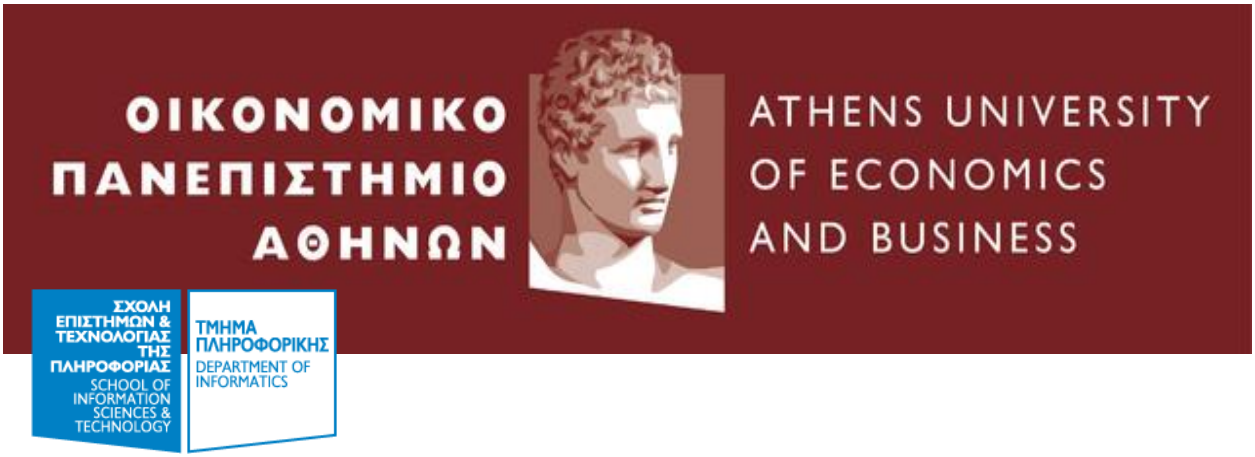

ΜΑΘΗΜΑ: ΣΤΟΙΧΕΙΑ ΔΙΚΑΙΟΥ

«Εξερευνώντας τις δραστηριότητες του Ethical Hacking: Μια διεξοδική περιγραφή του όρου αλλά και των ορίων που προκύπτουν από το υφιστάμενο νομοθετικό πλαίσιο»

Ευγένιος Γκρίτσης 3190045

Νικόλαος Χριστοδούλου 3190223

2023

Περιεχόμενα

Περίληψη

Το παρόν έγγραφο παρέχει μια διεξοδική περιγραφή των δραστηριοτήτων του Ethical Hacking, σε συνδυασμό με την εξέταση του υφιστάμενου νομοθετικού πλαισίου και τα όρια που τίθενται συναρτήσει του τελευταίου. Αρχικά, παρατίθεται μια τεχνική ανάλυση του όρου, αναλύεται η τεχνογνωσία και οι πολύπλευρες δεξιότητες που διακατέχουν οι ethical hackers, καθώς και η αναγκαιότητα της πρακτικής τους για τη συνολική βελτίωση της ασφάλειας των συστημάτων. Εν συνεχεία, εξετάζεται το νομοθετικό πλαίσιο, με έμφαση στην ελληνική νομοθεσία και τους κανονισμούς που σχετίζονται με τα εγκλήματα κατά των υπολογιστών και την προστασία των δεδομένων, κάνοντας αναφορά σε αντίστοιχους νόμους. Επιπροσθέτως, συζητούνται τα όρια που οφείλουν να τηρούν οι penetration testers από τους παραπάνω υφιστάμενους κανονισμούς. Παρουσιάζονται δύο επιλεγμένες μελέτες περιπτώσεων (case studies), στις οποίες αναδεικνύεται πως η μη βαθιά και πλήρη κατανόηση των νόμων και η παραβίαση των ορίων, διατρέχουν και τις αντίστοιχες συνέπειες κατά την ενασχόληση με το Ethical Hacking. Συνολικά, η παρούσα μελέτη μπορεί να συνεισφέρει ως πολύτιμος οδηγός για άτομα και οργανισμούς που ενδιαφέρονται για το Ethical Hacking και τις νομικές επιπτώσεις που περιβάλλουν τον τομέα.

1. Εισαγωγή

Η ασφάλεια στον κυβερνοχώρο έχει καταστεί ολοένα και πιο σημαντικό ζήτημα στην σύγχρονη εποχή. Η ραγδαία ψηφιοποίηση του τρόπου ζωής έχει επηρεάσει κάθε οντότητα, από τους απλούς πολίτες έως τους οργανισμούς και τις κυβερνήσεις, καθώς ένα μεγάλο μέρος της καθημερινότητας βασίζεται πλέον στους υπολογιστές, το διαδίκτυο και τα δεδομένα. Έτσι λοιπόν, τα ζητήματα της ασφάλειας στον κυβερνοχώρο, έχουν συγκεντρώσει το ενδιαφέρον μιας ευρείας δημογραφικής ομάδας της κοινωνίας, και δεν περιορίζονται μόνο στους εμπειρογνώμονες και στους ακαδημαϊκούς. Μια βασική πτυχή της κυβερνοασφάλειας είναι το ethical hacking, το οποίο περιλαμβάνει την ελεγχόμενη προσπάθεια διείσδυσης σε ένα σύστημα με σκοπό τον εντοπισμό αδυναμιών και την βελτίωση της ασφάλειας, μια πρακτική που αποκτά ολοένα και μεγαλύτερη σημασία στον κλάδο.

Με το παρόν έγγραφο, παρέχεται μια τεχνική περιγραφή του όρου ethical hacking ενώ ταυτόχρονα εξετάζονται τα νομοθετικά πλαίσια που τον αφορούν, τα όρια σχετικά με τις τεχνικές εφαρμογής του, συμπεριλαμβανομένων των νόμων και κανονισμών που ισχύουν. Ενώ το ethical hacking μπορεί να αποτελέσει ένα τελεσφόρο εργαλείο για τον εντοπισμό και την αντιμετώπιση των πολύμορφων τρωτοτήτων ενός πληροφοριακού συστήματος, δεν στερείται νομικών και ηθικών προβληματισμών. Το νομοθετικό πλαίσιο του ethical hacking, είναι πολύπλοκο και τείνει να διαφέρει αναλόγως με τις συγκεκριμένες συμβάσεις αλλά και με τις ποικίλες γεωπολιτικές συνθήκες.

Η κατανόηση της έννοιας του ethical hacking, του νομικού πλαισίου και των ηθικών ορίων είναι απαραίτητη για την διεξαγωγή αυτών των δραστηριοτήτων με υπεύθυνο και αποτελεσματικό τρόπο. Πιο συγκεκριμένα, η τεχνική περιγραφή παρουσιάζεται στο 2^{ο} κεφάλαιο, ενώ στο 3^{ο} ακολουθεί η παρουσίαση και ανάλυση των νομοθετικών πλαισίων που οριοθετούν τις παραπάνω δραστηριότητες. Τέλος, με βάση όσων έχουν αναλυθεί, εξάγονται χρήσιμα συμπεράσματα.

2. Ethical Hacker/Hacking

2.1 Ορισμός

Σύμφωνα με το NICCS[1] (National Initiative for Cybersecurity Careers and Studies) των Ηνωμένων Πολιτειών Αμερικής, ο ethical hacker είναι ένας ειδικός σε θέματα υπολογιστών και δικτύων ο οποίος χρησιμοποιώντας διάφορα εργαλεία και μεθοδολογίες, επιχειρεί να διεισδύσει στα συστήματα του στόχου του, με σκοπό τον εντοπισμό και την επιδιόρθωση τρωτοτήτων.

Με άλλα λόγια, το ethical hacking περιγράφεται ως μια πρακτική ελεγχόμενης και εγκεκριμένης διείσδυσης σε πληροφοριακά συστήματα, δίχως κακόβουλη πρόθεση. Οι ethical hackers χρησιμοποιούν τα ίδια εργαλεία και τεχνικές με τους κακόβουλους εισβολείς, αλλά δεν προκαλούν ζημιά στα συστήματα-στόχους, ούτε κλέβουν δεδομένα και πληροφορίες[2]. Αντίθετα, διενεργώντας ελεγχόμενες και συστηματικές αξιολογήσεις, βοηθούν οργανισμούς και εταιρείες να εντοπίσουν τα τρωτά σημεία των συστημάτων τους και παράλληλα παραθέτουν οδηγίες για τον τρόπο αντιμετώπισής τους. Απώτερος σκοπός, λοιπόν, της εν λόγω πρακτικής, αποτελεί η βελτίωση της συνολικής ασφάλειας του εκάστοτε συστήματος.

2.2 Τεχνογνωσία και Δεξιότητες

Στο επάγγελμα του ethical hacker ή αλλιώς γνωστό και ως “Red teaming”, “penetration testing” και “white hat hacking”, δεν αρκεί απλώς η πολύπλευρη γνώση των ποικίλων κλάδων της επιστήμης υπολογιστών αλλά απαιτείται και η εξειδίκευση σε πολλούς από αυτούς. Αναλυτικότερα, τα λειτουργικά συστήματα, τα ενσύρματα και ασύρματα δίκτυα υπολογιστών και επικοινωνιών, η γνώση πολλαπλών γλωσσών προγραμματισμού, οι τεχνολογίες στον ιστό, τα τεχνικά μέσα ασφαλείας, οι διάφορες έννοιες της ασφάλειας στον κυβερνοχώρο αλλά και τα νομικά και ηθικά πλαίσια αποτελούν χαρακτηριστικά παραδείγματα στα οποία ο penetration tester οφείλει να εξειδικεύεται.

Εκτός της βαθιάς τεχνογνωσίας στο ευρύ φάσμα της πληροφορικής, ο ethical hacker διακατέχει και ένα σύνολο από μη τεχνικές αρετές μέσω των οποίων καταφέρνει να εντείνει την αποτελεσματικότητά του. Η πρόθεσή του να μην παραβαίνει τα ηθικά και νομικά πλαίσια

[1] (“Ethical Hacking Tools and Techniques from Infosec Learning, LLC | NICCS,” n.d.)
[2] (Chowdappa and Lakshmi, 2014)

αποτελεί την σημαντικότερη από αυτές. Παρά το γεγονός πως διαθέτει τις δεξιότητες και την ικανότητα να υποκλέψει δεδομένα και πληροφορίες υψηλής αξίας, ο ethical hacker αποφασίζει να μην το κάνει και να δρα εντός των νόμιμων και καλά καθορισμένων ορίων[3]. Ταυτόχρονα, ο ethical hacker αντιμετωπίζει σε καθημερινή βάση σύνθετες προκλήσεις και προβλήματα, τα οποία απαιτούν κριτική σκέψη, δημιουργικότητα και καινοτομία.

Επιπροσθέτως, η ταχεία ανάπτυξη των συστημάτων ασφαλείας καθιστά αναγκαίες τις ιδιότητες της προσαρμοστικότητας, της περιέργειας αλλά και της συνεχής δίψας για μάθηση για τον penetration tester, καθώς νέες ευπάθειες, μέθοδοι και τεχνολογίες προκύπτουν σε καθημερινή βάση. Τελευταία αλλά και εξίσου σημαντική αρετή που τον αντιπροσωπεύει είναι η επικοινωνία. Κρίσιμο κομμάτι της δουλείας ενός "white hat" hacker, αποτελεί η παρουσίαση πολύπλοκων τεχνικών λεπτομερειών και ευρημάτων που προέκυψαν κατά την διάρκεια της έρευνας του στους οργανισμούς που συνεργάζεται. Αυτό σημαίνει πως για να είναι αποτελεσματική η δουλειά και έρευνά του, ο ίδιος οφείλει να είναι σαφής τόσο στον γραπτό λόγο (εκθέσεις ευρημάτων κλπ.) όσο και στον προφορικό (παρουσιάσεις).

2.3 Σημαντικότητα

Με την συνεχιζόμενη ψηφιοποίηση του σύγχρονου κόσμου και την προσπάθειά μας να αυτοματοποιήσουμε τα πάντα, θέματα που σχετίζονται με την κυβερνοασφάλεια, όπως παραβιάσεις δεδομένων, παραβιάσεις ασφαλείας κλπ., βρίσκονται και θα συνεχίσουν να βρίσκονται στο επίκεντρο του ενδιαφέροντος[4]. Η ραγδαία αύξηση του όγκου και της πολυπλοκότητας των κυβερνοεπιθέσεων, αλλά και η τρομερή αύξηση του αριθμού των παγκόσμιων χρηστών του διαδικτύου (από 2,53 δις το 2013 στα 5.16 δις το 2023[5]), πλέον καθιστούν την ασφάλεια στον κυβερνοχώρο ως αναγκαία συνθήκη για την διασφάλιση της ευδαιμονίας και της ομαλής λειτουργίας των πραγμάτων.

Το ethical hacking διαδραματίζει κρίσιμο ρόλο στην άμυνα απέναντι σε κακόβουλους hackers, όντας ένα πολύ συχνό προληπτικό μέσο αντιμετώπισης απειλών, καθώς μέσω αυτού εντοπίζονται εγκαίρως οι τρωτότητες των συστημάτων και δικτύων πριν προλάβουν να αξιοποιηθούν από κακόβουλους φορείς. Οι αδυναμίες που ανακαλύπτονται, θα περνούσαν

[3] ("Get Inside the Hacker's Mind," 2020)
[4] (Vishnuram et al., 2022)
[5] ("How Many People Use the Internet in 2023?," n.d.)

απαρατήρητες δίχως την συμβολή του penetration tester με αποτέλεσμα να ενισχύεται η συνολική ασφάλεια του οργανισμού-στόχου. Ένας από τους βασικούς λόγους που το ethical hacking θεωρείται πλέον αναγκαίο μέτρο πρόληψης και ασφάλειας, είναι το γεγονός πως μέσω αυτού οι ενδιαφερόμενες εταιρείες και οργανισμοί καταφέρνουν να προπορεύονται των πιθανών απειλών και να πληρούν τις κανονιστικές απαιτήσεις και να αποδεικνύουν την δέσμευσή τους για την διασφάλιση ευαίσθητων δεδομένων.

3. Νομοθετικό πλαίσιο και οριοθέτηση δραστηριότητας

Στο παρών κεφάλαιο, παρουσιάζονται και αναλύονται τα νομικά πλαίσια και οι περιορισμοί της δραστηριότητας του ethical hacking. Συγκεκριμένα, στην ενότητα 3.1 θα διερευνήσουμε τα πλαίσια και τους κανονισμούς που ρυθμίζουν και επηρεάζουν τις πρακτικές και μεθοδολογίες των "white hat" hackers, ενώ συνεχίζοντας η ενότητα 3.2 εξερευνεί τους περιορισμούς και την οριοθέτηση της δραστηριότητας των ethical hackers ως αποτέλεσμα των προαναφερθέντων νόμων και πλαισίων. Τέλος, -στην ενότητα 3.3- παρουσιάζονται επιλεγμένα παραδείγματα και μελέτες περιπτώσεων (case studies) με στόχο την ολοκληρωμένη κατανόηση των νομοθετικών πλαισίων αλλά και των δυσκολιών που προκύπτουν κατά την πρακτική του ethical hacking στον πραγματικό κόσμο.

3.1 Νομικά πλαίσια και κανονισμοί που αφορούν το ethical hacking

3.1.1 Ελληνικοί νόμοι για το έγκλημα κατά υπολογιστών

Οι Ελληνικοί νόμοι για το έγκλημα κατά υπολογιστών, αποτελούν ένα κρίσιμο νομικό πλαίσιο που διαμορφώνει τα όρια και τις δραστηριότητες του ethical hacking στην Ελλάδα. Οι "white hat" hackers που δραστηριοποιούνται εντός του ελληνικού νομικού τοπίου οφείλουν να γνωρίζουν και να συμμορφώνονται με αυτές τις ειδικές διατάξεις, με σκοπό να διασφαλίσουν την νομιμότητα των πρακτικών τους.

Για την καλύτερη παρουσίαση αλλά και κατανόηση των νομοθεσιών και κανονισμών, κρίνεται αναγκαία η εξέταση του όρου "hacking". Το hacking ή αλλιώς η μη εξουσιοδοτημένη πρόσβαση σε πληροφοριακά συστήματα ή ηλεκτρονικά δεδομένα, σύμφωνα με τον Ελληνικό Ποινικό Κώδικα (Ε.Π.Κ) αποτελεί ποινικό αδίκημα βάσει του άρθρου 370Γ παρ. 2 και τιμωρείται με φυλάκιση. Αξίζει, επιπλέον, να αναφερθούμε στην παράγραφο 3 του άρθρου 370Γ του Ε.Π.Κ, κατά την οποία δηλώνεται πως αν ο δράστης ανήκει στην υπηρεσία του νόμιμου κατόχου του πληροφοριακού συστήματος, η πράξη της παραγράφου 2 του ίδιου άρθρου (βλ. προηγούμενη παράγραφο) τιμωρείται μόνο αν απαγορεύεται ρητά από εσωτερικό κανονισμό ή από έγγραφη απόφαση του κατόχου ή αρμόδιου υπαλλήλου του. Αυτό σημαίνει πως κάθε είδους πρόσβαση σε πληροφοριακό σύστημα, δίχως την άδεια του ιδιοκτήτη του, θα θεωρηθεί έγκλημα ανεξάρτητα από τον σκοπό του δράστη και ανεξάρτητα από το αν προκλήθηκε ή όχι ζημιά, συμπεριλαμβανομένου του ethical hacking.

Εάν η ενέργεια αποσκοπεί στις διεθνείς σχέσεις ή στην ασφάλεια του κράτους, εφαρμόζονται άλλες διατάξεις του Ε.Π.Κ (άρθρο 148 του Ε.Π.Κ, ποινική διάταξη για την κατασκοπεία), με μέγιστη ποινή φυλάκισης δέκα (10) ετών εάν τα δεδομένα χρησιμοποιούνται για την πρόκληση ζημίας στο κράτος. Εν συνεχεία, το άρθρο 292Β με τίτλο «Παρακώλυση λειτουργίας πληροφοριακών συστημάτων» ορίζει πως το hacking αποτελεί αδίκημα που τιμωρείται με ποινή από ένα έως πέντε έτη αναλόγως με την σοβαρότητα του αποτελέσματος, εάν παρεμποδίζει σοβαρά ή διακόπτει την λειτουργία συστημάτων πληροφοριών με την εισαγωγή, διαβίβαση, διαγραφή, καταστροφή, αλλοίωση ψηφιακών δεδομένων ή με αποκλεισμό της πρόσβασης στα δεδομένα αυτά ως αποτέλεσμα της ενέργειας.

Παράλληλα, με τα άρθρα 381Α και 381Β του Ε.Π.Κ τα οποία αφορούν την φθορά ηλεκτρονικών δεδομένων, τιμωρούν με ποινή φυλάκισης -αναλόγως την ζημιά- όποιον χωρίς δικαίωμα διαγράφει, καταστρέφει, αλλοιώνει ή αποκρύπτει ψηφιακά δεδομένα ενός πληροφοριακού συστήματος. Επιπλέον, επιβαρύνουν και με φυλάκιση μέχρι δύο (2) ετών, όποιον δεν έχει το δικαίωμα και με σκοπό τη διάπραξη κάποιου από τα εγκλήματα που περιγράφονται στις παρ. 1, 2 και 3 του άρθρου 381Α, παράγει, πωλεί, προμηθεύεται προς χρήση, εισάγει, κατέχει διανέμει ή με άλλο τρόπο διακινεί συσκευές ή προγράμματα υπολογιστή, που προορίζονται για διάπραξη εγκλήματος, συνθηματικά ή κωδικούς πρόσβασης ή άλλα παρεμφερή δεδομένα με τα οποία μπορεί να αποκτηθεί πρόσβαση σε κάποιο πληροφοριακό σύστημα.

3.1.2 Νομοθεσία προστασίας δεδομένων στην Ελλάδα

Στην σημερινή ψηφιακή πραγματικότητα, οι κανονισμοί και οι νομοθεσίες για τα δεδομένα αποτελούν βασικούς παράγοντες για την διασφάλιση της ιδιωτικότητας και προστασίας των δεδομένων των ατόμων. Η κατανόηση των πλαισίων και των νόμων που αφορούν την προστασία των δεδομένων αποτελεί αναγκαία συνθήκη για τους ethical hackers, καθώς αφενός καθορίζει τα νομικά όρια εντός των οποίων ενεργούν και αφετέρου διαμορφώνει και τις ηθικές τους ευθύνες. Εν συνεχεία παρουσιάζονται σχετικοί κανονισμοί και νομοθεσίες.

Το άρθρο 9Α του Συντάγματος με τίτλο «Προστασία προσωπικών δεδομένων» ορίζει πως καθένας έχει δικαίωμα προστασίας από την συλλογή, επεξεργασία και χρήση, ιδίως με ηλεκτρονικά μέσα, των προσωπικών δεδομένων, όπως ο νόμος ορίζει και προβλέπει την

λειτουργία μιας ανεξάρτητης αρχής που είναι επιφορτισμένη με την προστασία των προσωπικών δεδομένων.

Ο Γενικός Κανονισμός για την Προστασία Δεδομένων 2016/679 (ΓΚΠΔ – GDPR) του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016, έχει αναδειχθεί σε κανονισμό ορόσημο για την διασφάλιση της ιδιωτικής ζωής και προστασίας των δεδομένων των ατόμων στην Ευρωπαϊκή Ένωση και με τον ελληνικό νόμο με αριθμό 4624/2019 καθορίζονται τα μέτρα εφαρμογής του ΓΚΠΔ σε εθνικό επίπεδο.

Ο ΓΚΠΔ δίνει μεγάλη έμφαση στην προστασία των δικαιωμάτων των ιδιωτικών δεδομένων των ατόμων και επιβάλλει νέες αυστηρές υποχρεώσεις, και ενισχύει προηγούμενες, στους οργανισμούς που επεξεργάζονται δεδομένα προσωπικού χαρακτήρα[6]. Παράλληλα, περιλαμβάνει απαιτήσεις για την ενημέρωση της εποπτικής αρχής εντός 72 ωρών καθώς και των θιγόμενων ατόμων χωρίς αδικαιολόγητη καθυστέρηση σε περίπτωση παραβίασης των δεδομένων[7]. Οι οργανισμοί που θεωρούνται «υπεύθυνοι επεξεργασίας δεδομένων» ή «εκτελούντες της επεξεργασίας δεδομένων» σύμφωνα με τον κανονισμό οφείλουν να ορίσουν ένα γραφείο προστασίας δεδομένων (Data Protection Office – DPO), το οποίο είναι υπεύθυνο για την διασφάλιση της συμμόρφωσης με τον ΓΚΠΔ και τη σύνδεση με τις εποπτικές αρχές[8]. Οι κυρώσεις για τη μη συμμόρφωση περιλαμβάνουν πρόστιμα ύψους 2% του ετήσιου παγκόσμιου κύκλου εργασιών ή έως και 10 εκατομμύρια ευρώ[9].

Αποκτώντας μια ολοκληρωμένη κατανόηση αυτών των νομικών απαιτήσεων, οι ηθικοί χάκερ μπορούν να πλοηγηθούν αποτελεσματικά στις δραστηριότητές τους, διασφαλίζοντας τον νόμιμο και υπεύθυνο χειρισμό των προσωπικών δεδομένων στο ελληνικό πλαίσιο.

3.2 Οριοθέτηση δραστηριότητας

Η δραστηριότητα ενός ethical hacker καθορίζεται και οριοθετείται από μια σειρά νόμων, κανονισμών και πλαισίων που στοχεύουν στην διασφάλιση της νομιμότητάς της. Δεν υπάρχει αμφιβολία ότι ο Γενικός Κανονισμός για την Προστασία Δεδομένων (ΓΚΠΔ) διαδραματίζει πρωταγωνιστικό ρόλο στον προσδιορισμό των ορίων της δραστηριότητας ενός penetration

[6] (Voigt and von dem Bussche, 2017)
[7] (O'Brien, 2016)
[8] (Rebe, 2023)
[9] (Group, n.d.)

tester. Αυτό συμβαίνει καθώς ο ΓΚΠΔ ορίζει αυστηρές οδηγίες σχετικά με την επεξεργασία και την προστασία των προσωπικών δεδομένων, επιβάλλοντας στον penetration tester -ο οποίος εργάζεται συχνά με ευαίσθητα προσωπικά δεδομένα και πληροφορίες- να συμμορφώνεται με τον ΓΚΠΔ για την τήρηση των προτύπων προστασίας της ιδιωτικής ζωής και των δεδομένων. Για τους παραπάνω λόγους, ο ethical hacker οφείλει να είναι πλήρως ενημερωμένος και να διασφαλίζει πως οι δραστηριότητές του εμπίπτουν εντός των απαιτήσεων του κανονισμού.

Ταυτόχρονα, ο ΓΚΠΔ ορίζει την υποχρέωση των οργανισμών να εφαρμόζουν αυστηρά μέτρα ασφαλείας με απώτερο στόχο την προστασία των δεδομένων τους, με αποτέλεσμα να κρίνεται απαραίτητη η ύπαρξη δοκιμών διείσδυσης από ειδικούς penetration testers. Επιπρόσθετα, με το άρθρο 7 του ΓΚΠΔ θέτονται πρότυπα για την λήψη συγκατάθεσης από τα άτομα για δραστηριότητες επεξεργασίας δεδομένων, περιορίζοντας την εργασία του ethical hacker καθώς απαιτείται η λήψη κατάλληλης συγκατάθεσης προτού προβεί σε επεξεργασία δεδομένων.

Όπως είδαμε και στην παράγραφο 3.1, εκτός από τον ΓΚΠΔ και τους νόμους περί προστασίας δεδομένων, η οριοθέτηση της δραστηριότητας του ethical hacking επηρεάζεται επίσης και από τους νόμους για το έγκλημα κατά υπολογιστών στην Ελλάδα. Ο Ελληνικός Ποινικός Κώδικας αναφέρεται σε εγκλήματα σχετικά με την μη εξουσιοδοτημένη πρόσβαση, χειραγώγηση δεδομένων, παρακώλυση λειτουργίας πληροφοριακών συστημάτων κλπ. Όπως τονίστηκε και νωρίτερα, η άδεια, η εξουσιοδότηση και η συγκατάθεση αποτελούν ζωτικής σημασίας παράγοντες για την διεξαγωγή οποιωνδήποτε δραστηριοτήτων ethical hacking. Ο penetration tester οφείλει να έρθει σε γραπτή συμφωνία με σκοπό τον σαφή καθορισμό του πεδίου εφαρμογής των δοκιμών διείσδυσης, καθώς οποιαδήποτε πρόσβαση σε πληροφοριακό σύστημα δίχως την άδεια του ιδιοκτήτη κρίνεται παράνομη. Η ολοκληρωμένη κατανόηση του νομικού τοπίου, αποτελεί μονόδρομο για την διασφάλιση της νόμιμης και αποτελεσματικής συμπεριφοράς.

3.3 Επιλεγμένα παραδείγματα

Σε αυτήν την ενότητα, θα εξετάσουμε πραγματικά περιστατικά τα οποία έχουν καταδείξει την σημασία της κατανόησης των ορίων και των νομικών περιορισμών του ethical hacking και του penetration testing. Τα παραδείγματα αυτά αποκαλύπτουν τις προκλήσεις που

αντιμετωπίζουν οι white hat hackers. Στην πρώτη περίπτωση, μια ομάδα από penetration testers συνελήφθη και κατηγορήθηκε για διάρρηξη σε βαθμό κακουργήματος και κατοχή εργαλείων διάρρηξης κατά την διεξαγωγή μιας εξουσιοδοτημένης δοκιμής εισχώρησης σε ένα δικαστήριο. Οι κατηγορίες εν τέλει αποσύρθηκαν, αλλά το περιστατικό καταδεικνύει τους νομικούς κινδύνους που ελλοχεύουν στα πλαίσια δράσης των ethical hackers. Ενώ, στο δεύτερο παράδειγμα που παρουσιάζεται, η ιστορία ενός Παλαιστίνιου hacker, ο οποίος -προσπαθώντας να βοηθήσει- παραβίασε τα συστήματα του Facebook για να στρέψει την προσοχή της εταιρείας σε μια ευπάθεια που ανακάλυψε ο ίδιος. Αυτές οι περιπτώσεις αποδεικνύουν τις δυσκολίες και τους κινδύνους που παραμονεύουν στον τομέα του ethical hacking, καθώς και τα -ουκ ολίγες φορές- ασαφή όρια που τον περιτριγυρίζουν.

3.3.1 Περίπτωση νόμιμου φυσικού penetration testing που πήγε στραβά

Συχνά, σε ένα penetration test υπάρχουν και δοκιμές φυσικής ασφάλειας. Σύμφωνα με την CISCO[10], κατά την διάρκεια αυτών των δοκιμών, ο penetration tester προσπαθεί να αποκτήσει πρόσβαση στο κτίριο ή να βρει έγγραφα και διαπιστευτήρια που μπορούν να χρησιμοποιηθούν για να παραβιάσουν την φυσική ασφάλεια. Μόλις εισέλθει στο κτίριο, ο επιτιθέμενος μπορεί να προσπαθήσει να συλλέξει πληροφορίες κρυφακούγοντας ή κρύβοντας συσκευές (ή και λογισμικά) παρακολούθησης στα γραφεία, με απώτερο σκοπό να αποκτήσει απομακρυσμένη πρόσβαση στο εσωτερικό του δικτύου της επιχείρησης/οργανισμού.

Στο παράδειγμα μας, σύμφωνα με το άρθρο της The Daily Swig[11], ο Justin Wynn και ο Gary DeMercurio, δύο ειδικοί penetration testers, εργαζόμενοι στην εταιρεία συμβούλων ασφαλείας Coalfire, συνελήφθησαν κατά τη διαδικασία διεξαγωγής φυσικής διείσδυσης και αρχικά κατηγορήθηκαν για διάρρηξη, ενώ αργότερα οι κατηγορίες μειώθηκαν σε εγκληματική καταπάτηση. Η πολιτεία της Αϊόβα είχε προσλάβει την εταιρεία Coalfire για να ελέγξει την ασφάλεια των δικαστηρίων.

Οι δύο penetration testers απέκτησαν, αρχικά, πρόσβαση στα δικαστικά κτίρια μέσω μιας ανοιχτής πόρτας κατά τις κανονικές ώρες λειτουργίας στις 11 Σεπτεμβρίου 2019. Έπειτα, επέστρεψαν στο ίδιο κτίριο λίγο μετά τα μεσάνυχτα και ενεργοποίησαν σκοπίμως τον συναγερμό προκειμένου να δοκιμάσουν την αντίδραση της ασφάλειας. Αυτό είχε ως

[10] ("What is Penetration Testing?," n.d.)
[11] ("Coalfire arrests," 2020)

αποτέλεσμα οι αστυνομικές αρχές να ανταποκριθούν στον συναγερμό και να συλλάβουν τους δύο ειδικούς παρά το γεγονός πως έδειξαν την νόμιμη επιστολή που ενέκρινε την εργασία τους από το δικαστικό τμήμα της Πολιτείας της Αϊόβα.

Στην συνέχεια, ο δικαστής όρισε την εγγύησή τους σε 50.000 δολάρια για τον καθένα για τις κακουργηματικές κατηγορίες και κρατήθηκαν σχεδόν 20 ώρες στα κρατητήρια μέχρις ότου η Coalfire να πληρώσει την εγγύηση και να αφεθούν ελεύθεροι. Ο υπεύθυνος σερίφης σε τοποθέτηση του στην εφημερίδα "The daily Swig" δήλωσε πως συνέλαβε τους δύο ειδικούς επειδή οι πράξεις τους «ξεπερνούσαν το πεδίο εφαρμογής της σύμβασής τους». Αργότερα, στις 30 Ιανουαρίου, 2020 η Coalfire ανακοίνωσε[12] πως οι penetration testers που συνελήφθησαν, κατά την διεξαγωγή ενός τυπικού τεστ διείσδυσης για την προστασία των πολιτών της Αϊόβα, αθωώθηκαν.

3.3.2 Ειδικός ασφαλείας εισβάλλει στην σελίδα του Zuckerberg στο Facebook για να εκθέσει ευπάθεια

Στο συγκεκριμένο παράδειγμα, θα μελετήσουμε την υπόθεση[13] του Παλαιστίνιου ειδικού ασφαλείας Khalil Shreateh, ο οποίος το 2013 εντόπισε μια ευπάθεια της ιστοσελίδας Facebook η οποία επέτρεπε σε οποιονδήποτε να κάνει αναρτήσεις στον τοίχο ενός αγνώστου. Παρά τις προσπάθειες του Khalil να αναφέρει το ζήτημα στην ομάδα ασφαλείας της εταιρείας, το προφανές κενό ασφαλείας όχι μόνο δεν διορθώθηκε αλλά δεν αναγνωρίστηκε και ως «σφάλμα» σύμφωνα με τους τεχνικούς του Facebook. Παρόλα αυτά, ο Khalil θέλοντας να αποδείξει πως η ευπάθεια ήταν όχι μόνο πραγματική αλλά και σοβαρή, αποφάσισε να χρησιμοποιήσει την αδυναμία για να παραβιάσει την προσωπική ιστοσελίδα του Mark Zuckerberg στο Facebook.

Πιο αναλυτικά, ο Khalil σε ανάρτησή του στην προσωπική ιστοσελίδα του ιδρυτή της εταιρείας Facebook έγραψε «Συγγνώμη για την παραβίαση της ιδιωτικής σας ζωής, δεν είχα άλλη επιλογή…μετά από όλες τις αναφορές που έστειλα στην ομάδα του Facebook». Λίγα λεπτά αργότερα, το Facebook επικοινώνησε μαζί του απαιτώντας να μάθει τον τρόπο που είχε παραβιάσει την προσωπική σελίδα του Zuckerberg. Παράλληλα, είναι σημαντικό να σημειωθεί πως το Facebook διέθετε ένα πρόγραμμα επικηρύξεων ευπαθειών με σκοπό την

[12] ("Charges Dismissed Against Coalfire Employees," n.d.)
[13] (Gardner, 2013)

ανταμοιβή των penetration testers που ενώ βρίσκουν τρωτότητες, δεν τις εκμεταλλεύονται αλλά τις αναφέρουν στην τεχνική ομάδα του Facebook. Τέτοιες επικυρωμένες αναφορές αξίζουν 500 δολάρια. Παρόλα αυτά, η εταιρεία δήλωσε πως ο Khalil δεν θα λάβει τα χρήματά του, καθώς για να δικαιούται την πληρωμή απαιτείται η αποφυγή οποιασδήποτε παραβίασης της ιδιωτικής ζωής και θα έπρεπε να έχει χρησιμοποιήσει έναν δοκιμαστικό αντί για έναν πραγματικό λογαριασμό όταν ερευνάει σφάλματα και αδυναμίες.

Με άλλα λόγια, ο Khalil Shreateh παρόλο που έπραξε «ηθικά» και δεν εκμεταλλεύτηκε την αδυναμία που εντόπισε προς όφελος του, δεν αναγνωρίστηκε η ενέργειά του ως νόμιμη, καθώς παραβίασε τους όρους χρήσης του Facebook και για αυτόν τον λόγο δεν ανταμείφθηκε για τα ευρήματά του. Το περιστατικό αυτό, όχι μόνο αποκάλυψε το κενό ασφαλείας της ιστοσελίδας, αλλά ανέδειξε και την σημασία κατανόησης των νομικών πλαισίων όπως και την σοβαρότητα των ορίων που οφείλει να δραστηριοποιηθεί ένας ethical hacker.

4. Συμπεράσματα

Από όλα τα παραπάνω, καθίσταται σαφές πως οι πρακτικές του ethical hacking πλέον αποτελούν αναπόσπαστο κομμάτι των αμυντικών μηχανισμών πρόληψης και επομένως και του συνολικότερου φάσματος της ασφάλειας των οργανισμών και εταιρειών απέναντι σε απειλές και επιθέσεις που διεξάγονται στον κυβερνοχώρο. Η αναγκαιότητα του ethical hacking προέρχεται από την ανάγκη εντοπισμού και μετριασμού των πιθανών ευπαθειών υπολογιστών και πληροφοριακών συστημάτων προτού τις εκμεταλλευτούν κακόβουλοι φορείς.

Ταυτόχρονα, γίνεται φανερό πως οι πρακτικές του ethical hacking πρέπει να διεξάγονται μόνο εντός των ορίων του νόμου και των συμφωνημένων συμβάσεων και με τις κατάλληλες νομικές άδειες και διασφαλίσεις. Ενώ οι "white hat" hackers καταβάλλουν έντιμες προσπάθειες εντοπισμού τρωτοτήτων, δεν είναι λίγες οι φορές που αντιμετωπίζουν οι ίδιοι τον κίνδυνο νομικών επιπλοκών και συνεπειών λόγω της ευαίσθητης φύσης της εργασίας τους. Κατά συνέπεια, κρίνεται απαραίτητη η ύπαρξη καλά καθορισμένων νόμων και πλαισίων που ορίζουν και περιορίζουν με σαφήνεια την δραστηριότητα τους, διασφαλίζοντας ότι οι πρακτικές τους διεξάγονται εντός των νομικών ορίων.

Εν κατακλείδι, σε συνδυασμό με την κατάλληλη νομική οριοθέτηση των δραστηριοτήτων των ethical hackers, κρίσιμη κρίνεται και η επίγνωση των ίδιων για τις πιθανές συνέπειες των ενεργειών τους συμπεριλαμβανομένων των ακούσιων παραβιάσεων της ιδιωτικής ζωής. Αυτό προϋποθέτει, οι penetration testers να έχουν μια βαθιά κατανόηση των σχετικών νομικών πλαισίων και των κανονισμών που οριοθετούν τις δραστηριότητές τους, καθώς και -συμπεριλαμβανόμενης της τεχνικής εμπειρογνωμοσύνης- την κριτική σκέψη, την αντίληψη και την ευαισθητοποίηση για την επιτυχή διαχείριση αυτών των καταστάσεων με υπεύθυνη και έννομη συμπεριφορά. Τέλος, καθίσταται απαραίτητη και η συνεχής εκπαίδευση και κατάρτιση των ethical hackers για να βελτιώνουν τις δεξιότητες και τις γνώσεις τους.

Βιβλιογραφία

Charges Dismissed Against Coalfire Employees [WWW Document], n.d. . Coalfire.com. URL https://www.coalfire.com/insights/news-and-events/press-releases/charges-dismissed-against-coalfire-employees (accessed 5.6.23).

Chowdappa, K.B., Lakshmi, S.S., 2014. Ethical Hacking Techniques with Penetration Testing 5.

Coalfire arrests: Charges against US pen testers finally dropped [WWW Document], 2020. . The Daily Swig | Cybersecurity news and views. URL https://portswigger.net/daily-swig/coalfire-arrests-charges-against-us-pen-testers-finally-dropped (accessed 5.6.23).

Ethical Hacking Tools and Techniques from Infosec Learning, LLC | NICCS [WWW Document], n.d. URL https://niccs.cisa.gov/education-training/catalog/infosec-learning-llc/ethical-hacking-tools-and-techniques (accessed 4.24.23).

Gardner, J., 2013. Security expert hacks Mark Zuckerberg's Facebook page to expose a site vulnerability after no one would listen to his warnings about the glitch [WWW Document]. Mail Online. URL https://www.dailymail.co.uk/news/article-2396628/Mark-Zuckerbergs-Facebook-page-hacked-Khalil-Shreateh-expose-site-vulnerability.html (accessed 5.6.23).

Get Inside the Hacker's Mind: Why They Do What They Do [WWW Document], 2020. . California State University, Long Beach. URL https://digitalskills.cpace.csulb.edu/cybersecurity/get-inside-the-hackers-mind-why-they-do-what-they-do/ (accessed 4.27.23).

Group, G.L., n.d. International Comparative Legal Guides [WWW Document]. International Comparative Legal Guides International Business Reports. URL https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/greece (accessed 5.2.23).

How Many People Use the Internet in 2023? [Feb 2023 Update] [WWW Document], n.d. URL https://www.oberlo.com/statistics/how-many-people-use-internet (accessed 5.1.23).

O'Brien, R., 2016. Privacy and security: The new European data protection regulation and it's data breach notification requirements. Business Information Review 33, 81–84. https://doi.org/10.1177/0266382116650297

Rebe, N., 2023. Regulating Cyber Technologies: Privacy Vs Security. World Scientific.

Vishnuram, G., Tripathi, K., Kumar Tyagi, A., 2022. Ethical Hacking: Importance, Controversies and Scope in the Future, in: 2022 International Conference on Computer Communication and Informatics (ICCCI). Presented at the 2022 International Conference on Computer Communication and Informatics (ICCCI), pp. 01–06. https://doi.org/10.1109/ICCCI54379.2022.9740860

Voigt, P., von dem Bussche, A., 2017. The EU General Data Protection Regulation (GDPR). Springer International Publishing, Cham. https://doi.org/10.1007/978-3-319-57959-7

What is Penetration Testing? - Pen Testing [WWW Document], n.d. . Cisco. URL https://www.cisco.com/c/en/us/products/security/what-is-pen-testing.html (accessed 5.6.23).