

## ΕΝΔΕΙΚΤΙΚΕΣ ΛΥΣΕΙΣ

### ΘΕΜΑ 4

#### 4.1 3 μονάδες κάθε κίνδυνος – Αναφέρονται ενδεικτικά κάποιοι κίνδυνοι από την ενότητα 5.3.1

Σε περίπτωση που ο χρήστης κάνει κλικ σε έναν τέτοιο σύνδεσμο μπορεί να προκαλέσει την εκτέλεση κάποιου κακόβουλου λογισμικού το οποίο μπορεί να:

- Συλλέξει δεδομένα από τη δραστηριότητα του χρήστη στον τοπικό υπολογιστή και να τα αποστέλλει στον αποστολέα του μηνύματος.
- Δημιουργήσει μια κερκόπορτα (backdoor) που θα επιτρέψει στον αποστολέα του μηνύματος να λάβει τον έλεγχο του υπολογιστή
- Προσβάλλει με έναν ιό τον τοπικό υπολογιστή αρχικά και στη συνέχεια το δίκτυο της εταιρείας.

#### 4.2 6 μονάδες κάθε αντίμετρο (3 για το είδος, 3 για την αντιμετώπιση) – Αναφέρονται ενδεικτικά κάποια από τις ενότητες 5.3.2, 5.3.3, 5.4.

Ως τεχνικοί ασφάλειας μπορείτε να λάβετε τα παρακάτω αντίμετρα:

- Εγκατάσταση λογισμικού προστασίας από ιούς ώστε να αναγνωριστεί το κακόβουλο λογισμικό και να μην μπορέσει να εγκατασταθεί.
- Εγκατάσταση όλων των ενημερώσεων του λειτουργικού συστήματος και του λογισμικού που χρησιμοποιείται στην εταιρεία ώστε να μην υπάρχουν γνωστές ευπάθειες που να μπορεί να εκμεταλλευτεί ο εισβολέας.
- Περιορισμός των δικαιωμάτων πρόσβασης των χρηστών ώστε ακόμα και αν επιλεγεί ο σύνδεσμος να μην μπορεί να εκτελεστεί το κακόβουλο λογισμικό.
- Εγκατάσταση τείχους προστασίας ώστε να μην μπορεί να υπάρξει επικοινωνία με τους υπολογιστές του αποστολέα.

### 4.3

Ναι, η παρακάτω επίθεση όντως αποτελεί παράδειγμα κοινωνικής μηχανικής γιατί εξαπατά τους χρήστες εκμεταλλευόμενη την αγωνία τους σχετικά με την τύχη των εισερχόμενων μηνυμάτων τους ώστε να κάνουν κλικ στον άγνωστο σε αυτούς σύνδεσμο.