Στοιχεία Δικαίου της Πληροφορίας

ETHICAL HACKING

Ν Ο Μ Ι Κ Ο Σ
Ο Δ Η Γ Ο Σ Γ Ι Α
HACKERS

ΓΕΩΡΓΟΠΟΥΛΟΥ
ΚΩΝΣΤΑΝΤΙΝΑ
(3180029)

ΛΙΑΡΟΚΑΠΗ
ΔΕΣΠΟΙΝΑ
(3180097)

2021

Το hacking είναι από τους δημοφιλέστερους όρους της εποχής. Γύρω από αυτόν έχουν συζητηθεί πολλοί ανακριβείς ορισμοί στην προσπάθεια να προσεγγιστεί. Δίνεται η εσφαλμένη εντύπωση πως όσοι ασχολούνται με αυτό είναι άτομα που περνούν αρκετά μεγάλο μέρος της ζωής τους μπροστά από έναν υπολογιστή προσπαθώντας να αποκτήσουν πρόσβαση, χωρίς εξουσιοδότηση σε άλλους υπολογιστές ή δίκτυα, να πάρουν δεδομένα και κωδικούς και να καταστρέψουν κάποιο σύστημα. Στην πραγματικότητα όμως, το hacking αναφέρεται σε άτομα που διαθέτουν τις κατάλληλες γνώσεις και δεξιότητες να εισβάλλουν και να διαχειρίζονται σε μεγάλο βαθμό διάφορα πληροφοριακά και υπολογιστικά συστήματα. Σε αυτό δεν γίνεται καμία ταύτιση με καταστροφή ή κλοπή δεδομένων.

Οι πλέον τόσο μεγάλες διαστάσεις του διαφαίνονται καθώς αποτελεί μάθημα σε πανεπιστήμια σε τμήματα πληροφορικής στην μορφή ασφάλειας των πληροφοριακών συστημάτων. Είναι ένας από τους βασικότερους τομείς στην πληροφορική γι' αυτό και άλλωστε μπορεί κάποιος να ξεκινήσει μια κανονική και νόμιμη καριέρα μέσα από αυτό. Η τοποθέτηση αυτή ίσως ακούγεται οξύμωρη, αλλά όπως προαναφέρθηκε, δεν υπάρχει μόνο για να δημιουργεί προβλήματα, για αυτό και υπάρχουν διάφορες κατηγορίες hacker.

-White hat hacker

Είναι γνωστοί και ως ηθικοί χάκερ (ethical hackers) και είναι ο καλός τύπος στον κόσμο του hacking. Συγκεκριμένα αναφέρεται σε έναν ειδικό ασφάλειας υπολογιστών, ο οποίος ειδικεύεται στις δοκιμές διείσδυσης και σε άλλες μεθοδολογίες δοκιμών για τη διασφάλιση της ασφάλειας των συστημάτων πληροφοριών ενός συστήματος. Άλλες ονομασίες αντίστοιχες αυτού του είδους είναι penetration tester, sneakers, red teams και tiger teams.

-Black hat hacker

Πιο συνηθισμένα ονόματα είναι crackers ή dark-side hackers. Σε αυτή την κατηγορία ανήκουν άτομα με εκτεταμένες γνώσεις στον υπολογιστή του οποίου σκοπός είναι να παραβιάσει ή να παρακάμψει την ασφάλεια στο διαδίκτυο. Συγκεκριμένα εισέρχονται σε ασφαλή δίκτυα για να καταστρέψουν δεδομένα ή να κάνουν το δίκτυο άχρηστο για όσους έχουν άδεια να το χρησιμοποιούν. Σε αυτήν εντάσσονται και όσοι δημιουργούν ιούς για τους υπολογιστές αν και από κάποιους διαχωρίζονται σε έναν παραπάνω τύπο γνωστό ως Coders ή Virus Writers.

-Grey hat hacker

Η κατηγορία αυτή είναι ένας συνδυασμός των δύο παραπάνω. Συνήθως δεν χακάρουν για προσωπικό κέρδος ή έχουν κακόβουλες προθέσεις, αλλά μπορεί να είναι διατεθειμένοι να διαπράξουν τεχνικά εγκλήματα κατά τη διάρκεια των τεχνολογικών τους εκμεταλλεύσεων προκειμένου να επιτύχουν καλύτερη ασφάλεια. Μερικές φορές ενεργούν παράνομα, αν και με καλή θέληση, ή για να δείξουν πώς αποκαλύπτουν τρωτά σημεία.

-Blue hat hacher

Είναι επαγγελματίες ασφαλείας που βρίσκονται εκτός των οργανισμών και χρησιμοποιούνται από τις εταιρείες για να βρουν ευπάθειες σε προϊόντα που δεν έχουν κυκλοφορήσει. Η Microsoft χρησιμοποιεί επίσης τον όρο BlueHat για να αντιπροσωπεύσει μια σειρά από συμβάντα ενημέρωσης ασφαλείας.

-Red Hat Hacker

Αυτή η κατηγορία αφορά αυτούς που επιλέγουν ακραίες και μερικές φορές παράνομες διαδρομές για να επιτύχουν τους στόχους τους. Οι στόχοι αυτοί είναι η αποτροπή του "έργου" των Black hat hackers και συνήθως ξεκινούν επιθέσεις πλήρους κλίμακας για να καταστρέψουν τους διακομιστές και τους πόρους τους.

-Green Hat Hacker

Σε αυτόν τον τύπο ανήκουν όσοι δεν γνωρίζουν τον μηχανισμό ασφαλείας και τις εσωτερικές λειτουργίες του διαδικτύου, η πρόθεσή τους δεν είναι απαραίτητα να προκαλέσει βλάβη σκόπιμα, αλλά μπορεί να το κάνουν ενώ παίζουν με διάφορες τεχνικές κακόβουλου λογισμικού και επιθέσεων. Συχνά όμως ακολουθούν την κατάλληλη

εκπαιδευτική πορεία, κερδίζουν πιστοποιητικά και παρακολουθούν μαθήματα ανάπτυξης δεξιοτήτων για να μάθουν.

Άλλες κατηγορίες μικρότερου εύρους είναι οι Elite hackers, που χρησιμοποιείται για να περιγράψει τους πιο ειδικευμένους, οι Script kiddies, που μοιάζουν με τους Green hat αλλά απλά ενδιαφέρονται να κατεβάσουν ή να αγοράσουν το κακόβουλο λογισμικό, τα εργαλεία και τα σενάρια στο διαδίκτυο και να τα χρησιμοποιήσουν χωρίς σοβαρό λόγο, οι Neophyte "newbies", οι οποίοι δεν έχουν σχεδόν καμία γνώση ή εμπειρία σχετικά με τη λειτουργία της τεχνολογίας και το hacking, οι Hacktivists, που χρησιμοποιούν την τεχνολογία για να ανακοινώσουν ένα μήνυμα (κοινωνικό, ιδεολογικό, θρησκευτικό ή πολιτικό), οι Nation states, που αναφέρεται σε υπηρεσίες πληροφοριών και πράκτορες πολέμου στον κυβερνοχώρο των εθνικών κρατών, οι Organized criminal gangs, οι οποίοι ενεργούν μόνο για το κέρδος και τέλος τα Bots, δηλαδή αυτοματοποιημένα εργαλεία λογισμικού τα οποία είναι διαθέσιμα για χρήση οποιουδήποτε τύπου χάκερ.

Από όλες τις παραπάνω κατηγορίες μόνο αυτοί που ανήκουν στη πρώτη, οι ethical hachers, δεν είναι παράνομοι και καταπολεμούν τις ανεπιθύμητες ενέργειες των υπολοίπων. Μελετώντας κανείς τη νομοθεσία που αφορά το hacking γίνεται αντιληπτό πώς το έργο τους είναι νόμιμο και οι περισσότερες χώρες έχουν θεσπίσει νόμους για την αντιμετώπιση των παράνομων hackers. Η ανανέωση αύτων είναι πολύ συχνή λόγω της ραγδαίας εξέλιξης της τεχνολογιάς, που έχει ως συνέπεια τη δημιουργία νομοθετικών κενών τα οποία πρέπει να καλύπτονται.

Ο νόμος 1805/1988 ήταν ο πρώτος νόμος που αφορούσε τη κακή χρήση των υπολογιστών. Πριν από αυτόν, τα εγκλήματα που αφορούσαν αυτά τα ζητήματα καλύπτονταν από εγκλήματα κλοπής, κλοπής χρόνου, και πλαστογραφίας. Μετά την ένταξη της πληροφορίας στη χώρα, με επιρροή από το γερμανικό Δεύτερο Νόμο της Οικονομικής Εγκληματικότητας του 1986, σκοπός του Ν. 1805/1988 είναι η διασφάλιση όσων στοιχείων εισάγονται στους υπολογιστές όπου προβλέπεται ειδική ποινική προστασία. Στην Ελλάδα το θέμα του Hacking καταπολεμάται μέσω του άρθρου 370Γ[1] του Ποινικού Κώδικα. Συγκεκριμένα, το άρθρο αυτό τιμωρεί την παράνομη αντιγραφή και χρήση λογισμικού και την πρόσβαση σε δεδομένα ηλεκτρονικού υπολογιστή χωρίς δικαίωμα. Στην πρώτη περίπτωση αποσκοπείται η κάλυψη των περιπτώσεων πειρατείας και η χρηματική ποινή κυμαίνεται από διακόσια ενενήντα ΕΥΡΩ έως πέντε χιλιάδες εννιακόσια ΕΥΡΩ. Στη δεύτερη περίπτωση ο δράστης τιμωρείται είτε με έως τρεις μήνες φυλάκιση ή με χρηματική ποινή τουλάχιστον είκοσι εννέα ΕΥΡΩ. Για περιπτώσεις που αφορούν κρατικά ζημήματα η ποινή ξεκινά με φυλάκιση το λιγότερο ενός έτους.

Επίσης, τιμωρούνται όσοι δεν είχαν δικαίωμα πρόσβασης σε στοιχεία που έχουν εισαχθεί σε έναν υπολογιστή, ακόμα και δεν γίνει με πρόθεση βλάβης αλλά μόνο για γνώση σε πληροφορίες που έχουν δωθεί σε αυτούς. Αν η υπόθεση αφορά αρχεία του επιστημονικού, επαγγελματικού, κρατικού ή δημοσίου απορρήτου εφαρμόζεται το άρθρο 370Β[2] παράγραφος 1 του Ποινικού Κώδικα. Σύμφωνα με αυτόν, η ποινή είναι τουλάχιστον τρεις μήνες φυλάκισης ενώ (παράγραφος 2) η ποινή γίνεται τουλάχιστον τριετής εάν ο δράστης εκμεταλλευτεί απόρρητο μεγάλης οικονομικής σημασίας ή βρίσκεται στην υπηρεσία που κατέχει τα στοιχεία αυτά. Για απόρρητο που αφορά το κράτος εν καιρώ ειρήνης, τιμωρείται μέχρι δέκα χρόνια κάθειρξης, ενώ σε εμπόλεμες περιόδους τα ξεπερνά[3].

Πολλές είναι οι περιπτώσεις που προγραμματιστές παρενέβησαν σε προγράμματα εταιριών για να αποσπάσουν χρηματικά ποσά. Αντίστοιχες απάτες που θήγουν την περιουσία άλλων μέσω των ηλεκτρονικών υπολογιστών τιμωρούνται από το Άρθρο 386[A] του Ποινικού Κώδικα. Σύμφωνα με τιμωρούνται τουλάχιστον τρεις μήνες όσοι επηρεάζοντας στοιχεία ηλεκτρονικών υπολογιστών έβλαψαν ξένη περιουσία, ενώ για μεγάλη ζημιά η ποινή φυλάκισης αυξάνεται στα τουλάχιστον δύο χρόνια.

1. Άρθρο 370Γ Ποινικού Κώδικα
2. Άρθρο 370Β Ποινικού Κώδικα
3. Άρθρο 146 Ποινικού Κώδικα

Από την άλλη πλευρά ο νόμος 2225/1994 αφορά την άρση του απορρήτου για διακρίβωση εγκλημάτων. Μια τέτοια περίπτωση είναι εάν το έγκλημα αφορά εσχάτη προδοσία, δηλαδή όταν τίθεται σε κίνδυνο το πολίτευμα και τα άτομα που ασκούν τη συνταγματική εξουσία[4], εάν προσβάλεται η ανθρώπινη αξιοπρέπια (παραδείγματος χάριν μέσω βασανιστηρίων) ακόμη και από στρατιωτικούς κατά την προσπάθεια απόσπασης πληροφοριών[5], και σε περιπτώσεις που απειλούνται τα σύνορα της χώρας και η ειρήνη, μέσω κατασκοπείας, παραβίασης μυστικών, νόθευσης εγγράγων εθνικών συμφερόντων και άλλων[6]. Επιπλέον το ίδιο εφαρμόζεται σε υποθέσεις που ο δράστης εισέρχεται παράνομα σε υπηρεσία αποτρέποντας τη λειτουργία της[7], αλλά και σε ενέργιες που σχετίζονται με πυρκαγιά[8], ή προκαλέσουν πρόβλημα στη συγκοινωνία μέσων σταθερής τροχιάς, πλοίων και αεροσκαφών[9]. Ανάλογα άρεται το απόρρητο υποθέσεων που αφορούν την ανθρώπινη ζωή, δηλαδή σε υποθέσεις ανθρωποκτονίας από πρόθεση[10], αρπαγής[11] και εκβίασης[12], αλλά και σε περιπτώσεις αλλοίωσης της περιουσίας, μέσω πλαστών χρημάτων[13] ή ληστείας[14]. Τέλος, επιτρέτεται αυτή η ενέργεια σε βασικά εγκλήματα, διακεκριμένες περιπτώσεις, κατάχρηση ιδιότητας γιατρών και φαρμακοποιών και επιβαρυντικές περιστάσεις σύμφωνα με τον νόμο 1729/1987[15]. Σε αυτές τις περιπτώσεις ακολουθώντας τη διαδικασία άρσης, μόνο όπως αναφέρεται στον Ν. 2225/1994 (και συγκεκριμένα στο άρθρο 5), είναι νόμιμη η πρόσβαση στο απόρρητο και οποισδήποτε άλλος τρόπος τιμωρείται.

Ο παραπάνω νόμος ύστερα από τροποποιήσεις με τον 3115/2003 επιβάλει ποινές σε όσους δεν ακολουθήσουν τη διαδικασία άρσης του απορρήτου και επιχειρήσουν τη παραβίαση του. Οι ποινές είναι διαφορετικές για άτομα που δεν έχουν επαφή με την υπηρεσία, για τα μέλη της Α.Δ.Α.Ε[16] και για διοικητικά μέλη. Στην πρώτη περίπτωση τιμωρείται με φυλάκιση τουλάχιστον ενός έτους και με το ποσό που κυμαίνεται από δεκαπέντε χιλιάδες ΕΥΡΩ έως εξήντα χιλιάδες ΕΥΡΩ. Στη δεύτερη, εάν αυτό γίνει από αμέλια επιβάλλεται φυλάκιση τριών μηνών και τριάντα χιλιάδες ΕΥΡΩ, ενώ σε αντίθετη περίπτωση η φυλάκιση ξεκινά από τα δύο χρόνια και το πρόστιμο από έξι χιλιάδες έως τριάντα χιλιάδες ΕΥΡΩ. Στην τελευταία περίπτωση επιβάλλονται κυρώσεις σύστασης για συμμόρφωση και προειδοποίηση για περαιτέρω κυρώσεις ή/και πρόστιμο από δεκαπέντε χιλιάδες ΕΥΡΩ έως ένα εκατομμύριο πεντακόσιες χιλιάδες ΕΥΡΩ.

Η θέσπιση του νόμου 2472/1997 πραγματοποιήθηκε ώστε να διαφυλάξει και να προστατέψει τον χρήστη από από την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Στόχος είναι να αποτραπεί η κοινοποίηση δεδομένων στοιχειών, παρά μόνο σε όσους απαιτείται, ώστε να αποφευχθεί η συσχέτιση αυτών των δεδομένων με το ατόμο που αφορούν. Οι ποινές κλιμακώνονται ξεκινώντας από προειδοποιήση, πρόστιμο, ανάκληση άδειας και καταλήγουν σε καταστροφή αρχείων ή διακοπή επεξεργασίας. Σήμερα, ο νόμος αυτός τείνει να καταργηθεί καθώς δημιουγούνται νέοι που καλύπτουν εκτενέστερα τις απαιτήσεις της εποχής.

Επιπλέον από το νόμο[17] τιμωρούνται όσοι αλλοιώσουν δεδομένα πληροφοριακών συστημάτων, διαγράφοντας, διαδιβάζοντας ή/και καταστρέφοντάς τα. Γενικά, η ποινή κυμαίνεται από ένα έως τρία χρόνια, και συγκεκριμένα επιβάλλεται για μεγάλο αριθμό επιθέσεων σε πληροφοριακά συστήματα μεγάλου χρονικού διαστήματος ή έκτασης με

4. Άρθρα 134, 135, 157 Ποινικού Κώδικα, Άρθρο 64 Στρατιωτικού Ποινικού Κώδικα
5. Άρθρα 137Α, 137Β Ποινικού Κώδικα
6. Άρθρα 138, 139, 140, 143, 144, 146, 148, 150, 151 Ποινικού Κώδικα, Άρθρα 26, 27, 28, 29, 31, 32, 33, 34, 35, 39, 40, 41, 63, 76, 93, 97 Στρατιωτικού Ποινικού Κώδικα
7. Άρθρο 168 Ποινικού Κώδικα
8. Άρθρα 264, 265, 270, 272 Ποινικού Κώδικα
9. Άρθρο 291 Ποινικού Κώδικα
10. Άρθρο 299 Ποινικού Κώδικα
11. Άρθρα 322, 324 Ποινικού Κώδικα
12. Άρθρο 385 Ποινικού Κώδικα
13. Άρθρα 207, 208, 211 Ποινικού Κώδικα
14. Άρθρο 380 Ποινικού Κώδικα
15. Άρθρα 5, 6, 7, 8
16. Άρθρα 10, 11 Ν. 3115/2003
17. Άρθρο 292Β Ποινικού Κώδικα

σημαντικές απώλειες, είτε χρημάτων είτε δεδομένων. Για περιπτώσεις που αφορούν συστήματα ζωτικής σημασίας, κυρίως για θέματα υγείας, εθνικής άμυνας, μεταφορές και άλλα, η φυλάκιση είναι τουλάχιστον ένα χρόνο, ενώ εάν δράσουν σε ομάδες άνω των τριών ατόμων η ποινή της φυλάκισης ανέρχεται σε τουλάχιστον δύο έτη.

Εκτός από τους ίδιους τους αυτουργούς υπάρχουν και ποινές για όσους τους βοηθούν να διαπράξουν τις ενέργειες που αναφέρονται στα άρθρα 370Β, 370Γ και 370Δ, δηλαδή την παρακολούθηση ή αποτύπωση σε υλικό φορέα μη δημόσιες διαβιβάσεις και την χωρίς δικαίωμα χρήση ή αντιγραφή προγραμμάτων υπολογιστών. Πιο συγκεκριμένα τιμωρούνται αυτοί που κατέχουν και διανέμουν προς χρήση συσκευές ή προγράμματα, που στοχεύουν στη διάπραξη των προηγούμενων εγκλημάτων, και κωδικούς και συνθηματικά που επιτρέπουν την παράνομη πρόσβαση σε πληροφοριακά συστήματα ή σε μέρη τους. Η ποινή για αυτούς είναι μέχρι δύο χρόνια φυλάκισης[18].

Ποινή από ένα έως τρία χρόνια επιβάλλεται σε όποιον φθείρει ηλεκτρονικά δεδομένα δηλαδή χωρίς δικαίωμα επεξεργάζεται ψηφιακά δεδομένα[19], κυρίως αλλοίωση, διαγραφή, καταστροφή ή απόκρυψη. Κάποιες περιπτώσεις με δικαστική απόφαση παραμένουν ατιμώρητες εάν κριθούν αμελητέες. Αναλυτικότερα, εάν προκληθούν σημαντικές ζημιές ή απειληθούν συστήματα πληροφοριών ζωτικής σημασίας η φυλάκιση είναι τουλάχιστον ένα έτος ενώ εάν συμπληρωματικά ο δράστης χρησιμοποιήσει κάποιο πρόγραμμα το οποίο έχει σχεδιαστεί για την πραγματοποίηση επιθέσεων φτάνει έως τα τρία χρόνια.

Πρέπει επίσης να σημειωθεί η ανάγκη για διασφάλιση των βάσεων δεδομένων. Σε σχέση με τις ηλεκτρονικές βάσεις δεδομένων, ο δημιουργός τους έχει το δικαίωμα να παραχωρεί Άδειες Χρήσης, δηλαδή έργο που περιέχει γενικούς όρους που επιτρέπουν τη χρησιμοποίηση τους από έναν άλλο χρήστη, ή μεταβίβασης σε τρίτο[20]. Μόνο ο δημιουργός έχει το δικαίωμα να απαγορεύσει την κάθε είδους αλλοίωση ή προσπέλαση του έργου του[21] αλλά και να επιτρέψει, εφόσον δεν υπάρχει αντίθετη συμφωνία, οποιαδήποτε μετατροπή ενός προγράμματος ή διόρθωσης σφαλμάτων από το πρόσωπο που νόμιμα το απέκτησε[22]. Αστικές κυρώσεις προβλέπονται στην περίπτωση προσβολής πνευματικής ιδιοκτησίας του δημιουργού της βάσης αλλά και του δικαιώματος ειδικής φύσης του κατσκευαστή[23]. Για όποιον διανέμει ή κατέχει σκοπεύοντας τη διανομή σε πρόγραμμα υπολογιστή την βάση δεδομένων, τιμωρείται για κάθε αντίτυπο με πρόστιμο χιλίων ΕΥΡΩ[24], ενώ με φυλάκιση τουλάχιστον ένα χρόνο και χρηματική ποινή δύο χιλιάδων διακοσίων έως δεκαπέντε χιλιάδων ΕΥΡΩ υπόκειται εγγράφει αντίτυπα και εκμεταλλεύεται έργα που είναι αντικείμενο πνευματικής ιδιοκτησίας[25]. Συνοπτικά, με τον Ν. 2121/1993 στόχος είναι η αποτροπή της πειρατίας και η τιμωρία όσων εκμεταλλεύονται βάσεις δεδομένων χωρίς την απαραίτητη άδεια χρήσης από τον δημιουργό της.

Επιπλέον, έχουν θεσπιστεί ενιαίοι κανόνες για τα κράτη μέλη της Ευρωπαϊκής Ένωσης που στρέφονται κατά των αδικημάτων στα συστήματα πληροφοριών[26]. Σκοπός της οδηγίας αυτής είναι η καταπολέμηση του ηλεκτρονικού εγκλήματος και την προώθηση της ασφάλειας των πληροφοριών μέσω ισχυρότερων εθνικών νόμων, αυστηρότερων ποινικών κυρώσεων και περισσότερης συνεργασίας μεταξύ των αρμόδιων αρχών. Σύμφωνα με αυτή, απαγορεύεται η χρήση κακόβουλου λογισμικού για εξ αποστάσεως απόκτησης του ελέγχου ενός δικτύου υπολογιστών, γνωστό και ως botnet, ώστε να αποφευχθεί η παράνομη πρόσβαση σε συστήματα πληροφοριών[27], η παρεμβολή στο σύστημα[28] ή σε δεδομένα[29] και

18. Άρθρο 370Ε Ποινικού Κώδικα
19. Άρθρο 381Α Ποινικού Κώδικα
20. Άρθρο 2.α Ν. 2121/1993
21. Άρθρο 4 Ν. 2121/1993
22. Άρθρο 42 Ν. 2121/1993
23. Οδηγία 96/9
24. Άρθρο 65Α Ν. 2121/1993
25. Άρθρο 66 Ν. 2121/1993
26. Οδηγία 2013/40/ΕΕ
27. Άρθρο 3 Οδηγίας 2013/40/ΕΕ
28. Άρθρο 4 Οδηγίας 2013/40/ΕΕ
29. Άρθρο 5 Οδηγίας 2013/40/ΕΕ

η υποκλοπή τους[30]. Εάν κάποιος διαπράξει κάποιο από αυτά τα εγκλήματα τιμωρείται με μέγιστη ποινή τα δύο έτη, ενώ εάν πρόκειται για υποθέσης που έχουν πλήξει μεγάλο αριθμό συστημάτων ή γίνει εκ προθέσεως, η ποινή αυξάνεται σε τουλάχιστον τρία έτη. Σε περιπτώσεις, όμως, που διαπραχθεί στο πλαίσιο εγκληματικής οργάνωσης ή κατά συστημάτων που αποτελούν μέρος ζωτικής σημασίας υποδομής, ο δράστης τιμωρείται σε τουλάχιστον πέντε έτη[31]. Στην Ελλάδα ενσωματώθηκε με το νόμο 4411/2016.

Επιγραμματικά, η προαναφερθήσα νομοθεσία στοχεύει στην εφαρμογή ποινών σε εγκλήματα που αφορούν την παράνομη πρόσβαση σε πληροφοριακά συστήματα, τα εγκλήματα κατά της λειτουργίας των πληροφοριακών συστημάτων, την παράνομη παρεμβολή σε ψηφιακά δεδομένα και την παράνομη υποκλοπή αυτών, και τα εγκλήματα σε σχέση με εργαλεία για την εκτέλεση κυβερνοεγκλημάτων. Αυτός που έχει πρόσβαση σε πληροφορίες ζωτικής σημασίας και σε ευαίσθητα προσωπικά δεδομένα χωρίς να έχει παρανομήσει είναι ο ηθικός hacker. Οι τεχνικές τους και τα εργαλεία που χρησιμοποιούν αν και μοιάζουν με των υπόλοιπων hacker, είναι απόλυτα νόμιμοι και στόχος τους είναι η προστασία από επιθέσεις αξιολογώντας το βαθμό ασφάλειας κάθε συστήματος, και έτσι αναφέρονται τα τρωτά σημεία και καλύπτονται ώστε να αποφευχθούν τυχόν καταστροφικές ενέργειες από hackers.

Παρά το σημαντικότατό τους έργο, λόγω των κοινών στοιχείων με τους κακόβουλους hackers, όπως προαναφέρθηκε, είναι μία διαδικασία που δεν αποπνέει εμπιστοσύνη. Εκτός από όσους εργάζονται επαγγελματικά σε αυτό το κομμάτι, υπάρχουν και κάποιοι οι δουλεύουν δημόσια, ανώνυμα και χωρίς πληρωμή με στόχο να αποκαλύψουν τρύπες σε τρέχοντα συστήματα. Η ακτιβιστική τους δράση, όμως, από πολλούς αμφισβητείται και υποστηρίζεται πως δρουν για να διαφημίσουν τις ενέργειες τους και να αποκτήσουν δημοσιότητα, κάνοντας έτσι τα συστήματα πιο ευάλωτα σε επιθέσεις, λόγω των πληροφοριών που προκύπτουν από την αυτοπροβολή τους. Από την άλλη πλευρά, οι εταιρίες, επιχειρήσεις και οργανισμοί έχουν ανάγκη να προσλαμβάνουν άτομα που θα τους βοηθήσουν στην όσο πιο δυνατή ασφαλή χρήση και λειτουργία των συστημάτων τους. Για να θεωρηθεί κάποιος αξιόπιστος και χρήσιμος ώστε να εργαστεί σε αυτόν τον τομέα, οφείλει να έχει εμπλουτίσει το βιογραφικό του με πιστοποιητικά που φανερώνουν τις ικανότητές του.

Η πιστοποίηση CEH, Certified Ethical Hacker[32], πρόκειται για μία πιστοποίηση, του International Council of E-Commerce Consultants (EC-Council), παγκοσμίως αναγνωρισμένη και εγκεκριμένη που οι κάτοχοι της καταρτίζονται σε πολλούς τομείς του ethical hacking, όπως Footprinting and Reconnaissance, Scanning Networks, Enumeration, System Hacking, Malware Threats, Sniffing Techniques, Social Engineering, Denial of Service, Session Hijacking, Evading IDS, Firewalls and Honeypots, Hacking Web Servers, Hacking Web Applications, SQL Injection, Hacking Wireless Networks, Hacking Mobile Platforms and IoTs, Cloud Computing, Cryptography και μεθοδολογίες Penetration Testing. Για επαγγελματίες σε περιβάλλοντα enterprise-level, που στοχεύουν στην διαχείριση κινδύνου ασφάλειας, στην ανάπτυξη και διαχείριση προγραμμάτων, στη διακυβέρνηση και στη διαχείριση και αντιμετώπιση των περιστατικών ασφάλειας υπάρχει από τον ISACA (Information Systems Audit and Control Association) η πιστοποίηση CISM, Certified Information Security Manager[33]. Συγκεκριμένα, σκοπεύει να παρέχει ένα κοινό σώμα γνώσεων για διαχειριστές ασφάλειας πληροφοριών σε όλο τον κόσμο και καλύπτονται ευρεία θέματα, όπως διέπουν την ασφάλεια πληροφοριών, την ανάπτυξη και τη διαχείριση προγραμμάτων ασφάλειας πληροφοριών και τη διαχείριση συμβάντων. Επιπλέον υπάρχει και η πιστοποίηση CISSP, Certified Information Systems Security Professional[34], η οποία διέπεται από το (ISC)², δηλαδή International Information Systems Security Certification Consortium, και έχει την έγκριση του DoD (Υπουργείο Άμυνας) μέσω των προγραμμάτων IAT (Information Assurance

30. Άρθρο 6 Οδηγίας 2013/40/ΕΕ
31. Άρθρο 9 Οδηγίας 2013/40/ΕΕ
32. https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/
33. https://www.isaca.org/credentialing/cism
34. https://www.isc2.org/Certifications/CISSP

Technical) και IAM (Information Assurance Managerial) και εξετάζοται τομείς που αφορούν τον έλεγχο πρόσβασης, τη ασφάλεια ανάπτυξης εφαρμογών, οι οποίες βασίζονται στην εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα. Το Offensive Security που διδάσκει μεθόδους δοκιμής διείσδυσης και τη χρήση των εργαλείων που περιλαμβάνονται στη διανομή Kali Linux και προσφέρει την OSCP, Offensive Security Certified Professional, πιστοποίηση[35]. Με αυτή, κάποιος αποκτά μία πιο τεχνική εμπειρία στον τομέα του hacking και συγκεκριμένα με παθητική συλλογή πληροφοριών, ενεργή συλλογή πληροφοριών, σάρωση ευπάθειας, υπερχείλιση buffer, εκμετάλλευση υπερχείλισης Win32 Buffer, εκμετάλλευση υπερχείλισης Buffer Linux, εργασία με εκμεταλλεύσεις, μεταφορές αρχείων, κλιμάκωση προνομίων, πλευρικές επιθέσεις πελατών ,επιθέσεις εφαρμογών ιστού, επιθέσεις κωδικού πρόσβασης, ανακατεύθυνση και σήραγγα λιμένων, το πλαίσιο Metasploit, παράκαμψη λογισμικού προστασίας από ιούς και ανάλυση δοκιμής διείσδυσης. Μια ακόμη διεθνώς αναγκνωρισμένη πιστοποίηση είναι η CREST[36], Council for Registered Ethical Security Testers, είναι μέρος μιας κοινοπραξίας με το CIISec και το Royal Holloway University of London (RHUL), η οποία στοχεύει στην υψηλή εξειδίκευση και εμπειρία στην κυβερνοασφάλεια, ακολουθώντας τις βέλτιστες πρακτικές σε όλους τους τομείς, συμπεριλαμβανομένης της εκτέλεσης των εργασιών, της προετοιμασίας, της κάλυψης, της προστασίας δεδομένων και της μετά τεχνικής παράδοσης. Επιπλέον η πιστοποίηση Tigerscheme[37] διασφαλίζει ότι ο κάτοχός του έχει κατανοήσει την ασφάλεια των πληροφοριών στον εταιρικό κόσμο και τις δεξιότητες που απαιτούνται από έναν ελεγκτή διείσδυσης, έχει αναπτύξει την κατανόηση της ηθικής και του ποινικού δικαίου σε σχέση με την ηθική πειρατεία, μπορεί να καταμετρήσει το δίκτυο και να κάνει τη χαρτογράφηση του, μπορεί να απαριθμήσει να διαχειριστεί και να εκμεταλλευτεί την υπηρεσία και να διαχειρίζεται τους κινδύνους. Για την τεχνολογία των πληροφοριών η πιστοποίηση CCNA[38], Cisco Certified Network Associate, επικυρώνει τις δεξιότητές και τις γνώσεις του κατόχου της σε βασικές αρχές δικτύου, πρόσβαση στο δίκτυο, συνδεσιμότητα IP, υπηρεσίες IP, βασικές αρχές ασφαλείας και αυτοματισμό και προγραμματισμό. Για προχωρημένους επαγγελματίες πληροφορικής που βρίσκονται στις αρχές σε δοκιμές διείσδυσης υπάρχει το eJPT[39], eLearnSecurity Junior Penetration Tester, του eLearnSecurity. Αυτή πιστοποιεί ότι υπάρχουν οι κατάλληλες γνώσεις για TCP / IP, δρομολόγηση IP, πρωτόκολλα και συσκευές LAN, HTTP και τεχνολογίες ιστού, βασικές διαδικασίες και μεθοδολογίες δοκιμής διείσδυσης, βασική αξιολόγηση ευπάθειας των δικτύων, βασική αξιολόγηση ευπάθειας των εφαρμογών ιστού, εκμετάλλευση με το Metasploit, απλή χειροκίνητη εκμετάλλευση εφαρμογών Ιστού, βασική συλλογή πληροφοριών και αναγνώριση και για απλή σάρωση και δημιουργία προφίλ στο στόχο. Τέλος, μια ακόμη παγκοόσμια πιστοποίηση είναι η CompTIA Security+[40], που επικυρώνει τις βασικές δεξιότητες που χρειάζεστε για να εκτελέσετε βασικές λειτουργίες ασφαλείας και να ακολουθήσετε μια καριέρα ασφάλειας στον τομέα της πληροφορικής. Συγκεκριμένα, διαθέτει γνώσεις που αφορούν τις απειλές, επιθέσεις και ευπάθειες, τη διαχείριση ταυτότητας, πρόσβασης και κινδύνων, για αρχιτεκνονική, κρυπτογραφία και PKI.

Από τα παραπάνω φαίνεται ότι οι ethical hackers είναι απαραίτητοι για κάθε επιχείρηση αφού μπορούν να αξιολογήσουν όχι μόνο τις δικτυακές άμυνες, αλλά και τις πολιτικές ασφάλειας των επιχειρήσεων καθώς και τη συμπεριφορά των χρηστών για πιθανούς κινδύνους ασφαλείας. Παρόλα αυτά, οι πιστοποιήσεις, οι γνώσεις και οι δεξιότητες του καθενός δεν αρκούν για να κερδίζουν την εμπιστοσύνη των εργοδοτών τους, καθώς τα συνήθη περιστατικά των ηλεκτρονικών εγκλημάτων συμβαίνουν εκ των έσω δημιουργώντας ανησυχίες για το πόσο εύκολο είναι, αν εργάζεται κάποιος στο εσωτερικό μιας εταιρίας , να κάνει επίθεση σε κάποιο σύστημα της. Αν και για αυτόν το λόγο πολλοί θεωρούν ότι ακόμη και το ethical hacking δημιουργεί προβλήματα δεν μπορεί κανείς να εκμηδενίσει τη αξία της δράσης τους κρίνοντας έτσι απαραίτητη την ύπαρξη τους ακόμη και με αυτό σαν αντίκτυπο.

35. https://www.offensive-security.com/pwk-oscp/
36. https://www.crest-approved.org/
37. https://www.tigerscheme.org/
38. https://www.cisco.com/c/en/us/training-events/training-certifications/certifications/associate/ccna.html
39. https://elearnsecurity.com/product/ejpt-certification/
40. https://www.comptia.org/certifications/security

ΠΕΡΙΛΗΨΗ

Η συνεχής ανάπτυξη της τεχνολογίας στοχεύει στη διευκόλυνση της καθημερινότητας του ανθρώπου, παρόλα αυτά δημιουργεί και νέα προβλήματα. Ένα απο τα πιο πολυσυζητημένα προβλήματα είναι η διαρροή πληροφοριών, η οποία συμβαίνει από τους hackers. Καθώς όμως, υπάρχουν πολλές κατηγορίες μία από αυτές, οι ethical hackers, στοχεύουν στην αποτροπή των υπολοίπων. Αυτό που τους ξεχωρίζει, πέραν της “καλοπροαίρετης” δράσης τους, είναι οι πλήρως νόμιμες ενέργειες που κάνουν ώστε να πετύχουν το στόχο τους. Λόγω της σπουδαιότητας του έργου τους, κάθε κράτος έχει θεσπίσει νόμους που παρουσιάζουν τα όρια που τους επιτρέπουν να κινούνται. Για να προβάλει ο κάθε ethical hacker τις δεξιότητες του, χρησιμοποιεί εγκεκρίμενες πιστοποιήσεις που του επιτρέπουν να εργαστεί στο χώρο, χωρίς όμως αυτό να σημαίνει ότι φανερώνουν και την ατομική ηθική που απαιτείται σε αυτό τον τομέα.

ΠΑΡΑΡΤΗΜΑΤΑ

- **Ιστοσελίδες**

https://sectigostore.com/blog/different-types-of-hackers-hats-explained/
https://www.cyberinsurancegreece.com/news/vasilis-georgopoylos-o-monadikos-ellinas-ithikos-chaker/
https://www.cyberinsurancegreece.com/hacking/
https://www.synopsys.com/glossary/what-is-ethical-hacking.html#4
https://www.lawspot.gr/
https://www.opi.gr/
https://www.offlinepost.gr/2020/05/27/%CF%84%CE%BF-%CE%B7%CE%BB%CE%B5%CE%BA%CF%84%CF%81%CE%BF%CE%BD%CE%B9%CE%BA%CF%8C-%CE%AD%CE%B3%CE%BA%CE%BB%CE%B7%CE%BC%CE%B1-%CE%BA%CE%B1%CE%B9-%CF%84%CE%BF-%CE%B5%CE%BB%CE%BB%CE%B7%CE%BD%CE%B9%CE%BA/
https://www.e-nomothesia.gr/
https://sectigostore.com/blog/different-types-of-hackers-hats-explained/
https://medium.com/@hackersleaguebooks/who-are-blue-hat-hackers-aeb443b90c29
https://searchsecurity.techtarget.com/answer/What-is-red-and-white-hat-hacking

- **Βιβλία**

Kevin Smith, HACKING The Ultimate Hacking for Beginners How to Hack
Ευάγγελος Παπακωνσταντίνου, Δίκαιο Πληροφορικής, Εκδόσεις Σακκουλά

- **Πτυχιακές**

http://repository.teiwest.gr/xmlui/bitstream/handle/123456789/7721/%CE%97%20%CE%9D%CE%9F%CE%9C%CE%9F%CE%98%CE%95%CE%A3%CE%99%CE%91%20%CE%93%CE%99%CE%91%20%CE%A4%CE%97%CE%9D%20%CE%95%CE%93%CE%9A%CE%9B%CE%97%CE%9C%CE%91%CE%A4%CE%99%CE%9A%CE%9F%CE%A4%CE%97%CE%A4%CE%91%20%CE%A3%CE%A4%CE%9F%20%CE%94%CE%99%CE%91%CE%94%CE%99%CE%9A%CE%A4%CE%A5%CE%9F.pdf?sequence=1&isAllowed=y
https://hellanicus.lib.aegean.gr/bitstream/handle/11610/17374/%20%20%20%20%20%20%20%20%20%20-%20%20%20%20%20%20%20%20-%20%20%20%20%20%20%20%20%20%20-%20%20-%20%20%20%20%20%20%20%20%20%20%20%20%20-%20%20%20%20%20%20%20%20%20%20-%20%20%20-ethical-hacking.pdf?sequence=1