Θέματα ασφαλείας διακίνησης πληροφοριών στη βιβλιοθηκονομική κοινότητα

Νικόλαος Καρεκλάς, Μάρκος Δενδρινός

Πρόλογος

Οι «απειλές» για την ασφάλεια ενός δικτύου βιβλιοθήκης μπορούν να προέλθουν από ένα μεγάλο αριθμό «πηγών», με πολλούς διαφορετικούς τρόπους, καλύπτοντας ένα ευρύ φάσμα περιπτώσεων. Η υπάρχουσα τάση για τη μεγαλύτερη δυνατή «αυτοματοποίηση» των επικοινωνιακών διαδικασιών αποτελεί ταυτόχρονα και την «αχίλλειο πτέρνα» πολλών διασυνδεδεμένων πληροφορικών συστημάτων.

Η ανάγκη για συνεχή επαγρύπνηση σε θέματα ασφαλείας είναι το «τίμημα», μεταξύ των άλλων, που καλούμαστε να πληρώσουμε για τα πολλαπλά οφέλη που προσφέρει μια «δικτυωμένη κοινωνία»

Στο άρθρο αυτό γίνεται αναφορά στους κινδύνους χρήσης του Διαδικτύου (του Παγκόσμιου Ιστού και του Ηλεκτρονικού Ταχυδρομείου) καθώς και στους τρόπους αποφυγής και αντιμετώπισης αυτών των κινδύνων.

1. Ιοί και Internet

Το Internet είναι ένα λειτουργικό μέσο. Μπορούμε να βρούμε οποιαδήποτε πληροφορία και να επικοινωνήσουμε με οποιονδήποτε χρήστη, ανταλλάσσοντας μηνύματα και αρχεία. Το πρόβλημα είναι ότι σε πολλές περιπτώσεις το αρχείο που βρήκαμε μετά από πολύ καιρό αναζήτησης, μπορεί να παρέχει και μερικές εντελώς ανεπιθύμητες παρενέργειες που ο κατασκευαστής δεν είχε την πρόθεση να περιλάβει στο πρόγραμμα. Στη διάρκεια όμως της διανομής αυτού του προγράμματος, έχει ενσωματωθεί και κάποιος ιός, που με την εγκατάσταση της εφαρμογής στον υπολογιστή μας θα ξεκινήσει τη λειτουργία του θέτοντας σε σημαντικό κίνδυνο την ακεραιότητα των πολύτιμων δεδομένων μας.

Οι ιοί που διακινούνται στο Internet φτάνουν τις μερικές χιλιάδες και λόγω της φύσης του μέσου, η διάδοσή τους είναι σε πολλές περιπτώσεις θέμα ωρών. Παλαιότερα, όταν οι δισκέτες αποτελούσαν το κύριο μέσο ανταλλαγής δεδομένων και shareware προγραμμάτων, για την προσβολή των υπολογιστών σε μία ευρεία γεωγραφική περιοχή ίσως θα έπρεπε να περάσουν και μήνες. Στο μεταξύ οι κατασκευαστές των antivirus προγραμμάτων διέθεταν το κατά περίπτωση κατάλληλο αντίδοτο και ελάχιστοι ήταν εκείνοι που αντιλαμβάνονταν την ύπαρξη του ίδιου του ιού.

Η διάδοση του Internet όμως οφέλησε τους ιούς, όπως ακριβώς τα σύγχρονα συγκοινωνιακά μέσα ευνόησαν τη μετάδοση του ιού της γρίπης. Ενώ παλαιότερα θα έπρεπε να περάσει αρκετός χρόνος για να "ταξιδέψει" ένας ιός από τις ΗΠΑ στην Ευρώπη, σήμερα κάτι τέτοιο μπορεί να γίνει με την αποστολή ενός και μόνο e-mail ή το κατέβασμα κάποιου αρχείου. Οποιοσδήποτε μπορεί να συνδεθεί με κάποιο απομακρυσμένο ftp site για να αποκτήσει ένα πρόγραμμα. Αν αυτό περιλαμβάνει και κάποιο ιό, ο αριθμός των υπολογιστών που μπορούν να προσβληθούν αυξάνεται εκθετικά. Οι κυριότερες κατηγορίες ιών που θα συναντήσουμε στο Internet είναι οι εξής:

α) Γνωστοί και κλασικοί ιοί: Αυτή η ομάδα των ιών θα μπορούσε να χαρακτηριστεί ως η κλασική. Περιλαμβάνει όλους τους ιούς που γνωρίζουμε εδώ και αρκετά χρόνια και απειλούν την ακεραιότητα των συστημάτων μας διαρκώς. Για τη συντριπτική πλειοψηφία των συγκεκριμένων ιών υπάρχουν δημοφιλή antivirus προγράμματα και σε γενικές γραμμές τα προβλήματα που μπορούν να προκαλέσουν στον χρήστη είναι ελάχιστα. Ακόμη και στην περίπτωση που πρόκειται

για εντελώς νέες παρουσίες, οι μέθοδοι αντιμετώπισης είναι γνωστές αφού βασίζονται σε παλαιότερους ιούς. Οι πιο δύσκολοι στην αντιμετώπιση είναι οι ιοί που προσβάλουν τον boot sector του συστήματος και οι ιοί που επηρεάζουν το partition table του σκληρού δίσκου.

β) Ιοί Μακροεντολών: Οι ιοί που ανήκουν σ' αυτή την κατηγορία δεν αποτελούν εκτελέσιμα τμήματα κώδικα, αλλά εκμεταλλεύονται το μηχανισμό μακροεντολών που περιλαμβάνουν δημοφιλείς εφαρμογές. Οι διασημότεροι ιοί της συγκεκριμένης κατηγορίας είναι αυτοί που επηρεάζουν το περιβάλλον εργασίας του Word. Μιλάμε κυρίως για τον Winword, τον Concept και τον Boza.

Στην ουσία πρόκειται για μακροεντολές που αντιμετωπίζονται σχετικά εύκολα, όμως δεν υπάρχουν μέχρι στιγμής αυτόματες μέθοδοι ανίχνευσής τους πράγμα που διευκολύνει σημαντικά τη διάδοσή τους. Κάποια στιγμή ακόμη και στις κεντρικές εγκαταστάσεις της Microsoft αναφέρθηκαν κρούσματα προσβολής από τους συγκεκριμένους ιούς. Πάρα πολλοί χρήστες ανταλλάσουν μέσω του ηλεκτρονικού ταχυδρομείου, έγγραφα τα οποία έχουν δημιουργηθεί στο Word και για το λόγο αυτό ο ρυθμός διάδοσης των συγκεκριμένων ιών είναι εξαιρετικά υψηλός.

γ) Ιοί Java και JavaScript: Αυτή η ομάδα ιών είναι ίσως και η πιο επικίνδυνη. Οι ειδικοί πιστεύουν ότι πάρα πολύ σύντομα θα κληθούμε να αντιμετωπίσουμε τους ιούς που έχουν κατασκευαστεί με τη γλώσσα Java ή την JavaScript.Το γεγονός ότι οι συγκεκριμένες γλώσσες αποδεικνύονται εξαιρετικά ισχυρές, έχει δημιουργήσει αρκετές ανησυχίες, αφού κάποιος με αρκετές γνώσεις στην Java θα μπορούσε να δημιουργήσει ένα applet, το οποίο θα τρέχει στον Web browser του ανυποψίαστου χρήστη, προκαλώντας άπειρα προβλήματα. Η κύρια μέθοδος αντιμετώπισης είναι η απενεργοποίηση της επιλογής για την εκτέλεση των applets που έχουν γραφτεί σε Java ή JavaScript.

δ) Trojan Horses ή Δούρειοι Ίπποι: Στην περίπτωση αυτή έχουμε ένα τμήμα ανεπιθύμητου κώδικα κρυμμένου μέσα σε ένα τμήμα επιθυμητού κώδικα. Προμηθευόμαστε, δηλαδή, ένα πρόγραμμα το οποίο εκτελεί ή υποστηρίζει ότι εκτελεί μια επιθυμητή λειτουργία και μόλις το χρησιμοποιήσουμε (είτε αμέσως είτε μόλις ικανοποιηθεί μια λογική ή χρονική συνθήκη), αυτό κάνει και κάτι άλλο, συνήθως βλαβερό για τον υπολογιστή. Υπάρχει μία μικρή ομάδα ιών που ανήκουν στην κατηγορία των Δούρειων Ίππων και που αφορούν πρωτίστως τους χρήστες του Intenet, καθώς και όσους χρησιμοποιούν Shareware προγράμματα. Πρόκειται για ιούς που εμφανίζονται με το όνομα κάποιου γνωστού προγράμματος (τελευταία έχει παρουσιαστεί μία προτίμηση στο γνωστό συμπιεστικό πρόγραμμα pkzip). Αν επιχειρήσουμε να τρέξουμε το πρόγραμμα ο ιός ξεκινά άμεσα τη λειτουργία του και συνήθως διαγράφει τα αρχεία του σκληρού δίσκου. Αρκετά κρούσματα αφορούν έναν ιό που εμφανίζονταν με τα ονόματα: pk300, pk300b, pkz300 και pkz300b.

2. Απειλές μέσω ηλεκτρονικού ταχυδρομείου

2.1. Ιοί

Το ηλεκτρονικό ταχυδρομείο για τους σύγχρονους βιβλιοθηκονόμους αποτελεί την βασικότερη πηγή επικοινωνίας. Η μετάδοση ιών μέσω ηλεκτρονικού ταχυδρομείου είναι και ο συνηθέστερος τρόπος διάδοσής τους. Οι ιοί επικολλώνται συνήθως στα συνημμένα αρχεία των μηνυμάτων και μολύνουν τον υπολογιστή του χρήστη, μόλις αυτός ανοίξει το συνημμένο αρχείο.

Δε θα πρέπει λοιπόν οι χρήστες να ανοίγουν ποτέ μηνύματα τα οποία προέρχονται από άγνωστο αποστολέα, ιδιαίτερα αν αυτά περιέχουν συνημμένα αρχεία (συνήθως με κατάληξη.exe,.com,.vbs,.dll,.sh,.bat κ.ά), ενώ πιθανόν να περιέχουν καταστροφικό κώδικα (μήνυμα μορφής.html) που ενεργοποιείται αυτόματα με την ανάγνωση του email.

Επίσης θα πρέπει να είναι ιδιαίτερα επιφυλακτικοί ακόμα και απέναντι σε μηνύματα που προέρχονται από γνωστό αποστολέα, αλλά με ύποπτο θέμα. Για αυτό το λόγο είναι καλό να

απενεργοποιείται η προεπισκόπηση στα εισερχόμενα μηνύματα, ώστε αυτά να μην ανοίγουν αυτόματα (για παράδειγμα στο Outlook Express επιλογή Προβολή →Διάταξη →απενεργοποίηση του «εμφάνιση παραθύρου προεπισκόπησης»).

Σε κάθε περίπτωση επιβάλλεται ο έλεγχος της αλληλογραφίας (εισερχόμενης και εξερχόμενης) από ένα καλό αντιβιοτικό πρόγραμμα, το οποίο θα ενημερώνεται συνεχώς.

Σε τακτά χρονικά διαστήματα εμφανίζονται διάφορα μηνύματα που προειδοποιούν τους χρήστες του Internet για την ύπαρξη μερικών "πονηρών" μηνυμάτων ηλεκτρονικού ταχυδρομείου, τα οποία μπορούν ακόμη και να "κάψουν" τον επεξεργαστή.

Ο πιο διάσημος ιός εδώ ονομάζεται Good Times και πολλοί (νέοι κυρίως) χρήστες αναφέρονται σ' αυτόν με δέος. Υποτίθεται πως αν λάβουμε ένα μήνυμα με τον τίτλο Good Times και επιχειρήσουμε να το διαβάσουμε, αυτόματα θα διαγραφούν όλα τα αρχεία από το σκληρό δίσκο και μπορεί να υποστεί ανεπανόρθωτη βλάβη ακόμη και ο επεξεργαστής.

Φυσικά δεν υπάρχει μήνυμα ηλεκτρονικού ταχυδρομείου που να μπορεί να εκτελέσει τέτοιου είδους λειτουργία. Για να λειτουργήσουν οι ιοί θα πρέπει κάποιος να τους ενεργοποιήσει, δηλαδή να εκτελέσει το πρόγραμμα που έχει προσβληθεί.

Οι τύποι των ιών που κυκλοφορούν στο Internet και που μπορούν να προσβάλουν τον υπολογιστή μας είναι αρκετοί. Για κάθε μία ομάδα υπάρχουν κάποιες τεχνικές προστασίας και εξουδετέρωσης. Σε όλες τις περιπτώσεις εκείνο που απαιτείται από την πλευρά του χρήστη είναι να δράσει γρήγορα, για να περιορίσει τις τυχόν βλάβες που μπορούν να δημιουργηθούν. Να σημειώσουμε επίσης ότι υπάρχουν και κάποιοι ιοί που μοιάζουν με... φαντάσματα. Πολλοί χρήστες αναφέρονται σ' αυτούς αλλά κανείς δεν τους έχει δει να λειτουργούν στην πράξη. Στην πραγματικότητα πρόκειται για διαδόσεις, οι οποίες όμως πολλές φορές προκαλούν πανικό στους ανυποψίαστους χρήστες.

Αν ο χρήστης συμμετέχει σε κάποιο newsgroup ή σε μία δημοφιλή mailing list, η ενημέρωσή του για τους πιο επικίνδυνους ιούς είναι άμεση. Ανεξάρτητα από το θέμα που συζητιέται, κάποιος θα τον ενημερώσει για την ύπαρξη ενός νέου ιού. Υπάρχουν newsgroups και mailing lists όπου συζητούνται αποκλειστικά θέματα που έχουν να κάνουν με τη δημιουργία και την αντιμετώπιση των ιών. Οι διευθύνσεις των μεγαλύτερων εταιρειών κατασκευής antivirus προγραμμάτων, διαθέτουν εκτενείς καταλόγους και αναλυτικές πληροφορίες για τους ιούς και οι περισσότεροι διανέμουν public-domain προϊόντα που θωρακίζουν σε μεγάλο βαθμό το σύστημά**.**

2.2. Spam mails

Spam ή junk mails είναι τα μηνύματα με ενοχλητικό ή και δυσάρεστο για τον παραλήπτη περιεχόμενο. Στα spam mails συγκαταλέγονται ανεπιθύμητες διαφημίσεις για προϊόντα, υπηρεσίες και ιστοχώρους, καθώς επίσης και διάφοροι άλλοι τύποι e-mail (π.χ.ανεπιθύμητα newsletters).Τα μηνύματα αυτά αποτελούν μία πρακτική που απαγορεύεται από την Δεοντολογία του Internet και από τις νομοθεσίες των περισσότερων ευρωπαϊκών κρατών. Αυτό συμβαίνει γιατί τίθεται σε κίνδυνο η ασφάλεια των προσωπικών δεδομένων των χρηστών του Internet και κινδυνεύει η ασφάλεια των δικτύων.

Ο χρήστης θα πρέπει να προσέχει ιδιαίτερα να μην απαντάει σε μηνύματα τέτοιου είδους, ούτε και σε αυτά με την ένδειξη "remove me from the mailing list", τα οποία αντί να αποσύρουν την ηλεκτρονική του διεύθυνση, όπως υπόσχονται, επιβεβαιώνουν ότι είναι ενεργή και συνεχίζουν να βομβαρδίζουν τα εισερχόμενα του χρήστη με μεγαλύτερη συχνότητα.

Ο χρήστης μπορεί να χρησιμοποιήσει τα φίλτρα που του προσφέρουν τα περισσότερα web mail για να διαγράφει τα μηνύματα αυτά, ή να ρυθμίσει κατάλληλα το πρόγραμμα διαχείρισης αλληλογραφίας του υπολογιστή του (συνηθέστερα το outlook express), μέσω των επιλογών που δίνονται από τις καρτέλες στο μενού του προγράμματος. Επίσης, στο Διαδίκτυο υπάρχουν

προγράμματα καταπολέμησης των spam mails, τα οποία μπορούν να εγκατασταθούν τοπικά και να ελέγχουν την εισερχόμενη αλληλογραφία του χρήστη.

Εάν στέλνετε ή λαμβάνετε μηνύματα ηλεκτρονικού ταχυδρομείου, συχνά λαμβάνετε και μηνύματα spam, και μάλιστα ίσως μια πληθώρα από μηνύματα spam. Έχετε αναρωτηθεί ποτέ γιατί λαμβάνετε τόσο μεγάλη ποσότητα άχρηστης αλληλογραφίας; Πρόκειται για μία κερδοφόρα επιχείρηση. Το κόστος αποστολής εκατομμυρίων, ακόμη και δισεκατομμυρίων μηνυμάτων ηλεκτρονικού ταχυδρομείου είναι χαμηλό. Σκεφτείτε: Εάν ακόμη και ένα ελάχιστο ποσοστό από τα εκατοντάδες εκατομμύρια ατόμων αποκριθούν στο μήνυμα και αγοράσουν κάτι, πρόκειται για αρκετά μεγάλο αριθμό! Λοιπόν, τι μπορείτε να κάνετε εσείς για τα μηνύματα spam; Αρκετά, όπως θα δείτε και παρακάτω. Ας εξετάσουμε μερικούς τρόπους για να σταματήσετε τον κατακλυσμό.

2.2.1. Τακτικές για αποφυγή των ανεπιθύμητων μηνυμάτων ηλεκτρονικού ταχυδρομείου (spam)

1. Δημιουργήστε μία διεύθυνση ηλεκτρονικού ταχυδρομείου αποκλειστικά για συναλλαγές στον Ιστό.
2. Σκεφτείτε τη χρήση κάποιας υπηρεσίας του Ιστού δωρεάν ηλεκτρονικού ταχυδρομείου, για τη δημιουργία ενός λογαριασμού που μπορείτε να χρησιμοποιείτε στις ηλεκτρονικές σας συναλλαγές. Έτσι θα μπορέσετε να διατηρήσετε την διεύθυνση σας ηλεκτρονικού ταχυδρομείου που σας έχει εκχωρηθεί από κάποιο πάροχο υπηρεσιών Διαδικτύου (ISP) ή σας έχει δοθεί στον επαγγελματικό σας χώρο απόρρητη.
3. Να δίνετε την προσωπική σας διεύθυνση ηλεκτρονικού ταχυδρομείου μόνον σε άτομα που γνωρίζετε.
4. Μην καταχωρίζετε τη διεύθυνση ηλεκτρονικού ταχυδρομείου σε μεγάλους καταλόγους του Διαδικτύου. Μην την αναφέρετε ούτε καν στην δική σας διαδικτυακή τοποθεσία.
5. Συγκαλύψτε (ή "μασκάρετε") τη διεύθυνση ηλεκτρονικού ταχυδρομείου.
6. Χρησιμοποιήστε μια "μασκαρισμένη" διεύθυνση όταν ανακοινώνετε ¨τη διεύθυνσή σας σε ομάδα συζήτησης, σε κανάλι συνομιλίας ή σε ηλεκτρονικό πίνακα ανακοινώσεων. Για παράδειγμα, θα μπορούσατε να δώσετε την ηλεκτρονική σας διεύθυνση ως "s0me0ne@example.c0m" χρησιμοποιώντας "0" (μηδέν) αντί για το "o." Κάποιο πρόσωπο μπορεί να καταλάβει τη διεύθυνσή σας, αλλά τα αυτοματοποιημένα προγράμματα που χρησιμοποιούν οι αποστολείς μηνυμάτων spam δεν μπορούν.
7. Προσέχετε τα πλαίσια επιλογών.
8. Όταν αγοράζετε αντικείμενα από το Διαδίκτυο, οι εταιρείες συνήθως προσθέτουν ένα πλαίσιο επιλογής (προεπιλεγμένο!) το οποίο υποδεικνύει ότι συμφωνείτε να πωλήσουν ή να δώσουν την διεύθυνσή σας ηλεκτρονικού ταχυδρομείου σε υπεύθυνα πρόσωπα. Κάντε κλικ στο πλαίσιο επιλογής για να το απο-επιλέξετε.
9. Ελέγξτε τις πολιτικές απορρήτου των διαδικτυακών τοποθεσιών
10. Όταν εγγράφεστε σε υπηρεσίες που βασίζονται στον Ιστό, όπως ηλεκτρονικές τραπεζικές συναλλαγές, αγορές ή δελτία ενημέρωσης, εξετάστε προσεκτικά την πολιτική απορρήτου προτού αποκαλύψετε τη δική σας διεύθυνση ηλεκτρονικού ταχυδρομείου. Η πολιτική απορρήτου θα εξηγεί τους όρους και τις περιπτώσεις σχετικά με το εάν ή το πώς η τοποθεσία θα κοινοποιήσει τα δεδομένα σας. (Εάν δεν διαβάσετε κάποια δήλωση, πιθανόν να "συμφωνήσετε" στην κοινοποίηση των προσωπικών σας δεδομένων, χωρίς να το γνωρίζετε.)
11. Εάν κάποια διαδικτυακή τοποθεσία δεν διαθέτει δήλωση απορρήτου, φροντίστε να είστε προσεκτικός και επικοινωνήστε πρώτα με τους ιδιοκτήτες της τοποθεσίας, προτού κοινοποιήσετε σημαντικές πληροφορίες.

12. Εάν η διαδικτυακή τοποθεσία δεν εξηγεί τον τρόπο με τον οποίο θα χρησιμοποιήσει τα προσωπικά σας δεδομένα, ξανασκεφτείτε το, προτού τα δώσετε. Πρέπει επίσης να γνωρίζετε ότι πολλές εταιρείες—ακόμη και νόμιμες—ενδέχεται να κοινοποιήσουν τα προσωπικά σας δεδομένα με ανεπιθύμητους για σας τρόπους.

2.2.2. Χειρισμός των ανεπιθύμητων μηνυμάτων ηλεκτρονικού ταχυδρομείου (spam)

Αν παρ' όλες τις προσπάθειές σας, έχετε λάβει μηνύματα ηλεκτρονικού ταχυδρομείου, τι θα πρέπει να κάνετε; Πρώτον, να τα αγνοήσετε, γιατί αν απαντήσετε, θα δεχτείτε ακόμη περισσότερα ανεπιθύμητα μηνύματα. Δεύτερον, να κοινοποιήσετε τα στοιχεία του αποστολέα τους.

Πιο συγκεκριμένα:

Βήμα 1: Αγνοήστε την ανεπιθύμητη ηλεκτρονική αλληλογραφία

1) Μην απαντάτε στα μηνύματα spam, ούτε καν για "διακοπή της συνδρομής." Εάν απαντήσετε σε μηνύματα spam, απλώς επιβεβαιώνετε ότι η δική σας διεύθυνση ηλεκτρονικού ταχυδρομείου είναι έγκυρη και χρησιμοποιείται. Οι αποστολείς άχρηστων μηνυμάτων ηλεκτρονικού ταχυδρομείου ίσως τότε να σας στείλουν περισσότερα μηνύματα spam ή να πουλήσουν τους καταλόγους τους σε τρίτους.

2) Προσέχετε τα πλαστά μηνύματα ηλεκτρονικού ταχυδρομείου. Τα πλαστά μηνύματα είναι αντιγραμμένα νόμιμα μηνύματα ηλεκτρονικού ταχυδρομείου, όπως τα ενημερωτικά δελτία κάποιας εταιρείας. Τα πλαστά μηνύματα μπορεί να χρησιμοποιηθούν για να σας παρασύρουν να μεταφορτώσετε έναν ιό ή να στείλετε προσωπικά δεδομένα, όπως ο αριθμός της πιστωτικής κάρτας. Όταν αμφιβάλλετε, επικοινωνήστε με την εταιρεία που πιστεύετε πως έστειλε το μήνυμα.

3) Μην απαντάτε στα μηνύματα ηλεκτρονικού ταχυδρομείου που σας ζητούν πληροφορίες. Οι περισσότερες νόμιμες εταιρείες δεν θα σας ζητήσουν προσωπικά δεδομένα μέσω ηλεκτρονικού ταχυδρομείου. Εάν κάποια εταιρεία που εμπιστεύεστε (π.χ. η εταιρεία της πιστωτικής σας κάρτας) σας γράψει για να σας ζητήσει προσωπικά δεδομένα, μην γράψετε και αναφέρτε το. Φροντίστε να χρησιμοποιήσετε έναν αριθμό τηλεφώνου που έχετε βρει ο ίδιος από τον χρυσό οδηγό, από έντυπο τραπεζικής ενημέρωσης, από λογαριασμό ή από άλλη πηγή. (Μην χρησιμοποιήσετε τον αριθμό που υπάρχει στο μήνυμα ηλεκτρονικού ταχυδρομείου). Εάν πρόκειται για νόμιμο αίτημα, η τηλεφωνήτρια θα μπορέσει να σας εξυπηρετήσει.

4) Μην αγοράζετε τίποτα από μηνύματα ηλεκτρονικού ταχυδρομείου spam. Πολλοί αποστολείς μηνυμάτων spam παίρνουν ποσοστά από τις αγορές των αντικειμένων που διαφημίζουν. Αντισταθείτε στον πειρασμό να αγοράσετε τα προϊόντα τους εάν δεν θέλετε να μπείτε σε περισσότερες λίστες διευθύνσεων αποστολής άχρηστων μηνυμάτων.

5) Σε καμία περίπτωση μην δίνετε χρήματα για φιλανθρωπία μέσω μηνυμάτων spam. Δυστυχώς, ορισμένοι αποστολείς μηνυμάτων spam κερδίζουν από τις καλές σας προθέσεις. Εάν δεχτείτε μια έκκληση για φιλανθρωπία, αντιμετωπίστε την ως μήνυμα spam. Εάν πρόκειται για φιλανθρωπικό σκοπό που θέλετε να υποστηρίξετε, καλέστε τους και μάθετε με ποιόν τρόπο μπορείτε να συνεισφέρετε. Ωστόσο, ποτέ μην στέλνετε πληροφορίες μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου.

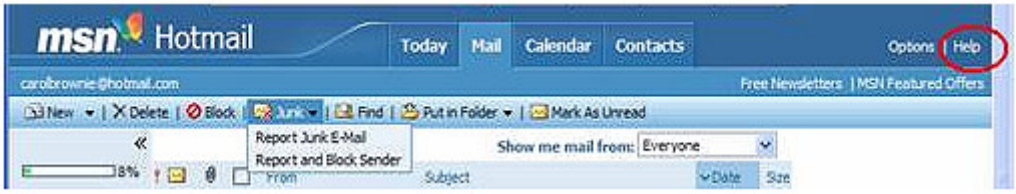
6) Προσέχετε ιδιαίτερα προτού ανοίξετε συνημμένα αρχεία, ακόμη κι αν γνωρίζετε τον αποστολέα. Εάν δεν μπορείτε να επιβεβαιώσετε ότι το μήνυμα είναι έγκυρο και ότι το συνημμένο είναι ασφαλές, διαγράψτε το μήνυμα αμέσως και εκτελέστε κάποιο ενημερωμένο πρόγραμμα προστασίας από ιούς για να ελέγξετε την ύπαρξη ιών στον υπολογιστή σας.

7) Μην προωθείτε αλυσιδωτά μηνύματα ηλεκτρονικού ταχυδρομείου. Τα αλυσιδωτά μηνύματα μπορεί να είναι φάρσες ή ακόμη και συστήματα μετάδοσης ιών. Και, επιπλέον, δεν γνωρίζετε πλέον ποιος γνωρίζει την ηλεκτρονική σας διεύθυνση. Επιπροσθέτως, έχει αναφερθεί ότι οι αποστολείς μηνυμάτων spam χρησιμοποιούν αλυσιδωτά μηνύματα για να συλλέξουν διευθύνσεις

ηλεκτρονικού ταχυδρομείου. Για να ελέγξετε την εγκυρότητα κάποιου αλυσιδωτού μηνύματος ή κάποιας ενδεχόμενης φάρσας, μεταβείτε στην διαδικτυακή τοποθεσία Hoaxbusters. http://hoaxbusters.ciac.org

Βήμα 2: Κοινοποιήστε την άχρηστη αλληλογραφία και τον αποστολέα της

1) Εάν χρησιμοποιείτε το MSN Hotmail, αναφέρετε τα άχρηστα μηνύματα ηλεκτρονικού ταχυδρομείου, πριν ακόμη τα ανοίξετε. Για να μάθετε πως, κάντε κλικ στο κουμπί Help (Βοήθεια), στο δεξί άκρο της οθόνης και κάντε κλικ στο Filters and Junk E-Mail (Φίλτρα και Άχρηστη αλληλογραφία). Στη συνέχεια κάντε κλικ στο Report junk e-mail (Αναφορά άχρηστης ηλεκτρονικής αλληλογραφίας).



2) Προωθήστε το μήνυμα spam στον Πάροχο υπηρεσιών Διαδικτύου (ISP) του αποστολέα μηνυμάτων spam. Εάν λάβετε ανεπιθύμητη ηλεκτρονική αλληλογραφία, η διεύθυνση του αποστολέα θα εμφανίσει το όνομα του Παρόχου μετά από το σύμβολο @. Εάν προήλθε από τον MSN.com, προωθήστε ολόκληρο το ηλεκτρονικό μήνυμα, μαζί με την κεφαλίδα, στη διεύθυνση abuse@hotmail.com. Εάν το μήνυμα spam προέρχεται από άλλον πάροχο, προωθήστε τις κεφαλίδες (ακολουθώντας τις παραπάνω οδηγίες) στη διεύθυνση παρενόχλησης που διαθέτει ο πάροχος για παράδειγμα, δοκιμάστε abuse@<όνομα παρόχου>.com.

3) **Χρησιμοποιήστε το Κεντρικό γραφείο διαλογής δικτυακών παρενοχλήσεων** για βοήθεια σχετικά με την προώθηση των παραπόνων σας σε διαχειριστές συστημάτων, οι οποίοι μπορούν να ενεργήσουν κατάλληλα

2.3 Ηλεκτρονικά μηνύματα με hoaxes

Πρόκειται για μηνύματα ηλεκτρονικού ταχυδρομείου ψευδούς προειδοποίησης, αναγγελίας ή ενημέρωσης.

Πιο συγκεκριμένα τα μηνύματα αυτά είναι:

1. «Προειδοποιητικά»: είτε ειδοποιούν στο χρήστη για την ύπαρξη ιού ή άλλου τύπου απειλής στο λειτουργικό του σύστημα και τον συμβουλεύουν να προβεί σε ορισμένες ενέργειες, είτε προειδοποιούν για πιθανές επιθέσεις από ιούς, που στην πραγματικότητα δεν αποτελούν απειλή για το σύστημα
2. «Συμπαράστασης»: παρουσιάζουν υποθετικά προβλήματα κάποιου ανθρώπου (συχνότατα αναφορές σε παιδιά που πάσχουν από σοβαρές ασθένειες) και ζητούν την κινητοποίηση όσο περισσότερων χρηστών γίνεται
3. «Εκφοβισμού»: οποιουδήποτε τύπου αλυσιδωτές επιστολές που εκφοβίζουν το χρήστη ότι θα του συμβεί κάτι αν δεν προωθήσει το μήνυμα και σε άλλους χρήστες.

Ο ουσιαστικός κίνδυνος από αυτά τα μηνύματα είναι κυρίως η τεράστια διάδοσή τους και, κατά συνέπεια, η επιβάρυνση των λογαριασμών των χρηστών με άχρηστα μηνύματα. Εκτός αυτού, δημοσιοποιούνται ευρέως και πολλές διευθύνσεις ηλεκτρονικού ταχυδρομείου, καθιστώντας τους ιδιοκτήτες τους ευκολότερα θύματα κάθε τέτοιου είδους ενοχλήσεως.

Τα μηνύματα αυτού του τύπου συνοδεύονται συχνά από την τυποποιημένη φράση «στείλτε αυτό το μήνυμα σε όσο περισσότερους χρήστες γνωρίζετε» ("send this to everyone you know").

Στην περίπτωση των «προειδοποιητικών» μηνυμάτων εμφανίζονται ως αποστολείς μεγάλες και γνωστές εταιρείες, με σκοπό να ξεγελάσουν το χρήστη και να τον κάνουν να εμπιστευτεί το περιεχόμενο του μηνύματος. Ο χρήστης πρέπει να αγνοήσει όλα τα μηνύματα τέτοιου τύπου, να τα διαγράψει χωρίς φόβο και, κυρίως, να μην τα προωθήσει σε γνωστούς του και προκαλεί άνευ λόγου πανικό. Τα γνωστά αντιβιοτικά προγράμματα συνήθως φιλτράρουν τα καταγεγραμμένα μηνύματα αυτού του είδους, ενώ είναι αρκετές οι εταιρείες που ζητούν από τους χρήστες των προγραμμάτων τους να τις ενημερώνουν όταν δέχονται τέτοιου είδους μηνύματα, για να προβούν στις κατάλληλες ενέργειες ενημέρωσης των αντιβιοτικών τους προγραμμάτων.

2.4. Επίθεση με καταιγισμό ηλεκτρονικών μηνυμάτων (E-mail bombing)

Το e-mail bombing από πολλούς δεν θεωρείται ως Denial of Service Attack. Denial of Service Attack έχουμε όταν ένα τερματικό πάψει να λειτουργεί, τότε ο επιτιθέμενος επικοινωνεί με άλλα μηχανήματα του ίδιου δικτύου "υποκρινόμενος" ότι τα πακέτα που στέλνει προέρχονται από το αχρηστεμένο και εκτός λειτουργίας πλέον τερματικό. Με τον τρόπο αυτό αυξάνονται σημαντικά οι πιθανότητες να επιτευχθεί πρόσβαση στα άλλα μηχανήματα του δικτύου, καθώς η εντολή πρόσβασης δεν δίνεται από έναν τρίτο, αλλά από μια έμπιστη πηγή (ένα μηχάνημα εντός του δικτύου), το E-mail bombing είναι πολύ αποτελεσματικό όταν χρησιμοποιείται εναντίον υπολογιστών οι οποίοι διαχειρίζονται mail. Το μόνο που έχει να κάνει κανείς είναι να τους στείλει τόσα πολλά (σε μέγεθος και αριθμό) email μηνύματα, ώστε ο φόρτος των εργασιών διαχείρισής τους να οδηγήσει το σύστημα σε κατάρρευση.

2.5. Ηλεκτρονικά μηνύματα και προσωπικά δεδομένα

Ο χρήστης των προγραμμάτων αλληλογραφίας πρέπει να είναι ιδιαίτερα προσεκτικός και να μην εκθέτει ποτέ μέσα στα μηνύματα του προσωπικά του στοιχεία, καθώς και αριθμούς πιστωτικών καρτών ή οποιαδήποτε άλλα δεδομένα. Τα e-mails είναι από τους συνηθέστερους στόχους των κάθε είδους hackers, οι οποίοι μπορούν να υποκλέψουν όλα τα στοιχεία. Μια καλή τακτική είναι η συχνή αλλαγή του κωδικού πρόσβασης του λογαριασμούς e-mail.

Ιδιαίτερη προσοχή χρειάζεται η διαχείριση λογαριασμών web mail, οι οποίοι είναι πολύ πρακτικοί και διαθέσιμοι από παντού, αλλά και με χαμηλό δείκτη προστασίας προσωπικών δεδομένων. Σε αυτούς τους λογαριασμούς συχνά παρέχεται επιλογή για απομνημόνευση του ονόματος χρήστη και του κωδικού στον υπολογιστή, ώστε ο χρήστης να μην πληκτρολογεί κανένα από τα στοιχεία του κάθε φορά που συνδέεται από τον ίδιο υπολογιστή ("Απομνημόνευση του ID μου σε αυτό τον υπολογιστή"). Το πρώτο μέτρο προστασίας είναι η μη ενεργοποίηση της παραπάνω επιλογής [1]

3. Βήματα για την προστασία του διακομιστή της βιβλιοθήκης μας

Μετά από τη γενική παρουσίαση των πρακτικών ασφαλείας του ηλεκτρονικού υπολογιστή από ιούς ή ενοχλητικά μηνύματα, παρατίθενται τα συγκεκριμένα βήματα για την προστασία του συστήματος μιας βιβλιοθήκης.

- Πρέπει να καθοριστεί μια συγκεκριμένη πολιτική ασφαλείας, η οποία να ακολουθείται πιστά
- Φιλτράρισμα πακέτων στα πλαίσια ενός firewall ή ενός δρομολογητή που έχει δυνατότητες φιλτραρίσματος.
- Τα εργαλεία λογισμικού και οι τεχνικές που χρησιμοποιούνται για την ασφάλεια του συστήματος πρέπει να ενημερώνονται συνεχώς.
- Συνεχής εκπαίδευση των Web administrators αλλά και των βιβλιοθηκονόμων που χρησιμοποιούν το σύστημα

- Καθημερινοί έλεγχοι ορθότητας (auditing) και περιοδικοί έλεγχοι για αδυναμίες του συστήματος.
- Σύσταση μιας λίστας χρηστών, στους οποίους θα επιτρέπεται η πρόσβαση σε εμπιστευτικά έγγραφα.
- Απενεργοποίηση όλων εκείνων των εφαρμογών που δε χρησιμοποιούνται από τον διακομιστή.
- Προστασία όλων των υπηρεσιών που παρέχονται από το σύστημα που "φιλοξενεί" τον διακομιστή (smtp, ftp κ.λ.π).
- Χρήση ασφαλών πρωτοκόλλων για την επικοινωνία με το υπόλοιπο Internet (shttp, SSL,RSA κ.λ.π) [2].
- Έλεγχος των δεδομένων που εισάγουν απομακρυσμένοι χρήστες στα πεδία μιας HTML φόρμας, ώστε να ανιχνεύονται "κακόβουλα" δεδομένα (π.χ shell μετα- χαρακτήρες).

4. Κοινωνική μηχανική (social engineering) σε βιβλιοθήκες

Ο όρος social engineering χρησιμοποιήθηκε σε μεγάλη έκταση από τον Kevin Mitnick για να δηλώσει την παράνομη ανάληψη κάποιου ρόλου από τον επιτιθέμενο για την απόκτηση σημαντικών πληροφοριών ή αρχείων.[2] Οι βασικοί στόχοι της κοινωνικής μηχανικής στο χώρο μιας βιβλιοθήκης είναι οι ίδιοι με αυτή του hacking γενικά: να κερδίσει κάποιος αναρμόδια πρόσβαση στα συστήματα ή τις πληροφορίες της βιβλιοθήκης με σκοπό να διαπράξει απάτη, να κερδίσει πρόσβαση στο ηλεκτρονικό της δίκτυο, ή απλά να αναστατώσει το σύστημα ή το δίκτυο της. Μα είναι δυνατόν, θα αναρωτηθεί κάποιος, μια βιβλιοθήκη να αποτελέσει στόχο ενός κοινωνικού μηχανικού; Η απάντηση είναι φυσικά και μπορεί. Οι κοινωνικοί μηχανικοί διψούν για πληροφορίες και οι δικτυωμένες βιβλιοθήκες στις μέρες μας συγκεντρώνουν μεγάλο όγκο πολύτιμου υλικού.

Ο εντοπισμός και η αναφορά πραγματικών περιπτώσεων κοινωνικών επιθέσεων εφαρμοσμένης μηχανικής είναι δύσκολη. Βιβλιοθήκες που έχουν πέσει θύματα επίθεσης είτε δεν θέλουν να αναγνωρίσουν ότι έχουν καταστεί θύματα (το να αναγνωρίσει μια θεμελιώδη παραβίαση ασφάλειας για μια βιβλιοθήκη είναι όχι μόνο ενοχλητική, αλλά συνάμα και καταστρεπτική για τη φήμη της) είτε η επίθεση δεν ήταν καλά τεκμηριωμένη και κανείς δεν είναι πραγματικά σίγουρος εάν υπήρξε επίθεση κοινωνικού μηχανικού ή όχι.

Οι επιθέσεις κοινωνικής μηχανικής πραγματοποιούνται σε δύο επίπεδα: φυσικό και ψυχολογικό. Κατ' αρχάς, θα εστιάσουμε από πού ένας κοινωνικός μηχανικός μπορεί να βρει υλικό για να εξαπολύσει μια επίθεση:

1. Ο χώρος της βιβλιοθήκης από τη στιγμή που είναι και χώρος υποδοχής ατόμων μπορεί να φιλοξενήσει και κοινωνικούς μηχανικούς που θα περιφέρονται ψάχνοντας να βρουν μια ανθρώπινη αδυναμία και να την εκμεταλλευτούν είτε αποκτώντας πρόσβαση στο δίκτυο της βιβλιοθήκης συλλέγοντας υλικό που δεν είναι διαθέσιμο στο κοινό είτε αποσπώντας βιβλία με την ανοχή μας παριστάνοντας πως είναι κάποιοι άλλοι. Για αυτό το λόγο θα ήταν πολύ συνετό αν κατά την είσοδο στη βιβλιοθήκη κάθε άτομο όφειλε να πιστοποιήσει ότι είναι αυτός που ισχυρίζεται πως είναι. Μια επίδειξη αστυνομικής ταυτότητας ή κάρτα μέλους της βιβλιοθήκης καθώς και η καταγραφή των επισκεπτών σε μια βάση δεδομένων θα αποτελούσε μια καλή λύση.
2. Το τηλέφωνο της βιβλιοθήκης επίσης μπορεί να αποτελέσει στόχο ενός κοινωνικού μηχανικούς φέρουμε ένα παράδειγμα όμως για να γίνουμε πιο κατανοητοί. Τηλεφωνεί κάποιος άγνωστος και ισχυρίζεται πως είναι από την εταιρεία που συντηρεί τους ηλεκτρονικούς υπολογιστές της βιβλιοθήκης. Μας ενημερώνει πως έχει προκύψει ένα πρόβλημα με τους υπολογιστές και ύστερα από εντολή της διεύθυνσης αυτό πρέπει να διορθωθεί άμεσα. Λέει λοιπόν πως πρέπει να κατεβάσουμε από το διαδίκτυο ένα αρχείο που θα ρυθμίσει το πρόβλημα. Ευγενικότατος και με πολύ υπομονή μας οδηγεί, αφού

κατεβάσουμε το αρχείο, βήμα προς βήμα προς την επίλυση του δήθεν προβλήματος. Το αρχείο αυτό δεν έχει καν installation mode κάτι που μας παρακινεί την περιέργεια αλλά ο κοινωνικός μηχανικός μας καθησυχάζει λέγοντας μας πως πρόκειται για αρχεία άλλου τύπου. Μόλις τελειώσουμε μας ευχαριστεί και κλείνει το τηλέφωνο αφού έχει αποκτήσει πρόσβαση στον υπολογιστή μας ή ακόμα χειρότερα και σε όλο το δίκτυο της βιβλιοθήκης μας. Πράγματι άθελα μας ανοίξαμε μια κεκρόπορτα γιατί το αρχείο που θα επίλυε το πρόβλημα τελικά αποδεικνύεται Trojan Horse με ότι αυτό συνεπάγεται. Ποια όμως θα έπρεπε να είναι τα βήματα μας σε όλη αυτή την διαδικασία; Αρχικά έπρεπε να πιστοποιήσουμε πως ο άνθρωπος που μας τηλεφώνησε ήταν αυτός που ισχυριζόταν και μετά θα έπρεπε να ελέγξουμε το αρχείο που κατεβάσαμε με ένα πρόγραμμα antivirus πριν το εγκαταστήσουμε στον υπολογιστή μας.

Η αλήθεια είναι πως κανείς δεν είναι απρόσβλητος στις επιθέσεις ενός κοινωνικού μηχανικού. Ο ρυθμός της ζωής μας είναι τέτοιος που δεν έχουμε συχνά χρόνο να σκεφτούμε τις αποφάσεις μας ακόμα και για ζητήματα σημαντικά. Πολύπλοκες καταστάσεις, έλλειψη χρόνου, τεταμένη συναισθηματική κατάσταση ή πνευματική κούραση μπορούν εύκολα να μας αποσπάσουν. Οπότε παίρνουμε κάποιες αποφάσεις χωρίς να αναλύσουμε τις πληροφορίες προσεκτικά και πλήρως. Αυτή η πνευματική διαδικασία που είναι γνωστή με το όνομα αυτόματη αντίδραση μπορεί να συμβεί ακόμα και σε αρχηγούς κρατών. [2].

Συμπέρασμα

Από αυτή την εργασία καταδεικνύεται ότι ο σύγχρονος βιβλιοθηκονόμος πρέπει να αντιμετωπίζει με μεγάλη προσοχή τα προβλήματα ασφαλείας στη βιβλιοθήκη του αφενός παίρνοντας όλα τα απαραίτητα τεχνικά μέτρα (αντιμετώπιση ιών, spam mails κλπ.) και αφετέρου όντας σε εγρήγορση ώστε να μην πέσει θύμα ενεργειών κοινωνικού μηχανικού.

Βιβλιογραφία

[1] http://www.microsoft.com/hellas/security/protect/
[2] Κέβιν Μίτνικ & Ουίλιαμ Σάιμον, "Η τέχνη της απάτης", Αθήνα: Ωκεανίδα [2003]
Τίτλος πρωτοτύπου Kevin Mitnick & William L. Simon, *The art of deception. Controlling the human element of security.*

[3] Ανδρέας Πομπόρτσης, Γεώργιος Παπαδημητρίου "*Ασφάλεια δικτύων υπολογιστών*", Αθήνα: Τζιόλα [2003]
[4] Lincoln D. Stein "*Ασφάλεια δικτύων Web*''
[5] Atkins Derek, "*Internet Security*", New Riders Publishing
[6] University of Cambridge Computer Laboratory
http://www.cl.cam.ac.uk/Research/Security/OtherSites/
[7] L.D.Stein and J.N. Stewart, "The World Wide Web Security Faq",
http://www.w3.org/Security/Faq
[8] R. Oppliger, "Internet and Intranet Security", Artech House [1998]
[9] L.D.Stein, "Web Security", Addison Wesley, [1997]
[10] W.Stallings. "Cryptography and Network Security", Prentice Hall [1999]
[11] Internet Security (Library of Congress)
http://lcweb.loc.gov/global/internet/security.html
[12] Computer Security Information
http://www/alw.nih.gov/Security/security.html