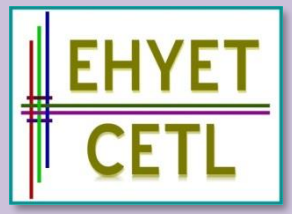
Επιδράσεις από τη χρήση του Διαδικτύου

3. ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ



www.cetl.upatras.gr

Χρήστος Θ. Παναγιωτακόπουλος
Ανθή Καρατράντου
Στέφανος Αρμακόλας

3. ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

Υποστηρικτική βιβλιογραφία Ενότητας

Παναγιωτακόπουλος, Χ. (2018). *Η ηθική στο διαδίκτυο και το ηλεκτρονικό έγκλημα*. Αθήνα: Εκδόσεις Παπαζήση.

Εναλλακτική υποστηρικτική βιβλιογραφία Ενότητας

- https://www.itsecuritypro.gr/ilektroniko-egklima-theoria-ke-pragmatikotita/
- https://sites.google.com/site/elektronikoenklema2012/home
- http://ikee.lib.auth.gr/record/133574/files/ΤΕΛΙΚΟ18.11.13.pdf
- https://www.offlinepost.gr/2020/05/27/το-ηλεκτρονικό-έγκλημα-και-το-ελληνικ/
- https://www.cnn.gr/tag/ilektroniko-egklima
- https://www.newsauto.gr/specials/people/manos-sfakianakis-etsi-tha-prostateftite-apo-ta-ilektronika-egklimata/
- http://www.crimetimes.gr/διεύθυνση-δίωξης-ηλεκτρονικού-εγκλή/
- https://euipo.europa.eu/ohimportal/el/web/observatory/faqs-on-copyright-el
- https://creativecommons.org/licenses/?lang=el
- https://legal.heal-link.gr/index.php/intellectual-property-limits

3. ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

Το έγκλημα και η απάτη

Το **έγκλημα** στη μη ψηφιακή ζωή μας είναι ένα κοινωνικό και οικονομικό φαινόμενο τόσο παλιό όσο και η κοινωνία μας. Πρόκειται για πράξη άδικη και καταλογιστή στον δράστη που τιμωρείται από τον νόμο.

Η πράξη θεωρείται ότι είναι μία συγκεκριμένη ανθρώπινη συμπεριφορά, η οποία συμπεριλαμβάνει όχι μόνο την ενέργεια αλλά και την παράλειψη. Άδικη θεωρείται μία πράξη η οποία ως κοινωνικό γεγονός βρίσκεται σε αντίθεση με το σύνολο των γραπτών ή άγραφων, υποχρεωτικών και εξαναγκαστικών κανόνων, που ρυθμίζουν τις σχέσεις των διαβιούντων προσώπων στην ίδια κοινωνία.

Το αδίκημα της **απάτης** διαπράττεται από όποιον, με σκοπό να αποκομίσει ο ίδιος ή άλλος παράνομο περιουσιακό όφελος, βλάπτει ξένη περιουσία πείθοντας κάποιον σε πράξη, παράλειψη ή ανοχή με την εν γνώσει του παράσταση ψευδών γεγονότων ως αληθινών ή την αθέμιτη απόκρυψη ή παρασιώπηση αληθινών γεγονότων.

3. ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

Το ηλεκτρονικό έγκλημα

Το **ηλεκτρονικό έγκλημα**, ως έγκλημα που διαπράττεται στον κυβερνοχώρο, ορίζεται ως έναν βαθμό διαφορετικά, ανάλογα με τον επιστημονικό χώρο από τον οποίο προσεγγίζεται. Ένας από όλους τους ορισμούς, αυτός της ένωσης των Διευθυντών της Βρετανικής Αστυνομίας, θεωρεί το ηλεκτρονικό έγκλημα ως *τη χρήση δικτυωμένων υπολογιστών ή τη χρήση της διαδικτυακής τεχνολογίας για τη διάπραξη ή τη διευκόλυνση της διάπραξης εγκλημάτων*.

Το ύψος του κόστους που αφορά το ηλεκτρονικό έγκλημα είναι τεράστιο.

Μέσα στο 2019 θα ανέλθει διεθνώς στο ποσό των 2,1 τρισεκατομμυρίων δολαρίων περίπου και το 2021 περίπου στο ποσό των 6 τρισεκατομμυρίων δολαρίων.

Όμως:

- Σε τι βαθμό και με ποιους τρόπους όμως το διαδίκτυο μπορεί να αποτελέσει εργαλείο παρανομίας;
- Ποιες παραβατικές συμπεριφορές μπορούν να βρουν χώρο ανάπτυξης σ' αυτό;

3. ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

Α. Το ηλεκτρονικό έγκλημα με στόχο τον υπολογιστή – ΤΥΠΟΙ

Α1. Μη εξουσιοδοτημένη πρόσβαση

- Εκτέλεση διαφόρων παράνομων πράξεων από το σύστημα μη εξουσιοδοτημένης πρόσβασης
- Μη εξουσιοδοτημένη αντιγραφή, τροποποίηση ή διαγραφή δεδομένων και εφαρμογών
- Κλοπή πληροφοριών, βιομηχανική κατασκοπία

Α2. Κακόβουλο λογισμικό

- Διασπορά διαφόρων μορφών κακόβουλου λογισμικού (ιών, σκουληκιών, βομβών λογισμικού, δούρειων ίππων κ.ά.)

Α3. Παρεμπόδιση ή εξουδετέρωση λειτουργίας υπολογιστών

- Διατάραξη, διακοπή ή άρνηση παροχής υπηρεσιών

3. ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

Β. Το ηλεκτρονικό έγκλημα με εργαλείο έναν υπολογιστή - ΤΥΠΟΙ

Β1. Παραβάσεις περιεχομένου

- Προσέλκυση και κακοποίηση παιδιού - παιδική πορνογραφία
- Περιεχόμενο που χαρακτηρίζεται από εχθρότητα ή προκατάληψη ενός ατόμου λόγω φυλής, εθνότητας, θρησκείας, πεποιθήσεων, σεξουαλικών προτιμήσεων κ.ά.
- Παραβίαση ιδιωτικότητας, δημοσιοποίηση προσωπικών δεδομένων, εκβιασμός
- Υποκλοπή και δημοσιοποίηση απόρρητων στρατιωτικών πληροφοριών
- Περιεχόμενο με δημοσιοποίηση υλικού που υπόκειται σε πνευματικά δικαιώματα ή πνευματική ιδιοκτησία, συμπεριλαμβανομένης της πειρατείας λογισμικού
- Παραποίηση ή πλαστογραφία εγγράφων

Β2. Μη εξουσιοδοτημένη αλλαγή - παραποίηση δεδομένων ή λογισμικού για αποκόμιση οφέλους

- Κλοπή ταυτότητας
- Ηλεκτρονική απάτη
- Δολιοφθορά (περιλαμβανομένης και της επίθεσης σε κύριες υποδομές)
- Ηλεκτρονική χειραγώγηση των αγορών μετοχών ή άλλων τίτλων

Β3. Παράνομη ή/και ανάρμοστη χρήση της επικοινωνίας

- Παρενόχληση & κυβερνοκαταδίωξη
- Ηλεκτρονικό ξέπλυμα χρημάτων και νομιμοποίηση εσόδων από παράνομες δραστηριότητες
- Μαζική αποστολή του ίδιου μηνύματος σε ένα πλήθος ανθρώπων για την προώθηση προϊόντων ή ιδεών ή για κλοπή δεδομένων
- Διακίνηση φαρμάκων, όπλων, ναρκωτικών και ανθρώπινων οργάνων
- Κοινωνική πληροφοριακή απάτη (π.χ. phishing)
- Μαζική επιτήρηση

3. ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

Δεν επιτρέπεται: [Κανόνες δεοντολογίας 1#2 για την αποφυγή του]

- *Η χρήση υπολογιστικών συστημάτων για τη δημιουργία βλάβης ή ζημίας άλλων ανθρώπων.*
- *Η χρήση υπολογιστικών συστημάτων για μετάδοση λανθασμένων, ψευδών ή παραπλανητικών μαρτυριών.*
- *Η μη εξουσιοδοτημένη πρόσβαση σε υπολογιστικά συστήματα και ιστοχώρους μέσω λογαριασμών, εξαιρουμένων των διαχειριστών τους.*
- *Η πρόσβαση σε υπολογιστικά συστήματα για τέλεση εγκλήματος ή ανέντιμης πράξης.*
- *Η πρόσβαση σε ξένα αρχεία και η χρήση ξένων υπολογιστικών πόρων χωρίς εξουσιοδότηση.*
- *Η ανεύθυνη χρήση υπολογιστικών συστημάτων, τα οποία δεν είναι επαρκώς προστατευμένα και μπορεί να χρησιμοποιηθούν ως μέσα επίθεσης σε άλλα υπολογιστικά συστήματα.*
- *Η δραστηριότητα σάρωσης θυρών σε υπολογιστικά συστήματα ή συσκευές, εξαιρουμένων των διαχειριστών τους ή ατόμων με εξουσιοδότηση.*
- *Η διασπορά κακόβουλου λογισμικού ή λογισμικού υφαρπαγής προσωπικών δεδομένων και στοιχείων λογαριασμών.*
- *Η κατασκευή και η χρήση λογισμικού για το οποίο δεν έχουν εξεταστεί οι κοινωνικές επιπτώσεις από τον σχεδιασμό και την εφαρμογή του.*
- *Η χρήση υλικού σε ιστοχώρους, για το οποίο δεν έχουμε τα πνευματικά δικαιώματα ή δικαιώματα χρήσης. Η λήψη υλικού από το διαδίκτυο δεν αναιρεί τα πνευματικά δικαιώματα εκείνου που το κατασκεύασε.*
- *Κάθε δραστηριότητα μέσω της οποίας διενεργείται κλοπή δεδομένων ή λογισμικού ή βανδαλισμός.*

3. ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

Δεν επιτρέπεται: [Κανόνες δεοντολογίας 2#2 για την αποφυγή του]

- *Κάθε δραστηριότητα που οδηγεί σε απόκτηση περιουσίας μέσω εξαπάτησης άλλων.*
- *Κάθε δραστηριότητα που παρεμποδίζει, περιορίζει ή παρεμβάλλεται σε εργασία άλλου χρήστη.*
- *Η δημοσίευση φωτογραφιών ή προσωπικών δεδομένων χωρίς τη συγκατάθεση των προσώπων που τους αφορά και η έλλειψη σεβασμού προς την ιδιωτικότητα κάθε χρήστη.*
- *Η χρήση αγενών ή προσβλητικών εκφράσεων στις διαδικτυακές συνομιλίες.*
- *Η μετάδοση και διασπορά ανακριβών πληροφοριών με στόχο να θιγεί η αξιοπρέπεια κάποιου ανθρώπου.*
- *Η αποθήκευση, επεξεργασία, αποστολή ή δημοσίευση ακατάλληλου, προσβλητικού ή άσεμνου περιεχομένου. Ιδιαίτερα μάλιστα, περιεχομένου σχετικού με παιδική πορνογραφία.*
- *Η παρακολούθηση, η με κάθε τρόπο έκφραση απειλής, η παρενόχληση, η ενοχλητική παρακολούθηση, η συνεχόμενη αποστολή ανεπιθύμητων μηνυμάτων ή ο εκφοβισμός χρήστη.*
- *Η χρήση λογισμικού, η προμήθεια του οποίου δεν έγινε με νόμιμο τρόπο.*
- *Η λήψη οποιουδήποτε τύπου λογισμικού, αρχείων εικόνας, αρχείων ήχου, ταινιών, για τα οποία δεν έχουμε δικαιώματα χρήσης.*
- *Η ενθάρρυνση, η υποκίνηση, η παραπλάνηση ή η παροχή βοήθειας σε ένα άτομο με σκοπό να επιχειρήσει να βλάψει κάποιο άλλο.*
- *Η κλοπή της ταυτότητας ή η μίμηση των χαρακτηριστικών άλλου ατόμου.*
- *Η χρήση υπολογιστικών συστημάτων με τρόπο που δείχνει έλλειψη εκτίμησης και σεβασμού για συνανθρώπους.*

3. ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

Οι χάκερς

Πρόκειται για απρόσκλητους επισκέπτες του διαδικτύου που δρουν είτε μεμονωμένα είτε σε ομάδες. Προτιμούν να δράσουν σε διακομιστές υψηλής σημασίας ή υποτιθέμενης υψηλής ασφάλειας κυβερνητικών οργανισμών ή εταιρειών.

Εισέρχονται (δηλαδή συνδέονται) χωρίς εξουσιοδότηση σε ένα υπολογιστικό σύστημα παρακάμπτοντας τους κανόνες ασφαλείας, είτε «σπάζοντας» τους κωδικούς εισόδου είτε μέσα από ηλεκτρονικές διόδους («πόρτες») πλημμελώς ασφαλισμένες.

Οι στόχοι τους είναι αρκετοί και διαφορετικοί. Μπορεί να έχουν ως στόχο απλά την προβολή τους, η οποία μετά την έκτιση της ποινής που επισύρει η πράξη τους οδηγεί σε εύρεση καλά αμειβόμενης εργασίας. Μπορεί ο στόχος να είναι η υποκλοπή ή η αλλοίωση δεδομένων για οικονομικό όφελος ή απλά ο βανδαλισμός.

Όσον αφορά τα κύρια αίτια της συμπεριφοράς τους, οι χάκερς λειτουργούν με τον τρόπο αυτό για:

- απλή ψυχαγωγία
- εκδίκηση
- αυτοπροβολή, αυτοεπιβεβαίωση, αποδοχή
- υποκλοπή ή αλλοίωση ή καταστροφή δεδομένων – οικονομικό όφελος
- αλλοίωση ή καταστροφή δεδομένων – βανδαλισμός.

3. ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

Μελέτη περίπτωσης (1#25)

Χάκερ εναντίον John McAfee

Στις 29 Δεκεμβρίου 2017 ανακοινώθηκε ότι ο λογαριασμός στο Twitter του ιδρυτή της εταιρείας McAffe που παράγει λογισμικό κατά των ιών, του Τζον ΜακΆφι (John McAfee), παραβιάστηκε από χάκερ και χρησιμοποιήθηκε για τη διαφήμιση συγκεκριμένων κρυπτονομισμάτων. Στόχος του χάκερ ήταν να επηρεαστούν οι χρήστες και να επενδύσουν σ' αυτά ώστε να αυξηθεί η τιμή τους.

Το γεγονός σχολιάστηκε ποικιλοτρόπως, αφού ο Τζον ΜακΆφι αποτελεί με τη δράση του ένα είδος πολέμιου των χάκερς και ειδικού στην κυβερνοασφάλεια!

3. ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

Μελέτη περίπτωσης (2#25)

Κενά ασφαλείας σε συνηθισμένους μικροεπεξεργαστές

Το καλοκαίρι του 2017, ερευνητές της Google σε συνεργασία με ειδικούς στην ασφάλεια συστημάτων διαπίστωσαν ότι στους μικροεπεξεργαστές της Intel, της AMD και της Arm υπάρχουν σφάλματα στον σχεδιασμό τα οποία επιτρέπουν σε ιούς ή χάκερς να αποκτήσουν πρόσβαση στη μνήμη ενός συστήματος και να υποκλέψουν κρίσιμα δεδομένα, τα οποία υπό φυσιολογικές συνθήκες δεν θα έπρεπε να είναι προσβάσιμα ή ορατά παρά μόνο από τον διαχειριστή του (Williams, 2018).

Με τον τρόπο αυτό, φάνηκε ότι ήταν ευάλωτα όλα τα υπολογιστικά συστήματα που συνδέονταν με το διαδίκτυο (διακομιστές, σταθεροί και φορητοί υπολογιστές, υπολογιστές τύπου tablet και «έξυπνα» κινητά τηλέφωνα).

3. ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

Μελέτη περίπτωσης (3#25)

Κακόβουλο λογισμικό σε σύστημα ελέγχου πυρηνικού αντιδραστήρα

Το 2016 το υπολογιστικό σύστημα που υποστήριζε έναν πυρηνικό σταθμό (Gundremmingen Nuclear Power Plant) παραγωγής ηλεκτρικού ρεύματος στη Γερμανία βρέθηκε μολυσμένο με ιούς.

Οι ιοί, μεταξύ των οποίων οι W32.Ramnit και Conficker, είχαν σχεδιαστεί για κλοπή αρχείων και για παράδοση του ελέγχου του συστήματος σε απομακρυσμένο χρήστη, όταν το σύστημα θα συνδεόταν στο διαδίκτυο.

Το ευτύχημα είναι ότι το σύστημα παρέμενε απομονωμένο από το διαδίκτυο.

3. ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

Μελέτη περίπτωσης (4#25)

Το κακόβουλο λογισμικό τύπου ransomware

Το ransomware είναι ένα είδος κακόβουλου λογισμικού το οποίο έχει σχεδιαστεί, αφού εισέλθει σε ένα υπολογιστικό σύστημα, να το μπλοκάρει και να αποτρέπει την πρόσβαση στα αποθηκευμένα δεδομένα έως ότου πληρωθούν «λύτρα» στον χάκερ.

Στις 12 Μαΐου 2017, εξαπολύθηκε παγκοσμίως μία επίθεση με έναν ιό της κατηγορίας αυτής (τον WannaCry), η οποία ήταν η μεγαλύτερη στην ιστορία του διαδικτύου. Μέσα σε λίγες ώρες είχαν μολυνθεί 200.000 υπολογιστές ιδιωτών αλλά και μεγάλων εταιρειών.

3. ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

Μελέτη περίπτωσης (5#25)

Η αποτελεσματικότητα του λογισμικού προστασίας

Σύμφωνα με δεδομένα σχετικής έρευνας, κανένα διαθέσιμο πρόγραμμα δεν είναι απολύτως αποτελεσματικό για την προστασία του χρήστη από κυβερνοεπιθέσεις με διασπορά κακόβουλου λογισμικού. Τα έως τώρα γνωστά προγράμματα προστασίας από κακόβουλο λογισμικό δείχνουν οριακά αποτελεσματικά. Πιο ευάλωτα είναι τα συστήματα που λειτουργούν με Microsoft Windows και λιγότερο αυτά που λειτουργούν με Apple OS X ή iOS.

3. ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

Μελέτη περίπτωσης (6#25)

Κυβερνοεπίθεση για έλεγχο ηλεκτρικού δικτύου

Μία σχετικά πρόσφατη επιτυχημένη κυβερνοεπίθεση σε ηλεκτρικό δίκτυο που έγινε γνωστή συνέβη στις 23 Δεκεμβρίου 2015 στην Ουκρανία. Η επίθεση οργανώθηκε από ομάδα χάκερς της Ρωσίας κατά τη διάρκεια των εχθροπραξιών μεταξύ των δύο χωρών και ήταν ενταγμένη σε ένα πλαίσιο απειλών με όνομα «Sandworm».

3. ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

Μελέτη περίπτωσης (7#25)

Παιδική πορνογραφία και διαδικτυακή παρακολούθηση

Το 2017 στο Μέριλαντ των ΗΠΑ καταδικάστηκε ένας τριαντάχρονος σε εικοσαετή φυλάκιση για παραγωγή υλικού παιδικής πορνογραφίας, εκβιασμό και διαδικτυακή παρακολούθηση ανηλίκων. Σύμφωνα με την απόφαση, μετά την εικοσαετία και για 25 επιπλέον χρόνια θα ελέγχεται συστηματικά από την αστυνομία, θα καταγραφεί και θα αναφέρεται στον τόπο που κατοικεί ως δράστης σεξουαλικών εγκλημάτων.

Ο τριαντάχρονος από το 2014 έως το 2017, προσποιούμενος το ανήλικο αγόρι ή κορίτσι, έψαχνε σε μέσα κοινωνικής δικτύωσης ανήλικα θύματα με διάφορους εικονικούς λογαριασμούς και αφού δημιουργούσε αίσθηση οικειότητας, τα έπειθε να δημιουργούν για λογαριασμό του φωτογραφίες και βίντεο σεξουαλικού περιεχομένου. Μέσα από τους εικονικούς λογαριασμούς διέσπειρε το πορνογραφικό υλικό, χρησιμοποιώντας συχνά και την ταυτότητα των ίδιων των θυμάτων του, προκειμένου να προσελκύσει κι άλλους ανηλίκους για να του αποστείλουν υλικό. Όταν κάποιο θύμα δεν επιθυμούσε να συνεχίσει, κοινοποιούσε υλικό στην οικογένεια και στους φίλους του. Επίσης, επικοινωνούσε με τα θύματά του και τις οικογένειές τους από εικονικούς λογαριασμούς, προκειμένου να τους εκβιάσει και να τους πιέσει συναισθηματικά.

3. ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

Μελέτη περίπτωσης (8#25)

Η βιομετρική ταυτοποίηση

Σήμερα, η βιομετρική τεχνολογία παρέχει τη δυνατότητα της αναγνώρισης ενός προσώπου με πολύ υψηλό βαθμό αξιοπιστίας.

Μέσω της βιομετρίας μπορεί να αναλυθούν χαρακτηριστικά τα οποία είναι μοναδικά, μετρήσιμα και να οδηγήσουν στην αναγνώριση της ταυτότητας ενός ανθρώπου. Τα βιομετρικά χαρακτηριστικά διαχωρίζονται σε δύο κατηγορίες: στα φυσιολογικά χαρακτηριστικά, στα οποία π.χ. περιλαμβάνεται το DNA, η ίριδα, ο αμφιβληστροειδής, το πρόσωπο, το δακτυλικό αποτύπωμα, το σχήμα των ώτων, και στα συμπεριφορικά χαρακτηριστικά, στα οποία περιλαμβάνεται π.χ. ο ρυθμός πληκτρολόγησης, η υπογραφή, το βάδισμα, οι χειρονομίες και η φωνή.

Στη χρήση βιομετρικών μεθόδων ταυτοποίησης, εκτός και αν πρόκειται για ειδικές περιπτώσεις που σχετίζονται με το δημόσιο συμφέρον, έχουν διατυπωθεί ανησυχίες για την προστασία της ιδιωτικής ζωής. Με τη χρήση τους αίρεται πλέον η ανωνυμία και η ψευδωνυμία, αφού η βιομετρική παρακολούθηση ενός ανθρώπου δίνει πλήρη εικόνα για τη συμπεριφορά και τον χαρακτήρα του, κάτι που μπορεί να χρησιμοποιηθεί εναντίον του.

3. ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

Μελέτη περίπτωσης (9#25)

Η διάχυτη υπολογιστική και η περιβάλλουσα νοημοσύνη

Η διάχυτη υπολογιστική και η περιβάλλουσα νοημοσύνη είναι μία τεχνολογία η οποία στοχεύει στην ενσωμάτωση των υπολογιστών με τη μορφή δικτυωμένων επεξεργαστικών μονάδων στα περιβάλλοντα εργασίας και διαβίωσης του ανθρώπου (σε ιδιωτικούς ή δημόσιους χώρους, σε σπίτια, γραφεία, αίθουσες διδασκαλίας κ.ά.) με έναν αόρατο και διακριτικό τρόπο. Οι επεξεργαστές με τη βοήθεια αισθητήρων και αλγορίθμων καταγράφουν και προσαρμόζουν, ανάλογα με τα πρότυπα συμπεριφοράς των χρηστών, τις συνθήκες του περιβάλλοντος ή παρέχουν πληροφορίες για τις ανάγκες τους, όπως τις αντιλαμβάνονται τα συστήματα, στοχεύοντας στη βελτίωση της ποιότητας της ζωής.

Όμως, η συνεχής καταγραφή των κινήσεων και αντιδράσεων του ανθρώπου, σε συνδυασμό με τη συνδεσιμότητα και την από κοινού λειτουργία όλων των συσκευών για μετάδοση δεδομένων και λήψη αποφάσεων, απειλεί την ιδιωτικότητα του ανθρώπου. Μπορεί εύκολα να δημιουργηθεί το προφίλ ενός ανθρώπου αν αναλογιστούμε ότι η τεχνολογία αυτή είναι διάχυτη στο περιβάλλον (βρίσκεται παντού), είναι αόρατη, είναι διασυνδεδεμένη, δεν ανιχνεύεται και καταγράφει συνεχώς κάθε αντίδραση.

3. ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

Μελέτη περίπτωσης (10#25)

Η δράση των χάκερς σε υψηλό επίπεδο

Τον Ιούνιο του 2011 στις ΗΠΑ παραβιάστηκε από χάκερς ο ιστοχώρος της Γερουσίας, προκαλώντας πανικό και ανασφάλεια.

Τον Δεκέμβριο του 2016, οι αρχές των ΗΠΑ κατήγγειλαν την Κίνα για πράξεις κλοπής αμυντικών στρατιωτικών μυστικών μέσω βιομηχανικής κατασκοπείας που πραγματοποιούσαν οι υπηρεσίες πληροφοριών της. Οι αμερικανικές υπηρεσίες πληροφοριών υποστήριξαν ότι η Κίνα υπέκλεψε τεχνολογία από το αμερικανικό μαχητικό αεροσκάφος F-35 και την εφάρμοσε στο νέο μαχητικό κινεζικό αεροσκάφος J-20.

3. ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

Μελέτη περίπτωσης (11#25)

Η κλοπή προσωπικών δεδομένων

Το 2015, έπειτα από μη εξουσιοδοτημένη πρόσβαση χάκερς στα υπολογιστικά συστήματα δύο μεγάλων ασφαλιστικών εταιρειών (Anthem και Premera Blue Cross), στον χώρο της υγείας στις ΗΠΑ, εκλάπησαν δεδομένα που αφορούσαν 90 εκατομμύρια πολίτες. Πρόκειται για μία από τις μεγαλύτερες διαρροές δεδομένων παγκοσμίως. Ωστόσο, σε αρκετές ακόμα περιπτώσεις γίνονται παραβιάσεις, ίσως μικρότερης έκτασης, οι οποίες δεν έχουν δει το φως της δημοσιότητας για ευνόητους λόγους.

Οι επίσημα καταγραμμένες διαδικτυακές επιθέσεις με παραβιάσεις συστημάτων και κλοπές προσωπικών δεδομένων έφτασαν παγκοσμίως μέσα στο 2016 τις 1.093, με κλοπή 39 εκατομμυρίων εγγραφών (από 780 το 2015 με κλοπή 169 εκατομμυρίων εγγραφών).

Ωστόσο, η μεγαλύτερης έκτασης παραβίαση προσωπικών δεδομένων έγινε το 2014, όταν από την εταιρεία παροχής εξυπηρετήσεων ηλεκτρονικού ταχυδρομείου Yahoo εκλάπησαν 500 εκατομμύρια λογαριασμοί χρηστών!

3. ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

Μελέτη περίπτωσης (12#25)

Μηνύματα τύπου scam

Τα μηνύματα αυτά αποστέλλονται μαζικά σε εκατομμύρια διευθύνσεις και υπόσχονται κέρδη από λοταρίες, κληρονομιές, επενδύσεις, δάνεια, τραπεζικές μεταφορές χρημάτων κ.ά., σε μια προσπάθεια χειραγώγησης της αγοράς. Προτρέπουν τους παραλήπτες, με διάφορους τρόπους εντέλει, να τους διαβιβάσουν προσωπικά δεδομένα για να τους μεταβιβάσουν ή για να τους καταθέσουν μεγάλα χρηματικά ποσά (τα οποία δεν λαμβάνονται ή δεν κατατίθενται ποτέ). Με κάποια άλλα μηνύματα τύπου scam, υποτίθεται ότι επιζητείται η δημιουργία προσωπικών σχέσεων. Μέσα από την υποτιθέμενη σχέση δημιουργείται η απαραίτητη οικειότητα για τη δημιουργία αιτήματος αποστολής χρημάτων, σεξουαλικών φωτογραφιών ή/και βίντεο και μετέπειτα εκβιασμού του θύματος με βάση το οπτικό υλικό.

Τέτοια μηνύματα θα πρέπει να διαγράφονται άμεσα από τα εισερχόμενα του ταχυδρομείου.

3. ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

Μελέτη περίπτωσης (13#25)

Η ανησυχία για το δίκτυο ελέγχου και διανομής ηλεκτρικής ενέργειας των ΗΠΑ

Τον Ιούλιο του 2017, μέσω αναφοράς από την Εθνική Ακαδημία Επιστημών των ΗΠΑ, εκφράστηκαν ανησυχίες για το δίκτυο ελέγχου και διανομής ηλεκτρικής ενέργειας της χώρας.

Η σχετική αναφορά περιέγραφε ότι το δίκτυο είναι ευάλωτο σε επιθέσεις από τον κυβερνοχώρο και πιθανή καταστροφή με κόστος δισεκατομμυρίων δολαρίων και σοβαρές απειλές για τη δημόσια ασφάλεια, την υγεία και ενδεχομένως την εθνική ασφάλεια.

Η αναφορά κατέληγε ότι είναι επιβεβλημένη η επαγρύπνηση και η ανάπτυξη τεχνολογιών και στρατηγικών για την ελαχιστοποίηση της πιθανότητας διακοπής και η επένδυση στην ανάπτυξη της προστασίας των συνεχώς αυξανόμενων απειλών και του τρόπου αντιμετώπισής τους.

3. ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

Μελέτη περίπτωσης (14#25)

Ψευδείς ειδήσεις και απώλεια στο χρηματιστήριο αξιών

Το 2013 χάθηκαν από το χρηματιστήριο αξιών των ΗΠΑ 136 δισεκατομμύρια δολάρια μέσα σε ένα λεπτό. Η αιτία ήταν μία ψευδής είδηση που μεταδόθηκε από το Associated Press μέσω του Twitter. Η είδηση έγραφε ότι βομβαρδίστηκε το Πεντάγωνο και τραυματίστηκε ο Πρόεδρος των ΗΠΑ. Είχε γίνει όμως από άγνωστο χάκερ που απέκτησε πρόσβαση στον λογαριασμό του πρακτορείου στο μέσο κοινωνικής δικτύωσης.

3. ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

Μελέτη περίπτωσης (15#25)

Η επίθεση στην τράπεζα Tesco Bank

Το 2016 και μέσα σε ένα σαββατοκύριακο έγινε επίθεση από χάκερ στην αγγλική τράπεζα Tesco Bank, η οποία αναγκάστηκε να σταματήσει τις διαδικτυακές εξυπηρετήσεις της. Διαπιστώθηκε ότι είχαν υπονομευτεί 40 χιλιάδες τρεχούμενοι λογαριασμοί πελατών της και σε 20 χιλιάδες από αυτούς είχαν πραγματοποιηθεί δόλιες συναλλαγές.

3. ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

Μελέτη περίπτωσης (16#25)

Η διαδικτυακή παρενόχληση

Αυτό το είδος της παρενόχλησης (cyber bullying) μπορεί να προκαλέσει σημαντικά ψυχολογικά προβλήματα και να οδηγήσει τα θύματα σε ακραίες πράξεις αυτοκαταστροφής. Η αίσθηση της κοινωνικής κατακραυγής και το αίσθημα της ντροπής ξεπερνούν τα όρια της απόγνωσης, συχνά, με θλιβερές συνέπειες.

3. ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

Μελέτη περίπτωσης (17#25)

Η εκδικητική πορνογραφία

Η εκδικητική πορνογραφία αποτελεί μία ακραία μορφή παρενόχλησης και σχετίζεται με δημοσιοποίηση αποκαλυπτικών ή σεξουαλικών φωτογραφιών ή βίντεο ενός προσώπου χωρίς τη συγκατάθεσή του από έναν πρώην σεξουαλικό σύντροφο, με στόχο τον διασυρμό και τη μείωση της προσωπικότητάς του.

Τον Σεπτέμβριο του 2016, μία γυναίκα 31 ετών στην περιοχή της Νάπολης στην Ιταλία αυτοκτόνησε όταν ο πρώην σύντροφός της ανάρτησε βίντεο ερωτικού περιεχομένου στο Facebook, το οποίο είχε τραβήξει με κινητό κατά την περίοδο που διατηρούσαν σχέσεις. Η ψυχολογική πίεση που δέχτηκε ήταν τόσο μεγάλη ώστε δυστυχώς δεν κατάφερε να την ξεπεράσει.

3. ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

Μελέτη περίπτωσης (18#25)

Η σεξουαλική παρενόχληση

Ένα είδος παρενόχλησης είναι και η σεξουαλική παρενόχληση (sexual bullying), η οποία αποτελεί ένα είδος διαδικτυακής παρενόχλησης. Μπορεί να περιλαμβάνει σεξιστικά σχόλια ή ενέργειες εστιασμένες στο φύλο ή στον σεξουαλικό προσανατολισμό ή στη σεξουαλική δραστηριότητα ενός ατόμου μέσω του διαδικτύου, με στόχο να προσβάλουν, να εκφοβίσουν ή να βλάψουν.

3. ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

Μελέτη περίπτωσης (19#25)

Το ξέπλυμα μαύρου χρήματος

Τα τελευταία χρόνια έχουν συλληφθεί και φυλακιστεί πολλά άτομα για ξέπλυμα μαύρου χρήματος. Κάποια από αυτά είναι στελέχη μεγάλων εταιρειών.

Σε μία μόνο περίπτωση, τον Ιανουάριο του 2017, η εταιρεία Western Union συμφώνησε με τις δικαστικές αρχές των ΗΠΑ να αποδώσει 586 εκατομμύρια δολάρια ώστε να μη δικαστεί για μη τήρηση αποτελεσματικού προγράμματος κατά της νομιμοποίησης εσόδων από παράνομες δραστηριότητες και ξεπλύματος μαύρου χρήματος.

3. ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

Μελέτη περίπτωσης (20#25)

Η κοινωνική πληροφοριακή απάτη και ο Κέβιν Μίτνικ

Ο όρος «κοινωνική πληροφοριακή απάτη» εισήχθη από τον πρώην χάκερ Κέβιν Μίτνικ, ο οποίος υποστήριξε ότι για έναν χάκερ είναι πολύ πιο εύκολο να παραπλανήσει το θύμα ώστε να του παραδώσει τα διακριτικά του παρά να αφιερώσει χρόνο και κόπο για να εισβάλει σε έναν λογαριασμό.

Ο Μίτνικ, που είναι σήμερα σύμβουλος ασφαλείας και έχει δική του εταιρεία, θεωρείται ο μεγαλύτερος χάκερ στην ιστορία των υπολογιστών. Συνελήφθη το 1988 και φυλακίστηκε για έναν χρόνο για μη εξουσιοδοτημένη πρόσβαση σε επικοινωνιακό δίκτυο υπολογιστών, κλοπή δεδομένων και κώδικα.

Ομοίως, συνελήφθη και πάλι το 1995 και φυλακίστηκε για περίπου πέντε χρόνια, για δεκατέσσερα ίδια όπως προηγουμένως αδικήματα. Από τα περίπου πέντε χρόνια που φυλακίστηκε, πέρασε οκτώ μήνες στην απομόνωση, λόγω των φόβων που είχαν διαδοθεί για τις ικανότητές του να προκαλέσει πρόβλημα ακόμα και από το τηλεφωνικό κέντρο της φυλακής. Επί τρία χρόνια μετά την αποφυλάκισή του δεν του επετράπη η πρόσβαση σε πληκτρολόγιο και υπολογιστή.

3. ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

Μελέτη περίπτωσης (21#25)

Παράδειγμα από αυθεντική προσπάθεια αθέμιτης απόκτησης διακριτικών ηλεκτρονικού ταχυδρομείου (phising)

Από: info@atacer.org.ar
Προς: undisclosed-recipients;
Θέμα: Your email account

Το γραμματοκιβώτιό σας έχει υπερβεί το μέγεθος που καθορίζεται από τους περιορισμούς διαχειριστή. Το μέγεθος του γραμματοκιβωτίου σας είναι 78.944 KB. Πρόκειται για μια προειδοποίηση που φτάνει το γραμματοκιβώτιό σας 70.000 KB. Δεν μπορείτε να στείλετε ή να λάβετε νέα μηνύματα ηλεκτρονικού ταχυδρομείου. Για να είναι διαθέσιμο, κάντε κλικ στον παρακάτω σύνδεσμο και συμπληρώστε τη φόρμα για να αυξήστε το μέγεθος του γραμματοκιβωτίου σας.
http://tinyurl.com/accounti
Διαφορετικά, θα έχει ως αποτέλεσμα το κλείσιμο εντός 24 ωρών από το μήνυμα.
Διαχειριστής συστήματος διαχείρισης ιστού

3. ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

Μελέτη περίπτωσης (22#25)

Πώληση προϊόντων μαζικής επιτήρησης στα αραβικά κράτη

Τον Ιούνιο του 2017 ήρθε στο φως έρευνα από το BBC Arabic και μια εφημερίδα από τη Δανία. Μέσα από αυτή, έγινε γνωστό ότι η βρετανική αμυντική βιομηχανία BAE Systems έχει πραγματοποιήσει πωλήσεις μεγάλης κλίμακας σε αραβικά κράτη, με προϊόντα εξελιγμένης τεχνολογίας επιτήρησης πολιτών.

Στα προϊόντα περιλαμβάνεται και εδικό λογισμικό αποκρυπτογράφησης μηνυμάτων και παρακολούθησης οποιασδήποτε διαδικτυακής κίνησης για εκατομμύρια ανθρώπους, καθώς και εντοπισμού θέσης. Τα προϊόντα που πωλήθηκαν δυνητικά θα μπορούσαν να χρησιμοποιηθούν και εναντίον του Ηνωμένου Βασιλείου.

3. ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

Μελέτη περίπτωσης (23#25)

Η ασφάλεια μηνυμάτων ηλεκτρονικού ταχυδρομείου

Πρέπει να ληφθεί υπόψη ότι, όταν αποσταλεί ένα μήνυμα ηλεκτρονικού ταχυδρομείου, φεύγει από τον διακομιστή αλληλογραφίας του παρόχου και ταξιδεύει σε ένα μεγάλο μέρος του διαδικτύου. Περνά από ένα πλήθος υπολογιστών-τροχονόμων και δεν είναι γνωστό σε κανέναν αν και ποιος έχει πρόσβαση σ' αυτούς. Κανένας δεν μπορεί να γνωρίζει επίσης ότι δεν έχει υπονομευτεί η ασφάλεια του μηνύματος. Θα γίνει γνωστό ότι υπονομεύτηκε μόνον εφόσον διαπιστωθεί κάτι τέτοιο. Η συλλογιστική αυτή αποτελεί αρχή στην Πληροφορική!

3. ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

Μελέτη περίπτωσης (24#25)

Διαδικτυακά παιχνίδια αυτοκαταστροφής

Το 2017 ξεκίνησε από τη Ρωσία το διαδικτυακό παιχνίδι αυτοκαταστροφής «Blue Whale Challenge» (Πρόκληση της μπλε φάλαινας), το οποίο εξαπλώθηκε γρήγορα σε όλο τον κόσμο με τη βοήθεια των μέσων κοινωνικής δικτύωσης. Το όνομά του συνδέθηκε με τις φάλαινες, επειδή αυτά τα θηλαστικά θεωρείται ότι έχουν την τάση να αυτοκτονούν πλέοντας σε αβαθή θαλάσσια μέρη.

Το παιχνίδι αποτελείτο από 50 ημερήσιες δράσεις-προκλήσεις. Κάθε μέρα ο παίκτης, προκειμένου να κερδίσει μία πρόκληση, θα έπρεπε να εκτελέσει μία εντολή, σύμφωνα με οδηγία που λάμβανε από την ομάδα των διαχειριστών του παιχνιδιού. Οι εντολές ξεκινούσαν από σχετικά ήπιες και αβλαβείς και κατέληγαν σε όλο και περισσότερο βλαπτικές ή αυτοκαταστροφικές για τους παίκτες. Για παράδειγμα, μία πρόκληση θα μπορούσε να είναι η λήψη μιας φωτογραφίας τύπου σέλφι του παίκτη, ενώ θα βρισκόταν στη στέγη του ψηλότερου κτιρίου της πόλης που διέμενε ή σε σιδηροδρομικές γραμμές με το τρένο να πλησιάζει. Τελικά, για να κερδίσει κανείς το παιχνίδι, ο μόνος τρόπος ήταν να αυτοκτονήσει.

Με το συγκεκριμένο παιχνίδι συνδέθηκαν οι αυτοκτονίες 130 εφήβων. Η «Πρόκληση της μπλε φάλαινας» αποτέλεσε τη συνέχεια στην έρευνα για τέτοιου είδους διαδικτυακά παιχνίδια, που οδηγούσαν σε αυτοκαταστροφή μέσω καθοδήγησης.

3. ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

Μελέτη περίπτωσης (25#25)

Διαδικτυακά παιχνίδια αυτοκαταστροφής

Τον Αύγουστο του 2017, επίσης, ένα άλλο παιχνίδι αυτοκαταστροφής, το «Salt and Ice Challenge», βρέθηκε να έχει μεγάλη απήχηση στη νεολαία, διαδιδόμενο από τα μέσα κοινωνικής δικτύωσης. Οι συμμετέχοντες συναγωνίζονταν για τη χρονική διάρκεια που μπορούν να αντέξουν τον πόνο, ο οποίος δημιουργείται αν τοποθετήσουν αλάτι σε ένα σημείο του σώματός τους και πιέσουν ακολούθως στο σημείο εκείνο με ένα παγάκι.

Υπόψη ότι το αλάτι σε συνδυασμό με τον πάγο φτάνει τοπικά τη θερμοκρασία έως -17oC και μπορούν έτσι σε χρονικό διάστημα μικρότερο από 10 λεπτά να δημιουργηθούν στο σώμα εγκαύματα έως τρίτου βαθμού.

3. ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

Η πνευματική ιδιοκτησία - Ο μύθος για το διαδίκτυο

- **Αποτελεί μύθο για το διαδίκτυο ότι οτιδήποτε είναι δημοσιευμένο εκεί μπορεί ελεύθερα να αντιγραφεί ή να μεταφορτωθεί σε υπολογιστή και να επαναχρησιμοποιηθεί.**
- **Το υλικό του διαδικτύου προστατεύεται από τα ίδια πνευματικά δικαιώματα και με τον ίδιο τρόπο, όπως και οποιοδήποτε άλλο υλικό συναντούμε στη βιβλιοθήκη ή στο βιβλιοπωλείο.**
- **Ουσιαστικά, όταν μεταφορτώνουμε ή αντιγράφουμε το περιεχόμενο μιας οποιασδήποτε ιστοσελίδας που δεν επιτρέπει ρητά κάτι τέτοιο, είναι ακριβώς το ίδιο από πλευράς πνευματικών δικαιωμάτων με το να δημιουργούμε ένα αντίγραφο ενός βιβλίου που βρήκαμε στη βιβλιοθήκη.**

3. ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

Η πνευματική ιδιοκτησία – είδη

Η πνευματική ιδιοκτησία (intellectual property) είναι η ιδιοκτησία ενός έργου που παράγεται από πρωτότυπη σκέψη και αναφέρεται σε:

Πνευματικά δικαιώματα (copyrights)

Διπλώματα ευρεσιτεχνίας (patents), και

Κατατεθέντα σήματα (trademarks).

***Η πνευματική ιδιοκτησία*:**

Προστατεύει την αυθεντικότητα των έργων και των χαρακτηριστικών που τα καθιστούν λειτουργικά και επιτρέπει στους δημιουργούς να επωφεληθούν από αυτά.

3. ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

Τα Πνευματικά Δικαιώματα και οι δημιουργοί

Τα πνευματικά δικαιώματα είναι δικαιώματα που κατέχουν οι δημιουργοί για:

- **Λογοτεχνικά έργα: μυθιστορήματα, ποιήματα, βιβλία, περιοδικές εκδόσεις, περιοδικά, εφημερίδες, συλλογές, θεατρικά έργα, ταινίες, μουσικές συνθέσεις, χορογραφίες.**

Στα προηγούμενα εντάσσονται οι εφαρμογές λογισμικού και το υλικό για τον σχεδιασμό τους, όπως π.χ. οι βάσεις δεδομένων (Ευρωπαϊκή Οδηγία 91/250 και Ν. 2121/1993).

- **Καλλιτεχνικά έργα: πίνακες ζωγραφικής, σχεδιαγράμματα, τεχνικά σχέδια, χάρτες, φωτογραφίες, γλυπτά, αρχιτεκτονική, διαφημίσεις.**

Τα πνευματικά δικαιώματα προστατεύουν ένα έργο καθ' όλη τη ζωή του δημιουργού του, συν 70 χρόνια μετά τον θάνατο του (άρθρο 8 Ν. 2557/1997).

3. ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

Η πνευματική ιδιοκτησία - Τα Διπλώματα Ευρεσιτεχνίας

Τα διπλώματα ευρεσιτεχνίας (πατέντες) υποδηλώνουν την κατοχή αποκλειστικών δικαιωμάτων σε μία εφεύρεση, δηλαδή σε ένα καινοτόμο προϊόν ή μια καινοτόμα διαδικασία ή καινοτόμα τεχνική λύση σε ένα πρόβλημα.

3. ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

Η πνευματική ιδιοκτησία - Τα Κατατεθέντα Σήματα

Τα κατατεθέντα σήματα αποτελούν διακριτά εμπορικά σήματα τα οποία ταυτοποιούν εταιρείες, προϊόντα, υπηρεσίες.

Σ' αυτά περιλαμβάνονται λογότυποι, συνθήματα, σχέδια, σήματα.

3. ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

Η πνευματική ιδιοκτησία στο διαδίκτυο…

Το ηλεκτρονικό έγκλημα αυτής της μορφής στον χώρο της τεχνολογίας διαπράττεται όταν ένα άτομο λαμβάνει στον υπολογιστή του λογισμικό, παιχνίδια, ταινίες, μουσική κ.ά. ή αναδημοσιεύει υλικό που δεν του ανήκει, χωρίς απόδοση πνευματικών δικαιωμάτων στους δημιουργούς.

Στο διαδίκτυο ιστοχώροι και εφαρμογές peer-to-peer υποβοηθούν τη λήψη κάθε είδους αρχείων χωρίς απόδοση δικαιωμάτων και σποραδικά στα ειδησεογραφικά πρακτορεία εμφανίζονται ειδήσεις από την εφαρμογή του νόμου στον χώρο αυτό και την τιμωρία τόσο ιδιωτών όσο και εταιρειών με υψηλά πρόστιμα.

3. ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

Η πνευματική ιδιοκτησία στο διαδίκτυο…

Σήμερα, η σύγχρονη ψηφιακή τεχνολογία επιτρέπει την εύκολη αναπαραγωγή και μετάδοση υλικού, με απώλεια παγκοσμίως δεκάδων δισεκατομμυρίων δολαρίων από τους δημιουργούς.

Οι πιο συνηθισμένες παραβάσεις: διαμοιρασμός αρχείων μουσικής, ταινιών και λογισμικού.

Καθημερινά, ένας τεράστιος αριθμός μουσικών κομματιών σε μορφή mp3 διακινείται παράνομα.

Εργαλεία που επιτρέπουν την αναζήτηση και τη λήψη μουσικών αρχείων χρησιμοποιούνται σε πραγματικό χρόνο από ιστοχώρους στο διαδίκτυο.

Το διαδίκτυο, από την αρχή της λειτουργίας του, έχει χαρακτηριστεί ως η μεγαλύτερη απειλή (κυρίως) για τα πνευματικά δικαιώματα.

3. ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

Η πνευματική ιδιοκτησία: Η απειλή - Το λογισμικό

Οι υποστηρικτές της τήρησης της νομιμότητας στη διακίνηση υλικού με πνευματικά δικαιώματα θεωρούν ότι η κλοπή των έργων εκτός από την οικονομική απώλεια αποδυναμώνει και δεν βοηθά την περαιτέρω δημιουργική προσπάθεια των δημιουργών.

Στον αντίποδα, υπάρχουν υποστηρικτές του ανοικτού - ελεύθερου λογισμικού, που μάχονται μετά μανίας την καθιέρωση της πνευματικής ιδιοκτησίας, ιδιαίτερα στο λογισμικό.

Ωστόσο, η πειρατεία του λογισμικού ανθεί στο διαδίκτυο.

- **Crackers**
- **Οι κατάλογοι με σειριακούς αριθμούς χρήσης (serial numbers)**
- **Cracks**

3. ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

Η πνευματική ιδιοκτησία - Λογισμικό shareware και freeware

Συχνά συναντώνται οι όροι shareware και freeware, που αναφέρονται σε λογισμικό στο οποίο *ο κατασκευαστής του διατηρεί τα αποκλειστικά δικαιώματα χρήσης και διανομής*.

Ο όρος shareware αναφέρεται σε λογισμικό το οποίο μπορεί να αντιγραφεί από οποιονδήποτε και να χρησιμοποιηθεί ελεύθερα εντός περιορισμένου χρονικού διαστήματος (δοκιμή). Μετά την παρέλευση του ορισμένου χρονικού διαστήματος το λογισμικό, συνήθως, κλειδώνει και η περαιτέρω χρήση του μπορεί να γίνει μόνο εφόσον αγοραστεί.

Ο όρος freeware αναφέρεται σε λογισμικό που διατίθεται ως ένα είδος προσφοράς, σε οποιονδήποτε το θελήσει, δωρεάν και για απεριόριστο χρόνο.

3. ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

Η πνευματική ιδιοκτησία - Πνευματικά δικαιώματα & λογισμικό

Ο Αμερικανός ακτιβιστής Richard Stallman συγκαταλέγεται μεταξύ των θεμελιωτών του Ιδρύματος Ελεύθερου Λογισμικού (1991).

Ο Stallman και το κίνημα που δημιουργήθηκε δεν αποδέχεται την ύπαρξη πνευματικών δικαιωμάτων στο λογισμικό.

Τόσο αυτός όσο και άλλοι που ασπάζονται τις ίδιες ιδέες θεωρούν ότι όλες οι εφαρμογές θα πρέπει να διαμοιράζονται χωρίς κόστος και με μορφή ανοικτού κώδικα.

- ***Ο αλγόριθμος***

Την ίδια στιγμή διάφορες επιστημονικές ενώσεις και εθελοντικές επιστημονικές οργανώσεις κινούνται όλο και περισσότερο προς την κατεύθυνση της παραγωγής ελεύθερου – ανοικτού λογισμικού (open source).

3. ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

Η πνευματική ιδιοκτησία - Ευρεσιτεχνία και αλγόριθμος

Η ευρεσιτεχνία σε έναν αλγόριθμο αποτελεί πολύπλοκο και αμφιλεγόμενο θέμα, γιατί:

- **Μπορεί να απαγορευτεί η χρήση των μαθηματικών τύπων από τους οποίους συνίσταται ο αλγόριθμος;**
- **Ανήκει σε κάποιον ένας μαθηματικός τύπος από τη στιγμή μάλιστα που για να φτάσει σ' αυτόν σίγουρα χρησιμοποίησε άλλους;**
- **Έχει ελεγχθεί ότι ο εξεταζόμενος αλγόριθμος δεν συγκρούεται ή δεν παραβιάζει δικαιώματα άλλων κατασκευαστών με ήδη κατοχυρωμένους αλγορίθμους; Πόσο εύκολο είναι αυτό;**

- Γενικά, *πρόκειται για χρονοβόρες και υψηλού κόστους διαδικασίες, που δεν ευνοούν μικρές εταιρείες ή ιδιώτες και δεν συμβάλλουν στην αύξηση του ανταγωνισμού*.

3. ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

Η πνευματική ιδιοκτησία - Το λογισμικό ανοικτού κώδικα

Η δήλωση ότι ένα λογισμικό είναι ανοικτού κώδικα (open source) συναρτάται με το αν επιτρέπεται σε οποιονδήποτε προγραμματιστή να έχει πρόσβαση σε όλο τον κώδικα αυτού και δυνατότητα επαναχρησιμοποίησης .

Το λογισμικό αυτής της μορφής δίνει τη δυνατότητα σε άλλους προγραμματιστές να δοκιμάσουν τις δυνατότητες μιας εφαρμογής, να συμβάλουν στη βελτίωσή της και να δημιουργήσουν τις δικές τους διανομές (εκδόσεις).

- ***Αποτελεί ένα είδος συνεισφοράς προς την κοινωνία, από αυτούς που κατέχουν τη γνώση σε ένα πεδίο.***
- ***Σχεδόν σε κάθε εμπορική εφαρμογή πλέον αντιστοιχεί και μία ανοικτού κώδικα.***

3. ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

Η πνευματική ιδιοκτησία - Το λογισμικό ανοικτού κώδικα

Πλεονεκτήματα

- **Συλλογικό έργο με στόχο τη βελτίωση ενός προϊόντος μέσα από ένα είδος κοινωνικής αλληλεπίδρασης, χωρίς οικονομική επιβάρυνση του χρήστη, χωρίς κακώς εννοούμενο ανταγωνισμό και μονοπωλιακές καταστάσεις.**
- **Ένα προϊόν μπορεί να εξελίσσεται συνεχώς και να προσαρμόζεται, επίσης, συνεχώς σε νέες απαιτήσεις.**

Μειονεκτήματα

- **Η δημιουργία γίνεται ερήμην των χρηστών, με απαιτήσεις που εξάγονται μόνο από προγραμματιστές και προδιαγραφές που απέχουν από τις ανάγκες του μέσου χρήστη σε λειτουργικότητα και φιλικότητα.**
- **Ανοικτός κώδικας = ευάλωτο σύστημα.**

3. ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

Η πνευματική ιδιοκτησία - Οι άδειες Creative Commons

Εξαιρουμένου του λογισμικού, οι δημιουργοί φωτογραφιών, μουσικών έργων ή συγγραφείς βιβλίων μπορούν να διαθέσουν σε ψηφιακή μορφή τα έργα τους για χρήση μέσω αδειών τύπου creative commons, προστατεύοντας τα δικαιώματα της πνευματικής ιδιοκτησίας τους.

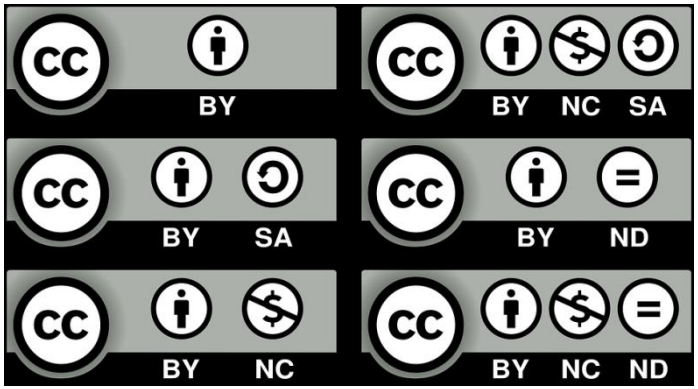
Οι τύποι των αδειών καθορίστηκαν από μία μη κερδοσκοπική οργάνωση που εδρεύει στις ΗΠΑ, την Creative Commons Corporation.

3. ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

Η πνευματική ιδιοκτησία - Οι άδειες Creative Commons

Κάθε άδεια αναφέρει τις προϋποθέσεις χρήσης ενός έργου, δηλαδή το θέμα της αναφοράς στον δημιουργό και το αν επιτρέπεται η εμπορική χρήση του, η μετατροπή του και η αναδιανομή του με νέα μορφή.

Ουσιαστικά, οι δημιουργοί παραχωρούν μέρος των δικαιωμάτων επί του έργου τους σε τρίτο πρόσωπο υπό προϋποθέσεις, προκειμένου αυτό να αξιοποιηθεί επωφελώς τόσο γι' αυτούς όσο και για το κοινωνικό σύνολο ή το δημόσιο συμφέρον.



3. ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

Η πνευματική ιδιοκτησία - Οι άδειες Creative Commons

Παντού και πάντα Αναφορά Δημιουργού (ΑΔ)

ΑΔ | CC BY

ΑΔ - Παρόμοια Διανομή | CC BY-SA

ΑΔ - Όχι Παράγωγα Έργα | CC BY-ND

ΑΔ - Μη Εμπορική Χρήση | CC BY-NC

ΑΔ - Μη Εμπορική Χρήση - Παρόμοια Διανομή | CC BY-NC-SA

ΑΔ - Μη Εμπορική Χρήση - Όχι Παράγωγα Έργα | CC BY-NC-ND

3. ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

Η πνευματική ιδιοκτησία - Η κατασκευή ενός ιστοχώρου

Μία από τις σημαντικότερες εξυπηρετήσεις του διαδικτύου έχει ως βάση τους ιστοχώρους. Για την κατασκευή ενός ιστοχώρου, ασχέτως σκοπού ή στόχων που θα εξυπηρετεί, θα πρέπει να δίνεται ιδιαίτερη προσοχή στα ακόλουθα:

- **Το περιεχόμενο ενός ιστοχώρου, από πλευράς πνευματικών δικαιωμάτων, θα πρέπει να ανήκει στον κατασκευαστή του.**
- **Δεν πρέπει να ενσωματώνονται τμήματα άλλων ιστοχώρων (κάθε μορφής πολυμορφική πληροφορία), εκτός και αν αυτά διατίθενται ελεύθερα.**
- **Αν αναρτηθούν κείμενα, ο συγγραφέας θα πρέπει να κατέχει την πνευματική ιδιοκτησία τους. Η χρήση του κειμένου ή της ιδέας κάποιου άλλου, ακόμα και με παράφραση, θα πρέπει να συνοδεύεται με αναγνώριση των πνευματικών δικαιωμάτων. Αν χρειαστεί να παρατεθούν ελάχιστα αποσπάσματα, ακριβώς όπως αναφέρονται στην πηγή τους, θα πρέπει να γραφούν εντός εισαγωγικών και με μνεία της πηγής λήψης.**
- **Δεν επιτρέπεται η παράθεση προσωπικών δεδομένων ή στοιχείων που ταυτοποιούν άλλους ανθρώπους.**
- **Δεν επιτρέπεται η ανάρτηση περιεχομένου συνομιλιών ή μηνυμάτων ούτε ηλεκτρονικές διευθύνσεις άλλων χωρίς την άδειά τους.**
- **Για κάθε λογότυπο, εικονίδιο ή αναγνωριστικό σήμα εταιρείας που χρησιμοποιείται και δεν ανήκει στον κατασκευαστή του ιστοχώρου θα πρέπει να υπάρχει άδεια χρήσης.**
- **Ακόμα και η σύνδεση με ιστοσελίδες άλλων ιστοχώρων γίνεται υπό προϋποθέσεις. Απαιτείται έλεγχος των απαιτήσεων (αν υπάρχουν) για οποιονδήποτε εξωτερικό σύνδεσμο σε άλλη ιστοσελίδα.**

3. ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

Η πνευματική ιδιοκτησία - Προσέχουμε!

Όπως προκύπτει από τα παραπάνω:

- **Από το διαδίκτυο ΤΙΠΟΤΑ δεν μπορούμε να χρησιμοποιήσουμε ελεύθερα, αλλά μόνο υπό προϋποθέσεις!**
- **Η χρήση στοιχείων από το διαδίκτυο πρέπει να γίνεται με μεγάλη προσοχή και σεβασμό στους δημιουργούς!**
- **Ο πολιτισμός μας στηρίζεται σε μεγάλο βαθμό στο σεβασμό!**
- **Αν θέλουμε να μας σέβονται οι άλλοι πρέπει πρώτα να τους σεβόμαστε εμείς!**

3. ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

Η αστυνομία του κυβερνοχώρου

Παγκοσμίως: *Αστυνομία του Παγκόσμιου Ιστού* (Web Police) – 1986. Συνεργάζεται με την Interpol, την Europol και τις Αρχές κάθε χώρας.

Ελλάδα: *Τμήμα Δίωξης Ηλεκτρονικού Εγκλήματος* της Ελληνικής Αστυνομίας, το οποίο το 2014 αναβαθμίστηκε σε *Διεύθυνση Ηλεκτρονικού Εγκλήματος*.

Το 2003 στη χώρα μας συστάθηκε η ανεξάρτητη ***Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ)***, με σκοπό «την προστασία του απορρήτου των επιστολών, της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιονδήποτε άλλο τρόπο καθώς και την ασφάλεια των δικτύων και πληροφοριών» (http://www.adae.gr/).

3. ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

Οι νομοθετικές παρεμβάσεις - Στην Ευρώπη:

• Οδηγία 1995/46 - για διασφάλιση των αρχών της δικαιοσύνης και νομιμότητας, της ακεραιότητας και ασφάλειας, της ανάγκης συλλογής και επεξεργασίας των δεδομένων.

• Οδηγία 2002/58 – για τον καθορισμό πλαισίου επεξεργασίας δεδομένων προσωπικού χαρακτήρα και προστασίας του ιδιωτικού βίου σε σχέση με την τεχνολογία και την ηλεκτρονική επικοινωνία. Τροποποιήθηκε με την Οδηγία 2009/136 και τον Κανονισμό 611/2013.

• Οδηγία 2006/24 – για τη διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημόσιων δικτύων επικοινωνιών. Με την ίδια τροποποιήθηκε η Οδηγία 2002/58.

• Οδηγία 2009/136 - για την καθολική υπηρεσία και τα δικαιώματα των χρηστών δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών.

• Οδηγία 2013/40 – επιβολή νέων κανόνων για την ποινικοποίηση και τις ποινές σειράς αδικημάτων που στρέφονται κατά των συστημάτων πληροφοριών.

• Κανονισμός 611/2013 - για κοινοποίηση παραβιάσεων προσωπικών δεδομένων και την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες.

• Κανονισμός 2120/2015 - καθιερώνεται η αρχή της δικτυακής ουδετερότητας στους παρόχους, οι οποίοι δεν περιορίζουν και δεν εισάγουν διακρίσεις σε περιεχόμενο, υπηρεσίες και εφαρμογές.

• Οδηγία 2016/1148 - για λήψη μέτρων για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ευρωπαϊκή Ένωση.

3. ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

Οι νομοθετικές παρεμβάσεις - Στην Ελλάδα (1#2):

- Ν. 2472/1997, για τη ρύθμιση θεμάτων που αφορούν την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα.
- Ν. 2672/1998, για θέματα που αφορούν τη διακίνηση εγγράφων με ηλεκτρονικά μέσα (τηλεομοιοτυπία, ηλεκτρονικό ταχυδρομείο).
- ΠΔ 342/2002, για το πλαίσιο της διακίνησης εγγράφων μέσω ηλεκτρονικού ταχυδρομείου μεταξύ φορέων και υπηρεσιών της δημόσιας διοίκησης ή μεταξύ νομικών και φυσικών προσώπων του ιδιωτικού δικαίου.
- Ν. 3115/2003 και Ν. 3472/2006, για τη διασφάλιση του απορρήτου των επικοινωνιών με οποιονδήποτε τρόπο, μέσω της ανεξάρτητης Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ).
- Ν. 3242/2004, για το πλαίσιο της διεκπεραίωσης τελικών πράξεων διοικητικών συναλλαγών με χρήση ηλεκτρονικών μέσων.
- Ν. 3471/2006, για το πλαίσιο της προστασίας των προσωπικών δεδομένων και της ιδιωτικής ζωής από τις ηλεκτρονικές επικοινωνίες (αποτελεί τροποποίηση του Ν. 2472/1997).
- Ν. 3674/2008, για τη διασφάλιση του απορρήτου των τηλεφωνικών επικοινωνιών και το Εθνικό Σχέδιο Ασφάλειας Ηλεκτρονικών Επικοινωνιών.

3. ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

Οι νομοθετικές παρεμβάσεις - Στην Ελλάδα (2#2):

- Ν. 3783/2009, για την ταυτοποίηση των κατόχων και χρηστών εξοπλισμού και υπηρεσιών κινητής τηλεφωνίας.
- Ν. 3917/2011, για τη ρύθμιση θεμάτων σχετικών με τη 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. Ο νόμος τροποποιήθηκε με τον Ν. 3994/2011 και τον Ν. 4139/2013.
- Ν. 3979/2011, για την υποχρέωση των δημόσιων φορέων στη δημιουργία και λειτουργία ιστοχώρου και την εισαγωγή της χρήσης της ψηφιακής υπογραφής για τη σήμανση, πιστοποίηση και εγκυροποίηση των ηλεκτρονικών εγγράφων που αποστέλλονται από φυσικά πρόσωπα (ηλεκτρονική διακυβέρνηση).
- Ν. 4070/2012, για τη ρύθμιση θεμάτων που αφορούν τις ηλεκτρονικές επικοινωνίες και τις διαδικασίες πολιτικής και ελέγχου των.
- Π.Δ. 178/2014, για τη ρύθμιση της οργάνωσης της Διεύθυνσης Δίωξης Ηλεκτρονικού Εγκλήματος στην Ελληνική Αστυνομία.
- Ν. 4411/2016, για την ποινικοποίηση ηλεκτρονικών εγκλημάτων σχετικών με ρατσισμό και ξενοφοβία.

3. ΤΟ ΗΛΕΚΤΡΟΝΙΚΟ ΕΓΚΛΗΜΑ

Οι νομοθετικές παρεμβάσεις – GDPR (από 25/5/2018)

Πλαίσιο για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα:

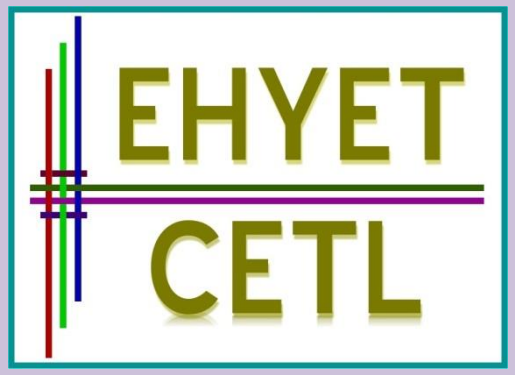
(1) Η επεξεργασία ιδιωτικών δεδομένων πρέπει να γίνεται μόνο κατόπιν σαφούς συγκατάθεσης του κατόχου.

(2) Ο κάτοχος των δεδομένων πρέπει να έχει εύκολη πρόσβαση στα προσωπικά του δεδομένα, να μπορεί να τα ελέγξει, να τα διορθώσει ή και να τα διαγράψει μονίμως από το διαδίκτυο.

(3) Η δημιουργία προφίλ κάθε ανθρώπου από την επεξεργασία των προσωπικών του δεδομένων, πρέπει να τίθεται ως διαδικασία υπό την έγκριση του κατόχου των δεδομένων.

(4) Οι εταιρείες μέσω των υπευθύνων προστασίας των ιδιωτικών δεδομένων που συλλέγουν από τους χρήστες των υπηρεσιών τους θα πρέπει: να παρέχουν εύκολη πρόσβαση στους κατόχους των δεδομένων και να τηρούν καθορισμένες διαδικασίες, που εγγυώνται την ασφάλεια των αποθηκευμένων δεδομένων ή την κοινοποίηση της ενδεχόμενης παραβίασής τους.

(5) Οι εταιρείες μέσω των υπευθύνων προστασίας των ιδιωτικών δεδομένων που συλλέγουν από τους χρήστες των υπηρεσιών τους θα πρέπει να παρέχουν στον κάτοχο το δικαίωμα της αντιγραφής των δεδομένων του σε μηχανικά αναγνώσιμο μορφότυπο, προκειμένου να ελεγχθούν από άλλον υπεύθυνο επεξεργασίας δεδομένων, εφόσον η συλλογή γίνεται αυτοματοποιημένα, με την έγκριση του κατόχου και σύννομα.



www.cetl.upatras.gr
cpanag@upatras.gr