

## ΕΝΔΕΙΚΤΙΚΕΣ ΛΥΣΕΙΣ

### ΘΕΜΑ 4

#### 4.1

Η βασική αρχή ασφάλειας η οποία παραβιάστηκε στην περίπτωση που αναφέρει το άρθρο είναι η Διαθεσιμότητα (Availability), η οποία εξασφαλίζει ότι το σύστημα θα μπορεί να παρέχει τις πληροφορίες του, όταν του ζητηθούν και μέσα σε αποδεκτά χρονικά όρια. Στη συγκεκριμένη περίπτωση το κλείδωμα των αρχείων δεν επέτρεπε στους γιατρούς να αντλήσουν χρήσιμες πληροφορίες για τους ασθενείς αλλά και για τις προγραμματισμένες επεμβάσεις, με αποτέλεσμα να μην μπορούν να εξυπηρετήσουν τους ασθενείς.

**4.2** 5 μονάδες κάθε μέτρο – Αναφέρονται ενδεικτικά κάποια από τις ενότητες 5.3.2 , 5.3.3.

Κάποια μέτρα για την αποφυγή τέτοιων επιθέσεων είναι:

- 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 να μην μπορεί να εκτελεστεί το κακόβουλο λογισμικό, αλλά και να κλειδώσει όσο το δυνατόν λιγότερα αρχεία.

#### 4.3

Η διαδικασία λήψης αντιγράφων ασφαλείας μπορεί να επιτρέψει στους διαχειριστές να αποκαταστήσουν τα κλειδωμένα αρχεία, έτσι ώστε να μην χρειαστεί να πληρωθούν τα λύτρα. Πρέπει όμως τα αντίγραφα ασφαλείας, να λαμβάνονται σε πολύ συχνά χρονικά διαστήματα ώστε οι αλλαγές που δεν μπορούν να ανακτηθούν να είναι οι ελάχιστες δυνατές. Το αυξητικό backup θα επιτρέψει αυτή η διαδικασία να γίνεται πολύ συχνά καθώς μπορεί να γίνει γρήγορα και κάθε αυξητικό αντίγραφο πιάνει λίγο χώρο.