιδιωτικότητας και προϊόντων (Security, privacy, and product counsel), Εμπιστοσύνης και προστασίας (Trust and safety), Τεχνολογίας αντιμετώπισης παρενοχλήσεων (Counter abuse technology), Υποστήριξης πελατών (Customer support).

Α/Α	Όνομα Παρόχου	Εργαλεία για διεξαγωγή εγκληματο-λογικών ερευνών	Διασύνδεση με κρατικές υπηρεσίες / διωκτικές αρχές	Εργαλεία επιμέλειας αλυσίδας (Chain of Custody)	Εργαλεία διαχείρισης ανάλυσης logs	Πληροφορίες από τους παρόχους
4	Alibaba Cloud	-	-	-	ActionTrail, Alibaba Cloud Log Service, Alibaba Cloud Config	Διεξαγωγή εγκληματολογικής έρευνας από το Alibaba Cloud Security Center. Αυτό είναι ένα αυτόματο σύστημα διαχείρισης ασφάλειας που αναγνωρίζει απειλές ασφάλειας, τις αναλύει και αποστέλλει ειδοποιήσεις σε πραγματικό χρόνο. Το σύστημα αυτό αναγνωρίζει αυτόματα την επίθεση, ενημερώνει τους ενδιαφερόμενους για τα βασικά εγκληματολογικά της στοιχεία, όπως η πηγή, ο στόχος και η αιτία της επίθεσης, αλλά προβαίνει επίσης και σε αυτόματα αντίμετρα.
5	IBM Cloud	NAI: L.E.I.P. (Law Enforcement Investigative Platform - μόνο για ΗΠΑ), IBM i2 Enterprise Insight Analysis	NAI (Μόνο στις ΗΠΑ)	IBM Multi-Cloud Encryption (διεξάγει κρυπτογράφηση δεδομένων ακόμα και σε ετερογενή περιβάλλοντα)	- IBM Qradar - IBM X-Force Exchange - IBM Resilient SOAR - IBM i2 Analyst's Notebook - IBM Trusteer - IBM Guardium Analyzer	Η IBM διαθέτει ξεχωριστό σύστημα για τη διεξαγωγή εγκληματολογικών ερευνών, το LEIP / Law Enforcement Investigative Platform. Ακολουθεί ειδική αναφορά σε αυτό.
6	Oracle Cloud	NAI: Oracle DEM (Oracle Digital Evidence Management Solution for Police – μόνο ΗΠΑ & μόνο για φυσικό έγκλημα)	NAI (Μόνο στις ΗΠΑ)	-	Oracle Log Analytics Service	Διεξαγωγή εγκληματολογικής έρευνας από αρμόδια υπηρεσία της Oracle, οι οποία ονομάζεται "Παγκόσμιος Οργανισμός Ασφάλειας της Oracle" (Oracle's Global Information Security Organization / GIS). Η υπηρεσία αυτή ενημερώνεται και επιλαμβάνεται του χειρισμού των περιστατικών, συντονίζοντας τις κατάλληλες ανά τον κόσμο ομάδες και κλιμακώνοντας τις απαιτούμενες ενέργειες, ανάλογα με τη φύση του περιστατικού. Η Oracle διαθέτει ξεχωριστό σύστημα για τη διεξαγωγή εγκληματολογικών ερευνών, το Oracle DEM, αλλά αφορά μόνο το φυσικό έγκλημα. Ακολουθεί σύντομη αναφορά σε αυτό.

Λογισμικό των μεγάλων παρόχων νέφους για διεξαγωγή εγκληματολογικών ερευνών.

Οι μόνοι πάροχοι που διαθέτουν ειδικό λογισμικό για τη διεξαγωγή εγκληματολογικών ερευνών είναι η IBM και η Oracle. Ακολουθεί επισκόπηση αυτών των λύσεων.

IBM Law Enforcement Investigative Platform / LEIP

Η βασική πλατφόρμα που έχει σχεδιάσει η IBM για τη διεξαγωγή εγκληματολογικών ερευνών ονομάζεται "Ερευνητική Πλατφόρμα Επιβολής Νόμου" (Law Enforcement Investigative Platform / LEIP). Το τεχνικό κείμενο με τίτλο «Ακολουθήστε τον χρόνο μέχρι να βρείτε τον στόχο, χρησιμοποιώντας μια λύση συγχώνευσης δεδομένων» (“Drive time to target using a data fusion solution”) [2] παρουσιάζει αναλυτικά την διάρθρωση αυτής της πλατφόρμας και τις δυνατότητές της. Σύμφωνα λοιπόν με αυτό το κείμενο, η πλατφόρμα αυτή χρησιμεύει στη διερεύνηση τόσο του φυσικού, όσο και του ψηφιακού εγκλήματος. Παρόλο που η IBM δεν αποκλείει τη χρήση αυτής της πλατφόρμας από ιδιώτες, κατά βάση προορίζεται για χρήση από κυβερνητικές διωκτικές αρχές, με έμφαση εκείνες των ΗΠΑ.

Η πλατφόρμα αυτή λειτουργεί τόσο στο νέφος, όσο και σε ιδιόκτητες εγκαταστάσεις, είτε με τη μορφή συνδρομής, είτε με τη μορφή αγοράς. Η δυνατότητα λειτουργίας στο νέφος παρέχει όλες εκείνες τις διευκολύνσεις που παρέχονται αξιωματικά από την υπολογιστική νέφους, όπως για παράδειγμα η δυνατότητα άμεσης χρήσης και η δυνατότητα άμεσης κλιμάκωσης ανάλογα με τις ανάγκες (scaling). Αυτό το σύστημα παρέχει δυνατότητα άμεσης διασύνδεσης με βάσεις δεδομένων των διωκτικών αρχών, με πηγές δημοσίων πληροφοριών (πχ μετεωρολογικοί ιστότοποι, συστήματα εντοπισμού γεωγραφικής θέσης, μέσα κοινωνικής δικτύωσης, κλπ), με βάσεις δεδομένων στο νέφος, κα. Η δυνατότητα συσχέτισης και επεξεργασίας όλων αυτών των πληροφορίων του υπό διερεύνηση εγκλήματος (φυσικού ή ψηφιακού) διευκολύνει και επιταχύνει την εγκληματολογική έρευνα. Εκτός αυτού, επειδή διαθέτει μηχανισμούς τεχνητής νοημοσύνης και μηχανικής εκμάθησης, έχει τη δυνατότητα να σχηματίζει πρότυπα εγκληματολογικής συμπεριφοράς, τα οποία χρησιμεύουν κατά τη διερεύνηση ενός εγκλήματος αλλά και στον εντοπισμό παρόμοιων εγκλημάτων στο μέλλον.

Σημειώνεται ότι η δυνατότητα διασύνδεσης με βάσεις δεδομένων διωκτικών αρχών, δεν είναι κάτι που μπορεί να έχει οποιοδήποτε λογισμικό εγκληματολογικής διερεύνησης, αφού οι βάσεις αυτές περιέχουν συνήθως, αν όχι πάντα, διαβαθμισμένες πληροφορίες, ακόμα και απόρρητες. Για παράδειγμα, κάποιες από αυτές τις πηγές πληροφοριών - πάντα

[2] https://www.ibm.com/downloads/cas/7AG71QDN

στον χώρο των ΗΠΑ - είναι το Εθνικό Κέντρο Πληροφοριών Εγκλήματος (National Crime Information Center / NCIC), το Κέντρο Παρακολούθησης Τρομοκρατών (Terrorist Screening Center / TSC), βάσεις καταγραφής ενταλμάτων, και άλλα. Για την επίτευξη αυτού του πολύ σημαντικού σκέλους πληροφόρησης της πλατφόρμας LEIP, η IBM εξασφάλισε τις αντίστοιχες πιστοποιήσεις των αμερικανικών διωκτικών αρχών. Τέτοιες είναι η πιστοποίηση από τον Τομέα Υπηρεσιών Πληροφοριών Ποινικής Δικαιοσύνης (Criminal Justice Information Services Division / CJIS) του Ομοσπονδιακού Γραφείου Ερευνών (Federal Bureau of Investigation / FBI), καθώς επίσης και πιστοποίηση από το Ομοσπονδιακό Πρόγραμμα Διαχείρισης Κινδύνων και Εξουσιοδοτήσεων (Federal Risk and Authorization Management Program / FedRAMP) του Γραφείου Διαχείρισης και Προϋπολογισμού (Office of Management and Budget / OMB) του Προεδρικού Γραφείου των ΗΠΑ.

Με τέτοιες πηγές πληροφοριών είναι προφανές ότι οι δυνατότητες εγκληματολογικής διερεύνησης αυτού του συστήματος, υπερβαίνουν κατά πολύ εκείνες των εφαρμογών Qradar, X-Force Exchange και Resilient SOAR της ίδιας εταιρείας, αφού οι τελευταίες μπορούν να συλλέξουν και να επεξεργαστούν πληροφορίες μόνο από εφαρμογές και συστήματα πληροφορικής. Για παράδειγμα, ένα σύστημα σαν το Qradar μπορεί να καταδείξει την ip διεύθυνση από την οποία εκδηλώθηκε μια επίθεση, όμως η Ερευνητική Πλατφόρμα Επιβολής Νόμου LEIP μπορεί να συσχετίσει την πληροφορία αυτή με άλλες, καταδεικνύοντας - μεταξύ άλλων - τη γεωγραφική θέση από την οποία εκδηλώθηκε η επίθεση, την τοπική ώρα, τις μετεωρολογικές και κλιματολογικές συνθήκες που επικρατούσαν στο συγκεκριμένο σημείο, τυχόν ιστορικό εκδήλωσης και άλλων επιθέσεων από το σημείο αυτό, κλπ.

Ωστόσο, σύμφωνα με τα στοιχεία που παραθέτει η IBM στο διαδίκτυο, αυτή η εξελιγμένη πλατφόρμα δεν φαίνεται να διατίθεται για άλλους χώρους πέραν των ΗΠΑ. Για τον υπόλοιπο πλανήτη, το σύστημα που η εταιρεία αυτή προτείνει είναι το "IBM i2 Enterprise Insight Analysis". Σύμφωνα με το τεχνικό κείμενο της IBM με τίτλο «Διερευνητική ανάλυση στην εφαρμογή του νόμου» (“Investigative Analysis in Law Enforcement”)[3], στο οποίο παρουσιάζεται το σύστημα αυτό, οι δυνατότητες που παρέχει στο αντικείμενο της εγκληματολογικής διερεύνησης, αφορούν την συλλογή πληροφοριών, την επεξεργασία και την ανάλυσή τους σε πραγματικό χρόνο, ακόμα και αν οι πληροφορίες αυτές έχουν πολύ μεγάλο όγκο, όπως εκατοντάδες terabytes. Επίσης διαθέτει δυνατότητες διασύνδεσης και διάθεσης των αναλύσεων αυτών σε τοπικές, εθνικές και διεθνείς διωκτικές αρχές. Το

[3] https://www.ibm.com/downloads/cas/OW3KJN1Y

σύστημα αυτό υποστηρίζει τη διεξαγωγή ψηφιακής εγκληματολογίας στο νέφος αλλά μπορεί να χρησιμεύσει επίσης και στους ακόλουθους τομείς:

- Εγκληματολογία κοινού εγκλήματος
- Ανάλυση εγκλήματος
- Ανάλυση στρατηγικών πληροφοριών
- Αντιμετώπιση τρομοκρατίας
- Διασυνοριακή και τελωνειακή ασφάλεια
- Καταπολέμηση απάτης και οικονομικού εγκλήματος
- Καταπολέμηση παιδοφιλίας
- Εγκληματολογία και παρακολούθηση του οργανωμένου εγκλήματος
- Εγκληματολογία εγκλημάτων μίσους
- Δίωξη ναρκωτικών

Oracle Digital Evidence Management Solution for Police" / Oracle DEM

Η Oracle διαθέτει ένα λογισμικό για την εξυπηρέτηση των αναγκών εγκληματολογικής διερεύνησης, αλλά αυτό αφορά το φυσικό έγκλημα και όχι το ψηφιακό. Ονομάζεται "Λύση Διαχείρισης Ψηφιακών Τεκμηρίων για την Αστυνομία" ("Oracle Digital Evidence Management Solution for Police" / Oracle DEM) και σύμφωνα με το ομώνυμο τεχνικό της εγχειρίδιο[4], χρησιμεύει στη συλλογή, την επεξεργασία και την εμπιστευτική διακίνηση πληροφοριών που προέρχονται από κάμερες παρακολούθησης, τηλεφωνικές κλήσεις, κλπ. Δεν σχετίζεται με εγκληματολογική έρευνα στον χώρο του νέφους.

[4] https://www.oracle.com/assets/ds-digital-evidence-management-3864416.pdf

Κεφάλαιο 3 - Υποδομές Ζωτικής Σημασίας και Εγκληματολογία σε αυτές

3.1 Μεθοδολογία

Στην παρούσα μελέτη εξετάζεται το κυβερνοέγκλημα που λαμβάνει χώρα στο νέφος, με έμφαση εκείνο το σκέλος που αφορά ή επηρεάζει υποδομές ζωτικής σημασίας. Καθώς με την πάροδο του χρόνου, όλο και πιο πολλές υποδομές ζωτικής σημασίας θα λειτουργούν στο νέφος ή θα συνεργάζονται με αυτό ή θα εξαρτώνται από αυτό, κρίνεται σκόπιμο να μελετηθούν τα ιδιαίτερα χαρακτηριστικά των υποδομών ζωτικής σημασίας. Τα χαρακτηριστικά αυτά εξετάζονται σε τούτο το κεφάλαιο. Η μεθοδολογία που ακολουθείται σε αυτό το σημείο της μελέτης έχει ως ακολούθως:

- Προσδιορισμός του όρου **υποδομές ζωτικής σημασίας (ΥΖΣ)** ή **κρίσιμες υποδομές**. Απαραίτητη για την κατανόηση της σπουδαιότητας των υποδομών ζωτικής σημαίας είναι η έννοια που τους δίνουν η επιστημονική κοινότητα, μέσα από τις δημοσιευμένες μελέτες, καθώς επίσης τα κράτη και οι διεθνείς οργανισμοί, μέσα από τα έγγραφά τους. Σε αυτό το σημείο παρατίθεται ενδεικτική τεκμηρίωση των τομέων Άμυνας, Οικονομίας και Υγείας, ως υποδομές ζωτικής σημασίας για τις περιοχές: Ευρωπαϊκή Ένωση, Ρωσία και ΗΠΑ.
- Εξέταση των γενικών θεμάτων εγκληματολογίας στο χώρο των υποδομών ζωτικής σημασίας και επισκόπηση μοντέλων υλοποίησης εγκληματολογικών ερευνών.

3.2 Υποδομές Ζωτικής Σημασίας

Η βιβλιογραφία για τις υποδομές ζωτικής σημασίας περιλαμβάνει **(α)** επιστημονικές μελέτες και **(β)** δημόσια έγγραφα κρατικών οργανισμών που καταδεικνύουν τους τομείς οι οποίοι αποτελούν υποδομές ζωτικής σημασίας.

3.2.1 Επιστημονικές μελέτες

Οι Cristina Alcaraz και Sherali Zeadallly [11] περιγράφουν σημεία για την προστασία των ΥΖΣ στον κυβερνοχώρο (ανάμεσα σε αυτά και η εγκληματολογία), προσδιορίζουν τον όρο ΥΖΣ και παραθέτουν τον αντίστοιχο προσδιορισμό της Ευρωπαϊκής Ένωσης για τον όρο αυτό. Αν και εστιάζουν περισσότερο στα συστήματα βιομηχανικού ελέγχου, κάνουν ειδική και εκτεταμένη αναφορά και στα ζητήματα εγκληματολογίας.

Ξεκινώντας με τον προσδιορισμό του όρου ΥΖΣ, οι Venkata Reddy Palleti, Jude Victor Joseph και Arlindo Silva [12] γράφουν: *«Μια κρίσιμη υποδομή αποτελείται από συστήματα, περιουσιακά στοιχεία και δίκτυα, είτε φυσικά είτε εικονικά και παίζει σημαντικό ρόλο στην οικονομία κάθε έθνους. Οποιαδήποτε διακοπή των κρίσιμων υποδομών επηρεάζει την οικονομία των χωρών, τη δημόσια υγεία, την ασφάλεια ή οποιονδήποτε συνδυασμό αυτών».*

3.2.2 Δημόσια έγγραφα κρατικών οργανισμών

Στη αυτή την κατηγορία της βιβλιογραφίας, καταγράφονται ορισμοί για τις ΥΖΣ που δίνουν η Ευρωπαϊκή Ένωση (ΕΕ), οι ΗΠΑ και η Ρωσία.

Ευρωπαϊκή Ένωση

Ξεκινώντας με την Ευρωπαϊκή Ένωση, η Οδηγία 2008/114/ΕΚ του Συμβουλίου της Ευρωπαϊκής Ένωσης, της 8ης Δεκεμβρίου 2008, σχετικά με τον προσδιορισμό και τον χαρακτηρισμό των ευρωπαϊκών υποδομών ζωτικής σημασίας, και σχετικά με την αξιολόγηση της ανάγκης βελτίωσης της προστασίας τους [13], δίνει τον ακόλουθο ορισμό στο Άρθρο 2: «*ως «υποδομές ζωτικής σημασίας» νοούνται τα περιουσιακά στοιχεία, συστήματα ή μέρη αυτών που βρίσκονται εντός των κρατών μελών και τα οποία είναι ουσιώδη για τη διατήρηση των λειτουργιών ζωτικής σημασίας της κοινωνίας, της υγείας, της ασφάλειας, της οικονομικής και κοινωνικής ευημερίας των μελών της, και των οποίων η διακοπή λειτουργίας ή η καταστροφή θα είχε σημαντικό αντίκτυπο για ένα κράτος μέλος, ως αποτέλεσμα της αδυναμίας διατήρησης των λειτουργιών αυτών*΄». Όμως, καθότι η Ευρωπαϊκή Ένωση είναι οργανισμός πολλών κρατών, το Συμβούλιο της Ευρωπαϊκής Ένωσης δίνει –στην ίδια Οδηγία και στο ίδιο άρθρο– έναν πρόσθετο ορισμό, αυτή τη φορά για τις «ευρωπαϊκές υποδομές ζωτικής σημασίας». Ο ορισμός αυτός έχει ως ακολούθως: «*ως «ευρωπαϊκές υποδομές ζωτικής σημασίας» ή «ΕΥΖΣ» νοούνται οι υποδομές ζωτικής σημασίας που βρίσκονται εντός των κρατών μελών και των οποίων η διακοπή λειτουργίας ή η καταστροφή θα είχε σημαντικό αντίκτυπο σε δύο τουλάχιστον κράτη μέλη. Η σπουδαιότητα των επιπτώσεων εκτιμάται βάσει οριζόντιων κριτηρίων. Συμπεριλαμβάνονται οι επιπτώσεις από οριζόντιες εξαρτήσεις από άλλες κατηγορίες υποδομών*΄». Εδώ, φαίνεται ρητά ότι, για την Ευρωπαϊκή Ένωση, δεν αρκεί η προστασία των υποδομών ζωτικής σημασίας, όπως το κάθε κράτος μέλος ξεχωριστά την προσδιορίζει, αλλά, δεδομένης της αλληλεξάρτησης που έχουν τα κράτη μέλη της ΕΕ μεταξύ τους, απαιτείται η προστασία και εκείνων των υποδομών, που η διακοπή λειτουργίας ή η καταστροφή τους έχει επιπτώσεις σε άλλα κράτη μέλη. Για τον προσδιορισμό της σπουδαιότητας των επιπτώσεων, η εν λόγω

Οδηγία προβλέπει ότι εκτιμάται βάσει οριζόντιων κριτηρίων, ορισμένα εκ των οποίων αναφέρονται στο άρθρο 3, ως ακολούθως:

α) κριτήριο απωλειών (αξιολόγηση ως προς τον πιθανό αριθμό νεκρών ή τραυματιών)·

β) κριτήριο οικονομικών επιπτώσεων (αξιολόγηση ως προς τη σπουδαιότητα της οικονομικής ζημίας και/ή υποβάθμισης προϊόντων ή υπηρεσιών, συμπεριλαμβανομένων των δυνητικών περιβαλλοντικών επιπτώσεων)·

γ) κριτήριο των επιπτώσεων για το κοινό (αξιολόγηση ως προς τις επιπτώσεις για την εμπιστοσύνη του κοινού, τη σωματική οδύνη και τη διατάραξη της καθημερινής ζωής, συμπεριλαμβανομένης της απώλειας υπηρεσιών ζωτικής σημασίας).

Ηνωμένες Πολιτείες Αμερικής

Αναφορικά με τον χώρο των ΗΠΑ, εκτενής αναφορά γίνεται σε Έκθεση της Επιτροπής του Προέδρου (των ΗΠΑ) για την προστασία των ΥΖΣ , η οποία έχει τον τίτλο «Κρίσιμες Δομές – Προστατεύοντας Τις Υποδομές Της Αμερικής» (“Critical Foundations – Protecting America’s Infrastructures”) [14]. Ο ορισμός που δίνεται σε αυτήν την αναφορά είναι ο ακόλουθος: «*Κρίσιμες Υποδομές: Υποδομές που είναι τόσο ζωτικής σημασίας ώστε η εξουδετέρωσή τους ή η καταστροφή τους θα είχαν ολέθριο αντίκτυπο στην άμυνα ή την οικονομική ασφάλεια*».

Ωστόσο στο ίδιο κείμενο, στο πρώτο κεφάλαιο, υπάρχει και η ακόλουθη επεξήγηση: «*Ως υποδομή εννοούμε κάτι περισσότερο από μια συλλογή μεμονωμένων εταιρειών που ασχολούνται με σχετικές δραστηριότητες - εννοούμε ένα δίκτυο ανεξάρτητων, ιδιόκτητων κυρίως, συστημάτων φτιαγμένων από ανθρώπους, και διαδικασιών που λειτουργούν συλλογικά και συνεργικά για να παράγουν και να διανέμουν μια συνεχή ροή βασικών αγαθών και υπηρεσιών*». Η αναφορά «ιδιόκτητων κυρίως, συστημάτων» έχει ξεχωριστή σημασία διότι, εμπλέκει στη διαδικασία προστασίας των υποδομών αυτών τον ιδιωτικό φορέα, αφού οι περισσότερες υποδομές εκεί είναι ιδιόκτητες και όχι δημόσιες. Τούτο γίνεται ακόμα πιο σαφές στη συνοδευτική επιστολή με την οποία υποβάλλεται η αναφορά αυτή προς τον Πρόεδρο των ΗΠΑ, αφού στην τέταρτη παράγραφο αναφέρεται ρητά: «*Επειδή οι υποδομές ανήκουν κυρίως σε ιδιώτες και λειτουργούν υπό την ευθύνη τους, καταλήξαμε στο συμπέρασμα ότι η διασφάλιση των κρίσιμων υποδομών αποτελεί κοινή ευθύνη του δημόσιου και του ιδιωτικού τομέα. Ο μόνος σίγουρος δρόμος για προστατευμένες υποδομές τα επόμενα χρόνια είναι μέσω μιας πραγματικής συνεργασίας μεταξύ ιδιοκτητών και φορέων εκμετάλλευσης υποδομών και της κυβέρνησης.*». Το πρώτο

συμπέρασμα είναι ότι το μοντέλο κοινής ευθύνης συναντάται ευρύτερα στο χώρο των κρίσιμων υποδομών. Το δεύτερο συμπέρασμα από την προσέγγιση αυτή είναι ότι, ενώ οι ΗΠΑ ρητά και ξεκάθαρα κατανέμουν μέρος της ευθύνης προστασίας των κρίσιμων υποδομών στους ιδιώτες, η ΕΕ, μολονότι η διάρθρωση της οικονομίας και της αγοράς της είναι δυτικού (καπιταλιστικού) τύπου, καθιστά μοναδικό υπεύθυνο μόνο τις κυβερνήσεις (τον κρατικό μηχανισμό) των κρατών μελών και δεν υπάρχει αναφορά σε ευθύνες ιδιωτών.

Στην εισαγωγή του ίδιου κειμένου παρατίθενται ευσύνοπτα και ονομαστικά οι τομείς των κρίσιμων υποδομών ως ακολούθως: «*Αυτές οι κρίσιμες υποδομές - ενέργεια, τραπεζικές και χρηματοοικονομικές υπηρεσίες, μεταφορές, υγεία και τηλεπικοινωνίες - πρέπει να εξεταστούν σε ένα νέο πλαίσιο στην εποχή της πληροφορίας*».

Η αναφορά «Κρίσιμες Δομές – Προστατεύοντας Τις Υποδομές Της Αμερικής» (“Critical Foundations – Protecting America’s Infrastructures”) υποβλήθηκε προς τον Πρόεδρο των ΗΠΑ το έτος 1997. Σήμερα, όπως προκύπτει από την ιστοσελίδα του Οργανισμού Κυβερνοασφάλειας και Προστασίας Υποδομών (Cybersecurity and Infrastructure Security Agency - CISA) των ΗΠΑ[5], οι τομείς ζωτικής σημασίας έχουν επεκταθεί σε δεκαέξι (16) και είναι οι ακόλουθοι: οι τηλεπικοινωνίες, τα χημικά, ένα κρίσιμο μέρος του κατασκευαστικού κλάδου, οι εμπορικές υποδομές, η πολεμική βιομηχανία, τα φράγματα, οι υπηρεσίες άμεσης επέμβασης (πχ πυροσβεστική, διακομιδές ασθενών, κλπ), η ενέργεια, η οικονομία, οι κυβερνητικές υποδομές (πχ τα υπουργεία), ο τομέας των τροφίμων και της γεωργίας, ο τομέας των πυρηνικών αντιδραστήρων, η πληροφορική, το νερό, οι μεταφορές και η υγεία.

[5] https://www.cisa.gov/critical-infrastructure-sectors

Εικόνα 3.1. Οι τομείς των κρίσιμων υποδομών των ΗΠΑ (πηγή: www.cisa.gov)

Ρωσία

Αναφορικά με τον χώρο της Ρωσίας, πρέπει εκ προοιμίου να επισημανθεί ότι οι δημόσιες πηγές πληροφοριών για το τι θεωρεί η χώρα αυτή υποδομές ζωτικής σημασίας και πώς τις προστατεύει, είναι εξαιρετικά λίγες και δυσεύρετες. Όπως προκύπτει από τη βιβλιογραφική έρευνα που εκπονήθηκε στο πλαίσιο της παρούσας εργασίας, η Ρωσία διέπεται από κάποια διστακτικότητα σχετικά με τη δημοσιοποίηση τέτοιων εγγράφων στο διαδίκτυο, πόσο μάλλον στην αγγλική γλώσσα. Ως εκ τούτου, οι πληροφορίες που παρατίθενται είναι κατά βάση έμμεσες, δηλαδή προέρχονται από φορείς που έχουν διεξάγει έρευνες για τις ρωσικές υποδομές ζωτικής σημασίας και οι οποίοι (φορείς) συνήθως δεν προέρχονται από τη Ρωσία, αλλά από τρίτες χώρες.

Μια τέτοια έρευνα, με τίτλο «Ρωσικές Κρίσιμες Υποδομές – Ευπάθειες και Πολιτικές» έχει διεξαχθεί από την Katri Pynnöniemi [15] για λογαριασμό του Φινλανδικού Ινστιτούτου Διεθνών Σχέσεων (The Finnish Institute of International Affairs). Το ινστιτούτο αυτό είναι ένας ανεξάρτητος (μη κυβερνητικός) οργανισμός, που διεξάγει έρευνες για γεωπολιτικά θέματα. Σύμφωνα με τη μελέτη αυτή, στη Ρωσία δεν χρησιμοποιείται ο όρος κρίσιμη υποδομή / υποδομή ζωτικής σημασίας αλλά αντ' αυτού ο όρος «αντικείμενα κρίσιμης σημασίας» ("critically important objects"). Η χώρα αυτή έχει διαφορετική προσέγγιση για το ζήτημα των κρίσιμων υποδομών: είχε και έχει επισταμένη μέριμνα για ζητήματα

επείγουσας παρέμβασης (“emergencies”) – μάλιστα έχει και ειδικό υπουργείο για τον τομέα αυτόν (Ministry of Emergency Situations of the Russian Federation[6]).

Η Katri Pynnöniemi παραθέτει στην εργασία της έναν έμμεσο προσδιορισμό του όρου κρίσιμα αντικείμενα, μέσω της ακόλουθης αναφοράς: «*Με την προσέγγιση του “Ομοσπονδιακού συστήματος παρακολούθησης των αντικειμένων κρίσιμων υποδομών ή/και επικίνδυνων αγαθών”, που εισήχθη τον Αύγουστο του 2005, η πολιτική* (*σημ:* εννοεί η πολιτική προστασίας υποδομών ζωτικής σημασίας) *ήταν συνυφασμένη με “αντικείμενα κρίσιμης σημασίας” των οποίων η δυσλειτουργία θα μπορούσε να οδηγήσει σε “αδυναμία διαχείρισης της οικονομίας και της διοικητικής-εδαφικής ακεραιότητας της χώρας”* και “*να επηρεάσει την ασφάλεια και την ευημερία του πληθυσμού για μεγάλη χρονική περίοδο”*».

Γενικά, στη μελέτη αυτή καθίσταται σαφές ότι η Ρωσία, με τον όρο προστασία αντικειμένων κρίσιμων υποδομών, εκτός από την προστασία των υποδομών αυτών από εγκληματικές, τρομοκρατικές ενέργειες, περιλαμβάνει και την προστασία από περιβαλλοντικές καταστροφές και ανθρώπινα λάθη στο χειρισμό τεχνολογικών υποδομών. Αναφέροντας ενδεικτικά ορισμένους τύπους «κρίσιμων αντικειμένων», η μελέτη αυτή επικαλούμενη το ομοσπονδιακό πρόγραμμα προστασίας των υποδομών ζωτικής σημασίας του έτους 2006, γνωστοποιεί ότι στη Ρωσία υπάρχουν «2.500 επικίνδυνα αντικείμενα χημικής φύσεως, πάνω από 1.500 τοποθεσίες πυρηνικών υποδομών, 8.000 σημεία με εύφλεκτες και εκρηκτικές υποδομές και πάνω από 30.000 υδροτεχνικά συστήματα» η πλειοψηφία των οποίων έχουν μεγάλη «οικονομική, στρατιωτική και κοινωνική σημασία για τη χώρα, αλλά και υφιστάμενο κίνδυνο για την υγεία και τη ζωή του πληθυσμού και του φυσικού περιβάλλοντος».

Σύνοψη

Συνοψίζοντας, θα μπορούσε κανείς, με βάση τα ανωτέρω, να διακρίνει ενδιαφέρουσες διαφορές στον τρόπο με τον οποίο η Ευρωπαϊκή Ένωση, οι ΗΠΑ και η Ρωσία προσεγγίζουν το ζήτημα της προστασίας υποδομών ζωτικής σημασίας:

- Η Ευρωπαϊκή Ένωση επισημαίνει ότι υποδομές ζωτικής σημασίας δεν είναι μόνον αυτές που θεωρεί το κράτος μέλος απαραίτητες για την λειτουργία του, αλλά και εκείνες που η τυχόν δυσλειτουργία τους θα μπορούσαν να έχουν επιπτώσεις σε άλλα κράτη μέλη.

[6] https://en.mchs.ru

- Οι ΗΠΑ κατανέμουν μέρος της ευθύνης προστασίας των υποδομών ζωτικής σημασίας και στους ιδιώτες που τις κατέχουν και τις λειτουργούν – όχι μόνο στο κράτος.
- Η Ρωσία, με την εμπειρία του πυρηνικού δυστυχήματος στο Τσέρνομπιλ, αλλά και τις αλλεπάλληλες εκτεταμένες φυσικές καταστροφές ένεκα της κλιματικής αλλαγής (πχ οι καταστροφικές φωτιές στη Σιβηρία), εντάσσει στα «αντικείμενα κρίσιμης σημασίας» - αυτός είναι ο όρος της Ρωσίας για τις υποδομές ζωτικής σημασίας – και την προστασία φυσικών περιβαλλοντικών υποδομών, δηλαδή όχι μόνο τους – συνήθεις – τομείς της άμυνας, της οικονομίας και της υγείας.

3.3 Εγκληματολογία στις Υποδομές Ζωτικής Σημασίας

Η ασφάλεια οποιασδήποτε υποδομής, από ένα νοικοκυριό μέχρι τις υποδομές ζωτικής σημασίας μιας ολόκληρης χώρας, απαιτεί κόστος, οι δε πόροι που διατίθενται για τον σκοπό αυτόν δεν είναι απεριόριστοι. Συνεπώς, προτού διατεθεί ο οποιοσδήποτε πόρος – όπως χρόνος, χρήματα, εργατοημέρες κλπ– ως κάλυψη μιας τέτοιας δαπάνης, μια σειρά κρίσιμων ερωτημάτων πρέπει να απαντηθούν. Έτσι, οι διατιθέμενοι πόροι μπορούν να επιφέρουν το βέλτιστο δυνατό αποτέλεσμα στην ασφάλεια της υποδομής που πρέπει να προστατευθεί. Τα ερωτήματα που ακολουθούν είναι εμπειρικά και είναι πάντα ίδια, ανεξαρτήτως της υποδομής:

- Ποιο σημείο της υποδομής μου είναι πιο ευάλωτο σε ζημιά ή κακόβουλη ενέργεια;
- Ποιο σκέλος της υποδομής μου είναι αυτό που θα μου προκαλέσει τα μεγαλύτερα προβλήματα σε περίπτωσης βλάβης η καταστροφής του;
- Είναι εφικτό να κοστολογήσω τυχόν ζημιά ή καταστροφή της υποδομής μου ή μέρος αυτής; Και, αν ναι, ποιο είναι αυτό το πόσο;
- Πόσο εύκολη είναι η εγκατάσταση ενός συστήματος προστασίας της υποδομής μου;
- Ποιο το κόστος μιας τέτοιας εγκατάστασης;
- Αξίζει τελικά η υλοποίηση μιας τέτοιας εγκατάστασης ή μήπως το κόστος της υπερβαίνει αυτό της υποδομής που θέλω να προστατέψω;

3.3.1 Προσδιορισμός κινδύνου για την προστασία των Υποδομών Ζωτικής Σημασίας

Τα ερωτήματα αυτά έρχονται να απαντηθούν από την διαδικασία **προσδιορισμού κινδύνου** (risk assessment) και την διαδικασία **προσδιορισμού ευπαθειών** (vulnerability assessment). Διεξάγονται, είτε εμπειρικά, είτε ακολουθώντας συγκεκριμένες μεθοδολογίες, κάθε φορά που εγκαθίσταται ένα σύστημα προστασίας υποδομών. Με αυτόν τον τρόπο,

στην περίπτωση ενός συστήματος προστασίας και παρακολούθησης ενός νοικοκυριού, προσδιορίζεται το πλήθος και το είδος των αισθητήρων και των καμερών που θα χρειαστούν, τα σημεία που πρέπει να τοποθετηθούν οι συσκευές αυτές κλπ. Στη δε περίπτωση προστασίας ΥΖΣ, οι διαδικασίες αυτές (προσδιορισμού κινδύνου και προσδιορισμού ευπαθειών) είναι προφανώς εξαιρετικά πολύπλοκες, απαραίτητες ωστόσο για τον προσδιορισμό των ποσών που απαιτούνται αλλά και την βέλτιστη δυνατή κατανομή τους.

Μια μελέτη που παρουσιάζει αναλυτικά μεθόδους **προσδιορισμού κινδύνου των ΥΖΣ στον χώρο της Ευρωπαϊκής Ένωσης**, είναι αυτή των Georgios Giannopoulos et al. [16] για λογαριασμό του Ινστιτούτου για την Προστασία και την Ασφάλεια του Πολίτη (Institute for the Protection and Security of the Citizen / IPSC), το οποίο υπάγεται στο Κοινό Κέντρο Ερευνών (Joint Research Centre / JRC), μια επιστημονική υπηρεσία της Ευρωπαϊκής Επιτροπής. Σύμφωνα με τη συγκεκριμένη μελέτη, οι μέθοδοι αυτοί εφαρμόζονται τόσο στην Ευρωπαϊκή Ένωση, όσο και σε διάφορα άλλα μέρη του πλανήτη:

- Better Infrastructure Risk and Resilience (BIRR)
- Protection of Critical Infrastructures - Baseline Protection Concept (BMI)
- CARVER2
- Critical Infrastructure Modelling Simulation (CIMS)
- Critical Infrastructure Protection Decision Support System (CIPDSS)
- Critical Infrastructure Protection modelling and Analysis (CIPMA)
- CommAspen
- COUNTERACT
- The DECRIS approach
- European Risk Assessment and Contingency Planning Methodologies for Interconnected Networks (EURACOM)
- Networks (EURACOM)
- Fast Analysis Infrastructure Tool (FAIT)
- Multilayer Infrastructure Network (MIN)
- Modular Dynamic Model

- Agent-Based Laboratory for Economics (N-ABLE)
- Net-Centric Effects-based operations MOdel (NEMO)
- Network Security Risk Assessment modelling (NSRAM)
- RAMCAP-Plus
- Risk and Vulnerability analysis (RVA)
- Sandia Risk Assessment Methodology
- National Infrastructure Protection Plan Risk Management Framework
- Risk Management for Critical Infrastructure Sectors (Canada)

3.3.2 Επιστημονική Έρευνα για τον Προσδιορισμό Κινδύνου Υποδομών Ζωτικής Σημασίας

Μια άλλη προσέγγιση στο ζήτημα του προσδιορισμού κινδύνου υποδομών ζωτικής σημασίας παρουσιάζεται από τους Venkata Reddy Palleti et al.[12]. Σε αυτή τη μελέτη, οι αρχές της θεωρίας του αξιωματικού σχεδιασμού (axiomatic design) από το σχεδιασμό συστημάτων χρησιμοποιούνται για τη μοντελοποίηση υποδομών ζωτικής σημασίας. Αυτή η μοντελοποίηση παρέχει μια γενική αναπαράσταση υποδομών ζωτικής σημασίας για την κατανόηση της συμπεριφοράς τους σε πιθανές επιθέσεις. Μέσα από τη μελέτη μιας περίπτωσης, δείχνουν πώς μπορεί κανείς να αξιολογήσει την ανίχνευση επιθέσεων και τρωτών σημείων χρησιμοποιώντας αρχές αξιωματικού σχεδιασμού, ενώ χρησιμοποιούν μια ρεαλιστική δοκιμαστική βάση για τη μελέτη των επιπτώσεων των επιθέσεων με βάση τις συγκεκριμένες αρχές σχεδιασμού.

Οι προσεγγίσεις αυτές έρχονται να προσδιορίσουν τους αναγκαίους πόρους για την προστασία των ΥΖΣ και να κατατάξουν τις υποδομές αυτές ανάλογα με την κρισιμότητά τους.

Μεγάλο μέρος της έρευνας και της ανάπτυξης γύρω από τον χώρο της προστασίας των υποδομών ζωτικής σημασίας, αφορά τα Συστήματα Βιομηχανικού Ελέγχου (Industrial Control Systems). Σύμφωνα με μελέτη των Leandros A. Maglaras et al.[17], με θέμα την κυβερνοασφάλεια στις ΥΖΣ , τα Συστήματα Βιομηχανικού Ελέγχου (ICS) είναι ένας όρος που περιλαμβάνει τα «Συστήματα Εποπτικού Ελέγχου και Συλλογής Δεδομένων» (Supervisory Control and Data Acquisition / SCADA), καθώς επίσης και τα «Κατανεμημένα Συστήματα Ελέγχου» (Distributed Control Systems / DCS). Με βάση αυτήν την έρευνα, αυτά τα συστήματα υφίστανται τα τελευταία χρόνια έναν ολοένα και αυξανόμενο αριθμό

επιθέσεων, οι οποίες επηρεάζουν σημαντικούς τομείς των υποδομών ζωτικής σημασίας, όπως, μεταξύ άλλων, οι επικοινωνίες, οι μεταφορές και η ενέργεια. Αναφέρουν τέτοιες περιπτώσεις, όπως η επίθεση με τον ιό SLAMMER το έτος 2003 σε βάρος των συστήματος SCADA πυρηνικού αντιδραστήρα των ΗΠΑ, καθώς επίσης και η επίθεση με τον ιό STUXNET το έτος 2010 σε βάρος υπολογιστών της βιομηχανίας με λειτουργικό σύστημα Windows, μέσω των οποίων οι επιτιθέμενοι αποκτούσαν έλεγχο σε Προγραμματιζόμενους Λογικούς Ελεγκτές (Programmable Logic Controllers/ PLCs). Καταλήγουν στο συμπέρασμα ότι η έγκαιρη και ακριβής ταυτοποίηση των επιτιθέμενων είναι, μεταξύ άλλων, ένα από τα ζητήματα στα οποία πρέπει να επικεντρωθεί η επιστημονική έρευνα γύρω από την προστασία των υποδομών ζωτικής σημασίας. Η επισήμανση αυτή είναι ιδιαιτέρως σημαντική και σχεδόν ταυτόσημη με την έννοια της εγκληματολογικής έρευνας, μιας που ο σκοπός της τελευταίας είναι ακριβώς η ταυτοποίηση του επιτιθέμενου με τρόπο τέτοιο που να τεκμηριώνει νομικά την δίωξή του.

Ειδικότερα για την εγκληματολογία σε ΥΖΣ , η μελέτη των Cristina Alcaraz και Sherali Zeadallly σχετικά με την προστασία υποδομών ζωτικής σημασίας στον 21ο αιώνα, δίνει μια εισαγωγική προσέγγιση και αναδεικνύει μείζονα ζητήματα. Μεταξύ άλλων, αναφέρουν σχετικώς ότι σε περιπτώσεις ασυνήθιστων συμπτωμάτων (των υποδομών ζωτικής σημασίας) ή απειλών, συνίσταται η άμεση μελέτη της ακολουθίας των στοιχείων, του τρόπου λειτουργίας και των ταυτοτήτων που προκάλεσαν αυτήν την κατάσταση. Δυστυχώς, αυτή η διαδικασία βασίζεται σε τεχνικές και μεθοδολογίες εγκληματολογικής διερεύνησης απολύτως συμβατικές. Για τον λόγο αυτό, χρειάζεται να αναπτυχθούν καινούργιες δυναμικές τεχνικές, κατάλληλες για τη διερεύνηση υποδομών ζωτικής σημασίας, οι οποίες να είναι συμβατές με τα βασικά βήματα της εγκληματολογικής διερεύνησης. Εκτός αυτού, δεδομένων των μεγάλων διαστάσεων ορισμένων υποδομών ζωτικής σημασίας, αυτές οι τεχνικές εγκληματολογικής διερεύνησης θα πρέπει να σχεδιαστούν με τέτοιο τρόπο, ώστε να μπορούν να εφαρμοστούν από οπουδήποτε, οποτεδήποτε, καθ' οιονδήποτε τρόπο (δηλαδή είτε on-line, είτε off-line, είτε επιτόπου) και χωρίς να θέτουν σε κίνδυνο την απόδοση ή τη λειτουργία του υπό διερεύνηση συστήματος. Ένας τρόπος για να επιτευχθεί αυτό είναι η χρήση συστημάτων υψηλής διαθεσιμότητας (redundant systems) κατά τη διενέργεια των φάσεων της εγκληματολογικής διερεύνησης.

Για την εφαρμογή των τεχνικών και των μεθοδολογιών της εγκληματολογικής διερεύνησης, είναι σημαντικό να λαμβάνονται υπ' όψιν οι περιορισμοί που προέρχονται από τα συστήματα που περιβάλλουν την υπό διερεύνηση υποδομή ζωτικής σημασίας. Οι

περιορισμοί αυτοί αφορούν περίπλοκες αρχιτεκτονικές, τυχόν ύπαρξη αλληλεπιδράσεων ανάμεσα στα περιφερειακά συστήματα, συνύπαρξη ετερογενών συστημάτων, κλπ. Πρέπει λοιπόν να αναπτυχθούν ελαφρείς, ευέλικτοι μηχανισμοί που να μπορούν να υποστηριχθούν από συσκευές πεδίου (π.χ. αισθητήρες, φορητές διεπαφές, έξυπνους μετρητές, RTUs ή οποιοδήποτε βιομηχανικό αντικείμενο εμπλέκεται σε εργασίες παρακολούθησης) για την αποτελεσματική ανάλυση και συσχέτιση καταστάσεων (δηλαδή των περιστατικών). Μια πιθανή λύση για τη συλλογή αποδεικτικών στοιχείων θα ήταν η χρήση εξωτερικών συσκευών αποθήκευσης που μπορούν να καταγράψουν την δικτυακή κίνηση χωρίς να επηρεάζουν τη συνολική απόδοση του συστήματος. Η πρόσθετη υποστήριξη από συστήματα εντοπισμού εισβολής και αισθητήρες δικτύου θα μπορούσε να βοηθήσει τις εργασίες παρακολούθησης της δικτυακής κυκλοφορίας.

Η συσχέτιση και η ανάλυση των πληροφοριών αυτών θα μπορούσαν να αποτελέσουν μια πολύτιμη πηγή στοιχείων για τεχνικές μηχανικής εκμάθησης (machine learning). Αυτές οι τεχνικές θα μπορούσαν να βελτιώσουν την αρχιτεκτονική, ώστε αυτή να αποκτήσει ορισμένες δυναμικές και αυτόνομες δυνατότητες για τη λήψη αποφάσεων. Δηλαδή, το σύστημα θα μπορούσε, για παράδειγμα, να μάθει (από μόνο του) από ακολουθίες ανώμαλων περιστατικών και να δημιουργήσει αυτόματα νέα μοτίβα και κανόνες που θα μπορούσαν να προκαλέσουν άμεση ανταπάντηση (rapid response). Εκτός αυτού, τεχνικές εξόρυξης δεδομένων μπορούν να αξιοποιηθούν για να προβλέψουν και να ανακαλύψουν νέα πρότυπα συμπεριφοράς μέσω συγκεκριμένων τεχνικών, όπως διαδοχικά μοτίβα ή αλληλουχίες περιστατικών και στατιστική ανάλυση. Η επιλογή και η εφαρμογή ελαφρών μηχανισμών εκμάθησης θα πρέπει να αποτελούν ερευνητικό πεδίο προτεραιότητας, όπου ένα σύνολο μεταβλητών και συνθηκών (όπως η κρισιμότητα του περιβάλλοντος) θα πρέπει να προσδιοριστεί κατάλληλα, όπως επίσης και οι τυχόν αλληλεξαρτήσεις μεταξύ των οντοτήτων του συστήματος.

Επειδή, όπως αναφέρθηκε προηγουμένως, η ταυτοποίηση του επιτιθέμενου πρέπει να γίνεται με τρόπο τέτοιο που να τεκμηριώνει νομικά την δίωξη του, μια βασική απαίτηση για τη χρήση, την επεξεργασία και την προσκόμιση των τεκμηρίων ενώπιον των διωκτικών και δικαστικών αρχών, είναι η κατάδειξη με τρόπο πρόδηλο και μη επιδεχούμενο οιασδήποτε αμφισβήτησης, ότι τα τεκμήρια αυτά είναι αυθεντικά και δεν έχουν υποστεί την παραμικρή αλλοίωση. Για τον λόγο αυτό, όπως αναφέρουν οι Afzaal et al. [18] σε σχετική μελέτη τους, προκειμένου να επιτυγχάνεται ασφαλή αποθήκευση των τεκμηρίων εγκληματολογικής έρευνας σε υποδομές ζωτικής σημασίας, τα οποία τεκμήρια κατά κανόνα είναι τα αρχεία

καταγραφής κινήσεων logs, οι εφαρμογές Διαχείρισης Πληροφορίων και Περιστατικών Ασφαλείας (Security Information and Event Management / SIEM) που χρησιμοποιούνται στον χώρο τον υποδομών ζωτικής σημασίας, διενεργούν κρυπτογράφηση. Συνεπώς, σε περίπτωση επίθεσης, τυχόν προσπάθεια του επιτιθέμενου να προσπελάσει τα αρχεία αυτά (τα logs), προκειμένου να αλλοιώσει τις πληροφορίες που καταδεικνύουν την ταυτότητά του και την προέλευση του, θα αποτύγχανε. Ωστόσο, σύμφωνα με την ίδια πάντα μελέτη, υπάρχουν κάποια σημεία τα οποία θα μπορούσαν να θεωρηθούν ευπάθειες των συγκεκριμένων υλοποιήσεων: οι πιο συνηθισμένες εφαρμογές που χρησιμοποιούνται για την ασφαλή αποθήκευση των κινήσεων καταγραφής σε υποδομές ζωτικής σημασίας, όπως λόγου χάρη οι εφαρμογές Assuria Log Manager (ALM) και AlienVault Open Source Security Information Management (AlienVault OSSIM), χρησιμοποιούν κλασικό αλγόριθμο κρυπτογράφησης RSA [19]. Το πρόβλημα με τη χρήση απλού αλγόριθμου κρυπτογράφησης RSA είναι ότι, αν ο επιτιθέμενος βρει το ιδιωτικό κλειδί (private key) που χρησιμοποιείται κατά την κρυπτογράφηση, τότε μπορεί να προσπελάσει και να αλλοιώσει τις πληροφορίες αυτές. Να σημειωθεί ότι δεν είναι ιδιαίτερα δύσκολο να βρει το ιδιωτικό κλειδί, αφού μια απλή αναζήτηση στον σκληρό δίσκο μπορεί να το ανασύρει. Εκτός αυτού, σε περίπτωση κατά την οποία ο επιτιθέμενος καταφέρει να θέσει εκτός λειτουργίας το σύστημα που διεξάγει την κρυπτογράφηση, για παράδειγμα με μια επίθεση άρνησης λειτουργίας (Denial Of Service / DoS attack) σε βάρος του, η κρυπτογράφηση μπορεί να σταματήσει, επιφέροντας έτσι καταγραφή των κινήσεων σε απλή μορφή (raw format) ή ακόμα και καθόλου καταγραφή.

Για την αντιμετώπιση αυτών των ζητημάτων, οι Afzaal et al. προτείνουν μια άλλη προσέγγιση, πάλι μεν με χρήση του αλγόριθμου κρυπτογράφησης RSA, αλλά όχι στην απλή του εφαρμογή. Χρησιμοποιούν ένα εξελιγμένο σχήμα αυτού του αλγόριθμου που ονομάζεται Υπογραφή Κατωφλίου RSA (“RSA Threshold Signature”). Με την κρυπτογράφηση κατωφλίου (threshold cryptography), το ιδιωτικό κλειδί κατακερματίζεται σε *n* μέρη. Στη συνέχεια, για τον επιτυχή σχηματισμό του ιδιωτικού κλειδιού, γίνεται χρήση ενός μόνο πλήθους *k* εκ του συνόλου των *n* μερών. Το γεγονός ότι τα *n* μέρη του ιδιωτικού κλειδιού μπορεί – και πρέπει – να έχουν αποθηκευτεί σε διαφορετικές τοποθεσίες (οι οποίες μπορεί και να μην είναι καν στον ίδιο υπολογιστικό σύστημα, αλλά σε διαφορετικά), αναγκάζει τον υποτιθέμενο να βρει τουλάχιστον *k* μέρη του κλειδιού, ώστε να καταφέρει να το ανασυνθέσει. Αυτό προφανώς είναι ασύγκριτα πιο δύσκολο σε σχέση με την κλασική υλοποίηση του αλγόριθμου RSA, κατά την οποία το ιδιωτικό κλειδί αποθηκεύεται (ολόκληρο) σε μια μόνο τοποθεσία.

Κατά την πειραματική εφαρμογή της ανωτέρω προσέγγισης, οι Afzaal et al. χρησιμοποίησαν κατανεμημένα συστήματα με πολυνηματικό προγραμματισμό αλλά και μια βελτιστοποιημένη δομή δεδομένων, η οποία επέτρεπε τον μέγιστο αριθμό νημάτων για ταυτόχρονη καταγραφή των δεδομένων. Αυτό είχε ως αποτέλεσμα εξαιρετική αύξηση της απόδοσης αυτού του συστήματος. Μάλιστα στη συνέχεια ενσωμάτωσαν την υλοποίηση τους στην εφαρμογή AlienVault OSSIM, επιτυγχάνοντας έτσι να αναβαθμίσουν την ακεραιότητα των δεδομένων (δηλαδή των κινήσεων στα αρχεία καταγραφής – logs) ακόμα και σε προβληματικές καταστάσεις, όπως η εκδήλωση μιας επίθεσης.

Η πρόταση των Afzaal et al. παρουσιάστηκε το έτος 2012. Στα χρόνια που ακολούθησαν, ακόμα πιο εξελιγμένες τεχνικές, όπως η τεχνολογία blockchain, προτάθηκαν για την προστασία των αρχείων καταγραφής (logs), κάτι απολύτως απαραίτητο για την ακεραιότητά τους και την αποτελεσματική χρήση τους κατά τη διενέργεια εγκληματολογικών ερευνών σε υποδομές ζωτικής σημασίας.

Κεφάλαιο 4 - Εγκληματολογική Έρευνα για Υποδομές Ζωτικής Σημασίας στο νέφος

4.1 Μεθοδολογία

Αρχικά διερευνώνται περιπτώσεις χρήσης και βέλτιστες πρακτικές εγκληματολογικής έρευνας για συστήματα που λειτουργούν στο νέφος. Οι πρακτικές αυτές εξετάζονται τόσο στον θεσμικό τομέα όσο και στον τεχνικό. Μέσα από αυτή τη διαδικασία ανακύπτουν προκλήσεις που εμφανίζονται κατά τη διεξαγωγή εγκληματολογικών ερευνών αλλά προτείνονται και λύσεις για την αντιμετώπισή τους.

Στη συνέχεια, επιχειρείται αξιολόγηση συστημάτων Υποδομών Ζωτικής Σημασίας που λειτουργούν στο νέφος, από πλευράς υποστήριξης της εγκληματολογικής έρευνας. Εδώ αναφέρονται παράγοντες με βάση τους οποίους μπορεί να διεξάγεται αυτή η αξιολόγηση και παρατίθεται ένα ολοκληρωμένο παράδειγμα χρήσης, ώστε να καταδειχθεί το πώς μπορεί να διεξαχθεί εγκληματολογική διερεύνηση σε ένα πραγματικό περιβάλλον υπολογιστικής νέφους.

Οι περιοχές του πλανήτη οι οποίες διερευνώνται και αξιολογούνται ως προς τις υποδομές αυτές, είναι οι Ηνωμένες Πολιτείες Αμερικής (ΗΠΑ), η Ευρωπαϊκή Ένωση (ΕΕ) και η Ρωσία. Οι δε κλάδοι της βιομηχανίας είναι η άμυνα, η οικονομία και η υγεία.

4.2 Περιπτώσεις Χρήσης Εγκληματολογικής Έρευνας για συστήματα ΥΖΣ που λειτουργούν στο νέφος

Οι προκλήσεις στον χώρο της εγκληματολογικής έρευνας για συστήματα υποδομών ζωτικής σημασίας που λειτουργούν στο νέφος μπορούν να χωριστούν στους εξής βασικούς τομείς: τον θεσμικό και τον τεχνικό. Στον θεσμικό τομέα υπάγονται ζητήματα όπως η νομοθεσία υπό την οποία διεξάγεται μια εγκληματολογική έρευνα, η δικαιοδοσία στην οποία υπάγεται το περιστατικό ή/και οι πληροφοριακοί πόροι που επηρεάστηκαν, οι διεθνείς συμφωνίες αμοιβαίας δικαστικής συνδρομής, το κανονιστικό πλαίσιο προς το οποίο συμμορφώνονται οι πάροχοι υπηρεσιών νέφους και άλλα. Στον τεχνικό τομέα υπάγονται κυρίως τα εργαλεία και οι υποδομές πληροφορικής που χρησιμοποιούνται κατά την διεξαγωγή της εγκληματολογικής έρευνας ή την διευκολύνουν.

4.2.1 Βέλτιστες πρακτικές εγκληματολογικής έρευνας στον θεσμικό τομέα

Όσον αφορά τον θεσμικό τομέα, αν ήθελε να συνοψίσει κανείς τις σχετικές προκλήσεις που εμφανίζονται στην εγκληματολογία νέφους σε μια μόνο πρόταση, θα μπορούσε να επικαλεστεί την ακόλουθη ρήση του Alexander Seger, επικεφαλής του τμήματος του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο[7]: *«Το πρόβλημα είναι ότι, όταν ψάχνεις να βρεις αποδεικτικό στοιχείο σε ένα υπολογιστικό σύστημα, αυτό το αποδεικτικό στοιχείο μπορεί να βρίσκεται σε έναν εξυπηρετητή μιας άλλης χώρας, ή θα μπορούσε να μετακινούνταν ανάμεσα σε διάφορους εξυπηρετητές, ή τα ίδια τα δεδομένα θα μπορούσαν να ήταν κατακερματισμένα σε διαφορετικές τοποθεσίες με διαφορετικές δικαιοδοσίες»*. Η φράση αυτή συνοψίζει μια σειρά προβλημάτων, η αντιμετώπιση των οποίων είναι πολύ πιο δύσκολη από εκείνη που αφορά τα τεχνικά ζητήματα. Επιπλέον, ο Alexander Seger αναφέρει ορισμένα χαρακτηριστικά προβλήματα με τα οποία έρχονται αντιμέτωπες οι διωκτικές αρχές, μεταξύ των οποίων είναι η δυσκολία με την οποία απαιτούν τη μεταβίβαση κάποιου αποδεικτικού στοιχείου από τις δικαστικές αρχές μιας άλλης χώρας, το ισχυρότατο ενδεχόμενο να απορριφθούν αποδεικτικά στοιχεία μιας υπόθεσης από τον δικαστή που εκδικάζει το έγκλημα, μιας που τα στοιχεία αυτά αποκτήθηκαν με τρόπο που δεν είναι συμβατός νομικά με τη χώρα στην οποία εκδικάζεται το έγκλημα, αλλά και η πολύ αργή ταχύτητα με την οποία ανταλλάσσονται πληροφορίες και αποδεικτικά στοιχεία ανάμεσα σε χώρες που έχουν συνάψει μεταξύ τους Συμφωνίες Αμοιβαίας Δικαστικής Συνδρομής (Mutual Legal Agreement Treaties / MLATs).

Ενδεικτικό της κρισιμότητας που έχει η διεθνής συνεργασία είναι ένα οξύμωρο περιστατικό που αναφέρει ο John Cauthen[8], ερευνητής του Ομοσπονδιακού Γραφείου Ερευνών (Federal Bureau of Investigation / FBI) στο Σακραμέντο των ΗΠΑ, σε άρθρο του στον ιστότοπο αυτής της υπηρεσίας: κατά την εκδίκαση μιας υπόθεσης σε Ομοσπονδιακό δικαστήριο (W.D. Wash) στις 23 Μαΐου 2001, ο ερευνητής του Ομοσπονδιακού Γραφείου Ερευνών (και ενάγων) προσκόμισε αποδεικτικά στοιχεία τα οποία είχε αποκτήσει από τρίτη χώρα. Όμως το γεγονός ότι, για την απόκτηση αυτών των αποδεικτικών στοιχείων, δεν είχε ζητήσει την άδεια της χώρας αυτής, είχε ως αποτέλεσμα να μην γίνουν αποδεκτά από το δικαστήριο τα στοιχεία αυτά αλλά και ο ερευνητής να βρεθεί διωκόμενος από τη συγκεκριμένη χώρα για πειρατεία (hacking)!

Κατόπιν αυτών, συμπεραίνεται ότι το πρώτο σκέλος των βέλτιστων πρακτικών εγκληματολογικής έρευνας για συστήματα που λειτουργούν στο νέφος, είναι η θέσπιση νομικών διαδικασιών που να επιτρέπουν στις ανά τον κόσμο διωκτικές αρχές τη γρήγορη

[7] https://news.sky.com/story/cybercrime-agreement-to-be-signed-by-global-leaders-10902968
[8] https://leb.fbi.gov/articles/featured-articles/executing-search-warrants-in-the-cloud

και νομικά αποδεκτή ανταλλαγή πληροφοριών και αποδεικτικών στοιχείων. Φυσικά η ίδια ακριβώς ανάγκη αφορά και χώρες οι οποίες είναι ομοσπονδίες κρατών ή πολιτειών, όπως για παράδειγμα οι ΗΠΑ, όπου η κάθε πολιτεία έχει το δικό της Δίκαιο.

Ωστόσο το εφαρμοστέο δίκαιο, δηλαδή το δίκαιο που θα εφαρμοστεί κατά τη διεξαγωγή εγκληματολογικής έρευνας (και πιθανά διώξεων) σε ένα έγκλημα στο νέφος, μπορεί να είναι και ανεξάρτητο από τον χώρο στον οποίο βρίσκονται τα κέντρα δεδομένων στα οποία συντελέστηκε. Αν, για παράδειγμα, σε ένα συμφωνητικό παροχής υπηρεσιών ανάμεσα σε έναν πάροχο νέφους και έναν πελάτη, προβλεφθεί ότι το εφαρμοστέο δίκαιο σε περίπτωση εγκλήματος θα είναι αυτό της χώρας του πελάτη, τότε αυτό ακριβώς το δίκαιο θα εφαρμοστεί, ανεξαρτήτως του που βρίσκονται τα κέντρα δεδομένων από τα οποία εξυπηρετείται ο πελάτης.

Σε κάθε περίπτωση όμως, οι διεθνείς συμβάσεις για την καταπολέμηση του κυβερνοεγκλήματος διευκολύνουν την εγκληματολογική έρευνα, ειδικά όταν διεξάγεται σε διεθνές επίπεδο, όπως στην περίπτωση του νέφους. Αν και ακόμα χρειάζεται πολλή προσπάθεια για να καθιερωθούν σε διεθνές επίπεδο οι συμφωνίες αυτές, τα τελευταία χρόνια έχει γίνει η αρχή με τη σύναψη ορισμένων τέτοιων συμφωνιών. Κατωτέρω παρατίθενται ενδεικτικά τέτοιες συμφωνίες, που, αν και δεν αφορούν αποκλειστικά τις ΥΖΣ αλλά τον χώρο τις κυβερνοασφάλειας γενικά, εντούτοις είναι νομικά εργαλεία που μπορούν να χρησιμοποιηθούν κατά τη διεξαγωγή εγκληματολογικών ερευνών (και διώξεων) σε διεθνές επίπεδο.

Ευρωπαϊκή Ένωση

Πίνακας 4.1. Συμβάσεις της Ευρωπαϊκής Ένωσης σχετικά με την καταπολέμηση του κυβερνοεγκλήματος

Όνομα Συμφωνίας	Σχόλια
«Η Σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον Κυβερνοχώρο» [20]	Όπως εξηγεί ο Sliwinski [21], οι ΗΠΑ υπέγραψαν και επικύρωσαν τη Σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο –γνωστή και ως Σύμβαση της Βουδαπέστης– η οποία εκφράζει την κοινή δέσμευση των δυο πλευρών για την τιμωρία των δραστών και την αποτροπή των απειλών στον κυβερνοχώρο. Η σύμβαση αυτή έχει επικυρωθεί και από πολλές άλλες χώρες, με αποτέλεσμα να έχει πλέον καταστεί η σημαντικότερη διεθνώς σύμβαση στον χώρο της κυβερνοασφάλειας. Ωστόσο υπάρχουν και χώρες με σημαντική δραστηριότητα στο διαδίκτυο, οι οποίες δεν έχουν αποδεχθεί αυτή τη σύμβαση. Τέτοιες είναι η Ρωσία, ο Καναδάς, Η Ινδία, οι Φιλιππίνες, κ.ά.
«Η Στρατηγική της Ευρωπαϊκής Ένωσης για τον κυβερνοχώρο - Για έναν ανοικτό, ασφαλή και προστατευμένο κυβερνοχώρο» [22]	Ο Philippe Vitel [23] αναφέρει πέντε προτεραιότητες του κειμένου, εκ των οποίων δυο αναφέρονται έμμεσα στην προστασία των ΥΖΣ: **(α)** ανάπτυξη των βιομηχανικών και τεχνολογικών πόρων για την κυβερνοασφάλεια και **(β)** θέσπιση συνεκτικής διεθνούς πολιτικής της Ευρωπαϊκής Ένωσης για τον κυβερνοχώρο και προώθηση των βασικών αξιών της ΕΕ. Μάλιστα, ο Vitel επικαλείται εισήγηση της Ευρωπαϊκής Επιτροπής με θέμα την αναθεώρηση του Ευρωπαϊκού Προγράμματος για την Προστασία ΥΖΣ [24], στην οποία η «Στρατηγική της Ευρωπαϊκής Ένωσης για τον κυβερνοχώρο» φέρεται ως συμπληρωματικό κείμενο για την προστασία των Ευρωπαϊκών ΥΖΣ στον χώρο των τηλεπικοινωνιών και της πληροφορικής.
«Ανακοίνωση Της Επιτροπής Στο Ευρωπαϊκό Κοινοβούλιο, Το Συμβούλιο, Την Ευρωπαϊκή Οικονομική Και Κοινωνική Επιτροπή Και την Επιτροπή Των Περιφερειών - Αξιοποίηση των δυνατοτήτων του υπολογιστικού νέφους» [25]	Πρόκειται για κείμενο της Ευρωπαϊκής Επιτροπής το οποίο τονίζει την ανάγκη προώθησης του διεθνούς διαλόγου για την επίλυση των μείζονων ζητημάτων της υπολογιστικής νέφους, τα οποία αποτελούν συνάμα και τα μείζονα ζητήματα της εγκληματολογίας υπολογιστικής νέφους. Τα ζητήματα αυτά αναφέρονται ρητά και είναι, μεταξύ άλλων, **(α)** το νομικό πλαίσιο, **(β)** η πρόσβαση σε δεδομένα εκ μέρους των διωκτικών αρχών, **(γ)** η χρήση συμφωνιών αμοιβαίας δικαστικής συνδρομής ώστε να μην προκύπτουν αντικρουόμενα αιτήματα από τις διωκτικές και τις δημόσιες εν γένει αρχές, **(δ)** ο συντονισμός της ασφάλειας των δεδομένων σε παγκόσμιο επίπεδο, η ασφάλεια στον κυβερνοχώρο, **(ε)** η ευθύνη των παρόχων υπηρεσιών νέφους κ.ά. Μάλιστα, το κείμενο αυτό έχει εκτεταμένη αναφορά και σε μια ακόμα πρόκληση της υπολογιστικής νέφους, που δεν αφορά αποκλειστικά την εγκληματολογία αλλά όλο το οικοσύστημα των προτύπων. Το γεγονός ότι ο κάθε πάροχος υπηρεσιών νέφους και γενικά κάθε φορέας αυτού του οικοσυστήματος έχει τα δικά του πρότυπα, προκαλεί σοβαρά εμπόδια στην εύκολη και γρήγορη διεξαγωγή εγκληματολογικής έρευνας. Για παράδειγμα, εξαιτίας του γεγονότος ότι ο κάθε πάροχος διαμορφώνει τα αρχεία καταγραφής κινήσεων (logs) με τον δικό του τρόπο, ο ερευνητής καλείται να ασχοληθεί με την μετατροπή των προτύπων από ένα τύπο (format) σε άλλο, ενώ τη δεδομένη χρονική στιγμή θα έπρεπε να ασχολείται μόνο με την εξιχνίαση της υπόθεσης. Στο κείμενο αυτό αναδεικνύεται η σημασία του εν εξελίξει διεθνούς διαλόγου για τα ζητήματα αυτά με τις ΗΠΑ, την Ινδία, την Ιαπωνία και άλλες χώρες, ενθαρρύνοντας κατ' αυτόν τον τρόπο αυτές τις δράσεις σε σχέση και με άλλες χώρες.

ΗΠΑ

Η σημαντικότερη διεθνής σύμβαση που έχουν υπογράψει οι ΗΠΑ σε σχέση με την καταπολέμηση του κυβερνοεγκλήματος είναι η προαναφερθείσα «Σύμβαση του Συμβουλίου της Ευρώπης για το έγκλημα στον Κυβερνοχώρο» (/«Σύμβαση της Βουδαπέστης»). Επιπλέον, οι ΗΠΑ έχουν υπογράψει διάφορες συμβάσεις του ΟΗΕ για την καταπολέμηση του διεθνούς οργανωμένου εγκλήματος, όπως για παράδειγμα η «Σύμβαση των Ηνωμένων Εθνών κατά του Διεθνικού Οργανωμένου Εγκλήματος» [26]. Όμως, οι συμβάσεις του ΟΗΕ είναι κατά βάση γενικά κείμενα για την εναρμόνιση της νομοθεσίας της κάθε χώρας σε σχέση με ένα κοινό πρότυπο και δεν μπορούν να χρησιμεύσουν στις κατά τόπους διωκτικές αρχές για την διεξαγωγή εγκληματολογικών ερευνών ή διώξεων. Απεναντίας, ιδιαίτερη σημασία για την διευκόλυνση των εγκληματολογικών ερευνών στο νέφος έχουν οι διμερείς συμφωνίες, ιδίως στις περιπτώσεις κατά τις οποίες τα κέντρα δεδομένων που εμπλέκονται σε ένα έγκλημα στο νέφος βρίσκονται σε χώρες μεταξύ των οποίων έχουν υπογραφεί συμφωνίες αμοιβαίας δικαστικής συνδρομής.

Κατωτέρω παρατίθεται ενδεικτικός πίνακας διμερών συμφωνιών των ΗΠΑ με άλλες χώρες.

Πίνακας 4.2. Διμερείς συμφωνίες των ΗΠΑ σχετικά με την καταπολέμηση του κυβερνοεγκλήματος

Όνομα Συμφωνίας	Σχόλια
Συμφωνία Συνεργασίας με Ιταλία (Ιούλιος 2009) [27]	Στις 6 Ιουλίου 2009 οι ΗΠΑ υπέγραψαν διμερή συμφωνία με την Ιταλία με αντικείμενο την από κοινού δίωξη του ηλεκτρονικού οικονομικού εγκλήματος. Η συμφωνία προέβλεπε τη δημιουργία κοινής ομάδας κρούσης (task force) με τίτλο «Ευρωπαϊκή Ομάδα Ηλεκτρονικού Εγκλήματος» (European Electronic Crime Task Force) και έδρα την πρωτεύουσα της Ιταλίας, τη Ρώμη. Σε επιχειρησιακό επίπεδο, αυτή είναι και η σημαντικότερη συμφωνία ανάμεσα στις ΗΠΑ και τον Ευρωπαϊκό χώρο.
Οι Κατευθυντήριες Γραμμές Για Την Αμυντική Συνεργασία Ιαπωνίας-ΗΠΑ (2015) [28]	Πρόκειται για μια διμερή συμφωνία αμυντικής συνεργασίας, η οποία έχει ανανεωθεί (επικαιροποιηθεί) πολλές φορές. Όπως αναλύουν οι Harold et al. [29], το έκτο από τα οκτώ κεφάλαια αναφέρεται στην συνεργασία για θέματα κυβερνοασφάλειας. Στο κεφάλαιο αυτό υπάρχει ξεχωριστή αναφορά στην προστασία των ΥΖΣ της Ιαπωνίας από επιθέσεις στον κυβερνοχώρο, στον τρόπο με τον οποίο οι δυο πλευρές θα πρέπει απαντήσουν σε τυχόν περιστατικό, αλλά και στις λεπτομέρειες που αφορούν την ανταλλαγή πληροφοριών στο πλαίσιο διεξαγωγής εγκληματολογικών ερευνών.
Συμφωνία Συνεργασίας με Ρωσία (2019)[9]	Σύμφωνα με δημοσίευμα του ειδησεογραφικού πρακτορείου Reuters της 17ης Οκτωβρίου 2019, οι ΗΠΑ επανέφεραν τη συνεργασία τους με τη Ρωσία για θέματα κυβερνοασφάλειας.
Συμφωνία Συνεργασίας με Κίνα (Απρίλιος 2017) [30]	Σύμφωνα με ανακοίνωση του Λευκού Οίκου που εκδόθηκε στις 7 Απριλίου 2017, κατόπιν της συνάντησης του Προέδρου των ΗΠΑ Ντόναλντ Τραμπ με τον Κινέζο ομόλογό του Σι Τσινπινγκ, οι δυο αρχηγοί συμφώνησαν στην έναρξη διαλόγου ανάμεσα στις δυο πλευρές, ο οποίος θα διεξάγονταν σε τέσσερις πυλώνες. Ένας εκ των τεσσάρων αυτών πυλώνων διαλόγου αφορούσε τις διωκτικές αρχές και την κυβερνοασφάλεια.

[9] https://www.reuters.com/article/us-russia-usa-cybersecurity/russia-says-it-is-starting-to-resume-u-s-cyber-cooperation-tass-idUSKBN1WW1TL

Ρωσία

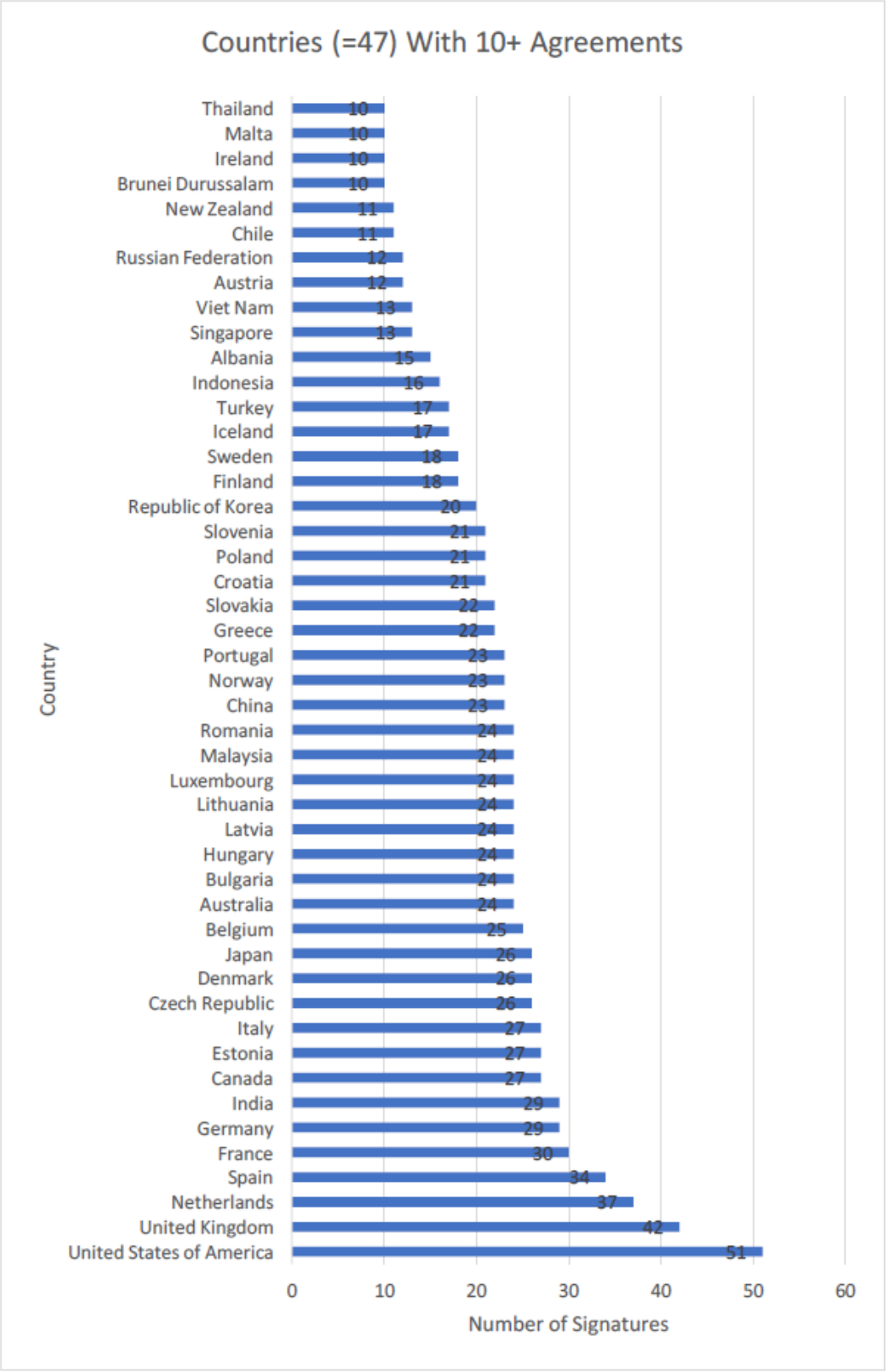
Η Ρωσία, όπως ήδη αναφέρθηκε, είναι μια από τις χώρες που δεν έχουν υπογράψει τη Σύμβαση της Βουδαπέστης. Αυτό, σύμφωνα με τους T. Hitchens και N. Goren [31], είναι ενδεικτικό της απροθυμίας της να βοηθήσει άλλα κράτη στην εξιχνίαση εγκλημάτων του κυβερνοχώρου που έχουν ως έδρα την ίδια, αρνούμενη δε τη χορήγηση πρόσβασης στους πληροφοριακούς της πόρους ακόμα και στην Interpol. Για την στάση της αυτή η Ρωσία επικαλείται λόγους προάσπισης της εθνικής της κυριαρχίας. Σύμφωνα με την έρευνα αυτή, η Ρωσία έχει υπογράψει τέσσερεις διεθνείς συμφωνίες ανταλλαγής πληροφοριών στο πλαίσιο της καταπολέμησης του κυβερνοεγκλήματος, συγκεκριμένα με το Ιράν, την Ινδία, τον Οργανισμό Συνεργασίας της Σαγκάης [32] και την Κίνα. Ωστόσο μια σημαντική διακρατική συμφωνία της Ρωσίας στον χώρο του διαδικτύου, είναι αυτή που συνήψε με την Κίνα στις 30 Απριλίου 2015 [33].

Πίνακας 4.3. Διμερείς συμφωνίες της Ρωσίας σχετικά με την καταπολέμηση του κυβερνοεγκλήματος.

Όνομα Συμφωνίας	**Σχόλια**
Συμφωνία Μεταξύ Της Ρωσικής Ομοσπονδίας Και Της Κυβέρνησης Της Λαϊκής Δημοκρατίας Της Κίνας Σχετικά Με Τη Συνεργασία Στον Τομέα Της Διεθνούς Ασφάλειας Πληροφοριών [33]	Στο τρίτο άρθρο, στις παραγράφους 5, 8 και 9 της συμφωνίας, προβλέπεται ρητά η συνεργασία των δυο πλευρών στον χώρο της καταπολέμησης του κυβερνοεγκλήματος αλλά και της ασφάλειας πληροφοριών εν γένει. Στα σημεία αυτά υπάρχουν σαφείς δεσμεύσεις για ανταλλαγή πληροφοριών στο πλαίσιο εγκληματολογικών ερευνών, ανταλλαγή πληροφοριών σχετικά με τη νομοθεσία των δυο πλευρών περί ασφάλειας πληροφοριών, τη βελτίωση του διεθνούς νομικού πλαισίου και τη δημιουργία κοινών μηχανισμών για την προάσπιση της ασφάλειας πληροφοριών. Αν και η συμφωνία αυτή διαμορφώνει ιδανικές συνθήκες για την απρόσκοπτη διεξαγωγή εγκληματολογικών ερευνών ανάμεσα στα δυο υπογράφοντα μέρη, έχει αντιμετωπιστεί από πολλούς με κάποια επιφύλαξη σε σχέση με ζητήματα ανθρωπίνων δικαιωμάτων και ατομικών ελευθεριών (μεταξύ αυτών και οι ίδιοι οι T. Hitchens και N. Goren [31]).

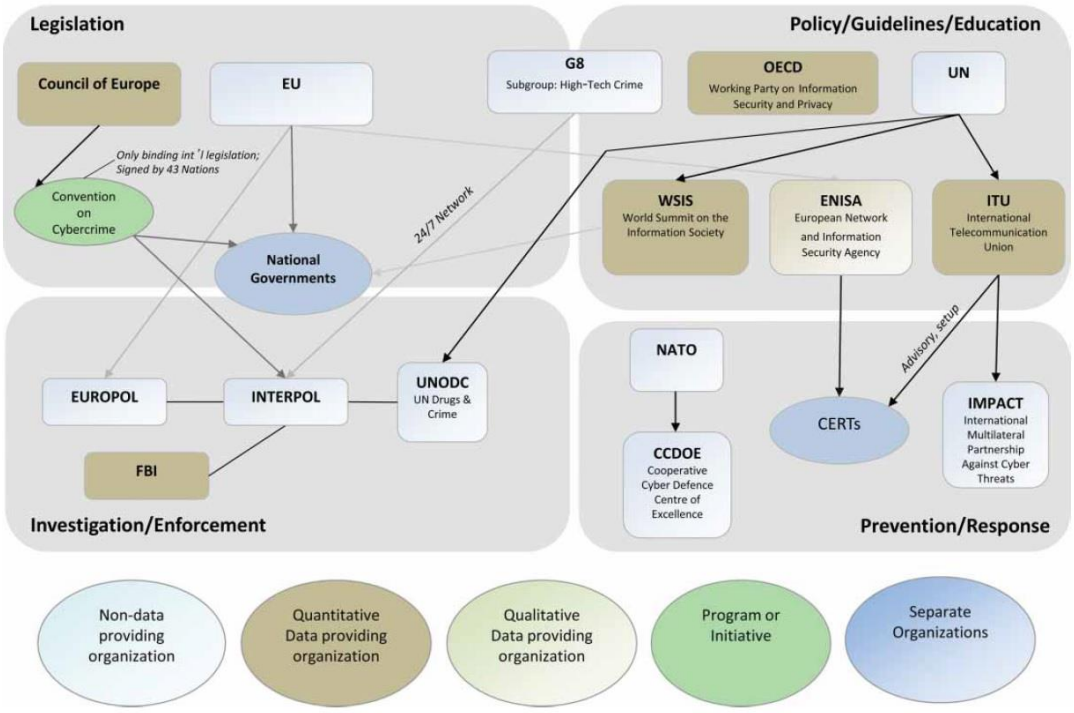
Η διεθνής συνεργασία για την καταπολέμηση του κυβερνοεγκλήματος

Πέραν των περιοχών που αναφέρθηκαν (Ευρωπαϊκή Ένωση, ΗΠΑ και Ρωσία), οι T. Hitchens και N. Goren παραθέτουν ένα κατατοπιστικό γράφημα (Εικόνα 4.1) με 47 χώρες και τον αριθμό των συμφωνιών ανταλλαγής πληροφοριών κυβερνοασφάλειας που έχει υπογράψει η καθεμία.



Εικόνα 4.1. Πλήθος διμερών συμφωνιών ανταλλαγής πληροφοριών κυβερνοασφάλειας που έχουν υπογράψει 47 χώρες [31]

Τέλος, μια συνοπτική απεικόνιση των διεθνών οργανισμών που ασχολούνται με την καταπολέμηση του κυβερνοεγκλήματος αλλά και του τρόπου με τον οποίο συνεργάζονται, συμμετέχοντας στην εγκληματολογική έρευνα υποθέσεων, παραθέτουν οι N. Choucri, S. Madnick και J. Ferwerda [34], ως ακολούθως:



Εικόνα 4.2. Βασικοί διακρατικοί θεσμοί καταπολέμησης του κυβερνοεγκλήματος και ο τρόπος με τον οποίο συνεργάζονται

4.2.2 Βέλτιστες πρακτικές εγκληματολογικής έρευνας στον τεχνικό τομέα

Μια γενική επισκόπηση των τεχνικών κυρίως προκλήσεων που παρουσιάζονται στον χώρο της εγκληματολογίας για συστήματα υποδομών ζωτικής σημασίας που λειτουργούν στο υπολογιστικό νέφος, αλλά και βέλτιστες πρακτικές για την αντιμετώπισή τους, διεξάγουν οι Pichan et al. [7] σε σχετική μελέτη τους. Η προσέγγισή τους αφορά όλες τις **φάσεις της εγκληματολογικής έρευνας**, οπότε και παραθέτουν αντίστοιχους πίνακες:

Πίνακας 4.4. Φάση Ταυτοποίησης (Identification): Προκλήσεις και Βέλτιστες Πρακτικές [7]

Α/Α	Πρόκληση	Βέλτιστη Πρακτική	Σχόλια
1	**Άγνωστη φυσική τοποθεσία (τέλεσης του εγκλήματος)**	Σήμανση πόρων (resource tagging)	Η έλλειψη της σήμανσης πόρων δυσχεραίνει την ικανότητα των παρόχων να διασφαλίσουν ευελιξία, διαθεσιμότητα υπηρεσιών και ευκολία διαχείρισης.
		Σύναψη συμφωνητικών παροχής υπηρεσιών με τους παρόχους υπηρεσιών νέφους που να προβλέπουν ρητά υποδομές και λειτουργίες για την υποστήριξη εγκληματολογίας νέφους	Οι περισσότεροι οδηγοί για συμφωνητικά παροχής υπηρεσιών επικεντρώνονται κυρίως στις απαιτήσεις ασφάλειας και λιγότερο στις απαιτήσεις εγκληματολογίας.
		Αρχεία καταγραφής κινήσεων σε επίπεδο συστήματος (system level logs)	Τα αρχεία καταγραφής κινήσεων σε επίπεδο συστήματος μπορούν να περιέχουν πρωτογενείς πληροφορίες αναφορικά με την πρόσβαση, τη δημιουργία και τη διαγραφή αντικειμένων του συστήματος
2	**Αποκεντρωμένα δεδομένα**	Καθορισμός κατάλληλου πλαισίου για την καταγραφή των κινήσεων (log frame work)	Τα αρχεία καταγραφής κινήσεων στο επίπεδο του hypervisor μπορούν να βοηθήσουν την εγκληματολογική έρευνα και να καταδείξουν τη σειρά των γεγονότων.
3	**Κλωνοποίηση των δεδομένων**	Σήμανση πόρων (resource tagging)	Η έλλειψη της σήμανσης πόρων δυσχεραίνει την απόδοση του συστήματος.
4	**Δικαιοδοσία**	Σύναψη συμφωνητικών παροχής υπηρεσιών (SLAs) που να δηλώνουν ρητά την τοποθεσία στην οποία αποθηκεύονται τα δεδομένα, καθώς επίσης και την τοποθεσία στην οποία κλωνοποιούνται (αντιγράφονται).	Η τυχόν έλλειψη τέτοιας πρόβλεψης στο συμφωνητικό παροχής υπηρεσιών μπορεί να δυσχεράνει την ικανότητα των παρόχων να διασφαλίσουν ευελιξία, διαθεσιμότητα υπηρεσιών και οικονομικά οφέλη στους καταναλωτές (μισθωτές).
		Η αντίστροφη αναζήτηση (reverse lookup) των συσκευών του δικτύου οδηγεί σε αντίστροφη αναζήτηση της τοπολογίας τους δικτύου.	Αυτή είναι μια κρίσιμη χρονικά ενέργεια εξαιτίας της δυναμικής φύσης της υπολογιστικής νέφους.
5	**Αλυσίδα εξαρτήσεων**	Καμία	Εδώ υπάρχει έλλειψη σε κατάλληλα εργαλεία λογισμικού, στη συγκρότηση τυποποιημένων διαδικασιών, κλπ
7	**Εξάρτηση από τον Πάροχο Υπηρεσιών Νέφους**	Σύναψη συμφωνητικών παροχής υπηρεσιών (SLAs) που να προβλέπουν συγκεκριμένες υπηρεσίες για την υποστήριξη εγκληματολογίας νέφους	Τα καλά Συμφωνητικά Παροχής Υπηρεσιών εξασφαλίζουν διαθεσιμότητα υπηρεσιών και συμμόρφωση προς το κανονιστικό πλαίσιο.

Πίνακας 4.5. Φάση Διαφύλαξης (Preservation): Προκλήσεις και Βέλτιστες Πρακτικές [7]

Α/Α	Πρόκληση	Βέλτιστη Πρακτική	Σχόλια
1	**Διαφύλαξη Αλυσίδας Αποδεικτικών Στοιχείων (Chain of Custody)**	Κρυπτογράφηση με χρήση αλγορίθμου RSA	Η κρυπτογράφηση με αλγόριθμο RSA μπορεί να εξασφαλίσει τη διαφύλαξη της αλυσίδας αποδεικτικών στοιχείων και την ακεραιότητα των δεδομένων.
2	**Διαχωρισμός αποδεικτικών στοιχείων (evidence segregation)**	Εφαρμογή τεχνικής Sandboxing (πρόκειται για τεχνική με βάση την οποία τα προγράμματα χωρίζονται σε εικονικούς θύλακες με τέτοιο τρόπο ώστε κανένας θύλακας να μη γνωρίζει την ύπαρξη των διπλανών του)	Τα προγράμματα χωρίζονται σε εικονικούς θύλακες. Η καταγραφή ολόκληρων των οντοτήτων (instances) του Sandbox απεικονίζει την τρέχουσα κατάσταση λειτουργίας των οντοτήτων των εικονικών υπολογιστών του χρήστη, οπότε και μπορούν (αυτά τα instances) να φορτωθούν σε έναν άλλο εικονικό υπολογιστή για ανάλυση.
3	**Κατανεμημένη αποθήκευση (distributed storage)**	Σήμανση των εικονικών υπολογιστών (VM instance tagging)	Η σήμανση των εικονικών υπολογιστών μπορεί να χρησιμεύσει στην κατάδειξη της τοποθεσίας τους.
4	**Προσωρινότητα των δεδομένων (data volatility)**	Μόνιμη αποθήκευση	Το πρόβλημα της διάθεσης μόνιμου αποθηκευτικού χώρου επιλύεται από την ελαστική φύση της υπολογιστικής νέφους.
5	**Ακεραιότητα των δεδομένων (data integrity)**	Εφαρμογή αλγόριθμων ελέγχου αθροίσματος (checksum algorithms), όπως για παράδειγμα οι αλγόριθμοι MD5, SHA1 SHA256	Εδώ υπάρχει έλλειψη σε κατάλληλα εργαλεία λογισμικού, στη συγκρότηση τυποποιημένων διαδικασιών, κλπ

Πίνακας 4.6. Φάση Συλλογής (Collection): Προκλήσεις και Βέλτιστες Πρακτικές [7]

Α/Α	Πρόκληση	Βέλτιστη Πρακτική	Σχόλια
1	**Αδυναμία πρόσβασης (inaccessibility)**	Απομακρυσμένη συλλογή δεδομένων	Χρήση εργαλείων επεξεργασίας δεδομένων (όπως για παράδειγμα τα EnCase, FTK Imager, X-Ways, F-Response, Paladin, κλπ) πάνω από ένα ασφαλές τηλεπικοινωνιακό κανάλι.
		Χρήση ανεξάρτητης κονσόλας διαχείρισης	Συνιστώμενη επιλογή, μιας που αποτρέπει την εξάρτηση από τον πάροχο
		Εν λειτουργία εγκληματολογία (live forensics)	Παρέχει χρήσιμες πληροφορίες του συστήματος σε λειτουργία. Τέτοιες πληροφορίες είναι – μεταξύ άλλων – η λίστα διεργασιών, οι ανοιχτές πόρτες, κα. Τέτοιου είδους πληροφορίες δεν είναι διαθέσιμες σε εγκληματολογία εκτός δικτύου (off-line forensics).
		Ανάλυση στιγμιότυπου (snapshot analysis)	Καταγραφή ολόκληρου του συστήματος σε μια δεδομένη χρονική στιγμή.
2	**Εξάρτηση από τον Πάροχο Υπηρεσιών Νέφους (Dependence on CSP)**	Χρήση ανεξάρτητης κονσόλας διαχείρισης	Συνιστώμενη επιλογή μεν, αλλά προσθέτει άλλο ένα επίπεδο εμπιστοσύνης: στην κονσόλα διαχείρισης.
		Σύναψη ισχυρών συμφωνητικών παροχής υπηρεσιών (SLAs)	Συνιστώμενη επιλογή για τους πελάτες (μισθωτές).
3	**Εφήμερη φύση των δεδομένων (ephemeral nature of data)**	Ανάλυση στιγμιότυπου (snapshot analysis)	Καταγραφή ολόκληρου του συστήματος σε μια δεδομένη χρονική στιγμή.
4	**Εμπιστοσύνη (trust) στον Πάροχο Υπηρεσιών Νέφους και τις υποδομές του**	Εφαρμογή Μοντέλου Έμπιστου Υλικού (Hardware Trust Model Platform / TPM)	Το μοντέλο αυτό έχει σχεδιαστεί για να λειτουργεί σε μεμονωμένους υπολογιστές με ένα λειτουργικό σύστημα. Δεν υποστηρίζει την κλιμάκωση, που συναντάται στα περιβάλλοντα υπολογιστικής νέφους.
		Εφαρμογή Εικονικών TPMs (Virtual TPMs)	Εικονικοί υπολογιστές με εφαρμογή μοντέλου TPM, μπορούν να δημιουργηθούν κατ' απαίτηση (on demand). Αυτό επιλύει το πρόβλημα της κλιμάκωσης.
		Εφαρμογή Μοντέλου Έμπιστου Εικονικού Περιβάλλοντος (Trusted Virtual Environment Module)	Αρθρωτή και επεκτάσιμη προσέγγιση, η οποία μάλιστα υποστηρίζει την μόνιμη αποθήκευση μυστικών κλειδιών.
		Εφαρμογή Πλατφόρμας Έμπιστης Υπολογιστικής Νέφους (Trusted Cloud Computing Platform)	Παρέχει ένα κλειστό περιβάλλον λειτουργίας εικονικών υπολογιστών. Εξασφαλίζει εμπιστευτικότητα και ακεραιότητα.
		Εφαρμογή μοντέλου Διερευνητικών Ελέγχων (Detective controls)	Συμπληρώνει το μοντέλο Προληπτικών Ελέγχων (preventive controls approach) και μπορεί να αντιμετωπίσει τον κίνδυνο που προέρχεται από το περιβάλλον του παρόχου.
5	**Πολύ-μίσθωση (multi-tenancy)**	Απομόνωση των οντοτήτων του νέφους (cloud instance isolation)	Εφαρμογή διαφόρων μεθόδων απομόνωσης οντοτήτων του νέφους.

Α/Α	Πρόκληση	Βέλτιστη Πρακτική	Σχόλια
		Εφαρμογή τεχνικής Sandboxing	Η πιο δημοφιλής μέθοδος απομόνωσης των οντοτήτων και ευρύτατα υποστηριζόμενη από τους παρόχους.
6	**Δικαιοδοσία (jurisdiction)**	Σύναψη κατάλληλου συμφωνητικού παροχής υπηρεσιών	Ο.Π.
		Διεθνής συνεργασία με τη σύναψη αμοιβαίων συμφωνιών και συνθηκών	Διεθνείς Συμφωνίες Αμοιβαίας Δικαστικής Συνδρομής (Για παράδειγμα: International Mutual Legal Assistance Treaties / MLAT)
7	**Διαγραφέντα δεδομένα (deleted data)**	Λήψη συχνών στιγμιότυπων (snapshots)	Είναι κάπως δύσκολο να εφαρμοστεί λόγω του μεγάλου όγκου που έχουν συνήθως τα στιγμιότυπα.
8	**Ελλειψη εξειδικευμένων εργαλείων εγκληματολογίας, ιδίως στο επίπεδο του hypervisor (lack of specialist commercial tools)**	Cloud Data Imager	Οι συνιστώμενες λύσεις δεν έχουν ακόμα ευρεία εμπορική κυκλοφορία.

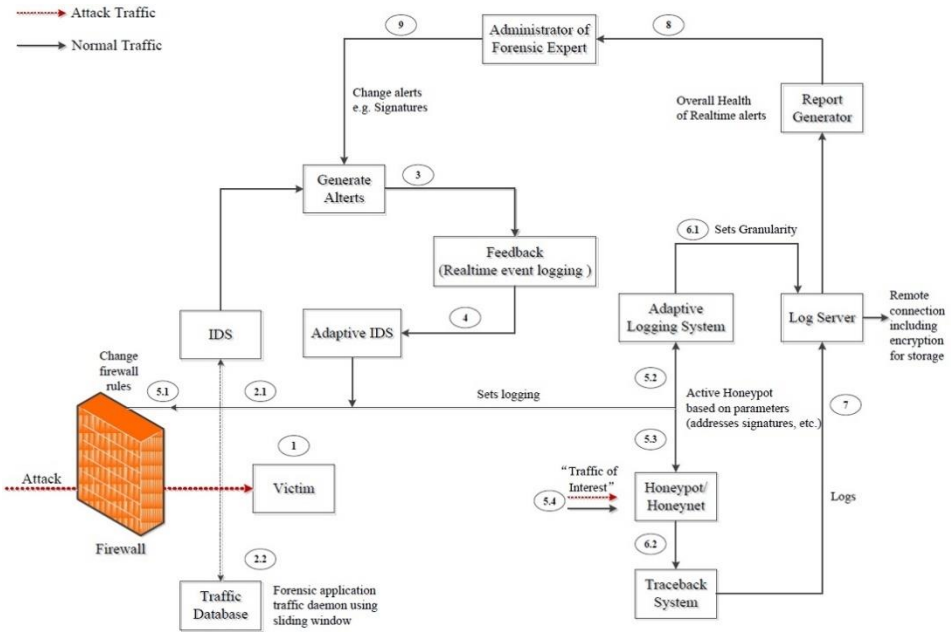
Πίνακας 4.7. Φάση Εξέτασης και Ανάλυσης (Examination and Analysis): Προκλήσεις και Βέλτιστες Πρακτικές [7]

Α/Α	Πρόκληση	Βέλτιστη Πρακτική	Σχόλια
1	**Έλλειψη ενιαίου πλαισίου για τα αρχεία καταγραφής κινήσεων (lack of log frame work)**	Χρήση εφαρμογών όπως: • Comprehensive Log Management system • Amazon AWS CloudTrail	Ένα αρχείο καταγραφής κινήσεων βοηθάει στην χρονική κατάταξη των γεγονότων και στην καλύτερη κατανόηση της υπόθεσης.
2	**Χρονική κατάταξη των αποδεικτικών στοιχείων (evidence time lining)**	Εφαρμογές σαν το Amazon AWS CloudTrail μπορούν να δώσουν κάποια αποσπασματική λύση	Η εφαρμογή Amazon AWS CloudTrail παρέχει σε UTC format πληροφορίες αναφορικά με τις προσβάσεις και διευκολύνει την χρονική αλληλουχία.
		Ασφαλή αρχεία καταγραφής κινήσεων (secure logs) με κατάλληλες χρονοσφραγίδες (time stamps)	Η σχολαστική καταγραφή στα αρχεία κινήσεων βοηθούν στον σχηματισμό της χρονικής σειράς των γεγονότων.
		Ασφαλής παρακολούθηση (secure provenance)	Παρέχει την πληροφόρηση αναφορικά με την ιδιοκτησία και την ιστορία των αντικειμένων που αφορούν δεδομένα.
3	**Κρυπτογραφημένα δεδομένα (encrypted data)**	Υποδομή διαχείρισης μυστικών κλειδιών μέσω υπολογιστικής νέφους (Cloud Key Management infrastructure)	Πιθανή μελλοντική υλοποίηση.
4	**Ενσωμάτωση των δεδομένων που αποτελούν αποδεικτικά στοιχεία (Evidence data integration)**	Η εφαρμογή AWS CloudTrail[38] υποστηρίζει κεντρική ενσωμάτωση (aggregation) αρχείων καταγραφής κινήσεων	Απαιτεί εργαλεία τρίτων (third-party) για τη διεξαγωγή επεξεργασίας και ανάλυσης.
		Σύστημα Διαχείρισης Πληροφοριών και Περιστατικών Ασφάλειας (Security Information and Event Management / SIEM) της Hewlett-Packard	Υλοποιείται με εργαλεία όπως το ArchSight.
		Καταγραφή κινήσεων των δεδομένων (data tracking)	Καταγραφή κινήσεων των δεδομένων (data tracking) χρησιμοποιώντας τεχνικές παρακολούθησης (provenance).

Πίνακας 4.8. Φάση Αναφοράς και Παρουσίασης (Reporting and Presentation): Προκλήσεις και Βέλτιστες Πρακτικές [7]

Α/Α	Πρόκληση	Βέλτιστη Πρακτική	Σχόλια
1	**Δικαιοδοσία**	Θέσπιση κατάλληλης διασυνοριακής νομοθεσίας, διαμόρφωση κατάλληλων διεθνών σχέσεων	Διεθνείς Συμφωνίες Αμοιβαίας Δικαστικής Συνδρομής (Για παράδειγμα: International Mutual Legal Assistance Treaties / MLAT)
2	**Διαφύλαξη Αλυσίδας Αποδεικτικών Στοιχείων (Chain of Custody)**	Σαφώς καθορισμένες αρχές και πρακτικές	Απολύτως απαραίτητες για την εξασφάλιση της αξιοπιστίας των αποδεικτικών μέσω.
3	**Αναδημιουργία της σκηνής του εγκλήματος (crime scene reconstruction)**	Γενικό πλαίσιο λειτουργίας, διαδικασίες και πρακτικές υποστηριζόμενα από κατάλληλα εργαλεία	Υπάρχει έλλειψη τέτοιων εργαλείων.
4	**Η πολυπλοκότητα της υπολογιστικής νέφους**	Δημιουργία της χρονικής σειράς των γεγονότων	Πάντα υπάρχει η δυσκολία της επεξήγησης της πολυπλοκότητας της υπολογιστικής νέφους στους δικαστές, εισαγγελείς και ενόρκους.
5	**Συμμόρφωση προς το κανονιστικό πλαίσιο (compliance)**	Εφαρμογή των θεσπισμένων αρχών, πολιτικών και διαδικασιών (όπως για παράδειγμα, ο Οδηγός Βέλτιστων Πρακτικών στην Ψηφιακή Εγκληματολογία της Ένωσης Αξιωματικών Αστυνομίας του Ηνωμένου Βασιλείου / ACPO	-

Επιπλέον, οι Ray Hunt και Jill Slay [6] παρουσιάζουν σε τεχνικό επίπεδο μια ενδιαφέρουσα προσέγγιση, η οποία έχει ως θέμα την επίτευξη προστασίας ΥΖΣ μέσω της αλληλεπίδρασης της ασφάλειας υπολογιστών (computer security) και της εγκληματολογίας τηλεπικοινωνιακών δικτύων (network forensics). Αναλύουν το πώς μπορούν οι δυο αυτοί κλάδοι να συνδυαστούν, ώστε τα περιστατικά ασφάλειας να εντοπίζονται και να αντιμετωπίζονται σε πραγματικό χρόνο, ενώ ταυτόχρονα να διεξάγεται εγκληματολογική διερεύνηση. Ο λόγος που καθιστά ενδιαφέρουσα την πρόταση αυτή, είναι ότι αντιμετωπίζει τα περιστατικά ασφάλειας εν τη γενέσει τους, ενώ ταυτόχρονα διεκπεραιώνει σε πραγματικό χρόνο βήματα της εγκληματολογικής διερεύνησης (τα οποία, όπως ήδη αναφέρθηκε, είναι η ταυτοποίηση του περιστατικού, η διατήρηση των τεκμηρίων με τρόπο που να μην επιτρέπει την αλλοίωσή τους, η συλλογή των δεδομένων, η επεξεργασία και η ανάλυση, και τέλος η παρουσίαση). Και ενώ σήμερα υπάρχουν πολλές λύσεις προστασίας υπολογιστών με δυνατότητες εντοπισμού περιστατικών και ενεργοποίησης ανταπάντησης (response) σε πραγματικό χρόνο, είναι δύσκολο να βρει κανείς λύσεις που να διεκπεραιώνουν βήματα της εγκληματολογικής διερεύνησης τη στιγμή της διενέργειας του περιστατικού (on-the-fly). Η προτεινόμενη από τους Ray Hunt και Jill Slay αρχιτεκτονική παρουσιάζεται στο ακόλουθο σχήμα και αποτελείται από τους εξής μηχανισμούς:



Εικόνα 4.3. Πρόταση των Hunt και Slay για σύστημα με μηχανισμό εγκληματολογικής έρευνας [6]

•Μηχανισμός **εξαπάτησης του επιτιθέμενου** (honeypot/honeynet). Ο μηχανισμός αυτός χρησιμεύει στην προσέλκυση του επιτιθέμενου σε ένα περιβάλλον που προσομοιάζει με το προστατευόμενο σύστημα, ώστε να εκδηλώσει μέσα σε αυτό την επιθετική του συμπεριφορά αποκαλύπτοντας (στους διαχειριστές του συστήματος) τον τρόπο λειτουργίας του.	• Μηχανισμός **καταγραφής** όλης της δικτυακής κίνησης (raw traffic data) με τρόπο συμμορφούμενο προς τις απαιτήσεις της εγκληματολογικής έρευνας (δηλ. αποτροπή αλλοίωσης). Ο μηχανισμός αυτός παρέχει ένα χρονικό παράθυρο ορισμένων ωρών (ή ακόμα και ημερών, ανάλογα με τις δυνατότητες και την παραμετροποίηση) για τη διερεύνηση της δικτυακής κίνησης σε περίπτωση επίθεσης.
• Μηχανισμός **αυτόματου εντοπισμού** της προέλευσης του επιτιθέμενου (traceback mechanism).	• Μηχανισμός **ασφαλούς μεταφοράς** όλων των αρχείων καταγραφής (log files) σε έναν κεντρικό εξυπηρετητή (log server).
• Μηχανισμός **αυτόματης διύλισης των πληροφορίων** που προέρχονται από τα αρχεία καταγραφής. Ο ερευνητής χρειάζεται ένα συγκεκριμένο πλήθος πληροφοριών κατάλληλων για να σχηματίσει την εικόνα της αλυσίδας των γεγονότων. Από την άλλη, σε ένα καλά προστατευμένο σύστημα, το ιδεατό είναι να καταγράφονται τα πάντα ή όσα περισσότερα είναι τεχνικά εφικτό. Συνεπώς απαιτείται ένας κατάλληλος μηχανισμός ο οποίος να εκμαιεύει από τη μεγάλα μάζα των πληροφοριών, εκείνες μόνο που απαιτούνται για να καταδειχθούν τα στοιχεία και οι λεπτομέρειες της επίθεσης.	• Μηχανισμός **αυτόματης ενεργοποίησης αντιμέτρων** (countermeasures). Ένας τέτοιος μηχανισμός θα πρέπει προφανώς να είναι πιο σύνθετος από την απλή διενέργεια κλεισίματος μιας πόρτας του firewall ή αποκλεισμού μιας εισερχόμενης διεύθυνσης ip (ip address). Αυτό συνήθως δεν είναι τόσο απλό, δεδομένου ότι πολλές συσκευές φέρονται - σύμφωνα με τους κατασκευαστές τους - να είναι αποτελεσματικές, ωστόσο εν τέλει είναι μάλλον απλοϊκές στον τρόπο λειτουργίας τους, οπότε και απαιτείται ένα ολόκληρο σύστημα για την κατάλληλη διαχείριση του firewall τη στιγμή της επίθεσης (σύστημα το οποίο, με χρήση δυνατοτήτων μηχανικής εκμάθησης και τεχνητής ευφυίας, καταφέρνει να διαχωρίσει την θεμιτή δικτυακή κίνηση από εκείνη που προκλήθηκε από την επίθεση, επιτρέποντας την πρώτη και αποκλείοντας την δεύτερη).
• Μηχανισμός **αυτόματης παραγωγής ειδοποιήσεων και αναφορών**, σε πραγματικό χρόνο, με ταυτόχρονη προστασία των αρχείων καταγραφής ώστε να καλύπτονται οι απαιτήσεις της εγκληματολογικής διερεύνησης.	

Η πρόταση αυτή των Hunt και Slay απαρτίζεται από ένα σύνολο μηχανισμών, άλλοι εκ των οποίων υπάρχουν και άλλοι όχι. Είναι ένα ιδεατό σύστημα το οποίο προστατεύει την ΥΖΣ ενώ ταυτόχρονα διεξάγει εγκληματολογική διερεύνηση, τη στιγμή της τέλεσης του εγκλήματος. Συνεπώς, η προσέγγιση αυτή είναι ίσως δύσκολο να υλοποιηθεί στο σύνολό της, δείχνει όμως μια κατεύθυνση για το πώς μπορούν να επιτευχθούν οι στόχοι που εξυπηρετεί.

Τα συστήματα προστασίας ΥΖΣ πρέπει, όπως το ανωτέρω πρότυπο, να εξασφαλίζουν την εμπιστευτικότητα, την ακεραιότητα και την διαθεσιμότητα αυτών των υποδομών, ενώ παράλληλα να συμμορφώνονται προς τις απαιτήσεις της εγκληματολογικής διερεύνησης και να διευκολύνουν την διεξαγωγή της.

Τέλος, ανάμεσα στις πιο εξελιγμένες τεχνολογίες για την διεκπεραίωση εγκληματολογικών ερευνών στο νέφος είναι η χρήση του ίδιου του νέφους (μοντέλο Forensics-as-a-Service) και η τεχνολογία blockchain. Σύμφωνα με τους R.B. van Baar, H.M.A. van Beek και E.J. van Eijk [35], το Forensics-as-a-Service είναι μια προσέγγιση η οποία βασίζεται στη χρήση υπηρεσιών νέφους για την επεξεργασία και τη διερεύνηση μεγάλου όγκου κατασχεθέντος ψηφιακού υλικού.

4.2.3 Forensics-as-a-Service

Η λύση που άρχισε να διαφαίνεται από τα πρώτα κιόλας χρόνια της εμπορικής λειτουργίας της υπολογιστικής νέφους, ήταν η χρήση της ίδιας της υπολογιστικής νέφους για τους σκοπούς εξυπηρέτησης της εγκληματολογικής έρευνας σε αυτό. Η λύση αυτή ονομάστηκε Digital-Forensics-as-a-Service (DFaaS) ή απλούστερα Forensics-as-a-Service (εφεξής αποκαλούμενο «FaaS»), και είναι ουσιαστικά ένα σκέλος του Software-as-a-Service, προσαρμοσμένο στις απαιτήσεις της εγκληματολογικής έρευνας στο νέφος. Τα πλεονεκτήματα είναι τα ακόλουθα: άμεση δυνατότητα χρήσης μεγάλου όγκου πληροφοριακών πόρων (όπως επεξεργαστική ισχύς, αποθηκευτικοί χώροι, κλπ) σε χαμηλό σχετικά κόστος και μόνο όταν είναι αναγκαίο, μείωση του χρόνου επεξεργασίας των δεδομένων της εγκληματολογικής έρευνας, λειτουργικές διευκολύνσεις σε αυτούς που διεξάγουν την έρευνα (που συνήθως είναι οι διωκτικές αρχές).

Μια μερίδα της επιστημονικής κοινότητας ασχολήθηκε εκτεταμένα με αυτή τη νέα και αποτελεσματική προσέγγιση, φωτίζοντας διάφορες πτυχές της και δίνοντας λύση στις προκλήσεις που τη συνόδευαν. Ορισμένες από τις μελέτες αυτές παρατίθενται ακολούθως.

Πίνακας 4.9. Επιστημονικές μελέτες για το μοντέλο Forensics-as-a-Service.

Επιστημονική Έρευνα	**Σχόλια - Επισημάνσεις**
Josiah Dykstra και Alan T. Sherman [36] σχετικά με τη συλλογή αποδεικτικών στοιχείων από περιβάλλον Infrastructure-as-a-Service.	• Υποστηρίζουν ότι τα παραδοσιακά εργαλεία για διεξαγωγή εγκληματολογικής διερεύνησης, όπως το EnCase και το Access Data Forensic (ADF) Toolkit, μπορούν να είναι αποτελεσματικά και για χρήση σε περιπτώσεις εγκλημάτων στο νέφος. • Κάνουν ειδική αναφορά στο μοντέλο FaaS, αναφέροντας την περίπτωση της Terremark ως ένα πάροχο ο οποίος προσέφερε αυτή την δυνατότητα εκείνη την εποχή (2012). • Επισημαίνουν ότι ο χρόνος ανταπόκρισης του παρόχου για την εξυπηρέτηση υπηρεσιών εγκληματολογίας είναι πολύ σημαντικός για την διεξαγωγή της έρευνας, αλλά αυτό το ζήτημα μπορεί να διευθετηθεί με τη σύναψη κατάλληλου συμφωνητικού παροχής υπηρεσιών.
Xiaoyu Du, Nhien-An Le-Khac και Mark Scanlon [37] σχετικά με το μοντέλο Forensics-as-a-Service.	• Διεξάγουν αξιολόγηση μοντέλων ψηφιακής εγκληματολογίας. • Επισημαίνουν ότι, το μοντέλο αυτό όχι μόνο θα επιταχύνει τη διερευνητική διαδικασία, αλλά μπορεί επίσης να οδηγήσει σε σημαντική εξοικονόμηση κόστους, διευκολύνοντας τους ερευνητές εγκληματολογίας αλλά και τις διωκτικές αρχές στη διεκπεραίωση της εργασίας τους. • Αναλύουν τα πλεονεκτήματα του μοντέλου Faas, τα οποία είναι: ✓ μεγάλη (σχεδόν απεριόριστη από τεχνικής πλευράς) επεξεργαστική ισχύς της υπολογιστικής νέφους, ✓ δυνατότητα άμεσης προσαρμογής αυτού του μοντέλου εγκληματολογίας (του FaaS) στις νέες τάσεις της υπολογιστικής νέφους. ✓ δυνατότητα αποθήκευσης των αποτελεσμάτων κάθε εξιχνιαζόμενης υπόθεσης, με σκοπό τη χρήση τους ως πηγή μηχανικής εκμάθησης και βελτίωσης του λογισμικού αυτής της υπηρεσίας.
R.B. van Baar, H.M.A. van Beek και E.J. van Eijk [35] σχετικά με το μοντέλο Forensics-as-a-Service.	• Αναλύουν τη διαδικασία εγκληματολογικής διερεύνησης και τους παράγοντες που την δυσχεραίνουν. • Εξηγούν το πώς θα μπορούσαν τα προβλήματα αυτά να αντιμετωπιστούν, ώστε να επιτευχθεί αύξηση της ταχύτητας και της αποτελεσματικότητας της εγκληματολογικής διερεύνησης. • Φέρνουν ως παράδειγμα μια περίπτωση χρήσης της υπηρεσίας FaaS στην Ολλανδία, η οποία ονομαζόταν XIRAF και υιοθετήθηκε χιλιάδες πλέον ερευνητές εγκληματολογίας. • Αναφέρουν και τα μειονεκτήματα αυτής της υπηρεσίας, τα οποία είναι: ✓ καθυστερήσεις στη λειτουργία της υπηρεσίας (latency), ✓ συνεχής εξάρτηση από τη σύνδεση στο διαδίκτυο, ✓ χρήση των αποθηκευμένων δεδομένων σε άλλες εφαρμογές. • Σημειώνουν ότι οι μελλοντικές υλοποιήσεις αυτής της υπηρεσίας θα πρέπει να βρουν τρόπους να αντιμετωπίσουν αυτά τα μειονεκτήματα.
van Beek et al. [38] σχετικά με την υπηρεσία FaaS "HANSKEN".	1. Εστιάζουν στην σωστή σχεδίαση υπηρεσιών FaaS με βάση οκτώ αρχές: 1. την ασφάλεια, 2. την ιδιωτικότητα, 3. την διαφάνεια, 4. την υποστήριξη πολυ-μίσθωσης (multi-tenancy), 5. την δυνατότητα μελλοντικών επεκτάσεων, 6. την διαφύλαξη της ακεραιότητας των δεδομένων, 7. την αξιοπιστία και 8. την υψηλή διαθεσιμότητα.

Επιστημονική Έρευνα	Σχόλια - Επισημάνσεις
	2. Παραθέτουν σωρεία από τεχνικές προδιαγραφές που τους απασχόλησαν κατά τη σχεδίαση αυτής της υπηρεσίας, όπως: 1. η επαναχρησιμοποίηση γνώσης από εγκληματολογικές διερευνήσεις, 2. η διανομή αποδεικτικών στοιχείων που εντοπίστηκαν στα τεκμήρια, 3. η διαχείριση κλειδιών κρυπτογράφησης, 4. η διαχείριση χρηστών και προσβάσεων, και πολλά άλλα. 3. Αυτές οι τεχνικές προδιαγραφές μπορούν κάλλιστα να χρησιμοποιηθούν ως κριτήρια αξιολόγησης υπηρεσιών FaaS.
Jooyoung Lee και Sungyong Un [39] σχετικά με μια λύση ευρετηριακής αναζήτησης ως υπηρεσία (Indexed-Search-as-a-Service).	• Επισημαίνουν ότι, στην εποχή των Big Data, οι συμβατικές υποδομές ψηφιακής εγκληματολογίας δεν μπορούν να αποδώσουν, δεδομένου ότι έχουν πεπερασμένες δυνατότητες. • Καταδεικνύουν τη λύση του FaaS ως τη μόνη ρεαλιστική για την επεξεργασία μεγάλου όγκου δεδομένων εγκληματολογικών ερευνών. • Επικεντρώνονται στη λύση ευρετηριακής αναζήτησης ως υπηρεσία (Indexed-Search-as-a-Service), την οποία σχεδίασαν οι ίδιοι με σκοπό την επιτάχυνση της ψηφιακής εγκληματολογικής διαδικασίας, μέσω της γρήγορης αναζήτησης εννοιών, ψηφιακών τεκμηρίων, προτύπων και λέξεων κλειδιών, σε ένα σύστημα ψηφιακής εγκληματολογίας. • Εφάρμοσαν τη λύση αυτή σε ένα σύστημα κατανεμημένης αποθήκευσης Apache Hadoop, με χρήση της τεχνικής MapReduce, εφαρμοζόμενη σε πολυδιάστατη (μη-σχεσιακή) βάση δεδομένων Hbase, ώστε να εξασφαλίσουν τη μέγιστη δυνατή απόδοση μέσω της παράλληλης επεξεργασίας των αναζητήσεων. • Αποδεικνύουν με μετρήσεις και γραφήματα ότι η δική τους μέθοδος αναζήτησης διεκπεραιώνεται στο μισό περίπου χρόνο, σε σχέση με συμβατικές (μη παράλληλες) μεθόδους αναζήτησης, • Αφήνουν κατά μέρος τα ζητήματα ασφάλειας για μελλοντική διερεύνηση.
Yuanfeng Wen, Xiaoxi Man, Khoa Le και Weidong Shi [40] σχετικά με δική τους λύση για την αντιμετώπιση θεμάτων του FaaS, διαχειριστικής κυρίως φύσεως.	• Καταδεικνύουντας τη λύση της υπολογιστικής νέφους ως τη μόνη ρεαλιστική μέθοδο για επεξεργασία μεγάλου όγκου δεδομένων εγκληματολογικών ερευνών. • Παρουσιάζουν τη δική τους λύση για την αντιμετώπιση διαφόρων θεμάτων του FaaS, διαχειριστικής κυρίως φύσεως, όπως η δυσκολία κατανόησης του τρόπου λειτουργίας των εργαλείων εγκληματολογικής διερεύνησης, η έλλειψη εμπειρίας στην παραμετροποίησή τους, η έλλειψη διαλειτουργικότητας στα λογισμικά επεξεργασίας δεδομένων εγκληματολογικών ερευνών, η επεξεργασία μεγάλου όγκου δεδομένων και η δυσκολία δημιουργίας και παραμετροποίησης ροών εργασιών επεξεργασίας δεδομένων εγκληματολογικών ερευνών (forensic data processing workflows). • Λειτουργούν την πλατφόρμα τους σε ένα σύστημα κατανεμημένης αποθήκευσης Apache Hadoop, με χρήση της τεχνικής MapReduce, εφαρμοζόμενη σε πολυδιάστατη (μη-σχεσιακή) βάση δεδομένων Hbase. • Τα πειραματικά τους αποτελέσματα κατέδειξαν σημαντική βελτίωση του χρόνου επεξεργασίας δεδομένων εγκληματολογικών ερευνών, της τάξης του 71%. • Το σκέλος της πλατφόρμας τους που αφορούσε τη διαχείριση ροών εργασιών επεξεργασίας δεδομένων εγκληματολογικών ερευνών (forensic data processing workflows), κατέδειξε αντίστοιχα

Επιστημονική Έρευνα	Σχόλια - Επισημάνσεις
	αποτελέσματα στην εξοικονόμηση χρόνου, της τάξεως του 87%. • Οι επιδόσεις αυτές, οι οποίες οφείλονται κατά κύριο λόγο στην τεχνική παράλληλης επεξεργασίας, διευκολύνουν την διεξαγωγή εγκληματολογικών ερευνών, αφού εξοικονομούν πολύτιμο χρόνο επεξεργασίας δεδομένων προς όφελος των ερευνητών αλλά και βελτίωση της ταχύτητας εξιχνίασης των εγκλημάτων.

4.2.4 Προστασία των Αρχείων Καταγραφής Κινήσεων (Logs)

Ειδική αναφορά χρειάζεται να γίνει σε ένα ιδιαίτερα ευαίσθητο θέμα: την προστασία των αρχείων καταγραφής κινήσεων (logs). Όπως έχει ήδη τονιστεί, τα logs αποτελούν σημαντικό μέρος της ψηφιακής εγκληματολογικής έρευνας (ίσως και το μεγαλύτερο, μαζί με την εξέταση των εικονικών μηχανών και των σκληρών δίσκων), οπότε και τα στοιχεία που αντλούνται από αυτά, πρέπει να παραμένουν άθικτα ως τη στιγμή της παρουσίαση τους ενώπιον των δικαστών και των ενόρκων. Επιπρόσθετα, πρέπει να είναι τεχνικά εφικτή η απόδειξη, ενώπιον των δικαστικών αρχών, ότι τα στοιχεία αυτά παρέμειναν άθικτα (αναλλοίωτα). Για τον λόγο αυτό, έχει δοθεί ιδιαίτερη προσοχή στο θέμα της διαφύλαξης της ακεραιότητας των logs και μάλιστα με τρόπο τέτοιο, που να μην επιδέχεται την παραμικρή αμφισβήτηση. Προσεγγίσεις όπως αυτή των Sagar Rane και Arati Dixit [41] με τη χρήση της τεχνολογίας Blockchain, και εκείνη των Syed Ahmed et al. [42] τη μέθοδο CLASS (Cloud Log Assuring Soundness and Secrecy), δίνουν αποτελεσματικές λύσεις και μπορούν να θεωρηθούν εξαιρετικές πρακτικές για το συγκεκριμένο ζήτημα.

4.3 Αξιολόγηση συστημάτων ΥΖΣ που λειτουργούν στο νέφος για την υποστήριξη της Εγκληματολογικής Έρευνας

Ένας σημαντικός παράγοντας για την αξιολόγηση συστημάτων υποδομών ζωτικής σημασίας που λειτουργούν στο νέφος, ως προς το σκέλος της υποστήριξης που παρέχουν στη διεξαγωγή εγκληματολογικής έρευνας, είναι το κατά πόσο συμμορφώνονται με πρότυπα των διωκτικών και των εποπτικών ανά κλάδο Αρχών. Αυτό είναι απολύτως λογικό, αφού στις περισσότερες περιπτώσεις (αν όχι σε όλες) τα συστήματα αυτά έχουν φτιαχτεί από ιδιώτες και λειτουργούν σε υποδομές ιδιωτών. Από την άλλη πλευρά, οι φορείς που διεξάγουν εγκληματολογικές έρευνες είναι διωκτικές αρχές, εισαγγελικές αρχές, εποπτικές αρχές διαφόρων κλάδων και γενικά υπηρεσίες κρατών ή οργανισμών κρατών με αρμοδιότητες που σχετίζονται με την επιβολή του νόμου. Συνεπώς, για να καταστεί εφικτή η συνεργασία ανάμεσα στις δυο αυτές πλευρές, πρέπει να υπάρχουν διαδικασίες, τεχνικές και υποδομές που να εξασφαλίζουν την εμπιστοσύνη της μιας πλευράς προς την άλλη. Αυτόν τον ρόλο διαδραματίζουν τα πρότυπα. Δεν είναι τίποτε άλλο από ένα σύνολο

προδιαγραφών που η απαράμιλλη τήρηση και εφαρμογή τους επιφέρει την εμπιστοσύνη ανάμεσα στις δυο πλευρές.

Για την περίπτωση των ΥΖΣ που λειτουργούν στο νέφος, τα πρότυπα τα θέτουν συνήθως οι κρατικές αρχές και καλούνται να τις εφαρμόσουν όσοι συμμετέχουν στη λειτουργία αυτών των συστημάτων στο νέφος (πχ. πάροχοι υπηρεσιών νέφους, κατασκευαστές λογισμικού, πάροχοι τηλεπικοινωνιακών υπηρεσιών, κα.).

Ένα ξεκάθαρο παράδειγμα, είναι η περίπτωση του συστήματος «Ερευνητική Πλατφόρμα Εφαρμογής Νόμου» (Law Enforcement Investigative Platform / LEIP) της IBM, που ήδη αναφέρθηκε. Αν το σύστημα αυτό δεν είχε συμμορφωθεί προς συγκεκριμένα πρότυπα των διωκτικών και κρατικών αρχών, δεν θα είχε κάποια ιδιαίτερη αποτελεσματικότητα – πιθανά να ήταν απλώς ένα ισχυρό σύστημα επεξεργασίας δεδομένων. Από τη στιγμή όμως που φέρει τις συγκεκριμένες πιστοποιήσεις, επιτυγχάνει την εμπιστοσύνη εκ μέρους των αμερικανικών αρχών, οπότε και μπορεί να προσπελάσει διαπιστευμένους πληροφοριακούς πόρους, στους οποίους μόνο οι ίδιες οι αρχές είχαν πρόσβαση.

Παρακάτω, επιχειρείται μια επισκόπηση του τοπίου αυτού. Αρχικά ερευνώνται οι φορείς που είναι επιφορτισμένοι με την προστασία συγκεκριμένων ΥΖΣ. Άλλωστε αυτοί συνήθως εκδίδουν και τα πρότυπα προς τα οποία πρέπει να συμμορφώνονται τα συστήματα. Οι τομείς που εξετάζονται είναι η **άμυνα**, η **οικονομία** και η **υγεία**. Στη συνέχεια, η έρευνα στρέφεται στο λογισμικό που χρησιμοποιείται από αυτούς τους κλάδους στο χώρο της υπολογιστικής νέφους. Στο τέλος, διεξάγεται επισκόπηση και αξιολόγηση εφαρμογών εγκληματολογικής έρευνας που λειτουργούν στο ίδιο νέφος (στον ίδιο πάροχο) ώστε να καταδειχθεί το κατά πόσο θα ήταν αποτελεσματική η διεξαγωγή εγκληματολογικής έρευνας σε περίπτωση επίθεσης σε βάρος κάποιου (ή κάποιων) από αυτών των συστημάτων. Στους μεγάλους παρόχους νέφους δεν υπάρχει άλλο ειδικό λογισμικό για εγκληματολογική έρευνα πέραν αυτού της IBM (του IBM LEIP). Για τον λόγο αυτό, παρατίθενται όσα εργαλεία μπορούν να χρησιμοποιηθούν για την διεξαγωγή εγκληματολογικής έρευνας.

Η μελέτη επικεντρώνεται στον χώρο των ΗΠΑ και ο πάροχος υπηρεσιών νέφους που εξετάζεται είναι η Amazon Web Services (AWS). Η επιλογή του συγκεκριμένου χώρου και του συγκεκριμένου παρόχου δεν είναι τυχαία. Καθόσον επιδιώκεται η εξέταση των συστημάτων υποδομών ζωτικής σημασίας και άλλων γεωγραφικών περιοχών, όπως προκύπτει από έρευνες, ο συγκεκριμένος πάροχος είναι κυρίαρχος και στην Ευρωπαϊκή Ένωση, ενώ φέρεται να έχει σημαντικό ποσοστό της αγοράς νέφους και στη Ρωσία (προς το παρόν).

4.3.1 Θεσμικό Πλαίσιο

Άμυνα

Το αμερικανικό Υπουργείο Άμυνας εστιάζει όλο και περισσότερο στα θέματα κυβερνοασφάλειας. Ισχυρή ένδειξη αυτού είναι το καινούργιο (Μάρτιος 2020) πρότυπο που ονομάζεται «**Πιστοποίηση Μοντέλου Ωριμότητας Κυβερνοασφάλειας**» (Cybersecurity Maturity Model Certification / CMMC) [43], το οποίο για θέματα εγκληματολογικής έρευνας προβλέπει: *«Για περιστατικά στον κυβερνοχώρο, (απαιτείται) συλλογή εγκληματολογικών δεδομένων από συστήματα που επηρεάζονται, κατοχυρώνοντας ασφαλή μεταφορά και προστασία των εγκληματολογικών δεδομένων.»*. Μια άλλη ισχυρή ένδειξη είναι η σύνταξη Οδηγού Απαιτήσεων Ασφαλείας Υπολογιστικής Νέφους ("Cloud Computing Security Requirements Guide" / CCSRG)[10].

Οι απαιτήσεις αυτές επηρεάζουν τους παγκόσμιους παρόχους υπηρεσιών νέφους (AWS, Microsoft, Google, κλπ) διότι είναι προμηθευτές υπηρεσιών προς το αμερικανικό υπουργείο άμυνας (DoD), όπως θα καταδειχθεί αναλυτικά κατωτέρω.

Οικονομία

Η γενική εποπτεία του τομέα πληροφορικής στις ΗΠΑ, υπάγεται στο Γραφείο Διαχείρισης και Προϋπολογισμού (Office of Management and Budget / OMB) του Προεδρικού Γραφείου των ΗΠΑ. Αυτός είναι ο φορέας έκδοσης του πιστοποιητικού «FedRAMP» (Ομοσπονδιακό Πρόγραμμα Διαχείρισης Κινδύνων και Εξουσιοδοτήσεων - Federal Risk and Authorization Management Program / FedRAMP), ένα από τα βασικά πιστοποιητικά των ΗΠΑ, για τη σύναψη συνεργασιών ανάμεσα σε υπηρεσίες της ομοσπονδιακής κυβέρνησης και τρίτους στον χώρο της πληροφορικής. Αναφορικά με το αντικείμενο της καταπολέμησης του κυβερνοεγκλήματος, αρμόδια υπηρεσία είναι ο «Οργανισμός Κυβερνοασφάλειας και Προστασίας Υποδομών» ("Cybersecurity and Infrastructure Security Agency" / CISA) [44], ενώ ειδικά για την καταπολέμηση του κυβερνοεγκλήματος στο αμερικανικό οικονομικό οικοσύστημα, αρμόδιες υπηρεσίες είναι το «Γραφείο Κυβερνοασφάλειας και Προστασίας Κρίσιμων Υποδομών» (The Office of Cybersecurity and Critical Infrastructure Protection)[11], το οποίο υπάγεται στο Γραφείο Χρηματοπιστωτικών Ιδρυμάτων ("Office of Financial Institutions") του Υπουργείου Οικονομικών (U.S. Department of the Treasurty / USDT) και οι

[10] U.S. Department of Defense / Defense Information Systems Agency, 2017. Department Of Defense Cloud Computing Security Requirements Guide - Version 1, Release 3.
[11] https://home.treasury.gov/about/offices/domestic-finance/financial-institutions

Μυστικές Υπηρεσίες (U.S. Secret Service)[12]. Οι δυο τελευταίες αυτές υπηρεσίες, δεν έχουν θεσπίσει κάποιο συγκεκριμένο πιστοποιητικό κυβερνοασφάλειας, αλλά σύμφωνα με τον Προϋπολογισμό Οικονομικού Έτους 2021 του Υπουργείου Οικονομικών (USDT), χρησιμοποιούν το (γενικότερο) Πλαίσιο Κυβερνοασφάλειας του Εθνικού Ινστιτούτου Προτύπων και Τεχνολογίας (National Institute of Standards and Technology's Cybersecurity Framework) [45].

Σύμφωνα με το κείμενο αυτό (τον Προϋπολογισμό του 2021), ενώ στις προηγούμενες υποβολές του προϋπολογισμού, το Υπουργείο Οικονομικών περιλάμβανε πρωτοβουλίες που οργανώθηκαν γύρω από συγκεκριμένες επενδύσεις στον χώρο της κυβερνοασφάλειας (π.χ. περιουσιακά στοιχεία υψηλής αξίας), ο προϋπολογισμός του έτους 2021 οργανώνεται αντ' αυτού γύρω από βέλτιστες πρακτικές και αποτελέσματα της κυβερνοασφάλειας που έχουν χρήση σε ολόκληρο τον κλάδο: Προσδιορισμός, προστασία, εντοπισμός, ανταπόκριση, και ανάκτηση. Υιοθετώντας αυτή τη μεθοδολογία, ο στόχος του Υπουργείου Οικονομικών είναι να παρέχει σαφέστερη εικόνα για τις επενδύσεις που αφορούν τον στρατηγικό τομέα της κυβερνοασφάλειας, να ευθυγραμμιστεί με τα αποδεκτά βιομηχανικά πρότυπα, οδηγίες και βέλτιστες πρακτικές και να διευκολύνει το Υπουργείο Οικονομικών στο να παρακολουθεί αποτελεσματικότερα τις απαιτήσεις αναφορών της ομοσπονδιακής κυβέρνησης.

Υγεία

Το έτος 2016, ο Τομέας Ανθεκτικότητας του Γραφείου Υγείας και Ανθρωπίνων Υπηρεσιών έθεσε υπό την αιγίδα του την πρωτοβουλία δημιουργίας μιας Ειδικής Ομάδας για την Κυβερνοασφάλεια στη Βιομηχανία Υγείας (Health Care Industry Cybersecurity Task Force). Την επόμενη χρονιά, η Ειδική Ομάδα για την Κυβερνοασφάλεια στη Βιομηχανία Υγείας κατέθεσε στη Γερουσία και στη Βουλή των Αντιπροσώπων μια αναφορά με τίτλο «Αναφορά για τη Βελτίωση της Κυβερνοασφάλειας στη Βιομηχανία Υγείας» ("Report On Improving Cybersecurity In The Health Care Industry") [46]. Οι συζητήσεις αυτής της Ειδικής Ομάδας οδήγησαν στην ανάπτυξη έξι απαιτήσεων για τη βελτίωση της κυβερνοασφάλειας στη βιομηχανία υγείας των ΗΠΑ, μαζί με συνοδευτικές συστάσεις και στοιχεία δράσης. Στη δεύτερη απαίτηση, η οποία σχετίζεται με την αναβάθμιση της ασφάλειας και της ανθεκτικότητας στις ιατρικές συσκευές και στην πληροφορική της υγείας, υπάρχει ρητή αναφορά στην ανάγκη ανάπτυξης της ψηφιακής εγκληματολογίας και προστασίας των αρχείων καταγραφής, η οποία έχει ως ακολούθως: «Η βιομηχανία (υγείας) πρέπει να

[12] https://www.secretservice.gov/investigation/#cyber

οικοδομήσει και να προβλέψει την ανάγκη για εγκληματολογία πληροφορικής που να συνοδεύει τις έρευνες για ανεπιθύμητα συμβάντα διασφαλίζοντας ότι τα αρχεία καταγραφής υπάρχουν και είναι προσβάσιμα». Η αναφορά αυτή, προτείνει βέλτιστες πρακτικές για την αναβάθμιση της κυβερνοασφάλειας σε αυτόν τον τομέα (δηλ. της υγείας), μεταξύ των οποίων είναι και η βελτίωση της επικοινωνίας και της συνεργασίας τόσο εντός του συγκεκριμένου τομέα, όσο και σε σχέση με άλλους τομείς υποδομών ζωτικής σημασίας. Αυτό ευνοεί την καλύτερη αντιμετώπιση περιστατικών ασφάλειας και διευκολύνει την ανάπτυξη εγκληματολογικών ερευνών.

Τα ευρήματα που αφορούν την Amazon Web Services (AWS), τόσο σε σχέση με τις προδιαγραφές φιλοξενίας υποδομών ζωτικής σημασίας (πχ. πιστοποιήσεις, κλπ), όσο και σε σχέση με τα εργαλεία διεξαγωγής εγκληματολογικών ερευνών, παρατίθενται στο Παράρτημα της παρούσας μελέτης. Εκεί επίσης παρατίθενται και τα εργαλεία ανάγνωσης και διαχείρισης αρχείων καταγραφής κινήσεων (logs) άλλων μεγάλων παρόχων νέφους.

Θα πρέπει τέλος να επισημανθεί ότι η αποτελεσματική διεξαγωγή εγκληματολογικών ερευνών στο νέφος είναι μια υπόθεση που υπερβαίνει κατά πολύ τη χρήση ενός καλού συστήματος συλλογής και επεξεργασίας δεδομένων από αρχεία καταγραφής κινήσεων. Είναι μια διαδικασία με μεγαλύτερες απαιτήσεις, οι οποίες, όπως καταδείχθηκε, αφορούν τόσο το θεσμικό όσο και το τεχνικό πλαίσιο.

Όσον αφορά το θεσμικό πλαίσιο, σημαντικοί παράγοντες υποστήριξης της εγκληματολογικής έρευνας αλλά και διεξαγωγής διώξεων είναι κυρίως οι διεθνείς συμβάσεις και οι διμερείς συμφωνίες αμοιβαίας δικαστικής συνδρομής, ανάμεσα σε χώρες που φιλοξενούν υποδομές υπολογιστικής νέφους.

Όσον αφορά το τεχνικό πλαίσιο, ιδιαίτερο ρόλο διαδραματίζουν οι πιστοποιήσεις που φέρει ο εκάστοτε πάροχος υπηρεσιών νέφους και κυρίως εκείνες που αποτελούν πλαίσιο προδιαγραφών για προσπέλαση πληροφοριακών πόρων κρατών και διωκτικών αρχών. Εξαιρετικά σημαντικό είναι επίσης και το επίπεδο ωριμότητας της υποδομής ασφάλειας της κάθε εφαρμογής και του κάθε συστήματος που λειτουργεί στο νέφος, όπως επίσης και η συμμόρφωσή τους προς τα πρότυπα που έχουν θεσπιστεί ανά χώρα, ευρύτερη περιοχή ή κλάδο της αγοράς. Τέλος, στο θέμα της εξεύρεσης της σειράς των γεγονότων που προκάλεσαν μια εγκληματική πράξη, σημαντικότεροι παράγοντες είναι: α) η τήρηση των βημάτων της εγκληματολογίας, όπως αυτά παρατέθηκαν, β) η χρήση αποτελεσματικών εργαλείων, κυρίως δε αυτών που παρέχουν οι πάροχοι νέφους, λόγω των εξελιγμένων χαρακτηριστικών τους και της δυνατότητας αξιοποίησης απεριόριστων πόρων του νέφους.

Κεφάλαιο 5 - Περιπτώσεις επιθέσεων σε Υποδομές Ζωτικής Σημασίας στο νέφος

5.1 Μεθοδολογία

Η μεθοδολογία που ακολουθείται έχει ως ακολούθως:

- Παράθεση περιστατικών ασφάλειας σε βάρος συστημάτων ΥΖΣ για κάθε μια από τις γεωγραφικές περιοχές που εξετάζονται στην παρούσα μελέτη: ΗΠΑ, ΕΕ και Ρωσία.
- Για κάθε γεωγραφική περιοχή, τα περιστατικά χωρίζονται στις τρεις κατηγορίες που διερευνώνται: Άμυνα, Οικονομία, Υγεία.
- Για κάθε περιστατικό παρατίθεται μια σύντομη περιγραφή, η υπηρεσία νέφους που επηρεάστηκε, η αποτελεσματικότητα της εγκληματολογικής έρευνας (αν βρέθηκε ο υπαίτιος σε επίπεδο φυσικού προσώπου) και κάποια βασικά σχόλια.
- Τέλος, διατυπώνονται κάποια συμπεράσματα για την εγκληματολογική έρευνα τόσο των συγκεκριμένων περιστατικών, όσο και γενικά. Τα συμπεράσματα αυτά αφορούν και τις επιπτώσεις των περιστατικών στη λειτουργία Υποδομών Ζωτικής Σημασίας.

5.2 Περιπτώσεις επιθέσεων σε βάρος συστημάτων ΥΖΣ στο νέφος

Περιστατικά ασφάλειας στο χώρο των υπολογιστών συμβαίνουν συνέχεια, επιφέροντας επιπτώσεις στα διάφορα θύματα – φυσικά πρόσωπα, αλλά ακόμα και σε Υποδομές Ζωτικής Σημασίας. Όμως δεν αφορούν όλα την υπολογιστική νέφους. Στις σελίδες που ακολουθούν επιχειρείται η ανάλυση περιστατικών ασφάλειας που έλαβαν χώρα στο νέφος, οι επιπτώσεις που είχαν σε υποδομές ζωτικής σημασίας, αλλά και οι ιδιαιτερότητες που αναδείχθηκαν κατά την εγκληματολογική έρευνα.

5.2.1 Ηνωμένες Πολιτείες Αμερικής

Πίνακας 5.1. Επιθέσεις σε υπηρεσίες νέφους που επηρέασαν ΥΖΣ των ΗΠΑ.

Τομέας	Περιστα-τικό	Επηρεαζόμενη υπηρεσία νέφους	Περιγραφή	Εντοπίστηκε ο δράστης (φυσικό πρόσωπο)	Σχόλια
Άμυνα	Docker Hub [13] [14] [15]	Docker Hub	Απρίλιος 2019 -Εισβολείς άγνωστης εθνικότητας υπέκλεψαν τους κωδικούς πρόσβασης από 190.000 χρήστες της συγκεκριμένης υπηρεσίας νέφους.	Όχι	Η συγκεκριμένη υπηρεσία χρησιμοποιείται και από το Αμερικανικό Υπουργείο Άμυνας (Department of Defense) [47].
Οικονομία	Capital One [48] [16]	Amazon Web Services	Ιούλιος 2019 – Ένα φυσικό πρόσωπο, υπέκλεψε προσωπικά δεδομένα και αριθμούς πιστωτικών καρτών 106 εκατομμυρίων πελατών της συγκεκριμένης τράπεζας, οι οποίοι είχαν υποβάλλει αιτήματα για χορήγηση πιστωτικής κάρτας.	Ναι.	Το FBI συνέλαβε αυτό το φυσικό πρόσωπο και ασκήθηκε ποινική δίωξη. Σύμφωνα με το κατηγορητήριο, το πρόσωπο αυτό έφτιαξε ένα μηχανισμό που έψαχνε στο νέφος για servers με κακή παραμετροποίηση, έτσι ώστε να μπορεί μέσω αυτών να υποκλέψει κωδικούς πρόσβασης, αλλά και να τους εκμεταλλευτεί για εξόρυξη κρυπτονομισμάτων.Η επίθεση βασίστηκε σε κακή παραμετροποίηση application firewalls πελατών της AWS. Ο όγκος των ψηφιακών τεκμηρίων είναι περίπου 30 TB (σύμφωνα με τις εισαγγελικές αρχές). Η δίκη διεκόπη λόγω της πανδημίας Covid-19.
Υγεία	AMCA data breach [49]	Optum 360	Ιούνιος 2019 – Άγνωστοι εισβολείς υπέκλεψαν προσωπικά, οικονομικά και ιατρικά δεδομένα 12 εκατομμυρίων ανθρώπων. Η εταιρεία AMCA ήταν εισπρακτική και διαχειριζόταν τις εισπράξεις των μεγαλύτερων διαγνωστικών κέντρων των ΗΠΑ, όπως – μεταξύ άλλων - η Quest Diagnostics και η LabCorp (Laboratory Corporation of America) [50].	Όχι	Το περιστατικό είχε διάρκεια από την 1η Αυγούστου 2018 ως και την 30η Μαρτίου 2019. Έλαβε χώρα στο σύστημα ηλεκτρονικών πληρωμών της αμερικανικής εταιρείας American Medical Collection Agency (AMCA), το οποίο λειτουργούσε στο νέφος της εταιρείας Optum[17].

[13] https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/docker-hub-repository-suffers-data-breach-190-000-users-potentially-affected

[14] https://www.zdnet.com/article/docker-hub-hack-exposed-data-of-190000-users/

[15] https://thenewstack.io/docker-hub-compromised-users-urged-to-reset/

[16] https://www.capitalone.com/facts2019/

[17] UNTANGLE, INC., 2019. HEALTHCARE DATA BREACH: MITM ATTACK TARGETS QUEST DIAGNOSTICS PATIENT INFORMATION.

5.2.2 Ευρωπαϊκή Ένωση

Πίνακας 5.2. Επιθέσεις σε υπηρεσίες νέφους που επηρέασαν ΥΖΣ στον χώρο της ΕΕ.

Τομέας	Περιστα-τικό	Επηρεαζόμενη υπηρεσία νέφους	Περιγραφή	Εντοπίστηκε ο δράστης (φυσικό πρόσωπο)	Σχόλια
Άμυνα	Turkish DNS-Hijacking[18]	Cloud storage credentials	Ιανουάριος 2020 -Εισβολείς, που φέρονταν να λειτουργούσαν για λογαριασμό της τουρκικής κυβέρνησης, επιτέθηκαν σε οργανισμούς στην Ευρώπη και τη Μέση Ανατολή, συμπεριλαμβανομένων κυβερνητικών υπουργείων, πρεσβειών, υπηρεσιών ασφαλείας και εταιρειών, υποκλέπτοντας, μεταξύ άλλων, κωδικούς πρόσβασης σε υπηρεσίες αποθήκευσης στο νέφος[19].	Όχι	Η επίθεση συνέβαινε από το 2018 ως τον Ιανουάριο του 2020. Οι εισβολές βασίστηκαν στην τεχνική DNS Hijacking με βάση την οποία προκαλείται μη εξουσιοδοτημένη τροποποίηση των εγγραφών του συστήματος Domain Name Service (DNS), που υλοποιεί την αντιστοίχιση ονομάτων χώρου με διευθύνσεις εξυπηρετητών. Ως αποτέλεσμα αυτής της τροποποίησης, τα θύματα της επίθεσης διοδεύονταν σε ψεύτικους εξυπηρετητές (που ανήκαν στους εισβολείς), πληκτρολογώντας σε αυτούς κωδικούς πρόσβασης για διάφορες υπηρεσίες νέφους, όπως email, υπηρεσίες αποθήκευσης, κα. Οι βασικότεροι στόχοι ήταν κυβερνητικές υποδομές σε Ελλάδα, Κύπρο, Ιράκ, Αλβανία, αλλά και κάποιοι οργανισμοί της Τουρκίας.
Οικονομία	Operation Cloud Hopper[18]	Managed IT Services διαφόρων παρόχων (μεταξύ αυτών οι IBM και HP Enterprise)[20] [21]	Απρίλιος 2017 – Ομάδα εισβολέων από την Κίνα χρησιμοποίησαν το νέφος διαφόρων παρόχων για να εισβάλλουν στις υποδομές των πελατών τους και να παραμείνουν σε αυτές για εκτεταμένο χρονικό διάστημα[22]. Μεγάλο πλήθος εταιρειών επλήγησαν από αυτήν την επίθεση, πολλές από αυτές στην ΕΕ[21].	Ναι. Πρόκειται για την ομάδα APT10, γνωστή και από προηγούμενες επιθέσεις. Δυο από τα μέλη της έχουν επικηρυχθεί από το FBI.	Κατά τη διάρκεια της επίθεσης, οι εισβολείς υπέκλεψαν, μέσω των παρόχων νέφους, εταιρικά δεδομένα και μυστικές εμπορικές συμφωνίες τόσο από τους παρόχους όσο και από τα τελικά θύματα, δηλαδή τους πελάτες τους. Μάλιστα, σύμφωνα με έρευνα του Reuters, οι εισβολείς πέτυχαν πλήρη έλεγχο στο εταιρικό δίκτυο ενός εκ των παρόχων (της HP Enterprise), αφήνοντας και μηνύματα που κορόιδευαν τους διαχειριστές του συστήματος.
Υγεία	-[23] [24]	-	-	-	-

[18] Center for Strategic and International Studies (CSIS), 2020. Significant Cyber Incidents Since 2006.

[19] https://www.reuters.com/article/us-cyber-attack-hijack-exclusive-idUSKBN1ZQ10X

[20] https://www.reuters.com/investigates/special-report/china-cyber-cloudhopper/

[21] PWC in collaboration with BAE Systems, 2017. Operation Cloud Hopper.

[22] Trend Micro Incorporated, 2017. Operation Cloud Hopper: What You Need Know.

[23] Στον χώρο της ΕΕ και ειδικότερα στον τομέα της Υγείας έχουν συμβεί πληθώρα περιστατικών ασφάλειας. Μάλιστα, σύμφωνα με έρευνα της ENISA [51], το πλήθος αυτών των επιθέσεων μεγαλώνει συνεχώς. Ειδικότερα δε, σύμφωνα με έρευνα της IBM[24], κατόπιν της πανδημίας του Covid19, οι επιθέσεις αυτές αυξήθηκαν ακόμα πιο πολύ. Ωστόσο, οι επιθέσεις αυτές αφορούσαν κυρίως επιτόπιες υποδομές (on-premises), καθώς επίσης και υποδομές IoT, όχι όμως υποδομές στον χώρο του νέφους (αναφερόμαστε πάντα στον χώρο της ΕΕ). Καθόσον η παρούσα μελέτη αφορά τον χώρο του νέφους, τα περιστατικά αυτά – αν και πάρα πολλά - δεν συμπεριλήφθηκαν.

[24] IBM Institute for Business Value, 2020. COVID-19 cyberwar: How to protect your business.

5.2.3 Ρωσία

Πίνακας 5.3. Επιθέσεις σε υπηρεσίες νέφους που επηρέασαν ΥΖΣ στη Ρωσία.

Τομέας	Περιστα-τικό	Επηρεαζόμενη υπηρεσία νέφους	Περιγραφή	Εντοπίστηκε ο δράστης (φυσικό πρόσωπο)	Σχόλια
Άμυνα	APT 28 Word 365 attack [25]	Word 365	Μάιος 2017 - Ρώσοι εισβολείς, γνωστοί με το προσωνύμιο «APT28» ή «Fancy Bear», έστειλαν παραπλανητικά email προς διπλωμάτες Ευρωπαϊκών χωρών, υποδυόμενοι αξιωματούχους του NATO. Στη συνέχεια, μέσω ενός συνημμένου αρχείου Word, εγκαθιστούσαν trojan εκμεταλλευόμενοι δυο ευπάθειες του Word 365, που είναι η έκδοση νέφους του γνωστού κειμενογράφου της Microsoft.	Όχι	Τέτοιου τύπου επιθέσεις διεξάγονται συχνά και πιθανά φέρουν την ανοχή (ή ακόμα και την υποστήριξη) της Ρωσική κυβέρνησης (state-sponsored attacks). Σύμφωνα με έρευνα της ENISA [52], 43% των κακόβουλων συνημμένων σε email, είναι αρχεία του Microsoft Office. Η τελευταία πανομοιότυπη με τούτη επίθεση, διεξήχθη τον Σεπτέμβριο του 2020, χρησιμοποιώντας στα μηνύματα εκπαιδευτικό υλικό του NATO ως δόλωμα[18].
Οικονομία	Cron Russian Bank hacking [26]	Google Play, Viber (μεταξύ και άλλων) [27]	Μάιος 2017 – Ομάδα εισβολέων από τη Ρωσία χρησιμοποιούσε υπηρεσίες νέφους όπως το Google Play και το Viber για να εγκαταστήσει το κακόβουλο λογισμικό Cron (trojan) σε χρήστες κινητών τηλεφώνων Android από τη Ρωσία.	Ναι. Πρόκειται για την ομάδα Cron, που πήρε αυτό το προσωνύμιο από το ομώνυμο κακόβουλο λογισμικό. Συνελήφθησαν 16 άτομα και απαγγέλθηκαν κατηγορίες από τις Ρωσικές διωκτικές αρχές.	Μέσω του κακόβουλου λογισμικού Cron έκλεβαν κωδικούς πρόσβασης αλλά και μηνύματα SMS από πελάτες τραπεζών, εκτελώντας στη συνέχεια μεταφορές χρημάτων σε λογαριασμούς τους. Οι Ρωσικές τράπεζες ζημιώθηκαν κατά το ποσό των 50 εκατομμυρίων ρουβλιών (κάπου 892 χιλιάδες δολάρια, με τις ισοτιμίες εκείνης της εποχής). Η ομάδα αυτή, κατά τη σύλληψή της ετοίμαζε επέκταση των επιθέσεών της σε πελάτες Ευρωπαϊκών τραπεζών, κυρίως Ισπανικών και Γαλλικών.
Υγεία	- [28]	-	-	-	-

[25] https://www.cyberscoop.com/dnc-hackers-impersonated-nato-attempt-hack-romanian-government/

[26] https://www.reuters.com/article/idUSKBN18I0VE

[27] https://www.securityweek.com/russian-hackers-infected-1-million-phones-banking-trojan

[28] Ισχύει και εδώ ό,τι αναφέρθηκε προηγουμένως για τον χώρο της ΕΕ στον τομέα της Υγείας, δηλαδή έχουν συμβεί πληθώρα περιστατικών ασφάλειας αλλά δεν αφορούν υποδομές στον χώρο του νέφους.

5.3 Συμπεράσματα ως προς την Εγκληματολογική αυτών των περιπτώσεων

Πίνακας 5.4. Συμπεράσματα ως προς την Εγκληματολογική αυτών των επιθέσεων.

Περιοχή	Τομέας	Περιστατικό	Συμπεράσματα
ΗΠΑ	Άμυνα	Docker Hub	1. Μια υπηρεσία νέφους φαινομενικά άσχετη με το Αμερικανικό Υπουργείο Άμυνας, όπως το Docker Hub, μπορεί πάραυτα να του δημιουργήσει πρόβλημα ασφάλειας, μιας που χρησιμοποιεί τους ίδιους κωδικούς πρόσβασης με το Docker, το οποίο χρησιμοποιείται από το Αμερικανικό Υπουργείο Άμυνας. 2. Η εγκληματολογική διερεύνηση δεν έφερε κανένα αποτέλεσμα, ούτε καν για την εθνικότητα των εισβολέων. 3. Συνεπώς η ανάγκη της πληγείσας Υποδομής Ζωτικής Σημασίας (εν προκειμένω του Αμερικανικού Υπουργείου Άμυνας) για ανεύρεση των εισβολέων, επαφίεται στην ικανότητα τέλεσης εγκληματολογικής έρευνας του παρόχου νέφους. Αν ο πάροχος νέφους δεν μπορεί να επιτελέσει αυτό το έργο, ο φορέας της επηρεαζόμενης υποδομής ζωτικής σημασίας δεν θα μάθει ποτέ ποιος ήταν ο υπαίτιος.
ΗΠΑ	Οικονομία	Capital One	1. Διέρρευσαν ευαίσθητες πληροφορίες περισσοτέρων από 100 εκατομμυρίων προσώπων, άρα το περιστατικό είναι ένα από τα χειρότερα όλων των εποχών. Άλλωστε, α) η Capital One είναι η 11η μεγαλύτερη τράπεζα στις ΗΠΑ, η δε AWS, ο πρώτος πάροχος νέφους παγκοσμίως, β) σύμφωνα με το κατηγορητήριο, εκτός της εν λόγω τράπεζας, από τη συγκεκριμένη επίθεση ζημιώθηκαν άλλες 30 ακόμα εταιρείες[29], καθώς επίσης σχολεία και διάφοροι οργανισμοί. 2. Δίωξη ασκήθηκε μόνο στο φυσικό πρόσωπο και στην τράπεζα. Όχι όμως και στον πάροχο νέφους (AWS), ο οποίος μάλιστα στο κατηγορητήριο ούτε καν αναφέρεται ονομαστικά[29]. Συνεπώς η αντίληψη ότι σε περίπτωση περιστατικού ασφάλειας στο νέφος, ζημιώνεται και ο πάροχος - πέραν του πελάτη - δεν ευσταθεί κατ' ανάγκη. 3. Δεν είναι σίγουρο ότι η συγκεκριμένη περίπτωση αποτελεί παράδειγμα επιτυχημένης εγκληματολογικής διερεύνησης, αφού το ίδιο το διωκόμενο πρόσωπο, από την πρώτη στιγμή της τέλεσης της επίθεσης, υπερηφανεύθηκε δημοσίως (σε δημοφιλείς ιστότοπους όπως το GitHub και το MeetUP) για το κατόρθωμά του[30] [31]. 4. Για να μπορεί μια οποιαδήποτε περίπτωση εγκλήματος στο νέφος να αναδειχθεί σε παράδειγμα ορθής και αποτελεσματικής εγκληματολογικής διερεύνησης, θα πρέπει οι κατηγορίες σε βάρος του διωκόμενου προσώπου να επιφέρουν καταδίκη και μάλιστα τελεσίδικα. Σύμφωνα με όσα αναφέρθηκαν στο κεφάλαιο 2, η εγκληματολογική έρευνα δεν εξαντλείται απλώς στην εύρεση του εισβολέα αλλά περιλαμβάνει και το στάδιο της «Παρουσίασης» (των αποδεικτικών στοιχείων ενώπιον των αρχών). Αν δεν διεξαχθούν σχολαστικά όλα τα βήματα, ο υπαίτιος δεν θα τιμωρηθεί και η εγκληματολογική έρευνα θα έχει αποτύχει. 5. Σύμφωνα με την AWS, καμία υπηρεσία της δεν υπέστη πλήγμα και όλα λειτούργησαν με τον τρόπο που είχαν σχεδιαστεί[31]. Η επίθεση πάντως έγινε στο επίπεδο της εφαρμογής, οπότε πιθανά, το μεγαλύτερο μέρος της ευθύνης - βάσει και του μοντέλου Κοινής Ευθύνης, που εξηγήθηκε σε προηγούμενο κεφάλαιο - να βαρύνει τον πελάτη και όχι τον πάροχο. 6. Ενώ οι αποζημιώσεις και οι χρηματικές ποινές που καλείται να πληρώσει η τράπεζα κυμαίνονται μεταξύ των 100 και 150 εκατομμυρίων δολαρίων, το διωκόμενο φυσικό πρόσωπο, αν καταδικασθεί τελεσίδικα, θα έρθει αντιμέτωπο με ποινές ύψους μέχρι 5 χρόνια φυλάκισης και μέχρι 250 χιλιάδες δολάρια[32]. Είναι εμφανές ότι οι επιπτώσεις, ακόμα και μετά την απονομή δικαιοσύνης, είναι πολύ βαρύτερες για το θύμα παρά για τον θύτη.

[29] https://www.wired.com/story/capital-one-paige-thompson-case-hacking-spree/

[30] https://www.foxbusiness.com/financials/who-is-paige-thompson-alleged-capital-one-hacker-alias-erratic

[31] https://www.cnbc.com/2019/07/30/paige-thompson-alleged-capital-one-hacker-stole-100-million-peoples-data.html

[32] https://www.geekwire.com/2019/capital-one-hacking-suspect-paige-thompson-appears-court-ordered-remain-custody/

ΗΠΑ	**Υγεία**	**AMCA data breach**	1. Και πάλι, μια υπηρεσία νέφους φαινομενικά άσχετη με τις υποδομές Υγείας, όπως η εισπρακτική εταιρεία AMCA και ο πάροχος νέφους Optum, μπορεί να δημιουργήσει σοβαρό πρόβλημα λειτουργίας αυτών των υποδομών υγείας. Τα υπέρογκα πρόστιμα που επιβλήθηκαν στα συγκεκριμένα διαγνωστικά κέντρα, λόγω της αποκάλυψης ευαίσθητων δεδομένων εκατομμυρίων πολιτών, τους δημιούργησαν σοβαρά οικονομικά προβλήματα και μάλιστα σε μια εποχή που το αμερικανικό σύστημα υγείας είχε απόλυτη ανάγκη τις υπηρεσίες που παρείχαν, λόγω της πανδημίας του Covid19. 2. Πάλι η εγκληματολογική διερεύνηση δεν έφερε κανένα αποτέλεσμα, ούτε καν για την εθνικότητα των εισβολέων. 3. Πρόστιμα επιβλήθηκαν στην εισπρακτική εταιρεία (η οποία ουσιαστικά πτώχευσε) αλλά και στα διαγνωστικά κέντρα, τα οποία άλλωστε ζημιώθηκαν και στο επίπεδο της φήμης. Δεν επιβλήθηκε πρόστιμο στον πάροχο της υπηρεσίας νέφους, δηλαδή την εταιρεία Optum που παρείχε προς την AMCA την υπηρεσία ηλεκτρονικών πληρωμών. Συνεπώς η αντίληψη ότι σε περίπτωση περιστατικού ασφάλειας στο νέφος, ζημιώνεται και ο πάροχος - πέραν του πελάτη – φαίνεται πάλι να μην ευσταθεί.
ΕΕ	**Άμυνα**	**Turkish DNS-Hijacking**	1. Η επίθεση αυτή έλαβε χώρα μέσω της τροποποίησης των εγγραφών του συστήματος Domain Name Service (DNS), που υλοποιεί την αντιστοίχιση ονομάτων χώρου με διευθύνσεις εξυπηρετητών. Η μη-εξουσιοδοτημένη πρόσβαση σε δομικά στοιχεία του διαδικτύου, όπως το σύστημα Domain Name Service (DNS), αποτελεί σοβαρή απειλή τόσο για τις υποδομές ζωτικής σημασίας, όσο και για την υπολογιστική νέφους. 2. Δεδομένου του μεγέθους και της βαρύτητας αυτής της επίθεσης, τουλάχιστον η έρευνα απέφερε κάποιες πληροφορίες σχετικά με την εθνικότητα των δραστών ή/και τα συμφέροντα που εξυπηρετούσαν. Τούτο όμως δεν συνιστά περίπτωση επιτυχημένης εγκληματολογικής έρευνας, αφού ούτε τα φυσικά πρόσωπα προσδιορίστηκαν, ούτε συγκεντρώθηκαν τα απαραίτητα αποδεικτικά στοιχεία για την άσκηση ποινικών διώξεων. 3. Σύμφωνα με το Reuters, η Ελληνική κυβέρνηση δεν διαπίστωσε καν την επίθεση αυτή, ούτε κατόπιν της αποκάλυψής της[19]. 4. Ακόμα και αν είχαν βρεθεί οι εισβολείς (σε επίπεδο φυσικών προσώπων), η εγκληματολογική έρευνα δύσκολα θα απέδιδε, μιας που η περίπτωση αυτή υπάγεται στην κατηγόρια των επιθέσεων που επιχορηγούνται από κράτη (state-sponsored attacks). Στις περιπτώσεις αυτές, η εγκληματολογική έρευνα συνήθως προσκρούει στην απροθυμία συνεργασίας της χώρας προέλευσης των δραστών.
ΕΕ	**Οικονομία**	**Operation Cloud Hopper**	1. Η μεγαλύτερη ευρωπαϊκή εταιρεία που επλήγη από αυτήν την επίθεση, ήταν η σουηδική Ericsson, κατασκευαστής προϊόντων υψηλής τεχνολογίας στον τομέα των τηλεπικοινωνιών και βασικός ανταγωνιστής κινεζικών εταιρειών αυτού του κλάδου. Σύμφωνα με τον Alastair MacGibbon, σύμβουλο εθνικής ασφάλειας της Αυστραλιανής κυβέρνησης[20], η επίθεση αυτή αφορούσε κλοπή βιομηχανικών και εμπορικών μυστικών για την εξυπηρέτηση οικονομικών συμφερόντων. 2. Σύμφωνα με τον Mike Rogers, πρώην Επικεφαλής της Υπηρεσίας Εθνικής Ασφάλειας των ΗΠΑ (National Security Agency / NSA), η επίθεση αυτή καταδεικνύει ότι η υπολογιστική νέφους, σε ό,τι αφορά τα ζητήματα ασφάλειας, δεν αποτελεί πανάκεια[20]. 3. Πράγματι, παρά το ότι οι πάροχοι που επηρεάστηκαν (δηλαδή η IBM και η Hewlett Packard Enterprise) αποτελούν κολοσσούς στον χώρο της υπολογιστικής νέφους, η μεγάλη χρονική διάρκεια αυτής της επίθεσης – από το 2010 ως το 2017, σύμφωνα με το Reuters[20] – δημιουργεί προβληματισμό αναφορικά με την ικανότητα των παρόχων να προστατέψουν αποτελεσματικά τους πελάτες τους. Μάλιστα, η Hewlett Packard, ως προκάτοχος της Hewlett Packard Enterprise μέχρι το έτος 2015, δεν είχε καν αντιληφθεί την επίθεση[20].
ΕΕ	**Υγεία**	**-**	-

ΡΩΣΙΑ	**Άμυνα**	**APT 28 Word 365 attack**	1. Η διείσδυση της υπολογιστικής νέφους στους υπολογιστές εκατομμυρίων τελικών χρηστών του διαδικτύου, μέσω εργαλείων της καθημερινότητας όπως ο κειμενογράφος Word 365, καθιστούν το νέφος φορέα σοβαρής απειλής για αυτούς, ειδικά όταν δεν διαθέτουν κάποια εμπειρία ή εκπαίδευση σε ζητήματα ασφάλειας. Και μέσω αυτών, απειλείται και ο τομέας στον οποίο εργάζονται, στην προκειμένη περίπτωση αυτός της Άμυνας / Εθνικής Ασφάλειας (τα θύματα εδώ ήταν διπλωμάτες). 2. Και σε αυτήν την περίπτωση, ακόμα και αν είχαν βρεθεί οι εισβολείς (σε επίπεδο φυσικών προσώπων), η εγκληματολογική έρευνα δύσκολα θα απέδιδε, μιας που η περίπτωση αυτή υπάγεται στην κατηγόρια των επιθέσεων που επιχορηγούνται από κράτη (state-sponsored attacks).
ΡΩΣΙΑ	**Οικονομία**	**Cron Russian Bank hacking**	1. Για την εξιχνίαση της υπόθεσης, στο σκέλος που αφορούσε τη διείσδυση του trojan στα κινητά τηλέφωνα των θυμάτων, χρησιμοποιήθηκε το σύστημα X-Force Threat Intelligence της IBM [94]. Το γεγονός, αυτό, μαζί με το αναφερθέν σε προηγούμενα κεφάλαια σύστημα LEIP (Law Enforcement Investigation Platform) της ίδιας εταιρείας, τη φέρνει σε καλό σχετικά επίπεδο ως προς τις παρεχόμενες λύσεις εγκληματολογικής έρευνας. 2. Σύμφωνα με τον Dmitry Volkov, επικεφαλής της ερευνητικής ομάδας της εταιρείας Group-IB, που διεξήγαγε την εγκληματολογική έρευνα[26], η επιτυχία αυτής της επίθεσης οφείλονταν σε δυο παράγοντες: α) στην ευρεία χρήση βοηθητικών προγραμμάτων για τη διανομή του trojan με πολλούς διαφορετικούς τρόπους, και β) την αξιοποίηση πολλών αυτόματων λειτουργιών των κινητών τηλεφώνων, που τους επέτρεψε να διεξάγουν τις κλοπές χωρίς άμεση συμμετοχή των ιδίων. 3. Το γεγονός ότι οι εισβολείς κατάφεραν και παραπλάνησαν την Google GOOGL.O, δηλαδή την εταιρεία που κατασκευάζει το λειτουργικό σύστημα Android, επιτυγχάνοντας τη διάθεση, μέσω του Google Play, εφαρμογών μολυσμένων με trojan, δημιουργεί – και εδώ - προβληματισμό αναφορικά με την ικανότητα της Google να προστατέψει αποτελεσματικά τους χρήστες του λειτουργικού της συστήματος. 4. Σημειώνεται ότι η επίθεση αποκαλύφθηκε λίγο πριν την επέκτασή της σε Ευρωπαϊκές τράπεζες. Ως εκ τούτου, οι οικονομικές επιπτώσεις ήταν σχετικά μικρές. Ειδεμή, λόγω του μεγάλου πλήθους των τραπεζών που θα επηρεάζονταν[26] [27], θα μπορούσε ίσως να προκληθεί πρόβλημα ακόμα και στη λειτουργία του ευρωσυστήματος.
ΡΩΣΙΑ	**Υγεία**	**-**	-

Με βάση τα ανωτέρω, θα μπορούσε να κανείς να καταλήξει στα ακόλουθα γενικά συμπεράσματα:

1. Η υπολογιστική νέφους δεν αποτελεί από μόνη της πανάκεια για ζητήματα ασφάλειας. Απαιτείται και η ενεργή συμμετοχή του πελάτη – λήπτη των υπηρεσιών νέφους.
2. Η εγκληματολογική έρευνα δύσκολα αποδίδει σε περιπτώσεις επιθέσεων υποστηριζόμενων από κράτη (state-sponsored attacks).
3. υποδομές ζωτικής σημασίας είναι δυνατόν να υποστούν σοβαρό πλήγμα από μικρές εταιρείες που λειτουργούν στο νέφος και δεν έχουν το κατάλληλο επίπεδο ασφάλειας.
4. Το μέγεθος των παρόχων νέφους και η διείσδυσή τους στην αγορά, δεν αποτελούν από μόνα τους επαρκή εχέγγυα για υψηλό επίπεδο προστασίας.
5. Η επιλογή κατάλληλου παρόχου υπηρεσιών νέφους πρέπει να διεξάγεται και με βάση την ικανότητά του να διεξάγει αποτελεσματική εγκληματολογική έρευνα. Ειδικά όταν πρόκειται για υποδομές ζωτικής σημασίας.
6. Η αντίληψη ότι, αν από ένα περιστατικό ασφάλειας, πληγεί ο πελάτης υπηρεσιών νέφους, τότε αυτόματα πλήττεται και ο πάροχος, δεν ευσταθεί.

7. Αποτελεσματική εγκληματολογική έρευνα έχουμε μόνο όταν έχουν διεξαχθεί όλα τα στάδιά της, με τρόπο σχολαστικό και ικανό να οδηγήσουν τον δράστη σε τελεσίδικη καταδίκη. Σε διαφορετική περίπτωση μιλάμε για ανεπιτυχή εγκληματολογική έρευνα ή απλώς για εξεύρεση κάποιων στοιχείων περί της ταυτότητας των δραστών.

Κεφάλαιο 6 - Πρόληψη και Αντιμετώπιση για επιτυχή Εγκληματολογία

6.1 Μεθοδολογία

Με δεδομένες τις δυσκολίες που παρουσιάζει η εγκληματολογία στην υπολογιστική νέφους, έτσι όπως αναλύθηκαν στα προηγούμενα κεφάλαια, σε τούτο το σημείο επιχειρείται διερεύνηση των δυνατοτήτων στο σκέλος της πρόληψης αλλά και της αντιμετώπισης (από πλευράς εγκληματολογικής έρευνας) περιστατικών ασφαλείας.

Στο ζήτημα της πρόληψης παρατίθεται μια λίστα μέτρων, τα οποία έχουν επισημανθεί σε προηγούμενα σημεία της παρούσας μελέτης. Στη λίστα αυτή όμως προστίθενται και μέτρα πρόληψης που αναφέρει ο Ευρωπαϊκός Οργανισμός Κυβερνοασφάλειας (ENISA) [53], σε μελέτη του αναφορικά με τα περιστατικά ασφάλειας στην υπολογιστική νέφους. Τα μέτρα πρόληψης χωρίζονται σε τεχνικό και θεσμικό επίπεδο.

Κατόπιν ακολουθεί αντίστοιχη λίστα, αυτή τη φορά για το σκέλος της αντιμετώπισης περιστατικών από πλευράς εγκληματολογικής έρευνας. Το περιεχόμενο αυτής της λίστας προκύπτει με τον ίδιο πάλι τρόπο: ανασκόπηση σχετικών επισημάνσεων από την παρούσα μελέτη, αλλά και παρουσίαση των μέτρων που παραθέτει ο ENISA.

6.2 Μέτρα Πρόληψης και Αντιμετώπισης

Τα μέτρα πρόληψης δεν αφορούν μόνο το λογισμικό και τα συστήματα που πρέπει να λειτουργούν πριν την εμφάνιση κάποιου περιστατικού ασφαλείας. Είναι πολύ περισσότερο από αυτό και περιλαμβάνουν προβλέψεις τόσο σε τεχνικό όσο και σε θεσμικό (νομικό κυρίως) επίπεδο.

Στη συνέχεια παρατίθενται μέτρα πρόληψης, πρώτα σε τεχνικό και κατόπιν σε θεσμικό επίπεδο.

6.2.1 Μέτρα πρόληψης σε τεχνικό επίπεδο

Μια λίστα μέτρων πρόληψης ανακύπτει από τις μελέτες που παρουσιάστηκαν στα προηγούμενα κεφάλαια και πιο πολύ στο κεφάλαιο 4, που περιλαμβάνει τη λίστα προληπτικών μέτρων του Pichan et al. . Αυτή η λίστα εμπλουτίζεται κατωτέρω και με τα μέτρα πρόληψης άλλων μελετητών που συμπεριλήφθηκαν στη παρούσα μελέτη.

Συνεπώς, τα μέτρα πρόληψης που μπορούν να βοηθήσουν στην αποτελεσματική διεξαγωγή εγκληματολογικής έρευνας (και δίωξης), είναι τα ακόλουθα:

1. Καλή γνώση των θεσπισμένων αρχών, πολιτικών και διαδικασιών εγκληματολογίας (όπως για παράδειγμα, ο Οδηγός Βέλτιστων Πρακτικών στην Ψηφιακή Εγκληματολογία της Ένωσης Αξιωματικών Αστυνομίας του Ηνωμένου Βασιλείου / ACPO)

2. Εξοικείωση με την προσέγγιση Forensics-as-a-Service, για τους λόγους που αναφέρονται στο κεφάλαιο 4.
3. Σήμανση πόρων (resource tagging)
4. Σύναψη ισχυρών συμφωνητικών παροχής υπηρεσιών (Service License Agreements / SLA) με τους παρόχους υπηρεσιών νέφους (CSPs), που α) να προβλέπουν ρητά υποδομές και λειτουργίες για την υποστήριξη εγκληματολογίας νέφους, β) να δηλώνουν ρητά την τοποθεσία στην οποία αποθηκεύονται τα δεδομένα, καθώς επίσης και την τοποθεσία στην οποία κλωνοποιούνται (αντιγράφονται), γ) να προβλέπουν αυστηρές μεθόδους απομόνωσης των οντοτήτων του νέφους (cloud instance isolation) , όπως για παράδειγμα η τεχνική Sandboxing.
5. Αρχεία καταγραφής κινήσεων σε επίπεδο συστήματος (system level logs) και καθορισμός κατάλληλου πλαισίου για την καταγραφή των κινήσεων (log frame work)
6. Κρυπτογράφηση της αλυσίδας αποδεικτικών στοιχείων (Chain of Custody) με χρήση αλγορίθμου RSA. Στην παρούσα μελέτη παρουσιάστηκαν και άλλες τεχνικές κρυπτογράφησης, όπως για παράδειγμα, η μέθοδος Blockchain-assisted Secure Logging-as-a-Service (BlockSLaaS) των Sagar Rane και Arati Dixit και η μέθοδος CLASS (Cloud Log Assuring Soundness and Secrecy) των Ahsan et al. (Κεφάλαιο 4).
7. Εφαρμογή τεχνικής Sandboxing για τον διαχωρισμό των αποδεικτικών στοιχείων (evidence segregation).
8. Σήμανση των εικονικών υπολογιστών (VM instance tagging).
9. Μόνιμη αποθήκευση των προσωρινών δεδομένων (volatile data) μέσω της διάθεσης μόνιμου αποθηκευτικού χώρου.
10. Εφαρμογή αλγόριθμων ελέγχου αθροίσματος (checksum algorithms) για την διασφάλιση της ακεραιότητας των δεδομένων (data integrity).
11. Εξ αρχής εγκατάσταση και εξοικείωση στη χρήση εργαλείων καταγραφής κινήσεων, ικανών να συνεργαστούν με πολλαπλούς παρόχους και συστήματα (πχ. splunk), να αποτρέπουν την εξάρτηση από συγκεκριμένο πάροχο και να χρονοθετούν τις κινήσεις με δικό τους ενιαίο σύστημα χρονοσφραγίδων.
12. Εξ αρχής εγκατάσταση συστήματος εν λειτουργία εγκληματολογίας (live forensics).
13. Εξ αρχής εγκατάσταση εργαλείων επεξεργασίας δεδομένων που διευκολύνουν την απομακρυσμένη συλλογή δεδομένων και εξοικείωση στη χρήση τους.
14. Εξ αρχής εγκατάσταση υποδομής διαχείρισης μυστικών κλειδιών μέσω υπολογιστικής νέφους (Cloud Key Management infrastructure) για την αντιμετώπιση του προβλήματος των κρυπτογραφημένων δεδομένων.

15. Εξ αρχής εγκατάσταση συστήματος διαχείρισης πληροφοριών και περιστατικών ασφάλειας (Security Information and Event Management / SIEM) της Hewlett-Packard, αλλά και συστήματος καταγραφής κινήσεων των δεδομένων (data tracking).
16. Εξ αρχής εφαρμογή πρακτικών που εξασφαλίζουν εμπιστοσύνη στις υποδομές του παρόχου, όπως το Μοντέλο Έμπιστου Υλικού (Hardware Trust Model Platform / TPM), το Μοντέλο Έμπιστου Εικονικού Περιβάλλοντος (Trusted Virtual Environment Module), η πλατφόρμα Έμπιστης Υπολογιστικής Νέφους (Trusted Cloud Computing Platform), η καθέρωση μοντέλου Διερευνητικών Ελέγχων (Detective controls),κα.
17. Προώθηση της διεθνούς συνεργασίας με τη σύναψη αμοιβαίων συμφωνιών και συνθηκών (πχ. Mutual Legal Assistance Treaties / MLATs).
18. Εξ αρχής πρόβλεψη συχνής λήψης στιγμιοτύπων (snapshots) και αποθήκευσή τους σε άλλο δίκτυο, απομονωμένο τόσο από τηλεπικοινωνιακής (δικτυακής) όσο και από φυσικής πλευράς.
19. Ειδικά για περιπτώσεις υποδομών ζωτικής σημασίας, οι Cristina Alcaraz και Sherali Zeadallly προτρέπουν σε άμεση προληπτική μελέτη της ακολουθίας στοιχείων και γεγονότων, κάθε φορά που διαπιστώνονται ασυνήθιστα συμπτώματα ή απειλές.
20. Ειδικά για την Προστασία της ιδιωτικότητας (δηλαδή της ιδιοκτησίας των δεδομένων τρίτων), εξ αρχής χρήση τεχνικών όπως το RAM mirroring και το Dynamic Taint Analysis των Zou et al. [54].

Ο Ευρωπαϊκός Οργανισμός Κυβερνοασφάλειας (ENISA) [53], σε μελέτη του με θέμα τη διερεύνηση περιστατικών ασφαλείας στην υπολογιστική νέφους, επισημαίνει ότι τα προληπτικά μέτρα είναι ο πιο σημαντικός παράγοντας για τη διεξαγωγή εγκληματολογικών ερευνών, διότι διευθετούν σωρεία θεμάτων που μπορούν να ανακύψουν αν και όταν χρειαστεί η διεξαγωγή εγκληματολογικής έρευνας. Παραθέτει δε τα ακόλουθα προληπτικά μέτρα:

1. Εξ αρχής συμφωνία ανάμεσα στον πάροχο και τον πελάτη για τις ενέργειες που πρέπει να διεξάγουν σε περίπτωση διεξαγωγής εγκληματολογικών ερευνών.
2. Προληπτικά μέτρα που αφορούν τον πάροχο:

2.1. Πλήρη καταγραφή όλων των κινήσεων σε όλα τα επίπεδα της υπολογιστικής νέφους (φυσικό επίπεδο, hypervisor, Host OS, κλπ) και διαχείρισή τους από έναν ενιαίο μηχανισμό.

2.2. Εγκατάσταση συστήματος αυτόματου εντοπισμού ασυνήθιστης συμπεριφοράς.

2.3. Για το μοντέλο Infrastructure-as-a-Service (SaaS): διάθεση προς τον πελάτη δυνατότητας αποθήκευσης των προσωρινών δεδομένων (volatile data) αλλά και εξασφάλιση της αποθήκευσης των μόνιμων δεδομένων για μεγάλο χρονικό διάστημα.

2.4. Για το μοντέλο Platform-as-a-Service (PaaS): διάθεση προς τον πελάτη διαγνωστικών εργαλείων που να παρέχουν δυνατότητα συλλογής και αποθήκευσης διαγνωστικών δεδομένων με τρόπο που να εύκολα διαχειρίσιμος.

2.5. Για το μοντέλο Software-as-a-Service (SaaS): διάθεση προς τον πελάτη εργαλείων καταγραφής κινήσεων, που να λειτουργούν στις υποδομές του παρόχου.

3. Προληπτικά μέτρα που αφορούν τον πελάτη, ο οποίος και θα πρέπει να τα απαιτήσει κατά τη σύναψη του συμφωνητικού παροχής υπηρεσιών με τον πάροχο:

3.1. Δικαίωμα απαίτησης δυνατότητας ανάκτησης τεκμηρίων (Proofs of Retrievability / POR) σε περίπτωση που χρειαστεί εγκληματολογική έρευνα.

3.2. Εξ αρχής διάθεση (εκ μέρους του παρόχου) και χρήση εργαλείων καταγραφής και επεξεργασίας κινήσεων.

3.3. Απαίτηση κρυπτογράφησης των αρχείων καταγραφής κινήσεων.

3.4. Για το μοντέλο Infrastructure-as-a-Service (SaaS): από τη στιγμή που ο πελάτης δεν έχει δυνατότητα ελέγχου – ή έστω πρόσβασης – στα υποκείμενα επίπεδα (δηλαδή στο φυσικό επίπεδο και στο επίπεδο του hypervisor), απαίτηση πρόσβασης στα αρχεία κινήσεων αυτών των επιπέδων, σε περίπτωση διεξαγωγής εγκληματολογικής έρευνας.

3.5. Για το μοντέλο Platform-as-a-Service (PaaS): απαίτηση η κύρια εφαρμογή να υπάγεται εξ ολόκληρου στον έλεγχο του πελάτη.

3.6. Για το μοντέλο Software-as-a-Service (SaaS): απαίτηση εφαρμογής μοντέλου αυθεντικοποίησης ενιαίας εισόδου (Single-Sign-On) - μιας που διευκολύνει πολύ την εγκληματολογική ανάλυση - εκτός και αν υπάρχουν συγκεκριμένοι λόγοι που δεν το επιτρέπουν.

4. Προληπτικά μέτρα που αφορούν τόσο τον πάροχο όσο και τον πελάτη και αφορούν το ζήτημα του μοντέλου Κοινής Ευθύνης (Shared Responsibility Model). Σημειώνεται ότι, όπως εξηγήθηκε σε προηγούμενα κεφάλαια, όλοι οι πάροχοι έχουν ασπαστεί το μοντέλο αυτό, και ως εκ τούτου, τα συμφωνητικά παροχής υπηρεσιών πρέπει εξ αρχής να περιλαμβάνουν τα ακόλουθα ζητήματα εγκληματολογικής έρευνας:

4.1. Καθορισμός της γεωγραφική τοποθεσία λειτουργίας των υπηρεσιών/υποδομών νέφους που εκμισθώνει ο πελάτης.

4.2. Καθορισμός του εφαρμοστέου δικαίου.

4.3. Αναλυτική καταγραφή της διαδικασίας εγκληματολογικής έρευνας που θα εκτελέσει ο πάροχος, σε περίπτωση που χρειαστεί.

4.4. Ακριβής καθορισμός του επιπέδου πρόσβασης που θα χρειαστεί να χορηγηθεί στον πελάτη και στον εγκληματολογικό ερευνητή, καθώς επίσης και ακριβής καθορισμός του τρόπου αυθεντικοποίησής τους.

4.5. Κατανομή ρόλων και ευθυνών μεταξύ του παρόχου και του πελάτη σχετικά με την εγκληματολογική ανάλυση.

4.6. Καθορισμός χρονικού περιθωρίου εντός του οποίου ο πάροχος θα πρέπει να έχει βρει και διαθέσει τα απαραίτητα δεδομένα.

4.7. Ο τύπος των μετα-δεδομένων (meta-data) και ο τύπος των αρχείων καταγραφής κινήσεων που θα χρειαστεί να περισυλλεχθούν.
4.8. Καθορισμός ζητημάτων κόστους. (Για παράδειγμα τα κόστη που ενδεχομένως ανακύπτουν σε περίπτωση περιστατικού, τυχόν ύπαρξη συγκεκριμένων προμηθειών για εγκληματολογικές αναλύσεις, κ.α.)
4.9. Καθορισμός των παραγόντων που δύνανται να πάρουν πρόσβαση στα συλλεχθέντα δεδομένα, αλλά και των προϋποθέσεων κάτω από τις οποίες θα αποκτούν την πρόσβαση αυτή.

Γενικά ο Ευρωπαϊκός Οργανισμός Κυβερνοασφάλειας (ENISA) διαπιστώνει στη μελέτη αυτή ότι, στο μοντέλο Infrastructure-as-a-Service (IaaS) ανακύπτουν λιγότερα θέματα οργανωτικής φύσεως κατά τη διεξαγωγή εγκληματολογικών ερευνών. Αυτό οφείλεται στο ότι ο πελάτης έχει απόλυτο έλεγχο στη συσκευή (φυσική ή εικονική) που εκμίσθωσε και άρα έχει εύκολη πρόσβαση στις πληροφορίες που αποθηκεύονται στη συσκευή αυτή. Απεναντίας, τα περισσότερα προβλήματα οργανωτικής φύσεως ανακύπτουν στο μοντέλο Software-as-a-Service (SaaS), διότι εκεί ο πελάτης δεν ελέγχει την υποκείμενη υποδομή και άρα χωρίς τη συνεργασία του παρόχου δεν μπορεί να έχει πρόσβαση στα απαιτούμενα δεδομένα.

Συνεπώς, για ζητήματα εγκληματολογικής έρευνας, ένα γενικό προληπτικό μέτρο είναι η προτίμηση του μοντέλου Infrastructure-as-a-Service (IaaS) έναντι των υπολοίπων, αν και όταν αυτό μπορεί να ικανοποιήσει τις λειτουργικές απαιτήσεις του πελάτη.

6.2.2 Μέτρα πρόληψης σε θεσμικό επίπεδο

Στο κεφάλαιο 4 παρουσιάστηκαν διεθνείς συμφωνίες που συμβάλλουν καθοριστικά στη διεξαγωγή εγκληματολογικών ερευνών, ειδικά στην υπολογιστική νέφους, που, λόγω της φύσης της, έχει διεθνή υπόσταση. Θα μπορούσε κανείς να πει ότι οι συμφωνίες αυτές είναι ο σημαντικότερος παράγοντας για την αποτελεσματική διεξαγωγή εγκληματολογικών ερευνών, αφού χωρίς αυτές, οι αναλύσεις και τα πορίσματα των εγκληματολογικών ερευνητών μπορούν να προσκρούουν στην αναποτελεσματικότητα, τη γραφειοκρατία και την απροθυμία των κατά τόπους διωκτικών αρχών.

Συνεπώς, τα μέτρα πρόληψης στο σημείο αυτό, μπορούν να είναι τα ακόλουθα:

1. Ενίσχυση και προώθηση των διεθνών και διμερών συμφωνιών που αφορούν την καταπολέμηση του κυβερνοεγκλήματος. Στο εξής θα πρέπει να υπογράφονται όλο και πιο πολλές τέτοιες συμφωνίες και να περιλαμβάνουν ρητές προβλέψεις για τα ζητήματα των εγκληματολογικών ερευνών.
2. Ενίσχυση των φορέων καταπολέμησης κυβερνοεγκλήματος, όπως αυτών που εμφανίζονται στο γράφημα της μελέτης των Nazli Choucri, Stuart Madnick και Jeremy Ferwerda (βλ. Εικόνα 4.2), δηλαδή η υπηρεσία Cooperative Cyber Defence Centre Of Excellence (CCDOE) του NATO, οι ομάδες CERT με τις οποίες συνεργάζεται ο ENISA και η διεθνής υπηρεσία International

Telecommunication Union (ITU), ο οργανισμός International Multilateral Partnership Against Cyber Threats (IMPACT) της υπηρεσίας ITU.

3. Ειδικότερα για τον χώρο της ΕΕ, το κείμενο της Ευρωπαϊκής Επιτροπής [26] που παρουσιάστηκε στο κεφάλαιο 4, υποδεικνύει την **προώθηση του διεθνούς διαλόγου** για την επίλυση των μείζονων ζητημάτων της υπολογιστικής νέφους, τα οποία αποτελούν συνάμα και τα μείζονα ζητήματα της εγκληματολογίας υπολογιστικής νέφους. Τέτοια είναι:

3.1. το νομικό πλαίσιο,

3.2. η πρόσβαση σε δεδομένα εκ μέρους των διωκτικών αρχών,

3.3. η χρήση συμφωνιών αμοιβαίας δικαστικής συνδρομής ώστε να μην προκύπτουν αντικρουόμενα αιτήματα από τις διωκτικές και τις δημόσιες εν γένει αρχές,

3.4. ο συντονισμός της ασφάλειας των δεδομένων σε παγκόσμιο επίπεδο,

3.5. η ασφάλεια στον κυβερνοχώρο,

3.6. η ευθύνη των παρόχων υπηρεσιών νέφους.

6.2.3 Μέτρα αντιμετώπισης

Μέχρι τώρα παρατέθηκαν κάποια μέτρα που εξυπηρετούν την εγκληματολογική έρευνα και μπορούν να λάβουν χώρα πριν την εμφάνιση ενός περιστατικού ασφάλειας στην υπολογιστική νέφους. Κατωτέρω παρουσιάζονται αντίστοιχα μέτρα που μπορούν να διεξαχθούν μετά από ένα τέτοιο περιστατικό ή κατά την εξέλιξή του.

Όπως και στην περίπτωση των προληπτικών μέτρων, η κατωτέρω λίστα μέτρων αντιμετώπισης βασίζεται στη μελέτη των Pichan et al. [7] που παρουσιάστηκε Κεφάλαιο 4 και εμπλουτίζεται με τις υποδείξεις άλλων μελετητών (αναφέρονται παραπλεύρως των υποδείξεών τους):

1. Άμεση εφαρμογή των θεσπισμένων αρχών, πολιτικών και διαδικασιών εγκληματολογίας (όπως για παράδειγμα, ο Οδηγός Βέλτιστων Πρακτικών στην Ψηφιακή Εγκληματολογία της Ένωσης Αξιωματικών Αστυνομίας του Ηνωμένου Βασιλείου / ACPO[1]).
2. Άμεση χρήση των υποδομών Forensics-as-a-Service, για τους λόγους που αναφέρονται στο κεφάλαιο 4.
3. Άμεση διεξαγωγή αντίστροφης αναζήτησης (reverse lookup) των συσκευών του δικτύου, διότι έτσι αποκαλύπτεται η τοπολογία του δικτύου του επιτιθέμενου.
4. Έγκαιρη και γρήγορη ανάλυση στιγμιότυπου (snapshot analysis).

Η προαναφερθείσα μελέτη του Ευρωπαϊκού Οργανισμού Κυβερνοασφάλειας (ENISA) με θέμα τη διερεύνηση περιστατικών ασφαλείας στην υπολογιστική νέφους, προβαίνει στον διαχωρισμό των μέτρων αντιμετώπισης σε δυο κατηγορίες: αυτά που αφορούν την εγκληματολογική έρευνα που διεξάγεται κατά την εξέλιξη του περιστατικού (live forensics) και εκείνα που αφορούν την

εγκληματολογική έρευνα που διεξάγεται κατόπιν της ολοκλήρωσης του περιστατικού (post-incident forensics).

Στην πρώτη κατηγορία μέτρων αντιμετώπισης (live forensics), ο ENISA περιλαμβάνει τη συλλογή των εγκληματολογικών δεδομένων από ένα σύστημα που βρίσκεται σε λειτουργία και δεν έχει κλείσει από τότε που διεξήχθη το περιστατικό ασφάλειας. Αυτού του είδους τα εγκληματολογικά δεδομένα είναι, για παράδειγμα, η μνήμη, οι διεργασίες (processes) που εκτελούνται στον υπολογιστή, τα τηλεπικοινωνιακά δεδομένα και γενικά όλες εκείνες οι πληροφορίες που παύουν να υφίστανται κατά την απενεργοποίηση ενός υπολογιστή.

Στην δεύτερη κατηγορία μέτρων αντιμετώπισης (post-incident forensics), ο ENISA περιλαμβάνει τη συλλογή όλων των φυσικών (ή λογικών) στοιχείων του εγκλήματος – όπως για παράδειγμα σκληροί δίσκοι και στιγμιότυπα εικονικών μηχανών – καθώς επίσης και τη χαρτογράφηση ολόκληρου του περιβάλλοντος που επηρεάστηκε από την επίθεση, αν αυτό είναι τεχνικά εφικτό και επιτρεπτό.

Ο χρόνος μετράει.

Σύμφωνα με τη μελέτη του του Ευρωπαϊκού Οργανισμού Κυβερνοασφάλειας (ENISA) αλλά και σύμφωνα με την κοινή λογική, ο χρόνος έχει μεγάλη σημασία για τη διεξαγωγή εγκληματολογικών ερευνών. Πιο συγκεκριμένα, ο χρόνος που παρήλθε μέχρι τον εντοπισμό του περιστατικού (time-to-detect), καθώς επίσης και ο χρόνος που καταναλώθηκε κατά την αντιμετώπισή του (time-to-respond), την συλλογή των στοιχείων και την ανάλυσή τους, είναι καθοριστικός για την αποτελεσματικότητα της εγκληματολογικής έρευνας.

Κεφάλαιο 7 - Προκλήσεις και Ανοιχτά ζητήματα

7.1 Προκλήσεις

Όπως ήδη αναφέρθηκε σε πολλά σημεία της παρούσας μελέτης, η εγκληματολογία στην υπολογιστική νέφους παρουσιάζει αρκετές προκλήσεις και αυτές εντείνονται περαιτέρω όταν αφορούν υποδομές ζωτικής σημασίας.

Οι προκλήσεις αυτές θα μπορούσαν να αποτελέσουν αντικείμενο επεξεργασίας μελλοντικών μελετών, ώστε να βρεθούν οι βέλτιστοι τρόποι αντιμετώπισής τους.

7.1.1 Προκλήσεις στο τεχνικό επίπεδο

Σύμφωνα λοιπόν με όσα παρουσιάστηκαν μέχρι τώρα, αλλά και με βάση σχετική μελέτη του Ευρωπαϊκού Οργανισμού Κυβερνοασφάλειας (ENISA) [53] αναφορικά με τα περιστατικά ασφάλειας στην υπολογιστική νέφους, τα ακόλουθα σημεία αποτελούν προκλήσεις της εγκληματολογίας υπολογιστικής νέφους και χρίζουν περαιτέρω επεξεργασίας:

1. **Αδυναμία πρόσβασης σε εγκληματολογικά δεδομένα λόγω μοντέλου υπηρεσιών υπολογιστικής νέφους**: πέραν του μοντέλου Infrastructure-as-a-Service (IaaS) στο οποίο οι πελάτες έχουν εύκολη πρόσβαση στα δεδομένα που απαιτούνται για εγκληματολογική έρευνα, στα υπόλοιπα συνήθη μοντέλα (δηλαδή Software-as-a-Service και Platform-as-a-Service) οι πελάτες έχουν ελάχιστη ως καθόλου πρόσβαση στα δεδομένα αυτά.
2. **Αδυναμία άμεσης φυσικής πρόσβασης στα δεδομένα** (inaccessibility).
3. **Εξάρτηση ή/και απροθυμία συνεργασίας από τον Πάροχο Υπηρεσιών Νέφους**: Οι πάροχοι ενίοτε παρουσιάζουν μειωμένη προθυμία να χορηγήσουν δεδομένα απαραίτητα για εγκληματολογική έρευνα (πχ σκληρούς δίσκους), κυρίως από φόβο αντιμετώπισης θεμάτων που σχετίζονται με την ιδιοκτησία δεδομένων τρίτων φορέων (δηλ. άλλων πελατών που έχουν τα δεδομένα τους στις ίδιες υποδομές με το υπο-διερεύνηση έγκλημα αλλά δεν σχετίζονται με αυτό).
4. **Πολυμίσθωση** (multi-tenancy) **και επαναχρησιμοποίηση πόρων**: ο ENISA επισημαίνει σε αυτό το σημείο ότι η πολυμίσθωση συστημάτων δεν είναι μια νέα πρόκληση για τις εγκληματολογικές έρευνες, ωστόσο, στην περίπτωση της υπολογιστικής νέφους, προκαλεί περαιτέρω πολυπλοκότητα στη διαδικασία συλλογής των στοιχείων, κυρίως λόγω της ελαστικής φύσης του νέφους. Εκτός αυτού, ο πάροχος υπηρεσιών νέφους μπορεί να αντιμετωπίσει πρόσθετες δυσκολίες στην περίπτωση που ο πελάτης έχει απελευθερώσει (έπαψε να χρησιμοποιεί) τις υποδομές που εκμίσθωσε και αυτές κατόπιν περιήλθαν σε άλλο πελάτη. Γενικά, λόγω της

επαναχρησιμοποίησης των πόρων από διαφορετικούς πελάτες, η εγκληματολογική έρευνα καθίσταται δύσκολη.

5. **(Από-)Κρυπτογράφηση των δεδομένων**: η κρυπτογράφηση των δεδομένων εγείρει δυσκολίες διότι η αποκρυπτογράφησή τους απαιτεί πολύ χρόνο και πολλούς πληροφοριακούς πόρους (πχ. επεξεργαστική ισχύ και χώρο). Η πρόκληση αυτή οξύνεται εκθετικά ανάλογα με τον όγκο των προς-αποκρυπτογράφηση δεδομένων.

6. **Το ιδιωτικό κλειδί (Private key)**: Στο κεφάλαιο 3 γίνεται αναφορά σε μελέτη των Afzaal et al. [18] η οποία αναφέρει ότι οι πιο συνηθισμένες εφαρμογές για την ασφαλή αποθήκευση των κινήσεων καταγραφής σε υποδομές ζωτικής σημασίας, χρησιμοποιούν κλασικό αλγόριθμο κρυπτογράφησης RSA. Το πρόβλημα με τη χρήση απλού αλγόριθμου κρυπτογράφησης RSA είναι ότι, αν ο επιτιθέμενος βρει το ιδιωτικό κλειδί (private key) που χρησιμοποιείται κατά την κρυπτογράφηση, τότε μπορεί να προσπελάσει και να αλλοιώσει τις πληροφορίες αυτές. Να σημειωθεί ότι δεν είναι ιδιαίτερα δύσκολο να βρει το ιδιωτικό κλειδί, αφού μια απλή αναζήτηση στον σκληρό δίσκο μπορεί να το ανασύρει.

7. **Υποχρέωση οριστικής διαγραφής δεδομένων**: λόγω κανονιστικού πλαισίου (πχ Γενικός Κανονισμός Προστασίας Προσωπικών Δεδομένων / GDPR [55]), οι πάροχοι υποχρεώνονται ενίοτε στην οριστική διαγραφή δεδομένων, τα οποία όμως θα μπορούσαν να χρειαστούν κατά την εγκληματολογική διερεύνηση ενός περιστατικού ασφαλείας.

8. **Υψηλό κόστος**: ορισμένες προσεγγίσεις εγκληματολογικής έρευνας, όπως για παράδειγμα η προσέγγιση live-forensics που παρουσιάστηκε στο προηγούμενο κεφάλαιο, έχουν υψηλές απαιτήσεις σε πόρους και τούτο προκαλεί αντίστοιχη οικονομική επιβάρυνση.

9. **Απουσία εξειδικευμένων πιστοποιήσεων, εργαλείων, πρακτικών και εκπαιδευτικών διαδικασιών:** Πιστοποιήσεις για επαγγελματίες εγκληματολογικών ερευνών στο χώρο της υπολογιστικής νέφους δεν υπάρχουν. Εργαλεία υπάρχουν αλλά και πάλι δεν εξειδικεύονται στον χώρο της υπολογιστικής νέφους, δεν έχουν πάντα δυνατότητες συνεργασίας με πολλαπλούς παρόχους (multi-cloud capabilities) και δεν έχουν ειδικές λειτουργίες για περιπτώσεις εγκλημάτων σε υποδομές ζωτικής σημασίας. Οι πρακτικές που εφαρμόζονται περιλαμβάνουν γενικές αρχές εγκληματολογίας ή/και ψηφιακής εγκληματολογίας και δεν εξειδικεύονται στην εγκληματολογία υπολογιστικής νέφους. Εκπαιδευτικές διαδικασίες δεν υπάρχουν και όσοι έχουν ειδικευθεί το έχουν καταφέρει κυρίως με δικές τους προσπάθειες εκμάθησης (είναι δηλαδή αυτοδίδακτοί).

10. **Πρόβλημα συγχρονισμού ώρας (time synchronization):** Στην υπολογιστική νέφους τα δεδομένα διανέμονται σε όλο τον κόσμο. Όταν λοιπόν απαιτείται ανακατασκευή δεδομένων και

περιστατικών που έλαβαν χώρα σε υπολογιστές διαφορετικών τοποθεσιών, ο συγχρονισμός της ώρας είναι ένα κρίσιμο ζήτημα και απαιτείται η χρήση πρωτοκόλλων συγχρονισμού δικτύου (όπως πχ το NTP).

11. **Διαφορετικοί τύποι δεδομένων και αρχείων καταγραφής κινήσεων:** υπάρχει έλλειψη ενιαίου πλαισίου για τα αρχεία καταγραφής κινήσεων (lack of log frame work).
12. **Άγνωστη φυσική τοποθεσία τέλεσης του εγκλήματος.**
13. **Αποκεντρωμένα δεδομένα και κατανεμημένη αποθήκευση** (distributed data & storage): υπάρχει εξαιρετική δυσκολία στην ενσωμάτωση δεδομένων που αποτελούν αποδεικτικά στοιχεία (Evidence data integration) και που προέρχονται από διαφορετικές πηγές.
14. **Κλωνοποίηση των δεδομένων.** Κατά την κλωνοποίηση (αντιγραφή) των δεδομένων, είναι δυνατό να βρεθούν τα δεδομένα σε δυο διαφορετικές τοποθεσίες, καθεμία εκ των οποίων έχει τη δική της νομοθεσία για εγκλήματα στον κυβερνοχώρο. Και έτσι ανακύπτουν προβλήματα εφαρμοστέου δικαίου.
15. **Προσωρινότητα και η εφήμερη φύση των δεδομένων** (data volatility / ephemeral nature of data)
16. **Δυσκολία συχνής λήψης συχνών στιγμιοτύπων (snapshots)**, λόγω του μεγάλου όγκου που έχουν συνήθως τα στιγμιότυπα.
17. **Δυσκολία αναδημιουργία της σκηνής του εγκλήματος** (crime scene reconstruction) ενώπιον του δικαστηρίου. Η δυσκολία αυτή οξύνεται από την πολυπλοκότητα της υπολογιστικής νέφους και την υποχρέωση επεξήγησής της, με απλά λόγια, στους δικαστές, τους εισαγγελείς και τους ενόρκους.
18. **Η συμμόρφωση προς το κανονιστικό πλαίσιο** (compliance) διαφορετικών φορέων.
19. **Περιορισμοί που υπαγορεύονται από ιδιαιτερότητες Υποδομών Ζωτικής Σημασίας:** Στο Κεφάλαιο 3, σε αναφορά που γίνεται σε μελέτη των Cristina Alcaraz και Sherali Zeadallly περί εγκληματολογίας σε ΥΖΣ, επισημαίνεται ότι για την εφαρμογή των τεχνικών και των μεθοδολογιών της εγκληματολογικής διερεύνησης, είναι σημαντικό να λαμβάνονται υπ' όψιν οι περιορισμοί που προέρχονται από τα συστήματα που περιβάλλουν την υπό διερεύνηση υποδομή ζωτικής σημασίας. Οι περιορισμοί αυτοί αφορούν περίπλοκες αρχιτεκτονικές, τυχόν ύπαρξη αλληλεπιδράσεων ανάμεσα στα περιφερειακά συστήματα, συνύπαρξη ετερογενών συστημάτων, κλπ.
20. **Το Έγκλημα-ως-Υπηρεσία (Crime-as-a-Service)**: Σε μελέτη των Reza Montasari και Richard Hill που παρουσιάστηκε στο κεφάλαιο 2, γίνεται αναφορά στο φαινόμενο «Έγκλημα ως υπηρεσία»

(Crime-as-a-Service), σύμφωνα με το οποίο οι επιτιθέμενοι μπορούν να βρουν εύκολα στο νέφος τα εργαλεία εκείνα που χρειάζονται για να πραγματοποιήσουν τις επιθέσεις τους. Συνεπώς, όπως το νέφος έρχεται να λύσει τα χέρια των ερευνητών εγκληματολογίας με λύσεις όπως το Forensics-as-a-Service, με τον ίδιο ακριβώς τρόπο λύνει και τα χέρια των κακοποιών.

21. **Το ζήτημα της Αλυσίδας Επιμέλειας (Chain Of Custody):** για το ζήτημα αυτό ο ENISA [53] επισημαίνει ότι, στην παραδοσιακή ψηφιακή εγκληματολογία, ένα αντίγραφο του σκληρού δίσκου του υπολογιστή που υπέστη την επίθεση μπορεί να χρησιμοποιηθεί στο δικαστήριο. Όμως στο περιβάλλον της υπολογιστικής νέφους, λόγω των διαφόρων χαρακτηριστικών του νέφους, όπως η κατανεμημένη διασπορά των δεδομένων, η πολυμίσθωση και η ελαστικότητα, η απόδειξη ενώπιον του δικαστηρίου ότι, τα τεκμήρια που παρουσιάζονται είναι αυθεντικά, γίνεται εξαιρετικά δύσκολη. Σε τούτο το σημείο μπορεί να ειπωθεί ότι ο μηχανισμός της Microsoft "Legal Hold", που παρουσιάστηκε στο κεφάλαιο 2 βοηθάει μεν σημαντικά στην επιμέλεια αλυσίδας (chain of custody), αλλά από την άλλη πλευρά, είναι εξαιρετικά δύσκολο να εξηγηθεί σε ένα δικαστήριο αυτός ο μηχανισμός αλλά και να τεκμηριωθεί (ενώπιον δικαστών, ενόρκων, κλπ) η αποτελεσματικότητά του.

7.1.2 Προκλήσεις στο θεσμικό επίπεδο

Ειδικότερα στο θεσμικό επίπεδο, οι ακόλουθες προκλήσεις πρέπει να αντιμετωπιστούν μελλοντικά από μελετητές και νομοθέτες:

1. **Δικαιοδοσία (jurisdiction) και πολύπλοκο νομικό καθεστώς:** Γενικά σε περιπτώσεις διεθνών εγκλημάτων, όπου εμπλέκονται διωκτικές αρχές αλλά και νομοθεσίες πολλών χωρών, η εγκληματολογική έρευνα μπορεί να κωλυσιεργήσει κατά την αντιμετώπιση θεμάτων που ανακύπτουν από τις διαφορετικές νομοθεσίες των εμπλεκομένων χωρών.

2. **Έλλειψη διεθνούς νομοθεσίας, μηχανισμών και καναλιών συνεργασίας** ανάμεσα στις υπηρεσίες εφαρμογής του νόμου, τις Ομάδες Αντιμετώπισης Περιστατικών (CERTs) και τις κρατικές αρχές για την διευκόλυνση της ανταλλαγής δεδομένων στο πλαίσιο διεξαγωγής εγκληματολογικών ερευνών.

3. **Γραφειοκρατία και δυσκολίες στη συνεργασία των διωκτικών αρχών:** στο κεφάλαιο 4 παρατέθηκαν ορισμένα τέτοια προβλήματα, όπως αυτά που ανέφερε ο Alexander Seger: δυσκολία με την οποία οι διωκτικές αρχές απαιτούν τη μεταβίβαση κάποιου αποδεικτικού στοιχείου από τις δικαστικές αρχές μιας άλλης χώρας, ισχυρότατο ενδεχόμενο να απορριφθούν αποδεικτικά στοιχεία μιας υπόθεσης από τον δικαστή που εκδικάζει το έγκλημα, μιας που τα στοιχεία αυτά αποκτήθηκαν με τρόπο που δεν είναι συμβατός νομικά με τη χώρα στην οποία εκδικάζεται το έγκλημα, πολύ αργή ταχύτητα με την οποία ανταλλάσσονται πληροφορίες και

αποδεικτικά στοιχεία ανάμεσα σε χώρες που έχουν συνάψει μεταξύ τους Συμφωνίες Αμοιβαίας Δικαστικής Συνδρομής (Mutual Legal Agreement Treaties / MLATs).

4. **Έλλειψη κανονιστικού πλαισίου για τις υποχρεώσεις των παρόχων:** Δεν υπάρχει ειδικό κανονιστικό πλαίσιο που να καθορίζει με ακρίβεια τις υποχρεώσεις των παρόχων υπηρεσιών νέφους ως προς τη διεξαγωγή εγκληματολογικών ερευνών. Για παράδειγμα ένα πλαίσιο που να ορίζει το χρονικό διάστημα μέσα στο οποίο ένας πάροχος πρέπει να παραδώσει τα στοιχεία που του ζητούνται, τις ενέργειες στις οποίες να προβαίνει πριν και μετά την έναρξη των εγκληματολογικών ερευνών, το πώς θα πρέπει να φυλάσσονται τα δεδομένα και τα αποδεικτικά στοιχεία, ώστε να εξασφαλίζεται η ακεραιότητά τους, κλπ. Ως εκ τούτου, κάθε πάροχος πράττει κατά βούληση στα ζητήματα αυτά.

5. **Έλλειψη επίσημων συμφωνιών μεταξύ των παρόχων** για τη διευκόλυνση της εγκληματολογικής έρευνας.

6. **Νομική απαγόρευση εξαγωγής δεδομένων πολιτών σε άλλες χώρες:** ορισμένες χώρες απαγορεύουν ρητά την εξαγωγή συγκεκριμένων κατηγοριών πληροφοριών προς τρίτες, ακόμα και αν οι πληροφορίες αυτά (/τα δεδομένα αυτά) ζητώνται με επίσημα έγγραφα διωκτικών αρχών.

7. **Έλλειψη συμφωνητικών παροχής υπηρεσιών (SLAs) που να περιλαμβάνουν συγκεκριμένες προβλέψεις για ζητήματα εγκληματολογικής έρευνας:** όπως πολλάκις επισημάνθηκε στην παρούσα μελέτη, οι προβλέψεις των συμφωνητικών παροχής υπηρεσιών για τα ζητήματα εγκληματολογικής έρευνας, είναι ένα από τα πιο αποτελεσματικά εργαλεία για την επιτυχή διεξαγωγή τέτοιων ερευνών. Όμως τέτοιες προβλέψεις σπανίως περιλαμβάνονται στα συμφωνητικά παροχής υπηρεσιών.

8. **Ειδικά για τον χώρο της ΕΕ, η έρευνα του ENISA παραθέτει τις ακόλουθες προκλήσεις:**

    i. Δαιδαλώδης νομοθεσία ανάμεσα στα κράτη μέλη: Δεν έχουν υιοθετήσει όλα τα κράτη μέλη την Οδηγία περί Προστασίας Δεδομένων Προσωπικού Χαρακτήρα 95/46/ΕΚ [56] με αποτέλεσμα το κάθε κράτος μέλος να εφαρμόζει δική του νομοθεσία στο ζήτημα της προστασίας δεδομένων προσωπικού χαρακτήρα. Μάλιστα, κατόπιν της εφαρμογής του Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR), που προέβλεπε νέες απαιτήσεις στην προστασία των δεδομένων, το πρόβλημα αυτό οξύνθηκε περαιτέρω.

    ii. Έλλειψη συνεργασίας, συντονισμού και καθορισμού αρμοδιοτήτων μεταξύ των διωκτικών αρχών των κρατών μελών της ΕΕ για ζητήματα πρόσβασης σε δεδομένα και ανταλλαγής τους.

iii. Έλλειψη ειδικών οδηγών βέλτιστων πρακτικών και προτύπων της ΕΕ που θα μπορούσαν να αξιοποιηθούν από τα κράτη μέλη για τη διεξαγωγή εγκληματολογικών ερευνών στο νέφος. Η έλλειψη αυτή μπορεί να προκαλέσει προβλήματα σε περίπτωση επίθεσης σε βάρος υποδομών ζωτικής σημασίας που λειτουργούν στο νέφος ή συνεργάζονται με αυτό.

iv. Οι μεγάλοι πάροχοι υπηρεσιών νέφους έχουν την έδρα τους σε χώρες εκτός ΕΕ. Αυτό έχει ως αποτέλεσμα να μη δεσμεύονται από την ευρωπαϊκή νομοθεσία και να εφαρμόζουν το δίκαιο της χώρας που εδρεύουν (συνήθως οι ΗΠΑ).

7.2 Ανοικτά ζητήματα

Μέχρι τώρα παρουσιάστηκαν ζητήματα που αφορούν την εγκληματολογία στην υπολογιστική νέφους και τα οποία αποτελούν προκλήσεις για την επιστημονική κοινότητα, τους νομοθέτες ή τους παράγοντες που δραστηριοποιούνται στο οικοσύστημα του νέφους.

Υπάρχουν όμως και άλλα ζητήματα τα οποία παραμένουν ανοικτά. Ακολούθως παρατίθενται ορισμένα:

1. **Επιθέσεις υποστηριζόμενες από κράτη (state-sponsored attacks):** όταν ένα κράτος αποφασίζει να υποστηρίξει εγκληματικές ενέργειες στο χώρο του νέφους, τότε η εγκληματολογική έρευνα που θα διενεργηθεί για αυτό το περιστατικό θα είναι κατά κανόνα καταδικασμένη να αποτύχει. Και τούτο διότι αυτά τα κράτη συνήθως δεν είναι πρόθυμα να καταδείξουν τον εγκληματία με τον οποίο συνεργάζονται και ο οποίος ενδεχομένως να διεκπεραιώνει εγκληματικές ενέργειες που το ίδιο το κράτος τους αναθέτει.
2. **Περιφρόνηση του Διεθνούς Δικαίου:** Στο κεφάλαιο 4 αναφέρθηκε η περίπτωση της Ρωσίας, μιας χώρας που δεν έχει υπογράψει τη Σύμβαση της Βουδαπέστης. Μάλιστα, όπως επισήμαναν οι Theresa Hitchens και Nilsu Goren στο κεφάλαιο 4, ενδεικτικό της απροθυμίας της να βοηθήσει άλλα κράτη στην εξιχνίαση εγκλημάτων του κυβερνοχώρου που έχουν ως έδρα την ίδια, είναι η άρνησή της να εγκρίνει τη χορήγηση πρόσβασης σε πληροφοριακούς πόρους που βρίσκονται στην επικράτειά της ακόμα και στην Interpol.

Κατόπιν αυτών, όσο τα παραπάνω ζητήματα παραμένουν ανοικτά, όσες επιστημονικές μελέτες και να εκπονηθούν, δεν θα μπορούν να καλύψουν πλήρως τα κενά που ανακύπτουν.

Κεφάλαιο 8 - Συμπεράσματα και Προτάσεις

Η υπολογιστική νέφους διεισδύει σταδιακά όλο και πιο πολύ στο χώρο των υποδομών ζωτικής σημασίας. Τούτο συμβαίνει ήδη σε πολύ μεγάλο βαθμό στον χώρο των ΗΠΑ – κάτι που δεν είναι άσχετο με το γεγονός ότι οι μεγάλοι πάροχοι νέφους έχουν την έδρα τους στη συγκεκριμένη χώρα. Ακολουθούν, με κάποια απόσταση, οι άλλες δυο περιοχές που εξετάστηκαν, δηλαδή η ΕΕ και η Ρωσία. Το κυβερνοέγκλημα που αναπτύσσεται στο οικοσύστημα του νέφους, επηρεάζει πλέον και τις υποδομές ζωτικής σημασίας, που λόγω της κρισιμότητάς τους, έχουν μεγαλύτερες απαιτήσεις σε προστασία. Η εγκληματολογική έρευνα υπολογιστικής νέφους που αφορά υποδομές ζωτικής σημασίας έρχεται να συμβάλλει στην προστασία αυτών των υποδομών. Αυτό γίνεται όχι μόνο με τον εντοπισμό και τη δίωξη των εγκληματιών, αλλά και με την ανάδειξη των τρόπων που επιτέθηκαν στις υποδομές αυτές, εξέλιξη που οδηγεί στη μελλοντική αποτροπή παρόμοιων επιθέσεων. Κατωτέρω παρουσιάζεται μια σειρά συμπερασμάτων γύρω από το θέμα που αναπτύχθηκε και υποβάλλονται προτάσεις, ως πιθανές μελλοντικές λύσεις στις προκλήσεις αυτού του χώρου.

8.1 Συμπεράσματα

Τα ακόλουθα συμπεράσματα ανακύπτουν από τη μελέτη αυτή και όσες άλλες συμπεριλήφθηκαν κατά την εκπόνησή της:

1. Η έγκαιρη και ακριβής ταυτοποίηση των επιτιθέμενων είναι, μεταξύ άλλων, ένα από τα ζητήματα στα οποία πρέπει να επικεντρωθεί η επιστημονική έρευνα γύρω από την προστασία των υποδομών ζωτικής σημασίας. Η επισήμανση αυτή είναι σχεδόν ταυτόσημη με την έννοια της εγκληματολογικής έρευνας, μιας που ο σκοπός της τελευταίας είναι ακριβώς η ταυτοποίηση του επιτιθέμενου με τρόπο τέτοιο που να τεκμηριώνει νομικά την δίωξή του.

2. Ο όγκος των προς εξιχνίαση υποθέσεων κυβερνοεγκλήματος στο χώρο του νέφους είναι ήδη πολύ μεγάλος προκαλώντας ήδη καταπόνηση στις ανά τον κόσμο διωκτικές αρχές. Ο όγκος αυτών των υποθέσεων αναμένεται να αυξηθεί περαιτέρω, αντί να μειωθεί. Η συσσώρευση αυτή προκαλεί δυστυχώς καθυστερούμενο απόθεμα (backlog), διαρκώς αυξανόμενο.

3. Επειδή οι κυβερνοεπιθέσεις στον χώρο του νέφους αυξάνονται όλο και πιο πολύ, προκαλούνται όλο και περισσότερα προβλήματα σε σημαντικούς τομείς υποδομών ζωτικής σημασίας (όπως, μεταξύ άλλων, οι επικοινωνίες, οι μεταφορές και η ενέργεια). Στη μελέτη αυτή παρουσιάστηκαν περιπτώσεις επιθέσεων στο χώρο του νέφους με δραματικές επιπτώσεις στους τομείς της άμυνας, της οικονομίας και της υγείας (ιδίως στον χώρο των ΗΠΑ).

4. Όπως προκύπτει από το κεφάλαιο 3, η διαδικασία με την οποία γίνεται η προτεραιοποίηση κατά σειρά κρισιμότητας των υποδομών ζωτικής σημασίας, ονομάζεται «προσδιορισμός κινδύνου» (risk assessment). Η διαδικασία αυτή πρέπει εξ αρχής να λαμβάνει χώρα, ώστε να επιτυγχάνεται αποτελεσματική προστασία αυτών των υποδομών. Αυτό οφείλεται στο ότι οι υποδομές ζωτικής σημασίας δεν είναι οι ίδιες για όλα τα κράτη ή όλους τους υπερεθνικούς οργανισμούς (πχ ΕΕ). Άρα κάθε κράτος ή υπερεθνικός οργανισμός έχει τα δικά του κριτήρια για τον χαρακτηρισμό μιας υποδομής ως «ζωτικής σημασίας». Με τον προσδιορισμό κινδύνου, ταξινομούνται κατά κρισιμότητα οι υποδομές αυτές, οπότε αναλόγως κατανέμονται και οι πόροι που απαιτούνται για την προστασία τους.

5. Η ψηφιακή εγκληματολογία στον χώρο του νέφους είναι πιο δύσκολη και πιο πολύπλοκη σε σχέση με την παραδοσιακή ψηφιακή εγκληματολογία. Αυτό οφείλεται στους εξής κυρίως λόγους: α) νομικά ζητήματα που αφορούν την ιδιοκτησία των δεδομένων πολλών διαφορετικών χρηστών στο ίδιο σύστημα, β) περιορισμένη και απομακρυσμένη πρόσβαση στα δεδομένα, γ) αποκεντρωμένη φύση (δηλαδή τη γεωγραφική διασπορά) των δεδομένων, δ) έλλειψη συνεργασίας ανάμεσα στους παρόχους του νέφους αλλά και ανάμεσα στις ανά τον κόσμο διωκτικές αρχές, ε) εξαιρετική δυσκολία στη συλλογή και ενσωμάτωση των αρχείων καταγραφής κινήσεων σε μια ενιαία κονσόλα, στ) έλλειψη εξειδικευμένων εργαλείων, προτύπων και κοινά αποδεκτών πρακτικών διεξαγωγής εγκληματολογικών ερευνών στο νέφος, ζ) έλλειψη επαρκών σχημάτων εκπαίδευσης και πιστοποίησης ερευνητών στον συγκεκριμένο χώρο.

6. Οι δυσκολίες στη διεξαγωγή εγκληματολογικών ερευνών στο νέφος προκύπτουν πρωτίστως από θεσμικά ζητήματα, παρά από τεχνικά.

7. Ένα σημαντικό εργαλείο για την επιτυχή διεξαγωγή εγκληματολογικών ερευνών στο νέφος, είναι τα συμφωνητικά παροχής υπηρεσιών (SLAs), διότι συμβάλλουν στην καλύτερη οργάνωση, συντονισμό και διεξαγωγή της έρευνας. Στα συμφωνητικά παροχής υπηρεσιών μπορεί, κατά τη σύναψή τους, να γίνει πρόβλεψη συγκεκριμένων ενεργειών, διαδικασιών, αρμοδιοτήτων και υποχρεώσεων περί εγκληματολογικής έρευνας. Χωρίς τις προβλέψεις αυτές, την κρίσιμη στιγμή της διεξαγωγής εγκληματολογικής έρευνας, ο κάθε παράγοντας (πάροχος, πελάτης, τρίτος φορέας) είναι πιθανό να πράξει κατά τον τρόπο που αυτός αντιλαμβάνεται τα πράγματα, προκαλώντας ίσως προβλήματα.

8. Η προσέγγιση Forensics-as-a-Service αναδεικνύεται, προς το παρόν, ως η πιο αποτελεσματική αλλά και πιο συμφέρουσα μέθοδος εγκληματολογικών ερευνών στο νέφος. Αυτό οφείλεται στη δυνατότητα που παρέχει για επεξεργασία μεγάλου όγκου δεδομένων εγκληματολογικών ερευνών. Για την αξιολόγηση υπηρεσιών Forensics-as-a-Service μπορούν να χρησιμοποιηθούν τα κριτήρια που επικαλούνται οι van Beek et al. στη μελέτη τους (βλ. κεφάλαιο 4). Αυτά είναι τα

εξής: α) η ασφάλεια, β) η ιδιωτικότητα, γ) η διαφάνεια, δ) η υποστήριξη πολυμίσθωσης (multi-tenancy), ε) η δυνατότητα μελλοντικών επεκτάσεων, στ) η διαφύλαξη της ακεραιότητας των δεδομένων, ζ) η αξιοπιστία και η) η υψηλή διαθεσιμότητα.

9. Επιτυχής εγκληματολογική έρευνα η διαδικασία που οδηγεί στην τελεσίδικη καταδίκη του επιτιθέμενου. Όχι απλώς ο εντοπισμός του.

8.2 Προτάσεις

Σε πολλά σημεία της παρούσας μελέτης παρουσιάσθηκαν προτάσεις για την επίλυση διαφόρων ζητημάτων. Στη συνέχεια παρατίθεται σύνοψη αυτών των προτάσεων σε ένα ενιαίο πλαίσιο. Οι προτάσεις χωρίζονται σε αυτές που αφορούν τεχνικά ζητήματα και σε εκείνες που αφορούν θεσμικά ζητήματα.

8.2.1 Προτάσεις σε Τεχνικό Επίπεδο

1. Σχεδιασμός και υλοποίηση σχημάτων πιστοποίησης για εγκληματολογικές έρευνες, που να αφορούν παρόχους υπηρεσιών νέφους αλλά και φυσικά πρόσωπα που έχουν ή επιθυμούν να αποκτήσουν την ιδιότητα του ερευνητή ψηφιακής εγκληματολογίας στο νέφος.

2. Σχεδιασμός νέων τεχνικών εγκληματολογικής διερεύνησης, με τρόπο τέτοιο που να μπορούν να εφαρμοστούν από οπουδήποτε, οποτεδήποτε, καθ' οιονδήποτε τρόπο (δηλαδή είτε on-line, είτε off-line, είτε επιτόπου) και χωρίς να θέτουν σε κίνδυνο την απόδοση ή τη λειτουργία του υπό διερεύνηση συστήματος υποδομής ζωτικής σημασίας.

3. Διασύνδεση των διωκτικών αρχών σε παγκόσμιο επίπεδο.

4. Αξιοποίηση και περαιτέρω ανάπτυξη έτοιμων λύσεων λογισμικού ψηφιακής εγκληματολογίας νέφους, όπως για παράδειγμα αυτή των Shumian Yang, Lianhai Wang, Dawei Zhao, Guangqi Liu και Shuhui Zhang [9] ή εκείνης των Michael P . Vega, James Regan, Matteo Michelini και Jean - Francois Legault [10] για λογαριασμό της JP Morgan Chase Bank, που παρουσιάστηκαν στο κεφάλαιο 2.

5. Ανάπτυξη νέων λύσεων λογισμικού εγκληματολογικών ερευνών στο νέφος, που να ικανοποιούν όσο το δυνατόν περισσότερες από τις ακόλουθες απαιτήσεις:

    i. Αρχιτεκτονική που να βασίζεται στις βέλτιστες πρακτικές καθιερωμένων οδηγών που επικαλούνται οι Ameer Pichan, Mihai Lazarescu και Sie Teng Soh [7] στο Κεφάλαιο 2, όπως για παράδειγμα ο Οδηγός Βέλτιστων Πρακτικών στην Ψηφιακή Εγκληματολογία της Ένωσης Αξιωματικών Αστυνομίας του Ηνωμένου Βασιλείου (ACPO), και ο Οδηγός για την Ενσωμάτωση των Εγκληματολογικών Τεχνικών στην Αντιμετώπιση Περιστατικών του Αμερικανικού Εθνικού Οργανισμού Προτύπων και Τεχνολογίας (NIST)[1].

ii. Συμμόρφωση προς τα πρότυπα διωκτικών και των εποπτικών ανά κλάδο Αρχών, όπως αυτά που αναλύθηκαν στο κεφάλαιο 4.

iii. Κρυπτογραφημένη βάση δεδομένων για την καταγραφή των τεκμηρίων, των πληροφοριών που αφορούν τους συμμετέχοντες στο περιστατικό (όπως ονοματεπώνυμα, στοιχεία ταυτότητας, profiles, κλπ), τους τρόπους διενέργειας των επιθέσεων (signatures), τα αρχεία καταγραφής κινήσεων (logs), και άλλα.

iv. Ενσωμάτωση σύγχρονων τεχνολογιών κρυπτογράφησης για την προστασία των αρχείων καταγραφής κινήσεων και των τεκμηρίων, όπως για παράδειγμα αυτές που παρουσιάστηκαν στο κεφάλαιο 2, ήτοι: α) η τεχνική BlockSLaaS (Blockchain Assisted Secure Logging-as-a-Service) με χρήση του blockchain που προτείνουν οι Sagar Rane et al., β) η τεχνική με χρήση του αλγόριθμου Υπογραφής Κατωφλίου RSA (“RSA Threshold Signature”) που προτείνουν οι Afzaal et al., γ) η μέθοδος CLASS (Cloud Log Assuring Soundness and Secrecy) που προτείνουν οι Ahsan, Manazir et al.

v. Δυνατότητες συνεργασίας μέσω έτοιμων διεπαφών (interfaces) με πολλαπλούς παρόχους (multi-cloud capabilities), πολλαπλά συστήματα Διαχείρισης Πληροφορίων και Περιστατικών Ασφαλείας (Security Information and Event Management / SIEM systems) και πολλαπλές λύσεις λογισμικού εγκληματολογικών ερευνών, όπως για παράδειγμα αυτές που παρουσιάστηκαν στο Κεφάλαιο 2 (από IBM, Oracle, κλπ)

vi. Κρυπτογραφημένη και καλά προστατευμένη πρόσβαση σε υποδομές κρατικών και διεθνών διωκτικών αρχών, στο πρότυπο του συστήματος LEIP της IBM στις ΗΠΑ.

vii. Καταγραφή και παρακολούθηση τρεχόντων υποθέσεων και ερευνών εγκληματολογίας, με χρήση σύγχρονων τεχνικών διαχείρισης ροών εργασιών εγκληματολογικών ερευνών (forensic data processing workflows), όπως αυτή που προτείνουν οι Yuanfeng Wen, Xiaoxi Man, Khoa Le και Weidong Shi στο κεφάλαιο 4.

viii. Αρχειοθέτηση ολοκληρωμένων υποθέσεων εγκληματολογικής έρευνας, που να περιλαμβάνει σύντομη περιγραφή του ιστορικού και της κατάληξης (της έρευνας), λέξεις κλειδιά, χαρακτηριστικά των profiles των συμμετεχόντων, signatures των επιθέσεων και άλλα κρίσιμα στοιχεία της έρευνας.

ix. Δυνατότητα γρήγορης αναζήτησης εννοιών, ψηφιακών τεκμηρίων, προτύπων και λέξεων κλειδιών, σαν αυτή που προτείνουν οι Jooyoung Lee και Sungyong Un στη μελέτη τους για την υπηρεσία «Indexed-Search-as-a-Service» (βλ. κεφάλαιο 4).

x. Χρήση αυτόματων λειτουργιών νέφους (Functions-as-a-Service) για την υποβολή, τη διαχείριση και τη διεκπεραίωση αιτημάτων εγκληματολογίας.

xi. Ειδικά για την υποστήριξη εγκληματολογικών ερευνών για υποδομές ζωτικής σημασίας, εξαιρετική σημασία έχουν και τα παρακάτω χαρακτηριστικά. Αυτά έρχονται να κατατάξουν τις ΥΖΣ ανάλογα με την κρισιμότητά τους και να προσδιορίσουν τους αναγκαίους πόρους για την προστασία τους:

a. Λειτουργία διεξαγωγής Risk Assessment για τον προσδιορισμό της κρισιμότητας της κάθε υποδομής, με χρήση μεθόδων σαν αυτές που αναφέρονται στο κεφάλαιο 3 στη μελέτη των Georgios Giannopoulos et al.

b. Λειτουργία αξιολόγησης επιθέσεων και τρωτών σημείων, όπως αυτή που παρουσιάστηκε στο κεφάλαιο 3 των Venkata Reddy Palleti et al., η οποία, με βάση τις αρχές της θεωρίας του αξιωματικού σχεδιασμού (axiomatic design) σχηματίζει ένα εργαλείο μοντελοποίησης των ΥΖΣ.

c. Δυνατότητα αυτόματης δημιουργίας εγκληματολογικών σεναρίων (/υποθέσεων) με χρήση Τεχνητής Νοημοσύνης που τροφοδοτείται τόσο από τα τρέχοντα τεκμήρια όσο και προηγούμενες περιπτώσεις (λεπτομέρειες για τη λειτουργία αυτή παρουσιάσθηκαν στο κεφάλαιο 3, με αναφορά στη μελέτη των Cristina Alcaraz και Sherali Zeadallly).

8.2.2 Προτάσεις σε Θεσμικό Επίπεδο

1. Προαγωγή του διαλόγου ανάμεσα στις πολιτικές ηγεσίες, τις διωκτικές αρχές και τις ομάδες αντιμετώπισης περιστατικών (CERTs) με σκοπό την αντιμετώπιση προβλημάτων δικαιοδοσίας και εφαρμοστέου δικαίου κατά τη διεξαγωγή εγκληματολογικών ερευνών.

2. Σύναψη περισσότερων πολυμερών (multilateral) ή διμερών (bilateral) συμφωνιών αμοιβαίας δικαστικές συνδρομής (MLATs), διότι σύμφωνα με τη μελέτη των Pichan et al. [7] δίνουν λύση σε πλήθος ζητημάτων.

3. Διαμόρφωση οδηγών από εθνικούς και διεθνείς φορείς κυβερνοασφάλειας (πχ ENISA, NSA, NCSC, CSA, κλπ) που να αναφέρονται: α) στις προβλέψεις που πρέπει να περιλαμβάνονται σε συμφωνητικά παροχής υπηρεσιών (SLAs) υπολογιστικής νέφους αναφορικά με τα ζητήματα εγκληματολογικών ερευνών, β) στις διαδικαστικές και τεχνικές προδιαγραφές που να πρέπει να πληρούνται στο σκέλος της επιμέλειας αλυσίδας (Chain of Custody), ώστε να εξασφαλίζεται η τεκμηρίωση της ακεραιότητας των ψηφιακών τεκμηρίων με τρόπο ενιαίο, κατανοητό και ευπαρουσίαστο.

4. Σχεδιασμός και προώθηση προγραμμάτων εκπαίδευσης των κατά τόπους διωκτικών αρχών αλλά και των ομάδων αντιμετώπισης περιστατικών ασφάλειας (CERTs) στο αντικείμενο των εγκληματολογικών ερευνών στην υπολογιστική νέφους.

5. Ειδικότερα για τον χώρο της ΕΕ, ο Ευρωπαϊκός Οργανισμός Κυβερνοασφάλειας (ENISA) [53] παραθέτει το ακόλουθο πακέτο προτάσεων για την προστασία των ΥΖΣ:

   i. Τα κράτη μέλη πρέπει να προβούν στη δημιουργία συγκεκριμένων πολιτικών και κατευθυντήριων οδηγιών για τα Κέντρα Λειτουργιών Ασφάλειας (Security Operations Centers / SOCs) που διαθέτουν, ώστε να διευκολύνουν την ανταλλαγή πληροφοριών και να προάγουν την από κοινού διερεύνηση περιστατικών κυβερνοασφάλειας.

   ii. Πρέπει να θεσπιστούν κανόνες και διαδικασίες σε πανευρωπαϊκό επίπεδο που να διευκολύνουν τη συνεργασία ανάμεσα στους φορείς του νέφους (όπως πάροχοι, πελάτες, τρίτοι παράγοντες) και τις διωκτικές αρχές κρατών μελών και Ευρωπαϊκής Ένωσης.

   iii. Οι εγκληματολογικές έρευνες στην υπολογιστική νέφους θα πρέπει στο εξής να αποτελούν μέρος των εθνικών ασκήσεων κυβερνοασφάλειας του κάθε κράτους μέλους.

Βιβλιογραφία

1. ENISA, 2015. *Secure Use of Cloud Computing in the Finance Sector - Good practices and recommendations*, ISBN: 978-92-9204-138-0.
2. A. Roy, S. Midya, K. Majumder and S. Phadikar, 2018. *Forensics-as-a-Service for Mobile Cloud*, 4th IEEE International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN), 22-23 Nov., Kolkata, India, pp. 6-11, doi: 10.1109/ICRCICN.2018.8718702.
3. H. Cheng-Ta, K. Hung-Jui, Z. Zhi-Wei, S.Ping-Cheng, W. Shiuh-Jeng, 2018. *Mobile Forensics for Cloud Storage Service on iOS Systems*, IEEE International Symposium on Information Theory and Its Applications (ISITA), 28-31 Oct., Singapore, Singapore, pp. 178-182, doi: 10.23919/ISITA.2018.8664393.
4. Á. MacDermott, T. Baker, Q. Shi, 2018. *IoT Forensics: Challenges For The IoA Era*, 9th IEEE IFIP International Conference on New Technologies, Mobility and Security (NTMS), 26-28 Feb. 2018, Paris, France, pp. 1-5, doi: 10.1109/NTMS.2018.8328748.
5. R. Montasari, R. Hill, 2019. *Next-Generation Digital Forensics: Challenges and Future Paradigms*, 12th IEEE International Conference on Global Security, Safety and Sustainability (ICGS3), 16-18 Jan., London, United Kingdom, pp. 205-212, doi: 10.1109/ICGS3.2019.8688020.
6. R. Hunt, J. Slay, 2010. *Achieving Critical Infrastructure Protection through the Interaction of Computer Security and Network Forensics*, 8th IEEE Annual International Conference on Privacy, Security and Trust, Ottawa, ON, Canada, pp. 23-30, doi: 10.1109/PST.2010.5593243.
7. A. Pichan, M. Lazarescu, S. Teng Soh, 2015. Cloud forensics: Technical challenges, solutions and comparative analysis, *Digital Investigation*, Vol. 13, pp. 38-57, doi: 10.1016/j.diin.2015.03.002.
8. NIST Computer Security Division (CSD), 2006. *NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response*. [Διαδίκτυο] Διαθέσιμο: https://csrc.nist.gov/publications/detail/sp/800-86/final
9. S. Yang, L. Wang, D. Zhao, G. Liu, S. Zhang, 2018. *The Design of a Cloud Forensics Middleware System Base on Memory Analysis*, Proceedings of the Tenth International Conference on Soft Computing and Pattern Recognition (SoCPaR 2018), 13-15 Dec., Porto, Portugal, pp. 258-267, doi: 10.1007/978-3-030-17065-3_26.

10. M. P. Vega, J. Regan, M. Michelini, J.-F. Legault, 2018. *System And Method For Implementing Digital Cloud Forensics*, Patent Number: WO2019/028328Al, US.
11. C. Alcaraz, S. Zeadally, 2015. Critical infrastructure protection: Requirements and challenges for the 21st century, *International Journal of Critical Infrastructure Protection*, Vol. 8, pp. 53-66, doi: 10.1016/j.ijcip.2014.12.002.
12. V.R. Palleti, J.V. Joseph, A. Silva, 2018. *A contribution of axiomatic design principles to the analysis and impact of attacks on critical infrastructures*, International Journal of Critical Infrastructure Protection, Vol. 23, pp. 21-32, doi: 10.1016/j.ijcip.2018.08.007.
13. Το Συμβούλιο Της Ευρωπαϊκής Ένωσης, 2008. *Οδηγία 2008/114/ΕΚ του Συμβουλίου, της 8ης Δεκεμβρίου 2008 , σχετικά με τον προσδιορισμό και τον χαρακτηρισμό των ευρωπαϊκών υποδομών ζωτικής σημασίας, και σχετικά με την αξιολόγηση της ανάγκης βελτίωσης της προστασίας τους*. [Διαδίκτυο] Διαθέσιμο: https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:32008L0114&from=EN.
14. USA President's Commission on Critical Infrastructure Protection, 1997. *Critical Foundations - Protecting America's Infrastructures*. [Διαδίκτυο] Διαθέσιμο: https://www.hsdl.org/?view&did=986.
15. K. Pynnöniemi (ed.), 2012. *Russian critical infrastructures - Vulnerabilities and policies.* Elsinki: The Finnish Institute of International Affairs, ISBN: 978-951-769-365-3.
16. G. Giannopoulos, R. Filippini, M. Schimmer, 2012. *Risk assessment methodologies for Critical Infrastructure Protection. Part I: A state of the art*. Ispra, Italy: Institute for the Protection and Security of the Citizen, ISBN: 978-92-79-23839-0.
17. L. Maglaras, K.H. Kim, H. Janicke, M.A. Ferrag, S. Rallis, P. Fragkou, A. Maglaras, T.J. Cruz, 2018. Cyber security of critical infrastructures, *ICT Express*, Vol. 4, pp. 42-45, doi: 10.1016/j.icte.2018.02.001.
18. M. Afzaal, C. Di Sarno, L. Coppolino, S. D'Antonio, L. Romano, 2012. *A Resilient Architecture for Forensic Storage of Events in Critical Infrastructures,* 14th IEEE International Symposium on High-Assurance Systems Engineering, 25-27 Oct., Omaha, NE, USA, pp. 48-55, doi: 10.1109/HASE.2012.9.
19. R.L. Rivest, A. Shamir, L. Adleman, 1978. A method for obtaining digital signatures and public-key cryptosystems*, Communications of the ACM,* Vol. 21, pp. 120-126, doi: 10.1145/359340.359342.
20. Council Of Europe, 2001. *Convention on Cybercrime*. Budapest: Secretary General of the Council of Europe, [Διαδίκτυο] Διαθέσιμο: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.

21. K.F. Sliwinski, 2014. Moving beyond the European Union's Weakness as a Cyber-Security Agent, *Contemporary Security Policy,* Vol. 35, pp. 468-486, doi: 10.1080/13523260.2014.959261.
22. Ευρωπαϊκή Επιτροπή, 2013. *Στρατηγική της Ευρωπαϊκής Ένωσης για την ασφάλεια στον κυβερνοχώρο: Για έναν ανοικτό, ασφαλή και προστατευμένο κυβερνοχώρο*. [Διαδίκτυο] Διαθέσιμο:https://eur-lex.europa.eu/legal-content/EL/ALL/?uri=CELEX%3A52013JC0001.
23. P. Vitel, 2014. *Cyber Space And Euro-Atlantic Security*. Paris: NATO Parliamentary Assembly, Science and Technology Committee. [Διαδίκτυο] Διαθέσιμο: https://www.nato-pa.int/document/2014-209-stc-14-e-rev-1-fin-cyberspace-vitel-report
24. Ευρωπαϊκή Επιτροπή, 2013. *COMMISSION STAFF WORKING DOCUMENT on a new approach to the European Programme for Critical Infrastructure Protection: Making European Critical Infrastructures more secure*. [Διαδίκτυο] Διαθέσιμο: https://ec.europa.eu/energy/sites/ener/files/documents/20130828_epcip_commission_staff_working_document.pdf
25. Ευρωπαϊκή Επιτροπή, 2012. *Ανακοίνωσης Της Επιτροπής Στο Ευρωπαϊκό Κοινοβούλιο, Το Συμβούλιο, Την Ευρωπαϊκή Οικονομική Και Κοινωνική Επιτροπή Και την Επιτροπή Των Περιφερειών - Αξιοποίηση των δυνατοτήτων του υπολογιστικού νέφους*. [Διαδίκτυο] Διαθέσιμο: https://op.europa.eu/en/publication-detail/-/publication/43391748-d9cd-4fc0-a046-0b7e54f3da18/language-el/format-PDF/source-190083542.
26. United Nations Office On Drugs And Crime, 2004. *United Nations Convention Against Transnational Organized Crime And The Protocols Thereto*. Vienna: Vienna International Centre. [Διαδίκτυο] Διαθέσιμο: https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf.
27. U.S Department of Homeland Security / United States Secret Service, 2009. *UNITED STATES SECRET SERVICE SIGNS PARTNERSHIP AGREEMENT WITH ITALIAN OFFICIALS ESTABLISHING THE FIRST EUROPEAN ELECTRONIC CRIMES TASK FORCE - New task force to combat transnational cybercrime*. [Διαδίκτυο] Διαθέσιμο: https://www.secretservice.gov/press/releases/2009/07/united-states-secret-service-signs-partnership-agreement-italian-officials.

28. U.S. Department of State, 2015. *The Guidelines for U.S.-Japan Defense Cooperation*. [Διαδίκτυο] Διαθέσιμο: https://archive.defense.gov/pubs/20150427_--_GUIDELINES_FOR_US-JAPAN_DEFENSE_COOPERATION.pdf.
29. H. W. Scott, L. C. Martin, T. Motohiro, I. Yurie, C. Roger, J. Ken, T. Yuki, 2016. *U.S.-Japan Alliance Conference: Strengthening Strategic Cooperation,* U.S.-Japan Alliance Conference, 14-15 Mar., Santa Monica, CA, USA, doi: 10.7249/CF351.
30. The White House, 2017. *Statement from the Press Secretary on the United States-China Visit*. [Διαδίκτυο] Διαθέσιμο: https://trumpwhitehouse.archives.gov/briefings-statements/statement-press-secretary-united-states-china-visit/
31. T. Hitchens, N. Goren, 2017. *International Cybersecurity Information Sharing Agreements*. College Park, MD, USA: Center for International & Security Studies, [Διαδίκτυο] Διαθέσιμο: https://cissm.umd.edu/research-impact/publications/international-cybersecurity-information-sharing-agreements.
32. The Shanghai Cooperation Organisation (SCO), 2001. *Declaration On The Establishment Of The Shanghai Cooperation Organization*. [Διαδίκτυο] Διαθέσιμο: http://eng.sectsco.org/load/193054/.
33. Government Of The Russian Federation, 2015. *Agreement Between The Government Of The Russian Federation And The Government Of The People'S Republic Of China On Cooperation In Ensuring International Information Security*. [Διαδίκτυο] Διαθέσιμο: https:\\cyber-peace.org\wp-content\uploads\2013\05\RUS-CHN_CyberSecurityAgreement201504_InofficialTranslation.pdf
34. N. Chourci, S. Madnick, J. Ferwerda, 2014. Institutions for Cyber Security: International Responses and Global Imperatives, *Information Technology for Development*, Vol. 20, pp. 96-121. hdl: 1721.1/109401.
35. R.B. Van Baar, H.M.A. Van Beek, E.J. Van Eijk, 2014. Digital Forensics as a Service: A game changer, *Digital Investigation*, Vol. 11, pp. 54-62. doi: 10.1016/j.diin.2014.03.007.
36. J. Dykstra, A.T. Sherman, 2012. Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques, *Digital Investigation*, Vol. 9, pp. 90-98. doi: 10.1016/j.diin.2012.05.001.
37. X. Du, L.K. Nhien-An, M. Scanlon, 2017. *Evaluation of Digital Forensic Process Models with Respect to Digital Forensics as a Service*, 16th European Conference on Cyber Warfare and Security (ECCWS 2017), 29-30 Jun, Dublin, Ireland, arXiv:1708.01730.

38. H.M.A. Van Beek, E.J. Van Eijk, R.B. Van Baar, M. Ugen, J.N.C. Bodde, A.J. Siemenlik, 2015. Digital forensics as a service: Game on, *Digital Investigation*, Vol. 15, pp. 20-38, doi: 10.1016/j.diin.2015.07.004
39. J. Lee, S. Un, 2012. *Digital Forensics as a Service: A case study of forensic indexed search*, IEEE International Conference on ICT Convergence (ICTC), 15-17 Oct., Jeju, South Korea, pp. 499-503, doi:10.1109/ICTC.2012.6387185.
40. Y. Wen, X. Man, K. Le, W. Shi, 2013. *Forensics-as-a-Service (FaaS): Computer Forensic Workflow Management and Processing Using Cloud*, 4th International Conference on Cloud Computing, GRIDs, and Virtualization, 27 May - 1 Jun., Valencia, Spain, pp. 208-214, ISBN:978-1-61208-271-4.
41. S. Rane, A. Dixit, 2018. *BlockSLaaS: Blockchain Assisted Secure Logging-as-a-Service for Cloud Forensics*, Security and Privacy: Second ISEA International Conference, ISEA-ISAP, 9-11 Jan., Jaipur, India, pp.77-88, doi: 10.1007/978-981-13-7561-3_6.
42. S.A. Ali, S. Memon, F. Sahito, 2018. *Challenges and Solutions in Cloud Forensics*, ICCBDC'18 2nd International Conference on Cloud and Big Data Computing, 3-5 Aug., Barcelona, Spain, pp. 6-10, doi: 10.1145/3264560.3264565.
43. Carnegie Mellon University and The Johns Hopkins University Applied Physics Laboratory LLC, 2020. *Cybersecurity Maturity Model Certification (CMMC) Version 1.02*. [Διαδίκτυο] Διαθέσιμο: https://www.acq.osd.mil/cmmc/draft.html
44. United States Congress, 208. *CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY ACT OF 2018*. [Διαδίκτυο] Διαθέσιμο: https://www.congress.gov/bill/115th-congress/house-bill/3359.
45. U.S. Department of the Treasury, 2020. *Department of the Treasury - Cybersecurity Enhancement Account - Congressional Budget Justification and Annual Performance Report and Plan - FY 2021, Section I – Budget Request*. [Διαδίκτυο] Διαθέσιμο: https://home.treasury.gov/system/files/266/04.-CEA-FY-2021-CJ.pdf.
46. U.S. Health Care Industry Cybersecurity Task Force, 2017. *Report On Improving Cybersecurity In The Health Care Industry*. [Διαδίκτυο] Διαθέσιμο: https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf.
47. C. Nicolas, 2019. U.S. DoD Enterprise DevSecOps Initiative (Software Factory) v1.7. [Διαδίκτυο] Διαθέσιμο: https://software.af.mil/wp-content/uploads/2019/12/DoD-Enterprise-DevSecOps-Initiative-Keynote-v1.7.pdf.
48. ENISA, 2020. *ENISA ETL2020 Data Breach*, ISBN:978-92-9204-354-4.
49. ENISA, 2020. *ENISA ETL2020 Information Leakage*, ISBN:978-92-9204-354-4.

50. US Office Of The Attorney General – Connecticut, 2019. *Connecticut And Illnois Open Investigation Into Quest Diagnostics, LabCorp Data Breach*. [Διαδίκτυο] Διαθέσιμο: https://portal.ct.gov/AG/Press-Releases/2019-Press-Releases/CT-AND-IL-OPEN-INVESTIGATION-INTO-QUEST-AND-LABCORP-DATA-BREACH.
51. ENISA, 2020. *Main Incidents In The EU And Worldwide - From January 2019 to April 2020*, ISBN:978-92-9204-354-4.
52. ENISA, 2020. *ENISA ETL2020 Phishing - From January 2019 to April 2020*, ISBN:978-92-9204-354-4.
53. ENISA, 2016. *Exploring Cloud Incidents*. [Διαδίκτυο] Διαθέσιμο: https://www.enisa.europa.eu/publications/exploring-cloud-incidents/at_download/fullReport.
54. D. Zou, J. Zhao, W. Li, Y. Wu, W. Qiang, H. Jin, Y. Wu, Y. Yifei, 2019. A Multigranularity Forensics and Analysis Method on Privacy Leakage in Cloud Environment, *IEEE Internet of Things Journal*, Vol. 6, pp. 1484 – 1494, doi: 10.1109/JIOT.2018.2838569.
55. Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο της Ευρωπαϊκής Ένωσης, 2016. *ΚΑΝΟΝΙΣΜΟΣ (ΕΕ) 2016/ 679 ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ - της 27ης Απριλίου 2016 - Γενικός Κανονισμός για την Προστασία Δεδομένων*. [Διαδίκτυο] Διαθέσιμο:https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32016R0679&from=EL.
56. Ευρωπαϊκό Κοινοβούλιο και το Συμβούλιο της Ευρωπαϊκής Ένωσης, 1995. *Οδηγία 95/46/ΕΚ ΤΟΥ ΕΥΡΩΠΑΪΚΟΥ ΚΟΙΝΟΒΟΥΛΙΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΙΟΥ - της 24ης Οκτωβρίου 1995*. [Διαδίκτυο] Διαθέσιμο: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:31995L0046&from=EL .
57. U.S. Federal Reserve System, 2020. *Federal Reserve Statistical Release - Large Commercial Banks*. [Διαδίκτυο] Διαθέσιμο: https://www.federalreserve.gov/releases/lbr/20200331/default.htm.

Παράρτημα Α

Δυνατότητες της AWS για λειτουργία ΥΖΣ και εγκληματολογική έρευνα

Πίνακας Παραρτήματος Ι. Πιστοποιήσεις της AWS για Βόρεια Αμερική, Ευρώπη, Μέση Ανατολή και Αφρική

Περιοχή	**Τίτλος Πιστοποίησης**
Βόρεια Αμερική (δηλ. ΗΠΑ και Καναδάς)	• CJIS - Criminal Justice Information Services • DoD SRG - DoD Data Processing • FedRAMP - Government Data Standards • FERPA - Educational Privacy Act • FIPS - Government Security Standards • FISMA - Federal Information Security Management • GxP - Quality Guidelines and Regulations • HIPAA - Protected Health Information • HITRUST CSF - Health Information Trust Alliance Common Security Framework • ITAR - International Arms Regulations • MPAA - Protected Media Content • NIST - National Institute of Standards and Technology • PIPEDA - Canada's Federal Private Sector Privacy Legislation • SEC Rule 17a-4(f) - Financial Data Standards • VPAT / Section 508 - Accessibility Standards
Ευρώπη, Μέση Ανατολή, Αφρική (Europe, Middle East, Africa / EMEA)	• ASIP HDS - Personal Health Data Protection in France • C5 - Operational Security Attestation in Germany • CISPE - Coalition of Cloud Infrastructure Services Providers in Europe • Cyber Essentials Plus - Cyber Threat Protection in the UK • ENS High - Government Standards in Spain • EU / US Privacy Shield - Privacy Shield Framework • G-Cloud - Government Standards in the UK • TISAX - Automotive Industry Standard

Πίνακας Παραρτήματος ΙΙ. Οι πλατφόρμες της AWS για τη λειτουργία Υποδομών Ζωτικής Σημασίας ειδικά για τις ΗΠΑ

Όνομα πλατφόρμας	**Λειτουργικά Χαρακτηριστικά**	**Τεχνικά Χαρακτηριστικά**
AWS GovCloud (US)[33]	• Επιτρέπει στους χρήστες - οι οποίοι εξ ορισμού είναι μόνον δημόσιοι υπάλληλοι / λειτουργοί των ΗΠΑ - να μπορούν να προσπελαύνουν σωρεία ευαίσθητων πληροφοριακών πόρων, όπως (ενδεικτικά): ✓ Ιατρικοί φάκελοι πολιτών ✓ Φορολογικά αρχεία και υποθέσεις ✓ Δεδομένα διωκτικών αρχών • Διευκολύνει τη διεξαγωγή	• Φέρει σημαντικές πιστοποιήσεις της αμερικανικής ομοσπονδιακής κυβέρνησης, όπως (ενδεικτικά): ✓ **FedRAMP** (Ομοσπονδιακό Πρόγραμμα Διαχείρισης Κινδύνων και Εξουσιοδοτήσεων - Federal Risk and Authorization Management Program / FedRAMP)

[33] https://aws.amazon.com/govcloud-us/?whats-new-ess.sort-by=item.additionalFields.postDateTime&whats-new-ess.sort-order=desc

	εγκληματολογικών ερευνών αφού επιτρέπει την προσπέλαση και χρήση πληροφοριών, στις οποίες μόνο το αμερικανικό δημόσιο έχει πρόσβαση.	✓ **CJIS** (Criminal Justice Information Services) του Υπουργείου Δικαιοσύνης ✓ **CCSRG** (Cloud Computing Security Requirements Guide / Impact Levels 2, 4 και 5) του Υπουργείου Άμυνας. • Κρυπτογράφηση δεδομένων για το περιβάλλον αποθήκευσης της AWS (δηλαδή το Amazon S3). • Αποθήκευση και διαχείριση μυστικών κλειδιών μέσω των εφαρμογών AWS CloudHSM και AWS Key Management Service (AWS KMS). • Διαχείριση προσβάσεων ανά φυσικό πρόσωπο, χρονική στιγμή, τοποθεσία, επιλεχθείσα ομοσπονδιακή υπηρεσία, τρόπο προσπέλασης. Για διεξαγωγή εγκληματολογικής έρευνας, παρέχει την εφαρμογή διαχείρισης των καταγραφών κινήσεων "**AWS CloudTrail**".
AWS Secret Region[34]	• Είναι ένας τομέας (Region) της AWS, που δεν έχει γεωγραφικά χαρακτηριστικά αλλά λειτουργικά. • Χρησιμοποιείται από την «Κοινότητα Πληροφοριών των Ηνωμένων Πολιτείων» (United States Intelligence Community / US IC)[35], στην οποία συμμετέχουν οι εξής υπηρεσίες (ενδεικτικά): ✓ Ομοσπονδιακό Γραφείο Ερευνών (Federal Bureau of Investigations / FBI) ✓ Κεντρική Υπηρεσία Πληροφοριών (Central Intelligence Agency / CIA) ✓ Υπηρεσία Εθνικής Ασφάλειας (National Security Agency / NSA) ✓ πληθώρα μυστικών υπηρεσιών των αμερικανικών ενόπλων δυνάμεων • Χειρίζεται και διεκπεραιώνει φορτία εργασιών του Αμερικανικού Δημοσίου τα οποία είναι διαβαθμισμένα μέχρι και το επίπεδο «Απόρρητο» ("Secret"). Το επίπεδο αυτό είναι το μεσαίο επίπεδο διαβάθμισης πληροφοριών του αμερικανικού κράτους, τα άλλα δυο επίπεδα είναι το «Άκρως Απόρρητο» (Top Secret), το οποίο είναι το ανώτατο, και το «Εμπιστευτικό» ("Confidential"), το κατώτατο[36]. • Διευκολύνει τις υπηρεσίες της Κοινότητας Πληροφοριών των Ηνωμένων Πολιτείων	• Φέρει σημαντικές πιστοποιήσεις της αμερικανικής ομοσπονδιακής κυβέρνησης, όπως (ενδεικτικά): ✓ **Intelligence Community Directive (ICD 503)** ✓ **National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 4.CJIS**

[34] https://aws.amazon.com/blogs/publicsector/announcing-the-new-aws-secret-region/
[35] https://www.intelligence.gov/how-the-ic-works
[36] The President of the United States of America, 2009. Executive Order 13526.

	στο να ανταλλάσσουν μεταξύ τους πληροφορίες και δεδομένα, στο πλαίσιο διεξαγωγής εγκληματολογικών ερευνών.	

Πίνακας Παραρτήματος III. Κατάλογος λογισμικού και μεγάλοι πελάτες της AWS στον χώρο της άμυνας των ΗΠΑ

Κατηγορία Λογισμικού	**Εφαρμογές**	**Μεγάλοι Πελάτες**
Ροές μεταφοράς δεδομένων (Streamlined Data Transfer)	• Amazon Kinesis • Amazon Athena • Amazon Redshift • Amazon ElastiCache • Amazon DynamoDB • Amazon Machine Learning	• Οργανισμός Εφοδιασμών (U.S. Defense Logistics Agency) • Πολεμικό Ναυτικό των ΗΠΑ (U.S. Navy). Το Πολεμικό Ναυτικό των ΗΠΑ (U.S. Navy) και οι Υπηρεσίες Εθνικής Ασφάλειας SAP (SAP National Security Services / SAP NS2) προέβησαν σε μετάπτωση του μεγαλύτερου συστήματος εταιρικού προγραμματισμού πόρων της SAP (SAP Enterprise Resource Planning / SAP ERP), το οποίο είχε 72000 χρήστες, στο νέφος της. • Πολεμική Αεροπορία των ΗΠΑ (U.S. Air Force) – Η Πολεμική Αεροπορία των ΗΠΑ (U.S. Air Force) χρησιμοποιεί το AWS GovCloud (US). • Διοίκηση Ειδικών Επιχειρήσεων των Η.Π.Α. (U.S. Special Operations Command / SOCOM) – Η Διοίκηση Ειδικών Επιχειρήσεων των Η.Π.Α. (U.S. Special Operations Command / SOCOM) χρησιμοποίησε το νέφος της AWS για να αυτοματοποιήσει διεργασίες τεχνητής νοημοσύνης για την υποβοήθηση του επιχειρησιακού της έργου.
Αποκατάσταση καταστροφών και Επιχειρησιακή Συνέχεια (Disaster Recover & Business Continuity)	• Elastic Load Balancing • AWS Storage • AWS Global Instrastructure	
Ανάλυση και διαχείριση δεδομένων (Data analytics & management)	• AWS Data Lakes and Analytics • AWS Storage	
Συμμόρφωση προς κανονιστικά πλαίσια (Compliance)	• AWS CloudFormation • **AWS CloudTrail (*)** • **Amazon CloudWatch (*)**	
* Σημείωση: Οι εφαρμογές AWS CloudTrail και Amazon CloudWatch είναι αυτές που χρησιμοποιούνται για τη διεξαγωγή εγκληματολογικών ερευνών.		

Πίνακας Παραρτήματος IV. Κατάλογος λογισμικού και μεγάλοι πελάτες της AWS στον χώρο της οικονομίας

Τεχνικά Χαρακτηριστικά	**Εφαρμογές**	**Μεγάλοι Πελάτες**
• **Ένα σύνολο πιστοποιήσεων (*) εξασφαλίζουν συμμόρφωση προς αμερικανικά και διεθνή πρότυπα [66], ε όπως:** ✓ **PCI-DSS**	• **Amazon WorkSpaces** – Πρόκειται για μια λύση Desktop-as-a-Service (DaaS), η οποία προβάλει εφαρμογές σε υπολογιστές και κινητά τηλέφωνα των χρηστών. • **Amazon Connect** –	• **Stripe** – Πρόκειται για εταιρεία συστημάτων πληρωμών με έδρα την Καλιφόρνια των ΗΠΑ. Από το 2011, το σύνολο των μηχανογραφικών της υποδομών λειτουργούν στο νέφος της AWS.

Τεχνικά Χαρακτηριστικά	Εφαρμογές	Μεγάλοι Πελάτες
✓ **SEC Rule 17-a-4(f)** ✓ **Reg SCI** ✓ **EU Data Protection Directive** ✓ **FedRAMP** ✓ **GDPR** ✓ **FIPS 140-2** ✓ **NIST 800-171**	Πρόκειται για λύση εικονικού τηλεφωνικού κέντρου, που μπορεί να στηθεί και να λειτουργεί μέσα σε λίγα μόλις λεπτά. Οι εργαζόμενοι ενός τέτοιου εικονικού τηλεφωνικού κέντρου μπορούν να εργάζονται από τα σπίτια τους, κάνοντας τις ίδιες ακριβώς εργασίες με εκείνες που θα έκαναν εάν ήταν στους χώρους ενός πραγματικού (φυσικού) τηλεφωνικού κέντρου. Για παράδειγμα, οι τηλεφωνητές μπορούν να δέχονται και να πραγματοποιούν τηλεφωνικές κλήσεις, οι προϊστάμενοι μπορούν να παρακολουθούν τις ουρές αναμονής, οι διευθυντές μπορούν να παράγουν αναφορές απόδοσης, κλπ. • **AWS Grid Computing** – Πρόκειται για λύση υπολογιστικής δικτύου, που διευκολύνει την αυτόματη δημιουργία συστοιχιών υπολογιστών υψηλής υπολογιστικής ισχύος (High Performance Computing clusters / HPC clusters), ώστε να εξυπηρετηθούν μεγάλα φορτία υπολογισμών, τις χρονικές στιγμές που προκαλούνται (πχ για τις Τράπεζες, όταν ξεκινούν τη λειτουργία τους, ή ακόμα χειρότερα, στα τέλη τριμήνων, εξαμήνων και ετών, οπότε και παράγουν αναφορές για τις εποπτικές αρχές, την επενδυτική αγορά, κλπ). * **Η AWS δεν κάνει αναφορά σε κάποιο συγκεκριμένο εργαλείο για την διεκπεραίωση εγκληματολογικών ερευνών σε αυτόν τον κλάδο.**	• **Bankinter** –είναι πάροχος υπηρεσιών ηλεκτρονικής τραπεζικής στην Ισπανία. Χρησιμοποιεί το νέφος της AWS για τη λειτουργία εφαρμογής προσομοίωσης εγκριτικού κινδύνου (credit-risk simulation), η οποία χρησιμοποιεί πολύπλοκους αλγόριθμους για να διεκπεραιώσει 5 εκατομμύρια προσομοιώσεις. Με τη χρήση της υπολογιστικής νέφους της AWS η Bankinter κατάφερε να μειώσει τον χρόνο διεκπεραίωσης αυτών των υπολογισμών από 23 ώρες σε 20 λεπτά. • **National Bank of Canada** – Πρόκειται για καναδική τράπεζα που χρησιμοποιεί το νέφος της AWS για την διεκπεραίωση μεγάλου φορτίου υπολογισμών. • **NuBank** – Πρόκειται για βραζιλιάνικη εταιρεία startup, που χρησιμοποίησε το νέφος της AWS προκειμένου να αναπτύξει γρήγορα διάφορες υποδομές της (όπως η εφαρμογή της για κινητά, η πλατφόρμα επεξεργασίας πιστωτικών καρτών) μειώνοντας στο ελάχιστο τον χρόνο διάθεσης αυτών των υποδομών στο πελατειακό της κοινό (time-to-market). • **Starling Bank** – Πρόκειται για εταιρεία startup οικονομικών υπηρεσιών (fintech), που χρησιμοποίησε το νέφος της AWS για να αναπτύξει γρήγορα υποδομές, κυρίως για το βασικό της επιχειρηματικό αντικείμενο που είναι η τραπεζική κινητής τηλεφωνίας (mobile banking). • **Capital** One – Πρόκειται για την 11η μεγαλύτερη αμερικανική τράπεζα (**), σύμφωνα με σχετική λίστα [57]. Η τράπεζα αυτή, χρησιμοποιεί το σύνολο σχεδόν των υπηρεσιών της AWS, οπότε και κατάφερε κατά το έτος 2018 να μειώσει

Τεχνικά Χαρακτηριστικά	Εφαρμογές	Μεγάλοι Πελάτες
		το περιβαλλοντολογικό αποτύπωμα των κέντρων δεδομένων της από το επίπεδο 8 στο επίπεδο 3.
* Σημείωση: οι πιστοποιήσεις αυτές δημιουργούν προϋποθέσεις ορθής και ασφαλούς λειτουργίας των εφαρμογών και των συστημάτων αλλά δεν συνεισφέρουν στην υποστήριξη εγκληματολογικών ερευνών.		
** Σημείωση: καμία από τις πρώτες 10 μεγαλύτερες τράπεζες, σύμφωνα με τη λίστα της Fed [57], δεν αναφέρεται από την AWS ως περίπτωση χρήσης του νέφους της, κάτι που ίσως υποκρύπτει κάποιο δισταγμό για την υιοθέτηση αυτής της πρακτικής από κάποιο μέρος των τραπεζικών ιδρυμάτων.		

Πίνακας Παραρτήματος V. Κατάλογος λογισμικού και μεγάλοι πελάτες της AWS στον χώρο της υγείας

Τεχνικά Χαρακτηριστικά	Εφαρμογές	Μεγάλοι Πελάτες
• **Ένα σύνολο πιστοποιήσεων (*) εξασφαλίζουν συμμόρφωση προς αμερικανικά και διεθνή πρότυπα της** [37] **[67], όπως:** ✓ **FedRAMP** ✓ **U.S. Health Insurance Portability and Accountability Act (HIPAA)** ✓ **HITRUST Common Security Framework** ✓ **Electronic Healthcare Network Accreditation Commission (EHNAC)**	• **Amazon Connect** – Εικονικό τηλεφωνικό κέντρο. • **AWS End User Computing** – Λογισμικό προβολής εφαρμογών στις επιφάνειες εργασίας επιτραπέζιων υπολογιστών και κινητών τηλεφώνων. • **HPC on AWS** – υποδομή υψηλής υπολογιστικής ισχύος της AWS. Χρησιμοποιείται εκτεταμένα αυτήν την περίοδο για διενέργεια διαγνώσεων και ερευνών σχετικά με την ασθένεια Covid-19. • **AWS Data Exchange** – δομή βάσεων δεδομένων, η οποία επίσης χρησιμοποιείται εκτεταμένα αυτήν την περίοδο για την αντιμετώπιση της ασθένειας Covid-19 (σε αυτή αποθηκεύονται τα δεδομένα σχετικά με αυτήν την ασθένεια, για λογαριασμό του ιδρύματος Johns Hopkins). **Η AWS δεν κάνει αναφορά σε κάποιο συγκεκριμένο εργαλείο για την διεκπεραίωση εγκληματολογικών ερευνών σε αυτόν τον κλάδο.**	• **Υπηρεσία Τροφίμων και Φαρμάκων των ΗΠΑ** (US Food and Drug Administration / FDA). • **Κέντρα Ελέγχου και Πρόληψης Νοσημάτων των ΗΠΑ** (US Centers for Disease Control and Prevention / CDC) • **Κέντρα Υπηρεσιών Medicare και Medicaid** (Centers for Medicare & Medicaid Services / CMS) • **3M Health Information Systems** • **Siemens HealthCare Diagnostics** • **GE Healthcare** • **Bristol-Myers Squibb** • **Johnson & Johnson** • **Novartis**
* Σημείωση: οι πιστοποιήσεις αυτές δημιουργούν προϋποθέσεις ορθής και ασφαλούς λειτουργίας των εφαρμογών και των συστημάτων υποδομών ζωτικής σημασίας αλλά δεν συνεισφέρουν στην υποστήριξη εγκληματολογικών ερευνών.		

[37] https://aws.amazon.com/health/case-studies/

Πίνακας Παραρτήματος VI. Βασικά χαρακτηριστικά της υπηρεσίας καταγραφής κινήσεων AWS CloudTrail

Λειτουργία	Περιγραφή
Εντοπισμός ασυνήθιστης δραστηριότητας	Μέσω μια λειτουργίας, η οποία ονομάζεται CloudTrail Insights, παρακολουθούνται οι κινήσεις που καταγράφονται στα logs και σε περίπτωση διαπίστωσης ασυνήθιστης δραστηριότητας, αποστέλλει αυτόματα ειδοποιήσεις στους κατάλληλους φορείς (συνήθως οι διαχειριστές συστημάτων ή εφαρμογών) αλλά προβαίνει επίσης και σε διορθωτικές ενέργειες. Ειδικότερα, το CloudTrail Insights είναι μια καινούργια σχετικά υπηρεσία της AWS, η οποία παρουσιάστηκε στις 21 Νοεμβρίου 2019 [38]. Η υπηρεσία αυτή, σύμφωνα και με την ανακοίνωση παρουσίασής της από την AWS, παρακολουθεί καθημερινά τις κινήσεις που καταγράφονται στα σχετικά αρχεία (logs), οπότε με την πάροδο του χρόνου σχηματίζει ένα πρότυπο συνήθους συμπεριφοράς. Έχοντας σχηματίσει αυτό το πρότυπο, κάθε φορά που εντοπίζει κινήσεις οι οποίες εκφεύγουν αυτού του προτύπου (δηλαδή της συνήθους συμπεριφοράς), παράγει ειδοποιήσεις. Οι ειδοποιήσεις αυτές, ανάλογα και με την παραμετροποίηση, διοδεύονται προς την κονσόλα ανακοινώσεων του AWS CloudTrail, προς το αποθηκευτικό σύστημα Amazon S3, προς την υπηρεσία Amazon CloudWatch και προς τα αρχεία καταγραφής κινήσεων (logs) της υπηρεσίας Amazon CloudWatch. Οι ειδοποιήσεις αυτές μπορούν να αξιοποιηθούν από συστήματα διαχείρισης συμβάντων (event management systems) και συστήματα ροών εργασιών (workflow systems), ώστε να συμμετέχουν στην έγκαιρη ανταπόκριση σε περιστατικά ασφάλειας και στην διεξαγωγή (ή/και έναρξη) εργασιών εγκληματολογίας. Η υπηρεσία CloudTrail Insights είναι διαθέσιμη σε όλους τους τομείς (regions) της AWS.
Συνεχής λειτουργία (always on)	Με την ενεργοποίησή της, αυτή η υπηρεσία καταγράφει όλες τις κινήσεις των λογαριασμών χρηστών και για βάθος 90 ημερών, χωρίς την ανάγκη ειδικής παραμετροποίησης. Το πλήθος αυτό (90 ημέρες) είναι ικανοποιητικό για τη διεξαγωγή εγκληματολογικών ερευνών για δυο λόγους: α) Επιτρέπει την επισκόπηση των αρχείων καταγραφής για μεγάλο βάθος χρόνου, και β) επιτρέπει την έναρξη εγκληματολογικών ερευνών ακόμα και αν έχει περάσει μεγάλο χρονικό διάστημα από τη στιγμή της διενέργειας της κακόβουλης πράξης (μερικές φορές οι κακόβουλες ενέργειες δεν γίνονται αντιληπτές άμεσα, αλλά με την πάροδο χρονικού διαστήματος, που μπορεί να είναι και μεγάλο).
Ιστορικότητα συμβάντων	Τα αρχεία αυτά μπορούν να κατέβουν και τοπικά στον υπολογιστή (download) για περαιτέρω επεξεργασία. Γενικά η επισκόπηση συμβάντων, πέραν της μεγάλης σημασίας της στο αντικείμενο της εγκληματολογικής έρευνας, βοηθάει πολύ και στην καλή παραμετροποίηση των ρυθμίσεων ασφαλείας, όπως επίσης και στη διαμόρφωση λύσεων για λειτουργικά προβλήματα.
Υποστήριξη πολλαπλών τομέων	Η δυνατότητα αυτή επιτρέπει στον χρήστη την κεντρική καταγραφή των κινήσεων σε όλους τους (γεωγραφικούς) τομείς και για όλα τα συστήματα που έχει εκμισθώσει ο χρήστης με χρήση του αποθηκευτικού συστήματος Amazon S3. Αυτό είναι εξαιρετικά βολικό, μιας που σε αντίθετη περίπτωση, η περισυλλογή των αρχείων κινήσεων από κάθε γεωγραφικό τομέα ξεχωριστά, θα επέφερε την ανάγκη ενσωμάτωσής τους σε ένα κεντρικό αρχείο, κάτι που θα μπορούσε να είναι χρονοβόρο και κουραστικό.
Επιβεβαίωση ακεραιότητας	Όπως έχει ήδη αναφερθεί, η απόδειξη ότι τα αρχεία καταγραφής, ως τεκμήρια της εγκληματολογικής έρευνας, δεν έχουν αλλοιωθεί, έχει μεγάλη

[38] https://aws.amazon.com/about-aws/whats-new/2019/11/aws-cloudtrail-announces-cloudtrail-insights/

Λειτουργία	Περιγραφή
των αρχείων καταγραφής (log file integrity validation)	νομική σημασία. Για τον λόγο αυτό, τηρείται ξεχωριστό αρχείο για τις ενέργειες που διεξάγονται επί των κεντρικών αρχείων κινήσεων του AWS CloudTrail, που φυλάσσονται στην αποθηκευτική υποδομή Amazon S3 bucket. Άλλωστε, πέραν της μεγάλης σημασίας αυτής της δυνατότητας για τον χώρο των εγκληματολογικών ερευνών, μπορεί να χρησιμεύσει και στη διενέργεια τακτικών ελέγχων ασφάλειας (IT security and auditing processes).
Κρυπτογράφηση	Η υπηρεσία AWS CloudTrail κρυπτογραφεί τα κεντρικά αρχεία κινήσεων χρησιμοποιώντας κρυπτογράφηση στην πλευρά του εξυπηρετητή (server side encryption). Ωστόσο, αν ο χρήστης επιθυμεί να προσθέσει ένα ακόμα επίπεδο κρυπτογράφησης, τότε μπορείς να το κάνει με τη χρήση της υπηρεσίας διαχείρισης μυστικού κλειδιού AWS Key Management System (AWS KMS).
Καταγραφή συμβάντων δεδομένων (Data events)	Τα συμβάντα δεδομένων είναι συχνά δραστηριότητες μεγάλου όγκου και περιλαμβάνουν λειτουργίες όπως οι κλήσεις API προς αντικείμενα του αποθηκευτικού συστήματος Amazon S3 και οι κλήσεις API για χρήση της υπηρεσίας AWS Lambda. Σε αυτές τις περιπτώσεις καταγράφονται αναλυτικές πληροφορίες του συμβάντος, όπως ο χρήστης AWS που κάλεσε το API, ο ρόλος του με βάση το σύστημα διαχείρισης ταυτοτήτων Identity & Access Management της AWS, η διεύθυνση IP του (ip address), η χρονική στιγμή της κλήσης, ποια λειτουργία της υπηρεσίας AWS Lambda κλήθηκε, κλπ.
Καταγραφή συμβάντων διαχείρισης (Management events)	Τα συμβάντα αυτά αφορούν τη διαχείριση αντικειμένων που χρησιμοποιεί / εκμισθώνει ο χρήστης στο νέφος της AWS. Για παράδειγμα, τέτοια συμβάντα είναι η δημιουργία, η διαγραφή και η τροποποίηση αντικειμένων στο περιβάλλον Amazon EC2 (σε αυτό το περιβάλλον τα αντικείμενα είναι συνήθως εικονικοί υπολογιστές). Για κάθε τέτοιο περιστατικό λοιπόν, το AWS CloudTrail καταγράφει όλες τις σχετιζόμενες λεπτομέρειες, όπως ο λογαριασμός AWS που προέβη στη διενέργεια του συμβάντος, ο ρόλος του με βάση το σύστημα διαχείρισης ταυτοτήτων Identity & Access Management της AWS, η διεύθυνση IP του (ip address), η χρονική στιγμή του συμβάντος και βέβαια τα αντικείμενα που επηρεάστηκαν.

Πίνακας Παραρτήματος VII. Βασικά χαρακτηριστικά της υπηρεσίας καταγραφής κινήσεων Amazon CloudWatch.

Λειτουργία	Περιγραφή
Παρακολούθηση πόρων (monitoring)	Το CloudWatch παρέχει πληροφορίες για την παρακολούθηση των εφαρμογών, των συστημάτων, τη βελτιστοποίηση της χρήσης πόρων και τη λειτουργική υγεία των υποδομών που εκμισθώνει ο πελάτης. Συλλέγει δεδομένα και συμβάντα από τα αρχεία καταγραφής κινήσεων παρέχοντας ενοποιημένη προβολή των πόρων, των εφαρμογών και των υπηρεσιών που εκτελούνται είτε στο νέφος της AWS, είτε στις εγκαταστάσεις του πελάτη (on-premises).
Αποστολή ειδοποιήσεων (notifications)	Παράγει ειδοποιήσεις, όπως και το προαναφερθέν AWS CloudTrail. Οι ειδοποιήσεις αυτές χρησιμεύουν στην έγκαιρη ενημέρωση των διαχειριστών, αλλά μπορούν, με την αντίστοιχη παραμετροποίηση, να εκκινήσουν διαδικασίες.
Αυτόματη κλιμάκωση πόρων (scaling)	Όταν η υπηρεσία Amazon CloudWatch διαπιστώσει από τις σχετικές μετρικές που παραλαμβάνει, ότι οι υποδομές που εκμισθώνει ο πελάτης έχουν έρθει σε σημείο κορεσμού, παράγει σχετική ειδοποίηση και προβαίνει αυτόματα στην επέκταση των υποδομών αυτών, με την

Λειτουργία	Περιγραφή
	προσθήκη επιπλέον πληροφοριακών πόρων.
Διεξαγωγή εγκληματολογικών ερευνών με χρήση γλώσσας ερωτημάτων (query language)	Αν και η βασική αποστολή της υπηρεσίας Amazon CloudWatch είναι κυρίως η βελτιστοποίηση χρήσης των πληροφοριακών πόρων, επειδή συλλέγει και επεξεργάζεται δεδομένα από τα αρχεία καταγραφής κινήσεων, αποτελεί συνάμα εργαλείο για τη διεξαγωγή εγκληματολογικών ερευνών. Για τον σκοπό αυτό διαθέτει ένα περιβάλλον χρήσης γλώσσας ερωτημάτων (query language, κάτι σαν την SQL), διευκολύνοντας έτσι την διερεύνηση και αναζήτηση πληροφοριών από τα αρχεία καταγραφής κινήσεων.

Πίνακας Παραρτήματος VIII. Εφαρμογές ανάγνωσης και διαχείρισης Αρχείων Καταγραφής Κινήσεων (Logs) μεγάλων παρόχων νέφους

Πάροχος	**Εργαλείο**
Microsoft Azure	Azure Sentinel [39]
Google Cloud	Security Command Center [40]
IBM Cloud	IBM Qradar [41]
Alibaba Cloud	Alibaba Cloud Log Service [42]
Oracle Cloud	Oracle Security Monitoring and Analytics [43]

[39] https://docs.microsoft.com/en-us/azure/sentinel/tutorial-investigate-cases
[40] https://cloud.google.com/security-command-center
[41] https://www.ibm.com/products/hosted-security-intelligence
[42] https://www.alibabacloud.com/product/log-service
[43] https://docs.oracle.com/en/cloud/paas/management-cloud/omsma/getting-started-oracle-security-monitoring-and-analytics.html