

ΘΕΜΑ 4

Στο δίκτυο μιας επιχείρησης παρουσιάστηκαν τα παρακάτω προβλήματα ασφάλειας.

α) Στη πρώτη περίπτωση ενώ δεν υπάρχει καμία ανοικτή εφαρμογή παρατηρήθηκε στο πρόγραμμα εποπτείας πόρων του συστήματος σημαντική κίνηση δεδομένων στο δίκτυο. Επιπλέον φάνηκε ότι την κίνηση την προκαλεί μια εφαρμογή - εργαλείο που έχει εγκατασταθεί για να διατηρεί τον υπολογιστή ταχύτερο, όπως αναφέρει ο δικτυακός τόπος από τον οποίο έγινε η λήψη του.

β) Στη δεύτερη περίπτωση, σε συγκεκριμένη ημερομηνία, παρουσιάστηκε το εξής φαινόμενο, αρχικά οι υπολογιστές ξεκίνησαν να λειτουργούν κανονικά, όμως μετά από κάποιο διάστημα, ένας – ένας σταμάτησαν να λειτουργούν. Κατόπιν δε διαπιστώθηκε ότι οι σκληροί δίσκοι στους υπολογιστές που παρουσιάστηκε αυτή η συμπεριφορά, δεν έχουν καθόλου δεδομένα. Ως ειδικού ασφάλειας σας ζητήθηκαν τα εξής:

4.1 Να αναγνωρίσετε και να δώσετε την ονομασία που αντιστοιχεί στο πρόβλημα ασφάλειας που ανιχνεύθηκε σε κάθε μια από τις δυο παραπάνω περιπτώσεις. Επιπλέον να αναφέρετε ποια είναι η κύρια διαφορά μεταξύ αυτών των δυο τύπων απειλής σχετικά με τον τρόπο διάδοσης τους.

Μονάδες 6

4.2 Εξηγήστε αν στην δεύτερη περίπτωση θα μπορούσε πιθανόν να ανιχνευθεί η παραβίαση από ένα antivirus και γιατί.

Μονάδες 5

4.3

Να αναφέρετε σε κάθε μια από τις παραπάνω περιπτώσεις παραβίασης της ασφάλειας, ποια από τα βασικά χαρακτηριστικά ασφάλειας (Διαθεσιμότητα, Ακεραιότητα, Εμπιστευτικότητα) παραβιάζονται;

Μονάδες 6

4.4 Στην πρώτη περίπτωση παραβίασης ασφάλειας εξηγήστε πως λειτουργεί και ποιος είναι ο πιο πιθανός λόγος πρόκλησης της;

Μονάδες 8