

Κεφάλαιο 16: Ασφάλεια και Προστασία στο Διαδίκτυο



Ασφάλεια Η/Υ – Κακόβουλο λογισμικό

- Τα δεδομένα και το λογισμικό, τα οποία είναι αποθηκευμένα με τη μορφή αρχείων σε ψηφιακά αποθηκευτικά μέσα, κινδυνεύουν να αλλοιωθούν, να διαγραφούν ή να υποκλαπούν, κυρίως από βλάβες στα αποθηκευτικά μέσα, από κακόβουλο λογισμικό (malware) και από μη εξουσιοδοτημένες παρεμβάσεις κακόβουλων χρηστών («επιθέσεις»).
- **Κακόβουλο λογισμικό ονομάζεται το λογισμικό** το οποίο εκ προθέσεως διαθέτει τις απαιτούμενες εντολές για να βλάψει ένα υπολογιστικό σύστημα. Επομένως, τίθενται θέματα ασφάλειας και προστασίας στα υπολογιστικά συστήματα.

Είδη κακόβουλου λογισμικού

- **Ιός (virus):** κακόβουλο πρόγραμμα που δημιουργεί προβλήματα στην ομαλή λειτουργία του υπολογιστή μας (π.χ. αδυναμία εκκίνησης, ελάττωση της ταχύτητας επεξεργασίας, προβλήματα στη λειτουργία των εγκατεστημένων εφαρμογών, εμφάνιση ενοχλητικών μηνυμάτων) και στην ασφάλεια των αρχείων μας (π.χ. καταστροφή).
- Ο ιός προσκολλάται σε κάποιο πρόγραμμα ή αρχείο και ενεργοποιείται συνήθως μόλις προσπαθήσουμε να τρέξουμε το πρόγραμμα ή να ανοίξουμε το αρχείο. Ένας ιός μπορεί να φτάσει στον υπολογιστή μας κυρίως μέσω του Διαδικτύου είτε ως συνημμένο αρχείο σε μήνυμα ηλεκτρονικού ταχυδρομείου (e-mail) είτε από την περιήγησή μας ή το κατέβασμα αρχείων από μη ασφαλείς ιστοσελίδες.
- Μεταδίδονται κυρίως μέσω φορητών μέσων αποθήκευσης (π.χ. USB disks) και μέσω δικτύων Η/Υ (π.χ. διαδίκτυο, e-mails)

Είδη κακόβουλου λογισμικού

- **Σκουλήκι (Worm):** βλαβερό πρόγραμμα που αναπαράγεται δημιουργώντας αντίγραφα του εαυτού του διαμέσου των δικτύων υπολογιστών. Δεν χρειάζεται κάποιο άλλο πρόγραμμα ως όχημα για τη διακίνησή του. Ένα σκουλήκι δεν είναι τόσο καταστροφικό όπως ένας ιός, επειδή δεν σβήνει αρχεία, αλλά μειώνει την ταχύτητα σύνδεσης στο Διαδίκτυο, μια και στέλνει αντίγραφά του σε άλλους υπολογιστές και καταναλώνει τους πόρους (π.χ. μνήμη) του υπολογιστή που έχει μολύνει κάνοντάς τον πιο αργό.

Είδη κακόβουλου λογισμικού

- **Δούρειος ίππος (Trojan horse):** κακόβουλο πρόγραμμα μεταμφιεσμένο σε θεμιτό λογισμικό (π.χ. παιχνίδι, πρόγραμμα ανίχνευσης ιών) που στην πραγματικότητα δρα παρασκηνικά αναλαμβάνοντας εξ αποστάσεως τον έλεγχο του μολυσμένου υπολογιστή. Μπορεί να διαγράψει αρχεία, να υποκλέψει προσωπικά δεδομένα (π.χ. κωδικούς πρόσβασης) ή να χρησιμοποιήσει τον μολυσμένο υπολογιστή για επίθεση σε άλλους υπολογιστές. Οι δούρειοι ίπποι δεν αναπαράγουν και δεν διαδίδουν τους εαυτούς τους.

Είδη κακόβουλου λογισμικού

- **Λογισμικό Κατασκοπίας (Spyware):** κακόβουλο πρόγραμμα που προσκολλάται κρυφά σε αρχεία που κατεβάζουμε από το Διαδίκτυο ή κατεβαίνει και εγκαθίσταται αυτόματα σε έναν υπολογιστή κατά την επίσκεψή μας σε μολυσμένες ιστοσελίδες. Παρακολουθεί τη διαδικτυακή δραστηριότητα του χρήστη του μολυσμένου υπολογιστή (π.χ. ποιους ιστότοπους επισκέπτεται πιο συχνά) και την αποστέλλει σε τρίτους, κυρίως εταιρείες, με σκοπό την αποστολή στοχευμένων διαφημιστικών μηνυμάτων.
- Ένα πρόγραμμα κατασκοπίας μπορεί να αλλάξει την αρχική σελίδα του φυλλομετρητή, να προσθέσει ανεπιθύμητες γραμμές εργαλείων σε αυτόν ή να εμφανίζει συνεχώς παράθυρα με ενοχλητικές διαφημίσεις.

Τρόποι προστασίας από κακόβουλο λογισμικό

Για να προστατέψουμε τον υπολογιστή μας από κακόβουλο λογισμικό κατά την περιήγησή μας στο Διαδίκτυο, θα πρέπει να:

- ενημερώνουμε τακτικά το Λειτουργικό Σύστημα και τις εφαρμογές του υπολογιστή μας.
- ρυθμίζουμε κατάλληλα τις επιλογές ασφαλείας του φυλλομετρητή μας.
- προσέχουμε ποιους ιστότοπους επισκεπτόμαστε και ποια αρχεία κατεβάζουμε από το Διαδίκτυο.
- μην ανοίγουμε συνημμένα αρχεία σε μηνύματα ηλεκτρονικού ταχυδρομείου που μας αποστέλλουν άγνωστοι ή με ύποπτο θέμα.
- έχουμε πάντα εγκατεστημένο στον υπολογιστή μας λογισμικό ασφαλείας: λογισμικό προστασίας από ιούς (antivirus) και τείχος προστασίας (firewall). Το λογισμικό προστασίας από ιούς (antivirus) πρέπει να ενημερώνεται τακτικά με πρόσφατους ορισμούς ιών (virus definitions). Οι ορισμοί ιών είναι αρχεία που περιέχουν τα ψηφιακά αποτυπώματα γνωστών ιών (virus signatures). Το λογισμικό προστασίας από ιούς για τον εντοπισμό κακόβουλου ή πιθανώς ανεπιθύμητου λογισμικού συγκρίνει το περιεχόμενο των αρχείων με τους ορισμούς των ιών που διαθέτει. Μόλις εντοπίσει μολυσμένο με ιό αρχείο, μας ενημερώνει και στις περισσότερες περιπτώσεις προτείνει επιδιόρθωση, σβήσιμο ή απομόνωσή του.

Επιβλαβή ή ανεπιθύμητα e-mail

- Το ηλεκτρονικό ταχυδρομείο αποτελεί αναμφισβήτητα μία από τις πιο χρήσιμες υπηρεσίες του Διαδικτύου. Δυστυχώς όμως υπάρχουν και οι παρακάτω αρνητικές πλευρές:
- **μετάδοση ιών:** μέσω μολυσμένων συνημμένων αρχείων.
- **ηλεκτρονικό ψάρεμα (phishing):** ένα e-mail, το οποίο φαινομενικά προέρχεται από μια γνωστή και αξιόπιστη εταιρεία, αποστέλλεται σε μεγάλο αριθμό διευθύνσεων ηλεκτρονικού ταχυδρομείου. Το e-mail αυτό μπορεί να παραπέμπει τον παραλήπτη σε έναν πλαστό ιστότοπο όπου πρέπει να δώσει τα προσωπικά του στοιχεία (π.χ. Κωδικούς πρόσβασης, στοιχεία πιστωτικής κάρτας).
- **ανεπιθύμητα μηνύματα spam:** το ηλεκτρονικό ισοδύναμο των μαζικών αποστολών διαφημιστικών επιστολών για προώθηση προϊόντων. Κάποια μηνύματα spam μπορούν να περιέχουν προσφορές για απάτες ή κακόβουλο λογισμικό.

Αξιολόγηση πληροφοριών

- διασταυρώνουμε τις πληροφορίες που βρίσκουμε στο Διαδίκτυο και με άλλες πηγές, π.χ. άλλους ιστότοπους, βιβλία, εγκυκλοπαίδειες.
- αναζητούμε πληροφορίες σε έγκυρους ιστότοπους, π.χ. έγκριτες ψηφιακές βιβλιοθήκες, Πανεπιστήμια, γνωστούς οργανισμούς, φορείς και ιδρύματα.
- αξιολογούμε την αξιοπιστία των ιστοσελίδων που επισκεπτόμαστε με έλεγχο του συγγραφέα τους, του σκοπού τους (π.χ. ενημερωτικός, εμπορικός), των βιβλιογραφικών παραπομπών, της δημοφιλίας, της ένδειξης ανανέωσης, ακόμα και της ορθογραφίας και αισθητικής τους

Πειρατεία λογισμικού (παράνομη αντιγραφή και χρήση προγραμμάτων χωρίς την άδεια του δημιουργού) – Κίνδυνοι:

- είναι πιθανό να χάσετε αρχεία ή δεδομένα με την εγκατάστασή του στον υπολογιστή σας
- το παράνομο λογισμικό μπορεί να είναι μολυσμένο με κακόβουλο λογισμικό (π.χ. spyware)
- το παράνομο λογισμικό συνήθως δεν ενημερώνεται με διορθωτικές εκδόσεις για την αντιμετώπιση ευπαθειών και έτσι είναι ευάλωτο σε επιθέσεις εισβολέων
- δεν παρέχεται τεχνική υποστήριξη
- δεν παρέχονται εγχειρίδια χρήσης

Προστασία προσωπικών δεδομένων

- Για να διατηρήσουμε προστατευμένα τα προσωπικά μας δεδομένα, καλό είναι να ακολουθούμε τις παρακάτω συμβουλές:
- να είμαστε γενικά φειδωλοί με τη δημοσιοποίηση προσωπικών μας δεδομένων σε ιστότοπους και σε υπηρεσίες κοινωνικής δικτύωσης. Κάθε στοιχείο που «ανεβάζουμε» στο Διαδίκτυο είναι δυνατό να υποπέσει στην αντίληψη οποιουδήποτε. Επιπρόσθετα, η δραστηριότητά μας στο Διαδίκτυο μπορεί να αφήσει ίχνη που δύσκολα σβήνουν, για παράδειγμα μια δημοσιοποιημένη φωτογραφία μας δύσκολα «κατεβαίνει».
- να αποφεύγουμε την εγγραφή μας σε άγνωστους και αμφιβόλου σκοπού ιστότοπους. Πρέπει να διαβάζουμε την πολιτική απορρήτου (privacy policy) των ιστοσελίδων που επισκεπτόμαστε, ώστε να ενημερωνόμαστε για το πώς θα χρησιμοποιήσουν τα προσωπικά μας δεδομένα και για το αν εγκαθιστούν cookies στον υπολογιστή μας.
- να χρησιμοποιούμε ψευδώνυμο στα chat rooms και να μην αποκαλύπτουμε ποτέ προσωπικά δεδομένα στους συνομιλητές μας.
- να επιλέγουμε «ισχυρούς» κωδικούς πρόσβασης (passwords) για τη σύνδεσή μας σε υπηρεσίες του Διαδικτύου.
- να έχουμε εγκατεστημένο λογισμικό ασφαλείας στον υπολογιστή μας, μια και το κακόβουλο λογισμικό μπορεί να υποκλέψει προσωπικά μας δεδομένα.