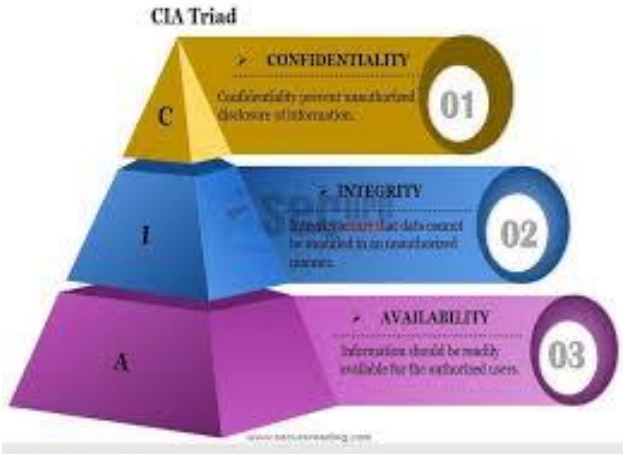
**ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΚΑΙ ΚΡΙΣΙΜΩΝ ΥΠΟΔΟΜΩΝ**




ΣΧΕΔΙΟ ΑΣΦΑΛΕΙΑΣ

**ΣΥΓΓΡΑΦΕΙΣ: Φίλιππος Χατζηφιλίππου 3160217, Λυδία Αθανασίου 3170003, Μαρία Ελένη Κοκκίνη 3170070**

**ΕΡΓΑΣΙΑ ΧΕΙΜΕΡΙΝΟΥ ΕΞΑΜΗΝΟΥ 2019**

Contents

## Α1. ΕΙΣΑΓΩΓΗ

Στο πλαίσιο αυτής της εργασίας θα αναπτυχθεί ένα σχέδιο ασφάλειας και τρόποι προστασίας για τον έλεγχο των υποδομών, διαδικασιών και λογισμικού του πληροφοριακού συστήματος μιας εταιρείας που εξειδικεύεται σε θέματα τραπεζών για επεξεργασία προσωπικών δεδομένων, αφού πρώτα εντοπιστούν πιθανές απειλές και ευπάθειες. Στο πληροφοριακό σύστημα πρέπει να τηρείται η ακεραιότητα, η εμπιστευτικότητα και η διαθεσιμότητα (C.I.A.).

### Α1.1 Περιγραφή Εργασίας

Στην εργασία καλούμαστε να κάνουμε ανάλυση επικινδυνότητας της data_central_bank. Συγκεκριμένα, θα εντοπίσουμε τα αγαθά και τα αντίστοιχα threats από τα οποία κινδυνεύουν, τις ευπάθειες που εμφανίζουν, τις επιπτώσεις από τη φθορά τους για το σύστημα και τρόπους αντιμετώπισης των απειλών. Τέλος θα αξιολογήσουμε το impact κάθε αγαθού όσον αφορά την ακεραιότητα, διαθεσιμότητα, εμπιστευτικότητα.

### Α1.2 Δομή παραδοτέου

Στην ενότητα Α1 παρουσιάζουμε επιγραμματικά τις ενότητες της εργασίας και τι θα αναλύσουμε κατά την μελέτη μας. Στην ενότητα Α2 παρουσιάζεται η μεθοδολογία που ακολουθήσαμε, στην ενότητα Α3 περιγράφονται τα κυριότερα στοιχεία από την μελέτη και την ανάλυση επικινδυνότητας που εκπονήθηκε. Εν συνεχεία στην ενότητα Β2 περιγράφουμε τα μέτρα ασφαλείας και στο Α4 μια εκτεταμένη περιγραφή των πιο κρίσιμων σημείων της ανάλυσης επικινδυνότητας για το data_central_bank.

## Α2. ΜΕΘΟΔΟΛΟΓΙΑ ΜΕΛΕΤΗΣ ΑΣΦΑΛΕΙΑΣ

Για τη Διαχείριση Επικινδυνότητας του/της *data_central_bank* χρησιμοποιήθηκε παραμετροποιημένη μέθοδος του ISO27001K[1]. Επιλέχθηκε για τη συγκεκριμένη εργασία για τους εξής λόγους:

- Αποτελεί πρότυπη μέθοδο και έχει αναπτυχθεί με σκοπό να εφαρμοστεί στην εκπαίδευση.
- Συνοδεύεται από αυτοματοποιημένο excel *(tool)* που υποστηρίζει όλα τα στάδια της εφαρμογής.
- Καλύπτει όλες τις συνιστώσες της ασφάλειας των πληροφοριακών συστημάτων, περιλαμβανομένων του τεχνικού παράγοντα, των θεμάτων διαδικασιών και προσωπικού, της φυσικής ασφάλειας, της ασφάλειας δικτύων κλπ.

[1] http://www.iso27001security.com/html/toolkit.html

| Στάδιο | Βήματα |
|---|---|
| **1.** Προσδιορισμός και αποτίμηση αγαθών *(identification and valuation of assets)* | *Βήμα 1*: Περιγραφή πληροφοριακών συστημάτων και εγκαταστάσεων<br>*Βήμα 2:* Αποτίμηση αγαθών πληροφοριακών συστημάτων και εγκαταστάσεων<br>*Βήμα 3:* Επιβεβαίωση και επικύρωση αποτίμησης |
| **2.** Ανάλυση επικινδυνότητας *(risk analysis)* | *Βήμα 1:* Προσδιορισμός απειλών που αφορούν κάθε Αγαθό (asset)<br>*Βήμα 2:* Εκτίμηση απειλών (threat assessment) και αδυναμιών (vulnerability assessment)<br>*Βήμα 3:* Υπολογισμός επικινδυνότητας συνδυασμών Αγαθό-Απειλή-Αδυναμία<br>*Βήμα 4:* Επιβεβαίωση και επικύρωση βαθμού επικινδυνότητας |
| **3.** Διαχείριση επικινδυνότητας *(risk management)* | *Βήμα 1:* Προσδιορισμός προτεινόμενων αντιμέτρων<br>*Βήμα 2:* Σχέδιο ασφάλειας πληροφοριακών συστημάτων και εγκαταστάσεων |

**Πίνακας 1:** *Στάδια και βήματα της Ανάλυσης και Διαχείρισης επικινδυνότητας*

### Α2.1 Περιγραφή Πληροφοριακού Συστήματος (ΠΣ) υπό έλεγχο

Στην ενότητα αυτή, καταγράφονται τα υφιστάμενα πληροφοριακά συστήματα της Central Bank Data Center, τα οποία με το πέρας της μελέτης θα επικαιροποιηθούν, αναβαθμιστούν ή σε κάποιες περιπτώσεις αντικατασταθούν.

#### Α2.1.1 Υλικός εξοπλισμός (hardware)

Υλικό(hardware) χαρακτηρίζεται το σύνολο των εξαρτημάτων ενός υπολογιστή/ υπολογιστικού συστήματος. Απαρτίζεται από συσκευές εισόδου, εξόδου και τη κεντρική μονάδα. Στο σύστημα μας τα αγαθά hardware είναι :

- Workstation
- Scanner
- Printer
- Web Server
- Database server
- Switch
- Router
- Laptop
- Automated Teller Machine
- Dedicated Line
- VoIP PHONE
- Camera(δε θα συμπεριληφθεί στην ανάπτυξη επικινδυνότητας)

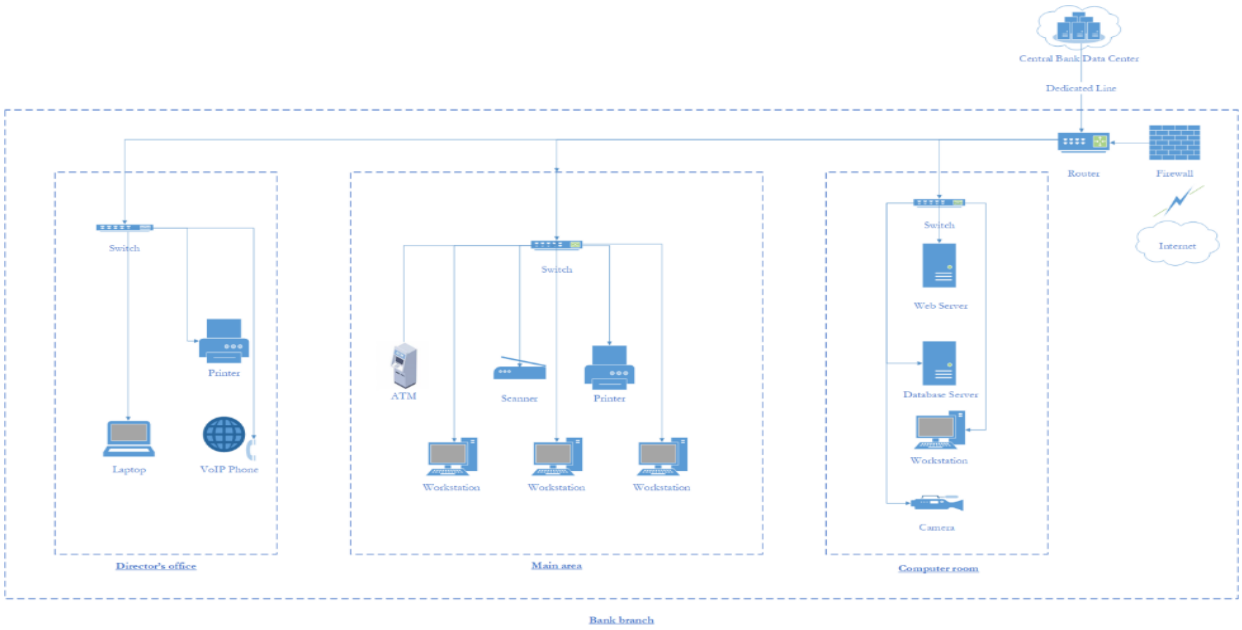
#### Α2.1.2 Λογισμικό και εφαρμογές

Λογισμικό (Software) είναι η συλλογή από προγράμματα υπολογιστών, διαδικασίες και οδηγίες που εκτελούν συγκεκριμένες εργασίες σε ένα υπολογιστικό σύστημα. Υπάρχει το

λογισμικό εφαρμογών, συστήματος, το ενδιάμεσο λογισμικό και το υλικολογισμικό. Στο σύστημά μας τα αγαθά Software είναι τα εξής:

- Software (windows 7 pro)
- Software(windows 10 pro)
- Firewall (δε θα συμπεριληφθεί στην ανάπτυξη επικινδυνότητας)

### A2.1.3 Δίκτυο




Δίκτυο είναι ένα σύνολο από δύο ή περισσότερους υπολογιστές που είναι συνδεδεμένοι μεταξύ τους, ώστε να μπορούν να ανταλλάσσουν δεδομένα και να μοιράζονται διαφορές συσκευές(πχ εκτυπωτές, σαρωτές κλπ.). Στο σύστημά μας εντοπίστηκε ένα Lan.

### A2.1.4 Δεδομένα

Πληροφοριακά δεδομένα είναι ένα σύνολο στοιχείων, μία συλλογή που αποτυπώνει τιμές επι αντικειμένων, προσώπων, γεγονότων. Στο σύστημά μας τα δεδομένα είναι τα εξής:

- Bank Customer Data
- Bank employee Data
- Camera footage data

### A2.1.5 Διαδικασίες

Διαδικασίες είναι μια σειρά από συγκεκριμένες εκτελούμενες πράξεις από τους ανθρώπους και τα συστήματα με τέτοιο τρόπο ώστε να επιτευχθεί ένα συγκεκριμένο αποτέλεσμα. Στο σύστημά μας οι διαδικασίες είναι οι εξής:

- Money Withdrawal from ATM
- Money Deposit
- New Account Opening
- Updating Balance

## Α3. ΑΠΟΤΙΜΗΣΗ ΠΣ ΚΑΙ ΕΓΚΑΤΑΣΤΑΣΕΩΝ ΤΡΑΠΕΖΑΣ

Κάθε πληροφοριακό σύστημα απαρτίζεται από ποικίλά αγαθά. Είναι ιδιαίτερα σημαντική η εύρεση και καταγραφή όλων. Ακόμη και το πιο ασήμαντο φαινομενικά αγαθό μπορεί να αποτελέσει αιτία για σοβαρά προβλήματα στην εταιρεία και τους πελάτες.

Κάποια από τα επιπλέον αγαθά που εντοπίστηκαν και χρήζουν προστασίας είναι τα εξής:

1) Το **Lan (local area network)** , είναι δίκτυο που εκτείνεται σε μια μικρή περιοχή, μπορεί να συνδεθεί με άλλα Lans μέσω τηλεφωνικών γραμμών ή ραδιοκυμάτων .

2) Το **dedicated line**, είναι ένα μονοπάτι τηλεπικοινωνιών μεταξύ δύο σημείων, συνήθως εξυπηρετεί μόνο έναν καθορισμένο χρήστη.

3) Το **λογισμικό ενημέρωσης υπολοίπου**, είναι το λογισμικό για την ορθή διαχείριση των οικονομικών δεδομένων κάθε πελάτη.

4) Το **footage της κάμερας**, είναι προσωπικά δεδομένα πελατών όπως πλάνα που μπορεί να αποκαλύπτουν κωδικούς, συναλλαγές τους και άλλα τέτοια δεδομένα.

Λίγα λόγια για τα υπόλοιπα αγαθά του συστήματος:

- **Workstation:** είναι ειδικός υπολογιστής σχεδιασμένος για τεχνικές ή επιστημονικές εφαρμογές.
- **Scanner:** Είναι η συσκευή η οποία ανακτά πληροφορίες στο σύστημα από έγγραφα, τα οποία μετατρέπει σε ηλεκτρονική μορφή.
- **Printer:** Είναι η συσκευή η οποία μετατρέπει τις πληροφορίες του συστήματος σε έντυπη μορφή.
- **Database Server:** Αποθηκεύει σημαντικά δεδομένα της εταιρίας συνήθως σε μορφή αρχείου, τα οποία αν τυχόν καταστραφούν θα επιφέρουν μεγάλες ζημιές.
- **Web server:** Ο διακομιστής Web χειρίζεται τα αιτήματα ιστού που αποστέλλονται από επισκέπτες που επισκέπτονται τον ιστότοπό του συστήματος.
- **Switch:** Είναι υλικό δικτύωσης που συνδέει συσκευές σε ένα δίκτυο.
- **Router:** Είναι μια συσκευή δικτύωσης η οποία συνδέει την συσκευή με την οποία ενώνεται στο διαδίκτυο.
- **Laptop:** Είναι ένας φορητός υπολογιστής ο οποίος περιέχει κάποια στοιχεία της εταιρείας.
- **VoIP PHONE:** Είναι μία τεχνολογία που μετατρέπει την φωνή του χρήστη σε ψηφιακό σήμα και του επιτρέπει να κάνει “τηλεφωνήματα” μέσω υπολογιστή.
- **Τα δεδομένα τραπέζης πελατών:** αφορούν τα προσωπικά δεδομένα όλων των πελατών της τράπεζας(πχ ονοματεπώνυμο, κατοικία, υπόλοιπο λογαριασμού κλπ.).
- **Τα Bank Employee Data**: αφορούν τα προσωπικά δεδομένα όλων των εργαζομένων της τράπεζας(πχ ονοματεπώνυμο, κατοικία, διοικητική θέση κ.α.)
- **Software (windows 7 pro):** αποτελεί ένα λειτουργικό σύστημα προσωπικών υπολογιστών που κατασκευάστηκε από την Microsoft.
- **Software (windows 10 pro):** Είναι μία σειρά λειτουργικών συστημάτων προσωπικών υπολογιστών που παράγονται από την Microsoft.
- **Η ανάληψη χρημάτων από ATM**: είναι η διαδικασία κατά την οποία ο πελάτης σηκώνει τα χρήματα του από την τράπεζα μέσω ειδικής μηχανής(ATM).

- **<u>Η κατάθεση χρημάτων</u>**: είναι η διαδικασία κατά την οποία ο πελάτης αποθηκεύει τα χρήματά του στην τράπεζα.
- **<u>Η διαδικασία δημιουργίας νέου λογαριασμού</u>**: είναι η διαδικασία με την οποία ένα πρόσωπο γίνεται τραπεζικός πελάτης.
- **<u>Το Automated Teller Machine(ATM)</u>**: Είναι το μηχάνημα της τράπεζάς μέσω του οποίου κάνουν συναλλαγές οι πελάτες της.
- **<u>Διαδικασία ενημέρωσης υπολοίπου</u>**: είναι η διαδικασία με την οποία ένας πελάτης της τράπεζας μπορεί να ενημερωθεί για το υπόλοιπο του λογαριασμού του.

### Α3.1 Απειλές που εντοπίστηκαν

Οι απειλές που εντοπίσαμε για το κάθε αγαθό είναι οι εξής(ακολουθούν το πρότυπο ISO):

1)<u>όσον αφορά τα αγαθά Hardware</u>:

| **ASSETS** | **THREATS** |
|---|---|
| Workstation | *Masquerading of identity, hardware maintance, Unauthorized installation of software* |
| Scanner | *Technical failures, User error, Disclosure of passwords and sensitive data* |
| Printer | *Operations error, Information leakage* |
| Database Server | *Misuse of system resources, Destruction of records, SQL Injection* |
| Web server | *Compromising confidential information, loss of records, unauthorised access and use* |
| Switch | *Technical failures, Power failure* |
| Router | Technical failures, *Access to the network by unauthorized persons* |
| Laptop | unauthorized use of an application, Malicious code (e.g. viruses), theft |
| ATM | masquerading user identity, Hardware and Software maintenance error, Fraud |
| Dedicated Line | Fire, Water damage, interfere in net |
| VoIP PHONE | *Divulge confidential information*, *Eavesdropping, malicious user's interference* |

2)<u>όσον αφορά τα αγαθά Software</u>:

| **ASSTES** | **THREATS** |
|---|---|
| Software (windows 7 pro) | *malicious code, all apps are trusted until they're determined to be a threat or are explicitly blocked, remote ransomware attack* |
| Software (windows 10 pro) | *unauthorised collection of data, smb is exploited to launch ransomware attack, remote code execution* |

3)<u>όσον αφορά τα αγαθά δικτύου</u>:

| **ASSETS** | **THREATS** |
|---|---|
| LAN | *Remotely data collection, unauthorised connection* |

4)<u>όσον αφορά τα αγαθά δεδομένων</u>:

| **ASSETS** | **THREATS** |
|---|---|
| Bank Customer Data | Masquerading of identity, divulge personal data to unauthorized users, Falsification of records |
| Bank Employee Data | Insider Employee gets employee personal data, Unauthorized use of an application, Compromising confidential information |
| Camera footage data | Disclosure of information (e.g. pins/codes), Eavesdropping |

5)<u>όσον αφορά τα αγαθά διαδικασιών</u>:

| **ASSETS** | **THREATS** |
|---|---|
| Money Withdrawal from ATM | *Theft, Masquerading of identity, Fraud* |
| Money Deposit | *Application software failure, Theft* |
| New Account Opening | *Concealing user identity, Fraud* |
| Updating balance | *Unauthorized access, Disclosure of information* |

**A3.2 Ευπάθειες που εντοπίστηκαν**

Οι ευπάθειες που εντοπίσαμε για το κάθε αγαθό είναι οι εξής:

1)<u>όσον αφορά τα αγαθά Hardware</u>:

| **ASSETS** | **vulnerabilities** |
|---|---|
| Workstation | *Iinadequate or irregular backup, Inadequate password management, Uncontrolled download from the Internet* |
| Scanner | *Complicated user interface, Equipment sensitivity to changes in voltage, Uncontrolled scanning of data* |
| Printer | *Inadequate supervision of employees, Disposal of storage media without* |

| | |
|---|---|
| | *deleting data* |
| Database Server | *Rules not appropriately configured, Inadequate or irregular backup, Lack of policy for the use of cryptography* |
| Web server | *Inadequate security awareness, Single copy, Lack of access control policy, cross site scripting (xss)* |
| Switch | *Equipment sensitivity to changes in voltage, Inadequate material protection* |
| Router | *Default passwords, incomplete package sender authentication, Inadequate cabling security* |
| Laptop | *Complicated unprotected interfaces, lack of clean desk and clear screen policy* |
| ATM | *Inadequate maintenance, Uncontrolled use of information systems, inadequate identification methods* |
| Dedicated Line | *Inadequate cabling security, Location vulnerable to flooding, public IP address* |
| VoIP PHONE | *Lack of or poor implementation of internal audit, Unprotected public connections* |

2)όσον αφορά τα αγαθά Software:

| **ASSTES** | **Vulnerabilities** |
|---|---|
| Software (windows 7 pro) | *Insecure library download, gdi access violation, windows 7 pro will soon stop support* |
| Software (windows 10 pro) | *Windows 10 Wi-Fi sense contact sharing, re-direct to smb vulnerability* |

3)όσον αφορά τα αγαθά Δικτύου:

| **ASSETS** | **Vulnerabilities** |
|---|---|
| LAN | *transmitting data through the air using radio frequency transmission or infrared, hotspots and guest networks operate in an open system mode allowing any stations to connect to that network without requiring any form of authentication* |

4)<u>όσον αφορά τα αγαθά Δεδομένων</u>:

| **ASSETS** | **Vulnerabilities** |
|---|---|
| Bank Customer Data | *Database not encrypted, inadequate or irregular backup, Inadequate security awareness* |
| Bank Employee Data | *Database not encrypted, iinadequate or irregular backup, Inadequate supervision of employees* |
| Camera footage data | *Inadequate security awareness, buffer overflow (maybe loose data), weak protocols* |

5)<u>όσον αφορά τα αγαθά Διαδικασιών</u>:

| **ASSETS** | **Vulnerabilities** |
|---|---|
| Money Withdrawal from ATM | *Lack of biometrical methods, uninformed users, button sound (like payphone)* |
| Money Deposit | *uninformed users, shortage of information about the receiver, lack of data protection* |
| New Account Opening | *Unorganized system, lack of data protection* |
| Updating balance | *lack of data protection, machine malfunction* |

### A3.3 Αποτελέσματα αποτίμησης

Ενδεικτικές επιπτώσεις για κάθε αγαθό όσον αφορά την κάθε κατηγορία του C.I.A:

Οι επιπτώσεις που εντοπίσαμε για το σύστημα, από το κάθε αγαθό είναι οι εξής:

1)<u>όσον αφορά τα αγαθά Hardware</u>:

| **Αγαθό** | **Επίπτωση στην διαθεσιμότητα (availability)** | **Επίπτωση στην ακεραιότητα (Integrity)** | **Επίπτωση στην εμπιστευτικότητα (confidentiality)** |
|---|---|---|---|
| Workstation | Loss of functionality, inability to operate successfully the functions of the bank. | Change important files and drives the system to misuse/ loose / change data. May change some important customers data. | Gives the opportunity to malicious people to find information about the bank or customers and use it for theirs's benefits. |
| Scanner | Loose the ability to convert files to data and use them. | Poor conversion to data may confuse the employee. | Divulge entrusted information about the bank or the customers to authorized people, so they can exploit them. |

| | | | |
|---|---|---|---|
| Printer | Great delays to transactions | Poor copy of the data may confuse the customers or the employee | May leak information about the bank or customers data and malicious users will use them for their purposes |
| Database Server | Inability to process electronic transactions. | destroy important data or information that we backed up, loose information | malicious user takes advantage of the data and use them to steal or fraud. |
| Web server | delays to the system and corruption of important procedures. | Change of data, queries and falsify, manipulate the operational functionality. | May steal important registrations and use them to exploit data. |
| Switch | cause serious delays to network connections. | No connection to the network or misrouting packages and manipulate data. | have access to network packages and reveal important information to the unauthorised user. |
| Router | Delays to the connection of internet, loss the ability to transfer data and information. | Enforced loss or modify data, information or share them with the wrong people. | let malicious people enter the LAN and steal data, information. |
| Laptop | Loss of functionality, inability to operate successfully the functions of the bank. | Change important files and drives the system to misuse /loose/change data and cause economic damage or operational problems. | divulge important information and private data about the bank or the customers to unauthorised users and allow them to use them for their own purpose. |
| ATM | Makes difficult, impossible for the client to make money transactions | change economics data and loose customer's and bank's money, causing legal problems. | Customer's passwords, balance can be revealed and used by unauthorised users to steal money. |
| Dedicated Line | Slows down the speed of internet and telephone connection. | cut of the link between the offices, the net, telephone communications. | Via dedicated line they send confidential data, so without an encryption anyone can stole them and use them for their |

| | | | |
|---|---|---|---|
| | | | own purpose. |
| VoIP phone | The delay in calls may make unable to remoted executives to communicate effectively and take decisions for the bank. This would cause disorientation. | If somebody take the control of the VoIP phones may redirect the call to another person and cause frauds. | May detect and steal important and private information. Or even use the voice of person for other frauds. |

2)<u>όσον αφορά τα αγαθά Software</u>:

| **Αγαθό** | **Επίπτωση στην διαθεσιμότητα (availability)** | **Επίπτωση στην ακεραιότητα (Integrity)** | **Επίπτωση στην εμπιστευτικότητα (confidentiality)** |
|---|---|---|---|
| Software (windows 7 pro) | A delay to the operating system will "crack" every single device that uses that system or even make impossible to detect a malicious software such as Rootkit, which causes an important delay. | If somebody can change the code of the software may embody viruses to the system or create loopholes to ensure full access to the system. So, they are able to destroy the operational system and make the machine useless. | If somebody is able to monitor the code and the data, this means that they are also able to find ways to enter and attack to the system. In conclusion to collapse the operational system. |
| Software (windows 10 pro) | A buffer delay may be caused and collect a number of waiting process that will probably cause collapse of the system (denial services) | A full access to the software, may allow the intrusive to unencrypt encrypted data and codes and take superusers' privileges. | If somebody is able to monitor the code and the data, this means that they are also able to find ways to enter and attack to the system. In conclusion to collapse the operational system. |

3)<u>όσον αφορά τα αγαθά δικτύου</u>:

| **Αγαθό** | **Επίπτωση στην διαθεσιμότητα (availability)** | **Επίπτωση στην ακεραιότητα (Integrity)** | **Επίπτωση στην εμπιστευτικότητα (confidentiality)** |
|---|---|---|---|
| Lan | May block or cause great delay to the propagation of the information and make problematic the functions of the | The malicious person may cut the connection of some components of the network and make impossible the | May monitor the moves of the network and detect information via the pulses of the network. |

| | | | |
|---|---|---|---|
| | bank. | transferring of the data. | |

4) <u>όσον αφορά τα αγαθά δεδομένων</u>:

| **Αγαθό** | **Επίπτωση στην διαθεσιμότητα (availability)** | **Επίπτωση στην ακεραιότητα (Integrity)** | **Επίπτωση στην εμπιστευτικότητα (confidentiality)** |
|---|---|---|---|
| Bank Customer Data | Loss of system functionality, the management of Bank customer data becomes hard to access them. | Falsification of important information that drives to operational problems. | Important confidential information and personal customer data are disclosed and used for fraud. |
| Bank Employee Data | Loss of operational effectiveness, the management of Bank Employee data becomes hard to access. This result in loss of productive time. | Drives the system to use wrong Employee data. This can cause operational problems due to error data management. | Important confidential information and personal Bank Employee data are disclosed and used by unauthorised users. |
| Camera footage data | Makes it difficult to recover in case that we need proofs/evidence for an action. | drives the system to continue using incorrect data which may lead to inaccuracies, fraud or wrong decisions. | divulge important camera footage data about the Bank, the employees, the customers etc (e.g. passwords if the camera is looking at the ATM space). |

5)<u>όσον αφορά τα αγαθά διαδικασιών</u>:

| **Αγαθό** | **Επίπτωση στην διαθεσιμότητα (availability)** | **Επίπτωση στην ακεραιότητα (Integrity)** | **Επίπτωση στην εμπιστευτικότητα (confidentiality)** |
|---|---|---|---|
| Money Deposit | impeding system's performance and cause annoying delays. | inaccuracies and wrong economic management. | Important confidential information (money deposits) and personal private data are violated and disclosed. |
| New Account Opening | discourage the customer to store their money in the bank, the system will lose customers. | Fake details, altered information or fault personal data will cause frauds. | Important entrusted information and personal customer data are disclosed and used by unauthorised |

| | | | |
|---|---|---|---|
| | | | malevolent users for their own purposes. |
| Updating balance | Causes problems in the operation of the business and the performance of the organization by losing time. | leads to inaccuracies and wrong economic management. | Important entrusted information and personal customer data are notified and used by unauthorised users for their own purpose. |
| Money withdrawal | discourage the customer to store their money in the bank, the system will lose customers. | Change of economic data and loss of costumers' money, this would cause legacy issues | Malicious users can see the balance of the customers. The customer will be targeted and the bank will be exposed. |

| | Απώλεια διαθεσιμότητας | | | | | | | Απώλεια ακεραιότητας | | | | | Αποκάλυψη | | | Αστοχίες και λάθη στην τηλεπικοινωνιακή μετάδοση | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Αγαθά των ΠΣ** | 3 ώρες | 12 ώρες | 1 μέρα | 2 μέρες | 1 εβδομάδα | 2 εβδομάδες | 1 μήνας | Ολική καταστροφή | Μερική απώλεια | Σκόπιμη αλλοίωση | Λάθη μικρής κλίμακας | Λάθη μεγάλης κλίμακας | Εσωτερικούς | Παρόχους Υπηρεσιών | Εξωτερικούς | Επανάληψη μηνυμάτων | Αποτοίχιση αποστολέα | Αποτοίχιση παραλήπτη | Άρνηση αποστολής ή παραλαβής | Παρεμβολή λανθασμένων μηνυμάτων | Λανθασμένη δρομολόγηση | Παρακολούθηση κίνησης | Μη παράδοση | | Απώλεια ακολουθίας μηνυμάτων |
| Bank Customer Data | 1 | 2 | 3 | 3 | 4 | 5 | 6 | 7 | 7 | 8 | 4 | 7 | 6 | 7 | 8 | 2 | 4 | 5 | 4 | 5 | 5 | 8 | 4 | 5 | |
| Bank Employee Data | 2 | 3 | 4 | 4 | 5 | 6 | 7 | 8 | 8 | 8 | 5 | 8 | 8 | 7 | 9 | 3 | 4 | 5 | 5 | 4 | 7 | 8 | 4 | 5 | |
| Camera footage data | 2 | 5 | 6 | 7 | 8 | 8 | 9 | 9 | 7 | 8 | 6 | 9 | 6 | 6 | 9 | | 2 | | 1 | 4 | | 8 | | | |
| Money Withdrawal from ATM | 1 | 2 | 2 | 3 | 4 | 4 | 6 | 7 | 4 | 7 | 5 | 7 | 4 | 4 | 8 | 2 | 5 | 7 | 4 | 3 | 5 | 7 | 6 | 3 | |

| | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Money Deposit | 1 | 2 | 2 | 3 | 3 | 3 | 4 | 6 | 3 | 3 | 4 | 8 | 6 | 3 | 7 | 2 | 2 | 5 | 5 | 6 | 6 | 7 | 5 | 2 |
| New Account Opening | 1 | 2 | 2 | 3 | 3 | 4 | 5 | 7 | 5 | 7 | 5 | 7 | 4 | 3 | 7 | 2 | | | 1 | | | 5 | | 1 |
| Updating balance | 1 | 2 | 2 | 3 | 3 | 3 | 4 | 6 | 6 | 7 | 7 | 7 | 4 | 3 | 7 | 2 | 4 | | | 5 | 4 | 6 | | 1 |
| Workstation | 6 | 7 | 7 | 8 | 8 | 8 | 8 | 9 | 7 | 8 | 4 | 6 | 3 | 4 | 7 | 3 | 2 | 2 | | 4 | | 8 | | 5 |
| Scanner | 1 | 1 | 2 | 2 | 3 | 3 | 4 | 5 | 4 | 5 | 2 | 6 | 2 | 2 | 7 | 1 | 2 | 2 | 3 | 3 | 7 | 7 | 4 | 3 |
| Printer | 1 | 2 | 2 | 3 | 3 | 4 | 5 | 5 | 4 | 7 | 4 | 7 | 3 | 3 | 8 | 2 | 2 | 1 | | 2 | 4 | 7 | 3 | 2 |
| Database Server | 7 | 7 | 8 | 8 | 8 | 9 | 9 | 10 | 7 | 8 | 6 | 9 | 6 | 7 | 9 | 2 | | | 6 | 4 | 8 | 10 | 4 | 6 |
| Web server | 7 | 7 | 8 | 8 | 8 | 9 | 9 | 10 | 7 | 9 | 6 | 9 | 6 | 7 | 9 | | | 1 | | 4 | 6 | 10 | | 6 |
| Switch | 3 | 4 | 5 | 5 | 6 | 7 | 7 | 3 | 3 | 2 | 1 | 3 | 1 | 1 | 1 | | | | | | 5 | 8 | | |
| Router | 4 | 4 | 5 | 6 | 7 | 7 | 8 | 4 | 3 | 7 | 4 | 7 | 3 | 2 | 8 | 2 | 2 | 1 | 2 | 7 | 9 | 9 | 6 | |
| Laptop | 3 | 4 | 5 | 6 | 7 | 7 | 8 | 7 | 7 | 9 | 6 | 8 | 5 | 4 | 9 | 4 | | | | 2 | 6 | 9 | | 6 |
| ATM | 3 | 4 | 4 | 4 | 5 | 5 | 7 | 8 | 7 | 8 | 6 | 8 | 4 | 4 | 9 | 3 | | 5 | | 5 | 5 | 9 | 6 | 5 |
| Dedicated Line | 2 | 2 | 3 | 3 | 4 | 4 | 5 | 3 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 5 | | | | | 6 | 7 | | |

| | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Software (windows 7 pro) | 4 | 6 | 7 | 8 | 8 | 9 | 9 | 7 | 9 | 7 | 8 | 6 | 6 | 6 | 10 | 2 | | | | 4 | 5 | 9 | 4 | 4 | |
| Software (windows 10 pro) | 4 | 6 | 7 | 8 | 8 | 9 | 9 | 7 | 9 | 7 | 8 | 6 | 6 | 6 | 10 | 2 | | | | 4 | 5 | 9 | 4 | 4 | |
| VoIP phone | 1 | 2 | 3 | 3 | 4 | 4 | 6 | 6 | 5 | 8 | 4 | 6 | 4 | 4 | 9 | 3 | 3 | 4 | 3 | 5 | 8 | 9 | 5 | 6 | |
| Lan | | 3 | 4 | 5 | 5 | 6 | 6 | 7 | 8 | 6 | 8 | 5 | 7 | 4 | 3 | 9 | | | | 3 | 5 | 8 | 9 | 5 | |

**Β2. ΠΡΟΤΕΙΝΟΜΕΝΑ ΜΕΤΡΑ ΑΣΦΑΛΕΙΑΣ**

Τα προτεινόμενα Μέτρα Προστασίας εντάσσονται σε έντεκα (11) γενικές κατηγορίες:

Α1. Προσωπικό – Προστασία Διαδικασιών Προσωπικού

Α2. Ταυτοποίηση και αυθεντικοποίηση

Α3. Έλεγχος προσπέλασης και χρήσης πόρων

Α4. Διαχείριση εμπιστευτικών δεδομένων

Α5. Προστασία από τη χρήση υπηρεσιών από τρίτους

Α6. Προστασία λογισμικού

Α7. Διαχείριση ασφάλειας δικτύου

Α8. Προστασία από ιομορφικό λογισμικό

Α9. Ασφαλής χρήση διαδικτυακών υπηρεσιών

Α10. Ασφάλεια εξοπλισμού

Α11. Φυσική ασφάλεια κτιριακής εγκατάστασης

Τα μέτρα έχουν εφαρμογή στο ΠΣ του/της *data_central_bank*.

Α1 **Προσωπικό – Προστασία Διαδικασιών Προσωπικού**

| ASSETS | Μέτρα ασφαλείας |
|---|---|
| Software (windows 7 pro) | Εστίαση της προσοχής των υπάλληλων στο τι κατεβάζουν και στα e-mails που ανταποκρίνονται. |

Α2 **Ταυτοποίηση και αυθεντικοποίηση**

| ASSETS | Μέτρα ασφαλείας |
|---|---|
| Money Withdrawal from ATM | Θα πρέπει να γίνει μια ισχυρή ταυτοποίηση των πελατών (πχ δακτυλικό αποτύπωμα, ίριδα ματιού) κάνοντας έτσι την ταυτοποίηση του ατόμου πιο έγκυρη. |
| Money Deposit | Ο αποστολέας και ο παραλήπτης θα πρέπει να επιβεβαιώσουν μέσω κατάλληλου εμπιστευτικού κωδικού την συναλλαγή. |
| Updating balance | Ενίσχυση βιομετρικών μεθόδων αναγνώρισης χρήστη. |
| Scanner | Περιοδική αναθεώρηση και έλεγχος των δικαιωμάτων πρόσβασης από τους χρήστες. Η περίοδος των 6 μηνών συνιστάται. |

A3 **Έλεγχος προσπέλασης και χρήσης πόρων**

| ASSETS | Μέτρα ασφαλείας |
|---|---|
| Bank Employee Data | Απόκρυψη των ευαίσθητων δεδομένων με χρήση επιπλέον περιορισμών, εξουσιοδοτήσεων, κωδικών. |
| Laptop | Για προστασία των δεδομένων μας σε περίπτωση κλοπής, πρέπει να θέσουμε ισχυρούς κωδικούς(π.χ. φράσεις) και να αποφύγουμε όσους περιέχουν στοιχεία σχετικά με εμάς. |
| Workstation | Ασφαλής χορήγηση προσωρινών passwords και αλλαγής τους από τους ίδιους τους χρήστες (π.χ. φράσεις) και να αποφύγουμε όσους περιέχουν στοιχεία σχετικά με εμάς. |
| Router | Ασφαλής χορήγηση passwords, τα οποία θα αλλάζουν τακτικά. |

A4 **Διαχείριση εμπιστευτικών δεδομένων**

| ASSETS | Μέτρα ασφαλείας |
|---|---|
| Bank Customer Data | Δημιουργία backup των data των πελατών. |
| Camera footage data | Θα πρέπει να πραγματοποιείται λήψη ημερήσιου backup των δεδομένων με καθορισμένες ασφαλείς μεθόδους και σε καθορισμένους χρόνους. |
| Atm | Χρήση τεχνολογίας “jitter” για να γίνει πιο δύσκολο σε κάποιον κακόβουλο να αντιγράψει δεδομένα χρεωστικών και πιστωτικών καρτών. |
| WEB Server | Χρήση κατάλληλων “response headers” |

**A5 Προστασία από τη χρήση υπηρεσιών από τρίτους**

| ASSETS | Μέτρα ασφαλείας |
|---|---|
| Bank Customer Data | Κρυπτογράφηση των στοιχείων των πελατών. |
| Bank Employee Data | Κρυπτογράφηση των προσωπικών στοιχείων των υπαλλήλων. |
| Camera footage data | κρυπτογράφηση δεδομένων κατά την αποθήκευση τους στην βάση με την χρήση ισχυρών αλγορίθμων. |
| New Account Opening | Απόκρυψη των ευαίσθητων δεδομένων από τρίτα πρόσωπα με χρήση επιπλέον περιορισμών, εξουσιοδοτήσεων, κωδικών. |
| New Account Opening | Κρυπτογράφηση κατά την αποθήκευση των |

| | |
|---|---|
| | στοιχείων. |
| VoIp phone | Αλλαγή των προκαθορισμένων κωδικών πρόσβασης με νέους ισχυρούς. |
| Printer | Έλεγχος πρόσβασης σε όλα τα συστήματα με τον καθορισμό διαφορετικών κατηγοριών χρηστών με συγκεκριμένα και αυστηρά καθορισμένα δικαιώματα. |
| WEB Server | Κρυπτογράφηση δεδομένων κατά την αποθήκευση τους στη βάση, όταν αυτό κριθεί αναγκαίο, με την χρήση ισχυρών αλγορίθμων. |

A6 **Προστασία λογισμικού**

| ASSETS | Μέτρα ασφαλείας |
|---|---|
| Updating balance | Ενημέρωση software για να αποφευχθούν τρύπες στο σύστημα. |
| Atm | Να κατεβάζουμε συχνά κατάλληλα "patches" και να ενημερώνουμε ATM windows προκειμένου να αποφευχθούν τρύπες στο software. |
| Software (windows 7 pro) | Διαρκής ενημέρωση του λογισμικού προστασίας καθώς και όλων των εφαρμογών. |
| Workstation | Διαρκής ενημέρωση και αναβάθμιση (update, patching) όλων των συστημάτων |
| WEB Server | Όλα τα στοιχεία του εξοπλισμού θα πρέπει να προστατεύονται με συστήματα UPS. |

A7 **Διαχείριση ασφάλειας δικτύου**

| ASSETS | Μέτρα ασφαλείας |
|---|---|
| Router | Απενεργοποίηση Wi-fi-protected setup (wps)(κρυπτογραφημένη σύνδεση μεταξύ της συσκευής και τους δικτύου. |
| Lan | Να το τοποθετηθεί σε ένα ξεχωριστό δευτερεύον δίκτυο πίσω από το δικό του Router ή firewall. |

A8 **Προστασία από ιομορφικό λογισμικό**

| ASSETS | Μέτρα ασφαλείας |
|---|---|
| Laptop | Εγκατάσταση ενός περιβάλλοντος εικονικής μηχανής για να κάνουμε οτιδήποτε επικίνδυνο μέσα σε αυτό(π.χ ένα άνοσο Linux Vm) αν μολυνθεί το διαγράφουμε και εγκαθιστούμε ένα νέο. |
| Software( windows 10 pro) | Να χρησιμοποιήσουμε BitLocker Drive encryption και έτσι προστατεύεται το λειτουργικό από "offline" επιθέσεις. |
| Software( windows 10 pro) | Να χρησιμοποιηθεί κατάλληλο και πλήρως ενημερωμένο antivirus πρόγραμμα συμβατό με windows 10. |
| Lan | Να εγκατασταθεί firewall σε κάθε access point του δικτύου και να χρησιμοποιηθούν κατάλληλα πρωτόκολλα ασφάλειας όπως το wpa/ wpa2. |
| Database Server | «καθαρισμός» από κακόβουλο λογισμικό και επικύρωση των δεδομένων του. |

A9 **Ασφαλής χρήση διαδικτυακών υπηρεσιών**

| ASSETS | Μέτρα ασφαλείας |
|---|---|
| VoIp phone | Να ενεργοποιηθεί το NAT(network address translation) έτσι ώστε η IP διεύθυνση να γίνει ιδιωτική και να μην είναι πλέον προσπελάσιμη από απομακρυσμένες συσκευές. |
| Dedicated Line | Μετατροπή της IP διεύθυνσής του από δημόσια σε ιδιωτική στο δίκτυο. |
| Dedicated Line | Να διαχωρίσουμε τη γραμμή internet-τηλεφώνου. |

A10 **Ασφάλεια εξοπλισμού**

| ASSETS | Μέτρα ασφαλείας |
|---|---|
| Money Withdrawal from ATM | Ενίσχυση φύλαξης στο ATM από κατάλληλο εκπαιδευμένο προσωπικό. |
| Money Deposit | Ενίσχυση φύλαξης στο ATM από κατάλληλο εκπαιδευμένο προσωπικό. |
| Switch | Υλική προστασία του switcher. |
| Switch | Όλα τα στοιχεία του εξοπλισμού θα πρέπει να προστατεύονται με συστήματα UPS. |

**A11 Φυσική ασφάλεια κτιριακής εγκατάστασης**

| ASSETS | Μέτρα ασφαλείας |
|---|---|
| Database Server | Τα αντίγραφα ασφάλειας θα πρέπει να φυλάσσονται σε διαφορετικούς χώρους από τον χώρο που λειτουργεί το κύριο πληροφοριακό σύστημα. |
| Database Server | Κλιματισμός προς αποφυγή υπερθέρμανσης. |

**Α4. ΣΥΝΟΨΗ ΠΙΟ ΚΡΙΣΙΜΩΝ ΑΠΟΤΕΛΕΣΜΑΤΩΝ**

Σύμφωνα με το "risk priority number" το 5% των σημαντικότερων ευρημάτων φαίνεται να είναι τα εξής τρία ευρήματα:

1. ***Software (Windows 7 pro):*** Το λειτουργικό αυτό σύστημα, έχει την ευπάθεια ότι σύντομα (2020) η Microsoft θα σταματήσει να του παρέχει υποστήριξη και υπηρεσίες με αποτέλεσμα να μην γίνονται αναβαθμίσεις ασφάλειας στο λειτουργικό. Αυτό μπορεί να το εκμεταλλευτεί κάποιος και να αρχίσει επιθέσεις εκτέλεσης απομακρυσμένου κώδικα και επιθέσεις τύπου "ransomware". Τρομαχτικές όμως καθυστερήσεις ή μπλοκαρίσματα του λειτουργικού θα το κάνουν σταδιακά να καταρρεύσει ή ακόμη θα καταστεί αδύνατο να εντοπίσουμε το κακόβουλο λογισμικό που το έχει προσβάλει. Μια λύση είναι να αποτρέψουμε το κατέβασμα πηγαίου κώδικα από το διαδίκτυο καθώς και να αποκλείσουμε e-mails ενεργού περιεχομένου. Αν τώρα προσβληθούμε η καταλληλότερη αντιμετώπιση είναι μάλλον το format του συστήματος.
2. ***Database server***: Σκοπός του διακομιστή είναι να εμποδίζει μη εξουσιοδοτημένα και επικίνδυνα αιτήματα. Δυστυχώς μπορεί συχνά να παραλείπεται η τακτική εξασφάλιση ολοκληρωμένου backup. Εγκυμονεί λοιπόν ο κίνδυνος να καταστραφούν οι εγγραφές του server. Ως επίπτωση λοιπόν ενδέχεται να καταστραφούν ή να χαθούν σημαντικά δεδομένα ή πληροφορίες της εταιρείας που δεν μπορούν να ανακτηθούν. Για να προφυλαχθούμε από αυτή την κατάσταση, οφείλουμε να κρατάμε πολλαπλά αντίγραφα των εγγραφών του server και μάλιστα σε διαφορετική τοποθεσία από αυτή που είναι η θέση του server (για να διαφυλαχθούν και σε περιπτώσεις φυσικών καταστροφών)
3. ***Web server***: Είναι ζωτικής σημασίας πόρος, καθώς είναι χρειάζεται για τις διαδικτυακές εφαρμογές της εταιρείας, την αποθήκευση επεξεργασία και μεταφορά ιστοσελίδων. Μια όμως σοβαρή ευπάθεια που αντιμετωπίζει είναι το λεγόμενο "cross site scripting(xss)" η δυνατότητα δηλαδή ενσωμάτωσης στην εφαρμογή javascript για να κάνει κάτι κακόβουλο. Υπάρχει λοιπόν ο κίνδυνος να αποκτήσουν πρόσβαση σε σημαντικά δεδομένα μη εξουσιοδοτημένοι χρήστες στα δεδομένα του συστήματος. Εάν συμβεί αυτό, τότε μπορεί να αλλαχθούν δεδομένα ή queries, να αλλοιωθούν εγγραφές και να χειραγωγηθούν λειτουργικές λειτουργίες. Για να ξεφύγουμε από τέτοιες επιθέσεις, μπορούμε να χρησιμοποιήσουμε κατάλληλα " response headers", για να αποτρέψουμε το XSS σε αποκρίσεις HTTP που δεν προορίζονται να περιέχουν οποιαδήποτε HTML ή JavaScript.

## A5. Bibliography


- https://advisera.com/27001academy/knowledgebase/threats-vulnerabilities/
- https://cyware.com/news/what-is-smb-vulnerability-and-how-it-was-exploited-to-launch-the-wannacry-ransomware-attack-c5a97c48
- https://www.upguard.com/articles/top-10-windows-7-vulnerabilities-and-remediation-tips
- https://www.upguard.com/articles/top-10-windows-10-security-vulnerabilities-and-how-to-fix-them?hsCtaTracking=cd58f39d-6b3c-49e8-94ff-63afbe46f6c7%7Cf368b6a3-4d48-4388-9fd8-d57004d3428c
- https://www.researchgate.net/publication/269524313_Wireless_LAN_Security_Threats_Vulnerabilities
- https://infosec.aueb.gr/Courses/lectures/iss/2b.%20Advanced%20Risk%20Assessment_RA_Controls_Processes-Stergiopoulos.pdf
- https://www.webopedia.com/TERM/L/local_area_network_LAN.html
- https://helpdeskgeek.com/windows-7/difference-between-windows-7-home-professional-and-ultimate/
- https://gadgets.ndtv.com/laptops/features/windows-10-home-vs-windows-10-pro-differences-new-features-718532
- https://www.bankinfosecurity.com/10-tips-to-improve-atm-security-a-2852
- https://askleo.com/how-to-keep-using-windows-7-safely-after-support-ends/
- https://www.onsip.com/voip-resources/voip-solutions/business-phone-security-5-measures-to-prevent-voip-fraud-and-hackers
- https://searchsecurity.techtarget.com/answer/How-to-protect-a-LAN-from-unauthorized-access
- https://www.lifewire.com/what-is-wifi-sense-windows-10-4586925
- https://www.commonplaces.com/blog/6-common-website-security-vulnerabilities/
- https://portswigger.net/web-security/cross-site-scripting