ΔΙΑΔΙΚΤΥΟ

1. Το Διαδίκτυο και η Επικοινωνία

Με την εμφάνιση οποιουδήποτε νέου μέσου, ο τομέας της επικοινωνίας αναμφισβήτητα επηρεάζεται. Η επίδραση αυτή πηγάζει κυρίως από την τεχνολογία του νέου μέσου.

Σύμφωνα με την προσέγγιση της "ιντερνετοφιλίας", το Διαδίκτυο, αλλά και η ψηφιακή τεχνολογία γενικότερα, έχουν την ικανότητα να δημιουργούν "εικονικούς χώρους", "εικονικές κοινότητες", όπου παύουν να υφίστανται οι κοινωνικές και πολιτιστικές διαχωριστικές γραμμές που υπάρχουν στον πραγματικό κόσμο και που τα παραδοσιακά μέσα επικοινωνίας αδυνατούν να ξεπεράσουν εύκολα. Δίνεται η δυνατότητα σε κάθε χρήστη ηλεκτρονικού υπολογιστή συνδεδεμένου στο Διαδίκτυο, να πληροφορηθεί αλλά και να πληροφορήσει ανταλλάσσοντας απόψεις μέσω ενός πιο συμμετοχικοί και λιγότερο ελεγχομένου διαύλου επικοινωνίας. Οι χρήστες αποκτούν ολοένα και περισσότερο την ιδιότητα του παγκοσμίου πολίτη.

2. ΙΣΤΟΡΙΑ ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ

Οι πρώτες απόπειρες για την δημιουργία ενός διαδικτύου ξεκίνησαν στις ΗΠΑ κατά την διάρκεια του ψυχρού πολέμου. Δημιουργήθηκε το πρώτο είδος διαδικτύου γνωστό ως ARPANET. Εγκαταστάθηκε και λειτούργησε για πρώτη φορά το 1969 με 4 κόμβους μέσω των οποίων συνδέονται 4 μίνι υπολογιστές. . Η ταχύτητα του δικτύου έφθανε τα 50 kbps και έτσι επιτεύχθηκε η πρώτη *dial up* σύνδεση μέσω γραμμών τηλεφώνου.Το 1974 λοιπόν, δημοσιεύεται η μελέτη των *Vint Cerf* και Bob Kahn από την οποία προέκυψε το πρωτόκολλο TCP (Transmission Control Protocol) που αργότερα το 1978 έγινε TPC/IP, προσετέθη δηλαδή το Internet Protocol (IP), ώσπου το 1983 έγινε το μοναδικό πρωτόκολλο που ακολουθούσε το ARPANET. Το 1984 υλοποιείται το πρώτο *DNS* (Domain Name System) σύστημα στο οποίο καταγράφονται 1000 κεντρικοί κόμβοι και οι υπολογιστές του διαδικτύου πλέον αναγνωρίζονται από διευθύνσεις κωδικοποιημένων αριθμών. Ένα ακόμα σημαντικό βήμα στην ανάπτυξη του Διαδικτύου έκανε το Εθνικό Ίδρυμα Επιστημών (National Science Foundation,NSF) των ΗΠΑ, το οποίο δημιούργησε την πρώτη διαδικτυακή πανεπιστημιακή ραχοκοκαλιά (backbone), το NSFNet, το 1986. Ακολούθησε η ενσωμάτωση άλλων σημαντικών δικτύων, όπως το Usenet, το Fidonet και το Bitnet. Ο όρος Διαδίκτυο/Ιντερνετ ξεκίνησε να χρησιμοποιείται ευρέως την εποχή που συνδέθηκε το ARPANET με το NSFNet και Internet σήμαινε οποιοδήποτε δίκτυο χρησιμοποιούσε TCP/IP. Η μεγάλη άνθιση του Διαδικτύου όμως, ξεκίνησε με την εφαρμογή της υπηρεσίας του Παγκόσμιου Ιστού από τον Τιμ Μπέρνερς-Λι στο ερευνητικό ίδρυμα CERN το 1989, ο οποίος είναι στην ουσία, η "πλατφόρμα", η οποία κάνει εύκολη την πρόσβαση στο Ίντερνετ, ακόμα και στη μορφή που είναι γνωστό σήμερα.

3. Οι πληροφορίες στο Διαδίκτυο

Το Διαδίκτυο, σε συνδυασμό με την ολοένα αναπτυσσόμενη ψηφιακή τεχνολογία, έχει

δημιουργήσει μία τεράστια αγορά γνώσεων/πληροφοριών. Παραδοσιακές μορφές τέχνης(όπως για παράδειγμα ο κινηματογράφος και η μουσική) μέσω της ψηφιακής τεχνολογίας παίρνουν την ίδια μορφή με αντικείμενα που εκ πρώτης όψεως είναι εντελώς διαφορετικά. Παρατηρείται λοιπόν μία συγκέντρωση γνώσης ή, αν είναι δυνατό να λεχθεί, πολιτιστικής κληρονομιάς, που σχετίζεται άμεσα με το Ίντερνετ. Το μεγάλο ερώτημα που προκύπτει πλέον είναι το "ποιος θα διοικήσει, ποιος θα ελέγξει την γνώση αυτή". Από τη στιγμή που το Διαδίκτυο είναι ένα δίκτυο συνδεδεμένων υπολογιστών, κάθε χρήστης έχει την δυνατότητα να μοιραστεί πληροφορίες με άλλους χρήστες γενόμενος, πολλές φορές, ο ίδιος δημιουργός και πάροχος των πληροφοριών αυτών. Δεν υπάρχει άμεσος έλεγχος των πληροφοριών που "ανεβαίνουν" στο Διαδίκτυο από κάποιον ιεραρχικά ανώτερο χρήστη ή οργανισμό. λόγω της μεγάλης συγκέντρωσης γνώσης στο Διαδίκτυο, η έννοια της κοινωνικής ισότητας παίρνει και πάλι μεγάλη σημασία. Το χάσμα ανάμεσα σε πληροφοριακά πλούσιους και πληροφοριακά φτωχούς θα διευρύνεται όσο αυξάνεται η συγκέντρωση της γνώσης αυτής. Το παραπάνω αποτελεί ακόμα έναν λόγο που κάνει πιο επιτακτική την ανάγκη για διερεύνηση του αρχικού ερωτήματος "ποιος θα ελέγξει τη γνώση αυτή". Η γλώσσα που χρησιμοποιείται περισσότερο στη διακίνηση της πληροφορίας στο Διαδίκτυο είναι η Αγγλική. Έχοντας αναπτυχθεί τα τελευταία χρόνια, το Διαδίκτυο περιλαμβάνει πλέον ποιοτικά και ποσοτικά ευρύ περιεχόμενο και στις υπόλοιπες γλώσσες των περισσότερο αναπτυγμένων χωρών. Ωστόσο, υπάρχουν ακόμα δυσλειτουργίες και τεχνικά προβλήματα σχετικά με την κωδικοποίηση, όπως το mojibake.

4. Νομικά και ηθικά ζητήματα

Η παραβίαση πνευματικών δικαιωμάτων, η πορνογραφία, η ψευδοπροσωπία και η προσφορά παρανόμων προϊόντων είναι φαινόμενα υπαρκτά στο Ίντερνετ και ο περιορισμός τους είναι ιδιαίτερα δύσκολος. Το Διαδίκτυο έχει κατηγορηθεί ως παράγοντας που έπαιξε ρόλο σε θανάτους. Επιπλέον, το Διαδίκτυο είναι μη ελεγχόμενο, με την έννοια ότι δεν υπάρχει κάποια ενιαία κυβερνητική ή άλλη αντίστοιχη αρχή, η οποία θα ελέγχει το περιεχόμενό του πριν αυτό δημοσιευθεί -σύμφωνα με πολλούς χρήστες αυτό θα αποτελούσε λογοκρισία. Επίσης παρά το γεγονός ότι το Ίντερνετ συχνά περιγράφεται ως αποκεντρωμένο, με απροσπέλαστο όγκο πληροφοριών και, συνεπώς, χωρίς κεντρικό έλεγχο, είναι εμφανής η εκτενής ιεράρχηση του περιεχομένου από μηχανές αναζήτησης και η γενικότερη διαιώνιση των ιστοτόπων με την υψηλότερη επισκεψιμότητα.

5. Πρόσβαση στο Διαδίκτυο

Το δικαίωμα των Ευρωπαίων πολιτών για ελεύθερη πρόσβαση στο Διαδίκτυο κατοχυρώνεται στο άρθρο 11 του Χάρτη των Θεμελιωδών Δικαιωμάτων της Ευρωπαϊκής Ένωσης περί ελευθερίας της έκφρασης και της ενημέρωσης. Πρόσφατα στο Ευρωπαϊκό Κοινοβούλιο ψηφίστηκε τροπολογία σύμφωνα με την οποία «δεν μπορεί να επιβάλλεται περιορισμός επί των θεμελιωδών δικαιωμάτων και ελευθεριών των τελικών χρηστών, χωρίς να προηγηθεί δικαστική απόφαση... εκτός από περιπτώσεις όπου απειλείται η ασφάλεια των πολιτών και στις οποίες η απόφαση δύναται να είναι αντίστοιχη». Ακόμη όμως και με την εν λόγω τροπολογία η πρόσβαση στο Διαδίκτυο θα μπορεί να απαγορευτεί με σχετικές δικαστικές

αποφάσεις που θα επιβάλλει η εκάστοτε εθνική νομοθεσία στο όνομα της απειλής της ασφάλειας. Συγκεκριμένα, η τροπολογία αναφέρει επίσης «…η πρόσβαση στο Διαδίκτυο δεν μπορεί να περιοριστεί χωρίς να προηγηθεί δικαστική απόφαση. Εξαιρούνται οι περιπτώσεις όπου απειλείται η ασφάλεια των πολιτών.». Είναι σημαντικό, επίσης, να κατανοηθεί πως οι χρήστες του Διαδικτύου δεν είναι πελάτες αλλά πολίτες και ως τέτοιοι θα πρέπει να λογίζονται σε θέματα που αφορούν αφενός την υποδομή του διαδικτύου και αφετέρου το δικαίωμα πρόσβασης σε αυτό.

7.ΔΙΑΔΙΚΤΥΑΚΟΙ ΚΙΝΔΥΝΟΙ

Η πρόσβαση στο Διαδίκτυο σήμερα δεν είναι ακίνδυνη, ανεξάρτητα από τον τρόπο χρήσης των υπηρεσιών του. Υπάρχουν κακόβουλοι χρήστες και αρκετές δυνατότητες πρόκλησης ζημιών, τόσο στο επίπεδο του χρησιμοποιούμενου λογισμικού και υλικού, όσο και σε προσωπικό επίπεδο.

> Πρόκληση ζημιών στο υπολογιστικό σύστημα

Ο κύριος κίνδυνος πρόκλησης ζημιών στο υπολογιστικό σύστημα ενός ανυποψίαστου χρήστη είναι η μόλυνση του συστήματος με κάποιον ιό. Η μόλυνση γίνεται όταν ο χρήστης καλείται να λάβει κάποιο -φαινομενικά αθώο- αρχείο όπως ένα κείμενο ή μια φωτογραφία και όταν δοκιμάσει να το χρησιμοποιήσει, ο ιός αναλαμβάνει δράση επιμολύνοντας το σύστημα. Μπορεί να καταστρέψει αρχεία ή και ολόκληρο το σκληρό δίσκο του συστήματος. Άλλες φορές είναι δυνατή η αποστολή ιού απευθείας από τον ιστοτόπο που επισκέπτεται ο χρήστης, χωρίς να εμφανισθεί κάποια ένδειξη λήψης αρχείου.

>Πρόκληση ζημιών σε προσωπικά δεδομένα

Στην κατηγορία αυτή υπάγονται τόσο οι δούρειοι ίπποι που προαναφέρθηκαν, όσο και κακόβουλα μηνύματα ηλεκτρονικού ταχυδρομείου. Με τον τρόπο αυτό όχι μόνον είναι δυνατό να υφαρπαγούν προσωπικά δεδομένα κάποιου χρήστη, όπως ο αριθμός ταυτότητάς του ή το ΑΦΜ του, όσο και, πιο σημαντικό, αριθμοί πιστωτικών καρτών, λογαριασμών τραπέζης κτλ. Η μέθοδος υφαρπαγής προσωπικών δεδομένων μέσω ηλεκτρονικού ταχυδρομείου αποκαλείται "Phishing". Οι χρήστες είναι καλό να γνωρίζουν ότι κανείς χρηματοπιστωτικός φορέας δεν χρησιμοποιεί το Διαδίκτυο για να ανανεώσει προσωπικές πληροφορίες, ενώ ένας προστατευμένος ιστοτόπος αρχίζει πάντα με το πρόθεμα http**s.**

>Παραπλάνηση

Αρκετές φορές οι χρήστες του Διαδικτύου χρησιμοποιούν τις υπηρεσίες του για να βρουν κάποιες πληροφορίες που χρειάζονται. Μερικοί ιστότοποι εμφανίζουν πληροφορίες, οι οποίες φαινομενικά είναι ακριβείς ή αναφέρουν απόλυτα αξιόπιστους δημιουργούς ή πηγές. Το κίνητρο για τέτοιες πράξεις μπορεί να είναι είτε η αποκομιδή ιδίου οφέλους είτε, απλά, η χαρά της παραπλάνησης των (αγνώστων) χρηστών. Ο όρος που περιγράφει αυτού του τύπου την παραπλάνηση είναι **"Hoax"**.

>Προστασία

Υπάρχουν τρεις τρόποι προστασίας, οι οποίοι θα πρέπει να χρησιμοποιούνται σε συνδυασμό:

- Χρήση τείχους προστασίας (firewall)
- Χρήση λογισμικού προστασίας ενάντια σε ιούς και προγράμματα κατασκοπείας

- Συνεχής ενημέρωση των χρηστών.

Οι πλέον συνηθισμένοι τρόποι εξαπάτησης των χρηστών είναι το **Phishing** και το **Pharming**.

Phishing

Το phishing είναι η πράξη με την οποία κάποιος προσπαθεί να αποκτήσει πληροφορίες, όπως ονόματα χρηστών, κωδικούς πρόσβασης καθώς και στοιχεία πιστωτικών καρτών, αφού έχει μεταμφιεστεί σε μια αξιόπιστη οντότητα μιας ηλεκτρονικής επικοινωνίας. Το phishing συνήθως εκτελείται από πλαστογραφημένο e-mail ή instant messaging και συχνά κατευθύνει τους χρήστες να εισάγουν τα στοιχεία σε μια πλαστή ιστοσελίδα, η εμφάνιση και αίσθηση της οποίας είναι σχεδόν πανομοιότυπη με τη νόμιμη. Το phishing είναι ένα από τα παραδείγματα της τεχνικής κοινωνικής μηχανικής που χρησιμοποιούνται για να εξαπατήσουν τους χρήστες και εκμεταλλεύεται την κακή χρηστικότητα των σημερινών τεχνολογιών ασφαλείας web. Οι προσπάθειες για την αντιμετώπιση του αυξανόμενου αριθμού των αναφερόμενων περιστατικών phishing περιλαμβάνουν τη νομοθεσία, την εκπαίδευση των χρηστών, την ευαισθητοποίηση του κοινού και τεχνικά μέτρα ασφαλείας. Μια τεχνική phishing περιγράφεται με λεπτομέρεια το 1987 και η πρώτη καταγεγραμμένη χρήση του όρου «phishing» έγινε το 1995. Ο όρος είναι μια παραλλαγή της αλιείας, πιθανώς επηρεασμένος από phreaking και παραπέμπει στο «δόλωμα». Χρησιμοποιείται με την ελπίδα ότι το ενδεχόμενο θύμα θα "δαγκώνει" κάνοντας κλικ σε ένα κακόβουλο link ή το άνοιγμα ενός κακόβουλου αρχείου, προγραμματισμένου να αντιγράψει οικονομικά στοιχεία ή και κωδικούς πρόσβασης. Επειδή η μέθοδος “phishing” βασίζεται στην πλάνη του θύματος με σκοπό την περιουσιακή του ζημία, είναι προφανές ότι οι Phishers μέσω αυτής προσπορίζουν στον εαυτό τους ή/και σε τρίτους παράνομο περιουσιακό όφελος. Επειδή οι δράστες έχουν γνώση και θέληση σχετικά με την παράνομη δραστηριότητά τους, συμπεραίνεται ότι το “phishing” συνιστά απάτη, κατά το άρθρο 386 του Ποινικού Κώδικα, σύμφωνα με το οποίο «όποιος 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 παράσταση ψευδών γεγονότων σαν αληθινών ή την αθέμιτη απόκρυψη ή παρασιώπηση αληθινών γεγονότων τιμωρείται με φυλάκιση τουλάχιστον τριών μηνών και αν η ζημία που προξενήθηκε είναι ιδιαίτερα μεγάλη, με φυλάκιση τουλάχιστον δύο ετών».

Pharming

Η τεχνική του “pharming” αποτελεί μέθοδο εξαπάτησης μέσω του διαδικτύου παρόμοια με το “phishing” αλλά σαφώς πιο επικίνδυνη από αυτό. Ένα ειδικό πρόγραμμα εκμεταλλεύεται κενά ασφαλείας του συστήματος, διεισδύει στον υπολογιστή του θύματος και το επηρεάζει κατά τέτοιο τρόπο, ώστε, ακόμα κι αν ο χρήστης πληκτρολογεί τη σωστή διεύθυνση του διαδικτυακού τόπου που θέλει να επισκεφτεί, θεωρώντας πως βρίσκεται σε ασφαλή χώρο, ο συγκεκριμένος υπολογιστής τον “οδηγεί” μόνο σε πλαστές ιστοσελίδες. Ειδικότερα, αν πρόκειται για ιστοσελίδα τράπεζας, η προσπάθεια του

θύματος να πραγματοποιήσει τις συναλλαγές του μέσω on-line banking καταλήγει στη μεταφορά των χρημάτων του στους δράστες (pharmers). Είναι σαφές ότι η αύξηση των ωρών χρήσης του διαδικτύου πολλαπλασιάζει τον κίνδυνο εγκατάστασης προγραμμάτων που καθιστούν δυνατό το “pharming”, το οποίο βαθμιαία εξελίσσεται σε μία από τις σοβαρότερες μορφές εγκληματικότητας στο διαδίκτυο. Η μέθοδος “pharming” αποτελεί ένα είδος διείσδυσης μέσω του διαδικτύου, χωρίς τη συναίνεση του νόμιμου κατόχου των στοιχείων. Συνεπώς, η μέθοδος αυτή, εφόσον είναι ολοφάνερο ότι τελείται με δόλο, συνιστά παραβίαση απορρήτου σύμφωνα με ένα άρθρο του Ποινικού Κώδικα, στο οποίο αναφέρετε πώς «όποιος αποκτά πρόσβαση σε στοιχεία που έχουν εισαχθεί σε υπολογιστή ή σε περιφερειακή μνήμη υπολογιστή ή μεταδίδονται με συστήματα τηλεπικοινωνιών, εφόσον οι πράξεις αυτές έγιναν χωρίς δικαίωμα, ιδίως με παραβίαση απαγορεύσεων ή μέτρων ασφαλείας που είχε λάβει ο νόμιμος κάτοχός τους, τιμωρείται με φυλάκιση μέχρι τρεις μήνες ή με χρηματική ποινή τουλάχιστον 29,00 € (…)». Συμπερασματικά, οι ανωτέρω δύο μέθοδοι μπορούν να τιμωρηθούν, σύμφωνα με τις ισχύουσες διατάξεις του Ποινικού Κώδικα. Για την αντιμετώπιση τέτοιων φαινομένων κρίνεται απαραίτητη η λήψη τεχνικών μέτρων ασφαλείας, καθώς και η ευαισθητοποίηση των χρηστών του Ίντερνετ, ώστε να μην γίνονται εύκολα θύματα των phishers και των pharmers.