Α. Υπόθεση εργασίας

Πρώην πελάτης του ιατρικού σας φορέα τηλεφωνεί διαμαρτυρόμενος ότι ασφαλιστής συνεργαζόμενος με ασφαλιστική εταιρεία (με την οποία δεν είχε ακόμα συνάψει σύμβαση) του έδειξε τον πλήρη ιατρικό του φάκελο με εξετάσεις από το ίδρυμά σας. Ο πελάτης έχει τραβήξει φωτογραφία με το κινητό του τηλέφωνο και σας τη δείχνει.

Με μια γρήγορη επισκόπηση διαπιστώνετε ότι πρόκειται πράγματι για αντίγραφο από εσωτερικό έγγραφο. Πιθανολογείτε εσωτερική διαρροή.

Υποπτεύεστε ότι κάποιος (ιατρός ή νοσηλευτής ή κάποιος που έχει πρόσβαση) μπορεί να έχει δώσει το αρχείο, αλλά δεν έχετε στοιχεία για το ποιος.

Β. Υπόθεση εργασίας

Υπάλληλός του ΙΤ αντιλαμβάνεται ότι η κεντρική εφαρμογή που χρησιμοποιεί ο φορέας σας έχει κενό ασφάλειας, το οποίο φαίνεται να μπορεί να επιτρέψει σε κακόβουλους (π.χ. hackers) την πρόσβαση σε ιατρικούς φακέλους. Ο υπάλληλος ενημερώνει τον προϊστάμενό του και αυτός άμεσα εσάς.

Το πρόβλημα φαίνεται να δημιουργήθηκε πριν 30 ημέρες μετά από μια αλλαγή του λογισμικού και τη διασύνδεσή του με το διαδίκτυο.

Δε γνωρίζετε όπως αν πράγματι έχει υλοποιηθεί η επίθεση. Πως ενεργείτε σε πρώτο στάδιο;

Αρχικές ενέργειες/στόχοι:

ΙΤ: Μετά από τη πρώτη έρευνα διαπιστώνετε ότι υπάρχουν υπόνοιες ότι κάποιος έχει διαβάσει τους φακέλους, καθώς διαπιστώνετε μεγάλο αριθμό ανεξήγητων «ερωτημάτων» στη Βάση Δεδομένων. Το αναφέρετε στη διοίκηση.

Διοίκηση: Καθώς δεν υπάρχει κανένα δημοσίευμα, όχληση από τρίτο (υποκείμενο ή hacker) ή άλλη ένδειξη, εκτιμάτε ότι πρέπει να προσπαθήσετε να περιορίσετε όσο γίνεται το περιστατικό.

DPO: Προσπαθείτε να πείσετε και να συμβουλεύσετε τη διοίκηση και το ΙΤ για να εφαρμοστεί ο ΓΚΠΔ.

Σημείωση: ετοιμαστείτε για τη συνέχεια…