Σύμφωνα με την μελέτη περίπτωσης που μας δίνετε στην εργασία για την εφαρμογή της μεθοδολογίας ανάλυσης απειλών ιδιωτικότητας LINDDUN. Πρέπει να υλοποιήσουμε 3 πίνακες. Πίνακας καταγραφής μερών του συστήματος, πίνακας με τις επτά κατηγορίες απειλών και πίνακας σεναρίων.

ΠΙΝΑΚΑΣ ΚΑΤΑΓΡΑΦΗΣ ΜΕΡΩΝ ΣΥΣΤΗΜΑΤΟΣ

|  |  |  |
| --- | --- | --- |
|  | Στοιχεία Συστήματος | Περιγραφή |
| 1. | Βάση δεδομένων | Η βάση δεδομένων, με την οποία είναι συνδεδεμένο το υποσύστημα φοιτητών, περιέχει όλες τις πληροφορίες για κάθε φοιτητή που προέρχονται από όλους τους εμπλεκόμενους στο σύστημα. |
| 2. | Υποσύστημα Φοιτητών | Διεπαφές για φοιτητές κάθε βαθμίδας, διδάσκοντες, Υπευθύνου καταχώρισης της Γραμματείας του τμήματος Πληροφορικής, διαχειριστές. |
| 3. | Κεντρικό Πληροφοριακό Σύστημα Αξιολόγησης | Εξωτερικό σύστημα που τραβά στατιστικά και αποδεικτικά τίτλων μέσω αίτησης. |
| 4. | Δίκτυα επικοινωνίας | Διεπαφές επικοινωνίας μέσω διαδικτύου, ενσύρματα ή ασύρματα (HTTPS, HTTPS – SQL, SQL Queries, HTTPS - SFTP) και Bluetooth. |
| 5. | Υπηρεσία SMS (I2GSM) | Για την επιβεβαίωση νέου αριθμού κινητού τηλεφώνου, το σύστημα στέλνει γραπτό μήνυμα (sms) στο χρήστη μέσω δικτύου κινητής τηλεφωνίας. |
| 6. | Cloud Storage Service | Αντίγραφο της βάσης δεδομένων δημιουργείται και αποθηκεύεται σε πραγματικό χρόνο σε υπηρεσία αποθήκευσης στο σύννεφο (cloud storage service) μέσω διαδικτύου. |
| 7. | Διαχειριστής Υποσυστήματος Φοιτητών | Δικαίωμα read/write στα δεδομένα του υποσυστήματος. |
| 8. | Διαχειριστής Κεντρικού Συστήματος Αξιολόγησης | Δικαιώματα μόνο read στις ανακοινώσεις του τμήματος Πληροφορικής, στο πρόγραμμα μαθημάτων και εξετάσεων του τμήματος και στα στοιχεία επικοινωνίας των διδασκόντων του μέσω αίτησης. |
| 9. | Διαχειριστής/Γραμματεία του τμήματος πληροφορικής | Δικαιώματα read/write στα δεδομένα του υποσυστήματος. |
| 10. | Φοιτητές(κάθε βαθμίδας) | Δικαιώματα read και σε περιπτώσεις write για καταχώρηση στοιχείων και δήλωση συμμετοχής σε μαθήματα/εργαστήρια και εξετάσεις. |
| 11. | Διδάσκοντες | Δικαιώματα μόνο για ανάγνωση στο ωρολόγιο πρόγραμμα, τα στοιχεία επικοινωνίας και σπουδών των φοιτητών, τις λίστες συμμετοχής σε εξετάσεις/εργαστήρια και τις λίστες δήλωσης κάθε μαθήματος. Δικαίωμα καταχώρισης για βαθμολογίες μαθημάτων και εργασιών, παρουσίες/απουσίες σε διαλέξεις και εξετάσεις και τη διαθεσιμότητά τους για την κατάρτιση του ωρολογίου προγράμματος. |
|  |  |  |

ΠΙΝΑΚΑΣ ΑΠΕΙΛΩΝ LINDDUN

|  |  |
| --- | --- |
| Κατηγορία | Περιγραφή απειλών |
| Information Disclosure(Εμπιστευτικότητα) | Earsdropping στο δίκτο επικοινωνίας: Υποκλοπή πιστοποιητικών και προσωπικών δεδομένων φοιτητών/διδασκόντων. |
| Information Disclosure(Εμπιστευτικότητα) | Αποστολή δεδομένων (π.χ. μέσω Bluetooth) μέσω μη κρυπτογραφημένου μέσου επικοινωνίας. |
| Unawareness(Άγνοια) | Φοιτητές/ διδάσκοντες δεν γνωρίζουν ή αγνοούν ότι τα προσωπικά τους δεδομένα κοινοποιούνται σε ένα σύστημα για στατιστική αξιολόγηση. |
| Unawareness(Άγνοια) | Μη ενημέρωσης διατήρης προσωπικών δεδομένων στα αντίγραφα ασφαλείας. |

ΠΙΝΑΚΑΣ ΣΕΝΑΡΙΩΝ ΑΠΕΙΛΩΝ

|  |  |  |
| --- | --- | --- |
| Εμπλεκόμενος | Περιγραφή Σεναρίου | Επιστώσεις |
| Φοιτητής | Ο Φοιτητής στέλνει την ταυτότητα μέσω Bluetooth χωρίς κρυπτογράφηση | Επιτιθέμενος σε κοντινή απόσταση διαβάζει τα πακέτα και συλλέγει ευαίσθητες πληροφορίες. |
| Διδάσκων | Ο διδάσκων συνδέεται σε WiFi WEP, αγνοώντας την ευπάθεια του πρωτοκόλλου. | Επιτιθέμενος αποκρυπτογραφεί τη σύνδεση, υποκλέπτει διαπιστευτήρια. |
| Φοιτητής | Ο φοιτητής εισέρχεται στην πλατφόρμα του πανεπιστημίου μη γνωρίζοντας ότι τα προσωπικά του δεδομένα θα χρησιμοποιηθούν για στατιστικές αναλύσεις | Έλλειψη συναίνεσης και αθέμιτη επεξεργασία δεδομένων. |
|  |  |  |
|  |  |  |