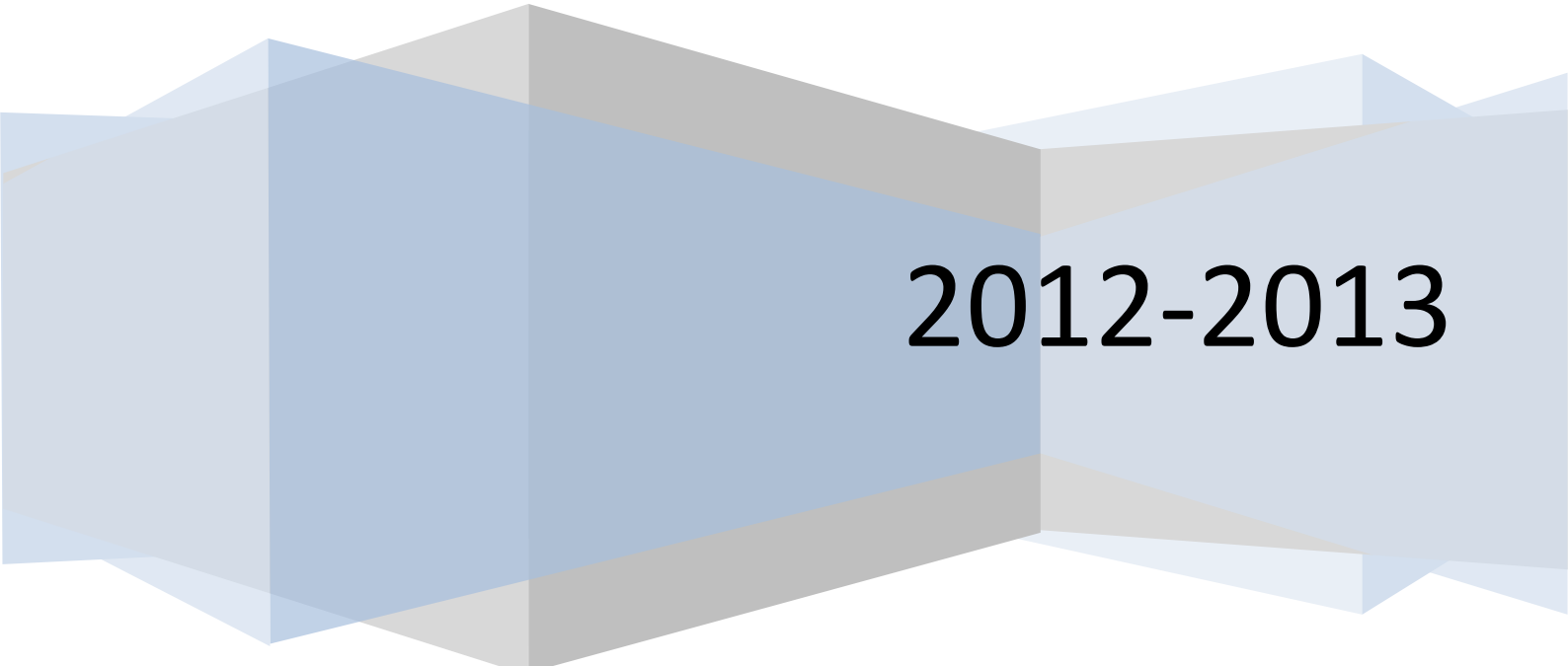


ΓΕΛ Μοιρών

Κοινωνικά αποτελέσματα δράσης ιών

Βασιλάκης Γιώργος, Μαρινάκης Ανδρέας,
Πολιουδάκης Μανόλης



2012-2013

Περιεχόμενα

Εισαγωγή.....	3
Χάκερ	4
Τι είναι ο cracker.....	4
Διαφορά hacker - cracker	5
Η Νέα Φιλοσοφία των Ιών Υπολογιστών	5
Οικονομικές συνέπειες ιών των υπολογιστών	6
<i>Worm conficker</i>	6
<i>Ο αρχιμαφιόζος «Conficker»</i>	7
<i>Ζημιές από κακόβουλο λογισμικό υπερβαίνουν τα \$ 13 δισεκατομμυρίων</i>	8
<i>Παγκόσμιο οικονομικό αντίκτυπο των Malware</i>	8
<i>Οι ιοί υπολογιστών και πώς επηρεάζουν την οικονομία μας</i>	8
ΗΘΙΚΕΣ ΕΠΙΠΤΩΣΕΙΣ ΤΩΝ ΙΩΝ ΤΩΝ ΥΠΟΛΟΓΙΣΤΩΝ	9
<i>Η σημασία της ηθικής Υπολογιστών</i>	9
<i>Αποτρέπει την κατάχρηση των προσωπικών πληροφοριών</i>	9
<i>Αποτρέπει την κλοπή της πνευματικής ιδιοκτησίας</i>	9
<i>Αποτρέπει την απώλεια του</i> Διάφορες Θέσεις εργασίας στον τομέα της ανάπτυξης λογισμικού	10
<i>Σας κρατά από το να είναι ανήθικη!</i>	10
<i>Κάνει τον υπολογιστή σας ένα καλύτερο και ασφαλές μέρος</i>	10
ΟΙ ΠΟΛΙΤΙΚΕΣ - ΚΟΙΝΩΝΙΚΕΣ ΕΠΙΠΤΩΣΕΙΣ ΤΩΝ ΙΩΝ ΤΩΝ Η/Υ	11
ΟΙ ΠΟΛΙΤΙΚΕΣ ΕΠΙΠΤΩΣΕΙΣ ΤΩΝ ΙΩΝ	12
ΟΙ ΕΠΙΠΤΩΣΕΙΣ ΤΩΝ ΙΩΝ ΜΠΟΡΟΥΝ ΝΑ ΔΙΑΧΥΘΟΥΝ ΣΕ ΚΑΘΕ ΠΟΛΙΤΙΚΟΚΟΙΝΩΝΙΚΗ ΠΤΥΧΗ ΤΗΣ ΖΩΗΣ, ΟΠΩΣ:.....	13
Πηγές :.....	13

Εισαγωγή

Το Internet είναι για τους περισσότερους από εμάς είναι το δεύτερό μας σπίτι. Για ορισμένους όμως είναι μια αστείρευτη πηγή παράνομου πλουτισμού- αφού ως γνωστόν οι πληροφορίες είναι χρήμα. Στην εργασία αυτή προσπαθούμε να αναλύσουμε μερικές από τις σημαντικές κοινωνικές , οικονομικές, και τις ηθικές επιπτώσεις των ηλεκτρονικών επικοινωνιών που γίνονται με την διαμεσολάβηση των υπολογιστών. Υπάρχουν περίπου 14.000-15.000 γνωστοί τύποι ιών υπολογιστών.

Τι είναι ο Χάκερ

Αρχικά ο όρος "χάκερ" σήμαινε στα αγγλικά το δημιουργό ενός επίπλου ή γενικότερα ξύλινου αντικειμένου με τη βοήθεια πελέκως (τσεκουριού).

Χάκερ ονομάζεται κάποιος που αντλεί ευχαρίστηση από τη βαθιά κατανόηση της εσωτερικής λειτουργίας ενός συστήματος, ειδικότερα ενός υπολογιστή ή δικτύου υπολογιστών, στον οποίο, όμως, δεν έχει δικαίωμα πρόσβασης. Ο όρος (ειδικά στην ελληνική γλώσσα) συγγέεται πολύ συχνά με τον όρο κράκερ (cracker), κάτι που αποτελεί σφάλμα.

Σε αντίθεση με τον χάκερ, ο κράκερ είναι άτομο (ή ομάδα ατόμων) που αποπειράται να αποκτήσει πρόσβαση σε υπολογιστικό σύστημα για την οποία όχι μόνο δε διαθέτει εξουσιοδότηση, αλλά με στόχο να το βλάψει με οποιοδήποτε τρόπο. Οι κράκερ είναι εξ ορισμού κακόβουλοι, αντίθετα προς τους χάκερ, ενώ διαθέτουν και πολλά εργαλεία για τις κακόβουλες ενέργειές τους.

Η διεθνής κοινότητα των χάκερ πιστεύει ότι η πρόσβαση στην πληροφορία αποτελεί παγκόσμιο κοινό αγαθό και ότι είναι ηθικό καθήκον τους να μοιράζονται τις ικανότητές τους τόσο δημιουργώντας λογισμικό ανοικτού κώδικα, όσο και διευκολύνοντας την πρόσβαση σε πληροφορίες και υπολογιστικούς πόρους, όπου αυτό είναι εφικτό.

Έχουν, επίσης, την αμφιλεγόμενη πεποίθηση ότι το "σπάσιμο" και η "εξερεύνηση" ενός υπολογιστικού συστήματος, τόσο σε επίπεδο υλικού όσο και (κυρίως) λογισμικού είναι ηθικά αποδεκτά, εφόσον ο χάκερ δεν διαπράττει κλοπή, βανδαλισμό ή παραβίαση εμπιστευτικότητας. Για τους χάκερς, όποιος "αξίζει αυτόν τον τίτλο, είναι στην πραγματικότητα ένας έξυπνος προγραμματιστής ή άτομο με ιδιαίτερες ικανότητες στην κατανόηση και το χειρισμό υπολογιστικών συστημάτων". Σε καμία, όμως, περίπτωση, δεν αποδέχονται ότι οι πράξεις ενός χάκερ έχουν κακόβουλους στόχους και αυτή η διαφορά είναι που τους διακρίνει από τους κράκερς.

Τι είναι ο cracker

Cracker είναι αυτός που είναι μεν hacker, είναι δηλαδή κι αυτός "expert" στους υπολογιστές, αλλά χρησιμοποιεί αυτή τη γνώση για να κάνει κάτι παράνομο.

Οι crackers χρησιμοποιούν όλη αυτή την γνώση για να "σπάσουν" προγράμματα, να δημιουργήσουν ζημιά σε μια ιστοσελίδα, να κλέψουν δεδομένα, να φτιάξουν ιούς με κακό σκοπό, κλπ.



Διαφορά *hacker* - *cracker*

Ο *cracker* κάνει ό,τι και ο *hacker*, αλλά δημιουργεί ζημιές και παραβιάζει τους νόμους. Για παράδειγμα, αν κάποιος καταφέρει και βρει - "σπάσει" τους κωδικούς από μία ιστοσελίδα, αποκτώντας πρόσβαση στα πάντα, και μείνει εκεί χωρίς να συνεχίσει, τότε ονομάζεται *hacker*.

Αν όμως προχωρήσει και κάνει μεταβολές στο περιεχόμενο εν αγνοία του ιδιοκτήτη της ιστοσελίδας, ή και δημιουργήσει ζημιά, τότε αυτός είναι *cracker*!

Τέλος, αξίζει να σημειώσουμε το αυτονόητο: όλοι οι *crackers* είναι και *hackers*, αλλά το αντίθετο δεν ισχύει.

Άρα όλοι αυτοί που αναφέρονται στις ειδήσεις ως "hackers που δημιουργήσαν πρόβλημα ή ζημιά", δεν είναι τίποτα άλλο, παρά *crackers*...

Οπότε κλείνοντας, η διαφορά *hacker-cracker* έγκειται στο πως χρησιμοποιεί ο καθένας τη γνώση του: με σκοπό μόνο να μάθει, ή με σκοπό να δημιουργήσει ζημιά.

Η Νέα Φιλοσοφία των Ίών Υπολογιστών

Οι ιοί των υπολογιστών έχουν αλλάξει χρήση τελευταία και από ένα παιχνίδι νεαρών κομπιουτεράδων έχουν αρχίσει να προσφέρουν τις υπηρεσίες τους στο οργανωμένο έγκλημα, κλέβοντας αριθμούς πιστωτικών καρτών, κωδικούς λογαριασμών (passwords), απόρρητα αρχεία και άλλα ψηφιακά μυστικά που αποκαλύπτουν οι χρήστες όταν κάνουν αγορές και παραγγελίες στο Διαδίκτυο. Οι νέοι ιοί έχουν ως αντικείμενο την υποκλοπή και αξιοποίηση στοιχείων και πληροφοριών για εγκληματικούς ή στρατιωτικούς σκοπούς και ήδη έχουν κάνει την εμφάνισή τους κάποιοι ιοί που θεωρούνται οι πρόδρομοι της νέας γενιάς των ιών «κατασκόπων».

Οι ιοί του μέλλοντος είναι πολύ πιθανό να χρησιμοποιηθούν στην κατασκοπεία και στον στρατό είτε για την καταστροφή αρχείων είτε για την συλλογή πληροφοριών. Οι ημέρες που τους ιούς τούς δημιουργούσαν έφηβοι που ήθελαν να διασκεδάσουν έχουν παρέλθει και είναι πολλοί αυτοί που θα τις αναπολήσουν. Αναλυτές θεμάτων που ασχολούνται με την ασφάλεια των συστημάτων υπολογιστών περιγράφουν τους ιούς της νέας γενιάς με τους όρους *Blended Threats*, δηλ. συνδυασμένες απειλές, και *Flash Threats*, δηλ. ακαριαίες απειλές, και εκτιμούν ότι θα τους συναντάμε όλο και συχνότερα στο άμεσο μέλλον.

Υπάρχει, όμως, και η εκτίμηση ειδικών αναλυτών που ισχυρίζονται ότι εφόσον η επόμενη γενιά των ιών θα είναι στην ουσία συλλέκτες απόρρητων δεδομένων, θα μπορούν κάλλιστα να χρησιμοποιηθούν στην κατασκοπεία, είτε για την διείσδυση και την καταστροφή αρχείων είτε απλά για την συλλογή πληροφοριών. Ήδη η χρήση και η αξιοποίηση των ιών του μέλλοντος εξετάζεται σοβαρά από σχολές πολέμου και μυστικές υπηρεσίες, ενώ μια πρώτη επιτυχής εφαρμογή τους φέρεται να έλαβε χώρα σε πρόσφατες πολεμικές συγκρούσεις.

Οικονομικές συνέπειες ιών των υπολογιστών

Worm conficker

Ένα πρόσφατο blog post, ισχυρίζεται ότι βασίζεται σε προηγούμενες μελέτες του στο μέσο κόστος αυτών των επιθέσεων malware, η οικονομική απώλεια που οφείλεται στον ιό τύπου worm Conficker θα μπορούσε να είναι τόσο υψηλή όσο 9,1 δισεκατομμύρια \$ δολάρια.

Παρά το γεγονός ότι η ανάλυση τους, επίσης, θεωρείται ένα πολύ περιορισμένο ποσοστό μόλυνσης (200.000 μολυσμένους ξενιστές), ισχυρίζονται ότι το κόστος του ιού στην περίπτωση αυτή εξακολουθεί να είναι περίπου 200 εκατομμύρια δολάρια. Η έρευνα αποκλείει ένα σημαντικό γεγονός όμως - δεν είναι μόνο Conficker, αλλά επίσης, σύμφωνα με την πιο πρόσφατη ισοτιμία, ο αριθμός των μολυσμένων ξενιστών είναι 3,5 εκατ. ευρώ.

Εδώ θα βρείτε περισσότερες λεπτομέρειες από την ανάλυση:

Επεκτείνοντας έξω από μελέτες για το μέσο κόστος παρόμοιων προηγούμενων επιθέσεων, το συνολικό οικονομικό κόστος αυτού του worm (συμπεριλαμβανομένου του κόστους των προσπαθειών για την καταπολέμηση του σκουληκιού, το κόστος για την αγορά αντι-μέτρο λογισμικού) θα μπορούσε να είναι τόσο υψηλό όσο 9,1 δισεκατομμύρια \$. Ακόμη και με χρήση του ενιαίου, των απομακρυσμένων πηγών δεδομένων που δείχνουν ένα πολύ πιο περιορισμένο πεδίο εφαρμογής της μόλυνσης (<200.000 κατά πολύ λιγότερο από όλες τις άλλες πηγές δείχνουν-το κόστος αυτού του ιού εξακολουθεί να είναι περίπου \$ 200 εκατομμύρια δολάρια.) "

Ο αριθμός των μολυσμένων ξενιστών Conficker είναι στην πραγματικότητα πολύ μεγαλύτερος από τον αριθμό που παρέχεται από την Ομάδα Εργασίας Conficker, υπό την έννοια ότι πίσω από ένα μοναδικό IP μπορεί να υπάρχουν πολλοί άλλοι ξενιστές NAT-ed στο τοπικό δίκτυο, προσθέτοντας μία ακόμη μεταβλητή που έχει τη δυνατότητα να υπονομεύσει αυτές τις εκτιμήσεις.

Επιπλέον, η ανάλυση αναφέρει ότι η εκτίμηση αυτή περιλαμβάνει το κόστος για την αγορά αντι-μέτρο του λογισμικού, ένα κόστος το οποίο πρέπει να αποκλειστεί λόγω του γεγονότος ότι η εργασία αντίμετρα είναι σχεδόν δωρεάν λόγω της επίδρασης του σκουληκιού. Ως εκ τούτου δεν προστίθεται επιπλέον κόστος για την αγορά αντίμετρου λογισμικού αφού με βάση τις ισχύουσες συμφωνίες με τους προμηθευτές της ασφάλειας, οι επιχειρήσεις έπρεπε να προστατεύονται αυτόματα από το σκουλήκι.

Στο παρελθόν, υπήρξαν πολλές προσπάθειες για να εκτιμηθεί το κόστος του κακόβουλου λογισμικού, από το mi2g 157 δισεκατομμυρίων δολαρίων και 192 δισεκατομμύρια δολάρια σε όλο τον κόσμο το 2004, λόγω λοιμώξεων κακόβουλου λογισμικού, που ακολουθείται από Economics computers, μελέτη αναφέρει ότι το 2006, οι άμεσες ζημιές μειώθηκαν στα 13,3 δισ. δολ., από 14,2 δισεκατομμύρια δολάρια το 2005, και \$ 17,5 δισεκατομμύρια το 2004.

Σε έναν τέλειο κόσμο όλων των ενδιαφερομένων μερών θα πρέπει να μοιράζονται πληροφορίες για το πραγματικό ποσοστό λοίμωξης και τα έξοδα που οφείλονται στη μόλυνση του σκουληκιού, επιβεβαιώνοντας έτσι ότι οι επιχειρήσεις τους έχουν παραβιαστεί και, ενδεχομένως, έχουν καταστρέφει. Στον πραγματικό κόσμο, μια μολυσμένη διεθνής εταιρεία θα προσπαθήσει να παραμείνει κάτω από το ραντάρ, αν μπορεί, όπως ακριβώς και ο μέσος χρήστης του Διαδικτύου.

Επιπλέον, με βάση την geolocated, ίσως ακόμη και εταιρείες με παράνομα αντίγραφα των Windows αντιπροσωπεύουν το μεγαλύτερο ποσοστό των μολυσμένων στο σύνολο, αξίζει να σημειωθεί ότι η άρνηση πρόσβασης σε κρίσιμα επιθέματα που χρησιμοποιούνται ως βάση για τα εν λόγω σκουλήκια αναφέροντας πειρατικά αντίγραφα, καταλήγει σε μια κατάσταση όπου οι νόμιμοι ιδιοκτήτες του λειτουργικού συστήματος θα αισθάνονται το spam / phishing / DDoS / crimeware επίδραση που προέρχεται από τους μολυσμένους ιδιοκτήτες των παράνομων αντιγράφων σε μακροπρόθεσμη βάση.

Υπάρχουν πάρα πολλές μεταβλητές να λυφθούν υπόψη, ειδικά σε παγκόσμιο αντίκτυπο του σκουληκιού, η διαφορετική κατανομή για την προστασία των περιουσιακών στοιχείων σε όλο τον κόσμο με βάση το τοπικό οικονομικό κλίμα, καθώς και η βελτίωση της αποτελεσματικότητας έχει επιτευχθεί στον καθαρισμό κακόβουλου λογισμικού μέσα σε μια συγκεκριμένη εταιρεία.

Ο αρχιμαφιόζος «Conficker»

Ο επονομαζόμενος «Conficker», όχι μόνο μεταλλάχθηκε για μία ακόμη φορά, παίρνοντας εντολές από τους άγνωστους δημιουργούς του, αλλά και άρχισε να εμφυτεύεται με ασύλληπτα γοργό ρυθμό σε χιλιάδες υπολογιστές κάθε μέρα.

Ο τρόπος με τον οποίο μεταδίδεται αυτή η τελευταία μετάλλαξη του Conficker (Win32/Conficker.D) είναι μέσω μίας κερκόπορτας που έχει ανακαλύψει σε δικτυακή υπηρεσία των Microsoft Windows, της κωδικοποιημένης ως «MS08-067 Microsoft Server Service vulnerability».

Στις 29 Απριλίου 2009 ο εφιάλτης πήρε συγκεκριμένη μορφή, καθώς οι εταιρείες δικτυακής ασφάλειας βεβαιώθηκαν ότι ο Conficker φυτεύει στα θύματά του έναν δευτερογενή ιό - τον Waledac- που τους μετατρέπει σε ταχυδρομικές θυρίδες αμέτρησης μηνυμάτων παρενόχλησης (spam mails).

Ετσι, οι δημιουργοί του ασύλληπτου αραχνοειδούς αποκτούν ένα παγκόσμιας κλίμακας «botnet», το οποίο μπορούν είτε να εκμισθώσουν στη μαύρη αγορά διακίνησης φαρμάκων είτε να χρησιμοποιήσουν εκβιαστικά ως απειλή μπλοκαρίσματος. Επίσης βγάζουν ήδη τον επιούσιο μέσω της προβολής ενός ψευτομηνύματος για... προστασία από τον ίδιο τον Conficker, λέγοντας στα θύματά τους: «Είμαι το λογισμικό προστασίας Spyware Protect 2009.

Πληρώστε με για να σας σώσω»- πράγμα που φυσικά δεν κάνει.

Τι κόστος μπορεί να επιφέρει αυτή η δράση του Conficker; Σύμφωνα με σχετική μελέτη του Cyber Security Institute το καθάρισμα 200.000 προσβεβλημένων PC μπορεί να κοστίσει ως και 9,1 δισ. δολάρια. Ωστόσο ήδη εκτιμάται ότι οι υπολογιστές που έχει μολύνει ο Conficker παγκοσμίως φθάνουν τα 3,5 εκατομμύρια!..

Ζημιές από κακόβουλο λογισμικό υπερβαίνουν τα \$ 13 δισεκατομμυρίων

Διεξήχθη πρόσφατα μια έρευνα από τους επαγγελματίες της ασφάλειας και των διαχειριστών σχετικά με τη συχνότητα και το οικονομικό αντίκτυπο των επιθέσεων malware στους οργανισμούς τους κατά τους προηγούμενους 12 μήνες. Η ανάλυση των αποτελεσμάτων της έρευνας έχει ολοκληρωθεί και είναι διαθέσιμη, η έκθεση του 2007 Malware: το οικονομικό αντίκτυπο των ιών, spyware, adware, botnets, και άλλου κακόβουλου κώδικα. Η πλήρης έκθεση παρέχει εκτιμήσεις του κακόβουλου λογισμικού σε όλο τον κόσμο ζημιών, σε οργανωτικό επίπεδο, όσο και σε επίπεδο μεμονωμένων εκδηλώσεων malware.

Παγκόσμιο οικονομικό αντίκτυπο των Malware

Η μελέτη διαπίστωσε ότι για δεύτερη συνεχή χρονιά, το κόστος αποζημίωσης κακόβουλου λογισμικού μειώθηκε σε παγκόσμιο επίπεδο. Το 2006, οι άμεσες ζημιές μειώθηκαν στα 13,3 δισ. δολ., από 14,2 δισ. δολ. το 2005, και 17,5 δισεκατομμύρια δολάρια το 2004.

Οι ιοί υπολογιστών και πώς επηρεάζουν την οικονομία μας

Η IT ασφάλεια βελτιώθηκε ως αποτέλεσμα των αυξημένων επιθέσεων των ιών. Cyber επιθέσεις, υπογράμμισαν τη δημοσιονομική επίπτωση της κακόβουλης δραστηριότητας και στις δύο επιχειρήσεις και, τελικά, στον καταναλωτή. Η επίδραση στην οικονομία περιλαμβάνει τις δαπάνες που έχουν οι εταιρείες, όταν πρέπει να αποκαταστήσουν τις ζημιές των ιών.

Κατά τη στιγμή της δημοσίευσης το 2011, ο αριθμός των επιθέσεων malware αριθμούσε περισσότερα από 200 εκατ. ευρώ. Μια έκθεση του 2010 από τη McAfee, μια εταιρεία λογισμικού ασφαλείας, αποκάλυψε ότι το κόστος για επιχειρήσεις του χρόνου εργασίας που χάνονται λόγω επιθέσεων ιών ήταν 6,3 εκατομμύρια δολάρια ανά ημέρα, και μια έκθεση Fox News, το 2009 εκτιμάται ότι 86 δισεκατομμύρια δολάρια χάνονται κάθε χρόνο σε όλο τον κόσμο. Νωρίτερα εκθέσεις, όπως την έκθεση του 2007 από Malware Υπολογιστών Οικονομικών σχετικά με την ετήσια παγκόσμια οικονομική ζημία που προκλήθηκε από κακόβουλες επιθέσεις κώδικα στις οργανώσεις έδειξαν ότι οι δαπάνες ήταν 13,3 δισεκατομμύρια δολάρια. Μια έκθεση από το 2000 (Information Week) ανέφερε ότι το συνολικό κόστος ήταν \$ 1,6 τρισεκατομμύρια.

ΗΘΙΚΕΣ ΕΠΙΠΤΩΣΕΙΣ ΤΩΝ ΙΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

Η σημασία της ηθικής Υπολογιστών

Με τη χρήση των ηλεκτρονικών υπολογιστών για την επικοινωνία προτιμώνται περισσότερο από ό, τι χαρτί και μολύβι, μετά από την ηθική του υπολογιστή έχουν γίνει ένα *must* για το καθένα και όλους! Το άρθρο αυτό τονίζει τα σημεία που ρίχνουν κάποιο φως σχετικά με τη σημασία της ηθικής του υπολογιστή και πώς θα συμβάλει σε μια καλύτερη και ασφαλή χρήση των υπολογιστών στην καθημερινή ζωή μας.

Με την εισαγωγή των υπολογιστών παγκοσμίως στη δεκαετία του 1990, η συνολική προσέγγιση της εργασίας, την επικοινωνία και την αποθήκευση σημαντικών πληροφοριών έχει αλλάξει. Θέλω να πω ποιος θα το φανταζόταν ότι μια μηχανή μπορεί να κάνει ένα μεταφέρω ένα μήνυμα σε κάθε γωνιά του κόσμου με μόνο ένα πάτημα ενός κουμπιού, όταν χρειάστηκε μέρες για να λάβει επιστολές και τηλεγραφήματα!

Ποιος θα το φανταζόταν ότι οι υπολογιστές θα μας δώσει την πρόσβαση σε όλες τις πληροφορίες σε όλο τον κόσμο μέσω της χρήσης του διαδικτύου. Θέλω να πω, που πηγαίνει στις βιβλιοθήκες αυτές τις μέρες για να διαβάσει βιβλία σχετικά με την ιστορία και αρχαίους πολιτισμούς, όταν μπορείτε να καθίσετε στο σπίτι και να σερφάρετε την κάθε πληροφορία.

Με τους υπολογιστές μας δίνει τόσο πολύ από την ευκολία και την ελευθερία, υπάρχουν υψηλές πιθανότητες ότι η ελευθερία αυτή μπορεί να χρησιμοποιηθεί σε ένα «ανήθικο τρόπο». Αυτό είναι όπου ο ρόλος της ηθικής υπολογιστών έρχονται σε εικόνα.

Αποτρέπει την κατάχρηση των προσωπικών πληροφοριών

Οι υπολογιστές έχουν φέρει τον κόσμο πιο κοντά, είτε πρόκειται για προσωπικά ή επαγγελματικά! Οι περισσότεροι από εμάς θεωρούν ότι είναι πιο βολικό για να ψωνίσετε σε απευθείας σύνδεση, αντί να βγείτε έξω.

Γι' αυτό καλούμαστε να δίνουμε προσωπικές πληροφορίες όπως το όνομα μας, την ημερομηνία γέννησης και το πιο σημαντικό, «πληροφορίες πιστωτικών καρτών» μας!

Ρωτήστε τον εαυτό σας, αν ξέρετε ότι οι άνθρωποι δεν ακολουθούν παντού την ηθική του υπολογιστή, θα αισθάνονται ασφαλείς να δίνουν όλες αυτές τις πληροφορίες;

Αντίθετα, αν έχετε διαβάσει τις πολιτικές απορρήτου τους και ξέρετε ότι συμμορφώνονται με τους νόμους και την ηθική στον κυβερνοχώρο υπολογιστή, ξέρετε για ένα γεγονός ότι τα προσωπικά σας στοιχεία δεν θα γίνει κατάχρηση.

Αποτρέπει την κλοπή της πνευματικής ιδιοκτησίας

Τι είναι η πνευματική ιδιοκτησία; Λοιπόν, σε αντίθεση με φυσικές μορφές του ιδιότητες όπως το αυτοκίνητο ή το σπίτι, η πνευματική ιδιοκτησία αναφέρεται στην

ιδιοκτησία που δημιουργείται από το μυαλό! Το Διαδίκτυο αποτελείται από πνευματική ιδιοκτησία που περιλαμβάνει έργα από διάφορους ερευνητές, συγγραφείς, καλλιτέχνες τραγούδι και ούτω καθεξής. Χωρίς την παρουσία της ηθικής υπολογιστή, το έργο που δημιουργήθηκε από την διάνοια ενός ατόμου μπορούν εύκολα να αντιγραφούν και να δημοσιοποιηθούν από κάποιον άλλο. Φανταστείτε πώς θα νιώθατε αν ποιήσή σας έχει αντιγραφεί και έχει δημοσιοποιηθεί κάτω από το όνομα κάποιου άλλου; Τώρα ξέρετε τι ακόλουθα ηθική υπολογιστή και πολιτικές προστασίας προσωπικών δεδομένων είναι σημαντική;

Αποτρέπει την απώλεια του Διάφορες Θέσεις εργασίας στον τομέα της ανάπτυξης λογισμικού

Υπάρχουν χιλιάδες άνθρωποι παγκοσμίως που εργάζονται σε εταιρείες που αναπτύσσουν προγράμματα ηλεκτρονικών υπολογιστών και του λογισμικού. Ωστόσο, αν βρούμε έναν τρόπο για να πάρουμε αυτά το λογισμικό χωρίς να χρειάζεται να πληρώσει το τίμημα, οι περισσότεροι από εμάς θα προτιμούσαν πειρατείας πέρα από την πληρωμή, έτσι δεν είναι;

Έχετε ποτέ αναρωτηθεί, πώς αυτό μπορεί να κοστίζει τους υπαλλήλους που εργάζονται σε αυτές τις εταιρείες δουλειά τους. Η γενική νοοτροπία των περισσότερων από τους ανθρώπους που παίρνουν παράνομα το λογισμικό είναι ότι αυτές οι εταιρείες είναι πολύ πλούσιες και πραγματικά δεν θα τους επηρεάσει ...,ακόμα και αν το κάνει, ποιος νοιάζεται;

Ωστόσο, το σημείο που πρέπει να έχουμε κατά νου είναι, τι θα γινόταν αν αυτός που έπρεπε να πληρώσει το τίμημα είναι κάποιος κοντά σε σας. Φανταστείτε, υπάρχουν χιλιάδες άνθρωποι να εμπλακούν σε ανήθικες downloads και διανομής. Στην πραγματικότητα, η έκθεση αποκαλύπτει ότι ένας σημαντικός αριθμός των ανθρώπων που δεν προτιμούν να πληρώσουν για ένα λογισμικό και να συμμετέχουν στην πειρατεία!

Σας κρατά από το να είναι ανήθικη!

Δεν είναι ότι θα πρέπει να ακολουθήσετε την ηθική του υπολογιστή για να δείξουμε στους άλλους. Ωστόσο, ακολουθώντας τα παρακάτω, θα ξέρετε τι πρέπει να κάνετε για ένα υπεύθυνο χρήστη και να κρατήσει τον εαυτό σας από να πάρει στο πρόβλημα με το να είναι ανήθικο. Πρόβλημα;

Λοιπόν, ναι, υπάρχουν διάφοροι νόμοι που μπορεί να σας βάλει πίσω από τα κάγκελα, αν είστε αλιεύτες, παραβιάζουν τις πολιτικές προστασίες προσωπικών δεδομένων και τους κανόνες των επιμέρους ιστοσελίδες. Θυμάμαι ότι διαβάζοντας ένα σχολείο έπρεπε να πληρώσει σχεδόν 5 εκατομμύρια δολάρια ως πρόστιμο για τη χρήση πειρατικού λογισμικού, ήταν ότι αργότερα συνειδητοποίησαν ότι να πάρει μια άδεια θα ήταν πολύ πιο οικονομική.

Κάνει τον υπολογιστή σας ένα καλύτερο και ασφαλές μέρος

Ο υπολογιστής σας δεν είναι απλά μια ηλεκτρονική συσκευή για την επικοινωνία, είναι τα δεδομένα σας, άλμπουμ φωτογραφιών σας, η εργασία σας,η συσκευή εγγραφής σας, κοινωνικό δίκτυο υπολογιστή και τι όχι ..., είναι αυτό που είσαι! Αν

εμπλακούν σε λήψη πληροφοριών ή την πρόσβαση σε πύλες που δεν επιτρέπεται, ανοίγει τις πόρτες του ,διάφορα ζητήματα και απειλές όπως οι ιοί και Trojans που μπορούν να εισέλθουν παράνομα το σύστημά σας και να καταρρεύσει εντελώς! Από την άλλη πλευρά, αν το σύστημά σας χρησιμοποιείται με τον τρόπο που υποτίθεται ότι, θα είναι η δημιουργία ενός ασφαλέστερου και μια καλύτερη ατμόσφαιρα, όπου μπορείτε να είστε σίγουροι ότι η εργασία σας και τα προσωπικά σας στοιχεία είναι απολύτως ασφαλή.

Ηθική υπολογιστή είναι κάτι που δεν μπορεί να επιβληθεί σε σας, είναι μάλλον κάτι που θα πρέπει να ακολουθηθεί από τη θέληση και την επιθυμία σας. Ο τρόπος που χρησιμοποιείτε τον υπολογιστή σας για να αποκτήσετε πρόσβαση σε πληροφορίες που μιλάει πολύ για σας και τις ηθικές αξίες σας. Τι θα κάνετε αν πάρετε τον κωδικό πρόσβασης του συναδέλφου σας; Θα τον ρωτήσετε ή θα το αλλάξετε από τη στιγμή που τυχαία βρέθηκαν έξω, ή θα προσπαθήσετε να πάρετε κάποιες πληροφορίες που δεν πρέπει; Υπάρχουν δύο είδη ανθρώπων σε αυτόν τον κόσμο, αυτός που ακολουθεί τους κανόνες και σέβεται την ίδια στιγμή, και οι άλλοι που δεν ενδιαφέρονται πραγματικά. Σε περίπτωση που σας ενδιαφέρει για την ηθική που εμπλέκονται στο να γίνει ένας υπεύθυνος πολίτης; Εσείς αποφασίζετε! Παρ 'όλα αυτά, αν είστε αλιεύτες, να είστε σίγουροι ότι οι αρχές δεν θα νοιάζονται για σας, όπως καλά!

ΟΙ ΠΟΛΙΤΙΚΕΣ - ΚΟΙΝΩΝΙΚΕΣ ΕΠΙΠΤΩΣΕΙΣ ΤΩΝ ΙΩΝ ΤΩΝ Η/Υ

ΟΙ ΠΟΛΙΤΙΚΕΣ ΕΠΙΠΤΩΣΕΙΣ ΤΩΝ ΙΩΝ

Πολιτικές μπορούμε να ονομάσουμε τις επιπτώσεις των ιών που άπτονται σε θέματα λειτουργίας του πολιτικού συστήματος αλλά και της καθημερινότητας του πολίτη. Συγκεκριμένα: Οι ιοί επεμβαίνουν και αλλοιώνουν ή κωλυσιεργούν ή ακυρώνουν λειτουργίες των πολιτικών θεσμικών οργάνων, όπως:

1. ΛΕΙΤΟΥΡΓΙΑ ΜΜΕ : η διείσδυση ιών στη λειτουργία των ΜΜΕ απειλεί τη λειτουργία τους και τον πολιτικό τους ρόλο.

- Αλλοιώνουν την αλήθεια μέσω της παρέμβασής τους στα ΜΜΕ. Τα ΜΜΕ αποτελούν σήμερα τον κύριο φορέα πολιτικής ενημέρωσης. Με την ενημέρωση αυτή ο πολίτης γνωρίζει τα γεγονότα, μαθαίνει τα προβλήματα, αποκτά πολιτική θέση, ενεργοποιείται και πολιτικοποιείται. Χωρίς σωστή και αντικειμενική ενημέρωση παραπληροφορείται, αποπροσανατολίζεται και χειραγωγείται. Τότε η Δημοκρατία απειλείται.
- Υπάρχει μεγάλος κίνδυνος αλλοίωσης του εκλογικού αποτελέσματος .
- Αλλοίωση επικοινωνίας μεταξύ κρατών με αποτέλεσμα σοβαρά προβλήματα στις διπλωματικές-διακρατικές σχέσεις. Σε αυτού του είδους την κακόβουλη διείσδυση ιών στα συστήματα της επικοινωνίας θα μπορούσε κανείς να υποθέσει ότι κρύβονται μηχανισμοί τρομοκρατίας ή κατασκοπίας.

2. ΛΕΙΤΟΥΡΓΙΑ ΤΩΝ ΘΕΣΜΩΝ ΠΡΟΣΤΑΣΙΑΣ ΤΟΥ ΠΟΛΙΤΗ: οι ιοί μπορούν να απειλήσουν τη λειτουργία της αστυνομίας και του στρατού είτε με την ακύρωση της λειτουργίας τους σε κάποια περίπτωση(απώλεια στοιχείων), είτε με την απώλεια πολύτιμου χρόνου ώστε η παρέμβασή τους να καθίσταται αναποτελεσματική.

3.ΛΕΙΤΟΥΡΓΙΑ ΚΟΙΝΩΝΙΚΩΝ ΘΕΣΜΩΝ :

- Παρέμβαση στη λειτουργία της εκπαίδευσης: απώλεια ωρών διδασκαλίας και πρόβλημα στη μεταφορά δεδομένων κυρίως για τη σωστή και αδιάβλητη λειτουργία των πανελληνίων εξετάσεων.
- Τεράστιο πρόβλημα στο σύστημα Υγείας, όπως στα νοσοκομεία, καθώς πλήθος δεδομένων μπορούν να χαθούν ή να αλλοιωθούν με άμεση επίπτωση στη ζωή ανθρώπων.
- Ασφάλεια μεταφορών στα μέσα μαζικής μεταφοράς που ελέγχονται από συστήματα πληροφορικής. Ιδίως οι αερομεταφορές ,με τη διείσδυση ιών στα συστήματα ελέγχου των αεροπλάνων και των αεροδρομίων, απειλούνται με ολική καταστροφή και κίνδυνο για εκατοντάδες ανθρώπινες ζωές.

ΟΙ ΕΠΙΠΤΩΣΕΙΣ ΤΩΝ ΙΩΝ ΜΠΟΡΟΥΝ ΝΑ ΔΙΑΧΥΘΟΥΝ ΣΕ ΚΑΘΕ ΠΟΛΙΤΙΚΟΚΟΙΝΩΝΙΚΗ ΠΤΥΧΗ ΤΗΣ ΖΩΗΣ, ΟΠΩΣ:

1. Απώλεια της ιδιωτικότητας. Τα προσωπικά δεδομένα αποτελούν σήμερα ένα μεγάλο μύθο. Μέσω ιών μπορούν να αλλοιωθούν αλλά και να κοινοποιηθούν σε οποιονδήποτε κακόβουλο καταχραστή.
2. Κίνδυνος στις συναλλαγές τραπεζών.
3. Αλλοίωση στις χρηματιστηριακές συναλλαγές
4. Εμπόδιο στην καθημερινή επικοινωνία, εργασία, ψυχαγωγία του πολίτη.

Πηγές :

- www.wikipedia.gr
- <http://www.asda.gr>
- <http://lipas.uwasa.fi>
- www.kouloukis.gr

