Πανεπιστήμιο Αιγαίου
Τμήμα Μηχανικών Πληροφοριακών
& Επικοινωνιακών Συστημάτων

Π.Μ.Σ. Τεχνολογίες και Διοίκηση Πληροφοριακών & Επικοινωνιακών Συστημάτων

Διπλωματική εργασία

«Διερεύνηση κυβερνοεγκλημάτων & εγκληματολογική ανάλυση σε περιβάλλον υπολογιστικού νέφους: τεχνολογικές προκλήσεις & νομική διάσταση»

Φοιτητές:

Γέρμανος Γεώργιος του Αθανασίου, Α.Μ. 323/2015022

Πέππα Αικατερίνη του Δημητρίου, Α.Μ. 323/2015072

Επιβλέπουσα:

Αναπληρώτρια Καθηγήτρια Μήτρου Ευαγγελία

Καρλόβασι, Φεβρουάριος 2017

University of the Aegean
Department of Information
& Communication Systems Engineering

M.Sc. Technologies & Administration of Information & Communication Systems

Thesis

"Cybercrime investigation & forensics analysis in cloud environments: technological & legal challenges"

Students:

Germanos Georgios, Peppa Aikaterini

Supervisor:

Associate Professor Dr. Mitrou Evangelia (Lilian)

Karlovassi, February 2017

Στις οικογένειές μας

για την πολύτιμη στήριξή τους

Περιεχόμενα

Περίληψη

Η διερεύνηση των διαφόρων μορφών εγκλημάτων και περιστατικών ασφαλείας στον κυβερνοχώρο αποτελεί σήμερα μια ιδιαίτερη πρόκληση για τις Αρχές Επιβολής του Νόμου, για τις εισαγγελικές και δικαστικές Αρχές και γενικότερα για τους ειδικούς ασφάλειας σε διεθνές επίπεδο. Ειδικά η συλλογή, εξέταση, ανάλυση και παρουσίαση ψηφιακών εγκληματολογικών πειστηρίων και δεδομένων απαιτούν προσεκτικούς και λεπτούς χειρισμούς, από εξειδικευμένο και ορθά καταρτισμένο προσωπικό και έχουν εξελιχθεί σε έναν ξεχωριστό επιστημονικό κλάδο. Ιδίως λόγω της προόδου της τεχνολογίας, όλο και περισσότεροι χρήστες του Διαδικτύου στρέφονται στο υπολογιστικό νέφος, προκειμένου να εκμεταλλευτούν τα διάφορα οφέλη του. Η υιοθέτηση της συγκεκριμένης τεχνολογίας, είτε πρόκειται για «Εξοπλισμό», «Πλατφόρμα» ή «Λογισμικό ως Υπηρεσία», συνεπάγεται μια σειρά επιπλέον τεχνολογικής και νομικής φύσεως («ατοπικότητα», διατήρηση δεδομένων και πρόσβαση σε αυτά κ.λπ.) εμπόδια, τα οποία καλείται να ξεπεράσει ένας ερευνητής. Όλα τα παραπάνω ζητήματα συνδυάζονται και παρουσιάζονται στο πλαίσιο της παρούσας διπλωματικής εργασίας.

Λέξεις κλειδιά

Κυβερνοέγκλημα, ηλεκτρονικό έγκλημα, ψηφιακό έγκλημα, υπολογιστικό νέφος, πειστήρια, διερεύνηση, τεχνολογικές προκλήσεις, νομικές προκλήσεις

Summary

Investigating different forms of cybercrimes and cyber security incidents is now a special challenge for the law enforcement authorities, for the judicial authorities and in general for the security specialists around the world. Mainly the collection, examination, analysis and presentation of digital forensic and evidentiary data require careful and delicate, qualified and properly trained staff and have evolved into a separate scientific branch. Especially because of technology advances, more and more Internet users are turning to the cloud technology to take advantage of its various benefits. The adoption of this technology, whether it is "Infrastructure", "Platform" or "Software as a Service" entails a number of additional obstacles of technical and legal nature ("loss of location", retention of data and access to them, etc.) for the researcher to overcome. All these issues are combined and presented in this thesis.

Keywords

Cybercrime, digital crime, cloud computing, evidence, investigation, technological challenges, legal challenges

Συντομογραφίες – Συντμήσεις

ACPO	Association of Chief Police Officers
API	Application Programming Interface
ATM	Automated Teller Machine
CERT	Computer Emergency Response Team
CFFTPM	Computer Forensics Field Triage Process Model
CSIRT	Computer Security Incident Response Team
DDoS	Distributed Denial of Service (attack)
ECHR	European Convention on Human Rights
ENISA	European Union Agency for Network and Information Security
FTK	Forensic Toolkit
GB	Gigabyte
GFS	Google File System
HDD	Hard Disk Drive
IaaS	Infrastructure as a Service
IDS	Intrusion Detection System
LEA	Law Enforcement Agency / Authority
NIST	National Institute of Standards and Technology
PaaS	Platform as a Service
RAM	Random Access Memory
SaaS	Software as a Service
SMS	Short Message Service
SSD	Solid-State Drive
USB	Universal Serial Bus
ΑΔΣ	Αμοιβαία Δικαστική Συνδρομή

ΔΕΕ	Διεύθυνση Εγκληματολογικών Ερευνών
ΕΕ	Ευρωπαϊκή Ένωση
ΕΕΕ	Ευρωπαϊκή Εντολή Έρευνας
ΗΠΑ	Ηνωμένες Πολιτείες Αμερικής
ΚΠΔ	Κώδικας Ποινικής Δικονομίας
ΠΚ	Ποινικός Κώδικας
ΤΠΕ	Τεχνολογίες Πληροφοριών & Επικοινωνιών

Ευχαριστίες

Με την ολοκλήρωση της ανά χείρας διπλωματικής εργασίας και παράλληλα της φοίτησής μας στο Π.Μ.Σ. «Τεχνολογίες και Διοίκηση Πληροφοριακών και Επικοινωνιακών Συστημάτων» του Τμήματος Μηχανικών Πληροφοριακών & Επικοινωνιακών Συστημάτων του Πανεπιστημίου Αιγαίου θα θέλαμε να ευχαριστήσουμε το σύνολο των διδασκόντων και συνεργατών του ιδρύματος για τις πολύτιμες γνώσεις και εμπειρίες που μας μετέδωσαν.

Θερμότερες ευχαριστίες οφείλουμε, βεβαίως, στην επιβλέπουσα καθηγήτριά της εργασίας μας κ. Λίλιαν Μήτρου, αναπληρώτρια Καθηγήτρια του Τμήματος Μ.Π.Ε.Σ. του Πανεπιστημίου Αιγαίου. Από την πρώτη στιγμή με χαρά και ενθουσιασμό δέχθηκε να συζητήσει την πρότασή μας γύρω από τη θεματική που επιλέξαμε και βέβαια στη συνέχεια μας καθοδήγησε κατά τη συγγραφή της. Οι εποικοδομητικές της υποδείξεις, επισημάνσεις και διορθώσεις συνέβαλαν καθοριστικά στην ολοκλήρωση του παρόντος πονήματος.

Ευχαριστούμε, τέλος, ειλικρινά τις οικογένειές μας για την ηθική τους στήριξη και τους ευγνωμονούμε που στέκονται πάντα δίπλα μας, στα εύκολα αλλά και στα δύσκολα, δίνοντάς μας την ελπίδα και τη δύναμη να συνεχίσουμε να προσπαθούμε για το καλύτερο.

Γέρμανος Αθ. Γεώργιος – Πέππα Δ. Αικατερίνη

Εισαγωγή

Η ψηφιακή τεχνολογία και τα μέσα επικοινωνίας γίνονται ολοένα και πιο πολύτιμα στην καθημερινότητά μας, σε όλους τους τομείς της ζωής μας. Παντού γύρω μας συναντάμε διασυνδεδεμένες συσκευές: όχι μόνο σταθερούς υπολογιστές, laptops, tablets ή έξυπνα κινητά τηλέφωνα, αλλά και οχήματα, ρολόγια και πλήθος οικιακών συσκευών.

Παράλληλα, όμως, με την ανάπτυξη της τεχνολογίας, καταγράφεται μια ταυτόχρονη ανάπτυξη της εγκληματικής δραστηριότητας. Το κυβερνοέγκλημα κερδίζει θέσεις έναντι των παραδοσιακών εγκλημάτων. Ομοίως, και οι εγκληματικές οργανώσεις στρέφονται στον ψηφιακό κόσμο, είτε για σκοπούς «ασφαλέστερης» επικοινωνίας μεταξύ των μελών τους, είτε γιατί ο κατάλογος των υποψήφιων θυμάτων online διευρύνεται. Την ίδια στιγμή, οι εκπρόσωποι των Αρχών επιβολής του Νόμου βρίσκονται αντιμέτωποι με νέες προκλήσεις σε ότι αφορά την εξέταση ψηφιακών πειστηρίων[1].

Τι είναι το κυβερνοέγκλημα;

Το σίγουρο είναι ότι δεν υπάρχει κάποιος «επίσημος», καθολικά αποδεκτός ορισμός. Διαφορετικοί οργανισμοί και φορείς υιοθετούν διαφορετικούς ορισμούς, ανάλογα με τις αρμοδιότητές τους. Παραδείγματος χάρη, ο ορισμός που δίνεται από τις Αρχές Επιβολής του Νόμου είναι διαφορετικός από αυτόν που δίνεται από τα CERTs (Computer Emergency Response Teams). Ένα cyber incident (περιστατικό), που απασχολεί ένα CERT, δεν χαρακτηρίζεται απαραίτητα και ως cyber crime (έγκλημα) για να απασχολήσει μια Αρχή Επιβολής του Νόμου[2].

Εξάλλου, για την αναφορά στα εγκλήματα που τελούνται μέσω των νέων τεχνολογιών πληροφοριών και επικοινωνιών ή με τη χρήση αυτών, χρησιμοποιούνται πολλοί διαφορετικοί όροι: ηλεκτρονικά εγκλήματα (electronic crimes), online εγκλήματα (online crimes), εγκλήματα Διαδικτύου (internet crimes), ψηφιακά εγκλήματα (digital crimes), εγκλήματα νέων τεχνολογιών (new technology crimes), κυβερνοεγκλήματα (cyber

[1] https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime

[2] The Fight against Cybercrime - Cooperation between CERTs and Law Enforcement Agencies to fight against cybercrime - A first collection of practices, ENISA, διαθέσιμο εδώ: https://www.enisa.europa.eu/publications/cooperation-between-certs-and-law-enforcement-agencies-in-the-fight-against-cybercrime-a-first-collection-of-practices

crimes)[3]. Το πρόθεμα κυβερνο- (cyber-) συχνά παρατίθεται δίπλα σε λέξεις αδικημάτων, υποδεικνύοντας ότι το έγκλημα αφορά τον ψηφιακό κόσμο: κυβερνο-εκφοβισμός, κυβερνο-εκβιασμός, κυβερνο-τρομοκρατία κ.α.. Είναι σαφές, δηλαδή, ότι υπάρχει δυσκολία ως προς την αποτύπωση των κυβερνοεγκλημάτων σε νομικά κείμενα σε διαφορετικές γλώσσες και σε διαφορετικά Κράτη.

Η Σύμβαση για τα εγκλήματα στον Κυβερνοχώρο (Σύμβαση της Βουδαπέστης)[4], του 2001, χρησιμοποιεί έναν ορισμό για το κυβερνοέγκλημα που βασίζεται στο ποια εγκλήματα θα έπρεπε να συμπεριληφθούν σε αυτόν (αντί να δώσει έναν ακριβή ορισμό). Σε αυτόν περιλαμβάνονται:

- εγκλήματα ενάντια στην εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα ψηφιακών δεδομένων και συστημάτων (παράνομη πρόσβαση, υποκλοπή, παρέμβαση σε δεδομένα και συστήματα),
- εγκλήματα που τελούνται με χρήση υπολογιστών (λ.χ. πλαστογραφία ή απάτη με χρήση υπολογιστή),
- εγκλήματα σχετικά με το περιεχόμενο (πορνογραφία ανηλίκων),
- εγκλήματα σχετικά με την παραβίαση πνευματικής ιδιοκτησίας και συγγενικών δικαιωμάτων.

Επειδή πρόκειται για κείμενο που γράφτηκε το 2001, πολλές μορφές κυβερνοεγκλήματος που έχουν εμφανιστεί έκτοτε, δε μπορούν να ενταχθούν στις τέσσερις προαναφερθείσες κατηγορίες.

Το 2007, λοιπόν, η Ευρωπαϊκή Επιτροπή έδωσε ένα νέο ορισμό για το κυβερνοέγκλημα, στον οποίο περιλαμβάνονται τρεις μεγάλες κατηγορίες:

- παραδοσιακά εγκλήματα, όπως η απάτη και η πλαστογραφία, που τελούνται με τη χρήση ψηφιακών μέσων και διαμέσου δικτύων επικοινωνιών,
- παράνομο περιεχόμενο που μεταδίδεται μέσα από ψηφιακά μέσα (για παράδειγμα υλικό σεξουαλικής εκμετάλλευσης ανηλίκων ή ρατσιστικός λόγος),

[3] Alkaabi, Ali, Mohay, George M., McCullagh, Adrian J., & Chantler, Alan N. (2010) *Dealing with the problem of cybercrime.* In Baggili, Ibrahim (Ed.) *Conference Proceedings of 2nd International ICST Conference on Digital Forensics & Cyber Crime,* ICST, Abu Dhabi.

[4] https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561

- εγκλήματα που τελούνται αποκλειστικά σε ψηφιακό περιβάλλον, όπως επιθέσεις εναντίον πληροφοριακών συστημάτων, επιθέσεις άρνησης παροχής υπηρεσιών (Denial of Service) και hacking[5].

Πρόσφατα, τον Ιούλιο του 2013, υιοθετήθηκε σε ευρωπαϊκό επίπεδο η νέα Οδηγία για τις επιθέσεις ενάντια στα πληροφοριακά συστήματα (προς αντικατάσταση της Council Framework Decision 2005/222/JHA). Η νέα αυτή οδηγία στοχεύει στην αντιμετώπιση περίπλοκων μορφών κυβερνοεγκλημάτων ενάντια σε πληροφοριακά συστήματα, όπως η χρήση των botnets[6].

Τύποι κυβερνοεγκλημάτων

Υπάρχουν πολλές διαφορετικές μορφές κυβερνοεγκλημάτων[7]. Συχνότερα συναντάμε:

- παράνομη πρόσβαση σε υπολογιστικά συστήματα (hacking & cracking – συχνά με εκμετάλλευση ευπαθειών του συστήματος),
- ανάπτυξη και/ή διασπορά κακόβουλου κώδικα (όπως ιούς και Trojans, που προκαλούν βλάβη σε υπολογιστικά συστήματα, ή χρησιμοποιούνται για τη διάπραξη άλλων εγκλημάτων),
- αποστολή μη ζητηθείσας αλληλογραφίας (spamming), δηλαδή αποστολή πολλαπλών μηνυμάτων ηλεκτρονικού ταχυδρομείου, συνήθως με τη χρήση μολυσμένων υπολογιστών (botnet),
- επιθέσεις κατανεμημένης άρνησης παροχής υπηρεσιών (Distributed Denial of Service - DDoS), ήτοι ένας τρόπος αποστολής υπερβολικά μεγάλου αριθμού αιτημάτων στον εξυπηρετητή, που οδηγεί σε κατάρρευση μιας ιστοσελίδας,
- διείσδυση σε δίκτυο (πρόσβαση σε δίκτυα υπολογιστών, με τη χρήση τεχνικών hacking, με σκοπό την υποκλοπή δεδομένων, τη διασπορά κακόβουλου λογισμικού ή την απόπειρα εκβίασης),
- πειρατεία λογισμικού,

[5] http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52007DC0267

[6] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:EN:PDF

[7] https://www.britannica.com/topic/cybercrime

- εγκλήματα βασισμένα στη λειτουργία δικτύων (λόγου χάρη phishing – μια προσπάθεια εξαπάτησης χρηστών μέσω ψεύτικων απεικονίσεων – και υποκλοπή ταυτότητας),
- εγκλήματα σχετικά με τα δικαιώματα πνευματικής ιδιοκτησίας (για παράδειγμα βιομηχανική κατασκοπεία ή διαμοιρασμός περιεχομένου που προστατεύεται από τη νομοθεσία περί πνευματικής ιδιοκτησίας, χωρίς σχετική άδεια – εικόνες, μουσική, ταινίες),
- κατοχή και διαμοιρασμός υλικού σεξουαλικής εκμετάλλευσης ανηλίκων,
- προσέλκυση ανηλίκων για γενετήσιους λόγους, π.χ. μέσω ιστοσελίδων κοινωνικής δικτύωσης,
- phreaking (μη εξουσιοδοτημένη χρήση συστημάτων τηλεφωνικής επικοινωνίας, είτε για την πραγματοποίηση δωρεάν τηλεφωνικών κλήσεων, είτε για την ανώνυμη επικοινωνία μεταξύ μελλών μιας εγκληματικής οργάνωσης),
- δορυφορική πειρατεία (για παράδειγμα παράνομη αποκρυπτογράφηση σήματος δορυφορικών τηλεοπτικών μεταδόσεων).

Αξίζει να σημειωθεί ότι μια πράξη μπορεί να εμπίπτει ταυτόχρονα σε πολλές από τις παραπάνω κατηγορίες εγκλημάτων: η πειρατεία λογισμικού συνδυάζεται με τον παράνομο διαμοιρασμό αρχείων, οι επιθέσεις phishing απαιτούν την αποστολή μη ζητηθείσας αλληλογραφίας (spamming).

Εύρος του κυβερνοεγκλήματος

Με δεδομένο το πλήθος των διαφορετικών ορισμών του κυβερνοεγκλήματος, είναι αναπόφευκτη η διαφωνία ως προς το πραγματικό εύρος του κυβερνοεγκλήματος στην Ευρώπη και στον υπόλοιπο κόσμο.

Στα περισσότερα Κράτη, τα σχετικά δεδομένα – όπου υπάρχουν – προέρχονται από καταγεγραμμένα στατιστικά των Αρχών επιβολής του Νόμου[8]. Επιπλέον στοιχεία μπορεί να δημοσιεύονται έπειτα από έρευνες ιδιωτικών οργανισμών και φορέων. Η χρήση των

[8] Για παράδειγμα δεδομένα για ηλεκτρονικά εγκλήματα εμπεριέχονται στον ετήσιο απολογισμό των δραστηριοτήτων της Ελληνικής Αστυνομίας, έτους 2015: http://www.astynomia.gr/index.php?option=ozo_content&lang=%27..%27&perform=view&id=62129&Itemid=1694&lang=

στατιστικών που προέρχονται από τις εισαγγελικές και δικαστικές Αρχές εγείρει προβληματισμούς, καθώς η νομοθεσία διαφέρει ανάμεσα στα Κράτη ή συχνά χρησιμοποιούνται διατάξεις συμβατικών εγκλημάτων που τελούνται στον κυβερνοχώρο.

Εξίσου διαφέρουν και οι εκτιμήσεις σχετικά με τις οικονομικές επιπτώσεις του κυβερνοεγκλήματος (σε οργανισμούς, σε Κράτη και σε μεμονωμένα άτομα), διότι:

- είναι δύσκολη η ποσοτικοποίηση ορισμένων μορφών κυβερνοεγκλήματος (π.χ. επιθέσεις DDoS),
- οι επιχειρήσεις προτιμούν να μη δημοσιοποιήσουν περιστατικά που τους αφορούν,
- τα θύματα δεν αναφέρουν – καταγγέλλουν ένα έγκλημα, είτε γιατί η απώλεια είναι μικρή, είτε γιατί νιώθουν ντροπή (π.χ. μόλυνση από κακόβουλο λογισμικό μετά την επίσκεψη σε έναν ιστότοποι με πορνογραφικό περιεχόμενο)[9].

Συχνά το φως της δημοσιότητας βλέπουν εκθέσεις ιδιωτικών επιχειρήσεων (π.χ. εταιρείες antivirus), τα στοιχεία των οποίων, ωστόσο, βασίζονται σε δεδομένα που προέρχονται από τους πελάτες τους – δηλαδή σε ένα μικρό ποσοστό του πληθυσμού[10]. Άρα ούτε σε αυτή την περίπτωση είναι φρόνιμη η γενίκευση των συμπερασμάτων.

Παρ' όλα αυτά, δεν υπάρχει αμφιβολία ότι το κυβερνοέγκλημα γνωρίζει αυξητικές τάσεις, σε παγκόσμιο επίπεδο. Αυτό συμβαίνει διότι:

- ο αριθμός των συσκευών που διασυνδέονται και αποκτούν τη δυνατότητα επικοινωνίας διαρκώς αυξάνεται, άρα μακραίνει και ο κατάλογος των υποψήφιων θυμάτων,
- το ρίσκο που παίρνουν οι κυβερνοεγκληματίες είναι σχετικά μικρό, λόγω της ανωνυμίας που επικρατεί στον κυβερνοχώρο,
- είναι εξαιρετικά προσοδοφόρο (γιατί να διαπράξει κάποιος μια ληστεία σε τράπεζα, όταν μπορεί να αφαιρέσει ένα ευρώ από λογαριασμούς εκατομμυρίων χρηστών του Διαδικτύου;),

[9] Maguire, M., Okada, D. (2014). *Critical Issues in Crime and Justice: Thought, Policy, and Practice*, SAGE Publications, chapter 14

[10] Για παράδειγμα η ετήσια έκθεση της Kaspersky για το 2015, που είναι διαθέσιμη εδώ: https://securelist.com/analysis/kaspersky-security-bulletin/73038/kaspersky-security-bulletin-2015-overall-statistics-for-2015/

- από τη φύση του, το κυβερνοέγκλημα δε γνωρίζει σύνορα και έτσι η διερεύνηση υποθέσεων από τις Αρχές Επιβολής του Νόμου είναι εξαιρετικά δύσκολη.

Νομοθεσία & συνεργασία

Εξαιτίας της ψηφιοποίησης των πάντων γύρω μας, της ανεξέλεγκτης ανάπτυξης των δικτύων υπολογιστών, της εξέλιξης των τεχνολογιών πληροφοριών και επικοινωνιών και των κινδύνων που φέρνουν μαζί τους, εντοπίζουμε βαθιές αλλαγές στην κοινωνική ζωή. Για να αντιμετωπίσουν τις απειλές στον κυβερνοχώρο, τα Κράτη και η διεθνής κοινότητα πρέπει αφενός να συνεργαστούν στενά μεταξύ τους, μέσω των αρμόδιων Υπηρεσιών και φορέων, και αφετέρου να αξιοποιήσουν κατάλληλα νομοθετικά εργαλεία για το σκοπό αυτό.

Το κυβερνοέγκλημα δεν έχει σύνορα. Ένα από τα βασικά ζητήματα στο οποίο πρέπει να δοθεί προσοχή είναι η απουσία παγκοσμίως αποδεκτών νομικών κειμένων ενάντια στο κυβερνοέγκλημα, στους τομείς της πρόληψης, της διερεύνησης, της εξέτασης ψηφιακών πειστηρίων και της ποινικής δίωξης. Υπάρχουν ορισμένες συμφωνίες σε παγκόσμιο επίπεδο, που σχετίζονται με το εσωτερικό δίκαιο των Κρατών, αλλά:

- κάποια Κράτη δεν έχουν κυρώσει τις συμβάσεις αυτές[11] ή
- τα εργαλεία αυτά εστιάζουν στην αντιμετώπιση ορισμένων περιπτώσεων κυβερνοεγκλήματος, αλλά όχι του συνόλου των περιπτώσεων (λ.χ. τα botnets),

Συνεπώς, ένα μεγάλο ποσοστό των ερευνών των αστυνομικών και δικαστικών Αρχών καταλήγουν να εξαρτώνται αποκλειστικά από την ισχύουσα σε κάθε Κράτος νομοθεσία, κάτι που με τη σειρά του οδηγεί σε μη αποτελεσματική εφαρμογή διαδικασιών και μη απόδοση δικαιοσύνης.

Ο τρόπος που κάθε Κράτος αντιμετωπίζει το κυβερνοέγκλημα ποικίλει, λόγω των προτεραιοτήτων που τίθενται σε κεντρικό επίπεδο, αλλά και εξαιτίας διαφορετικών προσεγγίσεων σε νομικό, τεχνικό και οικονομικό επίπεδο. Υφίστανται διαφορές στην οργάνωση των αστυνομικών, δικαστικών και εισαγγελικών υπηρεσιών και στις ισχύουσες

[11] Χαρακτηριστικότερο παράδειγμα η Σύμβαση για το Έγκλημα στον Κυβερνοχώρο (2001)

διατάξεις σχετικά με την απονομή της δικαιοσύνης (τόσο επί των προβλεπόμενων ποινών, όσο και επί των δικονομικών κανόνων)[12].

Ψηφιακά πειστήρια & άλλα εγκλήματα

Σε κάθε περίπτωση, δε μπορούμε να αγνοήσουμε το γεγονός ότι σε ένα μεγάλο αριθμό εγκλημάτων που τελούνται καθημερινά, από τα πιο απλά (λ.χ. δυσφημίσεις) έως τα πιο σύνθετα (λ.χ. τρομοκρατία[13]), τα αποδεικτικά στοιχεία για τη θεμελίωση της αντικειμενικής υπόστασης του εγκλήματος ή την ενοχή του δράστη έχουν ψηφιακή μορφή: δεδομένα ηλεκτρονικών επικοινωνιών, ψηφιακές φωτογραφίες, μηνύματα ηλεκτρονικού ταχυδρομείου και πολλά άλλα[14]. Με άλλα λόγια, σε ψηφιακά πειστήρια μπορεί να βρίσκονται αποθηκευμένες πληροφορίες που σχετίζονται με μια μεγάλη γκάμα εγκλημάτων, όχι απαραίτητα κυβερνοεγκλημάτων, υπό το πρίσμα που παρουσιάστηκαν προηγουμένως.

Πλέον, για τις Αρχές Επιβολής του Νόμου η συλλογή, τεκμηρίωση, εξέταση, ανάλυση και διαφύλαξη των ψηφιακών πειστηρίων διενεργούνται από εξειδικευμένες μονάδες ή υπηρεσίες που δημιουργούνται ειδικά για το σκοπό αυτό. Για παράδειγμα, στη Διεύθυνση Εγκληματολογικών Ερευνών του Αρχηγείου της Ελληνικής Αστυνομίας λειτουργεί το Τμήμα Εξέτασης Ψηφιακών Πειστηρίων, προκειμένου να υποστηρίξει τις ολοένα αυξανόμενες υποχρεώσεις διαλεύκανσης εγκλημάτων που σχετίζονται με τους Ηλεκτρονικού Υπολογιστές και γενικότερα με τα ψηφιακά υπολογιστικά συστήματα[15].

Τις ίδιες ως άνω διαδικασίες που αφορούν τα ψηφιακά πειστήρια είναι σε θέση να εφαρμόσουν και άλλοι φορείς ή εταιρείες του ιδιωτικού τομέα, για τη διασφάλιση της

---

[12] Chawki, M. (2005). *A Critical Look at the Regulation of Cybercrime: A Comparative Analysis with Suggestions for Legal Policy*, DROIT-TIC

[13] Βλ. σχετικό Δελτίο Τύπου της Ελληνικής Αστυνομίας σχετικά με σύλληψη υπηκόου Συρίας, σε βάρος του οποίου εκκρεμούσε Ευρωπαϊκό Ένταλμα Σύλληψης, κατηγορούμενου για συμμετοχή σε εγκληματική οργάνωση, παροχή βοήθειας για παράνομη είσοδο ατόμων και διαμονή, πλαστογραφία δημοσίων εγγράφων και εμπορία πλαστών - παραποιημένων εγγράφων: http://www.astynomia.gr/index.php?option=ozo_content&lang=%27..%27&perform=view&id=66245&Itemid=1767&lang=

[14] http://www.nij.gov/topics/forensics/evidence/digital/pages/welcome.aspx

[15] Άρθρο 30 του Π.Δ. 178/2014 «Οργάνωση Υπηρεσιών Ελληνικής Αστυνομίας»

ορθής λειτουργίας των υπολογιστικών τους συστημάτων ή τη διερεύνηση περιστατικών που δεν καταγγέλλονται απαραίτητα στις Αρχές Επιβολής του Νόμου.

Ψηφιακά πειστήρια και υπολογιστικό νέφος

Η ειδικότερη θεματολογία που θα μας απασχολήσει στο πλαίσιο της παρούσας εργασίας είναι τα ψηφιακά πειστήρια, τα οποία όμως δεν εμπεριέχονται στις συνηθισμένες έως σήμερα τοποθεσίες τους, όπως λ.χ. ένα σκληρό δίσκο του σταθερού υπολογιστή ή του laptop, μια εξωτερική μονάδα αποθήκευσης (τύπου USB stick) ή ενός ψηφιακού δίσκου DVD, αλλά στο υπολογιστικό νέφος.

Στα κεφάλαια που θα ακολουθήσουν θα παρουσιάσουμε αρχικά τις εφαρμοζόμενες τεχνικές για τη συλλογή, εξέταση, ανάλυση και παρουσίαση ψηφιακών πειστηρίων. Ακολούθως θα αναφερθούμε στην έννοια του υπολογιστικού νέφους και θα εξηγήσουμε πως αυτό έχει γίνει μέρος της καθημερινότητάς μας. Θα δούμε επιπλέον στη συνέχεια σε ποιο βαθμό είναι εφαρμόσιμες οι «παραδοσιακές» μέθοδοι εγκληματολογικής εξέτασης υπολογιστικών συστημάτων και ψηφιακών πειστηρίων όταν πρόκειται για δεδομένα που βρίσκονται στο υπολογιστικό νέφος. Τέλος, θα εξετάσουμε τα κυριότερα τεχνικά και θεωρητικά (νομικά και άλλα) ζητήματα γύρω από τη διερεύνηση κυβερνοεγκλημάτων και την εγκληματολογική εξέταση ψηφιακών πειστηρίων στο υπολογιστικού νέφους.

❑

Κεφάλαιο 1: Εγκληματολογική ανάλυση ψηφιακών πειστηρίων

Όπως αναφέρθηκε ήδη στην Εισαγωγή, προκειμένου να ευρεθούν στοιχεία που να σχετίζονται με την τέλεση ενός κυβερνοεγκλήματος – υπό την αυστηρή έννοια (σεξουαλική εκμετάλλευση ανηλίκων online, κυβερνοεπίθεση, απάτη με υπολογιστή κ.λπ.) – ή οποιουδήποτε άλλου εγκλήματος, στο οποίο η χρήση του Διαδικτύου και των Τεχνολογιών Πληροφοριών και Επικοινωνιών συνετέλεσε με οποιοδήποτε τρόπο (λ.χ. επικοινωνία μεταξύ των δραστών με σκοπό την οργάνωση μιας τρομοκρατικής επίθεσης, λογισμικό επεξεργασίας εικόνων και αντίστοιχα αρχεία για την πλαστογράφηση διαβατηρίων), προκύπτει η **ανάγκη εγκληματολογικής ανάλυσης ψηφιακών πειστηρίων**.

Στη συνέχεια του κεφαλαίου αυτού θα αναφερθούμε στις διαδικασίες «παραδοσιακής» εγκληματολογικής ανάλυσης ψηφιακών πειστηρίων, θα δούμε τις βασικές αρχές που τις διέπουν και θα εξετάσουμε τι προβλέπεται σε νομικό επίπεδο στην Ελλάδα ως προς την Υπηρεσία που είναι αρμόδια για την ανάλυση ψηφιακών πειστηρίων. Έτσι, στα επόμενα κεφάλαια θα μπορούμε να εξηγήσουμε τι είναι το υπολογιστικό νέφος και γιατί μας αναγκάζει να αναζητήσουμε νέες μεθόδους και διαδικασίες ανάλυσης ψηφιακών πειστηρίων.

Αξίζει να σημειωθεί ότι συχνά στο κείμενο μπορεί να αναφερόμαστε σε «ανάλυση» ψηφιακών πειστηρίων, ωστόσο αναφερόμαστε στο σύνολο των σταδίων που απαιτούνται για τη συλλογή, την εξέταση, την ανάλυση των πειστηρίων και την παρουσίαση των ευρημάτων και όχι αποκλειστικά στο συνονόματο στάδιο από τα προαναφερθέντα[16].

Τι είναι τα ψηφιακά πειστήρια και που εντοπίζονται;

Υπάρχουν πολλοί διαφορετικοί ορισμοί για τα ηλεκτρονικά ή ψηφιακά πειστήρια. Σύμφωνα με τη Σύμβαση για τα εγκλήματα στον Κυβερνοχώρο (Σύμβαση της Βουδαπέστης)[17], αναφερόμαστε σε **πειστήρια ενός εγκλήματος που μπορούν να συλλεχθούν σε ηλεκτρονική μορφή**.

[16] Βλ. και παρακάτω ενότητα «Διαδικασίες εγκληματολογικής ανάλυσης»

[17] Σε διάφορα σημεία του κειμένου αναφέρεται «the collection of evidence in electronic form of a criminal offence» (βλ. προοίμιο, άρθρα 14, 23, 25, 35 και 46

Θα μπορούσαμε να πει κάποιος ότι ψηφιακά πειστήρια είναι πληροφορίες και δεδομένα με ερευνητικό ενδιαφέρον, τα οποία βρίσκονται αποθηκευμένα ή έχουν μεταβιβαστεί σε οποιασδήποτε μορφής αποθηκευτικό μέσο, μέσω υπολογιστικού συστήματος[18].

Τα ψηφιακά πειστήρια μπορούν να εντοπιστούν σε **διάφορες πηγές**. Μεταξύ άλλων σε:

- Hardware (υλικό),
- Software (λογισμικό),
- Δίκτυα,
- Ηλεκτρονικό ταχυδρομείο,
- Ψηφιακές φωτογραφίες και βίντεο,
- Μηχανήματα αυτόματης ανάληψης χρημάτων (ATM),
- Logs συναλλαγών,
- Έγγραφα (τύπου MS Word κ.λπ.),
- Λογιστικά φύλλα (τύπου MS Excel κ.λπ.),
- Ιστορικό συνομιλιών
- Ιστορικού του περιηγητή (λ.χ. Chrome, Firefox, Edge κ.λπ.),
- RAM (random access memory – προσωρινή μνήμη),
- Internet cookies,
- Αρχεία logs ενός server[19].

Σκοπός της εγκληματολογικής ανάλυσης πειστηρίων

Για τις Αρχές Επιβολής του Νόμου, σκοπός της εγκληματολογικής ανάλυσης είναι η συλλογή, η εξέταση και ανάλυση πειστηρίων, ώστε αυτά να παρουσιαστούν κατά την

[18] Σύμφωνα με ορισμό του 1999 (!) από το Scientific Working Group on Digital Evidence (SWGDE) μιλάμε για «Information of probative value stored or transmitted in digital form», https://archives.fbi.gov/archives/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm

[19] https://articles.forensicfocus.com/2012/07/11/retrieving-digital-evidence-methods-techniques-and-issues/

ακροαματική διαδικασία στο δικαστήριο[20]. Η νομοθεσία, βέβαια, σε κάθε Κράτος μπορεί να είναι διαφορετική, σε ότι αφορά την αποδεικτική ισχύ των πειστηρίων ενώπιον των Εισαγγελικών και Δικαστικών Αρχών[21].

Κατά τη διάρκεια μιας έρευνας, ένας εμπειρογνώμονας επιδιώκει να επιβεβαιώσει ορισμένα δεδομένα σχετικά με τις συσκευές ή τα συστήματα που εξετάζει.

- Για μια συσκευή: πως λειτουργούσε και ποιος ήταν ο σκοπός λειτουργίας της, τι πληροφορίες περιέχει και ποιος τη διαχειριζόταν ή τη χρησιμοποιούσε.
- Για ένα υπολογιστικό σύστημα: ποιοι ήταν οι χρήστες του συστήματος και ποιος ήταν ο σκοπός του υπολογιστή πελάτη ή εξυπηρετητή.
- Για έναν εξυπηρετητή: αν αποτελούσε μέρος ενός πιο σύνθετου συστήματος διασυνδεδεμένων εξυπηρετητών και ποιοι ήταν οι διαχειριστές και οι χρήστες του.

Αν πρόκειται για σύστημα στο οποίο κάποιος απέκτησε μη εξουσιοδοτημένη πρόσβαση, τότε πρέπει να διακριβωθεί τι είδους πληροφορίες εξήχθησαν από αυτό, καθώς και αν πρόκειται για παραβίαση από χρήστη μέσω κάποιου δικτύου (π.χ. μέσω Διαδικτύου) ή τοπικά.

Πρόκληση αποτελεί, κατά τη διάρκεια της ψηφιακής διερεύνησης, η ανάκτηση δεδομένων που έχουν διαγραφεί ή καταστραφεί και δεδομένων που χαρακτηρίζονται ως «εύθραυστα», δηλαδή δεδομένα που μπορούν να χαθούν εύκολα[22].

---

[20] Cameron, S., (2011). *Digital Evidence* στο FBI Law Enforcement Bulletin, σελ. 15, διαθέσιμο στο https://leb.fbi.gov/2011/august/leb-august-2011

[21] Richter, J., Kuntze, N., & Rudolph, C. (2010, May). *Security digital evidence* στο Systematic Approaches to Digital Forensic Engineering (SADFE), 2010 Fifth IEEE International Workshop on (pp. 119-130). IEEE., διαθέσιμο εδώ: http://www.vogue-project.de/cms/upload/pdf/EvidentialIntegrity.pdf

[22] Ο όρος που χρησιμοποιείται συνήθως στην αγγλική βιβλιογραφία είναι «volatile», δηλαδή «πτητικά», ωστόσο θεωρούμε ότι η λέξη «εύθραυστα» αποδίδει καλύτερα στα ελληνικά την ασταθή κατάσταση των δεδομένων αυτών και τους προσεκτικούς χειρισμούς που απαιτούνται από τον ερευνητή για να μην καταστραφούν.

Μπορεί εκ πρώτης όψεως οι μέθοδοι ανάλυσης ψηφιακών πειστηρίων, που θα δούμε στη συνέχεια, να φαίνονται χρονοβόρες και με υψηλό κόστος, ωστόσο, είναι προφανές ότι πλέον τα δεδομένα που εξάγονται είναι υπερ-πολύτιμα[23].

Βασικές αρχές εξέτασης ψηφιακών πειστηρίων

Τα ψηφιακά πειστήρια είναι εξίσου πολύτιμα με τα «παραδοσιακά» πειστήρια ενός εγκλήματος και για το λόγο αυτό θα πρέπει οι εκπρόσωποι των Αρχών Επιβολής του Νόμου να τα διαχειρίζονται με μεγάλη προσοχή.

Κατά την εξέταση των «παραδοσιακών» ψηφιακών πειστηρίων, προκειμένου αυτά να χρησιμοποιηθούν ενώπιων των δικαστικών Αρχών, πρέπει να πληρούνται ορισμένες προϋποθέσεις.

Ειδικότερα, σύμφωνα με το εγχειρίδιο Good Practice Guide for Computer-Based Electronic Evidence της Association of Chief Police Officers (ACPO)[24], θα πρέπει να υπάρχει συμμόρφωση ως προς τις ακόλουθες τέσσερις βασικές Αρχές από τους εμπειρογνώμονες – ερευνητές:

- **Αρχή 1:** Τα δεδομένα που βρίσκονται σε έναν υπολογιστή ή μια συσκευή δεν πρέπει να τροποποιηθούν από οποιονδήποτε.
- **Αρχή 2:** Οποιοδήποτε πρόσωπο αποκτά πρόσβαση στον υπολογιστή ή στη συσκευή πρέπει να έχει την απαραίτητη άδεια για να το κάνει, καθώς και να είναι σε θέση να εξηγήσει την αναγκαιότητα των ενεργειών του και τα αποτελέσματα αυτών.
- **Αρχή 3:** Θα πρέπει να καταγράφονται πλήρως όλες οι διαδικασίες που πραγματοποιούνται από τους ερευνητές πάνω στον υπολογιστή ή τη συσκευή. Όταν κάποιος τρίτος το θελήσει, θα πρέπει να μπορεί να είναι σε θέση να επαναλάβει τις ίδιες ακριβώς διαδικασίες και να λάβει τα ίδια ακριβώς αποτελέσματα.

---

[23] Hak, J., *The Admissibility of Digital Evidence in Criminal Prosecutions*, διαθέσιμο στο http://www.crime-scene-investigator.net/admissibilitydigitaleveidencecriminalprosecutions.html

[24] Βλ. σελ. 4 του Οδηγού, διαθέσιμος εδώ: https://www.cps.gov.uk/legal/assets/uploads/files/ACPO_guidelines_computer_evidence[1].pdf

- **Αρχή 4:** Το άτομο που είναι υπεύθυνο για την υπόθεση έχει την ευθύνη να διασφαλίσει την τήρηση των παραπάνω Αρχών και φυσικά της νομιμότητας των διαδικασιών.

Διαδικασίες εγκληματολογικής ανάλυσης

Τόσο στη βιβλιογραφία όσο και στην πράξη, η εγκληματολογική ανάλυση υπολογιστικών συστημάτων και ψηφιακών πειστηρίων περιλαμβάνει διάφορα βήματα που έχουν να κάνουν με τη συλλογή, την εξέταση, την ανάλυση των ψηφιακών πειστηρίων και τελικά την παρουσίαση των αποτελεσμάτων των προαναφερθέντων διαδικασιών.

Τα παραπάνω βήματα μπορεί να διαφέρουν με βάση τις οδηγίες, τις θέσεις και τους ειδικότερους σκοπούς διαφορετικών οργανισμών και φορέων[25].

Στη συνέχεια, καθόσον εστιάζουμε στην εγκληματολογική ανάλυση για τους σκοπούς των Αρχών Επιβολής του Νόμου, υιοθετούμε και παρουσιάζουμε μια απλουστευμένη **προσέγγιση τεσσάρων σταδίων**: συλλογή, εξέταση και ανάλυση πειστηρίων και τελικά παρουσίαση των αποτελεσμάτων.

Πιο συγκεκριμένα, αναφερόμαστε σε:

- **Συλλογή**: αναζήτηση, αναγνώριση, κατάσχεση και διατήρηση πειστηρίων.
- **Εξέταση**: όπου τα δεδομένα γίνονται ορατά και διακριβώνεται η προέλευσή τους και η σημασία τους.
- **Ανάλυση**: εξέταση της σημασίας και της ισχύος των δεδομένων.
- **Παρουσίαση**: όπου προετοιμάζονται αναφορές ή εκθέσεις, με βάση τις εξετάσεις, οι οποίες θα χρησιμοποιηθούν ενώπιον των εισαγγελικών και δικαστικών Αρχών.

α. Συλλογή ψηφιακών πειστηρίων

Για τη συλλογή ψηφιακών πειστηρίων, ο ανακριτικός υπάλληλος απαιτείται να έχει την κατάλληλη γνώση, γύρω από τις νέες τεχνολογίες.

[25] Μια ενδιαφέρουσα παρουσίαση με τα γνωστότερα μοντέλα είναι διαθέσιμη στο άρθρο του Jawad Abbas, T., (2015). *Studying the Documentation Process in Digital Forensic Investigation Frameworks / Models*, Journal of Al-Nahrain University Vol.18 (4), December, 2015, pp.153-162, διαθέσιμο εδώ: http://www.iasj.net/iasj?func=fulltext&aId=107014

Κατά τη διάρκεια μιας έρευνας, ο ανακριτικός υπάλληλος πρέπει να συλλέξει πειστήρια που σχετίζονται άμεσα ή έμμεσα με το έγκλημα, εστιάζοντας σε όλα εκείνα τα δεδομένα που ανήκουν στη σφαίρα του ψηφιακού κόσμου. Ψηφιακά πειστήρια και δεδομένα μπορεί να περιέχονται σε αφαιρούμενους χώρους αποθήκευσης (USB sticks, εξωτερικούς σκληρούς δίσκους).

Η κατάσχεση υπολογιστών και λοιπών συσκευών θα πρέπει να γίνεται με τέτοιο τρόπο ώστε να μην προκληθούν φυσικές φθορές ή άλλες αλλοιώσεις στα δεδομένα. Ούτε βέβαια επιτρέπεται η εγκατάσταση, προσθήκη ή αφαίρεση λογισμικού ή δεδομένων κατά τη διάρκεια της κατάσχεσης. Οι ίδιοι περιορισμοί ισχύουν τόσο για τον πρώτο ανταποκριτή στη «σκηνή του εγκλήματος», όσο και για τον εμπειρογνώμονα που θα συνεχίσει στα επόμενα στάδια.

Ακόμα, στη «σκηνή του εγκλήματος» πρέπει να δοθεί προτεραιότητα στη διασφάλιση των **«εύθραυστων» δεδομένων** (online chat, απομακρυσμένη αποθήκευση, κρυπτογραφημένοι φάκελοι, RAM) και στον έλεγχο των τρεχουσών διαδικασιών και ενεργών συνδέσεων σε δίκτυο ή στο Διαδίκτυο[26].

Τέλος, αν πρόκειται για εταιρεία που χρησιμοποιεί εξυπηρετητή, δεν είναι πάντα εφικτό να κατασχέσει κάποιος το σύνολο του εξοπλισμού ή απλά να σταματήσει τη λειτουργία του, διακόπτοντας την παροχή ρεύματος. Οι πόροι του συστήματος μπορεί να χρησιμοποιούνται και για άλλες, νόμιμες δραστηριότητες, συνεπώς η παύση λειτουργίας του συστήματος μπορεί να προκαλέσει σοβαρά προβλήματα. Η βοήθεια ενός τεχνικού της εταιρείας ίσως είναι πολύτιμη σε αυτή την περίπτωση[27].

β. Εξέταση ψηφιακών πειστηρίων

Κατά τη διάρκεια ερευνών, η εξέταση του κατασχεμένου υλικού θα πρέπει να γίνεται από εκπαιδευμένο και έμπειρο προσωπικό. Οι προβλεπόμενες διαδικασίες θα πρέπει να ακολουθούνται αυστηρά, για την αποφυγή αλλοίωσης δεδομένων.

---

[26] Lee, S., Kim, H., Lee, S., & Lim, J. (2005, November). *Digital evidence collection process in integrity and memory information gathering*. Στο First International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE'05) (pp. 236-247). IEEE.

[27] Massachusetts Digital Evidence Consortium, (2015). *Digital Evidence Guide for First Responders*, σελ. 10, διαθέσιμο εδώ: http://www.iacpcybercenter.org/wp-content/uploads/2015/04/digitalevidence-booklet-051215.pdf

Υπάρχουν δύο εναλλακτικές επιλογές: είτε κατάσχεση πειστηρίων (π.χ. CD, DVD, σκληρών δίσκων, συσκευών τηλεφώνου) είτε δημιουργία αντιγράφων των αναγκαίων δεδομένων (ολόκληρου του δίσκου ή μεμονωμένων αρχείων).

Όποια διαδικασία κι αν ακολουθηθεί, είναι απαραίτητο (όταν τουλάχιστο είναι δυνατό), ο ερευνητής να δημιουργεί ένα **αντίγραφο backup** του κατασχεμένου υλικού, για δύο λόγους:

- αν κάτι πάει στραβά κατά τη διάρκεια της ανάλυσης (π.χ. αν καταστραφεί η δομή δεδομένων), υπάρχει πάντα η δυνατότητα να δημιουργηθεί ένα επιπλέον αντίγραφο και να συνεχιστεί η εξέταση και
- αν αργότερα οι ερευνητές χρειαστεί να αναπαράγουν στο γραφείο ή στο εργαστήριο την κατάσταση του δίσκου, όπως αυτή ήταν τη στιγμή της έρευνας, δε θα υπάρχουν δυσκολίες, γιατί τα πρωτότυπα μέσα δε χρησιμοποιήθηκαν για εργασίες ανάλυσης, συνεπώς τα δεδομένα τους δεν έχουν αλλάξει[28].

Εξάλλου, δεν πρέπει να ξεχνά κανείς ότι ο υπολογιστής, ή μια συσκευή αποθήκευσης, μπορούν να περιέχουν πληροφορίες και δεδομένα που να μην είναι εξ αρχής ορατά, δηλαδή να έχουν διαγραφεί ή να βρίσκονται σε κρυφούς φακέλους. Εξίσου πιθανό είναι τα δεδομένα να έχουν κρυπτογραφηθεί[29], ή να βρίσκονται σε τέτοια μορφή που δεν είναι εύκολο να αναλυθούν (λ.χ. μεγάλες βάσεις δεδομένων, φύλλα εργασίας κ.λπ.).

γ. Ανάλυση ψηφιακών πειστηρίων

Η ανάλυση των ψηφιακών πειστηρίων είναι ίσως το πιο σημαντικό στάδιο της έρευνας. Σε αυτή περιλαμβάνεται η εξέταση της σημασίας και της ισχύος των δεδομένων.

Στο βήμα αυτό, τα δεδομένα εξετάζονται ως προς τη σχέση και τη σύνδεσή τους με την ερευνώμενη υπόθεση. Αναζητούνται διασυνδέσεις ανάμεσα στα δεδομένα που προέκυψαν από την εξέταση και εκείνα που ήταν ήδη διαθέσιμα πριν αυτή ξεκινήσει. Το ευρήματα μπορούν να επιβεβαιώσουν υποθέσεις σχετικά με το υπό έρευνα έγκλημα.

---

[28] Wang, S. J. (2007). *Measures of retaining digital evidence to prosecute computer-based cyber-crimes.* Στο Computer Standards & Interfaces, 29(2), 216-223.

[29] Casey, E. (2002). *Practical approaches to recovering encrypted digital evidence*. Στο International Journal of Digital Evidence, 1(3), 1-26

Όπως και στα προηγούμενα στάδια, έτσι κι εδώ, τα άτομα που θα διενεργήσουν την ανάλυση θα πρέπει να έχουν λάβει την αντίστοιχη εκπαίδευση, να είναι έμπειρα στη χρήση διαφορετικών λειτουργικών συστημάτων, εξοπλισμού και δημοφιλών εφαρμογών – λογισμικών.

Υπάρχουν δύο τύποι ανάλυσης, η offline και η live (online).

i) Ανάλυση offline

Αναφερόμαστε στην ανάλυση κατά την οποία ο υπολογιστής, ο εξυπηρετητής, το αποθηκευτικό μέσο ή η συσκευή είναι εκτός λειτουργίας. Συνήθως, αλλά όχι πάντα, σημαίνει ότι η ερευνώμενη συσκευή έχει μεταφερθεί στο εργαστήριο, όπου θα πρέπει να ακολουθηθούν όλες οι νόμιμες διαδικασίες.

Είναι αναγκαία η ύπαρξη πλήρους backup της συσκευής, για τους λόγους που εξηγήθηκαν νωρίτερα. Θα πρέπει, επίσης, να χρησιμοποιούνται εργαλεία που να αποτρέπουν την εγγραφή στα πρωτότυπα πειστήρια (**write-blocking**), τα οποία μπορεί να βασίζονται σε software ή hardware. Σε κάθε περίπτωση, πρέπει να διασφαλίζεται η ακεραιότητα των παραγόμενων αντιγράφων (μέσω υπολογισμού του hash value, π.χ. με το MD5 ή το SHA-1).

ii) Ανάλυση live (online)

Πρόκειται για ανάλυση που πραγματοποιείται όσο η συσκευή είναι ακόμα σε λειτουργία. Κι εδώ ισχύει ο βασικός κανόνας, να μην τροποποιηθούν με οποιοδήποτε τρόπο τα δεδομένα. Δεν επιτρέπεται η εγκατάσταση εργαλείων ή λογισμικού, ούτε η αντιγραφή δεδομένων στο σκληρό δίσκο της συσκευής.

Για να πραγματοποιηθεί μια ανάλυση τέτοιου είδους, χρησιμοποιείται ειδικό λογισμικό – που σε καμία περίπτωση δεν εγκαθίσταται στο σύστημα. Τα δεδομένα της ανάλυσης εξάγονται απευθείας και αποθηκεύονται σε εξωτερικές συσκευές, λ.χ. μια συσκευή αποθήκευσης τύπου USB stick.

Οι συσκευές αποθήκευσης μπορεί να περιέχουν πλήθος δεδομένων, συνήθως, όμως, μόνο ένα μικρό μέρος αυτών είναι σχετικό με την ερευνώμενη υπόθεση. Η διαδικασία εντοπισμού των σχετικών δεδομένων μπορεί να είναι χρονοβόρα, ειδικά στις

περιπτώσεις εκείνες που ο ερευνητής δε γνωρίζει επακριβώς τι αναζητά (ή τι άλλο μπορεί να κρύβεται σε ένα αποθηκευτικό μέσο)[30].

δ. Παρουσίαση των ευρημάτων

Παρουσίαση των ευρημάτων σημαίνει προετοιμασία **εκθέσεων**, με βάση τις εξετάσεις και αναλύσεις που έγιναν, οι οποίες (εκθέσεις) θα χρησιμοποιηθούν ενώπιον των εισαγγελικών και δικαστικών Αρχών.

Κάθε βήμα της διαδικασίας έρευνας πρέπει να περιγράφεται λεπτομερώς, χωρίς παραλείψεις. Η πλήρης και αναλυτική περιγραφή των ενεργειών του ερευνητή διασφαλίζουν την ακεραιότητα και αξιοπιστία της ανάλυσης. Στόχος είναι τα ευρήματα να παρουσιαστούν με τρόπο απλό και κατανοητό στο ευρύ κοινό.

Εκτός από φωτογραφίες των πειστηρίων, στις εκθέσεις περιλαμβάνονται στοιχεία αναφορικά με την κατάσταση του εξοπλισμού και του λογισμικού που χρησιμοποιήθηκαν, τις διαδικασίες που ακολουθήθηκαν, καθώς και οτιδήποτε άλλο κατά την κρίση του ερευνητή συμβάλει στη διαλεύκανση της ερευνώμενης υπόθεσης[31].

Παραδεκτό (admissibility) των ψηφιακών πειστηρίων

Σε διεθνές επίπεδο **δεν υφίσταται κοινώς αποδεκτή μέθοδος** για την παρουσίαση των ευρημάτων στο δικαστήριο[32]. Ωστόσο, είναι κρίσιμης σπουδαιότητας η διασφάλιση των αποδείξεων ως προς την αλληλουχία των βημάτων της έρευνας[33], αλλά και της

[30] Οδηγίες και λεπτομέρειες σχετικά με τις διαδικασίες ανάλυσης είναι διαθέσιμες στο Guide to Integrating Forensic Techniques into Incident Response: του National Institute of Standards and Technology (NIST), εδώ http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf και στον ιστότοπο https://www.torridnetworks.com/services/incident-response/cyber-forensics

[31] Hershensohn, J., & Block, D. (2005). *IT Forensics: the collection of and presentation of digital evidence* στο ISSA (pp. 1-14)

[32] Roscini, M. (2016). *Digital evidence as a means of proof before the International Court of Justice* στο Journal of Conflict and Security Law, 21

[33] Γνωστό με τον όρο «chain of custody». Περιλαμβάνει καταγραφές των κινήσεων, των τοποθεσιών και των ατόμων που κατέχουν τα πειστήρια με την πάροδο του χρόνου.

εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών που διαχειρίζεται ο ερευνητής στη διάρκεια της διαδικασίας εγκληματολογικής ανάλυσης[34].

Τμήμα Εξέτασης Ψηφιακών Πειστηρίων / Δ.Ε.Ε.

Στην Ελλάδα αρμόδια Υπηρεσία για την εξέταση ψηφιακών πειστηρίων τυγχάνει η Διεύθυνση Εγκληματολογικών Ερευνών του Αρχηγείου της Ελληνικής Αστυνομίας και συγκεκριμένα το **Τμήμα Εξέτασης Ψηφιακών Πειστηρίων**.

Σύμφωνα με το άρθρο 30, παρ. 22 του Π.Δ. 178/2014, το Τμήμα Εξέτασης Ψηφιακών Πειστηρίων είναι αρμόδιο για να εξετάζει ή αναλύει ψηφιακά, ηλεκτρονικά ή ακουστικά μέσα και τα δεδομένα που περιέχονται σ' αυτά, τα οποία περισυλλέγονται από τον τόπο του εγκλήματος από το Τμήμα Εξερευνήσεων της Δ.Ε.Ε., ή αποστέλλονται με σχετική παραγγελία από ανακριτική, εισαγγελική ή δικαστική αρχή, υπό την προϋπόθεση ότι πρόκειται για μέσα που επιδέχονται εργαστηριακές εξετάσεις και μπορούν να συμβάλουν στην εξιχνίαση εγκληματικής πράξης.

Το Τμήμα διαθέτει Εργαστήριο Εξέτασης Πειστηρίων Υπολογιστικών Συστημάτων, το οποίο είναι αρμόδιο πρώτα απ' όλα να ενεργεί ανάγνωση, ανάκτηση – επαναφορά, εξέταση, αποκρυπτογράφηση, ανάλυση, σύγκριση, επεξεργασία, καταγραφή δεδομένων, ευρισκομένων σε αποθηκευτικούς ψηφιακούς χώρους τοπικών δικτύων ηλεκτρονικών υπολογιστών και περιφερειακών ή άλλων ειδικών σταθερών ή φορητών μέσων ψηφιακής αποθήκευσης δεδομένων *(εδ. α αα)*.

Επιπλέον, αποφαίνεται για τον τρόπο λειτουργίας λογισμικού ή ψηφιακού υλικού, διαπιστώνει την αλληλουχία των ενεργειών χρήσης λογισμικού ή υλικού και ενεργεί εξετάσεις για την εξακρίβωση του δημιουργού ή του χρήστη εφαρμογών ή δεδομένων επί ψηφιακών πειστηρίων, που είναι πρόσφορα προς ανάγνωση *(εδ. α ββ)*.

Πέρα από τους υπολογιστές, στο Εργαστήριο διενεργούνται εξετάσεις επί ηλεκτρονικών συσκευών ή άλλων ειδικών ηλεκτρονικών διατάξεων, οι οποίες είναι δυνατόν να αποθηκεύουν ψηφιακά δεδομένα, επί κινητών τηλεφώνων και συσκευών

[34] Prayudi, Y., & Sn, A. (2015). *Digital Chain of Custody: State of the Art*. Στο International Journal of Computer Applications, 114(5). Βλ. και Karyda, M., & Mitrou, L. (2007, August). *Internet forensics: Legal and technical issues.* Στο Digital Forensics and Incident Analysis, 2007. WDFIA 2007. Second International Workshop on (pp. 3-12). IEEE.

εντοπισμού θέσης, αλλά και εξειδικευμένες εξετάσεις, αναγνώσεις, ανακτήσεις και αναλύσεις ψηφιακών δεδομένων επί τραπεζικών ή άλλων καρτών *(εδ. α γγ, δδ, εε)*.

Ακόμα, εφόσον η εξέταση δεν είναι δυνατόν να διενεργηθεί στο Εργαστήριο Διερεύνησης Παραχάραξης – Κιβδηλείας και Πλαστότητας Εντύπων και Αξιών του Τμήματος Εργαστηρίων Δικαστικής Γραφολογίας και Πλαστότητας Εντύπων και Αξιών της Δ.Ε.Ε., διενεργεί εξετάσεις επί συναφών ειδικών ηλεκτρονικών μέσων (ηλεκτρονικών διαβατηρίων) *(εδ. α εε)*.

Τέλος, το Εργαστήριο ενεργεί εξετάσεις σε συστήματα τηλεπικοινωνιών, σε συσκευές λήψης δορυφορικού τηλεοπτικού ή άλλου σήματος τα οποία περιέχουν ψηφιακά δεδομένα πρόσφορα προς ανάγνωση *(εδ. α στστ)*.

Παράλληλα, συνεργάζεται με τις επιληφθείσες Υπηρεσίες για τη διασφάλιση της κατάσχεσης, ορθής διαχείρισης και ταχύτερης αποστολής των προς εξέταση πειστηρίων, παρέχοντας σε αυτές οδηγίες ασφαλούς μεταφοράς και φύλαξης, ενώ σε εξαιρετικά κρίσιμες περιπτώσεις παρέχει τεχνική συνδρομή στην κατάσχεση, δια της αποστολής εξειδικευμένου κλιμακίου *(εδ. α ζζ)*.

Οι υπηρετούντες στο Τμήμα Εξέτασης Ψηφιακών Πειστηρίων[35] συντάσσουν εκθέσεις πραγματογνωμοσύνης για κάθε εργαστηριακή εξέταση, προς χρήση από τις κατά νόμο αρμόδιες Αρχές[36].

Άρση του απορρήτου των επικοινωνιών

Σε ορισμένες περιπτώσεις οι Υπηρεσίες που αποστέλλουν πειστήρια προς εξέταση στο Τμήμα Εξέτασης Ψηφιακών Πειστηρίων υποβάλλουν ερωτήματα που αφορούν και στην εξέταση στοιχείων επικοινωνίας, όπως το περιεχόμενο αρχείων ή άλλων στοιχείων που περιλαμβάνονται σε ηλεκτρονική αλληλογραφία (emails), ή ηλεκτρονική συνομιλία (chat), καθώς και το περιεχόμενο γραπτών μηνυμάτων (SMS) από κινητά τηλέφωνα κ.λπ. που περιέχονται σε πειστήριο υπολογιστικό σύστημα. Τότε, απαιτείται **η έκδοση Βουλεύματος από το αρμόδιο δικαστικό συμβούλιο**, με το οποίο να διατάσσεται η «άρση του απορρήτου των επικοινωνιών» για τα συγκεκριμένα υπό εξέταση πειστήρια και

[35] Εφόσον τους έχει απονεμηθεί σχετική ειδικότητα, σύμφωνα με το άρθρο 111 του Π.Δ. 342/1977

[36] Παράγραφος 23 άρθρου 30 Π.Δ. 178/2014

να διατάσσεται ειδικά το Εργαστήριο Εξέτασης Πειστηρίων Υπολογιστικών Συστημάτων της Δ.Ε.Ε. να πραγματοποιήσει εξετάσεις επί αυτών[37].

Στην περίπτωση που δεν αποσταλεί στη Δ.Ε.Ε. σχετικό Βούλευμα περί «άρσης του απορρήτου των στοιχείων επικοινωνίας», **οι εξετάσεις περιορίζονται στα στοιχεία εκείνα για τα οποία αυτό δεν απαιτείται**. Τότε, βέβαια, γίνεται σχετική μνεία στην συνταχθείσα από το Τμήμα Εξέτασης Ψηφιακών Πειστηρίων έκθεση εργαστηριακής πραγματογνωμοσύνης.

Εγκληματολογική ανάλυση ψηφιακών πειστηρίων & υπολογιστικό νέφος

Τα όσα παρατέθηκαν στο παρόν κεφάλαιο είναι εύκολο να εφαρμοστούν όταν έχει κάποιος στα χέρια του τις συσκευές προς εξέταση (π.χ. εξωτερικό σκληρό δίσκο, αποθηκευτική μνήμη τύπου USB stick, CD-ROM). Λόγω της προόδου της τεχνολογίας, ωστόσο, και της εμφάνισης του υπολογιστικού νέφους (βλ. Κεφάλαιο 2), οι παραπάνω διαδικασίες δύσκολα μπορούν να εφαρμοστούν, τόσο για τεχνικούς, όσο και για νομικούς λόγους, που θα εξετάσουμε στα επόμενα κεφάλαια.

❑

[37] Σύμφωνα με Ν. 2225/1994 όπως τροπ. και ισχύει και Π.Δ. 47/2005, όπως τροπ. και ισχύει

Κεφάλαιο 2: Περί υπολογιστικού νέφους

Στις μέρες μας, στον κόσμο των Τεχνολογιών Πληροφοριών και Επικοινωνιών, μπορεί κάποιος να χρησιμοποιεί, μέσω Διαδικτύου, υλικό (hardware), λογισμικό (software) και υπηρεσίες (services) που του παρέχονται, συνήθως, από μια εταιρεία απομακρυσμένα, δωρεάν ή με κάποιο αντίτιμο. Για παράδειγμα, αντί να αγοράσει έναν εξωτερικό σκληρό δίσκο αποθήκευσης δεδομένων, τον οποίο θα συνδέει τοπικά στον υπολογιστή του, μπορεί να αγοράσει χώρο αποθήκευσης για τα αρχεία του online, στον οποίο θα έχει πρόσβαση με τη χρήση διαπιστευτηρίων (όνομα χρήστη ή e-mail και κωδικό πρόσβασης). Η πραγματική τοποθεσία των δεδομένων του χρήστη, στην τελευταία περίπτωση, είναι σχεδόν πάντα άγνωστη, αλλά ίσως και αδιάφορη.

Τι είναι το υπολογιστικό νέφος (cloud computing);

Σύμφωνα με τον ορισμό που δίνει το **National Institute of Standards and Technology (NIST)** των Ηνωμένων Πολιτειών Αμερικής, ως **υπολογιστικό νέφος** ορίζεται *«το μοντέλο το οποίο καθιστά δυνατή την κατ' αίτηση διαδικτυακή πρόσβαση σε ένα κοινόχρηστο σύνολο (shared pool) παραμετροποιήσιμων υπολογιστικών πόρων (π.χ. δίκτυα, διακομιστές, αποθηκευτικοί χώροι, εφαρμογές και υπηρεσίες) και το οποίο μπορεί να τροφοδοτηθεί γρήγορα και να διατεθεί με ελάχιστη προσπάθεια διαχείρισης ή αλληλεπίδραση με τον παρόχο της υπηρεσίας»*[38].

Βασικά χαρακτηριστικά του υπολογιστικού νέφους

Ορισμένα από τα βασικά χαρακτηριστικά του υπολογιστικού νέφους, σύμφωνα και πάλι με το NIST[39], είναι τα ακόλουθα:

- **On-demand self-service:** Ο κάθε χρήστης μπορεί ανεξάρτητα και μεμονωμένα να έχει πρόσβαση σε υπηρεσίες, όπως συνδεσιμότητα με ένα δίκτυο (network), αποθήκευση, αυτομάτως και όποτε το επιθυμεί, χωρίς να απαιτείται ανθρώπινη παρέμβαση για την διεκπεραίωση των λειτουργιών αυτών.

[38] Mell, P., Grance, T., (2011). *The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology*, Special Publication 800-145, διαθέσιμο στο http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

[39] Mell, P. Grance, T. ό.π.

- **Ευρεία πρόσβαση στο δίκτυο:** Οι υπολογιστικές δυνατότητες που παρέχονται είναι διαθέσιμες μέσω του δικτύου και προσβάσιμες μέσα από τυποποιημένους μηχανισμούς, οι οποίοι επιτρέπουν τη χρήση μέσα από ετερογενείς πλατφόρμες (thin or thick client platforms).
- **Resource pooling:** Οι υπολογιστικοί πόροι του παρόχου αποτελούν ένα κοινόχρηστο σύνολο το οποίο είναι ευέλικτο και δυναμικό, ανάλογα με τις απαιτήσεις του χρήστη. Ο χρήστης γενικά δεν γνωρίζει επακριβώς τη φυσική τοποθεσία των πόρων που χρησιμοποιεί, αλλά μπορεί να προσδιορίσει κάποια γενικά στοιχεία, όπως μια χώρα ή μια περιοχή.
- **Γρήγορη ελαστικότητα (Rapid elasticity):** Οι υπολογιστικές δυνατότητες προσφέρονται με ταχύτητα και ελαστικότητα, και σε κάποιες περιπτώσεις αυτόματα, με βάση τη ζήτησή τους. Στην πράξη οι πελάτες θεωρούν ότι οι δυνατότητές τους είναι απεριόριστες.
- **Measured Service:** Τα συστήματα cloud αυτόματα ελέγχουν και βελτιστοποιούν τη χρήση των πόρων ανάλογα με το είδος της υπηρεσίας (π.χ. αποθήκευση, bandwidth, ενεργοί λογαριασμοί χρηστών κ.λπ.). Η χρήση των πόρων ελέγχεται και παρακολουθείται συστηματικά, ώστε τόσο ο πελάτης όσο και ο πάροχος να έχουν σαφή εικόνα της κατάστασης της υπηρεσίας.

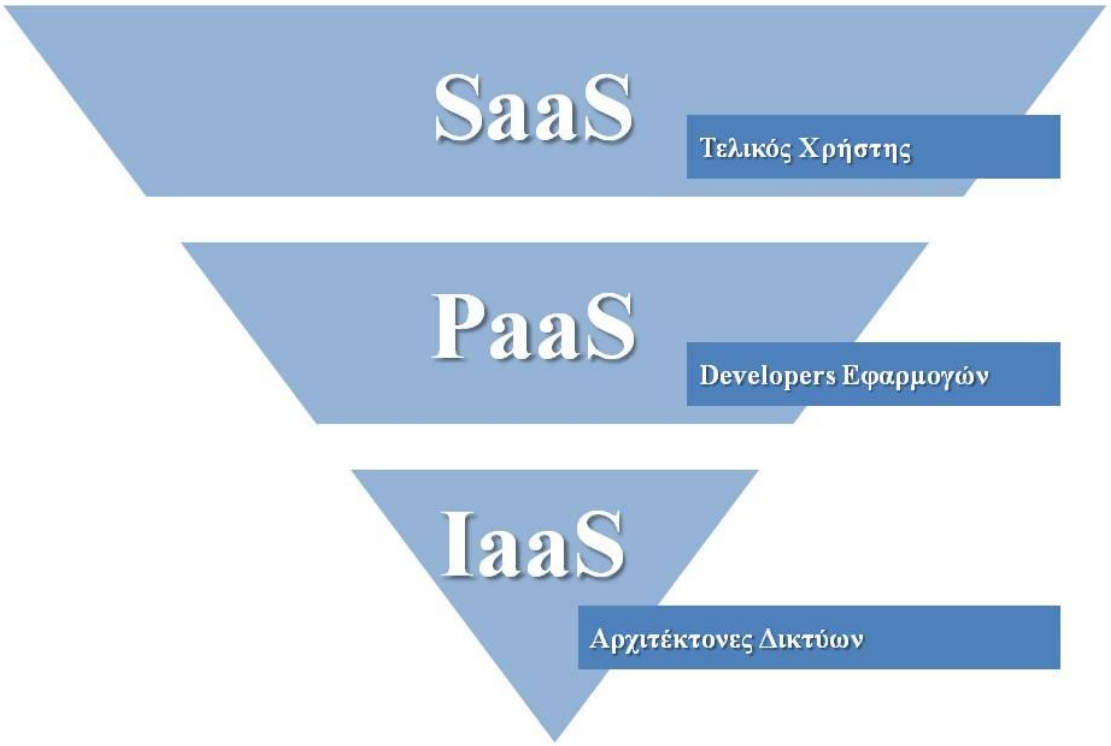
Μοντέλα παροχής υπηρεσιών υπολογιστικού νέφους

Στη συνέχεια παρουσιάζονται τα υπάρχοντα μοντέλα παροχής υπηρεσιών του υπολογιστικού νέφους, καθένα από τα οποία εξυπηρετεί διαφορετικές ανάγκες.

- **Software as a Service (SaaS):** Το «Λογισμικό ως Υπηρεσία» βασίζεται στην ιδέα της «ενοικίασης» λογισμικού που προσφέρει ένας πάροχος, αντί της αγοράς ενός πακέτου λογισμικού. Το λογισμικό βρίσκεται σε ένα δίκτυο εξυπηρετητών και διατίθεται μέσω Διαδικτύου. Εξίσου γνωστός είναι και ο όρος «Software on Demand». Πρακτικά, στην περίπτωση αυτή, ο πάροχος της υπηρεσίας φιλοξενεί τόσο την εφαρμογή, όσο και τα δεδομένα και με αυτό τον τρόπο οι χρήστες έχουν πρόσβαση σε αυτά από οπουδήποτε κι αν βρίσκονται. Χαρακτηριστικό πλεονέκτημα του SaaS είναι η μη απαίτηση από την πλευρά του πελάτη της συντήρησης ή της αναβάθμισης του λογισμικού, καθόσον αποκλειστικά υπεύθυνος γι’ αυτά είναι ο πάροχος της υπηρεσίας.

- **Platform as a Service (PaaS):** Η «Πλατφόρμα ως Υπηρεσία» περιλαμβάνει μια γκάμα εφαρμογών κυρίως για εταιρίες πληροφορικής αλλά και ιδιώτες, που δραστηριοποιούνται στην δημιουργία λογισμικού. Πρακτικά, παρέχει κατάλληλες υπηρεσίες για ανάπτυξη, διάθεση και συντήρηση εφαρμογών ή υπηρεσιών πληροφορικής μέσα σε μια ενιαία πλατφόρμα. Ο χρήστης δεν είναι διαχειριστής της υποδομής (δίκτυα, εξυπηρετητές, λειτουργικά συστήματα, μέσα αποθήκευσης κ.λπ.), αλλά είναι σε θέση να ελέγχει τις εφαρμογές που έχουν αναπτυχθεί και να παραμετροποιεί το περιβάλλον όπου αυτές φιλοξενούνται.
- **Infrastructure as a Service (IaaS):** Η «Υποδομή ως Υπηρεσία» αξιοποιείται κυρίως από επιχειρήσεις, καθώς έτσι έχουν στη διάθεσή τους προς «ενοικίαση» υπολογιστικούς και δικτυακούς πόρους. Με άλλα λόγια, η υποδομή της επιχείρησης (ή του χρήστη) είναι εικονική και μπορεί να προσαρμοστεί ανάλογα με τις ανάγκες που προκύπτουν[40].

Τα μοντέλα SaaS, PaaS και IaaS αποτυπώνονται γραφικά στο ακόλουθο σχήμα:



Γράφημα 1: Τα μοντέλα παροχής υπηρεσιών στο cloud computing

[40] https://support.rackspace.com/white-paper/understanding-the-cloud-computing-stack-saas-paas-iaas/

Το υπολογιστικό νέφος στην καθημερινότητά μας

Σχεδόν όλοι μας χρησιμοποιούμε το υπολογιστικό νέφος καθημερινά, χωρίς να το συνειδητοποιούμε.

Ακόμα και η πιο συνηθισμένη δραστηριότητά μας στο Διαδίκτυο, μια απλή αναζήτηση μέσω της μηχανής αναζήτησης της Google[41], ολοκληρώνεται γρήγορα και με ακρίβεια όχι γιατί ο υπολογιστής που χρησιμοποιούμε έχει όλες τις απαντήσεις έτοιμες, αλλά γιατί αξιοποιεί μέσω Διαδικτύου μια σειρά από άλλες υπηρεσίες: δεν είναι τίποτα παραπάνω από ένας «αγγελιοφόρος». Οι λέξεις που καταχωρεί κάποιος στη μηχανή αναζήτησης «ταξιδεύουν» μέσω Διαδικτύου σε έναν από τα εκατοντάδες χιλιάδες συμπλέγματα υπολογιστών της Google, τα οποία αναζητούν τα αποτελέσματα για μας και τα επιστρέφουν στην οθόνη μας. Με άλλα λόγια, για να πάρουμε εμείς τα αποτελέσματα της αναζήτησής μας στην οθόνη του υπολογιστή μας, έχει δουλέψει για εμάς στο παρασκήνιο μια συσκευή που η φυσική της τοποθεσία είναι στην Καλιφόρνια, στο Δουβλίνο, στο Τόκυο ή κάπου αλλού, που δεν το γνωρίζουμε – και προφανώς δε μας ενδιαφέρει να το γνωρίζουμε.

Παρόμοιος με τα παραπάνω είναι πλέον και ο τρόπος λειτουργίας του ηλεκτρονικού ταχυδρομείου μας. Παλαιότερα για να αποστείλει και να λάβει κάποιος μήνυμα ηλεκτρονικού ταχυδρομείου θα έπρεπε να έχει εγκατεστημένο τοπικά στον υπολογιστή του ένα συγκεκριμένο λογισμικό (π.χ. Microsoft Outlook). Σήμερα μας είναι πολύ πιο οικεία η διαχείριση του ηλεκτρονικού μας ταχυδρομείου μέσω ενός περιηγητή Διαδικτύου (browser): τα μηνύματά μας αποθηκεύονται σε έναν εξυπηρετητή – σε μια φυσική τοποθεσία που δε γνωρίζουμε – και έχουμε πρόσβαση σε αυτά για να τα επεξεργαστούμε μέσω Διαδικτύου από οποιοδήποτε σημείο του κόσμου.

Ένα τελευταίο, χαρακτηριστικό παράδειγμα χρήσης του υπολογιστικού νέφους είναι η online επεξεργασία εγγράφων, φύλλων εργασίας, παρουσιάσεων ή άλλου είδους αρχείων μέσω υπηρεσιών όπως το Google Docs[42]. Αντί για τα συνηθισμένα λογισμικά επεξεργασίας εγγράφων όπως το Microsoft Word ή το OpenOffice, που λειτουργούν τοπικά στον υπολογιστή μας, έχουμε τη δυνατότητα να χρησιμοποιήσουμε online λογισμικά – που δεν απαιτούν εγκατάσταση στη συσκευή μας – για να επεξεργαστούμε τα

[41] https://www.google.com

[42] https://docs.google.com

έγγραφά μας. Τα αρχεία μας μπορούμε να τα αποθηκεύσουμε online, στις αντίστοιχες πλατφόρμες αποθήκευσης που διατίθενται και, τελικά, με τον τρόπο αυτό να έχουμε τη δυνατότητα να «εργαστούμε» απομακρυσμένα με τα αρχεία μας απ' όπου κι αν βρισκόμαστε.

Πλεονεκτήματα και μειονεκτήματα χρήσης του υπολογιστικού νέφους

Η χρήση του υπολογιστικού νέφους, αντί για άλλες τεχνολογίες, στην καθημερινότητά μας, συνεπάγεται τόσο πλεονεκτήματα όσο και μειονεκτήματα.

Μεταξύ των **πλεονεκτημάτων** χρήστης των υπηρεσιών του cloud computing συγκαταλέγεται, αρχικά, το αποδοτικό κόστος αυτών: πρόκειται για μια συμφέρουσα επιλογή σε σχέση με το κόστος χρήσης τους, αλλά και συντήρησης και αναβαθμίσεών τους.

Εν συνεχεία, όταν μιλάμε για υπολογιστικό νέφος, είναι σχεδόν δεδομένη η μη ύπαρξη περιορισμών ως προς τον όγκο των πληροφοριών που μπορούμε να αποθηκεύσουμε σε αυτό. Σε γενικές γραμμές, βέβαια, στον τελικό χρήστη παρέχεται δωρεάν μόνο ένα συγκεκριμένο μέγεθος χώρου αποθήκευσης, ωστόσο υπάρχει πάντα η επιλογή αύξησης του μεγέθους του χώρου αποθήκευσης με το ανάλογο (χαμηλό) κόστος.

Εξίσου σημαντική για τους τελικούς χρήστες αναδεικνύεται η δυνατότητα αυτοματοποιημένης δημιουργίας αντιγράφων ασφαλείας, γνωστότερη με τον όρο «backup». Αντί για τη χειροκίνητη αποθήκευση αντιγράφων ασφαλείας σε μια εξωτερική συσκευή (π.χ. εξωτερικό σκληρό δίσκο ή μνήμη τύπου USB stick), η διαδικασία του backup γίνεται αυτόματα, εύκολα και ταχύτατα. Έτσι, σε περίπτωση απώλειας των δεδομένων εξαιτίας οποιασδήποτε αιτίας, τα αντίγραφα ασφαλείας στο cloud επιτρέπουν την επαναφορά των συστημάτων στην προηγούμενη κατάστασή τους.

Τέλος, σπουδαίο ρόλο στην θετική ανταπόκριση των χρηστών απέναντι στην τεχνολογία υπολογιστικού νέφους διαδραματίζει και η ευκολία χρήσης της: αφενός η διαδικασία εγκατάστασης του αναγκαίου λογισμικού διαρκεί ελάχιστα και αφετέρου οι πόροι και τα δεδομένα είναι διαθέσιμα σε οποιοδήποτε σημείο κι αν βρίσκεται ο χρήστης – αρκεί φυσικά να υφίσταται σύνδεση στο Διαδίκτυο[43].

---

[43] Miller, M. (2009). *Cloud Computing Pros and Cons for End Users*. Διαθέσιμο εδώ: http://dosen.narotama.ac.id/wp-content/uploads/2012/01/Cloud-Computing-Pros-and-Cons-for-End-Users.doc

Από την άλλη πλευρά, η τεχνολογία του υπολογιστικού νέφους συνδέεται με σειρά **μειονεκτημάτων**, που ενδέχεται να επηρεάσουν αρνητικά την εμπειρία του τελικού χρήστη.

Πρώτα απ' όλα, υφίστανται ζητήματα για τη μυστικότητα – και κατ' επέκταση την ασφάλεια – των δεδομένων που ο χρήστης «αναρτά στο σύννεφο». Τα δεδομένα αυτά πρακτικά περνούν στην κυριότητα τρίτων – σε άγνωστη για το χρήστη τοποθεσία – κάτι που ειδικά για τις επιχειρήσεις μπορεί να σταθεί ως ισχυρό εμπόδιο για τη χρήση της τεχνολογίας, αφού θεωρητικά θα μπορούσε κάποιος να αποκτήσει πρόσβαση σε εμπιστευτικές εταιρικές πληροφορίες[44].

Επιπλέον, οι χρήστες, ιδιώτες, επιχειρήσεις ή οργανισμοί, πρέπει να αποδεχθούν το γεγονός ότι ο έλεγχος χάνεται όταν τη διαχείριση δεδομένων και υποδομών έχει κάποιος τρίτος. Μια βλάβη σε ένα υπολογιστικό σύστημα (ίσως στην άλλη άκρη του κόσμου) θα μπορούσε να προκαλέσει σοβαρές δυσλειτουργίες σε μια εταιρεία που βασίζει τη δραστηριότητά της σε online υπηρεσίες υπολογιστικού νέφους. Και στην περίπτωση αυτή κανείς υπάλληλος της εταιρείας δε θα μπορούσε να διορθώσει τη βλάβη αυτή[45].

Το κόστος, που αναφέρθηκε νωρίτερα ως πλεονέκτημα, μπορεί να εξελιχθεί και σε μειονέκτημα. Με την επένδυση στην τεχνολογία του υπολογιστικού νέφους διασφαλίζεται υψηλότερη αποδοτικότητα σε σχέση με άλλες τεχνολογίες, ωστόσο το κόστος συχνά παραμένει υψηλό (είτε γιατί η τεχνολογία αυτή από μόνη της αξίζει αρκετά, είτε γιατί ο προγενέστερος εξοπλισμός δεν είναι απόλυτα συμβατός και απαιτείται αντικατάσταση / αναβάθμισή του)[46].

«Η ευρωπαϊκή πρωτοβουλία για το υπολογιστικό νέφος»

Στις 19 Απριλίου 2016 η **Ευρωπαϊκή Επιτροπή** παρουσίασε το σχέδιό της για υπηρεσίες βασιζόμενες στο υπολογιστικό νέφος και για υποδομή δεδομένων παγκόσμιας

---

[44] Carlin, S., & Curran, K. (2011). *Cloud computing security*. Στο Pervasive and Ubiquitous Technology Innovations for Ambient Intelligence Environments, pp. 14-15

[45] Armbrust, M. et al., (2010). *A view of cloud computing*. Στο Communications of the ACM, 53(4), pp. 50-58, διαθέσιμο εδώ: http://cacm.acm.org/magazines/2010/4/81493-a-view-of-cloud-computing/fulltext

[46] Armbrust, M., et al., (2009). *Above the clouds: A berkeley view of cloud computing*, pp. 12-14, διαθέσιμο εδώ: https://www2.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf

εμβέλειας με σκοπό να διασφαλιστεί ότι η επιστήμη, οι επιχειρήσεις και οι δημόσιες υπηρεσίες επωφελούνται από την επανάσταση των μαζικών δεδομένων.

Σύμφωνα με τη σχετική ανακοίνωση[47], *«η Ευρώπη είναι ο μεγαλύτερος παραγωγός επιστημονικών δεδομένων στον κόσμο, αλλά λόγω των ανεπαρκών και κατακερματισμένων υποδομών αυτά τα "μαζικά δεδομένα" δεν αξιοποιούνται πλήρως. Με την ενίσχυση και τη διασύνδεση των υφιστάμενων ερευνητικών υποδομών, η Επιτροπή προτίθεται να δημιουργήσει ένα νέο Ευρωπαϊκό Νέφος Ανοικτής Επιστήμης το οποίο θα παράσχει σε 1,7 εκατ. ερευνητές και 70 εκατ. επαγγελματίες στους τομείς των επιστημών και της τεχνολογίας στην Ευρώπη ένα εικονικό περιβάλλον για την αποθήκευση, την κοινοποίηση και την επαναχρησιμοποίηση των δεδομένων σε διεπιστημονικό και διασυνοριακό επίπεδο. Αυτό θα βασίζεται στην ευρωπαϊκή υποδομή δεδομένων, που διαθέτει δίκτυα υψηλής ευρυζωνικότητας, χώρους αποθήκευσης μεγάλης κλίμακας και συστήματα υπερυπολογιστών αναγκαία για την αποτελεσματική πρόσβαση και επεξεργασία μεγάλων συνόλων δεδομένων αποθηκευμένων στο υπολογιστικό νέφος. Αυτή η παγκόσμιας εμβέλειας υποδομή θα διασφαλίσει τη συμμετοχή της Ευρώπης στον παγκόσμιο αγώνα δρόμου για πληροφορική υψηλών επιδόσεων, σύμφωνα με τις οικονομικές δυνατότητες και το δυναμικό γνώσεων που διαθέτει»*.

Σύμφωνα με τον επίτροπο Έρευνας, Επιστήμης και Καινοτομίας Κάρλος Μοέδας, στόχος είναι η δημιουργία ενός «Ευρωπαϊκού Νέφους Ανοικτής Επιστήμης» ώστε να γίνει η επιστήμη πιο αποτελεσματική και παραγωγική και να διευκολυνθούν *«εκατομμύρια επιστήμονες στην ανταλλαγή και την ανάλυση των δεδομένων της έρευνας σε αξιόπιστο περιβάλλον χωρίς περιορισμούς όσον αφορά την τεχνολογία, τους επιστημονικούς κλάδους και τα σύνορα»*.

Σύμφωνα δε με τον επίτροπο Ψηφιακής Οικονομίας και Κοινωνίας Γκίντερ Έτινγκερ *«η ευρωπαϊκή πρωτοβουλία για το υπολογιστικό νέφος θα αξιοποιήσει τα μαζικά δεδομένα παρέχοντας υπερυπολογιστές παγκόσμιας κλάσης, συνδεσιμότητα υψηλής ταχύτητας και υπηρεσίες αιχμής όσον αφορά δεδομένα και λογισμικό για την επιστήμη, τη βιομηχανία και τον δημόσιο τομέα»*.

[47] «Η ευρωπαϊκή πρωτοβουλία για το υπολογιστικό νέφος θα δώσει στην Ευρώπη το παγκόσμιο προβάδισμα στη βασιζόμενη στα δεδομένα οικονομία», διαθέσιμο εδώ: http://europa.eu/rapid/press-release_IP-16-1408_el.htm

Η Ευρωπαϊκή Επιτροπή, σύμφωνα πάντα με την ανακοίνωση[48], θα θέσει σταδιακά σε εφαρμογή την ευρωπαϊκή πρωτοβουλία για το υπολογιστικό νέφος μέσω μιας σειράς δράσεων, όπως:

- ***Από το 2016:*** *τη δημιουργία ενός Ευρωπαϊκού Νέφους Ανοικτής Επιστήμης για τους Ευρωπαίους ερευνητές και τους επιστημονικούς συνεργάτες τους σε όλον τον κόσμο με την ενσωμάτωση και ενοποίηση πλατφορμών ηλεκτρονικών υποδομών, τη συγκέντρωση των υφιστάμενων επιστημονικών υπολογιστικών νεφών και των υποδομών έρευνας και τη στήριξη της ανάπτυξης υπηρεσιών βασιζόμενων στο υπολογιστικό νέφος.*
- ***2017:*** *το άνοιγμα εξ ορισμού όλων των επιστημονικών δεδομένων που θα παράγονται στο πλαίσιο μελλοντικών έργων του προγράμματος έρευνας και καινοτομίας «Ορίζοντας 2020» ύψους 77 δισ. ευρώ, ώστε να διασφαλίζεται ότι η επιστημονική κοινότητα θα μπορεί να επαναχρησιμοποιεί τον τεράστιο όγκο δεδομένων που παράγει.*
- ***2018:*** *την έναρξη μιας εμβληματικής πρωτοβουλίας για την επιτάχυνση της εκκολαπτόμενης ανάπτυξης της κβαντικής τεχνολογίας, η οποία αποτελεί τη βάση της επόμενης γενιάς υπερυπολογιστών.*
- ***Μέχρι το 2020:*** *ανάπτυξη και αξιοποίηση ευρωπαϊκών υποδομών μεγάλης κλίμακας για υψηλών επιδόσεων πληροφορική, αποθήκευση δεδομένων και δίκτυα, μέσω, μεταξύ άλλων, της απόκτησης δύο πρωτοτύπων υπερυπολογιστών επόμενης γενιάς, εκ των οποίων ο ένας θα συγκαταλέγεται μεταξύ των τριών καλύτερων στον κόσμο, της δημιουργίας ενός ευρωπαϊκού κέντρου μαζικών δεδομένων, και της αναβάθμισης του κεντρικού δικτύου για την έρευνα και την καινοτομία (GEANT).*

Τέλος, εκτός από την ευρωπαϊκή ερευνητική κοινότητα, στο **Ευρωπαϊκό Νέφος Ανοικτής Επιστήμης** και στην ευρωπαϊκή υποδομή δεδομένων θα έχουν πρόσβαση και θα αποκομίζουν οφέλη πολλοί άλλοι χρήστες:

- *Οι **επιχειρήσεις** θα έχουν οικονομικά προσιτή και εύκολη πρόσβαση σε δεδομένα και υποδομές πληροφορικής υψηλού επιπέδου, καθώς και σε πληθώρα επιστημονικών δεδομένων που καθιστούν δυνατή την καινοτομία που βασίζεται στα δεδομένα. Αυτό*

[48] http://europa.eu/rapid/press-release_IP-16-1408_el.htm

θα ωφελήσει κυρίως τις ΜΜΕ, οι οποίες συνήθως δεν έχουν πρόσβαση σε τέτοιους πόρους.

- *Η **βιομηχανία** θα αποκομίσει οφέλη από τη δημιουργία ενός οικοσυστήματος υπολογιστικού νέφους μεγάλης κλίμακας, που υποστηρίζει την ανάπτυξη νέων ευρωπαϊκών τεχνολογιών όπως μικροκυκλωμάτων (chip) χαμηλής κατανάλωσης για υπολογιστές υψηλών επιδόσεων.*
- *Οι **δημόσιες υπηρεσίες** θα επωφεληθούν από την αξιόπιστη πρόσβαση σε ισχυρούς υπολογιστικούς πόρους και τη δημιουργία μιας πλατφόρμας για το άνοιγμα των δεδομένων και των υπηρεσιών τους, πράγμα που μπορεί να οδηγήσει σε φθηνότερες, ταχύτερες και καλύτερα διασυνδεδεμένες δημόσιες υπηρεσίες. Οι ερευνητές θα επωφεληθούν επίσης από τη διαδικτυακή πρόσβαση στον πλούτο των δεδομένων που προκύπτουν από τις δημόσιες υπηρεσίες.*

❑

Κεφάλαιο 3: Τεχνικές προκλήσεις εγκληματολογικής ανάλυσης σε περιβάλλον υπολογιστικού νέφους

Στο παρόν κεφάλαιο θα εξετάσουμε τις τεχνικής φύσεως προκλήσεις που συνδέονται με το υπολογιστικό νέφος σε ότι αφορά τα υπάρχοντα στάδια εξέτασης ψηφιακών πειστηρίων που περιγράψαμε νωρίτερα. Η ανάλυσή μας βασίζεται στο απλουστευμένο μοντέλο εξέτασης των τεσσάρων σταδίων που παρουσιάστηκε στο Κεφάλαιο 1, δηλαδή συλλογή, εξέταση, ανάλυση και παρουσίαση, αλλά και στις αρχές και οδηγίες της ACPO. Το μοντέλο αυτό εξυπηρετεί το σκοπό της παρούσας ανάλυσης, καθώς μας βοηθά να κατανοήσουμε τόσο τα στάδια της εγκληματολογικής εξέτασης, όσο και την επίδραση της τεχνολογίας του υπολογιστικού νέφους σε αυτά.

Συλλογή

Το πρώτο στάδιο του μοντέλου περιλαμβάνει αρχικά τη διαπίστωση ότι μια πιθανολογούμενη εγκληματική πράξη σχετίζεται με Τεχνολογίες Πληροφοριών και Επικοινωνιών (ΤΠΕ). Τα γεγονότα αυτά μπορεί να αφορούν παραδοσιακά εγκλήματα ή δραστηριότητες που περιλαμβάνουν τη χρήση των ΤΠΕ, ή άλλα, που χωρίς την ύπαρξη ενός υπολογιστικού συστήματος δε θα μπορούσαν να τελεστούν. Η διαπίστωση μπορεί να προέλθει από καταγγελία ενός μεμονωμένου ατόμου για μια παράνομη πράξη που τελέστηκε σε βάρος του, από μη φυσιολογικές λειτουργίες που εντοπίζονται από ένα **σύστημα αναγνώρισης εισβολής** (Intrusion Detection System – IDS) που είναι εγκατεστημένο σε ένα υπολογιστικό σύστημα (και που τις διαπιστώνει κάποιος υπεύθυνος ασφαλείας)[49] ή κάποιας άλλης έρευνας που διενεργείται «αυτεπάγγελτα» από τις Αρχές Επιβολής του Νόμου. Παρά το γεγονός ότι η διαδικασία αναγνώρισης δε συνδέεται άμεσα με τα ψηφιακά πειστήρια, έχει επίδραση στην εξέλιξη και στον τρόπο διενέργειας της έρευνας, καθώς επίσης και στον προσδιορισμό του σκοπού αυτής.

Ο εντοπισμός ύποπτων συμβάντων στο υπολογιστικό νέφος εξαρτάται από το μοντέλο ανάπτυξης που έχει χρησιμοποιηθεί και τη μορφή των υπηρεσιών (δηλαδή αν

[49] Το IDS είναι κάτι ευρύτερο από ένα λογισμικό antivirus. Εκτενές κείμενο για το εν λόγω είδος συστημάτων έχει εκδοθεί από το NIST με τίτλο «Guide to Intrusion Detection and Prevention Systems (IDPS)» και είναι διαθέσιμο εδώ http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf (έκδοση του 2007) και εδώ http://csrc.nist.gov/publications/drafts/800-94-rev1/draft_sp800-94-rev1.pdf (αναθεωρημένη έκδοση draft του 2012).

πρόκειται για SaaS, Paas ή IaaS). Η χρησιμοποίηση συμβατικών συστημάτων IDS στο cloud έχει μελετηθεί και προταθεί από διάφορους ερευνητές[50]. Τέτοιου είδους συστήματα μπορούν να χρησιμοποιηθούν από χρήστες στα cloud IaaS, ή από παρόχους στα cloud SaaS και PaaS. Σε μια ιδιωτική cloud υποδομή, οι πάροχοι μπορούν να προσαρμόσουν καλύτερα τα συστήματα IDS, ώστε να ανταποκρίνονται στις ανάγκες ενός οργανισμού ή μιας επιχείρησης. Για τα δημόσια cloud, από την άλλη πλευρά, ενδέχεται να απαιτείται στρατηγική πολλαπλών επιπέδων. Οι **χρήστες** μπορούν να καταγράφουν τα ύποπτα περιστατικά στις υπηρεσίες που χρησιμοποιούν. Οι **πάροχοι**, τέλος, μπορούν να παρακολουθούν την υποδομή που έχουν στη διάθεσή τους για τη φιλοξενία του cloud και έτσι να εντοπίσουν επιθέσεις πολύ μεγαλύτερης κλίμακας που επηρεάζουν περισσότερους τελικούς χρήστες[51].

Διατήρηση

Με βάση τις διεθνείς πρακτικές και αρχές που εφαρμόζονται στην ψηφιακή εγκληματολογία, τα δεδομένα των πειστηρίων θα πρέπει να παραμείνουν **αναλλοίωτα** μέχρι την εξέταση και ανάλυσή τους, ενώ οι μέθοδοι που χρησιμοποιούνται για την παραγωγή των πειστηρίων θα πρέπει να μπορούν να επαναληφθούν – και προφανώς να δώσουν τα ίδια «αποτελέσματα». Με άλλα λόγια, θα πρέπει να διασφαλισθεί ότι το προς εξέταση πειστήριο περιέχει μια **ακριβή αναπαράσταση** των δεδομένων που βρέθηκαν στο υπολογιστικό σύστημα. Πολλά στοιχεία του σταδίου της διατήρησης επηρεάζονται από τη χρήση του περιβάλλοντος υπολογιστικού νέφους[52].

Δυνατότητες αποθήκευσης

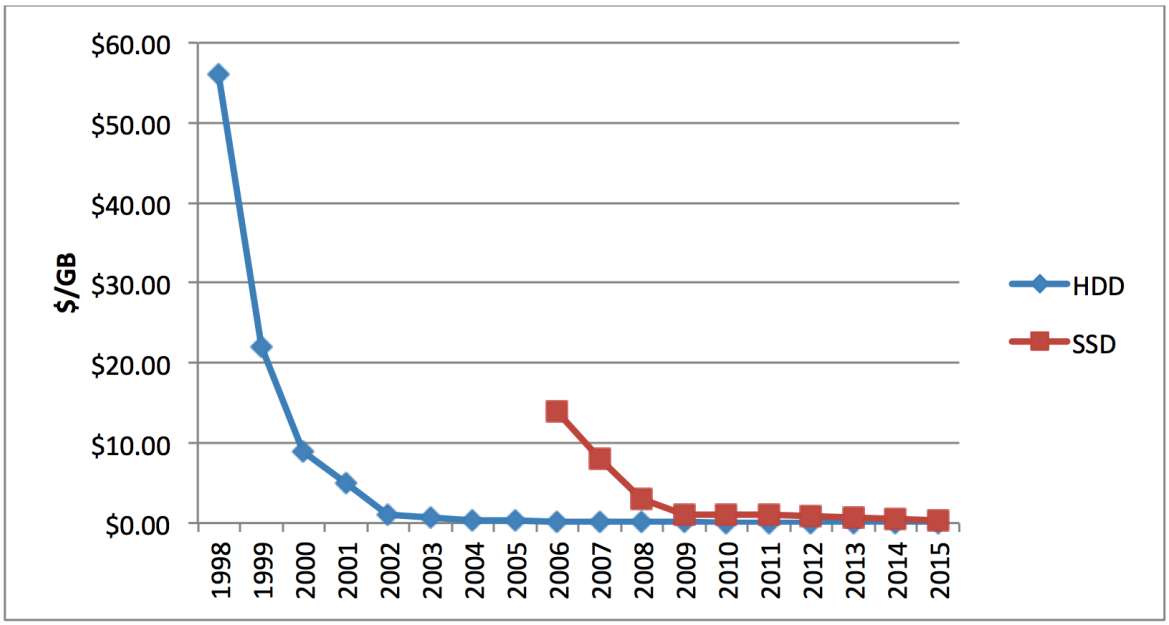
Στις συνηθισμένες έρευνες, προϋπόθεση για τη διατήρηση ηλεκτρονικών ιχνών είναι η ύπαρξη επαρκούς χώρου (ψηφιακής) αποθήκευσης για τα προς συλλογή δεδομένα. Παράλληλα, ωστόσο, παρατηρείται **μείωση του αποθηκευτικού κόστους**: διαρκώς

[50] Roschke, S., Cheng, F., & Meinel, C. (2009*). Intrusion detection in the cloud*. Στο Dependable, Autonomic and Secure Computing, 2009. DASC'09. Eighth IEEE International Conference on (pp. 729-734). IEEE, διαθέσιμο εδώ: http://ieeexplore.ieee.org/document/5380611/

[51] Dhage, S. N., & Meshram, B. B. (2012). *Intrusion detection system in cloud computing environment*. Στο International Journal of Cloud Computing, 1(2-3), 261-282

[52] Quick, D., & Choo, K. K. R. (2013). *Forensic collection of cloud storage data: Does the act of collection result in changes to the data or its metadata?*. Στο Digital Investigation, 10(3), 266-277, διαθέσιμο εδώ: http://www.sciencedirect.com/science/article/pii/S1742287613000741

αυξανόμενος όγκος αποθήκευσης προσφέρεται σε διαρκώς χαμηλότερες τιμές. Ενδεικτική είναι η απεικόνιση που ακολουθεί, όπου μπορούμε να δούμε την πτωτική πορεία του κόστους για την αποθήκευσης ενός GB (δολάρια ανά GB).



Γράφημα 2 Κόστος αποθήκευσης σε σκληρούς δίσκους HDD και SSD[53]

Έτσι, ο κάθε χρήστης μπορεί να έχει στη διάθεσή του, με πολύ χαμηλό κόστος, τεράστιο χώρο για να αποθηκεύει τα δεδομένα του, κάτι που για τον ερευνητή ενός εγκλήματος είναι τεράστιο πρόβλημα. Ο ερευνητής θα πρέπει αφενός να μεριμνήσει για την ασφαλή ψηφιακή διατήρηση των δεδομένων (και να έχει την ευθύνη φύλαξης αυτών) και αφετέρου να δαπανήσει πολύ περισσότερο (πολύτιμο) χρόνο για να ολοκληρώσει την εξέταση ενός αποθηκευτικού μέσου.

Στο περιβάλλον του υπολογιστικού νέφους, το πρόβλημα του **τεράστιου όγκου δεδομένων**, που είναι αποθηκευμένα σε αυτό, είναι σαφώς μεγαλύτερο. Οι χρήστες, βέβαια, βρίσκουν ελκυστικές τις υπηρεσίες αποθήκευσης στο υπολογιστικό νέφος κυρίως λόγω της «ελαστικότητάς» τους, με βάση τις απαιτήσεις τους. Από την πλευρά του χρήστη, μια τυπική δημόσια υποδομή υπολογιστικού νέφους IaaS φαίνεται να προσφέρει **«απεριόριστο»** αποθηκευτικό χώρο. Ο ερευνητής, από την άλλη πλευρά, είναι πολύ

[53] Προέλευση γραφήματος: http://www.eetimes.com/author.asp?doc_id=1327903

πιθανό να υποχρεωθεί να συλλέξει ένα εξαιρετικά μεγάλο όγκο ψηφιακών δεδομένων που έχει τοποθετήσει στο υπολογιστικό νέφος ο χρήστης[54].

Για τους εκπροσώπους των Αρχών Επιβολής του Νόμου μια λύση στο προαναφερθέν πρόβλημα θα μπορούσε να αποτελεί η χρησιμοποίηση δημοσίου υπολογιστικού νέφους για την αποθήκευση αντιγράφων πειστηρίων, κάτι που αναπόφευκτα συνεπάγεται νέες προκλήσεις, τόσο από νομικής όσο και από τεχνικής πλευράς. Στη συγκεκριμένη περίπτωση, είναι κρίσιμη η συμμόρφωση με την ισχύουσα νομοθεσία περί προσωπικών δεδομένων και ιδιωτικότητας[55].

Έχει προταθεί, εξάλλου, η υιοθέτηση της τεχνικής **«triage»**, που μπορούμε να αποδώσουμε με τον όρο «διαλογή», ως ένας τρόπος για τη μείωση του όγκου των δεδομένων που συλλέγονται και που απαιτείται να αναλυθούν από έναν ερευνητή. Αυτή η προσέγγιση πιθανώς είναι η καταλληλότερη σε περιπτώσεις όπου απαιτείται άμεση αντίδραση, όταν οι ερευνητές δεν ενδιαφέρονται για την μακροπρόθεσμη ακεραιότητα και αξιοπιστία του ψηφιακού πειστηρίου. Με τον τρόπο αυτό, οι ερευνητές μπορούν να διενεργήσουν γρήγορα εξετάσεις αποθηκευτικών μέσων σε σύντομο χρονικό διάστημα, ώστε να εντοπίσουν τα πολυτιμότερα στοιχεία, χωρίς να πραγματοποιήσουν μια ολοκληρωμένη εγκληματολογική εξέταση, και έτσι να τα χρησιμοποιήσουν για τη συνέχιση των ερευνών ή αναζητήσεών τους στο φυσικό κόσμο.

Για την εφαρμογή της «διαλογής» (triage) σε ένα ψηφιακό πειστήριο προτάθηκε και εφαρμόζεται το μοντέλο **Computer Forensics Field Triage Process Model** (CFFTPM). Το μοντέλο λειτουργεί αποκτώντας πρόσβαση στα δεδομένα που βρίσκονται στον κατάλογο «home» του συστήματος του χρήστη. Σε αυτό τον κατάλογο εντοπίζονται πληροφορίες σχετικές με τις τρέχουσες εφαρμογές που εκτελούνται από το χρήστη. Δεδομένα, όμως, συλλέγονται και από άλλες πηγές, όπως τη registry, το λειτουργικό

[54] Simou, S., Kalloniatis, C., Kavakli, E., & Gritzalis, S. (2014, June). *Cloud forensics: identifying the major issues and challenges*. Στο International Conference on Advanced Information Systems Engineering (pp. 271-284). Springer International Publishing

[55] Taylor, M., Haggerty, J., Gresty, D., & Lamb, D. (2011). Forensic investigation of cloud computing systems. Network Security, 2011(3), 4-10

σύστημα και τα αρχεία καταγραφής των εφαρμογών. Οι πληροφορίες που εμπεριέχονται στις παραπάνω τοποθεσίες συνοδεύονται (συνήθως) από χρονοσφραγίδες (timestamps)[56].

Στο περιβάλλον, ωστόσο, του υπολογιστικού νέφους, το CFFTPM δύσκολα μπορεί να εφαρμοσθεί απευθείας εκεί, αφού τα δεδομένα που σχετίζονται με τις εφαρμογές που εκτελεί ο χρήστης μπορεί να αποθηκεύονται είτε στο υπολογιστικό νέφος, είτε στην προσωρινή μνήμη του υπολογιστή, είτε και στα δύο. Αν ο ερευνητής αποφασίσει να ακολουθήσει την προσέγγιση «διαλογής», τότε πιθανότατα θα απαιτηθεί και η διενέργεια live εξέτασης των δεδομένων στο περιβάλλον του υπολογιστικού νέφους, όσο ο client – πελάτης είναι ακόμα συνδεδεμένος στο cloud[57]. Το κατά πόσο είναι εύκολο να γίνει αυτό θα το δούμε στη συνέχεια.

Αλληλουχία των βημάτων της έρευνας (Chain of custody)

Κατά τη διάρκεια μιας συνηθισμένης εγκληματολογικής εξέτασης, όπως έχει ήδη αναφερθεί και σε προηγούμενο κεφάλαιο, η αποδεκτή πρακτική είναι η διασφάλιση των αποδείξεων ως προς την αλληλουχία των βημάτων της έρευνας. Το «chain of custody» έχει ορισθεί ως ένα πλάνο που δείχνει πως τα πειστήρια συλλέχθηκαν, αναλύθηκαν και διατηρήθηκαν, ώστε να παρουσιαστούν ως αποδεικτικά στοιχεία στο δικαστήριο. Ο «κύκλος ζωής» ενός πειστηρίου καταγράφεται στο ιστορικό καταγραφών του ερευνητή[58]. Με βάση τις οδηγίες και αρχές της ACPO[59], η καταγραφή θα πρέπει να περιλαμβάνει επακριβώς τον τόπο, το χρόνο και τον τρόπο συλλογής των πειστηρίων, καθώς και κάθε άλλη ενέργεια που αφορά την εξέτασή τους, καθώς και τη διατήρηση και φύλαξή τους.

Σε μια συμβατική έρευνα, η αλληλουχία ξεκινάει όταν ο ερευνητής θεωρεί ότι έχει αποκτήσει το φυσικό έλεγχο του ψηφιακού πειστηρίου που σχετίζεται με την υπό έρευνα υπόθεση. Στη συνέχεια, υπάρχουν δύο επιλογές για τη διατήρηση δεδομένων ενός

[56] Rogers, M. K., Goldman, J., Mislan, R., Wedge, T., & Debrota, S. (2006, January). *Computer forensics field triage process model*. Στο Proceedings of the conference on Digital Forensics, Security and Law (p. 27). Association of Digital Forensics, Security and Law.

[57] Povar, D., Saibharath, & Geethakumari, G. (2015). *Real-time digital forensic triaging for cloud data analysis using MapReduce on Hadoop framework*. Στο International Journal of Electronic Security and Digital Forensics, 7(2), 119-133

[58] Ćosić, J., & Bača, M. (2010, January). *(Im) proving chain of custody and digital evidence integrity with time stamp*. Στο MIPRO–Proceedings of the 33rd International Convention (pp. 1226-1230)

[59] Βλ. Κεφάλαιο 1

υπολογιστικού συστήματος: είτε απενεργοποίηση του υπολογιστή δίνοντας την ανάλογη εντολή στο λειτουργικό σύστημα, ώστε να προκληθεί σταδιακή διακοπή λειτουργίας, είτε αφαίρεση της πηγής τροφοδοσίας, ώστε να προκληθεί άμεσο πάγωμα. Έτσι, οι συσκευές όπου βρίσκονται αποθηκευμένα τα δεδομένα μπορούν να αφαιρεθούν από το υπόλοιπο σύστημα και να εξετασθούν χωριστά. Στο ιστορικό καταγραφής θα γίνει κανονικά αναφορά στις συσκευές αυτές, που μπορούν να απομονωθούν και να αποσυνδεθούν από την παροχή ρεύματος με μικρό κίνδυνο απώλειας αποδείξεων[60].

Η απομακρυσμένη φύση των υπηρεσιών υπολογιστικού νέφους σημαίνει ότι δε μπορεί να γίνει κάτι αντίστοιχο στο περιβάλλον cloud. Οι υπηρεσίες μπορούν να προσπελαστούν από οποιοδήποτε σύστημα που διαθέτει δικτυακή σύνδεση στον πάροχο φιλοξενίας του cloud. Αν ο ερευνητής δεν καταφέρει να αποκτήσει πρόσβαση στην υπηρεσία και να την απενεργοποιήσει, τότε τα πειστήρια θα μπορούσαν να καταστραφούν σχετικά γρήγορα, είτε από ένα χρήση της υπηρεσίας, είτε από τον πάροχο των υπηρεσιών υπολογιστικού νέφους. Όλα εξαρτώνται από την ταχύτητα με την οποία ο ερευνητής μπορεί να αποκτήσει τον έλεγχο επί της υπηρεσίας, αλλά κυρίως από το νομικό πλαίσιο που θα του δίνει αυτή τη δυνατότητα[61].

Απόκτηση - δημιουργία ψηφιακού αντιγράφου (digital image acquisition)

Δεχόμενοι ότι ο ερευνητής έχει αποκτήσει τον έλεγχο της υπηρεσίας υπολογιστικού νέφους, είναι αναγκαίο να δημιουργήσει ένα ακριβές αντίγραφο των δεδομένων που τηρούνται στη συσκευή, για περαιτέρω ανάλυση σε μεταγενέστερο χρόνο. Με βάση τη διεθνή πρακτική, επιβάλλεται η χρήση του «**forensic imaging**»[62] για να αποκτήσει ο ερευνητής αντίγραφα των περιεχομένων της συσκευής αποθήκευσης, χωρίς να τροποποιηθούν τα αρχικά περιεχόμενά της. Συνήθως η συσκευή αποθήκευσης συνδέεται στον υπολογιστή του ερευνητή, μέσω λογισμικού ή υλικού **write-blocker**. Με

---

[60] ACPO, Good Practice Guide for Computer-Based Electronic Evidence, διαθέσιμο εδώ: https://www.cps.gov.uk/legal/assets/uploads/files/ACPO_guidelines_computer_evidence[1].pdf

[61] Birk, D., & Wegener, C. (2011). *Technical issues of forensic investigations in cloud computing environments*. Στο Systematic Approaches to Digital Forensic Engineering (SADFE), 2011 IEEE Sixth International Workshop on (pp. 1-10). IEEE.

[62] Δηλαδή ένα ακριβές αντίγραφο της κατάστασης της συσκευής αποθήκευσης κατά τη στιγμή του εντοπισμού της.

τη χρήση κατάλληλου λογισμικού (γνωστά είναι το FTK Imager[63]) ή την εντολή dd σε λειτουργικά συστήματα ανοιχτού κώδικα[64], γίνεται αντιγραφή byte προς byte ολόκληρης της συσκευής.

Η συλλογή πειστηρίων από ένα περιβάλλον cloud είναι βέβαιο ότι αποτελεί μια πρόκληση για τον ερευνητή. Τα εργαλεία «διαλογής» και το λογισμικό που χρησιμοποιείται για την ανάκτηση της προσωρινής μνήμης, σε αντίθεση με ότι συμβαίνει στις συμβατικές έρευνες, μπορούν σε περιβάλλον υπολογιστικού νέφους να συλλέξουν ελάχιστα δεδομένα από έναν υπολογιστή πελάτη (client).

Η εικονικοποίηση (virtualization)[65] των χώρων αποθήκευσης στο υπολογιστικό νέφος καθιστά ιδιαίτερα πολύπλοκη την αναγνώριση και απομόνωση των τμημάτων εκείνων, της μιας ή περισσοτέρων φυσικών αποθηκευτικών συσκευών που κατέχει και διαχειρίζεται ο πάροχος των υπηρεσιών υπολογιστικού νέφους, όπου εμπεριέχονται τα δεδομένα του χρήστη που πρέπει να συλλεχθούν προς ανάλυση. Με άλλα λόγια, τα virtualized δεδομένα, που είναι αποθηκευμένα στο υπολογιστικό νέφος, μπορεί να κατανεμηθούν ανάμεσα σε πολλές διαφορετικές φυσικές συσκευές, ενώ θα μπορούσε να χρησιμοποιείται και διαπροσωπεία (interface) ανάμεσα στον εικονικό χώρο αποθήκευσης και στον ερευνητή[66]. Στην πράξη, η Google χρησιμοποιούσε παλαιότερα το Google File System (GFS), για την αποθήκευση των δεδομένων των πελατών της στο υπολογιστικό νέφος.[67] Ο πελάτης – τελικός χρήστης αντιλαμβάνεται ότι τα δεδομένα του βρίσκονται αποθηκευμένα σε μια μόνο τοποθεσία. Στο φυσικό κόσμο, βέβαια, δεν είναι έτσι. Δύο χρήστες μπορεί να βρίσκονται εντός του ίδιου οργανισμού, αλλά τα δεδομένα τους θα μπορούσαν να έχουν κατανεμηθεί σε δύο ή περισσότερες φυσικές τοποθεσίες. Τα παραπάνω γίνονται καλύτερα κατανοητά στην ακόλουθη απεικόνιση *(Εικόνα 1)*, όπου

[63] http://accessdata.com/solutions/digital-forensics/forensic-toolkit-ftk

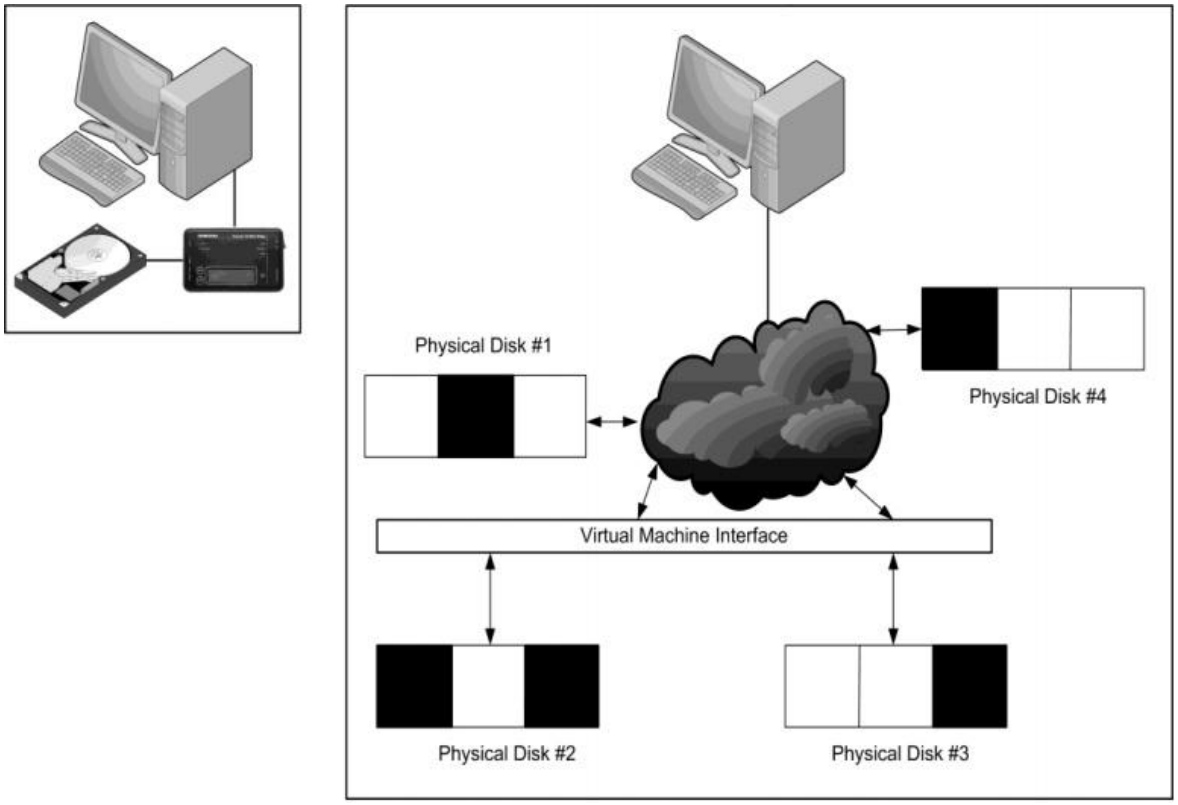
[64] http://pubs.opengroup.org/onlinepubs/9699919799/utilities/dd.html

[65] https://en.wikipedia.org/wiki/Virtualization

[66] Zargari, S., & Benford, D. (2012). Cloud forensics: Concepts, issues, and challenges. In Emerging Intelligent Data and Web Technologies (EIDWT), 2012 Third International Conference on (pp. 236-243). IEEE

[67] Ghemawat, S., Gobioff, H., & Leung, S. T. (2003). The Google file system. In ACM SIGOPS operating systems review (Vol. 37, No. 5, pp. 29-43). ACM

φαίνεται αριστερά η συλλογή δεδομένων κατά τη διάρκεια μιας συμβατικής έρευνας, και στα δεξιά η συλλογή δεδομένων από ένα περιβάλλον υπολογιστικού νέφους[68]:



Εικόνα 1 Η θέση των δεδομένων κατά τη διάρκεια μιας συμβατικής έρευνας (αριστερά) και μιας έρευνας στο υπολογιστικό νέφος (δεξιά)

Με βάση τις οδηγίες της ACPO, θα πρέπει ο ερευνητής να συλλέξει ολόκληρη τη συσκευή που περιέχει τις σχετικές πληροφορίες για το περιστατικό. Μια τέτοια ενέργεια, δηλαδή η συλλογή (κατάσχεση) ολόκληρων των συσκευών ενός περιβάλλοντος υπολογιστικού νέφους αποτελεί πρόβλημα όχι μόνο από τη σκοπιά του ερευνητή, που πρέπει να δαπανήσει πόρους και πολύτιμο χρόνο, αλλά και από τη σκοπιά του παρόχου των υπηρεσιών. Τεράστια, βέβαια, θα μπορούσε να είναι και η ποσότητα των δεδομένων που θα συλλέξει ο ερευνητής, με το μεγαλύτερο μέρος αυτών να είναι άσχετα με το περιστατικό. Στην πράξη, οι υπηρεσίες υπολογιστικού νέφους προσφέρουν απομακρυσμένη πρόσβαση σε μια λογική αναπαράσταση δεδομένων, που μπορεί να είναι εντελώς διαφορετική από την φυσική κατανομή των δεδομένων στον πραγματικό κόσμο. Η κατάσταση περιπλέκεται ακόμα περισσότερο όταν ο πάροχος των υπηρεσιών

[68] Grispos, G., Storer, T., & Glisson, W. B. (2013). *Calm before the storm: the challenges of cloud*. Στο Emerging digital forensics applications for crime detection, prevention, and security, 4, 28-48.

υπολογιστικού νέφους χρησιμοποιεί εικονικοποιημένη (virtualized) υποδομή ενός τρίτου παρόχου υπηρεσιών υπολογιστικού νέφους κ.ο.κ.[69].

Η χρήση του virtualization επηρεάζει, εξάλλου, την ιδιωτικότητα των άλλων χρηστών του υπολογιστικού νέφους, των οποίων τα δεδομένα μπορεί απροειδοποίητα να συλλεχθούν κατά τη διάρκεια μιας έρευνας για ένα περιστατικό. Σε ορισμένες περιοχές, η χωρίς εξουσιοδότηση πρόσβαση σε δεδομένα που δεν είναι σχετικά με την υπόθεση σε ένα περιβάλλον υπολογιστικού νέφους μπορεί να έχει νομικές συνέπειες (λόγω της ισχύουσας νομοθεσίας για τα προσωπικά δεδομένα και την ιδιωτικότητα)[70].

Μέχρι τώρα θεωρήσαμε ότι ο ερευνητής ενεργεί έχοντας μπροστά του μια **«νεκρή συσκευή»**, την οποία έχει απομονώσει και της οποίας έχει τον έλεγχο. Συχνά, ωστόσο, τα δεδομένα που χρησιμοποιούνται μπορεί να αποθηκεύονται στην volatile μνήμη στο υπολογιστικό νέφος, ή να βρίσκονται στην κρυφή μνήμη (cache) του υπολογιστή του χρήστη, όσο αυτός αλληλεπιδρά με τις υπηρεσίες υπολογιστικού νέφους. Η ζωντανή συλλογή[71] και έρευνα αποτελούν μια εναλλακτική προσέγγιση, κατά τη διάρκεια της οποίας τα δεδομένα εξετάζονται στον υπολογιστή στόχο όσο αυτός είναι ακόμα σε λειτουργία. Η εν λόγω προσέγγιση επιτρέπει στους ερευνητές να συλλέξουν δεδομένα που αλλιώς μπορεί να χανόταν αν ο υπολογιστής είχε απενεργοποιηθεί. Ιδιαίτερα:

- δεδομένα που αποθηκεύονται σε μια μη-μόνιμη μνήμη, όπως διαδικασίες και πληροφορίες για ενεργές συνδέσεις δικτύου,
- προσωρινά δεδομένα αποθηκευμένα στη μόνιμη μνήμη, όπως κλειδώματα αρχείων εφαρμογών (application file locks) και αρχεία περιήγησης στον ιστό που βρίσκονται στην κρυφή μνήμη (cache).

Η χρήση των τεχνικών ζωντανής συλλογής μπορεί να αυξήσει την ποσότητα των πληροφοριών που ένας ερευνητής θα εξάγει από έναν υπολογιστή – πελάτη του υπολογιστικού νέφους, ειδικά αν υφίσταται ανοικτή σύνδεση προς το περιβάλλον

[69] Wolthusen, S. D. (2009, September). *Overcast: Forensic discovery in cloud environments*. Στο IT Security Incident Management and IT Forensics, 2009. IMF'09. Fifth International Conference on (pp. 3-9). IEEE.

[70] Chowdhury, N. M. K., & Boutaba, R. (2009). *Network virtualization: state of the art and research challenges*. IEEE Communications magazine, 47(7), 20-26

[71] Με τη λέξη «συλλογή» αποδίδουμε τον αγγλικό όρο «acquisition».

υπολογιστικού νέφους[72]. Ωστόσο, η συλλογή της ψηφιακής εικόνας[73] θα μπορούσε να παρεμποδιστεί περαιτέρω με τη χρήση της κρυπτογράφησης σε περιβάλλοντα υπολογιστικού νέφους. Αρκετοί οργανισμοί δείχνουν απροθυμία για την υιοθέτηση υπηρεσιών υπολογιστικού νέφους, έως ότου εξαλειφθούν οι ανησυχίες τους σχετικά με την εμπιστευτικότητα και την ακεραιότητα των δεδομένων. Έτσι, οι πάροχοι υπηρεσιών υπολογιστικού νέφους στρέφονται στην κρυπτογράφηση ως μέσο επίτευξης της επιζητούμενης από τους πελάτες ασφάλειας. Μάλιστα, αρκετοί πάροχοι υπηρεσιών υπολογιστικού νέφους εφαρμόζουν ένα σύστημα «μηδενικής γνώσης», δηλαδή η κρυπτογράφηση των δεδομένων γίνεται από τους πελάτες πριν διαβιβαστούν και αποθηκευθούν στις υποδομές του υπολογιστικού νέφους. Τα κλειδιά κρυπτογράφησης δεν αποθηκεύονται ποτέ στο υπολογιστικό νέφος[74]. Αυτό σημαίνει ότι το να δοθεί μια εισαγγελική παραγγελία σε ένα πάροχο υπηρεσιών υπολογιστικού νέφους, για να αποκρυπτογραφήσει τις πληροφορίες που φιλοξενεί, θα μπορούσε να μην έχει κανένα νόημα, αφού μόνο ο πελάτης – ιδιοκτήτης των δεδομένων μπορεί να παρέχει το κλειδί για να αποκρυπτογραφηθούν οι πληροφορίες αυτές. Αν το συγκεκριμένο σύστημα υιοθετηθεί ευρέως, ώστε να πειστούν οι πελάτες ότι τα δεδομένα τους είναι ασφαλή, τότε οι ερευνητές θα μπορούσαν να εντοπίζουν μεγάλο όγκο πειστηρίων, όμως αν αυτά είναι κρυπτογραφημένα, τότε δε θα έχουν καμία απολύτως εγκληματολογική αξία, παρά μόνο αν γίνει ανάκτηση των κλειδιών κρυπτογράφησης.

Δεδομένα που έχουν διαγραφεί

Το υπολογιστικό νέφος θα μπορούσε να βοηθήσει αλλά και να παρεμποδίσει τις προσπάθειες των ερευνητών να ανακτήσουν δεδομένα που έχουν διαγραφεί ή θα είχαν διαγραφεί από τον ύποπτο, σε αντίθεση με ένα σκληρό δίσκο ή μια μονάδα flash USB, στα οποία ένας ύποπτος έχει φυσική πρόσβαση και θα μπορούσε ως εκ τούτου να τα καταστρέψει. Στο υπολογιστικό νέφος δεν είναι το ίδιο. Τα δεδομένα αυτά θα παραμείνουν

[72] Delport, W., Köhn, M., & Olivier, M. S. (2011). *Isolating a cloud instance for a digital forensic investigation*. Στο ISSA.

[73] Ψηφιακή εικόνα = digital image

[74] Agudo, I., Nuñez, D., Giammatteo, G., Rizomiliotis, P., & Lambrinoudakis, C. (2011). *Cryptography goes to the cloud*. Στο FTRA International Conference on Secure and Trust Computing, Data Management, and Application (pp. 190-197). Springer Berlin Heidelberg

στη διάθεση του ερευνητή, εκτός εάν ο ύποπτος έχει τη γνώση και τη δυνατότητα να διαγράψει ή να αλλοιώσει δεδομένα[75].

Στις συμβατικές έρευνες, τα δεδομένα που ο χρήστης έχει προσπαθήσει να διαγράψει (αλλά που εξακολουθούν να παραμένουν αποθηκευμένα σε μια συσκευή αποθήκευσης) είναι συχνά μια αξιόλογη πηγή αποδεικτικών στοιχείων. Ωστόσο, σε περιβάλλον υπολογιστικού νέφους είναι εξαιρετικά δύσκολη η ανάκτηση τέτοιου είδους δεδομένων, λόγω της ευθραυστότητάς τους. Προφανώς οι πάροχοι υπηρεσιών cloud υποστηρίζουν σθεναρά το απόρρητο για τους πελάτες – χρήστες τους. Οι δείκτες προς αυτά τα δεδομένα διαγράφονται επίσης, καθιστώντας τον εντοπισμό τυχόν υπολειπόμενων δεδομένων του χρήστη εξαιρετικά δύσκολο.

Ζητήματα Συνεργασίας με Οργανισμούς

Εάν ο ερευνητής δεν μπορεί να αποκτήσει ο ίδιος τον έλεγχο μιας υπηρεσίας υπολογιστικού νέφους, ίσως μπορεί να αποκτήσει μια «φωτογραφία» των δεδομένων της υπηρεσίας, την οποία «φωτογραφία» θα δημιουργήσει γι' αυτόν κάποιος υπάλληλος του οργανισμού «κατά παραγγελία». Ωστόσο, μια τέτοια προσέγγιση είναι προβληματική για διάφορους λόγους. Αν ο ερευνητής χρησιμοποιήσει τον πάροχο των υπηρεσιών του υπολογιστικού νέφους για να αποκτήσει την ψηφιακή εικόνα, τότε δεν ελέγχει εξ αρχής την αλληλουχία των σταδίων (chain of custody). Σε ένα πλήρες ιστορικό καταγραφής των βημάτων θα πρέπει να προσδιορίζονται επακριβώς όλα τα άτομα που έχουν έρθει σε επαφή με τα αποδεικτικά στοιχεία. Άρα, αν τη δουλειά του ερευνητή πρακτικά την κάνει κάποιος υπάλληλος, τότε η αλληλουχία των σταδίων αρχίζει με τους υπαλλήλους του παρόχου στους οποίους έχει ανατεθεί η εργασία αυτή.[76] Η δεύτερη αρχή στις οδηγίες της ACPO δηλώνει ότι το άτομο που είναι υπεύθυνο για τη συλλογή των αποδεικτικών στοιχείων πρέπει να είναι κατάλληλα εκπαιδευμένος και ικανός να το κάνει. Αλλά εδώ τίθεται το ερώτημα κατά πόσο ο ερευνητής μπορεί να είναι βέβαιος ότι ο εργαζόμενος σε ένα πάροχο είναι ικανός για τη συλλογή, με ορθό τρόπο, των αποδεικτικών στοιχείων για λογαριασμό του.

---

[75] Chow, R., Golle, P., Jakobsson, M., Shi, E., Staddon, J., Masuoka, R., & Molina, J. (2009, November). *Controlling data in the cloud: outsourcing computation without outsourcing control*. Στο Proceedings of the 2009 ACM workshop on Cloud computing security (pp. 85-90). ACM.

[76] Martini, B., & Choo, K. K. R. (2012). *An integrated conceptual digital forensic framework for cloud computing*. Στο Digital Investigation, 9(2), 71-80

Κι αν, βέβαια, ο ερευνητής δε μπορεί να είναι βέβαιος για τις ικανότητες του υπαλλήλου του παρόχου και ζητήσει να προχωρήσει στις διαδικασίες συλλογής μόνος του, τότε και πάλι ενδεχομένως να είναι αναγκαία η παρουσία ή η συμμετοχή στις διαδικασίες κάποιου υπαλλήλου, ο οποίος θα προσδιορίσει επακριβώς τη φυσική τοποθεσία των δεδομένων που αναζητά ο ερευνητής ή θα παρέμβει γιατί γνωρίζει καλύτερα την τεχνολογία και τη λειτουργία των συσκευών και πληροφοριακών συστημάτων του οργανισμού – παρόχου των υπηρεσιών υπολογιστικού νέφους. Άρα και πάλι μπορεί να χαθεί η αξιοπιστία της αλληλουχίας των βημάτων.[77]

Χρονοσφραγίδες

Ιδιαίτερα σημαντικό ρόλο στο στάδιο της συλλογής δεδομένων παίζουν οι χρονοσφραγίδες των δεδομένων, δηλαδή οι ημεροχρονολογίες δημιουργίας, τροποποίησης ή διαγραφής τους. Τα συγκεκριμένα στοιχεία προκύπτουν από τις χρονοσφραγίδες στα μετα-δεδομένα του συστήματος αρχείων και από τα αρχεία καταγραφής (log files) σε ένα ή περισσότερα συστήματα υπολογιστών. Έτσι, όταν ο ερευνητής έχει την πληροφορία αυτή, τότε μπορεί να τη χρησιμοποιήσει για να ανασυστήσει την αλληλουχία των γεγονότων που σχετίζονται με το ερευνώμενο περιστατικό. Πιο συγκεκριμένα, ο ερευνητής σκοπό έχει, μέσα από τις ενέργειές του, να προσδιορίσει επακριβώς την ώρα και τη ζώνη ώρας των συμβάντων στη συσκευή, για να τα αναπαραστήσει σωστά στη συνέχεια. Σε ένα περιβάλλον υπολογιστικού νέφους, ο προσδιορισμός των χρονοσφραγίδων είναι εξαιρετικά δύσκολος. Έχει αναφερθεί ήδη νωρίτερα ότι τα δημόσια υπολογιστικά νέφη ενδεχομένως κατανέμουν δεδομένα – και άρα τυχόν αποδεικτικά στοιχεία – σε πολλές διαφορετικές τοποθεσίες, έτσι που οι φυσικές θέσεις (των δεδομένων) θα μπορούσαν να βρίσκονται σε περισσότερες από μία ζώνες ώρας. Και ενδέχεται, τέλος, οι εικονικοποιημένες (virtualized) υπηρεσίες να λειτουργούν σύμφωνα με τις ζώνες ώρας των χρηστών τους και όχι με τη ζώνη ώρας της φυσικής τοποθεσίας όπου στεγάζεται η υποδομή τους.[78]

---

[77] Birk, D., & Wegener, C. (2011, May). *Technical issues of forensic investigations in cloud computing environments.* Στο Systematic Approaches to Digital Forensic Engineering (SADFE), 2011 IEEE Sixth International Workshop on (pp. 1-10). IEEE

[78] Thorpe, S., Ray, I., Grandison, T., & Barbir, A. (2012, July). *Cloud log forensics metadata analysis*. In *Computer Software and Applications Conference Workshops (COMPSACW),* 2012 IEEE 36th Annual (pp. 194-199). IEEE αλλά και Marangos, N., Rizomiliotis, P., & Mitrou, L. (2014). *Time synchronization: pivotal element in cloud forensics*. Security and Communication Networks

Εξέταση και ανάλυση

Για το στάδιο της εξέτασης και ανάλυσης των δεδομένων, εφόσον έχει ολοκληρωθεί η συλλογή των πειστηρίων, χρησιμοποιούνται ευρέως διάφορα δημοφιλή εργαλεία, όπως το FTK[79] ή το Encase[80]. Τα λογισμικά αυτά μπορούν να χρησιμοποιηθούν για να αναζητηθούν στα πειστήρια συγκεκριμένα μοτίβα ή να γίνει φιλτράρισμα των αρχείων με βάση το όνομά τους, τον τύπο τους ή το περιεχόμενο. Επιπλέον, μπορούν να χρησιμοποιηθούν για την ανάκτηση δεδομένων που ο χρήστης διέγραψε ή προσπάθησε να διαγράψει.

Κατά τη φάση της ανάλυσης της έρευνας, αξιολογείται η σπουδαιότητα των ευρημάτων ως αποδεικτικών στοιχείων. Δημιουργείται, με βάση τα ευρήματα, μια αναλυτική περιγραφή των περιστατικών και ένα χρονοδιάγραμμα των όσων συνέβησαν. Όπου κρίνεται σκόπιμο, μπορεί να συνδέονται συγκεκριμένα ευρήματα με χρήστες ή λογαριασμούς χρηστών. Ακόμα, τα ευρήματα μπορεί να υπόκεινται σε διαδικασία επικύρωσης, ώστε να επιβεβαιώνεται πως τα πειστήρια δεν έχουν τροποποιηθεί εξαιτίας κάποιας τεχνικής της ανάλυσης.[81]

Είδη αποδεικτικών στοιχείων στο υπολογιστικό νέφος

Αρκετοί τύποι αποδεικτικών στοιχείων που συναντώνται στο υπολογιστικό νέφος μοιάζουν με αυτά που εντοπίζονται συνήθως σε συμβατικές έρευνες: έγγραφα κειμένου, παρουσιάσεις, μηνύματα ηλεκτρονικού ταχυδρομείου, εικόνες κ.λπ.. Στο υπολογιστικό νέφος, ωστόσο, θα είναι διαθέσιμες και πολλές νέες μορφές αποδεικτικών στοιχείων, ιδίως τα αρχεία της αλληλεπίδρασης των χρηστών με τις υπηρεσίες του υπολογιστικού νέφους, που είναι γνωστά με τον όρο «αρχεία καταγραφής».

Για να αποκτήσει πρόσβαση στα προαναφερθέντα αρχεία καταγραφής, ένας ερευνητής χρειάζεται να έχει πρόσβαση στις υπηρεσίες του παρόχου όπου διενεργεί την έρευνα, με δικαιώματα διαχειριστή του συστήματος. Αφού τα αρχεία καταγραφής θα βρίσκονται στο υπολογιστικό νέφος, για να έχει κάποιος πρόσβαση σε αυτά θα χρειαστεί το όνομα χρήστη και τον κωδικό πρόσβασης ενός διαχειριστή των υπηρεσιών. Προφανώς

[79] http://accessdata.com/solutions/digital-forensics/forensic-toolkit-ftk

[80] https://www.guidancesoftware.com/encase-forensic

[81] Yusoff, Y., Ismail, R., & Hassan, Z. (2011). *Common phases of computer forensics investigation models*. International Journal of Computer Science & Information Technology, 3(3), 17-31.

υπάλληλοι του παρόχου θα μπορούσαν να υποστηρίξουν τις διαδικασίες της έρευνας, αλλά όπως αναφέρθηκε και νωρίτερα, εξακολουθεί να αποτελεί σοβαρό ζήτημα η αξιοπιστία της αλληλουχίας των βημάτων.[82]

Επικύρωση με τη χρήση εργαλείων κατακερματισμού (hashing)

Τα εργαλεία hashing αξιοποιούνται συνήθως σε συμβατικές έρευνες για την επικύρωση της ακεραιότητας των δεδομένων που χρησιμοποιούνται ως αποδεικτικά στοιχεία. Μια συνάρτηση κατακερματισμού είναι ένας αλγόριθμος για τη μετατροπή ακολουθιών δεδομένων (data strings) αυθαίρετου μήκους σε σταθερού μήκους τιμές (hash values), συνήθως μερικών εκατοντάδων bytes. Οι συναρτήσεις hash έχουν σχεδιαστεί έτσι ώστε οποιαδήποτε αλλαγή στα δεδομένα εισόδου θα πρέπει (με μεγάλη πιθανότητα) να παράγει μια διαφορετική τιμή εξόδου.[83] Οι τιμές hash μπορούν επομένως να υπολογίζονται σε τακτά χρονικά διαστήματα για τα images του δίσκου, τα αρχεία ή άλλα δεδομένα που αποτελούν εγκληματολογικά πειστήρια, ώστε να προκύπτει με βεβαιότητα πως τα στοιχεία δεν έχουν αλλάξει κατά τη διάρκεια της ανάλυσης.[84]

Τα δεδομένα που αποθηκεύονται σε μια υπηρεσία βασισμένη στο υπολογιστικό νέφος μπορούν επίσης να ελέγχονται μέσω συναρτήσεων κατακερματισμού, ώστε να επιβεβαιώνεται η ακεραιότητά τους. Η χρήση των εργαλείων κατακερματισμού όταν υλοποιείται, αναπτύσσεται και ελέγχεται από τους παρόχους υπηρεσιών υπολογιστικού νέφους και συνεπάγεται ορισμένους προβληματισμούς.

Όπως αναφέρθηκε και παραπάνω, όταν αναπτύχθηκε το θέμα της συλλογής των αποδεικτικών στοιχείων, η χρήση των ιδιόκτητων εγκαταστάσεων / υποδομών του παρόχου αναγκαστικά τοποθετεί τους υπαλλήλους του παρόχου στην αλληλουχία των βημάτων. Ο ερευνητής έχει περιορισμένες δυνατότητες για να δοκιμάσει και να αξιολογήσει τα εργαλεία κατακερματισμού στο υπολογιστικό νέφος, σε σύγκριση με τα εργαλεία που έχουν αναπτυχθεί για χρήση σε συμβατικούς επιτραπέζιους υπολογιστές. Πρακτικά, σε μια συμβατική έρευνα ένας ερευνητής μπορεί να χρησιμοποιήσει διάφορα εργαλεία που εφαρμόζουν την ίδια συνάρτηση κατακερματισμού για να υπολογίσει μια

[82] Guo, H., Jin, B., & Shang, T. (2012, August). *Forensic investigations in cloud environments*.Στο Computer Science and Information Processing (CSIP), 2012 International Conference on (pp. 248-251). IEEE.

[83] https://en.wikipedia.org/wiki/Hash_function

[84] https://www.cclgroupltd.com/cryptographic-hash-functions-important-digital-forensics/

τιμή hash για ορισμένα δεδομένα του δείγματος. Τυχόν διαφορές μεταξύ των αποτελεσμάτων που παράγονται μπορούν να διερευνηθούν. Ωστόσο, σε ένα περιβάλλον υπολογιστικού νέφους ο ερευνητής έχει μόνο μία επιλογή – εφαρμογή για να χρησιμοποιήσει: το checksum που πραγματοποιεί ο πάροχος του υπολογιστικού νέφους. Κατά συνέπεια, η ικανότητα του ερευνητή να επικυρώσει την ορθότητα των εργαλείων του είναι περιορισμένη.[85]

Παρουσίαση

Τα στοιχεία που συγκεντρώθηκαν κατά τη διάρκεια μιας ψηφιακής εγκληματολογικής έρευνας συνοψίζονται, συνήθως, σε μια έκθεση, μαζί με τα συμπεράσματα που προκύπτουν. Η έκθεση αυτή μπορεί να παρουσιαστεί ενώπιον των δικαστικών και εισαγγελικών αρχών, ενώ συχνά ζητείται από κάποιον ερευνητή ή εξεταστή να παρουσιαστεί στο δικαστήριο και να διευκρινίσει τυχόν «θολά» σημεία. Εναλλακτικά, τα αποτελέσματα της έρευνας θα μπορούσαν να χρησιμοποιηθούν από έναν οργανισμό για να βελτιωθεί η εταιρική του πολιτική και να αποτελέσουν τις βάσεις για περαιτέρω έρευνες στο μέλλον.

Σε κάθε περίπτωση, σε ένα δικαστήριο μπορεί να συζητηθεί το παραδεκτό ή όχι των επιστημονικών αποδείξεων. Είναι γενικά γνωστά τα κριτήρια Daubert[86], τα οποία δίνουν τη δυνατότητα στους δικαστές και τους καθοδηγούν ώστε να εξετάσουν τέσσερις τουλάχιστον παράγοντες, ώστε να αποφασίσουν αν τελικά θα αποδεχθούν ή όχι ένα επιστημονικό δεδομένο – στην περίπτωσή μας τα ευρήματα της ψηφιακής εγκληματολογικής εξέτασης.

Τα ερωτήματα που ζητούν απαντήσεις είναι τα εξής:

- Μπορεί να δοκιμαστεί η επιστημονική θεωρία, τεχνική ή μέθοδος που έχει προταθεί;
- Έχει υποβληθεί σε κριτική από ειδικούς η εν λόγω επιστημονική θεωρία, τεχνική ή μέθοδος;

---

[85] Ruan, K., James, J., Carthy, J., & Kechadi, T. (2012, January). *Key terms for service level agreements to support cloud forensics*. Στο IFIP International Conference on Digital Forensics (pp. 201-212). Springer Berlin Heidelberg.

[86] https://www.law.cornell.edu/wex/daubert_standard

- Έχει μετρηθεί το ποσοστό λάθους που μπορεί να εμπεριέχουν και, αν ναι, είναι αποδεκτό;
- Απολαμβάνει διαδεδομένη αποδοχή η θεωρία, τεχνική ή μέθοδος;

Προφανώς τα ίδια ερωτήματα θα πρέπει να απαντηθούν τόσο για τις συμβατικές ψηφιακές εγκληματολογικές αναλύσεις όσο και για τις μεθόδους εγκληματολογικής ανάλυσης δεδομένων από περιβάλλοντα υπολογιστικού νέφους. Γι' αυτό το λόγο, λαμβάνοντας υπόψη και την τεχνολογική πρόοδο, θα πρέπει να αναπτυχθούν και να τεκμηριωθούν για την ορθότητά τους νέες μέθοδοι αξιολόγησης για τα περιβάλλοντα υπολογιστικού νέφους.

Ένας εμπειρογνώμονας, άλλωστε, θα μπορούσε να βρεθεί στη δικαστική αίθουσα και να του ζητηθεί αρχικά να εξηγήσει την έννοια του υπολογιστικού νέφους και έπειτα να αναφερθεί στα εγκληματολογικά ευρήματα σε αυτό. Κι αυτό γιατί οι δικαστές και οι ένορκοι ανά τον κόσμο δε μπορούν να γνωρίζουν τα πάντα: μπορεί να χρησιμοποιούν τον υπολογιστή τους για πολύ βασικές λειτουργίες (π.χ. να συντάξουν ένα κείμενο ή να περιηγηθούν στο Διαδίκτυο) και να μην έχουν ιδέα για την ύπαρξη και τον τρόπο λειτουργίας των υπηρεσιών υπολογιστικού νέφους.

Η εξέλιξη της εγκληματολογικής ανάλυσης στο υπολογιστικό νέφος είναι ακόμα σε πρώιμο στάδιο. Επί του παρόντος δεν υπάρχει τυποποιημένη μέθοδος ή εργαλείο για τη διεξαγωγή ερευνών στο υπολογιστικό νέφος, ή ακόμα και για την αξιολόγηση και πιστοποίηση των προτεινόμενων εργαλείων. Αναμφίβολα η παρουσίαση αποδεικτικών στοιχείων που προέρχονται από μια υπηρεσία υπολογιστικού νέφους είναι μια προβληματική διαδικασία, που με περαιτέρω έρευνα μπορεί να βελτιωθεί στο μέλλον.

❑

Κεφάλαιο 4: Νομικές προκλήσεις διερεύνησης κυβερνοεγκλημάτων και εγκληματολογικής ανάλυσης σε περιβάλλον υπολογιστικού νέφους

Κατά τη διερεύνηση κυβερνοεγκλημάτων οι Αρχές Επιβολής του Νόμου ενός Κράτους έρχονται αντιμέτωπες με μια σειρά προκλήσεων νομικής φύσης, ειδικά στις περιπτώσεις εκείνες που απαιτείται πρόσβαση σε δεδομένα και στοιχεία που φιλοξενούνται από παρόχους υπηρεσιών Διαδικτύου, αλλά και υπηρεσιών υπολογιστικού νέφους, που έχουν την έδρα τους στην αλλοδαπή.

Αν θεωρήσουμε ότι η συλλογή αποδεικτικών στοιχείων από ένα υπολογιστικό σύστημα στο νέφος συνιστά απομακρυσμένη (συχνά διασυνοριακή) πρόσβαση στα δεδομένα κάποιου, τότε μπορούμε να υποθέσουμε ότι οι προκλήσεις για τους εκπροσώπους των Αρχών Επιβολής του Νόμου στις εν λόγω περιπτώσεις είναι σαφώς ευρύτερες.

Γι' αυτό το λόγο, θα εξετάσουμε αρχικά γενικότερα ζητήματα που σχετίζονται με τη διερεύνηση κυβερνοεγκλημάτων σε διασυνοριακό επίπεδο και ακολούθως θα εστιάσουμε στις περιπτώσεις εκείνες που απαιτείται από τον ερευνητή η συλλογή πειστηρίων που βρίσκονται αποθηκευμένα στο υπολογιστικό νέφος.

Προκλήσεις κατά τη διερεύνηση κυβερνοεγκλημάτων

Αρχικά θα αναφερθούμε σε ζητήματα που σχετίζονται γενικότερα με τη διερεύνηση εγκλημάτων που τελούνται στον κυβερνοχώρο. Οι προκλήσεις που παρατίθενται στη συνέχεια εξετάζονται με βάση τα ισχύοντα στη χώρα μας και στην Ευρωπαϊκή Ένωση και προκύπτουν μέσα από μια σειρά εκθέσεων και κειμένων εργασίας[87] του **Cloud Evidence Group** που έχει συσταθεί και λειτουργεί εντός της Cybercrime Convention Committee του Συμβουλίου της Ευρώπης[88].

[87] TCY(2016)5 Criminal justice access to data in the cloud: Recommendations for consideration by the T-CY, T-CY(2015)16 Draft Guidance Note on Production Orders (Article 18) - Version 4 May 2016 - Version 15 September 2016 - Version 15 November 2016 (16th T-CY Plenary), T-CY(2016)2 Criminal justice access to data in the cloud: cooperation with "foreign" service providers, TCY(2016)7 Criminal justice access to electronic evidence in the cloud - Informal summary of issues and options under consideration by the Cloud Evidence Group, T-CY(2015)10 Criminal justice access to data in the cloud: challenges και T-

Διατήρηση και απώλεια δεδομένων

Ο τύπος των δεδομένων που απαιτούνται συχνότερα κατά τη διάρκεια εγκληματολογικών ερευνών είναι κατά σειρά τα **στοιχεία του συνδρομητή** (εξωτερικά στοιχεία επικοινωνίας, όπως συνηθίζουμε να τα αποκαλούμε), τα **δεδομένα κίνησης** και έπειτα τα **δεδομένα περιεχομένου**. Η απόκτηση στοιχείων συνδρομητή αντιπροσωπεύει μια μικρότερης έκτασης «ανάμειξη» με τα δεδομένα του ατόμου σε σχέση με την απόκτηση δεδομένων κίνησης και ιδίως δεδομένων περιεχομένου[89].

Ωστόσο, αυτή η προσέγγιση δεν αντικατοπτρίζεται πάντα στην οικεία νομοθεσία σχετικά με την πρόσβαση σε αποδεικτικά στοιχεία και πειστήρια ενός εγκλήματος. Σε ορισμένα Κράτη οι απαιτήσεις στο πλαίσιο μιας ποινικής έρευνας προκειμένου κάποιος να έχει πρόσβαση σε στοιχεία συνδρομητή είναι σχετικά λίγες, ενώ σε άλλα ενδέχεται να απαιτείται παραγγελία από τις αρμόδιες εισαγγελικές και δικαστικές Αρχές. Τα παραπάνω έχουν επίδραση τόσο στις έρευνες των Αρχών Επιβολής του Νόμου εντός του Κράτους όσο και στη διεθνή συνεργασία, που είναι αναγκαία, λόγω της φύσεως των εγκλημάτων στον κυβερνοχώρο.

Τα στοιχεία συνδρομητή τηρούνται κατά κανόνα από ιδιωτικούς παρόχους υπηρεσιών Διαδικτύου και υπολογιστικού νέφους και αποκτώνται συνήθως μέσω παραγγελιών των εισαγγελικών και δικαστικών Αρχών. Μια **εισαγγελική παραγγελία** έχει σαφώς μικρότερο «αντίκτυπο» στα δικαιώματα του ατόμου και στα συμφέροντα τρίτων

CY(2016)13 - Emergency requests for the immediate disclosure of data stored in another jurisdiction through mutual legal assistance channels or through direct requests to service providers: Compilation of replies

[88] http://www.coe.int/en/web/cybercrime/ceg

[89] Με βάση το άρθρο 2 του Ν. 3471/2006 ως «δεδομένα κίνησης» θεωρούνται τα δεδομένα που υποβάλλονται σε επεξεργασία για τους σκοπούς της διαβίβασης μίας επικοινωνίας σε δίκτυο ηλεκτρονικών επικοινωνιών ή της χρέωσης της. Στα δεδομένα κίνησης μπορεί να περιλαμβάνονται, μεταξύ άλλων, ο αριθμός, η διεύθυνση, η ταυτότητα της σύνδεσης ή του τερματικού εξοπλισμού του συνδρομητή ή και χρήστη, οι κωδικοί πρόσβασης, τα δεδομένα θέσης, η ημερομηνία και ώρα έναρξης και λήξης και η διάρκεια της επικοινωνίας, ο όγκος των διαβιβασθέντων δεδομένων, πληροφορίες σχετικά με το πρωτόκολλο, τη μορφοποίηση, τη δρομολόγηση της επικοινωνίας καθώς και το δίκτυο από το οποίο προέρχεται ή στο οποίο καταλήγει η επικοινωνία. Επιπρόσθετα, ως «δεδομένα θέσης» προσδιορίζονται τα δεδομένα που υποβάλλονται σε επεξεργασία σε δίκτυο ηλεκτρονικών επικοινωνιών ή από μια υπηρεσία ηλεκτρονικών επικοινωνιών και που υποδεικνύουν τη γεωγραφική θέση του τερματικού εξοπλισμού του χρήστη μια διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών.

μερών σε σχέση με άλλες διαδικασίες, όπως λ.χ. η διεξαγωγή έρευνας σε οικία (ή χώρο εργασίας) και η κατάσχεση πειστηρίων ή η νόμιμη ακρόαση συνομιλιών και καταγραφή δεδομένων (μέσω επισύνδεσης).

Πρόβλημα, ωστόσο, δεν αποτελεί μόνο το είδος των δεδομένων που ζητούνται στο πλαίσιο μιας ποινικής έρευνας, αλλά και το βάθος χρόνου για το οποίο θα πρέπει τα δεδομένα των συνδρομητών να τηρούνται από τους παρόχους.

Σε επίπεδο Ευρωπαϊκής Ένωσης, με την Οδηγία 2002/58/ΕΚ, αναφορικά με την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες, καθορίστηκαν ειδικοί κανόνες για την επεξεργασία δεδομένων προσωπικού χαρακτήρα στον τομέα των ηλεκτρονικών επικοινωνιών, με ταυτόχρονη εξασφάλιση του δικαιώματος στο απόρρητο των επικοινωνιών (άρθρο 5) και υποχρέωση για τους παρόχους υπηρεσίας να διαγράφουν τα δεδομένα κίνησης όταν δεν είναι πλέον απαραίτητα για τον σκοπό της μετάδοσης της επικοινωνίας, εκτός εάν έχουν υποβληθεί σε επεξεργασία υπό ορισμένες προϋποθέσεις για τη χρέωση των συνδρομητών και την πληρωμή των διασυνδέσεων. Με βάση την παράγραφο 16 του άρθρου 15 της Οδηγίας, επιτρέπεται, υπό ορισμένες προϋποθέσεις, ο περιορισμός των δικαιωμάτων και των υποχρεώσεων που προβλέπονται σε αυτήν για συγκεκριμένους σκοπούς, μεταξύ άλλων, «**για την πρόληψη, διερεύνηση, διαπίστωση και δίωξη ποινικών αδικημάτων**».[90] Συνεπώς, επιτρέπεται υπό ορισμένες προϋποθέσεις η θέσπιση μέτρων διατήρησης εθνικών δεδομένων. Σκοπός της Οδηγίας 2006/24/ΕΚ, για τη διατήρηση δεδομένων, ήταν η εναρμόνιση των κανόνων αυτών, ώστε να εξασφαλιστεί

[90] Το άρθρο 15 παράγραφος 1 της οδηγίας 2002/58/ΕΚ έχει ως εξής: «Τα κράτη μέλη δύνανται να λαμβάνουν νομοθετικά μέτρα για να περιορίζουν τα δικαιώματα και τις υποχρεώσεις που προβλέπονται στα άρθρα 5 και 6, στο άρθρο 8 παράγραφοι 1 έως 4 και στο άρθρο 9 της παρούσας οδηγίας, εφόσον ο περιορισμός αυτός αποτελεί αναγκαίο, κατάλληλο και ανάλογο μέτρο σε μια δημοκρατική κοινωνία για τη διαφύλαξη της εθνικής ασφάλειας (δηλαδή της ασφάλειας του κράτους), της εθνικής άμυνας, της δημόσιας ασφάλειας, και για την πρόληψη, διερεύνηση, διαπίστωση και δίωξη ποινικών αδικημάτων ή της άνευ αδείας χρησιμοποίησης του συστήματος ηλεκτρονικών επικοινωνιών, όπως προβλέπεται στο άρθρο 13 παράγραφος 1 της οδηγίας 95/46/ΕΚ. Για το σκοπό αυτό, τα κράτη μέλη δύνανται, μεταξύ άλλων, να λαμβάνουν νομοθετικά μέτρα που θα προβλέπουν τη φύλαξη δεδομένων για ορισμένο χρονικό διάστημα για τους λόγους που αναφέρονται στην παρούσα παράγραφο. Όλα τα μέτρα που προβλέπονται στην παρούσα παράγραφο είναι σύμφωνα με τις γενικές αρχές του κοινοτικού δικαίου, συμπεριλαμβανομένων αυτών που αναφέρονται στο άρθρο 6 παράγραφοι 1 και 2 της συνθήκης για την Ευρωπαϊκή Ένωση.»

ότι τα στοιχεία είναι διαθέσιμα ιδίως για τους σκοπούς της διερεύνησης, διαπίστωσης και δίωξης σοβαρών ποινικών αδικημάτων.[91]

Η εν λόγω Οδηγία ενσωματώθηκε στην εθνική μας νομοθεσία με το νόμο 3917/2011.[92] Μεταξύ άλλων, το άρθρο 6 του νόμου 3917/2011 αναφέρεται στον τρόπο και το χρόνο διατήρησης των δεδομένων που αφορούν ηλεκτρονικές επικοινωνίες και ουσιαστικά υποχρεώνει τους ISPs να διατηρούν δεδομένα για τους χρήστες τους για ένα (1) μόνο έτος, και από εκεί και πέρα τα δεδομένα αυτά πρέπει να καταστρέφονται με αυτοματοποιημένη διαδικασία.

Ωστόσο, σύμφωνα με πρόσφατη απόφαση του Δικαστηριού της Ε.Ε.[93], τα Κράτη Μέλη δε μπορούν να επιβάλλουν γενική υποχρέωση διατηρήσεως δεδομένων στους παρόχους υπηρεσιών ηλεκτρονικών επικοινωνιών. Το Δικαστήριο της Ε.Ε. αποφάνθηκε κατηγορηματικά ότι η εθνική νομοθεσία η οποία προβλέπει γενική και χωρίς διάκριση διατήρηση των δεδομένων αντιβαίνει προς το δίκαιο της Ένωσης.

Επιτρέπεται, πάντως, στα Κράτη Μέλη να προβλέπουν προληπτικά τη στοχευμένη διατήρηση των δεδομένων αυτών προς τον σκοπό και μόνο της καταπολέμησης του **σοβαρού εγκλήματος**, υπό την προϋπόθεση, βέβαια, ότι η διατήρηση περιορίζεται σε ό,τι είναι **απολύτως αναγκαίο** όσον αφορά τις κατηγορίες διατηρούμενων δεδομένων, τα πρόσωπα των οποίων τα δεδομένα διατηρούνται καθώς και το διάστημα για το οποίο γίνεται δεκτό ότι πραγματοποιείται η διατήρηση.

Το Δικαστήριο της Ε.Ε. δέχεται ακόμα ότι η πρόσβαση των εθνικών Αρχών στα διατηρούμενα δεδομένα πρέπει να υπόκειται σε προϋποθέσεις, μεταξύ των οποίων, ιδίως,

---

[91] Τα παραπάνω, όπως και ορισμένα από τα επόμενα ζητήματα, αποτυπώνονται στο παράρτημα του υπ' αριθμ. 14369/15 από 23/11/2015 εγγράφου του Συμβουλίου της Ευρώπης, που είναι διαθέσιμο εδώ: http://data.consilium.europa.eu/doc/document/ST-14369-2015-INIT/en/pdf

[92] Ν. 3917/2011 - Διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών, χρήση συστημάτων επιτήρησης με τη λήψη ή καταγραφή ήχου ή εικόνας σε δημόσιους χώρους και συναφείς διατάξεις, ΦΕΚ 22/Α΄/21.2.2011

[93] Απόφαση στις συνεκδικασθείσες υποθέσεις C-203/15 Tele2 Sverige AB κατά Post - och telestyrelsen και C-698/15 Secretary of State for the Home Department κατά Tom Watson κ.λπ.. Ολόκληρη η Απόφαση είναι διαθέσιμη εδώ http://curia.europa.eu/juris/documents.jsf?num=C-203/15, ενώ σχετικό δελτίο τύπου του Δικαστηρίου της Ευρωπαϊκής Ένωσης είναι διαθέσιμο εδώ: http://curia.europa.eu/jcms/upload/docs/application/pdf/2016-12/cp160145el.pdf

ο προηγούμενος έλεγχος ανεξάρτητης Αρχής και η διατήρηση των δεδομένων εντός των εδαφικών ορίων της Ευρωπαϊκής Ένωσης.

Η εν λόγω απόφαση του Δικαστηρίου της Ευρωπαϊκής Ένωσης συνάδει με το ευρωπαϊκό νομοθετικό πλαίσιο και συγκεκριμένα με την Συνθήκη της Λισαβόνας, από την έναρξη ισχύος της οποίας, τον Δεκέμβριο 2009, ο Χάρτης Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης κατέστη νομικά δεσμευτικός.[94]

Ως αιτιολογική βάση της απόφασης αυτής επισημαίνεται η σοβαρότητα της διατήρησης των προσωπικών δεδομένων των χρηστών υπηρεσιών ηλεκτρονικών επικοινωνιών, η οποία πραγματοποιείται χωρίς οι χρήστες υπηρεσιών ηλεκτρονικών επικοινωνιών να ενημερώνονται σχετικά, κάτι που ενδεχομένως προκαλεί στα οικεία πρόσωπα την αίσθηση ότι η ιδιωτική τους ζωή αποτελεί το αντικείμενο διαρκούς παρακολούθησης. Συνεπώς, μόνον η καταπολέμηση του σοβαρού εγκλήματος μπορεί να δικαιολογήσει μια τέτοια επέμβαση και η εθνική ρύθμιση πρέπει να προβλέπει τη διατήρηση των δεδομένων εντός των εδαφικών ορίων της Ένωσης καθώς και την οριστική καταστροφή τους με το πέρας της διάρκειας της διατήρησής τους.

Εκτός από τη νομική διάσταση της υπόθεσης, όπως παρατέθηκε παραπάνω, είναι εξίσου σημαντικό να λάβει κανείς υπόψη του το **οικονομικό κόστος** που συνεπάγεται η επ' αόριστον και αδιάκριτη συλλογή δεδομένων από τους παρόχους υπηρεσιών Διαδικτύου, καθώς το κόστος για την αποθήκευση όλων αυτών των δεδομένων είναι εξαιρετικά υψηλό και επιβαρύνει, με τα σημερινά δεδομένα, τον πάροχο των υπηρεσιών.[95]

Αξίζει, τέλος, να σημειωθεί ότι στις 25 Μαΐου 2018 τίθεται σε εφαρμογή ο Κανονισμός (Ε.Ε.) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών.[96] Με βάση τον Κανονισμό αυτό, που αλλάζει άρδην το οικείο πλαίσιο, κάθε επεξεργασία δεδομένων προσωπικού χαρακτήρα θα πρέπει να είναι σύννομη και δίκαιη. Θα πρέπει να είναι σαφές

---

[94] Ολόκληρος ο Χάρτης Θεμελιωδών Δικαιωμάτων είναι διαθέσιμος εδώ: http://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex:12016P/TXT

[95] Kotzanikolaou, P. (2008). *Data retention and privacy in electronic communications*. IEEE Security & Privacy, 6(5).

[96] Ολόκληρος ο νέος Κανονισμός είναι διαθέσιμος εδώ: http://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A32016R0679

για τα φυσικά πρόσωπα ότι δεδομένα προσωπικού χαρακτήρα που τα αφορούν συλλέγονται, χρησιμοποιούνται, λαμβάνονται υπόψη ή υποβάλλονται κατ' άλλο τρόπο σε επεξεργασία, καθώς και σε ποιο βαθμό τα δεδομένα προσωπικού χαρακτήρα υποβάλλονται ή θα υποβληθούν σε επεξεργασία.

Από τη φύση τους, άλλωστε, τα ηλεκτρονικά αποδεικτικά στοιχεία είναι βραχύβια. Επιπρόσθετα, η αυξανόμενη χρήση live streaming (ζωντανής ροής), των τεχνικών κρυπτογράφησης, του σκοτεινού Διαδικτύου (dark web) και τελικά της ανωνυμοποίησης επιτρέπουν στους εγκληματίες να αποκρύπτουν τελείως από τις Αρχές Επιβολής του Νόμου κρίσιμα αποδεικτικά στοιχεία. Ως εκ τούτου, αν οι αρμόδιες Αρχές δεν διαθέτουν επαρκή μέσα για να αντιδράσουν αποτελεσματικά, μπορούν να χαθούν κρίσιμα ηλεκτρονικά αποδεικτικά στοιχεία. Η ύπαρξη, συνεπώς, αποτελεσματικού καθεστώτος διατήρησης δεδομένων θα μπορούσε να αποδειχθεί καθοριστικής σημασίας.

Διαδικασία αμοιβαίας δικαστικής συνδρομής (Α.Δ.Σ.)

Η συλλογή ηλεκτρονικών αποδεικτικών στοιχείων αποτελεί, κατ' αρχήν, ζήτημα που είναι ευαίσθητο στον παράγοντα χρόνο. Η ύπαρξη αποτελεσματικών διαδικασιών για τη διαφύλαξη και τη συλλογή ηλεκτρονικών αποδεικτικών στοιχείων είναι καθοριστικής σημασίας για την αποτελεσματική διεξαγωγή της ποινικής διαδικασίας. Δεδομένου ότι τα ηλεκτρονικά δεδομένα βρίσκονται συχνά σε αλλοδαπή δικαιοδοσία, οι αρμόδιες εθνικές Αρχές πρέπει να χρησιμοποιήσουν τα διαθέσιμα εργαλεία για διεθνή συνεργασία, δηλαδή να υποβάλλουν αιτήσεις **αμοιβαίας δικαστικής συνδρομής** (Α.Δ.Σ.)[97] ή, αν η διαδικασία αφορά Κράτη Μέλη της Ε.Ε., να προσφεύγουν κατά περίπτωση στα διαθέσιμα μέσα αμοιβαίας αναγνώρισης στον τομέα της δικαστικής συνεργασίας σε ποινικές υποθέσεις.[98]

Το κυρίαρχο μέσο για την απόκτηση των δεδομένων, στις περιπτώσεις εκείνες όπου τα αποδεικτικά στοιχεία βρίσκονται σε ξένο έδαφος και συνεπώς σε αλλοδαπή δικαιοδοσία, είναι το αίτημα Αμοιβαίας Δικαστικής Συνδρομής. Εξίσου σημαντική,

[97] Πράξη του Συμβουλίου της 29ης Μαΐου 2000 για την κατάρτιση, σύμφωνα με το άρθρο 34 της συνθήκης για την Ευρωπαϊκή Ένωση, της σύμβασης για την αμοιβαία δικαστική συνδρομή επί ποινικών υποθέσεων μεταξύ των κρατών μελών της Ευρωπαϊκής Ένωσης (2000/C 197/01). Περισσότερα στοιχεία εδώ: https://e-justice.europa.eu/content_request_for_judicial_assistance-91-el.do

[98] Ενδεικτικά αναφέρεται η νομοθεσία για συγκέντρωση αποδεικτικών στοιχείων σε ποινικές υποθέσεις από ένα Κράτος σε άλλο και για τη δέσμευση περιουσιακών και αποδεικτικών στοιχείων. Περισσότερα εδώ: https://e-justice.europa.eu/content_cooperation_in_criminal_matters-89-el.do

ωστόσο είναι πλέον και η Οδηγία 2014/41/ΕΕ περί της **ευρωπαϊκής εντολής έρευνας** (Ε.Ε.Ε.).[99] Από τις 22 Μαΐου 2017, αντικαθιστά την υπάρχουσα κατακερματισμένη νομοθεσία της Ε.Ε. σχετικά με τη συλλογή και διαβίβαση αποδεικτικών στοιχείων μεταξύ των κρατών μελών της Ε.Ε., με στόχο να καταστήσει τις διασυνοριακές έρευνες ταχύτερες και αποτελεσματικότερες. Η όσο τη δυνατόν αρτιότερη χρήση του καθεστώτος αυτού, σε σχέση με τα ηλεκτρονικά αποδεικτικά στοιχεία, αναμένεται να βοηθήσει αρκετά τις Αρχές Επιβολής του Νόμου στις έρευνές τους.

Συμβαίνει συχνά τα ηλεκτρονικά δεδομένα να βρίσκονται σε δικαιοδοσίες τρίτων Κρατών, εκτός της Ευρωπαϊκής Ένωσης. Στις περιπτώσεις αυτές θα πρέπει να υποβάλλεται αίτημα Α.Δ.Σ.. Τα ισχύοντα καθεστώτα Α.Δ.Σ. θεωρούνται, ωστόσο, όλο και περισσότερο ως **υπερβολικά αργά** και δύσκαμπτα και δεν επιτρέπουν την τήρηση των προθεσμιών.[100] Για παράδειγμα, από τις ελληνικές Αρχές τα αιτήματα αμοιβαίας δικαστικής συνδρομής υποβάλλονται σύμφωνα με το άρθρο 457 παρ. 1 του Κώδικα Ποινικής Δικονομίας, σύμφωνα με το οποίο *«οι αιτήσεις των ελληνικών δικαστικών Αρχών προς αλλοδαπές Αρχές για την εξέταση μαρτύρων και κατηγορουμένων, για την ενέργεια αυτοψίας και πραγματογνωμοσύνης και για την κατάσχεση πειστηρίων διαβιβάζονται από τον αρμόδιο εισαγγελέα εφετών στο Υπουργείο Δικαιοσύνης, που προκαλεί την εκτέλεσή τους μέσω του Υπουργείου Εξωτερικών με την τήρηση και των διεθνών συνθηκών και εθίμων. Σε επείγουσες περιπτώσεις οι αιτήσεις αυτές διαβιβάζονται και απευθείας στις επιτόπιες προξενικές Αρχές που ασκούν ανακριτικά καθήκοντα, ειδοποιείται όμως σχετικά το Υπουργείο Δικαιοσύνης»*. Από την άλλη πλευρά, σε ότι αφορά αιτήσεις ξένων δικαστικών Αρχών για ανακριτικές πράξεις, σύμφωνα με το άρθρο 458 του Κ.Π.Δ., αυτές *«διαβιβάζονται από το Υπουργείο Δικαιοσύνης και εκτελούνται με παραγγελία του αρμόδιου εισαγγελέα εφετών από τον ανακριτή στην περιφέρεια του οποίου πρόκειται να διεξαχθεί η ανακριτική πράξη, εκτός αν αυτή αντιβαίνει στις διατάξεις του κώδικα ή του οργανισμού δικαστηρίων. […] Κατά τα λοιπά τηρούνται οι σχετικές διατάξεις του κώδικα, οι διεθνείς συνθήκες και τα έθιμα»*.

[99] Οδηγία 2014/41/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 3ης Απριλίου 2014, περί της ευρωπαϊκής εντολής έρευνας σε ποινικές υποθέσεις, διαθέσιμη εδώ: http://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32014L0041

[100] Broadhurst, R. (2006). *Developments in the global law enforcement of cyber-crime.* Στο Policing: An International Journal of Police Strategies & Management, 29(3), 408-433.

Στο πλαίσιο επιτάχυνσης των διαδικασιών γενικότερα, θα μπορούσε να εξετασθεί η δυνατότητα ανάπτυξης ενός τυποποιημένου, απλοποιημένου και, ενδεχομένως, ηλεκτρονικά διαβιβάσιμου και αποδεκτού έντυπου αίτησης, μεταξύ άλλων, στο πλαίσιο της Ε.Ε.Ε..

ΥΠΟΕΝΟΤΗΤΑ Η7: Παρακολούθηση τηλεπικοινωνιών

1. Εάν ζητείται παρακολούθηση τηλεπικοινωνιών, να αναφερθεί γιατί θεωρείται ότι το ερευνητικό μέτρο έχει σημασία για την ποινική διαδικασία

.....

.....

2. Να παρασχεθούν οι ακόλουθες πληροφορίες:

(a) πληροφορίες ταυτότητας του παρακολουθουμένου

.....

(b) επιθυμητή διάρκεια της παρακολούθησης:

.....

(c) τεχνικά δεδομένα (ιδίως αναγνωριστικό στοιχείο του στόχου — λ.χ. κινητό τηλέφωνο, σταθερό τηλέφωνο, διεύθυνση ηλεκτρονικού ταχυδρομείου, σύνδεση Διαδικτύου), ώστε να είναι βέβαιο ότι μπορεί να εκτελεσθεί η ΕΕΕ:

.....

(3) Να αναφερθούν προτιμήσεις όσον αφορά τη μέθοδο εκτέλεσης

☐ Άμεση διαβίβαση

☐ Καταγραφή και εν συνεχεία διαβίβαση

Να αναφερθεί κατά πόσον ζητείται επίσης μεταγραφή, αποκωδικοποίηση ή αποκρυπτογράφηση του υλικού που προκύπτει από την παρακολούθηση (*):

.....

.....

_____

(*) Σημειωτέον ότι το κόστος της ενδεχόμενης μεταγραφής, αποκωδικοποίησης ή αποκρυπτογράφησης βαρύνει το κράτος έκδοσης.

Εικόνα 2 Απόσπασμα προτύπου Ευρωπαϊκής Εντολής Έρευνας – Στην Υποενότητα Η7 ζητείται η παρακολούθηση τηλεπικοινωνιών

Θα μπορούσε επίσης να διερευνηθεί η δυνατότητα περαιτέρω διαφοροποίησης των τυπικών απαιτήσεων στις διαδικασίες Α.Δ.Σ. ανάλογα με τα δεδομένα που ζητούνται – αν πρόκειται για δεδομένα συνδρομητή, κίνησης ή περιεχομένου. Αναφέρθηκε και νωρίτερα ότι σε πολλές δικαιοδοσίες, η πρόσβαση στα δεδομένα συνδρομητή υπόκειται σε απαιτήσεις λιγότερο αυστηρές από τις ισχύουσες για τα δεδομένα κίνησης, ενώ το αυστηρότερο καθεστώς ισχύει για τα δεδομένα περιεχομένου.

Επιπλέον, θα μπορούσαν να προβλεφθούν επισπευσμένες διαδικασίες για τη διαβίβαση των αποδεικτικών στοιχείων υπό ορισμένες προϋποθέσεις, όπως συμβαίνει με τη διατήρηση των αποδεικτικών στοιχείων σύμφωνα με τις σχετικές διατάξεις της

Σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον κυβερνοχώρο.[101] Εν γένει, υπό τις σημερινές συνθήκες, παρά το γεγονός ότι τα αποδεικτικά στοιχεία διατηρούνται, ενδέχεται να απαιτηθεί μεγάλο διάστημα προτού καταστούν διαθέσιμα για την ποινική διαδικασία στην αιτούσα χώρα.

Για να γίνει λειτουργική η διαδικασία συνεργασίας, θα πρέπει ακόμα να εξετασθεί η δυνατότητα έγκαιρου συντονισμού και συμμετοχής των δικαστικών αρχών στη δικαστική διαδικασία. Σε αυτό το πλαίσιο, θα μπορούσε να εξετασθεί η περαιτέρω ενίσχυση της συνεργασίας δικτύων που λειτουργούν σε καθημερινή εικοσιτετράωρη βάση (24/7), συμπεριλαμβανομένων των δικτύων δικαστικών αρχών, παραδείγματος χάρη με τη δημιουργία **δικτύου εισαγγελέων οι οποίοι ασχολούνται με υποθέσεις που έχουν σχέση με τον κυβερνοχώρο**. Αυτό θα είναι καθοριστικής σημασίας για την προώθηση και ενίσχυση των άμεσων επαφών μεταξύ των δικαστικών αρχών, μεταξύ άλλων σε σχέση με την υποβολή αιτήσεων Α.Δ.Σ. σε ολόκληρη την Ε.Ε. και παγκοσμίως.[102]

Σε κάθε περίπτωση, στο πλαίσιο των αιτημάτων Αμοιβαίας Δικαστικής Συνδρομής θα πρέπει να εξετάζονται όλες οι παράμετροι που έχουν σχέση με την προστασία προσωπικών δεδομένων των πολιτών, ιδιαίτερα στις περιπτώσεις εκείνες που τα δεδομένα πρόκειται να χρησιμοποιηθούν ως αποδεικτικά στοιχεία ενώπιον των δικαστικών Αρχών.

Απευθείας αιτήσεις και συνεργασία με αλλοδαπούς παρόχους υπηρεσιών

Ηλεκτρονικά πειστήρια και δεδομένα (στοιχεία συνδρομητή, δεδομένα κίνησης, δεδομένα περιεχομένου) συχνά τηρούνται από παρόχους που προσφέρουν διάφορες κατηγορίες υπηρεσιών και αποθηκεύουν δεδομένα σε διαφορετικές τοποθεσίες / δικαιοδοσίες. Παρά το γεγονός ότι οι Αρχές Επιβολής του Νόμου οφείλουν να ακολουθούν τις νόμιμες οδούς για την απόκτηση δεδομένων που βρίσκονται εκτός της δικαιοδοσίας τους, αξιοποιώντας τα αιτήματα Αμοιβαίας Δικαστικής Συνδρομής, παρατηρείται το φαινόμενο, όλο και συχνότερα, να ανταλλάσσονται δεδομένα ανάμεσα στις Αρχές Επιβολής του Νόμου και σε αλλοδαπούς παρόχους **απευθείας**, χωρίς τη μεσολάβηση των δικαστικών Αρχών.

[101] Άρθρο 16 «Κατεπείγουσα διατήρηση αποθηκευμένων δεδομένων υπολογιστών» και άρθρο 17 «Κατεπείγουσα διατήρηση και μερική αποκάλυψη στοιχείων κίνησης»

[102] Βλ. και παράρτημα του υπ' αριθμ. 14369/15 από 23/11/2015 εγγράφου του Συμβουλίου της Ευρώπης

Στην πράξη υπάρχουν κανονισμοί για τον τρόπο διασυνοριακής ροής (προσωπικών) δεδομένων από τις δικαστικές Αρχές ενός Κράτους στις δικαστικές Αρχές ενός άλλου Κράτους ή από μια ιδιωτική εταιρεία που εδρεύει σε ένα Κράτος σε μια ιδιωτική εταιρεία με έδρα ένα άλλο Κράτος. Όμως, δεν υπάρχουν ρητές προβλέψεις για τις περιπτώσεις όπου πάροχοι υπηρεσιών – ή άλλες ιδιωτικές εταιρείες – δύνανται να διαβιβάζουν δεδομένα στις δικαστικές Αρχές ενός άλλου Κράτους. Σε ορισμένες μόνο περιπτώσεις, η εθνική νομοθεσία μπορεί να επιτρέπει στους παρόχους υπηρεσιών να κοινοποιούν εκουσίως δεδομένα που δεν αφορούν το περιεχόμενο σε (αλλοδαπές) Αρχές Επιβολής του Νόμου.

Ορισμένοι πάροχοι, ιδίως με έδρα της **Ηνωμένες Πολιτείες Αμερικής**, απαντούν απευθείας σε νόμιμα αιτήματα που αφορούν παροχή στοιχείων συνδρομητών ή δεδομένων κίνησης από Αρχές Επιβολής του Νόμου σε άλλες δικαιοδοσίες όπου προσφέρουν μια υπηρεσία. Είναι εξίσου πιθανό πάροχοι να διατηρούν δεδομένα κατόπιν σχετικού αιτήματος για διατήρηση που λαμβάνουν απευθείας από μια αλλοδαπή Αρχή.[103]

Οι αλλοδαποί πάροχοι υπηρεσιών οι οποίοι δέχονται απευθείας αιτήσεις είναι υποχρεωμένοι να ανταποκριθούν σε αντικρουόμενες αιτήσεις από διαφορετικά Κράτη, αλλά και να σεβαστούν αντικρουόμενες απαιτήσεις για την προστασία της ιδιωτικής ζωής και για δικονομικές εγγυήσεις εφόσον λειτουργούν σε **πολλαπλές δικαιοδοσίες**. Παραδείγματος χάρη, οι πάροχοι υπηρεσιών ενδέχεται να παραβιάζουν τους κανόνες περί προστασίας δεδομένων που ισχύουν σε ένα Κράτος αν κοινοποιούν δεδομένα στις Αρχές άλλου Κράτους. Γι' αυτό και δεν είναι πάντα πρόθυμοι να συνεργαστούν, ακόμη και όταν αυτό επιτρέπεται από το εθνικό δίκαιο.

Στις περιπτώσεις αυτές, οι πάροχοι αξιολογούν οι ίδιοι τη νομιμότητα του αιτήματος και το αν εξυπηρετείται νόμιμο συμφέρον, προκειμένου να διατηρήσουν δεδομένα ή να διαβιβάσουν δεδομένα κίνησης ή στοιχεία συνδρομητών σε εθελοντική βάση. Ενδέχεται επίσης να ενημερώσουν τους πελάτες τους σχετικά με το αίτημα, κάτι που μπορεί να θέσει σε κίνδυνο μια έρευνα των Αρχών Επιβολής του Νόμου.

[103] TCY(2016)7 Criminal justice access to electronic evidence in the cloud - Informal summary of issues and options under consideration by the Cloud Evidence Group, διαθέσιμο εδώ: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016805a53c8

Το **μοντέλο εθελοντικής συνεργασίας** εγείρει συζητήσεις σχετικά με τις απαιτήσεις περί προστασίας προσωπικών δεδομένων και απορρήτου επικοινωνιών και γι' αυτό το λόγο οι πάροχοι που εδρεύουν στην Ε.Ε. συνήθως επιλέγουν να μη διαβιβάσουν δεδομένα απευθείας σε αλλοδαπές Αρχές, ούτε καν σε περιπτώσεις κατεπείγοντος χαρακτήρα.

Είναι εξίσου δυνατόν τα ηλεκτρονικά αποδεικτικά στοιχεία να μην είναι παραδεκτά, όπως θα δούμε και στην επόμενη υποενότητα, ενώπιον του δικαστηρίου του αιτούντος Κράτους ακόμη και αν ελήφθησαν μέσω εκούσιας κοινοποίησης, δεδομένου ότι ελήφθησαν εκτός του πλαισίου της Α.Δ.Σ.. Εν γένει, η διαδικασία αυτή θα μπορούσε να οδηγήσει σε ένα φαινόμενο δυνάμενο να ορισθεί ως Α.Δ.Σ. «άνευ συνδρομής», το οποίο ενδέχεται να εγείρει ζητήματα θεμελιωδών δικαιωμάτων και δικονομικών εγγυήσεων.[104]

Όταν δεδομένα που αφορούν στοιχεία συνδρομητών μπορούν να αποκτηθούν με βάση παραγγελίες – εντολές των οικείων εισαγγελικών και δικαστικών Αρχών, τότε θα είναι σαφώς μικρότερη η ανάγκη για ικανοποίηση αιτημάτων δικαστικής συνδρομής και η επιβάρυνση του συνολικού συστήματος Α.Δ.Σ..

Απαιτείται, συνεπώς, να διευκρινιστεί πότε ένας πάροχος υπηρεσιών που προσφέρει στο έδαφος ενός άλλου Κράτους τις υπηρεσίες του υπάγεται στη δικαιοδοσία των εισαγγελικών και δικαστικών Αρχών του Κράτους αυτού (έτσι ώστε να αποσαφηνιστούν ζητήματα σχετικά με τη νομοθεσία που θα πρέπει να εφαρμόζεται με βάση την εδαφικότητα).

Λαμβάνοντας υπ' όψιν τα ανωτέρω, πρέπει να καθορισθούν σαφείς προϋποθέσεις για ένα σταθερό πλαίσιο συνεργασίας μεταξύ ιδιωτικών φορέων και δημοσίων Αρχών όσον αφορά τη συλλογή ηλεκτρονικών αποδεικτικών στοιχείων, με απόλυτο σεβασμό των δικονομικών εγγυήσεων για τους ύποπτους και κατηγορούμενους στο πλαίσιο ποινικής διαδικασίας και της προστασίας των προσωπικών δεδομένων.

Παραδεκτό των ηλεκτρονικών αποδεικτικών στοιχείων

Ενδέχεται να απαιτείται, βάσει της εθνικής νομοθεσίας, η πλήρης αξιολόγηση από τις δικαστικές Αρχές της **νομιμότητας της συλλογής αποδεικτικών στοιχείων** βάσει των

[104] Βλ. και παράρτημα του υπ' αριθμ. 14369/15 από 23/11/2015 εγγράφου του Συμβουλίου της Ευρώπης, αλλά και Walden, I. (2013). *Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent.* Στο Privacy and Security for Cloud Computing (pp. 45-71). Springer London.

κριτηρίων που προβλέπονται από το Νόμο, ως προϋπόθεση για το παραδεκτό των εν λόγω στοιχείων ενώπιον του δικαστηρίου, κατ' αντίθεση προς τα νομικά μοντέλα τα οποία βασίζονται στην αρχή της εμπιστοσύνης, στα οποία όλα τα αποδεικτικά στοιχεία υποβάλλονται και αξιολογούνται ελεύθερα από τον δικαστή. Οι απαιτήσεις αυτές πρέπει να λαμβάνονται υπόψη κατά τη συλλογή και ανταλλαγή ηλεκτρονικών αποδεικτικών στοιχείων. Αυτό θα μπορούσε να οδηγήσει, για παράδειγμα, σε υποχρέωση των αρμοδίων Αρχών να εξασφαλίζουν και να συγκεντρώνουν αποδεικτικά στοιχεία σύμφωνα με τις απαιτήσεις αλλοδαπών δικαστικών συστημάτων.[105]

Στην Ελλάδα ισχύει, σύμφωνα με το άρθρο 177 του Κώδικα Ποινικής Δικονομίας η ***«αρχή της ηθικής απόδειξης»***, δηλαδή *«οι δικαστές δεν είναι υποχρεωμένοι να ακολουθούν νομικούς κανόνες αποδείξεων, πρέπει όμως να αποφασίζουν κατά τη πεποίθησή τους, ακολουθώντας τη φωνή της συνείδησής τους και οδηγούμενοι από την απροσωπόληπτη κρίση που προκύπτει από τις συζητήσεις και που αφορά την αλήθεια των πραγματικών γεγονότων, την αξιοπιστία των μαρτύρων και την αξία των άλλων αποδείξεων»*. Επιπρόσθετα, *«αποδεικτικά μέσα, που έχουν αποκτηθεί με αξιόποινες πράξεις ή μέσω αυτών, δεν λαμβάνονται υπόψη στην ποινική διαδικασία»*.

Η ορθή ερμηνεία των ηλεκτρονικών αποδεικτικών στοιχείων στην ποινική διαδικασία ενδέχεται να απαιτεί εμπειρογνωμοσύνη η οποία μπορεί να μην είναι επαρκώς ανεπτυγμένη στο πλαίσιο των εισαγγελικών και δικαστικών Αρχών. Επιπλέον, η ορθή παρουσίαση των ηλεκτρονικών αποδεικτικών στοιχείων σε δικαστική διαδικασία ενδέχεται να απαιτεί αντίληψη των εγκληματολογικών μεθόδων στο πλαίσιο του δικαστικού σώματος η οποία μπορεί να μην είναι πάντα διαθέσιμη.

Συνεπώς, θα πρέπει ίσως να εξετασθούν οι δυνατότητες παροχής στοχευμένης εκπαίδευσης στους εκπροσώπους των εισαγγελικών και δικαστικών Αρχών.

Διαδικασίες κατεπείγοντος χαρακτήρα

Σε εξαιρετικές περιπτώσεις είναι πιθανό να απαιτούνται τάχιστες ενέργειες για την αποτροπή άμεσου κινδύνου για τη ζωή ενός ατόμου ή για τη δημόσια ασφάλεια. Γι' αυτό το λόγο θα πρέπει να βρίσκονται σε ισχύ διαδικασίες κατεπείγοντος χαρακτήρα, για την

[105] Eurojust. (2014). Report of the Strategic Meeting on Cybercrime 19-20 November 2014 διαθέσιμο εδώ: http://www.eurojust.europa.eu/doclibrary/Eurojust-framework/ejstrategicmeetings/Eurojust%20Strategic%20Meeting%20on%20Cybercrime,%20November%202014/Report-Strategic-Seminar-Cybercrime_2014-11-20_EN.pdf

πρόσβαση σε δεδομένα που βρίσκονται σε αλλοδαπή δικαιοδοσία, μέσω Αμοιβαίας Δικαστικής Συνδρομής ή μέσω απευθείας επικοινωνίας μεταξύ παρόχου και αλλοδαπών Αρχών.[106]

Ατοπικότητα («απώλεια τοποθεσίας»)

Η αμοιβαία δικαστική συνδρομή δεν είναι συχνά καλή επιλογή για έναν ακόμη λόγο. Σε ορισμένες χαρακτηριστικές περιπτώσεις, όπως όταν η προέλευση μιας επίθεσης π.χ. DDoS είναι άγνωστη, όταν εμπλέκονται εξυπηρετητές που βρίσκονται σε διαφορετικές δικαιοδοσίες ή όταν η αρχή της εδαφικότητας δεν είναι δυνατό να εφαρμοστεί, τότε δε γίνεται στην πράξη να διαβιβασθεί ένα αίτημα Αμοιβαίας Δικαστικής Συνδρομής προς τις Αρχές ενός συγκεκριμένου Κράτους.

Ενώ η πρόσβαση σε ηλεκτρονικά αποδεικτικά στοιχεία σε αλλοδαπές δικαιοδοσίες γίνεται κυρίως στο πλαίσιο της Α.Δ.Σ., η αυξανόμενη χρήση των τεχνολογιών υπολογιστικού νέφους και υπηρεσιών βασισμένων στο Διαδίκτυο δημιουργεί πρόσθετο πρόβλημα για τις αρμόδιες Αρχές, το οποίο περιγράφεται ως **«ατοπικότητα»**. Με άλλα λόγια, συχνά αναφέρεται ότι τα ηλεκτρονικά αποδεικτικά στοιχεία είναι αποθηκευμένα **«κάπου στο νέφος»**, είτε σε έναν διακομιστή, είτε κατανεμημένα σε διάφορους διακομιστές, είτε κινούμενα μεταξύ διακομιστών σε διάφορους τόπους. Ως εκ τούτου, οι υλικοί φορείς των οικείων δεδομένων βρίσκονται σε αλλοδαπές, άγνωστες ή πολλαπλές δικαιοδοσίες ταυτόχρονα ή κινούνται μεταξύ δικαιοδοσιών.[107]

Κατ' αρχήν, ο **τόπος** είναι το κριτήριο βάσει του οποίου προσδιορίζονται οι αρμόδιες Αρχές και το εφαρμοστέο στην έρευνα δίκαιο, συμπεριλαμβανομένης της έκτασης των καταναγκαστικού χαρακτήρα εξουσιών που θα μπορούσαν να ασκηθούν, καθώς και οι δικονομικές εγγυήσεις που προβλέπονται για τους ύποπτους ή κατηγορούμενους. Στο πλαίσιο των ανωτέρω νέων τεχνολογικών εξελίξεων, όταν δεν είναι σταθερός ο τόπος των δεδομένων, η υποκείμενη αρχή της εδαφικότητας, η οποία είναι

[106] Η πολυπλοκότητα του ισχύοντος πλαισίου αποτυπώνεται στις απαντήσεις που έδωσαν τα Κράτη – Μέλη της Σύμβασης για το Έγκλημα στον Κυβερνοχώρο τον Απρίλιο του 2016, και οι οποίες είναι διαθέσιμες εδώ: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806 51a6f

[107] Βλ. και Μήτρου Λ. (2015). *Προστασία Προσωπικών Δεδομένων και υπολογιστικό νέφος*. Στο Περιοδικό ΔιΜΕΕ, Τεύχος 4/2015, αλλά και Vaciago, G. (2011). *Remote forensics and cloud computing: an Italian and European legal overview*. Στο Digital Evidence & Elec. Signature L. Rev., 8, 124.

κρίσιμη για τον καθορισμό της δικαιοδοσίας στην ποινική διαδικασία, δεν φαίνεται πλέον να έχει σημασία και δημιουργεί ζητήματα όσον αφορά την αποτελεσματική διεξαγωγή της ποινικής διαδικασίας.[108]

Κάποιες φορές, η νόμιμη έρευνα στο πλαίσιο του αρχικού συστήματος που βασίζεται στο έδαφος διενέργειας της ποινικής έρευνας θα μπορούσε να επεκταθεί σε συνδεδεμένο σύστημα πληροφοριών του εξωτερικού χωρίς να υπάρχει σχετική επίγνωση ή σε περιπτώσεις στις οποίες δεν είναι σαφές σε ποιο έδαφος βρίσκεται το σύστημα πληροφοριών. Η κατάσταση αυτή μπορεί να οδηγήσει στην πράξη σε **διασυνοριακή πρόσβαση «χωρίς συγκατάθεση»** σε δεδομένα που βρίσκονται σε αλλοδαπή δικαιοδοσία, πράγμα που υπερβαίνει τις υπάρχουσες νομικές δυνατότητες (όπως λ.χ. το άρθρο 32β της «Σύμβασης της Βουδαπέστης για το Έγκλημα στον Κυβερνοχώρο» του Συμβουλίου της Ευρώπης). Η διαχείριση και η χρήση των δεδομένων που ανακτώνται με αυτόν τον τρόπο διέπονται από τις ρυθμίσεις της εθνικής νομοθεσίας και υπάγονται, ως εκ τούτου, σε ποικίλους κανόνες περί δικονομικών εγγυήσεων.[109]

Όπου τα τμήματα των δεδομένων που τηρεί ο πάροχος βρίσκονται σε διαφορετικές τοποθεσίες ή και χώρες, θα ήταν πρακτικά εφικτό να προσδιορίζεται η τοποθεσία όπου αυτά τα τμήματα δεδομένων **συνενώνονται**, ώστε, πριν τα στοιχεία δοθούν στις Αρχές Επιβολής του Νόμου (κατόπιν αιτήματος), να εξετάζεται η νομιμότητα του αιτήματος και η υποχρέωση ή μη του παρόχου για συμμόρφωση.

Τόπος και καθεστώς ιδιοκτησίας των ψηφιακών υποδομών – η περίπτωση των Η.Π.Α.

Είναι κοινώς αποδεκτό ότι οι Ηνωμένες Πολιτείες Αμερικής και οι εταιρίες με έδρα στις Η.Π.Α. διαδραματίζουν ηγετικό ρόλο στη λειτουργία του Διαδικτύου. Επομένως, το νομικό πλαίσιο των Η.Π.Α. έχει σημαντικό αντίκτυπο για την επιβολή του

---

[108] Αναλυτικά και στο υπ' αριθμ. 13689/15 από 04/11/2015 έγγραφο του Συμβουλίου της Ε.Ε. με θέμα «Collecting E-evidence in the digital age - the way forward - Preparation of the Council meeting (Justice Ministers)», διαθέσιμο εδώ: http://data.consilium.europa.eu/doc/document/ST-13689-2015-INIT/en/pdf

[109] Βλ. την έκθεση της Διασυνοριακής Ομάδας του Συμβουλίου της Ευρώπης, της 6ης Δεκεμβρίου 2012, με τίτλο: *Transborder access and jurisdiction: What are the options?* διαθέσιμη εδώ: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/TCY/TCY2013/TCYreports/TCY_2012_3_transborder_rep_V31public_7Dec12.pdf αλλά και παράρτημα του υπ' αριθμ. 14369/15 από 23/11/2015 εγγράφου του Συμβουλίου της Ευρώπης.

Νόμου στον τομέα του εγκλήματος στον κυβερνοχώρο. Πέραν του ζητήματος των αποκλίσεων μεταξύ των κανόνων περί προστασίας των δεδομένων, αυστηρά από προοπτική ποινικής δικαιοσύνης η κατάσταση αυτή έχει επίπτωση στο κριτήριο νομικής αιτιολόγησης που απαιτείται για τις αιτήσεις Α.Δ.Σ. που αποστέλλονται στις Η.Π.Α., ιδίως όταν πρόκειται για αιτήσεις που αφορούν δεδομένα περιεχομένου.

Κατά κανόνα σε όλες τις αιτήσεις Α.Δ.Σ. πρέπει να δηλώνεται το **έννομο συμφέρον** της αρμόδιας Αρχής η οποία ζητά τα οικεία δεδομένα. Σύμφωνα με την αμερικανική νομοθεσία, οι αιτήσεις πρέπει να αξιολογούνται με γνώμονα το κριτήριο της **«πιθανής αιτίας»**, που αποτελεί υψηλότερο κριτήριο αιτιολόγησης σε σύγκριση με το κριτήριο της **«εύλογης υπόνοιας»** ή το αντίστοιχό του. Το κριτήριο της «πιθανής αιτίας» περιορίζει τις παρεμβάσεις των αρμόδιων Αρχών στις απολύτως απαραίτητες για τη συγκεκριμένη έρευνα. Είναι πολύ πιθανό, επομένως, να απορριφθεί αίτηση Α.Δ.Σ. από τις αμερικανικές Αρχές διότι δεν πληροί την απαίτηση αιτιολόγησης με κριτήριο την «πιθανή αιτία». Πρέπει, επίσης, να διασφαλισθεί η σωστή εξισορρόπηση των δυνατοτήτων των αμερικανικών και αλλοδαπών Αρχών να αποκτούν πρόσβαση σε «τοπικά» αμερικανικά δεδομένα αφενός και σε κάθε άλλο είδος δεδομένων, αφετέρου.[110]

Η ενίσχυση του διαλόγου και με άλλες χώρες οι οποίες έχουν καίρια σημασία σε επίπεδο λειτουργίας και ιδιοκτησίας ψηφιακών υποδομών μείζονος σημασίας είναι κρίσιμη.

Υπολογιστικό νέφος & προκλήσεις νομικής φύσεως

Μετά τις γενικότερες προκλήσεις νομικής φύσεως που αφορούν τη διερεύνηση κυβερνοεγκλημάτων, στην παρούσα ενότητα θα επικεντρωθούμε στα ζητήματα νομικής φύσεως που ανακύπτουν κατά την εγκληματολογική ανάλυση ψηφιακών πειστηρίων λόγω της χρήσης της τεχνολογίας του υπολογιστικού νέφους.

Πρακτικά, στην εγκληματολογική ανάλυση ψηφιακών δεδομένων που βρίσκονται στο υπολογιστικό νέφος, αναφερόμαστε σε απομακρυσμένη ανάκτηση δεδομένων και αντιγραφή αυτών. Η ανάκτηση μπορεί να πραγματοποιηθεί από τον ερευνητή, ωστόσο, στην πλειονότητα των περιπτώσεων, σημαντικό τμήμα της διαδικασίας ανάκτησης

[110] Βλ. παράρτημα του υπ' αριθμ. 14369/15 από 23/11/2015 εγγράφου του Συμβουλίου της Ευρώπης, ενότητα 4

πραγματοποιείται από υπαλλήλους του παρόχου υπηρεσιών υπολογιστικού νέφους, κατόπιν αιτήματος των Αρχών Επιβολής του Νόμου.

Η απομακρυσμένη ανάκτηση δεδομένων διαφέρει εκ φύσεως από την κατάσχεση της συσκευής του υπόπτου για εγκληματολογική εξέταση. Ενώ στη δεύτερη περίπτωση γίνεται **κατάσχεση** ενός αντικειμένου, στην πρώτη περίπτωση δημιουργείται ένα **αντίγραφο των δεδομένων** που ενδιαφέρουν, κι εδώ ακριβώς ανακύπτουν ζητήματα σχετικά με τη νομιμότητα της αντιγραφής αυτής. Δε μπορεί να γραφτεί με βεβαιότητα αν αυτού του είδους η παραβίαση του απορρήτου συνιστά προσβολή της αξίας της ιδιοκτησίας των αντικειμένων που έχει στην κατοχή του ένας άνθρωπος, κατά το άρθρο 1 του Πρωτοκόλλου 1 της **Ευρωπαϊκής Σύμβασης των Δικαιωμάτων του Ανθρώπου** (ECHR)[111], ή της αξίας της ιδιωτικότητάς του, κατά το άρθρο 8 της Σύμβασης[112]. Η Σύμβαση για το Έγκλημα στον Κυβερνοχώρο αναφέρεται τόσο στην κατάσχεση όσο και στην αντιγραφή των δεδομένων, αν και δεν είναι ξεκάθαρο αν η διάκριση έχει νομικές συνέπειες. Ωστόσο, μια παλαιότερη σύσταση του Συμβουλίου της Ευρώπης πρότεινε την εφαρμογή της αρχής της ισότητας, σύμφωνα με την οποία τα δεδομένα που είναι λειτουργικά ισοδύναμα με ένα παραδοσιακό έγγραφο θα πρέπει να αντιμετωπίζονται ως το ίδιο για τους σκοπούς του δικονομικού δικαίου που διέπουν την έρευνα και την κατάσχεση.[113]

---

[111] Προστασία της ιδιοκτησίας - Άρθρον 1.- Παν φυσικόν ή νομικόν πρόσωπον δικαιούται σεβασμού της περιουσίας του. Ουδείς δύναται να στερηθή της ιδιοκτησίας αυτού ειμή δια λόγους δημοσίας ωφελείας και υπό τους προβλεπομένους, υπό του νόμου και των γενικών αρχών του διεθνούς δικαίου, όρους. Αι προαναφερόμεναι διατάξεις δεν θίγουσι το δικαίωμα παντός Κράτους όπως θέση εν ισχύϊ νόμους ους ήθελε κρίνει αναγκαίον προς ρύθμισιν της χρήσεως αγαθών συμφώνως προς το δημόσιον συμφέρον ή προς εξασφάλισιν της καταβολής φόρων ή άλλων εισφορών ή προστίμων.

[112] Δικαίωμα σεβασμού της ιδιωτικής και οικογενειακής ζωής Άρθρον 8.- 1. Παν πρόσωπον δικαιούται εις σεβασμόν της ιδιωτικής και οικογενειακής ζωής του, της κατοικίας του και της αλληλογραφίας του. 2. Δεν επιτρέπεται να υπάρξη επέμβασις δημοσίας αρχής εν τη ασκήσει του δικαιώματος τούτου, εκτός εάν η επέμβασις αύτη προβλέπεται υπό του νόμου και αποτελεί μέτρον το οποίον, εις μίαν δημοκρατικήν κοινωνίαν, είναι αναγκαίον δια την εθνικήν ασφάλειαν, την δημοσίαν ασφάλειαν, την οικονομικήν ευημερίαν της χώρας, την προάσπισιν της τάξεως και την πρόληψιν ποινικών παραβάσεων, την προστασίαν της υγείας ή της ηθικής, ή την προστασίαν των δικαιωμάτων και ελευθεριών άλλων.

[113] Walden, I. (2013). *Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent*. Στο Privacy and Security for Cloud Computing (pp. 45-71). Springer London.

Στο επίκεντρο μιας έρευνας των Αρχών Επιβολής του Νόμου μπορεί να βρεθούν τόσο οι χρήστες όσο και οι πάροχοι των υπηρεσιών υπολογιστικού νέφους, είτε μέσω της χρήσης συγκεκαλυμμένων τεχνικών έρευνας (όπως επιτήρηση ή καταγραφή δεδομένων επικοινωνίας), είτε με την άσκηση εξουσίας (διεξαγωγή νομότυπων ερευνών και κατασχέσεων), προκειμένου οι Αρχές να συλλέξουν ψηφιακά πειστήρια[114]. Λόγω της διαστρωμάτωσης των υπηρεσιών υπολογιστικού νέφους, οι Αρχές θα μπορούσαν να απευθύνουν ένα αίτημα αναφορικά με δεδομένα που ο χρήστης έχει εμπιστευτεί στον πάροχο των υπηρεσιών υπολογιστικού νέφους σε έναν πάροχο υποδομών υπολογιστικού νέφους (λ.χ. Amazon Web Services[115]), χωρίς ο πάροχος της υπηρεσίας υπολογιστικού νέφους (λ.χ. Dropbox[116]), ή ο χρήστης να ενημερωθούν για την ύπαρξη του αιτήματος.

Η συλλογή ψηφιακών πειστηρίων από ένα υπολογιστικό σύστημα, είτε αυτά είναι απλά αποθηκευμένα σε αυτό είτε βρίσκονται σε διαδικασία μετάδοσης, είναι μια ιδιαίτερη πρόκληση για τους ερευνητές. Ειδικά σε ότι αφορά το υπολογιστικό νέφος, οι προκλήσεις επικεντρώνονται σε τέσσερα (4) ζητήματα[117]:

- **Πολλαπλότητα:** Για λόγους απόδοσης, διαθεσιμότητας ή ύπαρξης αντιγράφων ασφαλείας (backup) των δεδομένων, ο πάροχος μπορεί να δημιουργήσει πολλαπλά αντίγραφα αυτών. Τα διάφορα αντίγραφα είναι πιθανό να αποθηκεύονται σε διάφορες εικονικές και φυσικές συσκευές, ακόμα και σε διαφορετικές τοποθεσίες. Πρακτικά, αυτό σημαίνει ότι όταν ένας πάροχος απαντά σε ένα αίτημα των Αρχών Επιβολής του Νόμου, μπορεί να απαιτείται να συλλέξει / συγκεντρώσει δεδομένα που βρίσκονται αποθηκευμένα σε διαφορετικές φυσικές τοποθεσίες.

[114] Οι χρήστες του υπολογιστικού νέφους εξαρτώνται από τους παρόχους των υπηρεσιών. Από αυτούς ξεχωρίζουμε τρεις κατηγορίες: (α) Ένας πάροχος υπηρεσιών υπολογιστικού νέφους που έχει άμεση σχέση με το συνδρομητή της υπηρεσίας, είτε προσφέροντας υπηρεσίες SaaS, είτε PaaS ή IaaS, (β) Ένας πάροχος υπηρεσιών υποδομών υπολογιστικού νέφους, που παρέχει σε έναν πάροχο υπηρεσιών υπολογιστικού νέφους κάποιας μορφής υποδομή, συμπεριλαμβανομένου του αποθηκευτικού χώρου, (γ) Ένας πάροχος υπηρεσιών επικοινωνίας, που παρέχει την υπηρεσία μετάδοσης επιτρέποντας το χρήστη των υπηρεσιών υπολογιστικού νέφους να επικοινωνήσει με τον πάροχο των υπηρεσιών.

[115] https://aws.amazon.com/

[116] https://www.dropbox.com/

[117] Walden, I. (2013). *Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent.* Στο Privacy and Security for Cloud Computing (pp. 45-71). Springer London.

- **Κατανεμημένη αποθήκευση:** Στην τεχνολογία υπολογιστικού νέφους χρησιμοποιούνται ευρέως τεχνικές όπως το «sharding»[118] ή το «partitioning»[119]. Αυτό σημαίνει ότι τα δεδομένα συχνά αποθηκεύονται τμηματικά σε διάφορες συσκευές, και δεν αποτελούν ένα ενιαίο, συμπαγές πακέτο δεδομένων. Συνδέονται δε λογικά και ανασκευάζονται όταν ο χρήστης ζητήσει να έχει πρόσβαση σε αυτά.
- **Προστατευμένα δεδομένα:** Ο χρήστης των υπηρεσιών υπολογιστικού νέφους μπορεί να υποβάλλει δεδομένα σε προστατευμένη μορφή, λ.χ. χρησιμοποιώντας τεχνικές κρυπτογράφησης, που καθιστούν αυτά «μη ορατά» στον πάροχο των υπηρεσιών. Συνεπώς, όταν οι Αρχές Επιβολής του Νόμου απευθύνουν αίτημα στον πάροχο των υπηρεσιών για παροχή στοιχείων, τότε ενδέχεται οι πληροφορίες που θα αποκτηθούν να είναι μη αξιοποιήσιμες. Επιπρόσθετα, ενδέχεται οι διάφοροι πάροχοι υπηρεσιών υπολογιστικού νέφους να εφαρμόζουν δικούς τους μηχανισμούς κρυπτογράφησης για τα δεδομένα που υποβάλλει ο χρήστης, κατά τη μετάδοση ή κατά την αποθήκευση. Και στην περίπτωση αυτή, για να είναι αξιοποιήσιμα (αναγνώσιμα) τα δεδομένα από τις Αρχές Επιβολής του Νόμου, θα πρέπει να αποκρυπτογραφηθούν.
- **Ταυτότητα:** Για έναν μεμονωμένο υπολογιστή μπορεί να είναι δύσκολο να πιστοποιηθεί η σχέση / διασύνδεση ανάμεσα στα δεδομένα, στην εικονική ταυτότητα του χρήστη και στην πραγματική ταυτότητά του. Τα εν λόγω προβλήματα είναι ακόμα πιο σύνθετα σε ένα περιβάλλον υπολογιστικού νέφους, όπου υφίσταται η ανάγκη σύνδεσης των δεδομένων που βρίσκονται στο νέφος, της συσκευής του χρήστη από την οποία δημιουργήθηκαν ή προσπελάστηκαν τα δεδομένα, της υπηρεσίας και του μεμονωμένου χρήστη.

---

[118] Με τον όρο «sharding» αναφερόμαστε σε ένα είδος τμηματοποίησης μιας βάσης δεδομένων, όπου μεγάλες βάσεις δεδομένων διαχωρίζονται σε μικρότερες, ώστε να είναι ταχύτερη και ευκολότερη η πρόσβαση στα δεδομένα τους. Βλ. και http://searchcloudcomputing.techtarget.com/definition/sharding

[119] Παρόμοια με το sharding, και το partitioning είναι αυτή ακριβώς η τμηματοποίηση δεδομένων, όπου μπορεί τα τμήματά τους να αποθηκεύονται σε διαφορετικούς υλικούς φορείς, αλλά υπάρχει λογική σύνδεση μεταξύ τους.

Στις πρώτες τρεις περιπτώσεις, το πρόβλημα έχει να κάνει με την πρόσβαση: εντοπισμός των σχετικών δεδομένων και μετατροπή τους σε μια αξιοποιήσιμη μορφή. Επαναλαμβάνουμε εδώ τη βασική αρχή της ψηφιακής εγκληματολογίας, σύμφωνα με την οποία τα δεδομένα που συλλέγονται από τις Αρχές Επιβολής του Νόμου θα πρέπει να παραμείνουν αναλλοίωτα κατά τη διάρκεια της διαδικασίας συλλογής αλλά και στα επόμενα στάδια. Μέχρι σήμερα χρησιμοποιείται ευρέως και θα εξακολουθήσει να προσφέρει πολύτιμα στοιχεία η ανάλυση των δεδομένων που συλλέγονται από τη σκοπιά του χρήστη. Όμως, διαφαίνεται ότι η ανάκτηση δεδομένων από το υπολογιστικό νέφος θα γίνει σταδιακά ο κανόνας. Κάτι τέτοιο αυξάνει τις πιθανότητες τροποποίησης (αλλοίωσης) των δεδομένων, ειδικά όπου η πρόσβαση γίνεται μέσω APIs[120] και αρχιτεκτονικών υπολογιστικού νέφους που είναι άγνωστες στον ερευνητή. Κατά συνέπεια, τίθεται υπό αμφισβήτηση η αξιοπιστία των ερευνητών όταν καταθέτουν ως μάρτυρες ενώπιων των εισαγγελικών και δικαστικών Αρχών περί της αυθεντικότητας της διαδικασίας απόκτησης, ειδικά όταν κάποιες εμφανείς αλλαγές στα δεδομένα οφείλονται σε δικές τους ενέργειες.

Έκθεση του ENISA «Exploring Cloud Incidents»

Ιδιαίτερο ενδιαφέρον παρουσιάζει η έκθεση του **ENISA** για τις νομικές προκλήσεις που αφορούν το υπολογιστικό νέφος.[121] Η έκθεση *«Exploring Cloud Incidents»* αναφέρεται ειδικά σε τρεις κατηγορίες νομικών προκλήσεων: αυτές που σχετίζονται με την εδαφική αρμοδιότητα και διασυνοριακή συνεργασία, αυτές που έχουν να κάνουν με τους όρους που αποδέχεται ο χρήστης για τη χρήση των υπηρεσιών υπολογιστικού νέφους και αυτές που αφορούν την αλληλουχία των σταδίων της διαδικασίας («chain of custody»).

Αξίζει να σημειωθεί ότι ο σκοπός του Ευρωπαϊκού Οργανισμού για την Ασφάλεια Πληροφοριών και Δικτύων (European Union Agency for Network and Information Security - ENISA[122]) δεν ταυτίζεται απόλυτα με αυτό των Αρχών Επιβολής του Νόμου, καθώς ο ENISA εστιάζει κατά βάση για την ψηφιακή θωράκιση οργανισμών και επιχειρήσεων, μέσω κυρίως της βελτίωση της συνεργασίας ανάμεσα στα εθνικά /

[120] Application Programming Interface δηλαδή Διεπαφή Προγραμματισμού Εφαρμογών

[121] ENISA (2016). *Exploring Cloud Incidents*. Διαθέσιμη εδώ: https://www.enisa.europa.eu/publications/exploring-cloud-incidents

[122] https://www.enisa.europa.eu/

κυβερνητικά CERTs (Computer Emergency Response Teams) / CSIRTs (Computer Security Incident Response Teams).

Ζητήματα διασυνοριακής φύσης και πολύ-εδαφικότητας

Στην έκθεση επισημαίνονται τα προβλήματα που ανακύπτουν στις περιπτώσεις όπου οι εξυπηρετητές και τα κέντρα δεδομένων των παρόχων βρίσκονται σε διάφορες τοποθεσίες ανά τον κόσμο, ιδίως λόγω και του περιορισμένου διαθέσιμου χρόνου των Αρχών Επιβολής του Νόμου.

Πρώτα απ' όλα, έχουν διαπιστωθεί αναποτελεσματικοί μηχανισμοί επικοινωνίας και συνεργασίας ανάμεσα στις Αρχές Επιβολής του Νόμου, τα εθνικά / κυβερνητικά CERTs και διάφορους άλλους δημόσιους φορείς. Προφανώς ούτε η ισχύουσα νομοθεσία βοηθά προς αυτή την κατεύθυνση.

Τα επίσημα αιτήματα, έπειτα, που αποστέλλονται στο πλαίσιο διασυνοριακής διερεύνησης μιας υπόθεσης, για πρόσβαση σε δεδομένα που έχουν αποθηκευτεί απομακρυσμένα υπόκεινται στην τοπική ισχύουσα νομοθεσία. Μόνο μετά την προσεκτική εξέταση του αιτήματος από τις αρμόδιες εθνικές Αρχές του Κράτους όπου βρίσκονται τα δεδομένα μπορεί να χορηγηθεί άδεια πρόσβασης σε αυτά.

Εν συνεχεία, δεν υφίσταται ενιαία **ρυθμιστικό πλαίσιο** για τις υποχρεώσεις των παρόχων υπηρεσιών υπολογιστικού νέφους σε σχέση με τις διαδικασίες λειτουργίας, τις αναγκαίες ενέργειες στις οποίες πρέπει να προβεί ένας πάροχος σε περίπτωση έρευνας, το χρονικό περιθώριο για συμμόρφωση (άμεσα, μέσα σε μια βδομάδα, μέσα σε ένα μήνα κ.λπ.) και σίγουρα τις διαδικασίες με τις οποίες ο πάροχος θα πρέπει να τηρεί, να διαχειρίζεται και να αποθηκεύει τα αρχεία καταγραφής (log files) των δεδομένων, ώστε να είναι διαθέσιμα και αξιοποιήσιμα στις Αρχές Επιβολής του Νόμου.

Εξάλλου, δεν υπάρχει καμία απολύτως συμφωνία ανάμεσα σε παρόχους υπηρεσιών υπολογιστικού νέφους, Αρχές Επιβολής του Νόμου και πελάτες για συνεργασία και συμμόρφωση στο πλαίσιο ερευνών σε σχετική περίπτωση.

Ακολούθως, για τις Αρχές Επιβολής του Νόμου που εμπλέκονται σε διασυνοριακές έρευνες, η νόμιμη πρόσβαση σε δεδομένα εξακολουθεί να αποτελεί μια σημαντική πρόκληση, λόγω των ορίων ισχύος της εθνικής νομοθεσίας, αλλά και λόγω των ιδιαίτερων

κανόνων που εφαρμόζουν ορισμένα Κράτη σχετικά με τη διασυνοριακή ροή δεδομένων και την προστασία της ιδιωτικότητας.[123]

Service Level Agreements για εγκληματολογική έρευνα και εξέταση

Στις περισσότερες των περιπτώσεων, στους όρους χρήσης μιας υπηρεσίας υπολογιστικού νέφους δε γίνεται αναφορά στις **προϋποθέσεις** και στις **διαδικασίες** που μπορεί να πραγματοποιηθεί μια εγκληματολογική εξέταση στο πλαίσιο μιας έρευνας των Αρχών Επιβολής του Νόμου. Οι πελάτες του παρόχου συχνά αγνοούν το θέμα της εγκληματολογικής εξέτασης, ενώ οι πάροχοι δεν εφαρμόζουν διαφανείς διαδικασίες ώστε να ορίζουν ξεκάθαρα τι θα περιλαμβάνεται και τι όχι στους όρους που αφορούν τις έρευνες των Αρχών. Όσο πιο ξεκάθαροι είναι οι όροι, τόσο λιγότερα εμπόδια θα ανακύπτουν κατά τη διάρκεια των ερευνών. Δυστυχώς, τέτοιοι όροι σπανίως περιλαμβάνονται. Κι αν ακόμα περιλαμβάνονται, δεν είναι αρκετά σαφείς ώστε να είναι κατανοητοί στους πελάτες.

Για τη διευκόλυνση των διαδικασιών εγκληματολογικών εξετάσεων, οι πάροχοι υπηρεσιών υπολογιστικού νέφους θα πρέπει να περιλαμβάνουν όρους και προϋποθέσεις στα συμβόλαια που συνάπτουν με τους πελάτες τους. Τουλάχιστον για την αντιμετώπιση των περισσότερων πρακτικών ζητημάτων που ανακύπτουν στις έρευνες, οι πάροχοι θα πρέπει να περιλαμβάνουν ρυθμίσεις σχετικές με την πρόσβαση στα δεδομένα και τις διαδικασίες εγκληματολογικής εξέτασης. Ενδεικτικά **πεδία αναφοράς** που πρέπει να περιλαμβάνονται είναι τα εξής:

- Ο τύπος της πρόσβασης που παρέχει ο πάροχος υπηρεσιών υπολογιστικού νέφους στους πελάτες και στους ερευνητές και η μέθοδος αυθεντικοποίησης για τους ερευνητές.
- Ο καθορισμός ρόλων και ευθυνών ανάμεσα στον πάροχο και στον πελάτη σε ότι αφορά την εγκληματολογική έρευνα και εξέταση.
- Οι διαδικασίες που θα ακολουθούνται σε περιπτώσεις εγκληματολογικής έρευνας και εξέτασης.

[123] Βλ. και Μήτρου Λ. (2015). *Προστασία Προσωπικών Δεδομένων και υπολογιστικό νέφος*. Στο Περιοδικό ΔιΜΕΕ, Τεύχος 4/2015.

- Οι χρονικές προθεσμίες σχετικά με την παράδοση των δεδομένων.
- Ο τύπος των μεταδεδομένων και των αρχείων καταγραφής που θα συλλέγονται.
- Τυχόν κόστος που προκύπτει (ποιες ενέργειες κοστίζουν και σχετίζονται με τις διαδικασίες εξέτασης;).
- Ποιος μπορεί να έχει πρόσβαση στα δεδομένα που συλλέγονται και υπό ποιες προϋποθέσεις.

Αλληλουχία των σταδίων (Chain of custody)

Για το ζήτημα, τέλος, της αλληλουχίας των σταδίων έχουμε ήδη αναφέρει αρκετά πράγματα νωρίτερα. Το πρόβλημα στη συγκεκριμένη περίπτωση, που έχει να κάνει με την αποδεικτική διαδικασία ενώπιον του δικαστηρίου, είναι ότι **δεν υπάρχουν (πιστοποιημένα) εργαλεία** που μπορούν να χρησιμοποιηθούν από τους εκπροσώπους των Αρχών Επιβολής του Νόμου για να αποδείξουν ότι τα δεδομένα που παρουσιάζονται στο δικαστήριο είναι όλα εκείνα που ανήκαν στον ύποπτο και τελικά συλλέχθηκαν. Σε ορισμένες περιπτώσεις, βέβαια, στο Ηνωμένο Βασίλειο και στην Ιρλανδία, δικαστήρια έκαναν αποδεκτά τα πειστήρια που συλλέχθηκαν από το υπολογιστικό νέφος, όταν οι ερευνητές – εκπρόσωποι των Αρχών Επιβολής του Νόμου απέδειξαν ότι εφαρμόστηκαν προσεκτικά και με διαφανείς διαδικασίες οι τεχνικές συλλογής και οι βέλτιστες πρακτικές.

Σύνοψη

Η μετάβαση σε διαδικασίες απομακρυσμένης ανάκτησης δεδομένων συνεπάγεται αύξηση της εξάρτησης των Αρχών Επιβολής του Νόμου από τους παρόχους υπηρεσιών υπολογιστικού νέφους. Εναλλακτικά, η πρόσβαση στα δεδομένα θα μπορούσε να επιτευχθεί μέσω της συσκευής πρόσβασης του χρήστη, υπόπτου ή όχι, με ή χωρίς τη συγκατάθεσή του. Είτε με τον έναν, είτε με τον άλλο τρόπο, η τοποθεσία των δεδομένων και κατ' επέκταση η φυσική τοποθεσία των υπολογιστικών συστημάτων όπου αυτά φιλοξενούνται κατά τη στιγμή που ανακτώνται για τους σκοπούς της έρευνας, ενδέχεται να μην είναι γνωστή ή να μη μπορεί να προσδιοριστεί. Άρα, η «απώλεια της τοποθεσίας» μπορεί να έχει σοβαρό αντίκτυπο στην άσκηση των εξουσιών των Αρχών Επιβολής του Νόμου και στην αποδεικτική ισχύ των δεδομένων που προκύπτουν από το υπολογιστικό νέφος. Εξίσου σημαντικό πρόβλημα ανακύπτει από την ανομοιογένεια της ισχύουσας

νομοθεσίας σε ευρωπαϊκό και διεθνές επίπεδο, ειδικά σε ζητήματα προστασίας δεδομένων προσωπικού χαρακτήρα και προστασίας του απορρήτου επικοινωνιών.

❑

Κεφάλαιο 5: Επίλογος

Σύνοψη – συμπεράσματα

Μετά από όσα παρατέθηκαν νωρίτερα, κατέστη προφανές ότι η εγκληματολογική ανάλυση δεδομένων που βρίσκονται αποθηκευμένα στο υπολογιστικό νέφος επηρεάζεται από μια αρκετά μεγάλη λίστα παραγόντων. Κατ' αυτό τον τρόπο επηρεάζεται ακολούθως η ποιότητα των πειστηρίων που συλλέγονται και άρα και η αξιοπιστία και το παραδεκτό τους ενώπιον των εισαγγελικών και δικαστικών Αρχών, όταν εξετάζεται η ενοχή ή η αθωότητα του κατηγορουμένου.

Αν πρέπει να ξεχωρίσουμε ορισμένες παραμέτρους που δυσχεραίνουν τη διερεύνηση κυβερνοεγκλημάτων και την εγκληματολογική εξέταση σε περιβάλλοντα υπολογιστικού νέφους, τότε σίγουρα η πρώτη σχετίζεται με την **κοινή χρήση φυσικών εξυπηρετητών από πολλούς πελάτες**, αλλά και υλικού και λογισμικού, ακόμα και ταυτόχρονα. Η παραπάνω κατάσταση είναι ο κανόνας – υπάρχουν όμως κι εξαιρέσεις. Εξαιτίας αυτής της κατάστασης, ο ερευνητής δυσκολεύεται να «αποδώσει» συγκεκριμένες δραστηριότητες (π.χ. δημιουργία, τροποποίηση, διαγραφή αρχείων κ.λπ.) σε συγκεκριμένους χρήστες. Μάλιστα, όταν πρόκειται για κοινά χρησιμοποιούμενο αποθηκευτικό χώρο, ένας πάροχος υπηρεσιών υπολογιστικού νέφους είναι επιφυλακτικός ως προς την παροχή πρόσβασης σε έναν ερευνητή στον εν λόγω πόρο, καθώς σε αυτόν μπορεί να περιέχονται δεδομένα που ανήκουν σε άλλους πελάτες. Η πρόσβαση στα δεδομένα τρίτων είναι ένα εξαιρετικά σοβαρό ζήτημα, που σχετίζεται τόσο με θέματα ασφάλειας (εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα), όσο και με θέματα ιδιωτικότητας, η παραβίαση των οποίων συνήθως τιμωρείται αυστηρά με βάση την ισχύουσα εθνική νομοθεσία.

Μια δεύτερη παράμετρος σχετίζεται με την έννοια της **πολύ-δικαιοδοσίας** ή αλλιώς **«απώλεια τοποθεσίας»**. Ο προσδιορισμός της «τοπικής» αρμοδιότητας των Αρχών ενός Κράτους να παρέμβουν (να προσπελάσουν, να δημιουργήσουν αντίγραφα κ.λπ.) σε δεδομένα που βρίσκονται αποθηκευμένα στο υπολογιστικό νέφος, χωρίς να είναι γνωστή ή να μη μπορεί να προσδιοριστεί η φυσική τους τοποθεσία, είναι ένα εξαιρετικά σημαντικό πρόβλημα. Μάλιστα, αποκτά ακόμα μεγαλύτερη διάσταση αν συνυπολογίσουμε το γεγονός ότι η νομοθεσία γύρω από το απόρρητο της επικοινωνίας και

την προστασία των δεδομένων προσωπικού χαρακτήρα διαφέρει συχνά από χώρα σε χώρα.

Η **αλληλουχία των σταδίων της εξέτασης (chain of custody)** είναι η τρίτη παράμετρος που απαιτεί προσοχή από τους ερευνητές. Η σημασία της είναι τεράστια, καθώς μέσω της αναλυτικής καταγραφής και περιγραφής όλων των κινήσεων των ερευνητών διασφαλίζεται η αξιοπιστία της μεθόδου που ακολουθήθηκε και η παραδοχή της από τις εισαγγελικές και δικαστικές Αρχές. Σε μια παραδοσιακή εγκληματολογική εξέταση ψηφιακών πειστηρίων ο ερευνητής έχει από την αρχή τον έλεγχο της κατάστασης. Από την άλλη πλευρά, σε περιβάλλον υπολογιστικού νέφους απαιτείται μια αρκετά διαφορετική προσέγγιση: απομακρυσμένη πρόσβαση σε έναν εξυπηρετητή, με τρόπο που δε θα αλλοιώνονται τα δεδομένα που συλλέγονται, ώστε να παρουσιαστούν στη συνέχεια σε μια δικαστική διαδικασία. Μπορεί, επιπλέον, ο ερευνητής να μην έχει απευθείας πρόσβαση στα δεδομένα που επιθυμεί και να αναγκαστεί να αναζητήσει τη συμβολή υπαλλήλων του παρόχου υπηρεσιών υπολογιστικού νέφους προκειμένου να τα καταφέρει, κάτι που εμπλέκει τρίτους στην αλληλουχία των σταδίων.

Τελευταία άξια αναφοράς παράμετρος είναι αυτή που σχετίζεται με τους **όρους χρήσης των υπηρεσιών** υπολογιστικού νέφους (Service Level Agreements). Αρκετά συχνά απουσιάζει από τους όρους της συμφωνίας ανάμεσα στον πάροχο των υπηρεσιών και στον πελάτη η αναγκαία αναφορά στις διατάξεις σχετικά με τις διαδικασίες εγκληματολογικής εξέτασης που θα ακολουθηθούν, εφόσον προκύψει ανάγκη. Πολλά από τα εμπόδια που παρατέθηκαν στα προηγούμενα κεφάλαια θα μπορούσαν να προσπεραστούν εφόσον στους όρους της συμφωνίας εμπεριέχονταν ρητές διατάξεις για το πώς θα αντιμετωπίζεται η κάθε κατάσταση (λ.χ. ατοπικότητα, πρόσβαση σε δεδομένα προσωπικού χαρακτήρα, απόρρητο επικοινωνίας κ.λπ.). Οι επιλογές του πελάτη, προς το παρόν τουλάχιστον, είναι περιορισμένες, αφού είτε θα πρέπει να δεχθεί τους όρους που θέτει ο πάροχος, είτε να απορρίψει τις υπηρεσίες του.

Ζητήματα που απαιτούν περαιτέρω έρευνα & μελέτη

Στην παρούσα ενότητα παραθέτουμε ορισμένα ζητήματα που θεωρούμε ότι χρήζουν περαιτέρω έρευνας και μελέτης.

Επισημαίνεται, ωστόσο, ότι όλα τα τεχνικής και νομικής φύσεως ζητήματα, που αναφέρθηκαν στα κεφάλαια 2 έως 4, απασχολούν ήδη την ακαδημαϊκή και επιστημονική κοινότητα.

Εργαλεία για την εγκληματολογική εξέταση & χρονοσφραγίδες

Δεν υπάρχουν, προς το παρόν, εργαλεία (λογισμικά) εγκληματολογικής εξέτασης προοριζόμενα για αποκλειστική χρήση σε περιβάλλον υπολογιστικού νέφους. Οι ερευνητές αξιοποιούν τα εργαλεία που χρησιμοποιούνται κατά τις παραδοσιακές έρευνες. Συνεπώς, απαιτείται η εστίαση στις μελέτες γύρω από τη δημιουργία και δοκιμή εργαλείων που θα χρησιμοποιούνται σε περιβάλλον υπολογιστικού νέφους κατά την εγκληματολογική εξέταση, ιδίως εργαλεία για live ανάλυση του δυναμικού περιβάλλοντος που κυριαρχεί στο υπολογιστικό νέφος[124], αλλά και εργαλεία μέσω των οποίων θα μπορούσαν να σημανθούν με μη αλληλοσυγκρουόμενες χρονοσφραγίδες τα δεδομένα που κινούνται στο νέφος (κυρίως λόγω διαφοράς ζώνης ώρας, ή χρησιμοποιούμενης ώρας).[125]

Διαφάνεια στους πάροχους υπηρεσιών υπολογιστικού νέφους

Ο τρόπος οργάνωσης και οι υποδομές ενός παρόχου υπηρεσιών επηρεάζουν, χωρίς αμφιβολία, τις έρευνες από την πλευρά ενός ειδικού ερευνητή ασφαλείας ή των Αρχών Επιβολής του Νόμου. Οι περιορισμένες έως μηδενικές γνώσεις γύρω από τις «εσωτερικές» δομές και διαδικασίες ενός παρόχου μόνο προβλήματα μπορούν να δημιουργήσουν κατά την έρευνα. Ο αντίλογος είναι ότι ένας πάροχος δεν επιθυμεί να είναι γνωστά στο ευρύ κοινό τα παραπάνω, είτε γιατί θέλει να προστατεύσει τα δεδομένα που του εμπιστεύεται ο πελάτης του, είτε τις ίδιες του τις υποδομές από τους κυβερνοεγκληματίες ή άλλους ανταγωνιστικούς παρόχους.

Σε κάθε περίπτωση, ένας πάροχος υπηρεσιών υπολογιστικού νέφους δε μπορεί να λειτουργεί χωρίς κανένα έλεγχο. Το ίδιο, όμως, κι ένας πελάτης. Θα πρέπει να μελετηθεί νομικής φύσεως πρόβλεψη ώστε και οι δύο πλευρές, πάροχος και πελάτης, να μπορούν να υπόκεινται σε έλεγχο – από ένα τρίτο μέρος –, προκειμένου να διαπιστωθεί, εφόσον προκύψει ανάγκη, ποια πλευρά παραβίασε όρους της συμφωνίας ή ευθύνεται για ένα συμβάν (απώλεια ή διαρροή δεδομένων κ.λπ.).[126]

---

[124] Lalas, E., Mitrou, L., & Lambrinoudakis, C. (2013, August). *Procave: Privacy-preserving collection and authenticity validation of online evidence*. Στο International Conference on Trust, Privacy and Security in Digital Business (pp. 137-148). Springer Berlin Heidelberg.

[125] Βλ. και Marangos, N., Rizomiliotis, P., & Mitrou, L. (2014). *Time synchronization: pivotal element in cloud forensics*. Security and Communication Networks.

[126] Βλ. O'Shaughnessy, S., & Keane, A. (2013, January). *Impact of cloud computing on digital forensic investigations*. Στο IFIP International Conference on Digital Forensics (pp. 291-303). Springer Berlin αλλά

Service Level Agreements

Οι όροι χρήσης μιας υπηρεσίας υπολογιστικού νέφους θα πρέπει να περιλαμβάνουν σαφείς και ακριβείς διαδικαστικές πληροφορίες σχετικά με το πώς θα γίνεται μια εγκληματολογική έρευνα από έναν ερευνητή και από έναν πάροχο υπηρεσιών cloud, μετά από ένα συμβάν (περιστατικό ή έγκλημα). Οι ρόλοι πρέπει να ορίζονται με σαφήνεια και κάθε πλευρά πρέπει να έχει πλήρη επίγνωση των ευθυνών, των δυνατοτήτων και των περιορισμών της. Επιπλέον, στους όρους χρήσης θα πρέπει να καθορίζονται επακριβώς οι τρόποι αντιμετώπισης των νομικής φύσεως ζητημάτων κατά τη διάρκεια μιας έρευνας σε περιβάλλον υπολογιστικού νέφους, αφενός σε σχέση με τους άλλους χρήστες της υπηρεσίας και αφετέρου σε σχέση με τις Αρχές Επιβολής του Νόμου άλλων κρατών (ζητήματα δικαιοδοσίας).[127]

Forensics-as-a-Service (εγκληματολογική εξέταση ως υπηρεσία)

Μια υπηρεσία, τέλος, που θα μπορούσε να προσφέρεται από τον πάροχο υπηρεσιών υπολογιστικού νέφους θα ήταν το Forensics-as-a-Service (FaaS), δηλαδή η εγκληματολογική εξέταση ως υπηρεσία. Με άλλα λόγια, ο πάροχος υπηρεσιών cloud θα διευκόλυνε σημαντικά τις έρευνες των Αρχών Επιβολής του Νόμου αν αναλάμβανε την ευθύνη της συλλογής ψηφιακών πειστηρίων ή τουλάχιστον υποστήριζε με εξειδικευμένο προσωπικό τη διαδικασία συλλογής πειστηρίων σε συνεργασία με τις ΑΕΝ. Ένας πάροχος είναι σε θέση να διατηρεί και να συλλέγει δεδομένα καθώς ελέγχει πλήρως την υποδομή του, τα εικονικά του μηχανήματα (virtual machines), τα αρχεία καταγραφής (log files), τη πακέτα δεδομένων και τις οικονομικές συναλλαγές των πελατών του. Μια τέτοια υπηρεσία, η υλοποίηση της οποίας δεν είναι πολύπλοκη, θα διασφάλιζε υψηλής ποιότητας παροχές προς τους πελάτες, αλλά και υψηλής ακρίβειας αποτελέσματα που θα μπορούσαν να χρησιμοποιηθούν στην ποινική διαδικασία.[128]

και Haeberlen, A. (2010). *A case for the accountable cloud*. Στο ACM SIGOPS Operating Systems Review, 44(2), 52-57.

[127] Ruan, K., Carthy, J., Kechadi, T., & Crosbie, M. (2011, January). *Cloud forensics*. Στο IFIP International Conference on Digital Forensics (pp. 35-46). Springer Berlin Heidelberg.

[128] O'Shaughnessy, S., & Keane, A. (2013, January). *Impact of cloud computing on digital forensic investigations*. Στο IFIP International Conference on Digital Forensics (pp. 291-303). Springer Berlin

Εν κατακλείδι

Κλείνοντας, αξίζει να τονιστεί ότι η ταχύτατη εξέλιξη της τεχνολογίας υπολογιστικού νέφους σε συνδυασμό με την κατακόρυφη αύξηση της δημοφιλίας της διαμορφώνει νέες προκλήσεις στα πεδία της διερεύνησης (investigation) κυβερνοεγκλημάτων και της εγκληματολογική ανάλυσης (forensics). Πολλές από τις ήδη υπάρχουσες προκλήσεις κατά τη διερεύνηση κυβερνοεγκλημάτων γίνονται ακόμα εντονότερες λόγω της φύσης του υπολογιστικού νέφους (λ.χ. απώλεια τοποθεσίας), παράλληλα, ωστόσο, διαμορφώνονται οι συνθήκες για να αναδειχθούν νέες προσεγγίσεις, μέθοδοι και τεχνικές από την πλευρά των ερευνητών. Το ίδιο, άλλωστε, συμβαίνει και σε πολλές άλλες εκφάνσεις της ζωής μας: προκλήσεις, ευκαιρίες και ένας διαρκής αγώνας του νομοθέτη να προλάβει τις τεχνολογικές εξελίξεις ή έστω να προσαρμοστεί σε αυτές.

❑

Βιβλιογραφία – Πηγές

Α. Βιβλία – Μονογραφίες

- Chawki, M. (2005). *A Critical Look at the Regulation of Cybercrime: A Comparative Analysis with Suggestions for Legal Policy*, DROIT-TIC
- Maguire, M., Okada, D. (2014). *Critical Issues in Crime and Justice: Thought, Policy, and Practice*, SAGE Publications, chapter 14

Β. Κεφάλαια σε βιβλία

- Carlin, S., & Curran, K. (2011). *Cloud computing security.* Στο Pervasive and Ubiquitous Technology Innovations for Ambient Intelligence Environments, pp. 14-15
- Grispos, G., Storer, T., & Glisson, W. B. (2013). *Calm before the storm: the challenges of cloud.* Στο Emerging digital forensics applications for crime detection, prevention, and security, 4, 28-48.
- Walden, I. (2013). *Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent.* Στο Privacy and Security for Cloud Computing (pp. 45-71). Springer London.

Γ. Δημοσιεύσεις σε Επιστημονικά Περιοδικά

- Armbrust, M. et al., (2010). *A view of cloud computing.* Στο Communications of the ACM, 53(4), pp. 50-58
- Broadhurst, R. (2006). *Developments in the global law enforcement of cyber-crime.* Στο Policing: An International Journal of Police Strategies & Management, 29(3), 408-433
- Casey, E. (2002). *Practical approaches to recovering encrypted digital evidence.* Στο International Journal of Digital Evidence, 1(3), 1-26
- Chowdhury, N. M. K., & Boutaba, R. (2009*). Network virtualization: state of the art and research challenges.* Στο IEEE Communications magazine, 47(7), 20-26

- Dhage, S. N., & Meshram, B. B. (2012). *Intrusion detection system in cloud computing environment.* Στο International Journal of Cloud Computing, 1(2-3), 261-282
- Ghemawat, S., Gobioff, H., & Leung, S. T. (2003). *The Google file system.* Στο ACM SIGOPS operating systems review (Vol. 37, No. 5, pp. 29-43). ACM
- Haeberlen, A. (2010). *A case for the accountable cloud.* Στο ACM SIGOPS Operating Systems Review, 44(2), 52-57.
- Jawad Abbas, T. (2015). *Studying the Documentation Process in Digital Forensic Investigation Frameworks / Models*. Στο Journal of Al-Nahrain University Vol.18 (4), December, 2015, pp.153-162
- Kotzanikolaou, P. (2008). *Data retention and privacy in electronic communications.* Στο IEEE Security & Privacy, 6(5)
- Lalas, E., Mitrou, L., & Lambrinoudakis, C. (2013, August). *Procave: Privacy-preserving collection and authenticity validation of online evidence*. Στο International Conference on Trust, Privacy and Security in Digital Business (pp. 137-148). Springer Berlin Heidelberg.
- Marangos, N., Rizomiliotis, P., & Mitrou, L. (2014). *Time synchronization: pivotal element in cloud forensics.* Security and Communication Networks.
- Martini, B., & Choo, K. K. R. (2012). *An integrated conceptual digital forensic framework for cloud computing.* Στο Digital Investigation, 9(2), 71-80
- Μήτρου Λ. (2015). *Προστασία Προσωπικών Δεδομένων και υπολογιστικό νέφος*. Στο Περιοδικό ΔιΜΕΕ, Τεύχος 4/2015
- Povar, D., Saibharath, & Geethakumari, G. (2015). *Real-time digital forensic triaging for cloud data analysis using MapReduce on Hadoop framework.* Στο International Journal of Electronic Security and Digital Forensics, 7(2), 119-133
- Prayudi, Y., & Sn, A. (2015). *Digital Chain of Custody: State of the Art*. Στο International Journal of Computer Applications, 114(5)
- Quick, D., & Choo, K. K. R. (2013). *Forensic collection of cloud storage data: Does the act of collection result in changes to the data or its metadata?*. Στο Digital Investigation, 10(3), 266-277

- Roscini, M. (2016). *Digital evidence as a means of proof before the International Court of Justice.* Στο Journal of Conflict and Security Law, 21
- Taylor, M., Haggerty, J., Gresty, D., & Lamb, D. (2011). *Forensic investigation of cloud computing systems*. Στο Network Security, 2011(3), 4-10
- Vaciago, G. (2011). *Remote forensics and cloud computing: an Italian and European legal overview.* Στο Digital Evidence & Elec. Signature L. Rev., 8, 124
- Wang, S. J. (2007). *Measures of retaining digital evidence to prosecute computer-based cyber-crimes*. Στο Computer Standards & Interfaces, 29(2), 216-223
- Yusoff, Y., Ismail, R., & Hassan, Z. (2011). *Common phases of computer forensics investigation models.* Στο International Journal of Computer Science & Information Technology, 3(3), 17-31

Δ. Δημοσιεύσεις σε Πρακτικά Συνεδρίων

- Agudo, I., Nuñez, D., Giammatteo, G., Rizomiliotis, P., & Lambrinoudakis, C. (2011). *Cryptography goes to the cloud.* Στο FTRA International Conference on Secure and Trust Computing, Data Management, and Application (pp. 190-197). Springer Berlin Heidelberg
- Alkaabi, Ali, Mohay, George M., McCullagh, Adrian J., & Chantler, Alan N. (2010). *Dealing with the problem of cybercrime*. Στο Baggili, Ibrahim (Ed.) Conference Proceedings of 2nd International ICST Conference on Digital Forensics & Cyber Crime, ICST, Abu Dhabi.
- Birk, D., & Wegener, C. (2011). *Technical issues of forensic investigations in cloud computing environments.* Στο Systematic Approaches to Digital Forensic Engineering (SADFE), 2011 IEEE Sixth International Workshop on (pp. 1-10). IEEE.
- Chow, R., Golle, P., Jakobsson, M., Shi, E., Staddon, J., Masuoka, R., & Molina, J. (2009, November). *Controlling data in the cloud: outsourcing computation without outsourcing control.* Στο Proceedings of the 2009 ACM workshop on Cloud computing security (pp. 85-90). ACM.

- Ćosić, J., & Bača, M. (2010, January). *(Im) proving chain of custody and digital evidence integrity with time stamp.* Στο MIPRO–Proceedings of the 33rd International Convention (pp. 1226-1230)
- Delport, W., Köhn, M., & Olivier, M. S. (2011). *Isolating a cloud instance for a digital forensic investigation.* Στο ISSA.
- Guo, H., Jin, B., & Shang, T. (2012, August). *Forensic investigations in cloud environments.* Στο Computer Science and Information Processing (CSIP), 2012 International Conference on (pp. 248-251). IEEE.
- Hershensohn, J., & Block, D. (2005). *IT Forensics: the collection of and presentation of digital evidence.* Στο ISSA (pp. 1-14)
- Karyda, M., & Mitrou, L. (2007, August). *Internet forensics: Legal and technical issues.* Στο Digital Forensics and Incident Analysis, 2007. WDFIA 2007. Second International Workshop on (pp. 3-12). IEEE.
- Lee, S., Kim, H., Lee, S., & Lim, J. (2005, November). *Digital evidence collection process in integrity and memory information gathering.* Στο First International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE'05) (pp. 236-247). IEEE.
- O'Shaughnessy, S., & Keane, A. (2013, January). *Impact of cloud computing on digital forensic investigations.* Στο IFIP International Conference on Digital Forensics (pp. 291-303). Springer Berlin
- Richter, J., Kuntze, N., & Rudolph, C. (2010, May). *Security digital evidence.* Στο Systematic Approaches to Digital Forensic Engineering (SADFE), 2010 Fifth IEEE International Workshop on (pp. 119-130). IEEE.
- Rogers, M. K., Goldman, J., Mislan, R., Wedge, T., & Debrota, S. (2006, January). *Computer forensics field triage process model.* Στο Proceedings of the conference on Digital Forensics, Security and Law (p. 27). Association of Digital Forensics, Security and Law.
- Roschke, S., Cheng, F., & Meinel, C. (2009). *Intrusion detection in the cloud.* Στο Dependable, Autonomic and Secure Computing, 2009. DASC'09. Eighth IEEE International Conference on (pp. 729-734). IEEE.

- Ruan, K., Carthy, J., Kechadi, T., & Crosbie, M. (2011, January). *Cloud forensics*. Στο IFIP International Conference on Digital Forensics (pp. 35-46). Springer Berlin Heidelberg.
- Ruan, K., James, J., Carthy, J., & Kechadi, T. (2012, January). *Key terms for service level agreements to support cloud forensics.* Στο IFIP International Conference on Digital Forensics (pp. 201-212). Springer Berlin Heidelberg.
- Simou, S., Kalloniatis, C., Kavakli, E., & Gritzalis, S. (2014, June). *Cloud forensics: identifying the major issues and challenges.* Στο International Conference on Advanced Information Systems Engineering (pp. 271-284). Springer International Publishing
- Thorpe, S., Ray, I., Grandison, T., & Barbir, A. (2012, July). *Cloud log forensics metadata analysis.* Στο Computer Software and Applications Conference Workshops (COMPSACW), 2012 IEEE 36th Annual (pp. 194-199). IEEE
- Wolthusen, S. D. (2009, September). *Overcast: Forensic discovery in cloud environments.* Στο IT Security Incident Management and IT Forensics, 2009. IMF'09. Fifth International Conference on (pp. 3-9). IEEE.
- Zargari, S., & Benford, D. (2012). *Cloud forensics: Concepts, issues, and challenges.* Στο Emerging Intelligent Data and Web Technologies (EIDWT), 2012 Third International Conference on (pp. 236-243). IEEE.

Ε. Εκθέσεις – Έρευνες – Κείμενα Εργασίας

- Cloud Evidence Group - Cybercrime Convention Committee
    - T-CY(2012)3 Transborder access and jurisdiction: What are the options?
    - T-CY(2015)10 Criminal justice access to data in the cloud: challenges
    - T-CY(2015)16 Draft Guidance Note on Production Orders (Article 18) - Version 4 May 2016 - Version 15 September 2016 - Version 15 November 2016 (16th T-CY Plenary)
    - T-CY(2016)2 Criminal justice access to data in the cloud: cooperation with "foreign" service providers

- TCY(2016)5 Criminal justice access to data in the cloud: Recommendations for consideration by the T-CY
- TCY(2016)7 Criminal justice access to electronic evidence in the cloud - Informal summary of issues and options under consideration by the Cloud Evidence Group
- T-CY(2016)13 - Emergency requests for the immediate disclosure of data stored in another jurisdiction through mutual legal assistance channels or through direct requests to service providers: Compilation of replies

- ENISA (2016). Exploring Cloud Incidents
  - https://www.enisa.europa.eu/publications/exploring-cloud-incidents
- ENISA (2012). *The Fight against Cybercrime - Cooperation between CERTs and Law Enforcement Agencies to fight against cybercrime - A first collection of practices*
  - https://www.enisa.europa.eu/publications/cooperation-between-certs-and-law-enforcement-agencies-in-the-fight-against-cybercrime-a-first-collection-of-practices
- Eurojust. (2014). *Report of the Strategic Meeting on Cybercrime 19-20 November 2014*
  - http://www.eurojust.europa.eu/doclibrary/Eurojust-framework/ejstrategicmeetings/Eurojust%20Strategic%20Meeting%20on%20Cybercrime,%20November%202014/Report-Strategic-Seminar-Cybercrime_2014-11-20_EN.pdf
- Kaspersky (2015). *Kaspersky Security Bulletin 2015. Overall statistics for 2015*
  - https://securelist.com/analysis/kaspersky-security-bulletin/73038/kaspersky-security-bulletin-2015-overall-statistics-for-2015/
- Συμβούλιο της Ε.Ε.
  - Υπ' αριθμ. 13689/15 από 04/11/2015 έγγραφο. *Collecting E-evidence in the digital age - the way forward - Preparation of the Council meeting (Justice Ministers).*

- http://data.consilium.europa.eu/doc/document/ST-13689-2015-INIT/en/pdf

ΣΤ. Εγχειρίδια – Επαγγελματικοί Οδηγοί

- Association of Chief Police Officers (ACPO). *Good Practice Guide for Computer-Based Electronic Evidence*. Διαθέσιμο στο https://www.cps.gov.uk/legal/assets/uploads/files/ACPO_guidelines_computer_evidence[1].pdf
- Massachusetts Digital Evidence Consortium, (2015). *Digital Evidence Guide for First Responders*. Διαθέσιμο στο http://www.iacpcybercenter.org/wp-content/uploads/2015/04/digitalevidence-booklet-051215.pdf
- Mell, P., Grance, T., (2011). *The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology*, Special Publication 800-145. Διαθέσιμο στο http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf
- National Institute of Standards and Technology (NIST). *Guide to Integrating Forensic Techniques into Incident Response.* Διαθέσιμο στο http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf
- NIST. *Guide to Intrusion Detection and Prevention Systems (IDPS).* Διαθέσιμο στο http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf (έκδοση του 2007) και στο http://csrc.nist.gov/publications/drafts/800-94-rev1/draft_sp800-94-rev1.pdf (αναθεωρημένη έκδοση draft του 2012).
- Scientific Working Group on Digital Evidence (SWGDE). *Proposed Standards for the Exchange of Digital Evidence.* Διαθέσιμο στο https://archives.fbi.gov/archives/about-us/lab/forensic-science-communications/fsc/april2000/swgde.htm

Ζ. Νομικά κείμενα

- Χάρτης Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης. Διαθέσιμος στο http://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex:12016P/TXT
- Πράξη του Συμβουλίου, της 29ης Μαΐου 2000, για την κατάρτιση, σύμφωνα με το άρθρο 34 της συνθήκης για την Ευρωπαϊκή Ένωση, της σύμβασης για την

αμοιβαία δικαστική συνδρομή επί ποινικών υποθέσεων μεταξύ των κρατών μελών της Ευρωπαϊκής Ένωσης (2000/C 197/01). Διαθέσιμη στο http://eur-lex.europa.eu/legal-content/el/TXT/?uri=CELEX:C2000/197/01

- Ανακοίνωση της Επιτροπής προς το Ευρωπαϊκό Κοινοβούλιο, το Συμβούλιο και την Ευρωπαϊκή Επιτροπή των Περιφερειών προς την κατεύθυνση γενικής πολιτικής σχετικά με την καταπολέμηση του εγκλήματος στον κυβερνοχώρο {SEC(2007) 641}{SEC(2007) 642}, Διαθέσιμη στο http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52007DC0267
- Οδηγία 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 12ης Αυγούστου 2013 για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης-πλαισίου 2005/222/ΔΕΥ του Συμβουλίου. Διαθέσιμη στο http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:EN:PDF
- Οδηγία 2014/41/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 3ης Απριλίου 2014, περί της ευρωπαϊκής εντολής έρευνας σε ποινικές υποθέσεις. Διαθέσιμη στο http://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX:32014L0041
- Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων). Διαθέσιμος στο http://eur-lex.europa.eu/legal-content/EL/TXT/?uri=CELEX%3A32016R0679
- Απόφαση στις συνεκδικασθείσες υποθέσεις C-203/15 Tele2 Sverige AB κατά Post - och telestyrelsen και C-698/15 Secretary of State for the Home Department κατά Tom Watson κ.λπ. Διαθέσιμη εδώ http://curia.europa.eu/juris/documents.jsf?num=C-203/15
- Νόμος 2225/1994 «Για την προστασία της ελευθερίας της ανταπόκρισης και επικοινωνίας και άλλες διατάξεις».
- Ν. 3917/2011 «Διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών

ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών, χρήση συστημάτων επιτήρησης με τη λήψη ή καταγραφή ήχου ή εικόνας σε δημόσιους χώρους και συναφείς διατάξεις».

- Νόμος 4411/2016 «Κύρωση της Σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον Κυβερνοχώρο και του Προσθέτου Πρωτοκόλλου της, σχετικά με την ποινικοποίηση πράξεων ρατσιστικής και ξενοφοβικής φύσης, που διαπράττονται μέσω Συστημάτων Υπολογιστών - Μεταφορά στο ελληνικό δίκαιο της Οδηγίας 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης - πλαισίου 2005/222/ΔΕΥ του Συμβουλίου, ρυθμίσεις σωφρονιστικής και αντεγκληματικής πολιτικής και άλλες διατάξεις».
- Π.Δ. 47/2005 «Διαδικασίες καθώς και τεχνικές και οργανωτικές εγγυήσεις για την άρση του απορρήτου των επικοινωνιών και για τη διασφάλισή του».
- Π.Δ. 178/2014 «Οργάνωση Υπηρεσιών Ελληνικής Αστυνομίας».

Η. Διαδικτυακές Πηγές

- «Η ευρωπαϊκή πρωτοβουλία για το υπολογιστικό νέφος θα δώσει στην Ευρώπη το παγκόσμιο προβάδισμα στη βασιζόμενη στα δεδομένα οικονομία»
    - http://europa.eu/rapid/press-release_IP-16-1408_el.htm
- Hak, J., The Admissibility of Digital Evidence in Criminal Prosecutions
    - http://www.crime-scene-investigator.net/admissibilitydigitaleveidencecriminalprosecutions.html
- Cameron, S., (2011). Digital Evidence στο FBI Law Enforcement Bulletin
    - https://leb.fbi.gov/2011/august/leb-august-2011
- Forensic Toolkit
    - http://accessdata.com/solutions/digital-forensics/forensic-toolkit-ftk
- dd - convert and copy a file
    - http://pubs.opengroup.org/onlinepubs/9699919799/utilities/dd.html
- Definition “sharding”

- http://searchcloudcomputing.techtarget.com/definition/sharding

- Ιστότοπος Ελληνικής Αστυνομίας
  - http://www.astynomia.gr/
- Cloud Evidence Group - Cybercrime Convention Committee
  - http://www.coe.int/en/web/cybercrime/ceg
- 3D TLC NAND To Beat MLC as Top Flash Storage
  - http://www.eetimes.com/author.asp?doc_id=1327903
- Digital Evidence and Forensics
  - http://www.nij.gov/topics/forensics/evidence/digital/pages/welcome.aspx
- Retrieving Digital Evidence: Methods, Techniques and Issues
  - https://articles.forensicfocus.com/2012/07/11/retrieving-digital-evidence-methods-techniques-and-issues/
- Hash function
  - https://en.wikipedia.org/wiki/Hash_function
- Virtualization
  - https://en.wikipedia.org/wiki/Virtualization
- Understanding the Cloud Computing Stack: SaaS, PaaS, IaaS
  - https://support.rackspace.com/white-paper/understanding-the-cloud-computing-stack-saas-paas-iaas/
- Cybercrime – Britannica
  - https://www.britannica.com/topic/cybercrime
- Why Are Cryptographic Hash Functions Important in Digital Forensics?
  - https://www.cclgroupltd.com/cryptographic-hash-functions-important-digital-forensics/
- European Union Agency for Network and Information Security (ENISA)
  - https://www.enisa.europa.eu/

- Encase Forensic
  - https://www.guidancesoftware.com/encase-forensic
- Cybercrime - INTERPOL
  - https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime
- Daubert Standard
  - https://www.law.cornell.edu/wex/daubert_standard
- Miller, M. (2009). Cloud Computing Pros and Cons for End Users
  - http://dosen.narotama.ac.id/wp-content/uploads/2012/01/Cloud-Computing-Pros-and-Cons-for-End-Users.doc
- Συνεργασία σε ποινικές υποθέσεις
  - https://e-justice.europa.eu/content_cooperation_in_criminal_matters-89-el.do
- Cyber Forensics – Torrid Networks
  - https://www.torridnetworks.com/services/incident-response/cyber-forensics

❑