2012

ΚΟΙΝΩΝΙΚΗ ΜΗΧΑΝΙΚΗ ΚΑΙ ΑΣΦΑΛΕΙΑ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΜΠΛΕΤΣΑΣ ΙΩΑΝΝΗΣ

Α.Μ. : 2004036

ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ

ΤΜΗΜΑ ΧΡΗΜΑΤΟΟΙΚΟΝΟΜΙΚΗΣ ΚΑΙ ΕΛΕΓΚΤΙΚΗΣ

Επιβλέπων καθηγητής :

Νικολαΐδης Βασίλειος

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

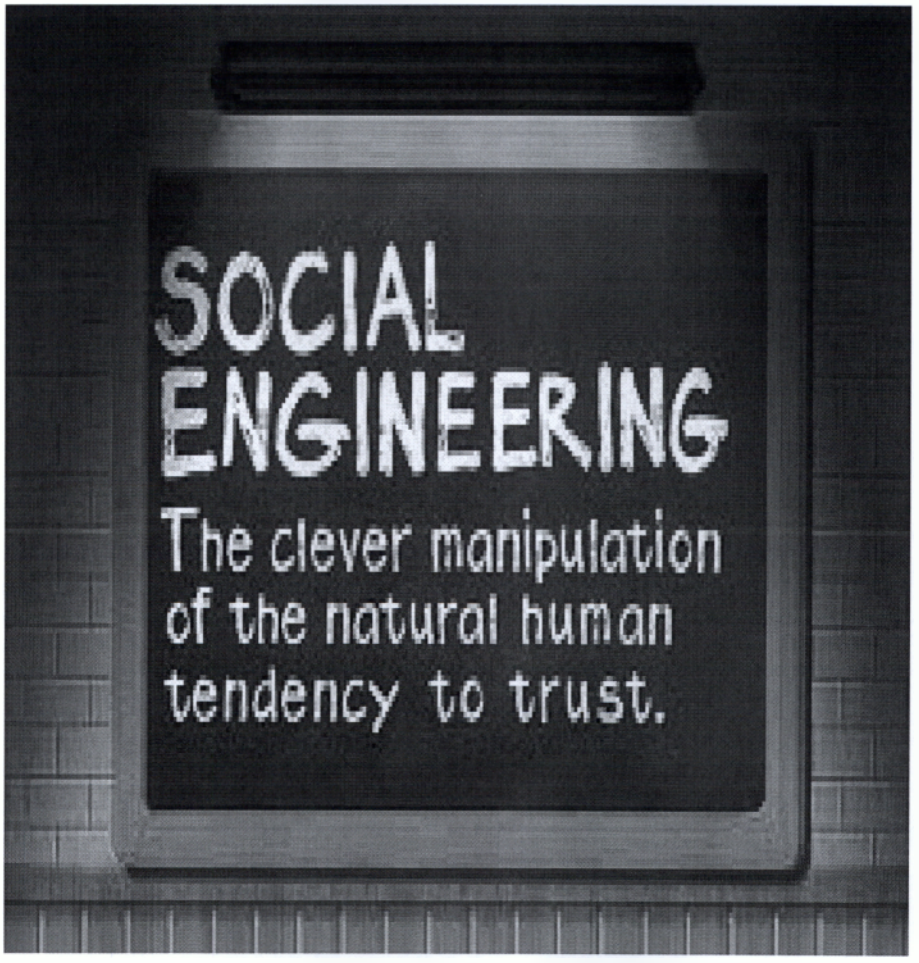
Υπεύθυνη Δήλωση *: Βεβαιώνω ότι είμαι συγγραφέας αυτής της πτυχιακής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της αναφέρεται στην πτυχιακή εργασία. Επίσης έχω αναφέρει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Επίσης βεβαιώνω ότι αυτή η πτυχιακή εργασία προετοιμάστηκε από εμένα προσωπικά ειδικά για τις απαιτήσεις του προγράμματος σπουδών του Τμήματος Χρηματοοικονομικής και Ελεγκτικής του Α.Τ.Ε.Ι. Καλαμάτας.*

Περίληψη

Δεν παίζει ρόλο το τί γνωρίζεις, αλλά τον ποιόν γνωρίζεις. Είτε πρόκειται για μια καλή συμφωνία για ένα προϊόν, είτε για ένα δωρεάν μέρος να πάτε διακοπές ή ένα πλεονέκτημα για να χτυπήσετε τον ανταγωνισμό για μια θέση εργασίας, το να γνωρίζεις τους σωστούς ανθρώπους σου δίνει το πλεονέκτημα που χρειάζεσαι για να πετύχεις τους στόχους σου. Το να γνωρίζεις τους σωστούς ανθρώπους είναι μια μορφή κοινωνικής μηχανικής. Η κοινωνική μηχανική χρησιμοποιεί τις σχέσεις μεταξύ ανθρώπων για να επιτευχθούν οι στόχοι του καθενός. Δυστυχώς, όταν μιλάμε για την ασφάλεια των δεδομένων και την δομή μιας επιχείρησης, η κοινωνική μηχανική επιτίθεται στο μεγαλύτερο εργαλείο που μπορεί να έχει στην διάθεση του ένας υπάλληλος, τον ηλεκτρονικό του υπολογιστή. Στην πτυχιακή αυτή θα αναφερθούμε και θα περιγράψουμε την κοινωνική μηχανική, κάποιες από τις κοινές τεχνικές που χρησιμοποιούνται από τους κοινωνικούς μηχανικούς, θα προτείνουμε πολιτικές, πρότυπα και διαδικασίες για να βοηθήσουν στην καταπολέμηση μιας τέτοιας απειλής σε μια επιχείρηση. Επίσης θα αναφερθούμε στην χρήση των υπολογιστών των υπαλλήλων και την χρήση τους για την καλύτερη ασφάλεια, προστασία και αξιοποίηση των εργαλείων που έχουν στην διάθεση τους.

ΚΕΦΑΛΑΙΟ 1

ΕΙΣΑΓΩΓΗ ΣΤΗΝ ΚΟΙΝΩΝΙΚΗ ΜΗΧΑΝΙΚΗ



Εισαγωγή

Στο πλαίσιο της ασφάλειας, κοινωνική μηχανική δεν πρέπει να θεωρηθεί απλώς ως η τέχνη της χειραγώγησης των ανθρώπων να εκτελούν διάφορες ενέργειες ή να αποκαλύπτουν εμπιστευτικές πληροφορίες. Ενώ η έννοια της είναι παρόμοια με την απάτη, έχει να κάνει συνήθως με την παραπλάνηση ή την εξαπάτηση για το σκοπό της συλλογής πληροφοριών και την είσοδο σε μη εξουσιοδοτημένα πληροφοριακά συστήματα με σκοπό την υποκλοπή πληροφοριών. Παρότι που ο επιτιθέμενος σε ελάχιστες περιπτώσεις θα έρθει πρόσωπο με πρόσωπο με το θύμα του, οι επιθέσεις του θεωρούνται ως πράξεις κυρίως ψυχολογικής χειραγώγησης καθώς μπορούμε να πούμε ότι συνδέετε με τις κοινωνικές επιστήμες. Μπορεί να μην φαίνεται και τόσο επικίνδυνο αλλά με την χρήση της από επαγγελματίες του είδους μπορεί να προκαλέσει ανεπανόρθωτες ζημίες σε έναν μια εταιρία.

1.1 Ορισμός κοινωνικής μηχανικής

Σύμφωνα με το λεξικό του Merriam Webster, η κοινωνική μηχανική είναι "η διαχείριση των ανθρώπινων όντων σύμφωνα με τη θέση και τη λειτουργία τους στην κοινωνία"[1]. Η κοινωνική μηχανική χρησιμοποιεί τις ανθρώπινες σχέσεις για να επιτύχει ένα στόχο και δεν χρησιμοποιείται απαραιτήτως για κακόβουλο σκοπό. Έχει αναφερθεί ότι χρησιμοποιείτε από τις αστυνομικές αρχές σε διαφορές αποστολές ή ακόμη και για κατασκοπεία προσπαθώντας να αποκτήσουν διάφορες πληροφορίες σχετικά με κάποιο τρομοκρατικό χτύπημα. Σε αυτή την πτυχιακή θα αναφερθούμε στην κοινωνική μηχανική ως κακόβουλη πρόθεση συγκεκριμένων ατόμων να θέσουν σε κίνδυνο εταιρικά περιουσιακά στοιχεία.

Ορισμένοι λένε ότι η κοινωνική μηχανική είναι μια τέχνη ή μια δεξιότητα που δεν την κατέχουν όλοι. Αυτό είναι εν μέρει αλήθεια καθώς δεν έχει ο καθένας καλές κοινωνικές δεξιότητες. Ωστόσο, οι περισσότεροι άνθρωποι έχουν "προγραμματιστεί" να είναι κοινωνικοί μηχανικοί από νεαρή ηλικία. Ως παιδία, οι άνθρωποι μαθαίνουν να παίρνουν αυτό που θέλουν χρησιμοποιώντας κοινωνικές μηχανικές τακτικές για να επιτύχουν τον σκοπό τους όπως για παράδειγμα να κλαίνε όταν χρειάζονται προσοχή ή φαγητό. Με λίγη σκέψη και προσπάθεια, η κοινωνική μηχανική μπορεί να γίνει ένας εύκολος και αποτελεσματικός τρόπος για ένα άτομο με κακόβουλη πρόθεση να

[1] Merriam Webster, Unabridged Dictionary

κάνει τη ζωή για κάθε οργανισμό δύσκολη. Η κοινωνική μηχανική δεν απαιτεί μεγάλη τεχνική γνώση, αλλά βασίζεται σε μεγάλο βαθμό από τις κοινωνικές δεξιότητες. Ένας χάκερ που περνάει αρκετές ώρες προσπαθώντας να σπάσει κωδικούς θα μπορούσε να γλυτώσει πολύ χρόνο καλώντας έναν εργαζόμενο μιας επιχείρησης και προσποιώντας ότι είναι υπάλληλος του IT ή του helpdesk να ζητήσει τους κωδικούς που χρειάζεται.

1.2 Εργαλεία για την επίτευξη στόχων

Οι κοινωνικοί μηχανικοί χρησιμοποιούν διάφορες τακτικές για να αξιοποιήσουν την εμπιστοσύνη, την εξυπηρετικότατα, την εύκολα προσβάλαμε πληροφορία, τη γνώση των εσωτερικών διαδικασιών, την εξουσία, την τεχνολογία ή και οποιοσδήποτε συνδυασμό αυτών. Συχνά χρησιμοποιούν διάφορες "μικρές" επιθέσεις πριν μπούνε σε θέση ώστε να πετύχουν τον σκοπό τους. Η κοινωνική μηχανική έχει να κάνει με την εκμετάλλευση των υπολοίπων για την συλλογή πληροφοριών πριν την τελική διεισδυτική επίθεση. Μια επιτυχημένη προσπάθεια κοινωνικής μηχανικής θα μπορούσε να οδηγήσει σε μεγάλες οικονομικές απώλειες στην επιτιθέμενη επιχείρηση. Ένας κοινωνικός μηχανικός με κίνητρο είναι πρόθυμος να αποκτήσει τις πληροφορίες που χρειάζεται με κάθε δυνατό τρόπο.

1.2.1 Εξασφάλιση της εμπιστοσύνης

Η εκμετάλλευση της ανθρώπινης φύσης είναι το δυνατότερο χαρτί ενός κοινωνικού μηχανικού. Ως μέρος της ανθρώπινης φύσης, οι άνθρωποι έχουν ανάγκη την εμπιστοσύνη και παίρνουν ικανοποίηση βοηθώντας αυτούς που έχουν ανάγκη. Προκειμένου όμως ένας κοινωνικός μηχανικός να αποκτήσει τις πληροφορίες που χρειάζεται, όπως έναν τηλεφωνικό αριθμό ή έναν κωδικό, ο εισβολέας θα πρέπει πρώτα να κερδίσει την εμπιστοσύνη από το άτομο που σκοπεύει να αποκτήσει τις πληροφορίες που χρειάζεται. Οι κοινωνικοί μηχανικοί συχνά χρησιμοποιούν μια άμεση προσέγγιση για να αποκτήσουν τις πληροφορίες που χρειάζονται για μια επίθεση με ένα απλό τηλεφώνημα ζητώντας πληροφορίες. Συχνά ο εισβολέας πιθανόν να χρησιμοποιήσει μια σειρά από κλήσεις σε περισσότερα από ένα άτομα για να αποκτήσει πληροφορίες ή ακόμα και την πρόσβαση που χρειάζεται για να προκαλέσει ζημία. Ο κοινωνικός μηχανικός ίσως "δοκιμάζει τα νερά" με ένα άτομο που έχει έρθει

σε επαφή ρωτώντας απλές ερωτήσεις ή απλώς κάνοντας κουβέντα πάνω στο θέμα που τον ενδιαφέρει. Ένας αποτελεσματικός κοινωνικός μηχανικός είναι πολύ καλός στο να λαμβάνει προειδοποιητικά σημάδια όπως τον δισταγμό του ατόμου να προσφέρει ορισμένες πληροφορίες. Μια αίσθηση δισταγμού δείχνει στον εισβολέα ότι η εμπιστοσύνη δεν έχει καθιερωθεί και ότι το άτομο είναι πιο πιθανό να μην αποκαλύψει πληροφορίες.

Ο ευκολότερος τρόπος για έναν κοινωνικό μηχανικό να αποκτήσει πληροφορίες είναι να μην κάνει ύποπτες ερωτήσεις που θα κάνει τους γύρω του να τον υποψιαστούν. Ένας κοινωνικός μηχανικός που θα ρωτάει ευαίσθητες πληροφορίες όπως κωδικούς θα έχει λιγότερες πιθανότητες να πετύχει τον σκοπό του σε σχέση με εκείνον που δεν κάνει τόσο ύποπτες ερωτήσεις. Αυτός είναι ο λόγος που οι κοινωνικοί μηχανικοί υποκινούν μια σειρά ερωτήσεων για να αποκτήσουν αργά αλλά σταθερά τα κομμάτια πληροφοριών που χρειάζονται. Ένας κοινωνικός μηχανικός θα ξεκινήσει κάνοντας απλές ερωτήσεις που φαίνονται αβλαβής για τον επιτιθέμενο. Αν ένας εισβολέας διαισθανθεί δισταγμό στην φωνή του συνομιλητή του στο τηλέφωνο θα μείνει στις απλές ερωτήσεις περιμένοντας να αποσπάσει πληροφορίες από το επόμενο άτομο που αυτός ή αυτή θα επιλέξει να καλέσει. Όσο μεγαλύτερη είναι η επιχείρηση, τόσο ευκολότερο είναι να κερδίσει την εμπιστοσύνη των ατόμων που εργάζονται. Σε ένα μικρότερο περιβάλλον ο στόχος είναι πολύ πιο πιθανό να γνωρίζει εάν ή όχι ο εισβολέας είναι αυτός που ισχυρίζεται ότι είναι.

1.2.2 Τεχνικές κοινωνικής μηχανικής

Ένας κοινωνικός μηχανικός μπορεί να χρησιμοποιήσει μια τεχνική γνωστή και ως αντίστροφη κοινωνική μηχανική. Υπάρχουν τρία μέρη για να αντιστρέψουν την κοινωνική μηχανική: "το σαμποτάζ, η διαφήμιση και η παροχή βοήθειας." Η αντίστροφη κοινωνική μηχανική περιλαμβάνει τη δημιουργία μιας κατάστασης όπου ο εισβολέας πρέπει να βοηθήσει τον στόχο. Αυτός είναι ένας πολύ καλός τρόπος για την ίδρυση της εμπιστοσύνης γιατί ένας στόχος ο οποίος παίρνει βοήθεια από τον εισβολέα θα είναι πιο πρόθυμος να βοηθήσει τον εισβολέα σε αντάλλαγμα. Όταν δημιουργείται μια κατάσταση για αντίστροφη κοινωνική μηχανική, ένας εισβολέας γενικά θα τοποθετηθεί σαν κάποιος του οποίου το χτύπημα θα αναγνωριστεί ως ένα

άτομο που μπορεί ταυτόχρονα να λύσει τα προβλήματα τους και να λαμβάνει προνομιούχες πληροφορίες.

Ο εισβολέας θα προσπαθήσει και θα διαλέξει ένα άτομο που αυτός ή αυτή πιστεύει ότι έχει πληροφορίες για να τους βοηθήσει. Ένας εισβολέας μπορεί να δημιουργήσει μια κατάσταση όπου τίποτα δεν πάει στραβά ακόμα και να χρησιμοποιήσει αποτελεσματικά την αντίστροφη προσέγγιση. Για παράδειγμα να προσποιηθεί ότι είναι υπάλληλος του τμήματος IT και να καλέσει το άτομο που έχει ως σκοπό να του αποσπάσει πληροφορίες, προειδοποιώντας το ότι υπάρχει πρόβλημα συνδεσιμότητας μεταξύ του υπολογιστή του και του δικτύου της εταιρίας πράγμα το οποίο δεν θα ισχύει. Στην συνέχεια θα του κάνει ερωτήσεις σχετικά με το πρόβλημα που έχει δημιουργηθεί και στο τέλος θα του ζητήσει να επαληθεύσει και ο υπάλληλος ότι δεν υπάρχει πρόβλημα συνδεσιμότητας, πράγμα που ο εισβολέας θα ξέρει ότι δεν υπάρχει.

Μετά τη δημιουργία μιας τέτοιας κατάστασης, ο εισβολέας έχει δημιουργήσει ένα επίπεδο εμπιστοσύνης που μπορεί να χρησιμοποιηθεί για να ζητήσει βοήθεια στην απόκτηση πληροφοριών στο μέλλον. Αυτό είναι επίσης ένας καλός τρόπος για έναν κοινωνικό μηχανικό για να εγκαταστήσει κακόβουλο λογισμικό σε ένα μηχάνημα στόχων.

Ο κοινωνικός μηχανικός που τοποθετείται σαν ένας υπάλληλος του IT ή προμηθευτής του λογισμικού μπορεί να ζητήσει από τον στόχο να πάει σε μια ιστοσελίδα ή να ανοίξει ένα συνημμένο ηλεκτρονικό ταχυδρομείο που στάλθηκε στον στόχο το οποίο μπορεί να περιέχει έναν ιό ή ένα κακόβουλο λογισμικό. Σε αυτήν την περίπτωση ο κοινωνικός μηχανικός μπορεί να πει, για παράδειγμα, ότι το λογισμικό απαιτείται για να εγκατασταθεί ως μέρος μιας αναβάθμισης.

1.2.3 Εύκολα προσβάσιμη πληροφορία

Δυστυχώς, οι κοινωνικοί μηχανικοί ευδοκιμούν σε εύκολα προσβάσιμες πληροφορίες όπως είναι οι αριθμοί τηλεφώνου. Οι κοινωνικοί μηχανικοί σχεδιάζοντας να παρουσιαστούν σαν υπάλληλοι της επιχείρησης θα πρέπει πρώτα να αναγνωρίσουν την ταυτότητα κάποιου έτσι ώστε να μπορούν να "μεταμφιεστούν" σαν αυτόν. Οι εταιρικοί κατάλογοι είναι συχνά εύκολο να βρεθούνε και στα μάτια των εσωτερικών υπαλλήλων δεν φαίνονται σαν ευαίσθητα δεδομένα διότι πολλά άτομα μπορεί να σκέφτονται ότι ανταλλάσοντας ονόματα, τοποθεσίες και αριθμούς τηλεφώνου είναι ακίνδυνο. Οι κοινωνικοί μηχανικοί το κάνουν αυτό για να αποκτήσουν πρόσβαση στα προσωπικά στοιχεία των ατόμων που θέλουν να επωφεληθούν. Ένα απλό τηλεφώνημα προς μια εταιρική ρεσεψιονίστ είναι το μόνο που χρειάζεται για έναν κοινωνικό μηχανικό για να μάθει το όνομα και το τηλέφωνο ενός διαχειριστή, ή κάποιον σε μια συγκεκριμένη θέση, για να αποκτήσει πληροφορίες για το θέμα που χρειάζεται. Οι κοινωνικοί μηχανικοί μπορούν να καλούν στο τμήμα ανθρωπίνων πόρων για να μαθαίνουν τα ονόματα των υπαλλήλων που θέλουν να στοχεύσουν. Ο εισβολέας επίσης μπορεί να συλλέξει εύκολα προσβάσιμες πληροφορίες από την περιήγηση σε εταιρικές ιστοσελίδες.

1.2.4 Γνώση εσωτερικών διαδικασιών

Ένας επιτιθέμενος μπορεί να έχει μεγάλη επιτυχία στο να επιτύχει τον σκοπό του με το να γνωρίζει τις διάφορες εσωτερικές λειτουργίες μιας επιχείρησης. Με την κατάλληλη χρήση ορολογίας, ένας κοινωνικός μηχανικός μπορεί να ξεγελάσει τον στόχο του και να τον κάνει να νομίζει ότι ο κοινωνικός μηχανικός είναι πράγματι ένας υπάλληλος της εταιρίας. Για παράδειγμα, γνωρίζοντας την μέθοδο που χρησιμοποιεί ένα γραφείο υποστήριξης για την επαλήθευση ταυτότητας και ανταποκρίνοντας αντίστοιχα θα αυξήσει την πειστικότητα της κλήσης στην υπηρεσία υποστήριξης και υποκρινόμενος τον υπάλληλο που ξέχασε τον κωδικό του μπορεί να αποκτήσει εύκολα πρόσβαση. Υπάρχει όμως και το ενδεχόμενο ότι ένας κοινωνικός μηχανικός μπορεί να έχει ήδη ένα μεγάλο μέρος των πληροφοριών σχετικά με τον στόχο του. Ένας αλλόφρων πρώην υπάλληλος που θέλει να διαταράξει την επιχειρηματική δραστηριότητα γνωρίζει πιθανόν ήδη τους ανθρώπους που μπορεί να χρησιμοποιήσει σαν πιόνια για την επίθεση. Ο πρώην υπάλληλος θα μπορούσε επίσης να έχει κάνει κάποιου είδους προεργασία πριν την αποχώρηση του, όπως η

εγκατάσταση κακόβουλου λογισμικού. Για αυτό τον λόγο οι κίνδυνοι για τα περιουσιακά στοιχεία μιας εταιρείας δεν είναι απαραίτητο να είναι μόνο εξωτερικοί αλλά και εσωτερικοί. Αντιθέτως μια επιχείρηση πρέπει να προστατευτεί και από κοινωνικούς μηχανικούς που ίσως άλλοτε εργαζόντουσαν σε εκείνη.

1.2.5 Επιρροή

Επιρροή, ή απλά έχοντας εξουσία πάνω από κάποιον, είναι μία τεχνική που χρησιμοποιείται από τους κοινωνικούς μηχανικούς για να φοβίσουν τον στόχο. Αυτό συχνά επιτυγχάνεται, παρουσιάζοντας τους εαυτούς τους ως μία δεσποτική φιγούρα όπως αυτή του μάνατζερ. Αφού ο κοινωνικός μηχανικός εκμαιεύσει πληροφορίες για τους υπευθύνους, μπορεί να παρουσιαστεί στον στόχο με τέτοιον τρόπο ώστε να του απαιτήσει, πλέον, πληροφορίες. Για να χρησιμοποιηθεί η μέθοδος της Επιρροής αποδοτικότερα, οι κοινωνικοί μηχανικοί δεν χρειάζεται πάντα να παρουσιαστούν σαν προϊστάμενοι. Μπορούν να πουν πως καλούν εκ μέρους του CEO, CFO ή κάποιου άλλου υψηλόβαθμου εργαζομένου που χρειάζεται πληροφορίες άμεσα και δεν δέχεται το όχι σαν απάντηση. Όταν οι ευαίσθητες πληροφορίες αποκαλυφθούν, η εμπιστοσύνη γεφυρώνεται, εννοώντας πως μελλοντικά ο επιτιθέμενος μπορεί να χρησιμοποιήσει την ίδια μέθοδο κατά του ίδιο ατόμου.

1.2.6 Τεχνολογία

Παρόλο που μία επιτυχημένη επίθεση ενός κοινωνικού λειτουργού, δεν απαιτεί πολλές τεχνολογικές γνώσεις, χρησιμοποιώντας την τεχνολογία σε συνδυασμό με τις αρχές της κοινωνικής μηχανικής μπορεί να είναι πολύ αποτελεσματικό. Ένας κοινωνικός λειτουργός μπορεί να χρησιμοποιήσει τις παραπάνω τεχνικές για να μάθει την τεχνική κατασκευή μίας εταιρίας έτσι ώστε να εξαπολύσει έναν ιό που θα μπορούσε να ρίξει κάτω ένα ολόκληρο δίκτυο. Οι κοινωνικοί μηχανικοί μπορούν να αναπτύξουν έναν "Δούρειο ίππο" (Trojan), ένα πρόγραμμα στο οποίο εμπεριέχεται κακόβουλος ή επιβλαβές κώδικας και μπορεί να υπάρξει σε ένα φαινομενικά άκακο πρόγραμμα ή δεδομένο με τέτοιο τρόπο που μπορεί να έχει έλεγχο και να κάνει τι ζημιά που επιλέχτηκε να κάνει.

Ο κοινωνικός λειτουργός μπορεί να στείλει έναν ιό ή trojan horse ως μία επισύναψη σε e-mail· να αφήσει μία δισκέτα ή ένα δίσκο CD στην τοποθεσία που

εργάζεται με επιβλαβές software μέσα· να χρησιμοποιήσει ψεύτικα pop-up window's παραπέμποντας τον χρήστη να κάνει είσοδο με τον κωδικό του δικτύου του· να στείλει δωρεάν software ή patch, για το θύμα να κάνει install.

1.3 Κερδίζοντας σωματική πρόσβαση

Πολλά εταιρικά γραφεία έχουν πολλές εύκολα προσβάσιμες πληροφορίες που μπορούν να βοηθήσουν έναν κοινωνικό μηχανικό να διαπράξει την επίθεσή του/της. Παρόλο που οι κοινωνικοί μηχανικοί συνήθως αποφεύγουν να βρεθούν στη θέα του στόχου, το να το κάνουν μπορεί να είναι εύκολο. Τις μέρες αυτές, οι περισσότεροι μεγάλοι οργανισμοί χρησιμοποιούν ένα σύστημα με καρτελάκια ή ταυτότητες ώστε να μπεις στο κτήριο ή την φυλασσόμενη περιοχή. Στις μεγάλες επιχειρήσεις οι περισσότεροι υπάλληλοι μπορεί να μην γνωρίζονται μεταξύ τους ούτε να μπορούν να αναγνωρίσουν το κάθε πρόσωπο και ευχαρίστως θα κράταγαν και την πόρτα ανοιχτή για να περάσει κάποιος, ακόμα και εάν τον έβλεπαν πρώτη φορά. Με το που αποκτήσουν πρόσβαση, οι κοινωνικοί μηχανικοί μπορούν να αποκτήσουν ένα πλήθος πληροφοριών κάνοντας απλά μια βόλτα ανάμεσα από τους χώρους εργασίας των εργαζομένων που λείπουν από τα γραφεία τους. Από αυτή την απλή βόλτα ανάμεσα από τα γραφεία, ο κοινωνικός μηχανικός μπορεί να βρει διαφόρους κωδικούς σε σημειώματα κολλημένα στις οθόνες των υπαλλήλων, οικονομικά στοιχεία όπως τιμολόγια και εντολές αγοράς ή ακόμα και έγγραφα σχετικά με την τεχνική υποδομή και στην συνέχεια να φύγει ανενόχλητος.

Η απόκτηση πληροφοριών γίνεται πιο εύκολα τις απογευματινές ή τις βράδυνες ώρες που οι περισσότεροι υπάλληλοι λείπουν. Εκείνες τις ώρες ο κοινωνικός μηχανικός μπορεί να υποδύεται κάποιον καθαριστή ή κάποιον συντηρητή για να κερδίσει εύκολη πρόσβαση στην επιχείρηση. Μερικοί ίσως προσπαθήσουν να αποκτήσουν θέση σε ένα συνεργείο καθαρισμού για να μπορέσουν να κερδίσουν πρόσβαση στην επιχείρηση. Εφόσον μπούνε στην εταιρεία θα προσπαθήσουν να βρούνε τον υπολογιστή κάποιου χρήστη που δεν έχει κλείσει ή δεν έχει κλειδώσει τον υπολογιστή του και να εγκαταστήσει κακόβουλο λογισμικό ή να κλέψει πληροφορίες. Επίσης μπορεί να αποκτήσει πρόσβαση σε ευαίσθητες για την επιχείρηση πληροφορίες που δεν έχουν καταστραφεί όπως θα έπρεπε. Θα μπορούσε επίσης να εγκαταστήσει εξοπλισμό δικτύωσης, όπως ασύρματα σημεία πρόσβασης. Ένας

κοινωνικός μηχανικός που θα αποκτήσει πρόσβαση στην επιχείρηση που έχει βάλει στον στόχο του, θα προσπαθήσει να είναι όσο τον δυνατόν πιο γρήγορος. Εάν αποκτήσει όμως πρόσβαση την νύχτα που δεν βρίσκεται κανείς τριγύρω θα μπορέσει να ξεκλέψει περισσότερο χρόνο στην συλλογή πληροφοριών. Ένας κοινωνικός μηχανικός που βρίσκεται σε ένα γραφείο απαρατήρητος για αρκετή ώρα, μπορεί να κλέψει εύκολα υλικό, λογισμικό ή οτιδήποτε άλλο πιστεύει ότι θα τον βοηθήσει να πετύχει τον στόχο του.

ΚΕΦΑΛΑΙΟ 2

ΤΡΟΠΟΙ ΠΡΟΣΤΑΣΙΑΣ ΚΑΙ ΠΟΛΙΤΙΚΕΣ ΕΝΑΝΤΙΑ ΣΤΗΝ ΚΟΙΝΩΝΙΚΗ ΜΗΧΑΝΙΚΗ

Εισαγωγή

Καθώς περνάει ο καιρός, συνεχώς αυξάνονται τα επεισόδια κοινωνικής μηχανικής. Νέοι και εξελιγμένοι τρόποι κάθε φορά προσπαθούν να ξεγελάσουν τον κόσμο και να τους αποσπάσουν όσο το δυνατόν περισσότερες πληροφορίες. Αυτό όμως δεν σημαίνει ότι και η ασφάλεια ενάντια στην κοινωνική μηχανική παραμένει η ίδια. Συνεχώς αναπτύσσονται νέοι και ευέλικτοι τρόποι από τις επιχειρήσεις και τους διάφορους οργανισμούς για να περιοριστούν όσο το δυνατόν περισσότερο τα επεισόδια επίθεσης. Σε αυτό το κεφάλαιο θα αναλύσουμε τους τρόπους προστασίας και τις διάφορες πολιτικές καθώς επίσης και τις διάφορες διαδικασίες που πρέπει να ακολουθούνται από τους υπαλλήλους της επιχείρησης για να μειωθεί όσο τον δυνατόν ο κίνδυνος.

2.1 Τρόποι προστασίας ενάντια στην Κοινωνική Μηχανική

Για να καταλάβουμε πως μπορούμε να προστατευτούμε από μια επίθεση κοινωνικής μηχανικής θα πρέπει πρώτα να καταλάβουμε το πως δρα η κοινωνική μηχανική. Μια επιτυχημένη επίθεση από κοινωνικό μηχανικό βασίζεται στους υπαλλήλους μίας επιχείρησης. Οπότε για να περιοριστεί μια τέτοιου είδους επίθεση, οι εργαζόμενοι θα πρέπει να εκπαιδευτούνε και να ενημερωθούνε για τις πιο συχνές τεχνικές κοινωνικής μηχανικής. Επίσης είναι σημαντικό για έναν οργανισμό να καθιερωθεί μια σαφής και ισχυρή πολιτική ασφαλείας, συμπεριλαμβανομένων των προτύπων ασφαλείας και των διαφόρων μεθόδων και διαδικασιών τα οποία θα βοηθήσουν στην εξάλειψη της απειλής της κοινωνικής μηχανικής. Μια καλή άμυνα ενάντια σε μια τέτοια επίθεση θα πρέπει να περιλαμβάνει. :

- Πολιτικές κωδικών
- Δοκιμές διείσδυσης
- Ταξινόμηση δεδομένων
- Συγκεκριμένη χρήση πολιτικής
- Ελέγχους ιστορικού
- Διαδικασία τερματισμού
- Αντιμετώπιση περιστατικών
- Φυσική ασφάλεια

2.1.1 Πολιτικές κωδικών πρόσβασης και πρότυπα

Για μια κοινωνική μηχανική, το να αποκτήσει πρόσβαση σε ένα σύστημα, μπορεί να σημαίνει τη διαφορά ανάμεσα στην επιτυχημένη ή αποτυχημένη επίθεση. Πρέπει να υπάρχει μια πολιτική για την διανομή και την δημιουργία κωδικών εντός της επιχείρησης. Μια καλή πολιτική κωδικών πρόσβασης, θα πρέπει να περιλαμβάνει πληροφορίες σχετικές με το :

- Να μην μοιράζονται οι εργαζόμενοι τους κωδικούς τους.
- Να μην σημειώνουν τους κωδικούς τους.
- Να μη χρησιμοποιούν τους προεπιλεγμένους κωδικούς.
- Μεθόδους για την αναγνώριση των χρηστών σε περίπτωση επαναφοράς του κωδικού πρόσβασης.
- Μεθόδους για την παράδοση κωδικών προς τους χρήστες.
- Περιοδική αλλαγή του κωδικού πρόσβασης.
- Να υπάρχει χρονική περίοδος για κωδικούς που επρόκειτο να λήξουν
- Κλείδωμα λογαριασμού, ύστερα από 3 τρεις αποτυχημένες προσπάθειες εισόδου.

Οι εργαζόμενοι πρέπει να καταλάβουν την σοβαρότητα του να χρησιμοποιούν έναν "δυνατό" κωδικό, ειδικά σε ένα περιβάλλον στο οποίο δουλεύουν αρκετά άτομα. Επίσης είναι σημαντικό να μην αποθηκεύονται ποτέ οι κωδικοί στα διαφορά προγράμματα πλοήγησης στο διαδίκτυο για τον λόγο ότι είναι πολύ εύκολο ακόμα και για κάποιον που έχει βασικές γνώσεις υπολογιστών να υποκλέψει τους κωδικούς αυτούς. Άλλος ένας τρόπος προστασίας των δεδομένων μας είναι να χρησιμοποιούμε διαφορετικούς κωδικούς στα προγράμματα που χρησιμοποιούμε. Με τον τρόπο αυτό ένας κοινωνικός μηχανικός θα δυσκολευτεί περισσότερο να υποκλέψει τους κωδικούς.

Οι κοινωνικοί μηχανικοί τείνουν να πλησιάζουν τους εργασιακούς χώρους των υπαλλήλων για να αποκτήσουν πληροφορίες που μπορούν να χρησιμοποιήσουν. Η χρήση λοιπόν των σημειωμάτων γύρω από τον υπολογιστή μας είναι πονοκέφαλος για την ασφάλεια της εταιρίας αλλά αντιθέτως για έναν κοινωνικό μηχανικό αυτό είναι ευλογία. Έχει αποδειχθεί ότι η χρήση σημειωμάτων είναι πολύ συχνή από τους υπαλλήλους, τοποθετώντας τα είτε στην οθόνη είτε σε κάποιο εύκολα προσβάσιμη

σημείο. Μια καλή πολίτική πάνω σε αυτό το θέμα θα ήταν να απαιτεί από τους υπαλλήλους της να μην σημειώνουν τους κωδικούς τους.

Οι πολιτικές γράφονται για να ακολουθούνται και χρειάζεται πλήρη συνεργασία των εργαζομένων διότι το να εντοπιστούν οι επιτιθέμενοι κοστίζει και είναι χρονοβόρα διαδικασία. Για αυτό τον λόγο η εκπαίδευση των εργαζομένων είναι ένα από τα κύρια ζητήματα στον τρόπο αντιμετώπισης των κοινωνικών μηχανικών. Εάν οι υπάλληλοι καταλάβουν το πόσο επικίνδυνο είναι να σημειώνουν τους κωδικούς τους σε σημειώματα ή να μοιράζονται τους κωδικούς τότε οι πιθανότητες να το ξανακάνουν λιγοστεύουν.

Το προσωπικό του γραφείου υποστήριξης και IT ενός οργανισμού πρέπει να ακολουθεί μια αυστηρή πολιτική στην αναγνώριση ταυτότητας και στην παράδοση κωδικών στους υπαλλήλους του οργανισμού. Η επαλήθευση της ταυτότητας σε αυτή την περίπτωση, αναφέρεται στην επικύρωση ότι ένας επισκέπτης είναι πράγματι αυτός που ισχυρίζεται. Στον κόσμο του σήμερα, η αναγνώριση φωνής δεν είναι ένας επαρκής μηχανισμός για επαλήθευση ταυτότητας. Έπειτα, υπάρχει το θέμα κάποιου να έχει την δυνατότητα να αλλάξει κάποιον κωδικό. Ένας θυμωμένος υπάλληλος υποστήριξης ή ένας διαχειριστής συστήματος που μπορεί να αλλάξει κωδικούς θα μπορούσε πολύ εύκολα να κλέψει ευαίσθητες πληροφορίες και να δημιουργήσει πρόβλημα στον οργανισμό. Για να βοηθήσει στην καταπολέμηση αυτού, το βάρος της αναγνώρισης ατόμων για επαναφορές κωδικών πρόσβασης μπορεί να μετατοπιστεί από το γραφείο υποστήριξης. Με τεχνολογίες και προγράμματα αυτόματης επαναφοράς κωδικού πρόσβασης, δεν χρειάζεται κάποιος υπάλληλος για να επικυρώνει ότι το άτομο στην απέναντι γραμμή του τηλεφώνου είναι αυτός που ισχυρίζεται ότι είναι. Οι τεχνολογίες ανταπόκρισης σε προκλήσεις γίνονται όλο και πιο δημοφιλείς και χρησιμοποιούνται ευρέως σε επιχειρησιακά περιβάλλονται. Με την ανταπόκριση σε προκλήσεις, ένας χρήστης χρειάζεται να απαντήσει σε μια ερώτηση ή πολλαπλές ερωτήσεις πριν του δοθεί η ικανότητα να αλλάξει το δικό του κωδικό πρόσβασης μέσω ενός web interface.

Υπάρχουν πολλές προτάσεις για την κατάλληλη διανομή κωδικού πρόσβασης. Για παράδειγμα, μερικοί οργανισμοί ίσως να επιμένουν ότι οι κωδικοί πρόσβασης πρέπει να διανέμονται από ενδοεταιρικά mail ή άλλες υπηρεσίες ταχυμεταφορών. Αυτό σημαίνει ότι οι κωδικοί πρόσβασης σημειώνονται σε κάποιο αρχείο και μπορεί να υποκλαπούν. Κάποιοι οργανισμοί επικυρώνουν τους κατόχους των λογαριασμών

ρωτώντας τους διάφορες προσωπικές πληροφορίες, όπως τον αριθμό κοινωνικής ασφάλισης. Αυτό στηρίζεται στην αποθήκευση πληροφοριών του υπαλλήλου κατά τέτοιο τρόπο που μπορεί να μην μπορεί να επιτευχθεί είσοδος από υπόλοιπο υπαλληλικό προσωπικό που ίσως μοιράζεται τον κωδικό με άλλους ή υποκλαπεί από τον εισβολέα. Δυστυχώς οι περισσότερες μέθοδοι διανομής κωδικού πρόσβασης δεν είναι 100% ασφαλείς. Εάν οι κωδικοί πρόσβασης διανέμονται μέσω κάποιου εγγράφου ή μέσω ηλεκτρονικού ταχυδρομείου η ταυτότητα σύνδεσης και οι πληροφορίες του συστήματος δεν θα πρέπει ποτέ να γίνουν γνωστές.

Εάν το ηλεκτρονικό ταχυδρομείο δεν είναι απαραίτητο μέσο για μια εταιρεία να δίνει κωδικούς , θα μπορούσε αντί αυτού να χρησιμοποιηθεί για να ενημερώνει τον χρήστη του λογαριασμού να γνωρίζει ότι έχει πραγματοποιηθεί μια αίτηση αλλαγής κωδικού πρόσβασης. Για παράδειγμα, ένας οργανισμός με τη χρήση μιας εφαρμογής μπορεί να στέλνει και να ενημερώνει, μέσω ενός αυτοματοποιημένου e-mail, τον κάτοχο του λογαριασμού ότι πραγματοποιήθηκε αλλαγή στον κωδικό του. Το αυτοματοποιημένο αυτό e-mail θα περιλαμβάνει επίσης την ημερομηνία και την ώρα που έγιναν οι αλλαγές καθώς και την διεύθυνση IP του μηχανήματος από το οποίο έγινε η αλλαγή του συγκεκριμένου κωδικού.

2.1.2 Δοκιμές διείσδυσης (Penetration tests)

Είτε από εξωτερικούς παράγοντες είτε από εσωτερικούς, οι οργανισμοί θα πρέπει να εκτελούν διεισδυτικές αξιολογήσεις. Τέτοιες αξιολογήσεις συνήθως απαρτίζονται από την χρήση γνωστών εργαλείων και τεχνικών hacker για να δοκιμάσουν την ασφάλεια ενός δικτύου. Η προσθήκη της κοινωνικής μηχανικής είναι απαραίτητη για την παροχή μιας ακριβής αξιολόγησης. Τέτοιου είδους δοκιμές είναι απαραίτητο να γίνονται τουλάχιστον μια φορά τον χρόνο, ανάλογα βέβαια και το μέγεθος και το ιστορικό του οργανισμού. Από τότε που τέτοιου είδους επιθέσεις εκμεταλλεύονται από τους υπαλλήλους, χρησιμοποιώντας την κοινωνική μηχανική ως μέρος μιας διεισδυτικής δοκιμής ίσως υπάρξει κίνδυνος νομικών επιπτώσεων και ως εκ τούτου πρέπει να οριστεί ξεκάθαρα και να εγκριθεί πριν υπάρξει εφαρμογή.

2.1.3 Ταξινόμηση δεδομένων

Εφόσον οι κοινωνικοί μηχανικοί χρησιμοποιούνε την γνώση των άλλων για να επιτύχουν τον σκοπό τους, είναι απαραίτητο να υπάρχει ένα μοντέλο ταξινόμησης δεδομένων όπου οι εργαζόμενοι θα βλέπουν και θα τηρούν. Κάθε είδος ταξινόμησης έχει και διαφορετικά επίπεδα ευαισθησίας ως προς την εταιρία. Με αυτό τον τρόπο κάθε επίπεδο περιλαμβάνει και διαφορετικούς κανόνες για το ποιός έχει πρόσβαση να το δει. Η ταξινόμηση δεδομένων βοηθά στον περιορισμό της κοινωνικής μηχανικής εφοδιάζοντας τους εργαζόμενους της επιχείρησης ένα μηχανισμό για την κατανόηση ποιών πληροφοριών μπορούν να κοινοποιηθούν. Επίσης βοηθά στην εξασφάλιση της ακεραιότητας των δεδομένων, ανάλογα την ταξινόμηση τους, και θα πρέπει να υπάρχει ένας υπεύθυνος ή μια ομάδα ατόμων που θα είναι υπεύθυνα για την ενημέρωση αυτών των αρχείων. Τα αρχεία αυτά ταξινομούνται ως εξής :

Άκρως απόρρητα : Ιδιαίτερα ευαίσθητα έγγραφα εσωτερικής χρήσης. Π.χ. διάφορες επενδυτικές στρατηγικές, συγχωνεύσεις ή εξαγορές εταιριών που θα μπορούσαν να βλάψουν σοβαρά μια επιχείρηση ή έναν οργανισμό εάν πληροφορίες σαν αυτή χανόντουσαν ή γινόντουσαν γνωστές στο ευρύ κοινό. Πληροφορίες που ταξινομούνται ως άκρως απόρρητες έχουν μια πολύ περιορισμένη διανομή και πρέπει να προστατεύονται κάθε στιγμή με όσο το δυνατόν μεγαλύτερη ασφάλεια.

Άκρως εμπιστευτικά : Έγγραφα τα οποία εάν δημοσιοποιηθούν ή εάν γίνουν γνωστά έστω και εντός της επιχείρησης θα μπορούσαν να παρεμποδίσουν σημαντικά την διοργάνωση ενεργειών και να βλάψουν σημαντικά της διάφορες ενέργειες που βρίσκονται σε εξέλιξη. Τέτοιου είδους έγγραφα μπορεί να είναι διάφορες λογιστικές πληροφορίες, επιχειρηματικά σχέδια, ευαίσθητα στοιχεία των πελατών της κλπ.

Άκρως ιδιωτικά : Πληροφορίες που έχουν να κάνουν με την ιδιωτική φύση της εταιρίας. Τέτοιου είδους πληροφορίες μπορεί να είναι οι διάφορες διαδικασίες της εταιρίας, το ωράριο των υπαλλήλων της, τα επιχειρηματικά σχέδια, σχεδιασμός νέων προγραμμάτων και οποιαδήποτε άλλη πληροφορία έχει να κάνει με την λειτουργία της επιχείρησης. Αυτές οι πληροφορίες είναι συνήθως μόνο για ιδιωτική χρήση και είναι διαθέσιμη σε εξουσιοδοτημένο προσωπικό. Η ασφάλεια και η προστασία των συγκεκριμένων δεδομένων είναι υψηλή.

Έγγραφα για εσωτερική χρήση: Πληροφορίες που δεν έχουν εγκριθεί για την γενική κυκλοφορία τους εκτός της επιχείρησης, με συνέπεια κατά την απώλεια τους εκτός

του περιβάλλοντος της επιχείρησης θα μπορούσαν να προκληθούν σοβαρά προβλήματα. Τέτοιου είδους έγγραφα εσωτερικής χρήσης μπορεί να είναι τα πρακτικά των συνεδριάσεων, οι εσωτερικές εκθέσεις σχεδίων, εσωτερικά υπομνήματα κ.α. Η Ασφάλεια σε αυτό το επίπεδο είναι ελεγχόμενη άλλα κανονική.

Δημόσια έγγραφα : Πληροφορίες δημόσιου τομέα, ετήσιες εκθέσεις, δηλώσεις στον τύπο. Είναι δηλαδή έγγραφα που έχουν εγκριθεί για δημόσια χρήση. Η ασφάλεια σε αυτό το επίπεδο είναι ελάχιστη.

Με τον τρόπο αυτό, οι πληροφορίες θα πρέπει να προστατεύονται βάση της κατάταξης που τους έχει δοθεί. Έτσι η ασφάλεια μιας απόρρητης πληροφορίας θα διαφέρει από την ασφάλεια ενός δημόσιου εγγράφου. Η απόρρητη πληροφορία θα πρέπει να προστατεύεται πίσω από κάποιο τοίχος προστασίας (firewall) που μόνο συγκεκριμένα άτομα θα έχουν πρόσβαση στους διακομηστές (hosts) όπου περιέχουν τα δεδομένα και τις πληροφορίες, σε αντίθεση με τα δημόσια έγγραφα τα οποία μπορεί να είναι εμφανή ακόμη και στην ιστοσελίδα της επιχείρησης. Επίσης το να υπάρχουν τέτοια είδη ταξινόμησης βοηθούν στο να ελαχιστοποιηθεί ο κίνδυνος να αποκτήσουν στα χέρια τους οι κοινωνικοί μηχανικοί τις πληροφορίες που χρειάζονται για να επιτύχουν τον σκοπό τους. Όπως επίσης θα βοηθήσει τους υπαλλήλους να κατανοήσουν το εάν πρέπει ή όχι να μοιραστούν τις πληροφορίες με άλλα άτομα.

2.1.4 Αποδεκτή χρήση πολιτικής

Μια αποδέκτη χρήση πολιτικής βοηθάει στην εξασφάλιση ότι τα διάφορα εμπιστευτικά δεδομένα εντός της επιχείρησης δεν μπορούν να καταχραστούν ή ακόμα και να μοιραστούν στο εξωτερικό περιβάλλον της. Τέτοιου είδους πολιτικές περιλαμβάνουν πληροφορίες για το πώς ένα τέτοιο σύστημα πρέπει να λειτουργεί. Μια αποδέκτη χρήση τέτοιας πολιτικής περιλαμβάνει τα ακόλουθα.

- Συστήματα πληροφοριών και δικτύου θα πρέπει να διατίθενται μόνο σε εξουσιοδοτημένο προσωπικό.
- Απαγορεύεται η παροχή ή η χρήση κωδικών σε μη εξουσιοδοτημένο προσωπικό.
- Απαγορεύεται να δίνονται ή να μοιράζονται εμπιστευτικές πληροφορίες σε τρίτους.

- Απαγορεύεται η χρήση ηλεκτρονικού ταχυδρομείου για προσωπικούς λόγους.
- Παραχάραξη των πληροφοριών.
- Απαγορεύεται η προσπάθεια να αποκτηθεί πρόσβαση από μη εξουσιοδοτημένους χρήστες.
- Κατάχρηση της σύνδεσης στο διαδίκτυο για προσωπικούς λόγους.
- Αποθήκευση ή ακόμα και χρήση μη εξουσιοδοτημένων ή παράνομων λογισμικών.
- Χρήση του διαδικτύου της επιχείρησης για παράβαση νομοθετικών ή συνταγματικών διατάξεων.
- Άρνηση Υπηρεσιών (Denial of Service)

2.1.5 Έλεγχοι ιστορικού υπαλλήλων

Οι κοινωνικοί μηχανικοί θα χρησιμοποιήσουν κάθε δυνατή μέθοδο για να επιτύχουν τον σκοπό τους. Συνήθως οι επιθέσεις των κοινωνικών μηχανικών βασίζονται έμμεσα στις επιθέσεις μέσω κάποιου που δουλεύει στις επιχείρηση που θέλουν να "χτυπήσουν". Δεν θεωρείται όμως απίθανο για έναν κοινωνικό μηχανικό να αναζητήσει μια θέση εργασίας στην συγκεκριμένη επιχείρηση για να πετύχει τον σκοπό του. Γι' αυτό λοιπόν οι έλεγχοι ιστορικού σε μια εταιρία είναι σημαντικοί διότι είναι η πρώτη και βασική άμυνα απέναντι στους κοινωνικούς μηχανικούς. Ο έλεγχος ιστορικού δεν θα πρέπει να είναι πιο ευέλικτος ή να διαφέρει στους εσωτερικούς υπαλλήλους έστω και εάν δουλεύουν αρκετό καιρό στην επιχείρηση. Τέτοιου είδους έλεγχοι πρέπει να γίνονται από τους courier, τα συνεργεία καθαρισμού μέχρι τους τυχόν εποχιακούς υπαλλήλους της επιχείρησης πριν τους δοθεί έγκριση για είσοδο στην εταιρία ή ακόμα και την άδεια να συνδεθούνε στο δίκτυο της εταιρίας. Οι οργανισμοί θα πρέπει να γνωρίζουν το είδος και την αυστηρότητα του ελέγχου του ιστορικού και με το να γίνουν απλοί έλεγχοι δεν είναι αρκετό. Ένας καλός έλεγχος ιστορικού θα πρέπει να περιλαμβάνει :

- Ιατρικό ιστορικό
- Έλεγχος ποινικού μητρώου
- Έρευνα για διεθνές ποινικό μητρώο

- Την διεύθυνση του και την προηγούμενη διεύθυνση του εάν υπάρχει
- Αναφορά και έλεγχο του αυτοκινήτου ή της μηχανής εφόσον υπάρχει
- Πιστοποίηση σπουδών
- Συστατικές επιστολές προηγούμενου εργοδότη εφόσον υπάρχει

2.1.6 Διαδικασία τερματισμού

Μια αποτελεσματική διαδικασία τερματισμού είναι απαραίτητη για την αποτροπή των υπαλλήλων, που έχουν φύγει από την εταιρεία να χρησιμοποιούνε την πρόσβαση που είχαν, σε πληροφορίες υλικών περιουσιακών στοιχείων του ομίλου για να προκαλέσουν κάποια βλάβη. Με τον όρο τερματισμό εννοείται ο τερματισμός της πρόσβασης των υπαλλήλων σε πληροφορίες και υλικά περιουσιακά στοιχεία του οργανισμού και θα πρέπει να συμβαίνει κάθε φορά που ένας υπάλληλος σταματήσει να εργάζεται, απολυθεί ή παίρνει άδεια. Μια διαδικασία για τον τερματισμό της πρόσβασης πρέπει να περιλαμβάνει την άμεση αφαίρεση της πρόσβασης στο δίκτυο, απομακρυσμένη πρόσβαση, πρόσβαση στις εγκαταστάσεις καθώς και πρόσβαση σε όλες τις εφαρμογές που χρησιμοποιούνται από τους υπαλλήλους. Όταν ένας εργαζόμενος έχει απολυθεί η διαδικασία τερματισμού θα πρέπει να γίνεται την στιγμή που του ανακοινώνεται η απόλυση του. Παρόλο που οι οργανισμοί ίσως δεν θέλουν να διακόπτουν την πρόσβαση τους μέχρι οι υπάλληλοι να απομακρυνθούνε από την εταιρεία, μια συντονισμένη προσπάθεια από το τμήμα ανθρωπίνων πόρων, τον διευθυντή του εργαζομένου και του τμήματος ασφαλείας του οργανισμού. Όταν ένας υπάλληλος παίρνει μια βραχυπρόθεσμη άδεια θα πρέπει να υπάρχει μια διαδικασία σύντομου τερματισμού. Όπως για παράδειγμα ένα κλείδωμα στον λογαριασμού του συγκεκριμένου υπαλλήλου μειώνει τον κίνδυνο κάποιου περιστατικού όσο ο εργαζόμενος δεν βρίσκεται στην θέση εργασίας του για εκείνο το συγκεκριμένο χρονικό διάστημα.

2.1.7 Αντιμετώπιση επεισοδίου κοινωνικής μηχανικής

Στο ατυχές συμβάν μιας επίθεσης χρειάζεται άμεσα περιορισμός της επίθεσης και συλλογή όσο το δυνατόν περισσότερες και σαφέστερες πληροφορίες σχετικά με την επίθεση. Μια επίθεση που περάσει απαρατήρητη ίσως είναι η αρχή για μια σειρά

επιθέσεων. Το να αναγνωριστεί και να αντιμετωπιστεί μια επίθεση είναι ένας αποτελεσματικός τρόπος για να διασφαλιστεί το σύστημα της επιχείρησης από μελλοντικές επιθέσεις. Για να αντιμετωπιστούν αυτές οι επιθέσεις πριν συμβούν πρέπει να υπάρχει ένα προσχέδιο, τα προσχέδια αυτά διαφέρουν από εταιρία σε εταιρία βάση των πολιτικών που ακολουθούνε. Το πιο εύκολο και γνωστό προσχέδιο απέναντι στις επιθέσεις είναι η πληροφόρηση των υπαλλήλων και η αντίδραση τους σε τέτοιου είδους επιθέσεις. Οπότε σε περίπτωση επίθεσης να ξέρουν τι να κάνουν και ποιόν να ενημερώσουν. Με το να συγκεντρώνουμε σχετικές εκθέσεις σχετικά με περιστατικά επιθέσεων, μια επίθεση που άλλοτε θα περνούσε απαρατήρητη μπορεί να εντοπιστεί και να προληφθεί ο κίνδυνος. Στο γεγονός ότι μπορεί να έχουμε συστηματικές επιθέσεις ενάντια στην επιχείρηση, η καταγραφή τους είναι απαραίτητη για τον εντοπισμό του στόχου του επιτιθέμενου.

2.1.8 Εσωτερική Ασφάλεια

Το να υπάρχουν μέτρα εσωτερικής ασφάλειας μας βοηθάει να ελαχιστοποιήσουμε τον κίνδυνο να εισέλθει στην επιχείρηση ένας κοινωνικός μηχανικός. Υπάρχουν βασικές αρχές που εάν ακολουθηθούν σωστά θα μειώσουν σημαντικά τον κίνδυνο αυτό.

Α) Αναγνώριση όσων δεν εργάζονται στην επιχείρηση:

Τα άτομα που δεν εργάζονται στην επιχείρηση αλλά χρειάζεται να εισέλθουν σε αυτή σε καθημερινή ή εβδομαδιαία βάση. Αυτά τα άτομα είναι υποχρεωμένα να υπογράφουν ειδικά έγγραφα αναγνώρισης καθώς επίσης και την ώρα που εισήλθαν και εξήρθαν από την επιχείρηση. Τέτοια άτομα μπορεί να είναι διάφοροι εργαζόμενοι που εφοδιάζουν τους αυτόματους πωλητές, τα μηχανήματα αυτόματης ανάληψης (ATM) ακόμα και εκείνοι που κάνουν κάποιες παραδόσεις στην επιχείρηση (π.χ.Courier)

Β) Αναγνώριση επισκεπτών:

Οι επισκέπτες θα πρέπει να δείχνουν κάποια ταυτότητα ή το δίπλωμα του αυτοκινήτου τους καθώς επίσης να υπογράφουν, να δηλώνουν την ώρα που εισήλθαν στην εταιρία, ποιον ήρθαν να επισκεφθούν και περίπου τι ώρα σκοπεύουν να φύγουν. Η σύγκριση της υπογραφής της ταυτότητας τους και η αναγνώριση τους από την φωτογραφία της ταυτότητας ή του διπλώματος μπορούν να βοηθήσουν στην

ασφάλεια της εταιρίας καθορίζοντας ότι ο επισκέπτης είναι το άτομο που ισχυρίζεται. Η ταυτότητα ή το δίπλωμα τους θα πρέπει να φωτοτυπείται και να κρατείται για κάποια συγκεκριμένη χρονική περίοδο εντός της εταιρίας οπότε σε περίπτωση που υπάρξει κάποιο περιστατικό αφού ο επισκέπτης έχει αποχωρήσει από την εταιρία να γνωρίζουμε ποίοι εισήλθαν και τον λόγο που εισήλθαν. Επίσης κατά την επίδειξη ταυτότητας ο επισκέπτης θα πρέπει να χορηγείται μια συγκεκριμένη κάρτα που θα του επιτρέπει την πρόσβαση στην εταιρία και είναι υποχρεωμένος να την επιστρέψει κατά την αποχώρηση του

Γ) Συνοδοί επισκεπτών:

Από την στιγμή όπου ο επισκέπτης λάβει την κάρτα που του επιτρέπει την πρόσβαση στην εταιρία δεν σημαίνει ότι μπορεί να περιφέρεται μόνος του μέσα στην εταιρία. Για αυτό τον λόγο ένας συνοδός θα πρέπει να είναι μαζί του κατά την διάρκεια της παραμονής του.

Δ) Προσωρινές κάρτες:

Ακόμα και οι υπάλληλοι που έχουν ξεχάσει ή χάσει την προσωπική τους κάρτα θα πρέπει να τους δοθεί μια προσωρινή κάρτα αφού πρώτα επιβεβαιωθεί η ταυτότητα του. Ο προϊστάμενος του υπαλλήλου θα πρέπει να ενημερωθεί μέσω ενός μηνύματος ηλεκτρονικού ταχυδρομείου (e-mail) ότι έχει χορηγηθεί μια προσωρινή κάρτα ο υφιστάμενος του για όλη την διάρκεια της ημέρας. Στο τέλος της ημέρας όλες οι προσωρινές κάρτες θα πρέπει να επιστρέφονται. Στην περίπτωση που δεν επιστραφούν θα πρέπει η κάρτα να απενεργοποιηθεί από τους εργαζομένους ασφάλειας της εταιρίας.

Ε) Πινακίδες αυτοκινήτων:

Στην περίπτωση που υπάρχει χώρος στάθμευσης οι πινακίδες, η μάρκα και το χρώμα του αυτοκινήτου θα πρέπει να έχουν αναφερθεί από τους υπαλλήλους της εταιρίας καθώς επίσης και το προσωπικό ασφαλείας να κάνει ελέγχους για αυτοκίνητα που δεν έχουν αναφερθεί ως υπαλληλικά ή έστω και ως αυτοκίνητα επισκεπτών.

Ζ) Κάδοι απορριμμάτων:

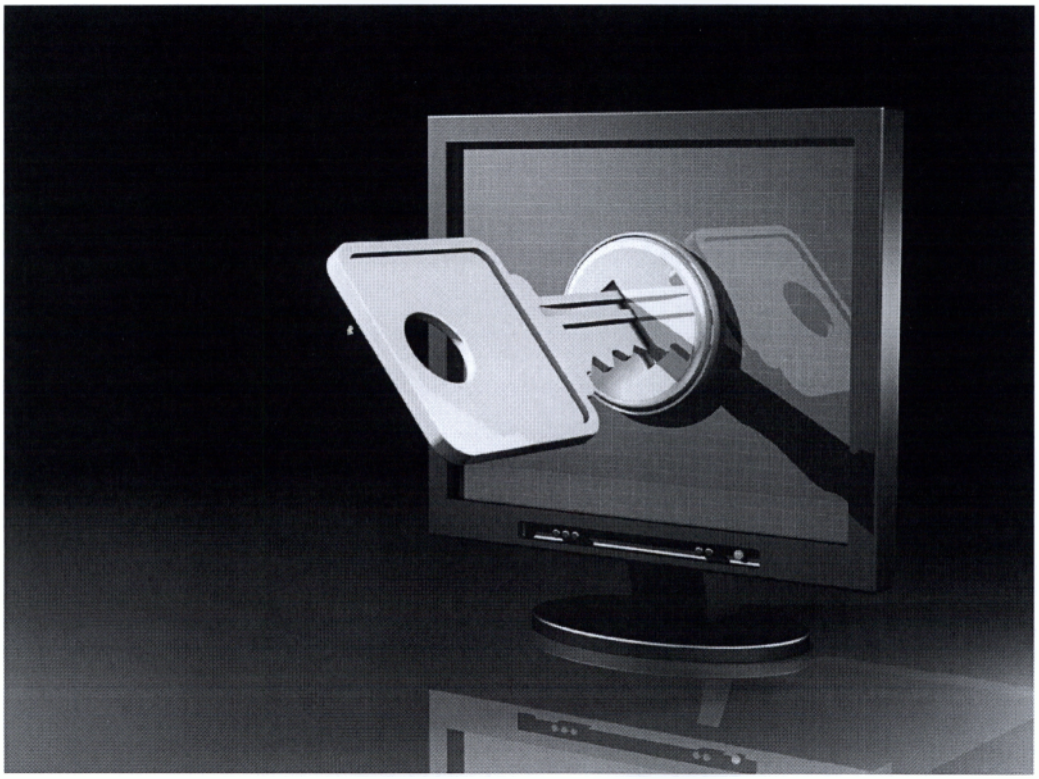
Οι κάδοι απορριμμάτων της εταιρίας δεν θα πρέπει να είναι προσβάσιμη στο ευρύ κοινό. Υπάρχει κίνδυνος διέρρευσες διαφόρων εμπιστευτικών εγγράφων τα οποία ίσως να μη έχουν καταστραφεί όπως πρέπει. Για τον λόγο αυτό ακόμα και οι κάδοι

απορριμμάτων θα πρέπει να φυλάσσονται σε ασφαλή και φυλασσόμενη περιοχή. Το ψάξιμο των κάδων απορριμμάτων είναι σύνηθες φαινόμενο και είναι γνωστό και ως "dumpster diving[2]"

[1] Mitnick, *Η τέχνη της παραπλάνησης* σελ. 324-326

ΚΕΦΑΛΑΙΟ 3

ΕΙΣΑΓΩΓΗ ΣΤΗΝ ΑΣΦΑΛΕΙΑ ΥΠΟΛΟΓΙΣΤΩΝ



Εισαγωγή

Η ασφάλεια υπολογιστών έχει ζωτική σημασία. Αναρωτηθείτε τα εξής σχετικά με την ασφάλεια του σπιτιού σας

- Θα αφήνατε ξεκλείδωτες τις πόρτες του σπιτιού σας ακόμα και όταν δεν βρισκόσασταν εσείς εκεί;
- Αφήνετε προσωπικά έγγραφα και στοιχεία τραπεζικών λογαριασμών σε κοινή θέα;
- Παραμελείτε τις μεγάλες τρύπες και τα κενά στον φράχτη ή τη μάντρα του σπιτιού σας;

Οι περισσότεροι άνθρωποι κλειδώνουν τις πόρτες τους όταν φεύγουν από το σπίτι, τοποθετούν τα προσωπικά τους έγγραφα σε ασφαλές σημείο, διατηρούν τους φράχτες του σε καλά κατάσταση και προσέχουν ποιούς βάζουν στο σπίτι τους. Ίσως φαίνεται υπερβολικό να συγκρίνουμε την ασφάλεια ενός υπολογιστή με την ασφάλεια ενός σπιτιού αλλά οι crackers θα τρίβουν τα χέρια τους όπως και οι διαρρήκτες ενός σπιτιού όταν αποκτήσουν πρόσβαση στα στοιχεία του τραπεζικού λογαριασμού ή ακόμη και της ταυτότητας σας. Οι ειδικοί ανακοινώνουν ότι η υποκλοπή της ταυτότητας είναι η πιο ταχέως αναπτυσσόμενη μορφή εγκλήματος και ο υπολογιστής σας μπορεί να αποτελέσει έναν εύκολα προσβάσιμο στόχο για τους επίδοξους ληστές. Γνωρίζοντας τα θέματα που αφορούν την ασφάλεια ενός υπολογιστή, την εφαρμογή κάποιων ουσιαστικών μέτρων προστασίας και την προσεκτική παρακολούθηση της ασφάλειας του μηχανήματος σας, μπορείτε να εξασφαλίσετε την προστασία του υπολογιστή σας τόσο στο παρόν όσο και στο μέλλον.

3.1 Το κόστος προστασίας του υπολογιστή

Η προστασία του υπολογιστή σας δεν χρειάζεται να είναι ακριβή. Πολλά από τα εργαλεία προστασίας του υπολογιστή που θα αναφέρουμε διατίθενται δωρεάν στον οικιακό χρήστη, με μικρό κόστος στον επαγγελματία, ενώ πολλά εργαλεία υπάρχουν ήδη στα λειτουργικά προγράμματα που χρησιμοποιούμε.

3.2 Ιστορικό ασφαλείας υπολογιστών

Θα πρέπει να προστατεύσετε τον υπολογιστή σας και τα πολύτιμα δεδομένα που περιέχει από τις σύγχρονές απειλές. Ο λόγος της ιστορικής αυτής αναδρομής είναι για να δείξουμε ότι οι αλλαγές που σημειώθηκαν στον τομέα των προσωπικών υπολογιστών μπορούν στην πραγματικότητα να μας διδάξουν πολλά για την ασφάλεια των υπολογιστών, γιατί ο προσωπικός υπολογιστής έχει γίνει καθημερινό εργαλείο πλέον στην ζωή μας αλλά και γιατί το πλήθος των απειλών είναι πολύ μεγαλύτερο.

3.2.1 Οι πρώτοι υπολογιστές

Όταν οι προσωπικοί υπολογιστές μπήκαν στα σπίτια των χρηστών, το κύριο ζήτημα προστασίας του υπολογιστή ήταν η υλική ασφάλεια του ίδιου του μηχανήματος. Αυτό σήμαινε ότι για να αποτρέψει κάποιος μια ανεπιθύμητη πρόσβαση στα αρχεία του, έπρεπε να βεβαιωθεί ότι τα μη εξουσιοδοτημένα άτομα δεν μπορούσαν να χρησιμοποιήσουν τον υπολογιστή. Καθώς τα μόντεμ και τα δίκτυα υπήρχαν σε ελάχιστα σπίτια οπότε και ο κίνδυνος κάποιος εκτός του σπιτιού να μπει στον υπολογιστή σας από μακριά ήταν ανύπαρκτος. Οι ιοί εκείνη την εποχή μεταδίδονταν κυρίως από τις δισκέτες και έτσι έπρεπε να προσέχετε τις δισκέτες τις οποίες εισάγατε στις μονάδες δίσκων.

3.2.2 Windows 3,1

Η σειρά windows 3,1 είδε την εμφάνιση μερικών νέων απειλών λόγω της εισαγωγής βελτιωμένων δυνατοτήτων δικτύωσης. Ξαφνικά, οι απειλές μπορούσαν να έρθουν από κάποιον άλλο υπολογιστή του δικτύου καθώς και από αυτόν που χρησιμοποιούσατε.

3.2.3 Windows 95 και μεταγενέστερες εκδόσεις

Τα Windows 95 διευκόλυναν την πρόσβαση στο διαδίκτυο και μολονότι το διαδίκτυο άλλαξε ριζικά τη διαδικασία αναζήτησης πληροφοριών, υπολογιστές συνδεδεμένοι στο μεγαλύτερο παγκόσμιο δίκτυο μπορούν πιθανώς να αποκτήσουν

πρόσβαση στον προσωπικό μας υπολογιστή. Έκτοτε, η ασφάλεια των υπολογιστών είναι ακόμα πιο σημαντική.

3.3 Απειλές που δέχεται ο υπολογιστής

Ένας από τους καλύτερους τρόπους για να εφαρμόζουμε τα μέτρα ασφαλείας από την ευρεία σειρά απειλών που μπορούν να βλάψουν τον υπολογιστή μας και τα δεδομένα μας είναι να κατανοήσουμε και να αποκωδικοποιήσουμε τους όρους και τα ονόματα που χρησιμοποιούνται για την περιγραφή αυτών των απειλών. Μόλις κατανοήσουμε ποιες απειλές υπάρχουν και τι κάνουν, είναι ευκολότερο να αντιμετωπιστούνε. Τέτοιες απειλές είναι οι ακόλουθες :

Κακόβουλα λογισμικά (Malware)

Ο όρος κακόβουλο λογισμικό είναι ένας γενικός όρος ο οποίος αναφέρεται σε όλους τους τύπους κακόβουλων λογισμικών. Περιλαμβάνει τους ιούς, τα σκουλήκια, τους δούρειους ίππους, τα διαφημιστικά λογισμικά και τα κατασκοπευτικά λογισμικά.

Γκρίζα λογισμικά (Grayware)

Ο όρος γκρίζο λογισμικό είναι ακόμα ένας όρος που αναφέρεται στα κακόβουλα λογισμικά αλλά δεν περιλαμβάνει ιούς. Είναι μια ονομασία που επινοήθηκε για να περιγράψει κακόβουλα λογισμικά που κατατάσσονται στην "γκρίζα" ζώνη μεταξύ ιών και τυπικών προγραμμάτων.

Ιοί (Viruses)

Ο ιός υπολογιστή είναι ένα πρόγραμμα, με συνήθως κακόβουλες προθέσεις, το οποίο μπορεί να αναπαραχθεί και να μολύνει άλλα μηχανήματα, όπως ένας κανονικός ιός που μολύνει ανθρώπους. Οι ιοί περιέχουν συνήθως έναν "εκρηκτικό μηχανισμό" ο οποίος αντιστοιχεί στη δράση που λαμβάνει, όπως η διαγραφή αρχείων ή εμφάνιση ενός μηνύματος σε συγκεκριμένη χρονική στιγμή ή λειτουργία. Οι ιοί χρησιμοποιούν κανονικά αρχεία του υπολογιστή σας και εκτελούνται μέσα από αυτά.

Σκουλήκια (Worms)

Τα σκουλήκια είναι παρόμοια με τους ιούς, αλλά χρησιμοποιούν δίκτυα υπολογιστών προκειμένου να "μολύνουν" άλλα μηχανήματα στέλνοντας αντίγραφα του εαυτού τους. Άλλη μια λειτουργία τους είναι να καθυστερούν τη λειτουργία των δικτύων υπολογιστών και μπορούν να εξαπλωθούν με εξαιρετικά ταχύ ρυθμό. Υπολογίζεται πως το σκουλήκι My Doom[3] (η καταδίκη μου) μόλυνε 400.000 με 500.000 υπολογιστές μέσα σε μία μέρα.

Δούρειοι ίπποι(Trojans)

Οι δούρειοι ίπποι είναι συνήθως επιβλαβή προγράμματα τα οποία μπορεί να κρύβονται μέσα σε μία τυπική εφαρμογή. Μπορούν να "κρυφτούν" μέσα σε υπάρχοντα προγράμματα, ή να μεταμφιεστούν σε χρήσιμες εφαρμογές, όπως δωρεάν προφύλαξη οθόνης και να ενεργοποιηθεί όταν ο χρήστης τρέξει κάποιο πρόγραμμα. Οι δούρειοι ίπποι δίνουν συχνά στους hacker και τους cracker πρόσβαση στον υπολογιστή σας μέσω της δικτυακής δομής του Διαδικτύου.

Κατασκοπευτικά λογισμικά (Spyware)

Τα κατασκοπευτικά λογισμικά εγκαθίστανται χωρίς την συγκατάθεση του χρήστη με σκοπό να συλλέξουν πληροφορίες και να τις στείλουν σε συγκεκριμένη πηγή. Τέτοιου είδους λογισμικά σχεδιάζονται ορισμένες φορές για την ανίχνευση στοιχείων τραπεζικών λογαριασμών τα οποία στέλνουν σε άλλο υπολογιστή. Επίσης χρησιμοποιούνται για την αποστολή πληροφοριών από αναζητήσεις στο Ιστό σε διαφημιστές, οι οποίοι στη συνέχεια στοχεύουν τους χρήστες με αυτόκλητες διαφημίσεις.

Διαφημιστικά λογισμικά (Adware)

Τα διαφημιστικά λογισμικά εγκαθίστανται στον υπολογιστή που αυτόματα εμφανίζει διαφημίσεις στον χρήστη, συχνά υπό την μορφή αναδυόμενων παραθύρων. Ενδέχεται να περιλαμβάνουν επίσης χαρακτηριστικά κατασκοπευτικού λογισμικού

[3] http://news.cnet.com/2100-7349-5149764.html

και να στέλνουν πληροφορίες σε έναν απομακρυσμένο υπολογιστή χωρίς την συγκατάθεση του χρήστη.

Ανεπιθύμητα ηλεκτρονικά μηνύματα ή ενοχλητικά μαζικά μηνύματα

Όπως ακριβώς λαμβάνετε "ανεπιθύμητες" επιστολές στο ταχυδρομικό κουτί του σπιτιού σας, έτσι υπάρχει περίπτωση να λαμβάνετε ανεπιθύμητα μηνύματα στα εισερχόμενα του ηλεκτρονικού σας ταχυδρομείου. Τα ανεπιθύμητα μηνύματα, γνωστά και ως "ενοχλητικά μαζικά μηνύματα", αντιστοιχούν σε ένα μεγάλο ποσοστό μηνυμάτων Διαδίκτυο. Μολονότι είναι φαινομενικά αβλαβή, η διαγραφή τους είναι χρονοβόρα, ενώ μπλοκάρουν και τα εισερχόμενα του ηλεκτρονικού ταχυδρομείο. Στις πιο ακραίες περιπτώσεις, οδηγούν στην κατάρρευση διακομιστών ηλεκτρονικού ταχυδρομείου.

Ηλεκτρονικό ψάρεμα

Το ηλεκτρονικό ψάρεμα είναι μια μέθοδος που χρησιμοποιούν οι διαρρήκτες για να αποκτήσουν πρόσβαση στα προσωπικά δεδομένα ενός ατόμου με δόλο. Αυτές οι απόπειρες έχουν συχνά τη μορφή ηλεκτρονικού μηνύματος. Συνήθως το ηλεκτρονικό ψάρεμα παίρνει τη μορφή ενός τραπεζικού αιτήματος για πληροφορίες λογαριασμού, αλλά μπορεί επίσης να πάρει τη μορφή μηνύματος από κάποια υπηρεσία όπως της EBay ή της PayPal. Οι τεχνικές ηλεκτρονικού ψαρέματος χρησιμοποιούν την κοινωνική μηχανική για να αποσπάσουν προσωπικά δεδομένα από τον κόσμο. Η κοινωνική μηχανική, όπως θα αναφερθούμε και παρακάτω είναι η διαδικασία εξαπάτησης των ανθρώπων ώστε να δώσουν προσωπικές πληροφορίες όπως στοιχεία λογαριασμού ή κωδικούς πρόσβασης.

Κατανεμημένη επίθεση άρνησης υπηρεσίας (DDOS)

Οι κατανεμημένες επιθέσεις άρνησης υπηρεσίας, στοχεύουν στον αποκλεισμό της επικοινωνίας μεταξύ πόρων υπολογιστών και των χρηστών τους. Αποτελούν συνήθως απόπειρες παρακώλυσης διακομιστών Ιστού ώστε να μην εμφανίζουν ιστοσελίδες στους επισκέπτες. Οι κατανεμημένες επιθέσεις άρνησης υπηρεσίας χρησιμοποιούν μεγάλο αριθμό υπολογιστών που εξαπολύουν συντονισμένες

επιθέσεις. Ο υπολογιστής σας θα μπορούσε να χρησιμοποιηθεί για μία τέτοια επίθεση χωρίς να το γνωρίζετε.

Υπολογιστές Ζόμπι

Ο υπολογιστής Ζόμπι είναι ένας υπολογιστής ο οποίος βρίσκεται υπό τον έλεγχο κάποιου ατόμου ή κάποιου κακόβουλου προγράμματος και στην συνέχεια να χρησιμοποιηθεί για μια κατανεμημένη επίθεση άρνησης υπηρεσίας, ή για διάφορες άλλες επιθέσεις ανάλογα για αυτό που επιδιώκει ο χρήστης του.

Rootkit

Τα rootkit επιχειρούν να μεταμφιέσουν διαδικασίες από τον χρήστη και τα ίδια τα Windows, καλύπτοντας πιθανώς την ύπαρξη κακόβουλου λογισμικού.

Crackers (Criminal hackers)

Θεωρούνται ως οι κακόβουλοι hackers και έχουν ως στόχο την πρόκληση ζημιάς σε δίκτυα υπολογιστών, την εισβολή σε υπολογιστές χρηστών χωρίς εξουσιοδότηση, την δημιουργία ιών, την παραβίαση κωδικών ασφαλείας, την καταστροφή ή και την αλλοίωση δικτυακών τόπων (Web sites) όπου αφήνουν περήφανα την δικτυακή τους σφραγίδα με το ψευδώνυμό τους, την δημιουργία πειρατικών αντιγράφων προγραμμάτων ή τραγουδιών ή και βίντεο κ.ά. Με απλά λόγια, πρόκειται για hackers οι οποίοι προβαίνουν σε πράξεις που παραβιάζουν διατάξεις του κοινού ποινικού κώδικα. Συνήθως πρόκειται για άτομα με έντονη ανάγκη για επίδειξη, οι οποίοι διεισδύουν σε συστήματα και προκαλούν ζημιές. Οι κυριότερες διαφορές τους από τους hackers είναι ότι δεν έχουν ιδιαίτερες γνώσεις για την πληροφορική και τον προγραμματισμό καθώς και το ότι δεν διέπονται από κανενός είδους ηθική αρχή. Για τους λόγους αυτούς μπορούν πολύ εύκολα να καταστρέψουν ολόκληρα συστήματα υπολογιστών απλά και μόνο για να κάνουν το κέφι τους, όταν βρουν βέβαια την κατάλληλη ευκαιρία. Το hacking είναι ποινικό αδίκημα σε πολλές χώρες καθώς η κοινωνία μας εξαρτάται όλο και περισσότερο από τους υπολογιστές και το Internet και πιο συγκεκριμένα τιμωρείται όποιος αποκτήσει χωρίς εξουσιοδότηση πρόσβαση σε συστήματα πληροφοριών, προκαλέσει ζημιά,

αποκομίσει από τις ενέργειές του οικονομικό όφελος ή αποδειχθεί ότι είναι μέλος ενός δικτύου οργανωμένου εγκλήματος.

ΚΕΦΑΛΑΙΟ 4

Η ΑΠΕΙΛΗ ΤΩΝ ΙΩΝ ΚΑΙ ΑΣΦΑΛΕΙΑ ΕΝΑΝΤΙΑ ΤΟΥΣ

Εισαγωγή

Παλαιότερα η αποθήκευση δεδομένων σε μια επιχείρηση γινόταν σε κλειδωμένα συρτάρια με αρχεία σε διαφορετικά τμήματα. Σήμερα ένα μεγάλο μέρος πληροφοριών αποθηκεύεται ηλεκτρονικά, ενώ ταυτόχρονα υπάρχει κάποιο σύστημα διαχείρισης πληροφορικής για την προστασία αυτών των δεδομένων, το οποίο αποτελεί πλέον εργασία πλήρους απασχόλησης.

Σε μια επιχείρηση λοιπόν δεν επιτρέπεται σε όλους να έχουν πρόσβαση σε όλες τις πληροφορίες της εταιρείας, ανεξάρτητα από τη σπουδαιότητά τους. Το τμήμα μάρκετινγκ δεν μπορεί να δει τις μισθοδοσίες όλων των υπαλλήλων και η ομάδα πωλήσεων δεν μπορεί να συνδεθεί και να χρησιμοποιήσει όλα τα δεδομένα του τμήματος πληροφορικής, για παράδειγμα.

4.1 Στρατηγικές λογαριασμού χρήστη

Στην στρατηγική ασφάλειας του χρήστη, θα πρέπει να συμπεριλαμβάνονται τα ακόλουθα στοιχεία:

- Αποφυγή μοιράσματος του κωδικού πρόσβασης λογαριασμού διαχειριστή
- Ο κωδικός πρόσβασης λογαριασμού διαχειριστή να ικανοποιεί τις απαιτήσεις ισχύος του κωδικού πρόσβασης
- Αποφυγή σύνδεσης στον λογαριασμό του διαχειριστή για εκτέλεση τυπικών εργασιών: δημιουργία ενός ξεχωριστού λογαριασμού τυπικού χρήστη για προσωπική χρήση
- Δημιουργία ενός ξεχωριστού λογαριασμού για κάθε χρήστη του μηχανήματος
- Απενεργοποίηση του λογαριασμού «επισκέπτης» (guest)
- Ενημέρωση των υπόλοιπων χρηστών για όλα όσα πρέπει και δεν πρέπει να αποθηκεύονται στον «δημόσιο φάκελο».
- Προστασία αρχείων στα οποία μπορούν οι άλλοι να έχουν πρόσβαση αλλά απαγορεύεται να τροποποιήσουν.

4.2 Τι είναι οι Ιοί;

Η πιο διαβόητη απειλή για την ασφάλεια των υπολογιστών είναι αναμφισβήτητα οι ιοί. Οι περισσότεροι ιοί είναι γραμμένοι με κακόβουλο λογισμικό το οποίο αλλάζει με τα χρόνια.

4.2.2 Ιοί – Μια βιολογική σύγκριση

Όταν το ανθρώπινο σώμα κολλάει κάποιον ιό, αυτός ξεκινάει να πολλαπλασιάζεται και να εξαπλώνεται σε όλο το σύστημά του ατόμου και έχει τη δυνατότητα να εξαπλωθεί και σε άλλα άτομα. Η διαδικασία αυτή θα έχει σίγουρα κάποιες

Δυσάρεστες παρενέργειες. Ο ιός υπολογιστή έχει σχεδόν ταυτόσημα χαρακτηριστικά από τεχνολογικής άποψης:

- Αναπαράγεται
- Προσπαθεί να εξαπλωθεί σε άλλα συστήματα
- Μπορεί να περιέχει ένα «εκρηκτικό μηχανισμό» ο οποίος έχει ανεπιθύμητο αποτέλεσμα στο μηχάνημα του θύματος.

4.2.3 Ορολογία ιών

Ο όρος «ιός» χρησιμοποιείται συχνά ως ορισμός που καλύπτει τα περισσότερα κακόβουλα προγράμματα και όσον αφορά την καταπολέμηση απειλών, αυτή είναι μια χρήσιμη προσέγγιση. Υπάρχουν τρία βασικά είδη απειλών που διαφέρουν μεταξύ τους:

- Ιοί (viruses). Ένας πραγματικός ιός πρέπει να μπορεί να αναπαράγεται και να εκτελείται μόνος του.
- Σκουλήκια (worms). Τα σκουλήκια χρησιμοποιούν δίκτυα υπολογιστών για να εξαπλωθούν, συνήθως μέσω συστημάτων ηλεκτρονικού ταχυδρομείου και επίσης αναπαράγονται.
- Δούρειοι ίπποι (Trojan horses). Ένας δούρειος ίππος σε κάποιον υπολογιστή μεταμφιέζεται σε ένα τυπικό πρόγραμμα άλλα όταν εκτελείται έχει κακόβουλους σκοπούς.

4.2.4 Ιστορία των ιών

Πολλοί πιστεύουν πως ο ιός "Brain[4]" ήταν ο πρώτος πραγματικός ιός επειδή ήταν ο πρώτος που μόλυνε τον προσωπικό υπολογιστή της IBM, ο οποίος είναι σήμερα γνωστός απλά ως προσωπικός υπολογιστής. Στην αρχική του μορφή, μόλυνε δισκέτες και κατέστρεφε το περιεχόμενο τους. Μεταγενέστερες εκδόσεις του ιού "Brain" μόλυναν και σκληρούς δίσκους προκαλώντας απώλειες δεδομένων, ένα σαφώς σοβαρό πρόβλημα για τα θύματα του.

4.2.5 Τρόποι μόλυνσης

Την εποχή των πρώτων ιών τα δίκτυα δεν ήταν τόσο διαδεδομένα και η πρόσβαση στο διαδίκτυο ήταν χαμηλή, έτσι οι προγραμματιστές ιών βασίζονταν στην εξάρτηση των χρηστών από δισκέτες για την ανταλλαγή δεδομένων. Σήμερα ο κόσμος είναι συνδεδεμένος τόσο μέσω εταιρικών δικτύων όσο και μέσω ενός τεράστιου πλήθους υπολογιστών στο διαδίκτυο. Το γεγονός αυτό διαγράφει ένα σαφή δρόμο για τους προγραμματιστές ιών. Πολλές από τις μεγαλύτερες απειλές για την

[4] http://www.spamlaws.com/history.html

ασφάλεια υπολογιστών έχουν τη μορφή σκουληκιών, κάτι αναμενόμενο, καθώς τα σκουλήκια χρησιμοποιούν δίκτυα υπολογιστών για να εξαπλωθούν.

4.2.6 Κακόβουλες προθέσεις

Οι πρώτοι ιοί προσπαθούσαν συνήθως να προκαλέσουν κάποια βλάβη στο λειτουργικό σύστημα ή τα δεδομένα του μηχανήματος και επεδείκνυαν την τεχνική ικανότητα του προγραμματιστή τους. Οι σύγχρονοι ιοί (όπως και τα σκουλήκια και οι δούρειοι ίπποι) είναι πιθανό να παραμείνουν κρυφοί και συχνά χρησιμοποιούνται για εγκληματικούς σκοπούς, είτε πρόκειται για κλοπή ταυτότητας ή για σοβαρή αναστάτωση με τη μορφή κατανεμημένων επιθέσεων άρνησης υπηρεσίας. Η λύση στο πρόβλημα αυτό ανιχνεύεται στην εγκατάσταση ενός προγράμματος που προσφέρει προστασία του υπολογιστή από όλων των ειδών απειλών.

4.3 Έλεγχος τους υπολογιστή για ιούς. Υπάρχει μόλυνση;

Ακόμα και με ισχυρή προστασία από ιούς, σε κάποιες περιπτώσεις οι ιοί καταφέρνουν να υπερνικούν τα εμπόδια και μολύνουν τα μηχανήματα, ειδικά όταν οι ορισμοί ιών δεν έχουν ενημερωθεί. Υπάρχουν διάφορες ενδείξεις που υποδηλώνουν ότι ένας υπολογιστής έχει πιθανώς μολυνθεί. Στην περίπτωση αυτή πρέπει να ενημερωθούν οι ορισμοί ιών και να εκτελεσθεί ένας πλήρης έλεγχος συστήματος.

4.3.1 Ένδειξης μόλυνσης

Η ύπαρξη ιών μπορεί να επιφέρει περίεργες αλλαγές στην απόδοση του υπολογιστή ή να μην παρουσιάσει καμιά αξιόλογη μεταβολή.

Πιο συγκεκριμένα:

- Προβλήματα απόδοσης. Οι ιοί εκτελούν διαδικασίες στον υπολογιστή και επιβραδύνουν την απόδοσή του. Πολλοί ιοί δεν είναι κωδικοποιημένοι σωστά και έτσι επηρεάζουν πολύ την απόδοση του υπολογιστή.
- Αναγκαστική επανεκκίνηση.
- Αλλαγές στην εμφάνιση. Η εμφάνιση του συστήματος μπορεί να αλλάξει με κάποιο τρόπο, όπως μείωση της ποιότητας προβολής ή των χρωμάτων.

- Το λογισμικό προστασίας από ιούς είναι κλειστό. Ορισμένοι ιοί προσπαθούν να κλείσουν τα προγράμματα προστασίας έτσι ώστε ο χρήστης να μην ειδοποιηθεί για την ύπαρξη κακόβουλου προγράμματος.
- Αλλαγή ή διαγραφή αρχείων. Οι ιοί πρέπει να κάνουν τροποποιήσεις στο σύστημα του υπολογιστή για να λειτουργήσουν, επομένως κάπου θα πρέπει να γίνεται κάποιων αρχείων. Είναι συνήθως προγραμματισμένοι να το κάνουν κρυφά, αλλά επειδή κάποιοι είναι εκρηκτικοί μηχανισμοί ιών διαγράφουν αρχεία.
- Προβλήματα σε εφαρμογές. Οι ιοί μακροεντολών χρησιμοποιούν την ισχύ των μακροεντολών για να εκτελέσουν τον κακόβουλο κώδικά τους.

4.3.2 Πρόληψη από ιούς

Ακόμα και στην περίπτωση προστασίας ενός υπολογιστή από κάποιο λογισμικό και παρακολούθησης για εμφανείς ενδείξεις μόλυνσης από ιό, υπάρχει η δυνατότητα πιθανής μόλυνσης.

Κανόνες ελαχιστοποίησης κινδύνου μόλυνσης από ιούς:

- Αποφυγή λήψης οποιουδήποτε αρχείου από το διαδίκτυο
- Εκτέλεση σχολαστικού ελέγχου των αφαιρούμενων μέσων αποθήκευσης, όπως φήμες φλας USB, δισκέτες και CD-ROM.
- Να αποφεύγεται το άνοιγμα συνημμένων αρχείων τα οποία προέρχονται από αγνώστους αποστολείς.
- Αποφυγή χρήσης υπηρεσιών μερισμού αρχείων μεταξύ ομότιμων, οι οποίες διευκολύνουν την εύκολη μετάδοση μολυσμένων αρχείων.
- Προσοχή στα προγράμματα ανταλλαγής άμεσων μηνυμάτων, καθώς συχνά περιλαμβάνουν λειτουργία μερισμού αρχείων.

Τέλος, είναι πολύ σημαντικό τα προγράμματα κατά των ιών να είναι πάντα ενημερωμένα. Συνεχώς εμφανίζονται καινούριοι ιοί και επειδή εκτιμάται ότι έχουν δημιουργηθεί περισσότεροι από 70.000 στην ιστορία των υπολογιστών, η ενημέρωση συνιστά απαραίτητη προϋπόθεση για την προστασία του μηχανήματος σας.

ΚΕΦΑΛΑΙΟ 5

ΑΣΦΑΛΕΙΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Εισαγωγή

Όπως είδαμε και στο πρώτο κεφάλαιο, οι σύγχρονοι υπολογιστές πρέπει να προστατεύονται από πληθώρα απειλών. Η κατάσταση έχει εξελιχθεί λόγω των δυναμικών του σύγχρονου υπολογιστή. Ο υπολογιστής σας είναι πιθανό να ανήκει σε κάποιο είδος δικτύου, συμπεριλαμβανόμενου του μεγαλύτερου δικτύου υπολογιστών στον κόσμο, το γνωστό σε όλους μας διαδίκτυο (Ιντερνέτ), το οποίο εμπεριέχει απειλές όπως :

- Ιούς
- Κατασκοπευτικά και διαφημιστικά λογισμικά
- Άλλου είδους κακόβουλων λογισμικών, όπως τα rootkit, τα προγράμματα καταγραφής πληκτρολόγησης(keystroke loggers) και παραπλανητικά προγράμματα κλήσεων (rogue dialers)
- Cracker

5.1 Επιπτώσεις της σύνδεσης στο Διαδίκτυο

Η Δυναμική των υπολογιστών έχει επίσης αλλάξει. Στα χρόνια που πέρασαν, η κύρια μέθοδος σύνδεσης στο Διαδίκτυο ήταν η ανάλογη τηλεφωνική γραμμή με μόντεμ 56k(η χαμηλότερη). Μολονότι η απόδοση δεν είχε καμία σχέση με τις σύγχρονες πολύ ανώτερες ευρυζωνικές συνδέσεις, από πλευράς ασφαλείας είχε ορισμένα οφέλη.

- Οι χρήστες έκαναν την τηλεφωνική σύνδεση, επισκέπτονταν το Διαδίκτυο και μετά αποσυνδέονταν. Οι ευκαιρείς επομένως που είχαν οι cracker, οι ιοί και οι άλλες απειλές να διεισδύσουν στον υπολογιστή ήταν πολύ λιγότερες.
- Η χαμηλότερη ταχύτητα σύνδεσης σήμαινε πως οι απειλές χρησιμοποιούσαν μικρότερο εύρος ζώνης προκειμένου να εκπληρώσουν τις κακόβουλες προθέσεις τους.

Οι περισσότεροι άνθρωποι έχουν σήμερα ευρυζωνικές συνδέσεις οι οποίες είναι πάντα ανοιχτές και αυτό σημαίνει ότι θα πρέπει να είναι πολύ προσεκτικοί όταν ασφαλίζουν τους υπολογιστές τους.

5.2 Windows Defender

Απαντώντας στην ταχέως αναπτυσσόμενη απειλή των κατασκοπευτικών λογισμικών και με κίνητρο τη δημιουργία ενός ανθεκτικού και ασφαλούς λειτουργικού συστήματος, η Microsoft μετέτρεψε την προστασία από τα κατασκοπευτικά λογισμικά σε ένα κομμάτι του λειτουργικού συστήματος των Windows.

Το Windows Defender, με την εύστοχη ονομασία, διαθέτει τρεις μεθόδους προστασίας του υπολογιστή σας από τα αδιάκριτα μάτια των κατασκοπευτικών λογισμικών.

5.2.1 Άμυνα σε πραγματικό χρόνο

Το Windows Defender εκτελείται σε πραγματικό χρόνο. Αυτό σημαίνει ότι παρακολουθεί συνεχώς τι προσπαθεί να εκτελέσει ο υπολογιστής σας και σας προειδοποιεί όταν πιθανώς κακόβουλα προγράμματα προσπαθούν να κάνουν εγκατάσταση.

5.2.2 Έλεγχοι

Το Windows Defender εκτελεί και παραδοσιακούς ελέγχους. Η λειτουργία αυτή μπορεί να συγκριθεί με την πραγματοποίηση σάρωσης για ιούς στον υπολογιστή σας, με την διαφορά ότι κάνει έλεγχο για κατασκοπευτικά λογισμικά. Από προεπιλογή, το Windows Defender προγραμματίζει τον ημερήσιο έλεγχο στις 02:00 αυτόματα. Σας προτείνουμε να μην αλλάξετε την προεπιλογή αυτή για να έχετε μέγιστη προστασία από κακόβουλα λογισμικά που ενδέχεται να πέρασαν από την προστασία σε πραγματικό χρόνο.

5.3 Microsoft SpyNet

Οι κοινότητες του Διαδικτύου είναι ένας εξαιρετικός τρόπος διανομής πληροφοριών προς όφελος όλων των ενδιαφερομένων. Η κοινότητα SpyNet παρέχει πληροφορίες για όσα άλλοι χρήστες επέτρεψαν να εκτελεστούν στους υπολογιστές τους και προσφέρει βαθμολογίες αξιολόγησης της κοινότητας που σας βοηθάνε να κάνετε σωστές κρίσεις και επιλογές.

5.4 AdAware

Ένα από τα πρώτα πακέτα προστασίας από κατασκοπευτικά λογισμικά με τεράστιο πλήθος χρηστών παγκοσμίως, το AdAware της Lavasoft αποτελεί ένα καλό διεκδικητή για την επιλογή προγράμματος προστασίας. Είναι δωρεάν για ιδιωτική χρήση αλλά όπως και τα περισσότερα προγράμματα ιδιωτικής προστασίας δεν περιλαμβάνει πολλές από τις πλήρης λειτουργίες τους. Για αυτό τον λόγο επιτρέπετε η αναβάθμιση αγοράζοντας την πλήρης έκδοσης τους.

5.5 Spybot Search & Destroy

Το Spybot Search & Destroy είναι άλλη μία καλή εναλλακτική λύση. Μολονότι δεν προσφέρει επιλογή προστασίας σε πραγματικό χρόνο, αξίζει να κάνετε περιοδική σάρωση με το πρόγραμμα αυτό στον υπολογιστή σας προληπτικά για να εντοπίσετε τυχόν απειλές.

5.6 Συμβουλές περιήγησης στο Διαδίκτυο

Με την χρήση του διαδικτύου ένας χρήστης μπορεί να θέσει τον υπολογιστή σας σε κίνδυνο και αυτό το φαινόμενο είναι σε έξαρση. Ενώ στο Διαδίκτυο οι χρήστες είναι ευάλωτοι σε επιθέσεις από κατασκοπευτικά και διαφημιστικά λογισμικά, σκουλήκια, δούρειους ίππους, επιθέσεις ηλεκτρονικού ψαρέματος και υποκλοπής δεδομένων. Σας παραθέτουμε μερικές συμβουλές περιήγησης στο Διαδίκτυο για να παραμένετε ασφαλείς :

- Αποφεύγετε το πάτημα συνδέσεων σε ιστοσελίδες που προσφέρουν μεγάλες αμοιβές και μη ρεαλιστικές προσφορές. Εάν κάτι φαίνεται πολύ καλό για να είναι αληθινό, τότε μάλλον έτσι είναι.

- Μην κάνετε λήψεις και μην χρησιμοποιείτε εφαρμογές μερισμού αρχείων μεταξύ ομότιμων, οι οποίες μερικές φορές αποκαλούνται και εφαρμογές "P2P" Αυτά τα πακέτα μπορούν να αυξήσουν τις πιθανότητες λήψης επικίνδυνων αρχείων, εκθέτουν τον υπολογιστή σε crackers και κακόβουλα προγράμματα και συχνά σας εμπλέκουν σε παράνομο μερισμό αρχείων.

- Αποφεύγετε τις τοποθεσίες Ιστού με ύποπτο περιεχόμενο.

- Όταν κάνετε αγορές μέσω Διαδικτύου ή χρησιμοποιείτε ηλεκτρονικές τραπεζικές συναλλαγές, ελέγξτε την αναφορά ασφαλείας πριν εισαγάγετε προσωπικά στοιχεία και κωδικούς πρόσβασης. Δεξιά από την γραμμή διευθύνσεων υπάρχει ένα εικονίδιο με σχήμα λουκέτο εάν το πατήσετε θα σας προβάλει το πιστοποιητικό για να ελέγξετε την πιστοποίηση της τοποθεσίας.

- Να προσέχετε ιδιαίτερα όταν κατεβάζετε αρχεία. Να βεβαιωθείτε ότι εμπιστεύεστε την εκάστοτε τοποθεσία όταν κατεβάζετε αρχεία με κατάληξη .exe , .bat , .zip, . bas, .bat, .cmd, .com, .js, jse, .lnk, .msi, . pif, .reg, .scr, .vb, .vbe, . vbs, .wsc και .wsf. Όλοι αυτοί οι τύποι αρχείων μπορούν να χρησιμοποιηθούν από κακόβουλες πηγές, για αυτό εάν αμφιβάλλετε μην κάνετε λήψη και μην εκτελείτε αυτά τα αρχεία.

- Να είστε εξαιρετικά προσεκτικοί όταν χρησιμοποιείτε αίθουσες συνομιλίας (chat rooms) και φόρουμ του Διαδικτύου. Ποτέ μην δίνεται προσωπικές πληροφορίες ακόμα και όταν φαίνεται ακίνδυνο. Είναι πολύ σημαντικό να δώσετε τις συμβουλές αυτές και στα παιδία που συχνά δεν γνωρίζουν τους κινδύνους.

5.7 Ηλεκτρονικές τραπεζικές συναλλαγές

Δεν είναι υπερβολή να πούμε ότι το Διαδίκτυο και ο Παγκόσμιος ιστός έχουν μεταμορφώσει τη ζωή μας και το τρόπο που εκτελούμε κάποιες εργασίες. Ένα από τα μεγαλύτερα οφέλη αυτής της μεταμόρφωσης είναι η δυνατότητα να κάνουμε τραπεζικές συναλλαγές και διαχείριση από την άνεση του σπιτιού μας.

Είναι, λοιπόν, αναμενόμενο ότι οι ηλεκτρονικές τραπεζικές συναλλαγές αποτελούν έναν από τους βασικότερους στόχους για τους cracker και τον τομέα τον οποίο θα πρέπει να προσέχετε ιδιαίτερα όταν εργάζεστε στο Διαδίκτυο. Με λίγα λόγια οι τραπεζικές σας συναλλαγές είναι η καθημερινή δουλειά για τους crackers και την πλειοψηφία των κοινωνικών μηχανικών.

5.8 Φίλτρο των Windows κατά του ηλεκτρονικού ψαρέματος (phising)

Οι επιθέσεις ηλεκτρονικού ψαρέματος στο Διαδίκτυο γίνονται πολλές φορές συνεργατικά με σκοπό να "ψαρέψουν" διευθύνσεις ηλεκτρονικού ταχυδρομείου. Η μέθοδος που εφαρμόζει ο κακόβουλος χρήστης όταν προσπαθεί να υποκλέψει τραπεζικά στοιχεία ακολουθεί έναν γενικό κανόνα:

- Ο κακόβουλος χρήστης στέλνει πληθώρα διερευνητικών ηλεκτρονικών μηνυμάτων σε μια τεράστια βάση διευθύνσεων ηλεκτρονικού ταχυδρομείου.

- Πολλοί παραλήπτες διαγράφουν ή αγνοούν το ηλεκτρονικό μήνυμα επειδή δεν συνεργάζονται με την τράπεζα την οποία υποτίθεται πως εκπροσωπεί ο κακόβουλος χρήστης.

- Από τους χρήστες που συνεργάζονται με την επιλεγμένη τράπεζα, πολλοί καταλαβαίνουν ότι το μήνυμα είναι ψεύτικο και το διαγράφουν, το αγνοούν ή φιλτράρεται από το λογισμικό ασφαλείας τους.

- Εάν ο κακόβουλος χρήστης έχει επιτυχία, ορισμένα άτομα θα δεχτούν το μήνυμα ως γνήσιο και θα ακολουθήσουν τον ψεύτικο σύνδεσμο στην τοποθεσία Ιστού του κακόβουλου χρήστη ο οποίος έχει σχεδιαστεί για να αποτυπώνει τα στοιχεία τραπεζικών λογαριασμών των χρηστών.

Μολονότι δεν υπάρχει υποκατάστατο στην επαγρύπνηση και την προσοχή, το φίλτρο κατά του ηλεκτρονικού ψαρέματος των Windows σας βοηθάει να αντιμετωπίσετε τις επίθεσης ηλεκτρονικού ψαρέματος στον υπολογιστή σας.

5.9 Εκκαθάριση του ιστορικού σας

Επιστρέφοντας στη σύγκριση της ασφάλειας του υπολογιστή σας με την ασφάλεια του σπιτιού σας, ποιό θα ήταν το επιπλέον όφελος για έναν ληστή εάν του αφήνατε μερικά ακούσια "στοιχεία" με την μορφή εγγράφων, επιστολών και άλλων αντικειμένων;

Προφανώς το όφελος θα ήταν σημαντικά μεγαλύτερο. Όταν δεν κάνετε εκκαθάριση του ιστορικού των περιηγήσεων σας παρέχετε τα ίδια οφέλη σε

οποιονδήποτε "εικονικό" εισβολέα στον υπολογιστή σας. Εάν κατάφερε να συνδεθεί στον υπολογιστή σας με τον λογαριασμό χρήστη και είδε ότι επισκεφτήκατε για παράδειγμα την υπηρεσία τραπεζικών συναλλαγών της τράπεζας σας, τότε έχει κάνει μια καλή αρχή για να μπει στον λογαριασμό σας.

Έχοντας αυτό το παράδειγμα κατά νου, είναι καλό να κάνετε συχνή εκκαθάριση του ιστορικού των τοποθεσιών που επισκεφτήκατε με το Internet Explorer και των προσωρινών αρχείων Internet τα οποία αποθηκεύτηκαν στον υπολογιστή σας.

5.10 Παραπλανητικά προγράμματα κλήσεων

Εάν γνωρίζετε κάποιον που έχει πέσει θύμα ενός παραπλανητικού προγράμματος κλήσεων, ή ακόμα χειρότερα, εάν έχετε πέσει εσείς θύμα θα είστε διατεθειμένοι να κάνετε ότι μπορείτε για να εμποδίσετε την εγκατάσταση αυτού του κακόβουλου λογισμικού στον υπολογιστή σας.

5.10.1 Τι είναι το πρόγραμμα κλήσεων;

Μολονότι τα προγράμματα κλήσεων έχουν νόμιμους σκοπούς, όπως η διευκόλυνση της σύνδεσης του μόντεμ στην υπηρεσία παροχής Διαδικτύου, τα παραπλανητικά προγράμματα κλήσεων εκμεταλλεύονται τα χαρακτηριστικά των προγραμμάτων αυτών για να ξεγελάσουν τους χρήστες που πατούν ένα κουμπί και καλούν ένα συγκεκριμένο αριθμό τηλεφώνου συνήθως υψηλής χρέωσης. Ενδέχεται επίσης να εγκατασταθούν μόνα τους χωρίς να το γνωρίζετε ή να εγκατασταθούν ανεξάρτητα από το αν συμφωνείτε ή διαφωνείτε με την εγκατάσταση τους.

5.10.2 Χρησιμοποιείτε σύνδεση ευρείας ζώνης

Τα παραπλανητικά προγράμματα κλήσεων είναι προϊόν της εποχής που το μόντεμ της σύνδεσης μέσω τηλεφώνου ήταν η κυρίαρχη μορφή σύνδεσης στο Διαδίκτυο. Οι ευρυζωνικές συνδέσεις έχουν συνήθως "ανοσία" σε αυτή μορφή κακόβουλου λογισμικού, εάν λοιπόν ψάχνετε έναν καλό λόγο για να αναβαθμίσετε τη σύνδεσή σας και υπάρχει υπηρεσία σύνδεσης ευρείας ζώνης στην περιοχή σας, αξίζει να προσθέσετε αυτόν το λόγο στη λίστα σας.

5.10.3 Ενημερώνετε το πρόγραμμα προστασίας από κατασκοπευτικά λογισμικά

Όπως ακριβώς πρέπει να ενημερώνουμε τα anti-virus προγράμματα, έτσι είναι απαραίτητο να ενημερώνουμε και τα προγράμματα κατασκοπευτικών λογισμικών. Μολονότι τα παραπλανητικά προγράμματα είναι λιγότερο διαδεδομένα πλέον, δεν υπάρχει εγγύηση ότι δεν θα κυκλοφορήσει κάποιο νέο για υπολογιστές σαν το δικό σας. Συνήθως τέτοιου είδους προγράμματα έχουν αυτόματες ενημερώσεις όπως και τα anti-virus αλλά πότε δεν είναι κακό κοιτάμε και εμείς για ενημερώσεις.

5.10.4 Κοινή λογική

Ίσως το πιο ισχυρό εργαλείο στην εργαλειοθήκη της ασφάλειας σας, όπως και στην ασφάλεια του υπολογιστή σας, είναι η κοινή λογική. Μην αποδέχεστε ύποπτες προσφορές για "δωρεάν" περιεχόμενο για ενήλικες και προσέξτε την προειδοποίηση των Windows για μη αναμενόμενες εγκαταστάσεις λογισμικών, βεβαιωθείτε ότι το μόντεμ σας είναι αποσυνδεδεμένο ή κλειστό όταν δεν χρησιμοποιείτε το Διαδίκτυο και κοιτάτε αν πραγματοποιεί κλήσεις όταν δεν το έχετε ζητήσει.

5.10.5 Αφαίρεση

Εάν μολυνθήκατε και το λογισμικό προστασίας από κατασκοπευτικά λογισμικά δεν αφαιρεί το πρόγραμμα κλήσεων, κάντε μια αναζήτηση στην ιστοσελίδα του επιλεγμένου σας λογισμικού για οδηγίες αφαίρεσης χειροκίνητα και ακολουθήστε τις με προσοχή.

5.10.6 Απενεργοποίηση της αυτόματης καταχώρισης

Η λειτουργία αυτόματης καταχώρισης του προγράμματος πλοήγησης σας εξυπηρετεί γιατί μπορεί να "θυμάται" τοποθεσίες Ιστού, δεδομένα που συμπληρώσατε σε φόρμες, ονόματα χρηστών ακόμα και κωδικούς πρόσβασης.

Μολονότι είναι χρήσιμη και σας εξοικονομεί χρόνο, δεν είναι πάντα επιθυμητή. Εάν κάποιος μη εξουσιοδοτημένος χρήστης εισβάλει στον υπολογιστή σας και συνδεθεί με τα στοιχεία σας, θα μπορεί να δει τις τοποθεσίες που επισκεφτήκατε και να χρησιμοποιήσει τα αποθηκευμένα ονόματα χρηστών και

κωδικούς πρόσβασης. Επομένως, συστήνεται να μη επιτρέπετε στο πρόγραμμα πλοήγησης στο Διαδίκτυο να θυμάται κανένα από αυτά τα στοιχεία.

5.10.7 Απενεργοποίηση πρόσθετων προγραμμάτων

Τα περισσότερα προγράμματα πλοήγησης υποστηρίζουν την χρήση πρόσθετων προγραμμάτων. Τα πρόσθετα είναι μικρά προγράμματα τα οποία συνεργάζονται με τον πλοηγό σας για την παροχή επιπλέον λειτουργιών και βελτιώσεων.

Ένα δημοφιλές παράδειγμα πρόσθετου είναι το Adobe Flash. Πρόσθετα όπως το Flash παρέχουν ορισμένες πολύ χρήσιμες και συναρπαστικές δυνατότητες και λειτουργίες για την περιήγησή σας στον Ιστό.

Ωστόσο, μερικά πρόσθετα αξιοποιούνται για την παραβίαση της ασφάλειας του συστήματος ενώ άλλα πρόσθετα είναι σχεδιασμένα ειδικά, από κακόβουλα στοιχεία, για να ανοίγουν "πίσω πόρτες" και ευπάθειες σε cracker και παραπλανητικά λογισμικά.

Εάν πιστεύετε πως ένα πρόσθετο πρόγραμμα μπορεί να θέσει σε κίνδυνο την ασφάλεια του υπολογιστή σας, ή ότι το πρόσθετο αυτό έχει σχεδιαστεί με κακόβουλες προθέσεις, θα πρέπει να το απενεργοποιήσετε αμέσως μέσω του μενού εργαλείων του κάθε πλοηγού που χρησιμοποιείτε.

5.10.8 Τείχος προστασίας των Windows

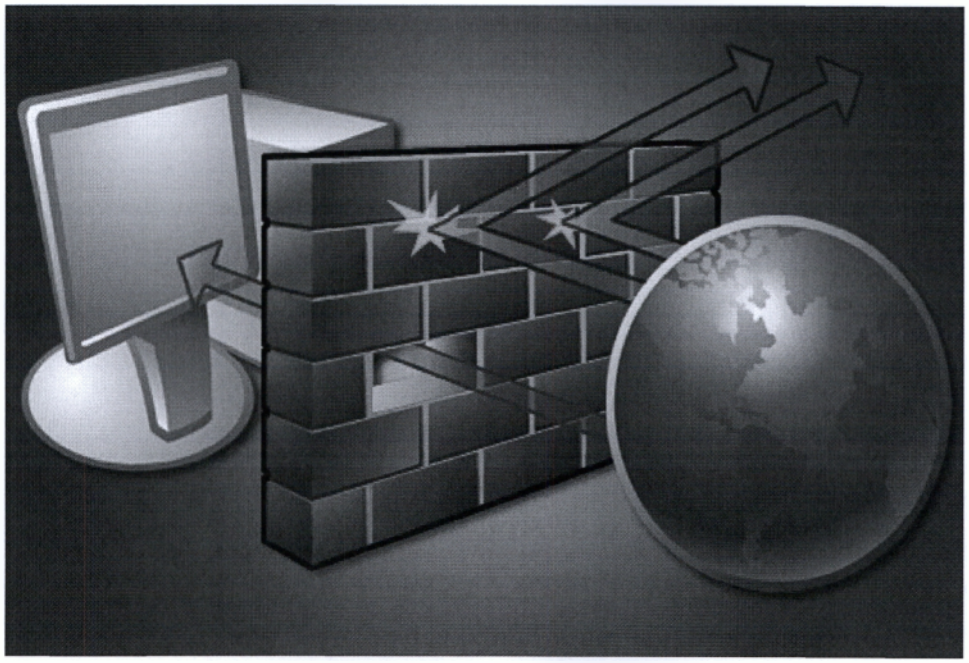
Από πλευράς δομής και κατασκευής, ένα Firewall (Αγγλικός όρος για το τείχος προστασίας) αποτελεί μέρος ενός κτηρίου και παρέχει πυρασφάλεια. Όταν ένα μέρος του κτηρίου πιάσει φωτιά, το τείχος προστασίας εμποδίζει την εξάπλωση της στο μέρος του κτηρίου από την άλλη πλευρά του τείχους.

Με την έλευση της δικτύωσης και την ανάπτυξη του μεγαλύτερου παγκοσμίου δικτύου, του Διαδικτύου, η έννοια του τείχους προστασίας αποτελεί θεμελιώδες στοιχείο της σύγχρονης υπολογιστικής. Το τείχος προστασίας ασφαλίζει τον υπολογιστή σας από εξωτερικές απειλές εφαρμόζοντας μια πολιτική ασφαλείας για τον έλεγχο πληροφοριών δικτύου που μετακινούνται μεταξύ του υπολογιστή σας και διαφόρων δικτύων, συμπεριλαμβανομένου του Διαδικτύου. Τα Windows

περιλαμβάνουν ένα ολοκληρωμένο και "έτοιμο" τείχος προστασίας που σας παρέχει ασφάλεια στο Διαδίκτυο και πρέπει πάντα για έναν μέσω χρήστη να είναι ενεργοποιημένο.

Βέβαια υπάρχουν και οι εξαιρέσεις του τείχους προστασίας των Windows. Τέτοιου είδους εξαιρέσεις είναι τα προγράμματα στα οποία παραχωρήθηκε ρητά δικαίωμα πρόσβασης μέσω της ασφάλειας του τείχους.

Είναι πιθανό να θέλετε να τροποποιήσετε τη λίστα των εξαιρέσεων. Μπορεί να θεωρείτε πως ένα πρόγραμμα που έχει αποκλειστεί από τον υπολογιστή σας, είναι ασφαλές και να επιθυμείτε να το προσθέσετε στις εξαιρέσεις. Ίσως θεωρείτε επίσης ότι κάποιο άλλο πρόγραμμα είναι απειλή για την ασφάλεια του υπολογιστή σας και θέλετε να το αφαιρέσετε από τις εξαιρέσεις.



ΚΕΦΑΛΑΙΟ 6

ΑΣΦΑΛΕΙΑ ΗΛΕΚΤΡΟΝΙΚΟΥ ΤΑΧΥΔΡΟΜΕΙΟΥ

Εισαγωγή

Ιοί, κατασκοπευτικά λογισμικά, κράκερ, κακόβουλοι χρήστες και άλλες απειλές χρησιμοποιούν τα συστήματα ηλεκτρονικού ταχυδρομείου ως κανάλι για την εκτέλεση των κακόβουλων έργων τους. Συνεπώς, είναι λογικό ότι θα πρέπει να ασφαλίζετε και να προστατεύετε το σύστημα του ηλεκτρονικού σας ταχυδρομείου. Με την εφαρμογή ορισμένων μέτρων ασφαλείας, τη χρήση κάποιων εργαλείων και μια επιφυλακτική και συντηρητική συμπεριφορά, μπορείτε να είστε σίγουροι ότι το κενό ασφαλείας του γραμματοκιβωτίου σας έχει κλείσει.

6.1 Κατανόηση της ασφάλειας ηλεκτρονικού ταχυδρομείου

Τα πρώτα προγράμματα αποστολής μηνυμάτων, μετέδιδαν μόνο απλά κείμενα μεταξύ υπολογιστών. Αυτό σήμαινε ότι ήταν σχεδόν αδύνατο για τα κακόβουλα προγράμματα να χρησιμοποιήσουν το μέσο για τις προθέσεις τους. Το μοναδικό κακόβουλο στοιχείο ηλεκτρονικού ταχυδρομείου εκείνο τον καιρό ήταν οι ίδιες οι λέξεις. Οι κακοποιοί δεν είχαν δει τις δυνατότητας του ηλεκτρονικού ταχυδρομείου ως κανάλι για την εκτέλεση των ενεργειών τους και έτσι δεν εκμεταλλευόντουσαν τα συστήματα για αυτό τον σκοπό. Η κύρια ευπάθεια ήταν ότι τα συστήματα ηλεκτρονικού ταχυδρομείου δεν χρησιμοποιούσαν τη μέθοδο της κρυπτογράφησης για να "περιπλέξουν" τα κείμενα που ανταλλάζονταν μεταξύ χρηστών και ένας προχωρημένος χρήστης υπολογιστή μπορούσε πιθανώς να υποκλέψει το κείμενο στο μήνυμα.

Μολονότι τα σύγχρονα συστήματα ηλεκτρονικού ταχυδρομείου δεν χρησιμοποιούν την κρυπτογράφηση από προεπιλογή, την προσφέρουν ως ρύθμιση. Επιπλέον, υπάρχουν περισσότερα εμπόδια για την εισβολή απειλών όπως ηλεκτρονικό ψάρεμά, ιοί, δούρειοι ίπποι, σκουλήκια και ανεπιθύμητα ηλεκτρονικά μηνύματα.

6.1.1 Ηλεκτρονικό ψάρεμα

Οι επιθέσεις ηλεκτρονικού ψαρέματος χρησιμοποιούν τα μηνύματα ηλεκτρονικού ταχυδρομείου για να αποσπάσουν προσωπικά δεδομένα με σκοπό να τα εκμεταλλευτούν για δόλιους σκοπούς όπως υποκλοπή ταυτότητας.

6.1.2 Ιοί, δούρειοι ίπποι και σκουλήκια

Οι ιοί, οι δούρειοι ίπποι και τα σκουλήκια μεταφέρονται μέσω συστημάτων ηλεκτρονικού ταχυδρομείου ως συναπτόμενα αρχεία. Όταν ανοίγετε το επισυναπτόμενο αρχείο ανυποψίαστοι, το κακόβουλο πρόγραμμα επιχειρεί να μολύνει το σύστημα σας.

6.1.3 Ανεπιθύμητη ηλεκτρονική αλληλογραφία (spam)

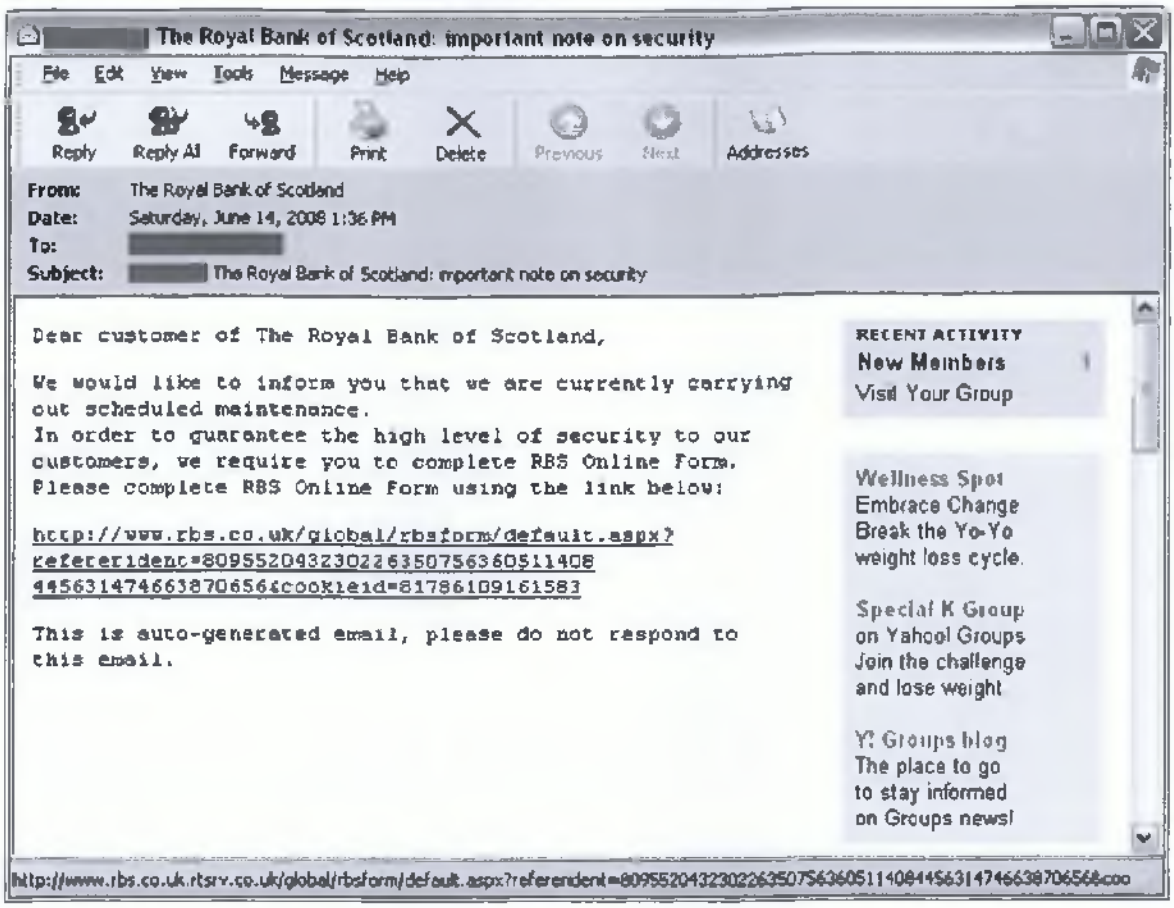
Μολονότι φαινομενικά φαίνεται πιο ενοχλητική από οτιδήποτε άλλο, θα δούμε πώς η ανεπιθύμητη ηλεκτρονική αλληλογραφία μπορεί να επιβραδύνει την απόδοση του μηχανήματός σας, να προκαλέσει συμφόρηση στο γραμματοκιβώτιό σας και να εισαγάγει κινδύνους ασφαλείας.

6.2 Τι ακριβώς είναι το ηλεκτρονικό ψάρεμα ;

Όπως ο ψαράς ρίχνει το δόλωμά του στο νερό ελπίζοντας ότι θα τσιμπήσει κάποιο ψάρι, έτσι και μια απόπειρα "ηλεκτρονικού ψαρέματος" στηρίζεται στο σκεπτικό ότι εάν αρκετά άτομα γίνουν στόχος, ένα ποσοστό αυτών επίσης θα τσιμπήσει το δόλωμα. Οι "ψαράδες" ή κακόβουλοι χρήστες, στέλνουν ηλεκτρονικά μηνύματα τα οποία μεταμφιέζονται σε γνήσια μηνύματα προκειμένου να εξαπατήσουν τον κόσμο και να αποσπάσουν προσωπικά στοιχεία. Αυτά τα στοιχεία χρησιμοποιούνται στη συνέχεια για εγκληματολογικούς σκοπούς, είτε πρόκειται για την πώληση τους σε άλλους κακοποιούς είτε με την αξιοποίησή τους για χρηματικό όφελος.

6.2.1 Παράδειγμα συχνού ηλεκτρονικού ψαρέματος

Ένα μεγάλο ποσοστό επιθέσεων ηλεκτρονικού ψαρέματος χρησιμοποιούν ως βιτρίνα τα τραπεζικά συστήματα για τη παράνομη δράση τους. Στο παρακάτω παράδειγμα, το μήνυμα ηλεκτρονικού ψαρέματος μοιάζει σαν να προέρχεται από την Royal Bank of Scotland και ζητάει από τον χρήστη να συμπληρώσει μία φόρμα με τα στοιχεία του.



Εάν κάποιος παραλήπτης ακολουθήσει τυφλά τις οδηγίες, το αποτέλεσμα θα είναι πιθανώς το εξής :

- Ο παραλήπτης ακολουθεί τον σύνδεσμο σε μια τοποθεσία Ιστού η οποία βρίσκεται στην πραγματικότητα σε διακομιστή που ανήκει στον κακόβουλο χρήστη και έχει σχεδιαστεί για να συγκεντρώνει δεδομένα.
- Ο παραλήπτης εισαγάγει τα προσωπικά του στοιχεία στην ιστοσελίδα.
- Ο κακόβουλος χρήστης συγκεντρώνει τα στοιχεία και είτα τα πουλάει είτε τα χρησιμοποιεί ο ίδιος παράνομα.

6.2.2 Αναγνώριση του ηλεκτρονικού ψαρέματος

Σε σχέση με το προηγούμενο παράδειγμα ηλεκτρονικού ψαρέματος θα δούμε πώς μπορούμε να καταλάβουμε ότι πρόκειται για μια τέτοια επίθεση. Όταν έχουμε την γνώση, τότε ξέρουμε πως να αντιμετωπίσουμε το περιστατικό.

- Είσαστε πελάτης του υποτιθέμενου αποστολέα; Πολλές επιθέσεις ηλεκτρονικού ψαρέματος μπορούν να εξαλειφθούν αμέσως. Συνεργάζεστε με την Royal Bank of Scotland;
- Σας φαίνεται πειστικό; Παρά τις συνεχείς προσπάθειες, πολλά μηνύματα ηλεκτρονικού ψαρέματος περιέχουν πολύ αδέξια κείμενα και είναι γεμάτα ορθογραφικά λάθη.
- Μήπως το μήνυμα ζητάει προσωπικά στοιχεία; Να θυμάστε ότι οι τράπεζες και οι εταιρείες στεγαστικής πίστης δεν ζητούν ποτέ στοιχεία του λογαριασμού μέσω ηλεκτρονικού ταχυδρομείου. Πότε μην παραχωρείτε αυτές τις πληροφορίες.
- Οι επιθέσεις ηλεκτρονικού ψαρέματος ακολουθούν συχνά τακτικές εκφοβισμού ώστε να εξαπατήσουν τον κόσμο που έτσι λαμβάνει γρήγορες αποφάσεις. Μήπως το μήνυμα σας ενημερώνει ότι ο λογαριασμός σας θα παγώσει αμέσως ή ότι κάποιος άλλος τον χρησιμοποιεί; Να είστε επιφυλακτικοί απέναντι σε αντίστοιχες δηλώσεις και αν πιστεύετε πως η ασφάλεια του λογαριασμού σας τίθεται σε κίνδυνο, επικοινωνήστε με την τράπεζά σας.
- Καταδείξτε με το ποντίκι σας του συνδέσμους που σας ζητάνε να ακολουθήσετε και ελέγξτε τη διεύθυνση που εμφανίζεται στο κάτω μέρος του μηνύματος, η οποία δείχνει πού ακριβώς σας οδηγεί ο σύνδεσμος.
- Όσο παραπλανητικοί είναι αυτοί οι σύνδεσμοι, άλλο τόσο παραπλανητική μπορεί να είναι και μια διεύθυνση ηλεκτρονικού ταχυδρομείου. Μία μέθοδος που εφαρμόζουν τόσο οι "ψαράδες" όσο και άλλοι αδίστακτοι χρήστες ηλεκτρονικού ταχυδρομείου, γνωστή ως παραπλάνηση (spoofing), είναι ότι κάνουν τον παραλήπτη του μηνύματος να πιστεύει ότι στέλνει απάντηση σε μια απόλυτα νόμιμη διεύθυνση ηλεκτρονικού ταχυδρομείου. Όπως και με τους συνδέσμους Ιστού έτσι και στην περίπτωση των συνδέσμων διευθύνσεων ηλεκτρονικού ταχυδρομείου, μπορείτε να τους καταδείξετε για να ανακαλύψετε τον πραγματικό τους προορισμό
- Να χρησιμοποιείτε πάντα τη λογική σας όσον αφορά στην ηλεκτρονική αλληλογραφία. Μην παίρνετε ποτέ απερίσκεπτες αποφάσεις, μην εισαγάγετε προσωπικά στοιχεία παρά μόνο όταν είστε απόλυτα βέβαιοι για την

γνησιότητα του μηνύματος και εάν έχετε την παραμικρή αμφιβολία, διαγράψτε το μήνυμα εντελώς.

6.2.3 Αντιμετώπιση του ηλεκτρονικού ψαρέματος

Όπως η γνώση του τρόπου δράσης των εγκληματιών σας βοηθάει να προστατέψετε τον εαυτό σας και το σπίτι σας, έτσι και η κατανόηση του τρόπου λειτουργίας των μηνυμάτων ηλεκτρονικού ψαρέματος σας δίνει τη δυνατότητα να προστατευτείτε από αυτές τις επιθέσεις.

Μερικοί βασικοί κανόνες για τον τρόπο αντιμετώπισης του ηλεκτρονικονικού ψαρέματος είναι οι εξής:

- Επιβεβαιώστε την ορθότητα της αναγνώρισης σας εκτελώντας αναζήτηση στο Διαδίκτυο. Μια σύντομη αναζήτηση στην τοποθεσία κατά του ηλεκτρονικού ψαρέματος phisery.internetdefence.net επιβεβαιώνει τις υποψίες μας.
- Μην απαντάτε. Εάν το κάνετε, επιβεβαιώνετε την διεύθυνση του ηλεκτρονικού ταχυδρομείου σας και παρέχετε ένα ίχνος στον κακόβουλο χρήστη.
- Ποτέ μην ακολουθείτε τους συνδέσμους της τοποθεσίας Ιστού, ακόμα και αν είστε περίεργοι να δείτε που οδηγούν.

6.3 Ανεπιθύμητη ηλεκτρονική αλληλογραφία

Η ανεπιθύμητη ηλεκτρονική αλληλογραφία, μερικές φορές αποκαλείται και αυτόκλητη εμπορική ή αυτόκλητη μαζική ηλεκτρονική αλληλογραφία ή απλώς "Spam", είναι παρόμοια από πλευράς αρχής με την αυτόκλητη αλληλογραφία που λαμβάνετε στο γραμματοκιβώτιο του σπιτιού σας. Η διαφορά είναι ότι τα ανεπιθύμητα ηλεκτρονικά μηνύματα επιβαρύνουν τον παραλήπτη από πλευράς χώρου αποθήκευσης στον δίσκο, επεξεργασίας, κόστους διανομής (σύνδεση στο Διαδίκτυο) και βέβαια χρόνου τον οποίο ξοδεύει για την αντιμετώπισή τους.

6.3.1 Όγκος και τύποι ανεπιθύμητης αλληλογραφίας

Η ανεπιθύμητη ηλεκτρονική αλληλογραφία αποτελεί ένα τεράστιο πρόβλημα. Υπολογίζεται πως τον Ιούνιο του 2006 αποστέλλονταν καθημερινά 55 δισεκατομμύρια ανεπιθύμητα μηνύματα[5]. Λόγω του σημαντικού όγκου της προκαλεί συμφόρηση στις θυρίδες εισερχομένων σε όλο τον κόσμο και κάνει ολόκληρα συστήματα να ασχολούνται με αυτή, για να μην αναφερθούμε στον χρόνο που ξοδεύουν οι παραλήπτες. Η ανεπιθύμητη ηλεκτρονική αλληλογραφία επιμένει γιατί αποτελεί μια φτηνή επιλογή για τους δράστες, κοστίζοντας ελάχιστα σε σχέση με την ίδια προσέγγιση άμεσου μάρκετινγκ μέσω ταχυδρομείου.

6.3.2 Αναγνώριση ανεπιθύμητου ηλεκτρονικού μηνύματος

Κανένα πρόγραμμα ανεπιθύμητης ηλεκτρονικής αλληλογραφίας δεν μπορεί να αναγνωρίσει όλα τα σχετικά μηνύματα και επειδή οι αποστολείς αναπτύσσουν συνεχώς νέες μεθόδους για να αποφεύγουν την εύκολη αναγνώριση, είναι χρήσιμο να μπορείτε εσείς, ως χρήστες, να αναγνωρίζετε μόνοι σας ένα ανεπιθύμητο μήνυμα.

From	Subject
Adelaide Fatimah	a $12000 watch, we sell at $200, Quality watches at ...
antonino rodney	Goodiest c1alis
Irina Gidget	FDA Approved Medications: $1.12/pill forViagr...
tom@messagingtime...	tom@messagingtimes.com, Up to 20% OFF
Samantha Hickey	Enlarge, Widen and Strengthen
churchill ravi	MSG #:19846 The world's largest online presc...
abel yanjun	MSG #:84037 World's lowest prices on largest...
Maureen Orr	Recapture a bit of your youth again
nanako258@yahoo.c...	40□Î^È□ã,Å□5,à□g'Ì,à–ü,ã,³,ë,½,¢•û,Í[–ü,ã,...
Jerald Shook	a xmas gift to your wife is your bigger PE gs ft...
Blanca Petty	Mit und schaffen Sie das was Frauen wollern!
Lynne Mcneal	xp oem software
emerson forrest	from Stella Vargas
Revolution Jobs	Hundreds of digital careers on Revolution Jobs
Auto Loan Department	GET APPROVED!
jacquelyn	hi from jacquelyn
ParkRoyalCancun	Visit Cancun With A 3 Night Free Stay - No Pur...
Colon Cleanse Samples	View this LifeChanging Breakthrough
o05689ok97@tom.com	40□Î^È□ã,Å□5,à□g'Ì,à–ü,ã,³,ë,½,¢•û,Í[–ü,ã,...

[5] Mark Lee, Securing your Pc σελ. 106

Υπάρχουν μερικές ενδείξεις που μας οδηγούν γρήγορα στο συμπέρασμα ότι πρόκειται για αυτόκλητο εμπορικό ηλεκτρονικό μήνυμα. Μερικές από αυτές είναι οι εξής :

- Τα ηλεκτρονικά μηνύματα είναι εξαιρετικά αντιεπαγγελματικά στην πλειοψηφία τους. Ίσως περιέχουν αρκετά ορθογραφικά λάθη, έχουν υποστεί κακή μορφοποίηση, η γραμματική δεν είναι σωστή και η γλώσσα είναι ακατάλληλη.
- Ο αποστολέας δεν είναι γνωστός στον παραλήπτη. Θα μπορούσε να είναι κάποιο όνομα χρήστη που έχουν σαρώσει οι αποστολείς του ή ένα τυχαίο όνομα "μεταμφιεσμένο" προκειμένου να κρύβει την πραγματική ταυτότητα του αποστολέα. Βέβαια ενδέχεται να είναι και η διεύθυνση ηλεκτρονικού ταχυδρομείου ενός ανυποψίαστου χρήστη του οποίου ο υπολογιστής χρησιμοποιείται για αυτόν το σκοπό.
- Το κείμενο του μηνύματος συνήθως περιέχει λέξεις με συγκεκριμένη ορθογραφία για να αποτρέπεται η ανίχνευσή του από τα φίλτρα ανεπιθύμητης ηλεκτρονικής αλληλογραφίας. Για παράδειγμα η λέξη "Congratulations" γράφεται "G0ngratu1at10ns'.
- Το όνομα της εταιρείας δεν αναγράφετε στο μήνυμα, ποιος λοιπόν ωφελείται από την κοινοποίηση αυτής της πληροφορίας σε εσάς; Γιατί κάποιος που κατέχει "εγγυημένη" γνώση μιας επερχόμενης κερδοφόρας χρηματιστηριακής ευκαιρίας θέλει να σας το πει;
- Τα μηνύματα δεν θα είναι καθόλου πιστευτά. Για παράδειγμα, θα υποστηρίζουν ότι η τιμή μιας μετοχής πρόκειται να απογειωθεί και πως αν επενδύσετε θα έχετε "εγγυημένο" κέρδος 500%. Η συμπεριφορά των μετοχών δεν είναι βέβαια ποτέ εγγυημένη και το 500% είναι ένα εξαιρετικά μη ρεαλιστικό νούμερο.

6.4 Αποκλεισμός ανεπιθύμητης ηλεκτρονικής αλληλογραφίας

Είναι δύσκολο να αποδεχτούμε το γεγονός ότι δεν μπορούμε να κάνουμε πολλά για να αποφύγουμε τη λήψη και συσσώρευση ανεπιθύμητης αλληλογραφίας στα εισερχόμενα μας σε καθημερινή βάση. Αποτελεί ένα ενοχλητικό στοιχείο της σύγχρονης πληροφορικής το οποίο θα εξακολουθεί να υπάρχει και στο άμεσο μέλλον.

Με αυτό το δεδομένο, παραθέτουμε ορισμένα μέτρα που μπορείτε να πάρετε για να αποκλείσετε την ανεπιθύμητη ηλεκτρονική αλληλογραφία. Εναλλακτικά, εάν σας ενοχλούν κάποια ανεπιθύμητα μηνύματα τα οποία λάβατε, μπορείτε να προβείτε σε ορισμένες ενέργειες για την καταπολέμησή τους.

6.4.1 Ελαχιστοποίηση και αποκλεισμός ανεπιθύμητης ηλεκτρονικής αλληλογραφίας

Ας δούμε τα βήματα που μπορείτε να ακολουθήσετε για να ελαχιστοποιήσετε το πλήθος των ανεπιθύμητων ηλεκτρονικών μηνυμάτων που λαμβάνετε.

- Δίνετε με προσοχή τη διεύθυνση του ηλεκτρονικού σας ταχυδρομείου. Οι αποστολείς κυνηγούν πάντοτε έγκυρες διευθύνσεις ηλεκτρονικού ταχυδρομείου.
- Αποφεύγετε την κοινοποίηση της διεύθυνσης του ηλεκτρονικού σας ταχυδρομείου σε πίνακες ανακοινώσεων και φόρουμ εκτός και αν είναι απολύτως απαραίτητη. Υπάρχουν τοποθεσίες οι οποίες αποτελούν θησαυρό για αποστολείς που θέλουν να σαρώσουν ποιοτικές διευθύνσεις
- Όπως προαναφέραμε, δεν θα πρέπει ποτέ να απαντάτε σε ανεπιθύμητα μηνύματα ακόμα και αν θέλετε να ακυρώσετε τη συνδρομή σας ή να παραπονεθείτε.
- Να ζητάτε από τους άλλους να μην περιλαμβάνουν το όνομα σας στις λίστες «Προς» και «Κοινοποίηση» όταν προωθούν μηνύματα. Αυτές οι λίστες είναι δώρο για τους αποστολείς ανεπιθύμητων μηνυμάτων.
- Εφαρμόστε ένα φίλτρο ηλεκτρονικού ταχυδρομείου. Θα αναφερθούμε για τα φίλτρα ηλεκτρονικού ταχυδρομείου παρακάτω.

6.4.2 Ανταπόδοση της επίθεσης στους αποστολείς ανεπιθύμητων μηνυμάτων

Εάν είστε αποφασισμένοι να καταπολεμήσετε τα ανεπιθύμητα μηνύματα που λαμβάνετε, τα οποία είναι πιθανώς παράνομα, προσπαθήστε να εντοπίσετε την προέλευση του μηνύματος από τη διεύθυνση IP. Οι αποστολείς των μηνυμάτων αυτών δεν έχουν την δυνατότητα να αλλάξουν τη διεύθυνση IP που διακρίνεται στην πηγή του μηνύματος.

6.5 Εξωτερικό φίλτρο ανεπιθύμητης ηλεκτρονικής αλληλογραφίας

Μια άλλη επιλογή στη μάχη κατά της ανεπιθύμητης ηλεκτρονικής αλληλογραφίας είναι η χρήση ενός εξωτερικού φίλτρου. Μολονότι η αλληλογραφία των Windows διαθέτει ένα νέο φίλτρο το οποίο θα δούμε παρακάτω, υπάρχει και άλλη μια επιλογή που αξίζει να εκμεταλλευτείτε.

6.5.1 Χρήση του Mailwasher

Το Mailwasher είναι μια εφαρμογή πρόληψης και φιλτραρίσματος ανεπιθύμητων ηλεκτρονικών μηνυμάτων. Διαφέρει από τα άλλα παρεμφερή συστήματα επειδή μπορεί να αποκλείει ανεπιθύμητα ηλεκτρονικά μηνύματα στο διακομιστή αλληλογραφίας και το μήνυμα να μην φτάνει ποτέ στον υπολογιστή σας. Επειδή οι αποστολείς ανεπιθύμητων ηλεκτρονικών μηνυμάτων εκμεταλλεύονται λειτουργίες των πελατών ηλεκτρονικού ταχυδρομείου που ανιχνεύουν εάν ανοίξατε το μήνυμα, είναι χρήσιμο να έχετε ένα εργαλείο το οποίο εμποδίζει αυτά τα μηνύματα να φτάνουν στον υπολογιστή σας.

6.5.2 Τρόπος λειτουργίας του Mailwasher

Το Mailwasher διαβάζει τα μηνύματά σας απευθείας από το διακομιστή της υπηρεσίας παροχής Διαδικτύου χωρίς να τα κατεβάζει στο πρόγραμμα του ηλεκτρονικού ταχυδρομείου. Μπορείτε να διαγράψετε τα ανεπιθύμητα μηνύματα στον διακομιστή ηλεκτρονικού ταχυδρομείου μέσω του Mailwasher ή ακόμα και να ορίσετε ένα μήνυμα επιστροφής το οποίο ενημερώνει τον αποστολέα ότι η διεύθυνση σας δεν ισχύει, με την ελπίδα ότι ο επιτιθέμενος θα διαγράψει την διεύθυνση σας από την λίστα του. Ίσως είναι απίθανο να είναι αρκετά οργανωμένος και σχολαστικός για να το κάνει και το επιστρεφόμενο μήνυμά σας μπορεί να καταλήξει σε κάποια παραπλανητική διεύθυνση, αλλά αξίζει να το προσπαθήσετε.

6.5.3 Άλλες επιλογές

Το Mailwasher και άλλα παρόμοια φίλτρα περιλαμβάνουν και άλλες επιλογές για την καταπολέμηση της ανεπιθύμητης ηλεκτρονικής αλληλογραφίας. Μπορείτε να δημιουργείτε λίστες αποκλεισμένων στοιχείων ορίζοντας ονόματα χρηστών και

τομέων των αποστολέων και να θέτετε τους δικούς σας κανόνες για το αυτόματο φιλτράρισμα μηνυμάτων.

6.6 Windows : Φίλτρο ανεπιθύμητης ηλεκτρονικής αλληλογραφίας

Τα Windows σχεδιαστήκαν από την Microsoft με γνώμονα την ασφάλεια του συστήματος σας. Ένα από τα κυριότερα νέα στοιχεία είναι το φίλτρο ανεπιθύμητης ηλεκτρονικής αλληλογραφίας το οποίο σας βοηθάει να αντιμετωπίζετε το αυξανόμενο πλήθος μαζικών και ανεπιθύμητων μηνυμάτων και των επιθέσεων ηλεκτρονικού ψαρέματος.

6.6.1 Ο Φάκελος "Ανεπιθύμητη αλληλογραφία"

Η αλληλογραφία των Windows διαθέτει ένα φάκελο, ο οποίος ονομάζετε "Ανεπιθύμητη αλληλογραφία" όπως είχαμε προαναφέρει από την ενότητα για την αντιμετώπιση των επιθέσεων ηλεκτρονικού ψαρέματος που καλύψαμε νωρίτερα στην πτυχιακή.

Ο Φάκελος "ανεπιθύμητη αλληλογραφία" είναι μια περιοχή απόθεσης όλων των ύποπτων μηνυμάτων. Η αλληλογραφία των Windows μετακινεί εκεί τα μηνύματα που θεωρεί "ανεπιθύμητα" εφαρμόζοντας διάφορα κριτήρια και ανάλογα με το επίπεδο προστασίας το οποίο επιλέξατε να εφαρμόσετε.

6.6.2 Επίπεδο προστασίας

Το επίπεδο προστασίας του φίλτρου ανεπιθύμητων μηνυμάτων ενημερώνει την αλληλογραφία των Windows για τον τρόπο αντιμετώπισης των ύποπτων μηνυμάτων.

Μπορείτε να επιλέξετε ανάμεσα σε τέσσερα επίπεδα προστασίας.

- Χωρίς αυτόματο φιλτράρισμα: Όταν έχετε ενεργοποιημένη αυτή τη ρύθμιση, τα ανεπιθύμητα μηνύματα δεν θα μετακινούνται στον φάκελο ανεπιθύμητη αλληλογραφία παρά μόνο όταν ο αποστολέας είναι στην λίστα "Αποκλεισμένοι αποστολείς".

- Χαμηλή: Αυτό είναι το προεπιλεγμένο επίπεδο και όταν το έχετε ενεργοποιήσει, η προφανής ανεπιθύμητη αλληλογραφία μεταφέρεται στο φάκελο ανεπιθύμητη αλληλογραφία.
- Υψηλή: Το φίλτρο ανεπιθύμητης αλληλογραφίας είναι πιο αυστηρό στην επιλογή ύποπτων ανεπιθύμητων μηνυμάτων όταν ενεργοποιείτε αυτή τη ρύθμιση.
- Μόνο ασφαλή λίστα: Με την ενεργοποίηση αυτής της ρύθμισης λαμβάνετε μηνύματα στα εισερχόμενά σας μόνο από άτομα ή τομείς που περιλαμβάνονται στη λίστα ασφαλών αποστολέων.

ΣΥΜΠΕΡΑΣΜΑΤΑ

Είτε βρισκόμαστε στο επιχειρησιακό μας περιβάλλον, είτε στο σπίτι οι κίνδυνοι ενός επεισοδίου κοινωνικής μηχανικής είναι μεγάλοι και η πιθανότητα να καταστούμε επόμενα θύματα μιας τέτοιας επίθεσης ακόμα μεγαλύτερη εάν είμαστε απρόσεκτοι. Όσο πιο καθησυχασμένοι είμαστε ότι δεν πρόκειται να πέσουμε ποτέ θύματα υποκλοπής, άλλο τόσο και η κοινωνική μηχανική θα βρίσκει νέους τρόπους για να μας παραπλανεί.

Μπορεί στην ασφάλεια του προσωπικού μας υπολογιστή να αρκούμαστε σε ένα πρόγραμμα κατά των κακόβουλων λογισμικών αλλά αυτό δεν αρκεί για μεγάλες πολυεθνικές εταιρίες. Οι υπάλληλοι των τμημάτων IT αγανακτούν στο άκουσμα του όρου κοινωνική μηχανική και δυστυχώς δεν είναι κάτι που περνάει μόνο από το χέρι τους για να μπορέσουν να σταματήσουν μια τέτοιου είδους επίθεση. Το μόνο που μπορούνε να κάνουν είναι να πείσουν τους υπάλληλους της εταιρίας να προσέχουν για "σημάδια" μιας τέτοιας επίθεσης και να τους ενημερώσουν όσο το δυνατόν γρηγορότερα.

Με τη χρήση των πολιτικών που αναπτύσσει η κάθε εταιρία, μειώνονται οι πιθανότητες μιας τέτοιας επίθεσης αλλά για να εξασφαλίσει την ασφάλεια και την προστασία της είναι απαραίτητη η εφαρμογή τους. Στη χειρότερη περίπτωση που δεν θα μπορέσουμε να σταματήσουμε μια επίθεση με την βοήθεια των υπαλλήλων της εταιρίας, ίσως καταστούμε ικανοί να καταλάβουμε τον σκοπό του επιτιθέμενου πριν κάνει την τελική του επίθεση και να ασφαλίσουμε ακόμα περισσότερο τις πληροφορίες που θέλει να υποκλέψει.

Το θέμα όμως δεν είναι να μπορούνε να προστατευτούνε μόνο οι επιχειρήσεις από τέτοιες επιθέσεις, αλλά και εμείς να μπορούμε να προστατεύσουμε στο σπίτι μας τις πληροφορίες μας και τα προσωπικά μας δεδομένα από τους κακόβουλους χρήστες. Οι επιλογές και οι δυνατότητες που έχουμε στην διάθεση μας για να το καταφέρουμε είναι πολλές και δεν είναι ανάγκη να τις πληρώνουμε πανάκριβα. Υπάρχουν άλλωστε αρκετές εφαρμογές που διατίθενται στο κοινό δωρεάν, οι οποίες συμβάλλουν εν μέρει στην προστασία των δεδομένων μας. Προσφέρουν δηλαδή όση το δυνατόν μεγαλύτερη και καλύτερη προστασία χρειάζεται ένας μέσος χρήστης.

Ζούμε πλέον στην εποχή της τεχνολογίας, ο κόσμος μας δεν θα λειτουργούσε έτσι όπως τον γνωρίζουμε εάν δεν υπήρχαν οι υπολογιστές. Δυστυχώς ή ευτυχώς για κάποιους από εμάς έχει καταστεί απαραίτητο εργαλείο, αλλά για κάποιους άλλους έχει γίνει τρόπος ζωής το να υποκλέπτουν πληροφορίες και να κερδίζουν χρήματα μέσα από απάτες. Η τεχνολογία της εποχής μας κρύβει πολλούς κινδύνους, αλλά και πολλούς τρόπους για να προστατευτούμε. Εμείς αρκεί μόνο να τους εφαρμόζουμε.

Πηγές

Έρευνα πολιτικών κατά της κοινωνικής μηχανικής στην ΑΓΕΤ ΗΡΑΚΛΗΣ, Lafarge

Merriam Webster, Unabridged Dictionary

Η Τέχνη της αποπλάνησης, Kevin Mitnik 2002

Securing your Pc, Mark Lee 2007

Compusics.blogspot.com

Pearless.citec-us/blog/social-engineering

Igniq.com

Howto-hsk.blogspot.com

Myitforum.com

Blog.group.com

Yasitariq.wordpress.com

Safestudying.com

Updatetechno.com

Secure-my-internet.com

Blog.policypatrol.com