Θέματα Ασφάλειας Προσωπικού Υπολογιστή & Δικτύων Η/Υ

- Πιθανές απειλές από το διαδίκτυο
  - Τύποι Ηλεκτρονικών Μολύνσεων
  - Πειρατεία Πόρων
  - Ανεπιθύμητη Αλληλογραφία
  - “Ψάρεμα” (Phishing)
- Άσκοπη επιβάρυνση δικτύου
- Τρόποι αποτελεσματικής προστασίας
  - Μέσω ειδικού λογισμικού
  - Χρήση κωδικών πρόσβασης
  - Κατά τη χρήση ηλεκτρονικής αλληλογραφίας (email)
  - Κατά την περιήγηση στο internet

Ηλεκτρονικές Μολύνσεις - Ιοί

- Οι γνωστοί ιοί (viruses)
  - Ηλεκτρονικού Ταχυδρομείου. Κυρίως ως επισυναπτόμενο
  - Σκουλήκια (worms), Αυτό-εξαπλώμενοι
  - Σε αρχεία (πλέον σπάνιο)

- Ένας ιός αποτελείται από
  - Μηχανισμό εξάπλωσης (π.χ. μέσω email)
  - Μηχανισμός ενεργοποίησης (*trigger*)
    - Trigger = πλήρωση κάποιας συνθήκης (ημερομηνία, αριθμός μολύνσεων, συμπεριφορά χρήστη)
  - Μηχανισμός μόλυνσης (τροποποίηση λειτουργικού, αρχείων κτλ)

Ηλεκτρονικές Μολύνσεις - Ιοί

- Συνέπειες
  - απλή ενόχληση ή καθυστέρηση που μπορεί να εξελιχθεί σε denial-of-service attack (DoS attack)
  - Μερική ή ολική καταστροφή των δεδομένων μας (format c:, Del *.*)
  - Καταγραφή κωδικών και αποστολή σε συγκεκριμένο παραλήπτη. Εδώ η ζημιά είναι πολύ ύπουλη ακόμα και να έχουμε καθαρίσει το ιό
  - Αποστολή αρχείων από my documents σε τυχαίους παραλήπτες από τα contacts μας στο λογισμικό διαχείρισης της αλληλογραφίας (π.χ. Outlook)

Ηλεκτρονικές Μολύνσεις - Malicious Software

- Malicious Software – Κακόβουλο Λογισμικό
  - Spyware - Κατασκοπευτικό λογισμικό.
    - Αναφέρει σε εμπορικές εταιρίες δραστηριότητα χρηστών και συνήθειες (τι sites προτιμούν, τι αγοράζουν, τι μουσική ακούν)
    - Συνέπειες: αργοπορία του υπολογιστή, δικτύου κτλ.
    - Ο χρήστης εξαπατάται στο να τα εγκαταστήσει. Συνήθως συνοδεύονται από δωρεάν χρήσιμες λειτουργίες (hotbar, smilies, screen savers)
  - Addware – Διαφημίσεις
    - Προβολή διαφημίσεων στο χρήστη
    - Κύρια συνέπεια: αργοπορία του δικτύου και υπολογιστή, ενοχλητικά pop-ups
    - Συνήθως είναι μέρος «δωρεάν» προγραμμάτων (που το κόστος τους το εισπράττουν από τις εταιρίες που πληρώνουν για τις διαφημίσεις)
  - Key loggers – υποκλοπείς δεδομένων
    - υποκλοπείς πληροφοριών που πληκτρολογούμε, βλέπουμε, κτλ (κρυφά από τον χρήστη)
    - Συνέπειες: διαρροή ευαίσθητων πληροφοριών (passwords, usernames, urls, mail) σε τρίτους με σκοπό συνήθως την απάτη.

Ηλεκτρονικές Μολύνσεις - Malicious Software

- Malicious Software – Κακόβουλο Λογισμικό
  - Trojans – Δούρειοι Ίπποι
    - Προγράμματα που εξαπατούν το χρήστη (εμφανίζονται ως παιχνίδια, εικόνες κτλ) με κρυφές λειτουργίες (backdoors, key loggers). Ο χρήστης ξεγελιέται ανοίγοντας
    - Συνέπειες: Απομακρυσμένος μη εξουσιοδοτημένος έλεγχος υπολογιστή από κακόβουλα τρίτα άτομα (hackers), υποκλοπή στοιχείων, καταστροφή στοιχείων, DoS.
    - Πολλές φορές τα Trojans εγκαθίστανται χωρίς άμεση ενέργεια του χρήστη (πχ από ένα κενό ασφαλείαστου Internet Explorer)
  - Dialers - Τηλεφωνητές
    - Προγράμματα που αφού τερματίσουν την υπάρχουσα (pstn ή isdn) σύνδεση με το internet καλούν σε αριθμούς υψηλής χρέωσης (εσωτερικού ή εξωτερικού), χρεώνοντας υπέρογκα τον λογαριασμό τηλεφώνου του χρήστη.
    - Συνέπειες: Υψηλή χρέωση τηλεφώνου
    - Συνήθως «πλασάρονται» σαν απαραίτητο λογισμικό για πρόσβαση σε κάποια «δωρεάν» υπηρεσία (προβολή δωρεάν video, δωρεάν πρόσβαση σε δικτυακούς τόπους πορνογραφικού περιεχομένου).

Πειρατεία Πόρων

- Κακόβουλοι χρήστες (hackers ή ακόμα και υπάλληλοι εντός του οργανισμού) χρησιμοποιούν υπολογιστικούς πόρους (πχ δίσκος, network bandwidth).
- Οι πόροι μπορούν τώρα να χρησιμοποιηθούν για διακίνηση άσεμνου υλικού, πειρατικού λογισμικού κτλ. Συνηθισμένο φαινόμενο που δύσκολα γίνεται αντιληπτό.
- Ο mail-server της εταιρίας/οργανισμού χρησιμοποιείται από spammers όπου στέλνουν διαφημιστικά μηνύματα ανά τον κόσμο.
  - Συνέπειες είναι τόσο νομικές όσο και λειτουργικές (ο mail server έχει άσκοπη κίνηση και κατάληψη εύρους ενώ υπάρχει άμεσος κίνδυνος να γίνει blacklisted και να μην λειτουργούν όλα τα mails κανονικά)

Ανεπιθύμητη Αλληλογραφία (Spam Mail)

- Είναι η αλληλογραφία που έρχεται στο ηλεκτρονικό ταχυδρομείο μας χωρίς να έχουμε ζητήσει να μας στείλουν. Συνήθως περιέχει
  - Διαφημίσεις προϊόντων (viagra, φάρμακα, ηλεκτρονικά, software)
  - Διαφημίσεις υπηρεσιών (porn, consulting, έκδοση πλαστά πτυχίων)
  - Απάτες
- Υποκατηγορίες SPAM
  - Αλληλογραφία με αστείο περιεχόμενο (Fun – jokes) όπως *ανέκδοτα, video* κτλ
  - Αλυσίδες (Chain letters) όπως *«..στείλε αυτό το email σε άλλους 10 και θα έχεις καλή τύχη»*.
- Επιπτώσεις
  - Μείωση αποδοτικότητας προσωπικού (ασχολείται με άχρηστα emails)
  - Κατασπατάληση διαθέσιμου εύρους και πόρων στους email servers

Phishing “Ψάρεμα”

- Επιθέσεις μέσω email
- Στο phishing οι επιτιθέμενοι προσπαθούν να εξαπατήσουν νόμιμους χρήστες
  - Συνήθως με emails που φαίνεται να τα έχει στείλει η νόμιμη εταιρία και έχουν την επίσημη εμφάνιση των emails που θα έστελνε αυτή η εταιρία.
  - Τους προτρέπουν να του δώσουν τους κωδικούς τους με προφάσεις ότι τα χρειάζεται το τμήμα ασφαλείας της εταιρείας κτλ.
  - Οι χρήστες οδηγούνται σε **πλαστά web** site που μοιάζουν στο αυθεντικό (πχ ενώ το link γράφει www.bank.gr τελικά σε παραπέμπει σε www.fakebank.gr)
- **ΠΟΤΕ** οι χρήστες δεν πρέπει να δείχνουν σε ΚΑΝΕΝΑΝ προσωπικούς κωδικούς μέσω email. Θα πρέπει να είναι καχύποπτοι.

Επιβάρυνση Δικτύου - Ανεπιθύμητο Λογισμικό

- P2P (Peer to Peer) – Προγράμματα Ανταλλαγής Δεδομένων
  - Προγράμματα για την ανταλλαγή προγραμμάτων (κυρίως πειρατικών), αρχείων (κυρίως πειρατικών) όπως MP3, ταινίες κτλ
  - Συνέπειες: Άσκοπη καθυστέρηση δικτύου εις βάρος άλλων εργαζόμενων-χρηστών. Κατασπατάληση εύρους (bandwidth). Νομικοί κίνδυνοι για τον οργανισμό λόγω διακίνησης παράνομου λογισμικού και δεδομένων. Κίνδυνοι να εισέλθουν ιοί και άλλο κακόβουλο λογισμικό στον οργανισμό.
  - Γνωστά P2P: Kazaa, eMule κτλ
- Instant messaging – Προγράμματα Ανάλλαγης Μηνυμάτων (chat)
  - Προγράμματα γραπτής άμεσης συνομιλίας με παράπλευρες λειτουργίες όπως ανταλλαγή αρχείων.
  - Συνέπειες: Αλόγιστη χρήση κατασπατάληση χρόνου εργασίας. Κίνδυνοι να εισέλθουν ιοί και άλλο κακόβουλο λογισμικό στον οργανισμό.
  - Γνωστά IM: Microsoft Messenger, mIRC, yahoo IM
- Internet Telephony
  - Προγράμματα συνομιλίας φωνής
  - Συνέπειες: Άσκοπη καθυστέρηση δικτύου εις βάρος άλλων εργαζόμενων-χρηστών. Κατασπατάληση εύρους (bandwidth).
  - Γνωστά IT: Skype, Google talk

Επιβάρυνση Δικτύου – Ανεπιθύμητοι Δικτυακοί Τόποι

- Ανεπιθύμητοι δικτυακοί τόποι (κατηγορίες)
  - Πορνογραφικού περιεχομένου
  - Παιδικού πορνογραφικού περιεχομένου
  - Προώθησης βίας - ναρκωτικών
  - Προώθησης εξτρεμιστικών ιδεολογιών
  - Εύρεσης κακόβουλου λογισμικού ή κωδικών για “ξεκλείδωμα λογισμικού” (hacking software)

- Λόγοι αποτροπής πρόσβασης
  - Νομικοί
  - Λειτουργικοί (αποτροπή κατασπατάλησης εύρους)

Προστασία: Λογισμικό Firewall

- Windows Firewall
  - Αρκετά καλό
  - Προλαμβάνει όμως μόνο την εισερχόμενη ανεπιθύμητη διακίνηση δεδομένων
- Firewall διπλής κατεύθυνσης (inbound/outbound)
  - Σταματούν τις προσπάθειες εφαρμογών spyware να στείλουν προσωπικά δεδομένα στους δημιουργούς τους
  - π.χ. ZoneAlarmPro (www.zonelabs.com)

Προστασία: Παρακολούθηση Ανεπιθύμητου Λογισμικού

- Το firewall δεν προστατεύει από:
  - μολυσμένα emails και σελίδες web που εκμεταλλεύνται κενά ασφαλείας των browsers
  - Adware που κατεβαίνουν εν αγνοία του χρήστη από το web
- Χρήση προγράμματος κατά των ιών
  - Avira AntiVir (Δωρεάν - www.freeav.com)
- Χρήση προγράμματος καταπολέμησης adware
  - Spyware Doctor (www.pctools.com)
  - Webroot Spy Sweeper (www.webroot.com)
  - ZoneAlarm Security Suite (antivirus, spyware, antispam, firewall)
  - Δωρεάν εφαρμογές
    - Avast! 4 Home Edition (www.avast.com)
    - ZoneAlarm (Για προσωπική χρήση)

Προστασία: Ανεπιθύμητο Λογισμικό & File Extensions

- Εξ' ορισμού τα windows κρύβουν τον τύπο του αρχείου (π.χ. το αρχείο image.jpg φαίνεται ως image)
- Τα malware προγράμματα εκμεταλλεύονται αυτό το γεγονός (π.χ. το αρχείο image.jpg.exe φαίνεται ως image.jpg)

Προτείνεται η αλλαγή των ρυθμίσεων των windows ώστε να φαίνονται τα file extensions

Προστασία: Προγράμματα Προστασίας

- Συστηματική ενημέρωση νέων εκδόσεων του λογισμικού
  - Windows
  - Λογισμικό καταπολέμησης ιών, spam κτλ
- Χρυσοί κανόνες για τη χρήση προγραμμάτων προστασίας:
  - Όχι ταυτόχρονη χρήση περισσότερων του ενός προγραμμάτων antivirus
  - Απομάκρυνση της παλιάς έκδοσης πριν της εγκατάσταση κάποιας άλλης
  - Περιοδική χρήση Online scanners
  - Εργαλεία καταπολέμησης spyware

Προστασία: Κωδικοί πρόσβασης

- **ΔΕΝ ΠΡΕΠΕΙ**
  - Να είναι **κενοί** (να μην υπάρχει κωδικός)
  - Να είναι το **ίδιο** όπως και το **Login** username ή να περιέχει μέρος του ή να προέρχεται από αυτό (password και Login πρέπει να είναι ανεξάρτητα μεταξύ τους)
  - Να είναι μια εύκολα μαντέψιμη πληροφορία (όπως ημερομηνία ή **χρονολογία γέννησης**, όνομα συγγενή, συζύγου, κατοικίδιου κτλ). Ούτε συνδυασμός αυτών (πχ kostas1967)
  - Να μην είναι **τετριμμένοι** (1234, 4444, abc, qwerty, aaaa κτλ) ή συνδυασμοί τετριμμένων κωδικών (abc123)
  - Να είναι **μικροί** σε πλήθος χαρακτήρων (qk1, 234a κτλ). Προτείνεται να είναι 8 με 10 χαρακτήρες
  - Να είναι εύκολα **προβλέψιμοι**. Πχ κάποιος να χρησιμοποιεί ως κωδικό το όνομά του ακολουθούμενο από τον τρέχον μήνα (kostasjuly) ή το όνομά του ακολουθούμενο από το όνομα του συστήματος (kostasmail, mariawebserver)
  - Να είναι απλές **λέξεις** που συναντιόνται σε **λεξικό**. Σε αυτή την περίπτωση αυτοματοποιημένα προγράμματα μπορούν να τους βρουν σε ελάχιστα δευτερόλεπτα
  - Ότι και να είναι ο κωδικός ΔΕΝ τον αποκαλύπτουμε σε κανέναν ούτε στον διαχειριστή ούτε στο συνάδελφο. Οι μεγαλύτερες απάτες έχουν γίνεί με αυτό τον τρόπο.
    - Αν τον αποκαλύψουμε τον αλλάζουμε σε νέο το συντομότερο

Προστασία: Κωδικοί πρόσβασης

Καλό είναι

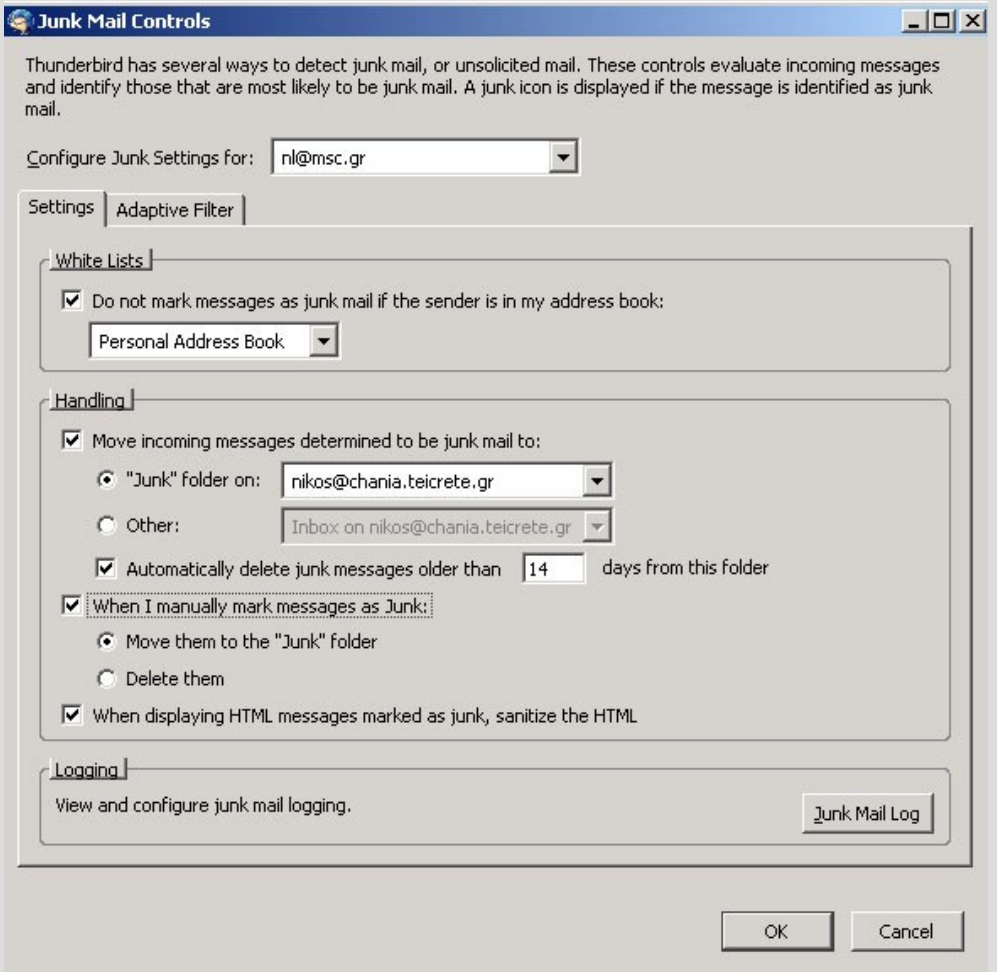
- Να περιέχει εκτός από **γράμματα, αριθμούς ή/και σύμβολα** (πχ p4pak11!)
- Αν πρέπει να χρησιμοποιηθεί λέξη (για να είναι ευκολο-μνημόνευτος ένας κωδικός) τότε συνίσταται η λέξη να γράφετε **ανορθόγραφα** και με κάποια από τα γράμματα **διπλές φορές** (πχ indeerneet12 αντί Internet). Να μην χρησιμοποιούνται λέξεις ή ονόματα αγγλικά αλλά ελληνικά γραμμένα με λατινικούς χαρακτήρες και αντικατάσταση κάποιον από αυτά με αριθμούς που ομοιάζουν με γράμματα (0 αντί ο, 4 αντί Α, 3 αντί ε) (πχ η λέξη χελιδόνι θα γράφονταν x3lidd0ni ενώ η λέξη αυτοκίνητο θα μπορούσε να γραφτεί aftookin1to)
- Εναλλακτικά αντί λέξεων κωδικών προτείνεται να χρησιμοποιούνται **φράσεις κωδικοί** (passphrases). Μια πρόταση (στίχος, παροιμία έκφραση που αποτελείτε από πολλές λέξεις) μπορεί να χρησιμοποιηθεί ως ασφαλέστερος τρόπος αυθεντικοποίησης. Η διαφορά από τους πολύπλοκους κωδικούς είναι ότι ο χρήστης μπορεί να τον θυμάται πιο εύκολα. Τέτοιες προτάσεις είναι
  - “osa-denftane-i-ialepou”
  - “tokalotopalikari”
  - “tospitimoueinaiaspro”
  - “eimai_78_kila_mono”
  - “sousami-anoi3e”

Χρήση Ηλεκτρονικού Ταχυδρομείου

- Χρυσοί κανόνες κατά τη χρήση ηλεκτρονικού ταχυδρομείου
  - Όχι στην προεπισκόπηση των μηνυμάτων
    - Για αποφυγή πιθανής μόλυνσης από ιούς
    - Για αποφυγής επαλήθευσης email λογαριασμού σε spammers
  - Προσοχή στη χρήση συνημμένων
  - Προσοχή στα “Undeliverable” messages
  - Spam emails
    - Όχι στις προτεινόμενες αγορές
    - Όχι διαγραφή από την υποτιθέμενη λίστα
  - Χρήση φίλτρων για τα τα spam emails
  - Χρήση εναλλακτικών email clients
    - Thunderbird 1.5+
    - Seamonkey 1.0+
    - Eudora 7.0+

Αντιμετώπιση spam στο λογισμικό ηλεκτρονικής αλληλογραφίας

- Παράδειγμα ρύθμισης φίλτρου για μηνύματα spam στο πρόγραμμα διαχείρισης ηλεκτρονικής αλληλογραφίας **Thunderbird**



Πλοήγηση στο Internet

- Παρεμπόδιση POP-UPs
- Internet explorer: “Trusted Sites”
- Προσοχή στις παροτρύνσεις κατά την περιήγηση π.χ. στο κατέβασμα δωρεάν software
- Χρήση εναλλακτικών browsers
  - Seamonkey 1.0+
  - Firefox 1.5+
  - Netscape 8.0+
  - Opera 8.00+

Σχετικές Πληροφορίες

http://nog.chania.teicrete.gr/

- Τρόποι Προστασίας
- Σχετικοί δικτυακοί τόποι
- Διαθέσιμο Λογισμικό
  - Browsers
  - Email clients