ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΚΑΙ ΚΡΙΣΙΜΩΝ ΥΠΟΔΟΜΩΝ

ΣΧΕΔΙΟ ΑΣΦΑΛΕΙΑΣ

ΣΥΓΓΡΑΦΕΙΣ: Σίγας Γιώργος 3160158, Νταλές Θανάσης 3160117, Λάκκας Γιάννης 3160078

ΕΡΓΑΣΙΑ ΧΕΙΜΕΡΙΝΟΥ ΕΞΑΜΗΝΟΥ 2019

Contents

Α1. ΕΙΣΑΓΩΓΗ

Το Σχέδιο Ασφαλείας (Security Plan) για τα πληροφοριακά συστήματα ενός οργανισμού αποτελείται από την Πολιτική Ασφάλειας και το σύνολο των Μέτρων Ασφάλειας. Η Πολιτική Ασφάλειας των πληροφοριακών συστημάτων περιλαμβάνει το σκοπό και τους στόχους της ασφάλειας , οδηγίες , διαδικασίες , κανόνες , ρόλους και υπευθυνότητες που αφορούν την προστασία των Π.Σ. του οργανισμού, διατυπώνεται σε ένα έγγραφο το οποίο θα πρέπει να γνωρίζουν και να εφαρμόζουν όλοι οι χρήστες των Π.Σ. . Οι οδηγίες και οι διαδικασίες που περιλαμβάνονται στην πολιτική ασφάλειας υλοποιούνται με την εφαρμογή των μέτρων ασφάλειας ή προστασίας.

Α1.1 Περιγραφή Εργασίας

Το παρόν έγγραφο αποτελεί προϊόν μελέτης του σχεδίου ασφάλειας μιας εταιρίας που ειδικεύεται σε θέματα τραπεζών που επεξεργάζονται προσωπικά δεδομένα στα πλαίσια της γραπτής εργασίας προόδου του μαθήματος «Ασφάλεια Πληροφοριακών Συστημάτων» . Το παρόν σχέδιο ασφάλειας συντάχθηκε σύμφωνα με το πρότυπο ISO27001K και παρουσιάζει όλα τα βήματα ανάλυσης και διαχείρισης της επικινδυνότητας του πληροφοριακού συστήματος της εταιρίας . Συνεπώς γίνεται προσδιορισμός και αποτίμηση των αγαθών του πληροφοριακού συστήματος της εταιρίας , ανάλυση της επικινδυνότητας που προκύπτει από αυτά (αγαθά) καθώς και εντοπισμός και περιγραφή των οργανωτικών και τεχνικών μέτρων που πρέπει να ληφθούν για τη διαχείριση της επικινδυνότητας.

Α1.2 Δομή παραδοτέου

Αρχικά γίνεται μια σύντομη παρουσίαση της μεθοδολογίας που χρησιμοποιήθηκε για την μελέτη και σύνταξη του σχεδίου ασφάλειας . Ακολουθεί η αναλυτική καταγραφή του υπάρχοντος πληροφοριακού συστήματος της εταιρίας . Έπειτα ακολουθεί το κύριο μέρος της ανάλυσης της επικινδυνότητας , δηλαδή η αποτίμηση των αγαθών του πληροφοριακού συστήματος καθώς και των εγκαταστάσεων της τράπεζας , η αποτίμηση των ευπαθειών και των πιθανών απειλών που εντοπίστηκαν . Στη συνέχεια παρουσιάζονται τα προτεινόμενα μέτρα ασφάλειας που έχουν ως σκοπό να μειώσουν την πιθανότητα εμφάνισης περιστατικών ανασφάλειας , να αντιμετωπίσουν ευπάθειες του Π.Σ. ή/και να περιορίσουν τις συνέπειες των ανεπιθύμητων γεγονότων που μπορεί να συμβούν στο Π.Σ. . Τέλος γίνεται μια σύντομη περιγραφή των πιο κρίσιμων (με την υψηλότερη επικινδυνότητα) αποτελεσμάτων.

Α2. ΜΕΘΟΔΟΛΟΓΙΑ ΜΕΛΕΤΗΣ ΑΣΦΑΛΕΙΑΣ

Για τη Διαχείριση Επικινδυνότητας της Τράπεζας 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.

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

- 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.

Στάδιο	Βήματα
1. Προσδιορισμός και αποτίμηση αγαθών *(identification and valuation of assets)*	*Βήμα 1*: Περιγραφή πληροφοριακών συστημάτων και εγκαταστάσεων *Βήμα 2:* Αποτίμηση αγαθών πληροφοριακών συστημάτων και εγκαταστάσεων *Βήμα 3:* Επιβεβαίωση και επικύρωση αποτίμησης
2. Ανάλυση επικινδυνότητας *(risk analysis)*	*Βήμα 1:* Προσδιορισμός απειλών που αφορούν κάθε Αγαθό (asset) *Βήμα 2:* Εκτίμηση απειλών (threat assessment) και αδυναμιών (vulnerability assessment) *Βήμα 3:* Υπολογισμός επικινδυνότητας συνδυασμών Αγαθό-Απειλή-Αδυναμία *Βήμα 4:* Επιβεβαίωση και επικύρωση βαθμού επικινδυνότητας
3. Διαχείριση επικινδυνότητας *(risk management)*	*Βήμα 1:* Προσδιορισμός προτεινόμενων αντιμέτρων *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 Τράπεζας, τα οποία με το πέρας της μελέτης θα επικαιροποιηθούν, αναβαθμιστούν ή σε κάποιες περιπτώσεις αντικατασταθούν.

➤ ΠΑΡΑΔΟΧΕΣ

Θεωρούμε ότι το υποκατάστημα της τράπεζας είναι χωρισμένο σε 3 χώρους . Τον κύριο χώρο (Main Area) , το γραφείο του διευθυντή(Director's Office) και τέλος την αίθουσα υπολογιστών(Computer Room) .

Α2.1.1 Υλικός εξοπλισμός (hardware)

Στο κύριο χώρο (Main Area) υπάρχουν 3 όμοιοι υπολογιστές (Workstations) , ένας εκτυπωτής , μια συσκευή σάρωσης (Scanner), το ATM της τράπεζας και τέλος ένα switch στο οποίο συνδέονται όλες οι συσκευές του κύριου χώρου δημιουργώντας ένα μικρό δίκτυο που αποτελείται από όλες τις συσκευές της Main Area.

Στο γραφείο του διευθυντή υπάρχει το προσωπικό laptop του διευθυντή , ένα VoIP τηλέφωνο ,μια συσκευή εκτύπωσης (printer) και τέλος ένα switch στο οποίο συνδέονται όλες οι συσκευές του γραφείου.

Στην αίθουσα υπολογιστών (Computer Room) υπάρχει ο Database και ο Web Server της τράπεζας, ένας υπολογιστής (Workstation), μια κάμερα παρακολούθησης του χώρου και ένα switch στο οποίο συνδέονται μέσω Ethernet όλες οι συσκευές της αίθουσας δημιουργώντας ένα ακόμη μικρό δίκτυο αποτελούμενο μόνο από τις συσκευές της αίθουσας υπολογιστών. Τέλος στην αίθουσα υπολογιστών βρίσκεται ένα router στο οποίο συνδέονται τα 3 switch και είναι υπεύθυνο για την πρόσβαση στο Internet καθώς και στο Central Bank Data Center μέσω μιας αποκλειστικής γραμμής. Η σύνδεση του router με το Internet προστατεύεται από μια συσκευή Firewall που επίσης βρίσκεται στο Computer Room.

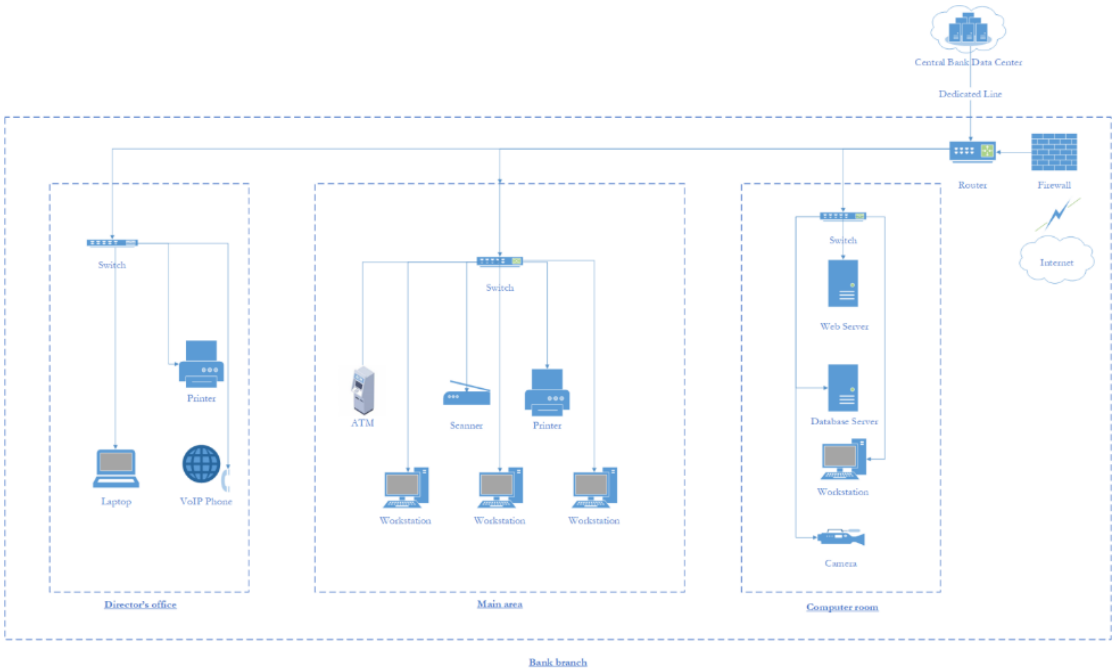
1. Κυρίως Χώρος (Main Area)
    - HP Pro G2 MT Workstation (A-0002 / AMCWS002)
    - HP Pro G2 MT Workstation (A-0003 / AMCWS003)
    - HP Pro G2 MT Workstation (A-0004 / AMCWS004)
    - Epson Perfection V370 Scanner (A-0005 / AMSC0001)
    - HP DeskJet 2130 Printer (A-0007 / AMPR0002)
    - TP-LINK TL-SG1005D Switch (A-0012 / AMCSW002)
    - NCR Personas 75-Series Automated Teller Machine (A-0025 / Automated Teller Machine (ATM))
2. Γραφείο Διευθυντή(Director's Office)
    - HP DeskJet 2130 Printer (A-0006 / AMPR0001)
    - TP-LINK TL-SG1005D Switch (A-0013 / AMCSW003)
    - VoIP Phone (A-0016 / VIPH0001)
    - Apple MacBook Air Laptop (A-0017 / AMLPS001)
3. Αίθουσα Υπολογιστών (Computer Room)
    - HP Pro G2 MT Workstation (A-0001 / AMCWS001)
    - Hikvision DS-2CV1021G0-IDW1 Camera (A-0008 / AMCAM001)
    - Web Server (A-0009 / AMSRV001)
    - Database Server (A-0010 / AMSRV002)
    - TP-LINK TL-SG1005D Switch (A-0011 / AMCSW001)
    - Cisco C886VA-K9 Router (A-0014 / AMCRT001)
    - Fortinet-Fortigate-400D Firewall (A-0015 / AMFW001)

A2.1.2 Λογισμικό και Εφαρμογές

- Windows 10 Pro σε όλους τους υπολογιστές (Workstations)
- Windows Server 2008 R2 στον Web Server
- Microsoft Windows 2016 Server SP1 στον Database Server
- Cisco proprietary software στο router

- Windows 10 Advanced IP Services στη συσκευή Firewall
- MAC-OS στο προσωπικό laptop του διευθυντή της τράπεζας
- Windows XP στη συσκευή ATM

A2.1.3 Δίκτυο



Το δίκτυο της τράπεζας είναι ουσιαστικά χωρισμένο σε 3 υποδίκτυα που αντιστοιχούν στους 3 προαναφερθέντες χώρους εργασίας (Main area, Director's office, Computer Room) με τη χρήση συσκευών switch, όπου ένα switch αντιστοιχεί σε κάθε χώρο. Έτσι στο switch του computer room είναι συνδεδεμένος ο Web Server της εταιρίας, ένας υπολογιστής (Workstation), και σε μια κοινή γραμμή η κάμερα παρακολούθησης του χώρου και ο Database server. Στο switch του κύριου χώρου είναι συνδεδεμένοι 3 υπολογιστές (Workstation), ένας εκτυπωτής, μια συσκευή σάρωσης (Scanner) και το ATM. Τέλος στο switch που βρίσκεται στο γραφείο του διευθυντή της τράπεζας είναι συνδεδεμένος ένας εκτυπωτής, ο προσωπικός υπολογιστής του διευθυντή (Laptop) και ένα VoIP τηλέφωνο. Οι 3 αυτές συσκευές switch συνδέονται σε ένα router το οποίο συνδέεται στο διαδίκτυο μέσω του παρόχου. Η σύνδεση με το διαδίκτυο προστατεύεται από μια συσκευή Firewall η οποία παρεμβάλλεται μεταξύ του router που είναι εγκατεστημένο στο computer room της τράπεζας και του Internet. Το router επίσης συνδέεται και στο Central Bank Data Center μέσω μιας απομονωμένης γραμμής.

A2.1.4 Δεδομένα

- **Bank Customer Data :** Τα δεδομένα που αφορούν τους πελάτες της τράπεζας.
- **Bank Employee Data :** Τα δεδομένα που αφορούν το προσωπικό της τράπεζας.
- **Paper Documents :** Έγγραφα τα οποία μπορεί να περιέχουν προσωπικά δεδομένα των υπαλλήλων ή πελατών, δεδομένα που σχετίζονται με τις διαδικασίες της

τράπεζας και είναι αρκετά σημαντικά για τη λειτουργία της, διάφορες πληροφορίες για τη δομή του πληροφοριακού συστήματος ή του δικτύου, ή ακόμα και κωδικούς πρόσβασης σε διάφορες υπηρεσίες του Π.Σ. .

- **Backup Tapes :** Τα Backup των δεδομένων της τράπεζας . Είναι όλα τα δεδομένα του Database Server.

A2.1.5 Διαδικασίες

- **Money Withdrawal from ATM :** Διαδικασία με την οποία γίνεται ανάληψη χρημάτων από τους πελάτες μέσω της αυτόματης ταμειακής μηχανής (ATM) η οποία είναι εγκατεστημένη στον κυρίως χώρο (Main Area) του υποκαταστήματος .
- **Money Deposit :** Η διαδικασία κατάθεσης χρημάτων από τους πελάτες με την υποστήριξη του προσωπικού που είναι υπεύθυνο για αυτές τις συναλλαγές . Η συγκεκριμένη διαδικασία πραγματοποιείται στο κυρίως χώρο (Main Area) , ενώ απαιτεί και την ύπαρξη κάποιου υπολογιστή (Workstation) .
- **New Account Opening :** Η διαδικασία ανοίγματος λογαριασμού πελατών με την υποστήριξη του προσωπικού που είναι που είναι υπεύθυνο για αυτές τις συναλλαγές . Η συγκεκριμένη διαδικασία πραγματοποιείται στον κυρίως χώρο (Main Area) , ενώ απαιτεί και την ύπαρξη κάποιου υπολογιστή (Workstation) για τις πληροφοριακές εργασίες (π.χ. αποθήκευση στη βάση).

A3. ΑΠΟΤΙΜΗΣΗ ΠΣ ΚΑΙ ΕΓΚΑΤΑΣΤΑΣΕΩΝ ΤΡΑΠΕΖΑΣ

Στο κομμάτι αυτό παρουσιάζονται τα αγαθά που βρίσκονται στο σύνολο του πληροφοριακού συστήματος, καθώς και πιθανές ευπάθειες, που μπορούν να τύχουν εκμετάλλευσης από διάφορες απειλές.

A3.1 Αγαθά που εντοπίστηκαν

Τα αγαθά που εντοπίστηκαν είναι :

- **Database Server :** Η βάση δεδομένων της τράπεζας. Περιέχει σημαντικά δεδομένα και πληροφορίες για κάθε πτυχή της λειτουργίας του οργανισμού.
- **Router :** Παρέχει τη σύνδεση του πληροφοριακού συστήματος της τράπεζας με το διαδίκτυο και την κεντρική βάση δεδομένων του οργανισμού (Central Bank Data Center), υποστηρίζοντας έτσι κάθε διαδικτυακή δραστηριότητα αυτού.
- **Automated Teller Machine (ATM) :** Συσκευή υπεύθυνη για την εκτέλεση συναλλαγών με τους πελάτες χωρίς τη παρέμβαση κάποιου υπαλλήλου.
- **Web Server :** Ένας εξυπηρετητής ιστού είναι το πρόγραμμα που χρησιμοποιεί HTTP (Hypertext Transfer Protocol) για την παράδοση των αρχείων που σχηματίζουν ιστοσελίδες στους χρήστες, ανταποκρινόμενος στα αιτήματά τους, τα οποία προωθούνται από τους υπολογιστές τους.
- **Bank Customer Data :** Τα δεδομένα που αφορούν τους πελάτες της τράπεζας.
- **Laptop** : Ο προσωπικός υπολογιστής του διευθυντή της τράπεζας.
- **Printer (Director's office) :** Μια συσκευή εκτύπωσης που είναι συνδεδεμένη στο δίκτυο και βρίσκεται στο γραφείο του διευθυντή.
- **Printer (Main Area) :** Μια συσκευή εκτύπωσης που είναι συνδεδεμένη στο δίκτυο και βρίσκεται στον κύριο χώρο της τράπεζας.

- **Money Withdrawal from ATM (Process) :** Διαδικασία με την οποία γίνεται ανάληψη χρημάτων από τους πελάτες μέσω της αυτόματης ταμειακής μηχανής (ATM) η οποία είναι εγκατεστημένη στον κυρίως χώρο (Main Area) του υποκαταστήματος.
- **Paper Documents :** Έγγραφα τα οποία μπορεί να περιέχουν προσωπικά δεδομένα των υπαλλήλων ή πελατών, δεδομένα που σχετίζονται με τις διαδικασίες της τράπεζας και είναι αρκετά σημαντικά για τη λειτουργία της, διάφορες πληροφορίες για τη δομή του πληροφοριακού συστήματος ή του δικτύου, ή ακόμα και κωδικούς πρόσβασης σε διάφορες υπηρεσίες του Π.Σ. .
- **Backup Tapes :** Τα Backup των δεδομένων της τράπεζας. Είναι όλα τα δεδομένα του Database Server.
- **Workstations (Main Area) :** Υπολογιστές που χρησιμοποιούνται για την εκτέλεση των διάφορων συναλλαγών καθώς και την επεξεργασία των δεδομένων.
- **Switch (Main Area) :** Συσκευή η οποία λαμβάνει, επεξεργάζεται και διαβιβάζει δεδομένα στις συσκευές του κυρίου χώρου.
- **Scanner :** Συσκευή σκαναρίσματος εγγράφων, η οποία είναι συνδεδεμένη στο δίκτυο και είναι εγκατεστημένη στον κύριο χώρο του οργανισμού.
- **Camera :** Η συγκεκριμένη συσκευή είναι εγκατεστημένη στην αίθουσα υπολογιστών και χρησιμοποιείται για την επίβλεψη του χώρου.
- **Switch(Director's office)** : Συσκευή η οποία λαμβάνει, επεξεργάζεται και διαβιβάζει δεδομένα στις συσκευές του γραφείου του διευθυντή της τράπεζας.
- **New Account Opening Process :** Η διαδικασία ανοίγματος λογαριασμού πελατών με την υποστήριξη του προσωπικού που είναι που είναι υπεύθυνο για αυτές τις συναλλαγές. Η συγκεκριμένη διαδικασία πραγματοποιείται στον κύριο χώρο (Main Area), ενώ απαιτεί και την ύπαρξη κάποιου υπολογιστή (Workstation) για τις πληροφοριακές εργασίες (π.χ. αποθήκευση στη βάση).
- **Facilities** : Οι κτηριακές εγκαταστάσεις της τράπεζας.
- **Switch (Computer Room) :** Συσκευή η οποία λαμβάνει, επεξεργάζεται και διαβιβάζει δεδομένα στις συσκευές του computer room.
- **Firewall :** Η συσκευή του firewall. Η τράπεζα επενδύει ένα συγκεκριμένο χρηματικό ποσό κάθε χρόνο για την αγορά ή συντήρησή της, καθώς είναι υπεύθυνη για τη παρακολούθηση και τον έλεγχο της εισερχομένης κυκλοφορίας του δικτύου.
- **Workstation (Computer Room) :** Υπολογιστής που χρησιμοποιείται για την εκτέλεση των διάφορων συναλλαγών καθώς και την επεξεργασία των δεδομένων.
- **Bank Employee Data :** Τα δεδομένα που αφορούν το προσωπικό της τράπεζας.
- **Windows 10 Pro :** Το λειτουργικό σύστημα που τρέχουν οι υπολογιστές(Workstations) του οργανισμού.
- **Money Deposit (Process) :** Η διαδικασία κατάθεσης χρημάτων από τους πελάτες με την υποστήριξη του προσωπικού που είναι υπεύθυνο για αυτές τις συναλλαγές. Η συγκεκριμένη διαδικασία πραγματοποιείται στον κύριο χώρο (Main Area), ενώ απαιτεί και την ύπαρξη κάποιου υπολογιστή (Workstation).
- **VoIP Phone :** Συσκευή η οποία χρησιμοποιείται για την πραγματοποίηση κλήσεων μέσω του δικτύου.

Α3.2 Απειλές που εντοπίστηκαν

Οι απειλές παρατίθενται με τη σειρά που παρουσιάστηκαν τα αγαθά.

- **SQL Injection :** Είναι μια τεχνική έκχυσης κώδικα , η οποία μπορεί να καταστρέψει τη βάση δεδομένων. Εισάγοντας ανεπιθύμητες εντολές στα δεδομένα που αποστέλλονται στον διερμηνέα της εφαρμογής.
- **Unauthorized access to the database :** Πρόσβαση στο περιεχόμενο της βάσης δεδομένων από μη εξουσιοδοτημένους χρήστες εξαιτίας της κακής διαχείρισης κωδίκων.
- **Denial of service :** Επιθέσεις άρνησης εξυπηρέτησης ονομάζονται γενικά οι επιθέσεις εναντίον ενός υπολογιστή, ή μιας υπηρεσίας που παρέχεται, οι οποίες έχουν ως σκοπό να καταστήσουν τον υπολογιστή ή την υπηρεσία ανίκανη να δεχτεί άλλες συνδέσεις και έτσι να μην μπορεί να εξυπηρετήσει άλλους πιθανούς πελάτες.
- **Access to the network of unauthorized user :** Πρόσβαση στο δίκτυο από μη εξουσιοδοτημένο άτομο, η οποία του επιτρέπει να στείλει ή να λάβει εμπιστευτικά για τον οργανισμό δεδομένα.
- **Failure of power supply or Power fluctuation :** Αποτυχίες τροφοδοσίας ή διακυμάνσεις ισχύος, οι οποίες μπορεί να θέσουν τη συσκευή(router) ανίκανη να επιτελέσει το σκοπό της και συνεπώς να θέσουν όλο το δίκτυο εκτός λειτουργίας.
- **Remotely running arbitrary code and subsequently escalating privileges :** Απομακρυσμένη εκτέλεση εντολών κώδικα, η οποία μπορεί να οδηγήσει στην μη ελεγχόμενη ανάληψη χρήματων από το ATM.
- **External device connection to the USB or PS/2 interface, exit from kiosk mode and run commands in the ATM OS :** Σύνδεση μιας εξωτερικής συσκευής USB ή μιας PS/2 διεπαφής με την οποία το ATM «βγαίνει από το kiosk mode(όταν μια εφαρμογή τρέχει σε kiosk mode σημαίνει ότι ο χρήστης δε μπορεί να εκτελέσει άλλα προγράμματα ή να αποκτήσει πρόσβαση σε λειτουργίες του λειτουργικού συστήματος)» με αποτέλεσμα ο επιτιθέμενος να μπορεί να παρακάμψει τους περιορισμούς αυτούς και να εκτελέσει εντολές στο λειτουργικό σύστημα του ATM.
- **Execute remotely arbitrary code :** Απομακρυσμένη εκτέλεση κώδικα, η οποία μπορεί να οδηγήσει σε αποκάλυψη των δεδομένων που περιέχει ο Web Server ή να επηρεάσει τη διαθεσιμότητα του.
- **Cross-site scripting attacks(XSS) :** Επίθεση στην οποία κακόβουλα scripts εκχέονται σε εμπίστους ιστότοπους των χρηστών.
- **User error during data insertions :** Λάθη στις εισαγωγές των δεδομένων στη βάση, με αποτέλεσμα τα δεδομένα να είναι ανακριβή.
- **Installation of mallicious software :** Εγκατάσταση μη εξουσιοδοτημένης εφαρμογής η οποία μπορεί να έχει ως αποτέλεσμα την άρνηση πρόσβασης στην συσκευή(laptop) στους εξουσιοδοτημένους χρήστες τους.
- **E-mails with seemingly unoffending harmless links or attachments which install malware like trojans or ransomware in case of a execution :** Email με φαινομενικά αξιόπιστους συνδέσμους η συνημμένα μπορεί να οδηγήσουν στην εγκατάσταση κακόβουλου λογισμικού.
- **Unauthorized software installation :** Εγκατάσταση κακόβουλου λογισμικού από μη εξουσιοδοτημένο χρήστη.

- **Deliberate destruction of documents / data** : Απειλούνται τα δεδομένα του προσωπικού υπολογιστή του διευθυντή από σκόπιμη καταστροφή.
- **Unauthorized access in device's memory :** Πρόσβαση στη μνήμη του εκτυπωτή, όπου υπάρχουν αποθηκευμένα δεδομένα από τις τελευταίες εκτυπώσεις.
- **Malicious crafted file :** Εγκατάσταση κακόβουλου αρχείου το οποίο μπορεί να επιτρέψει την προβολή, αλλαγή ή διαγραφή δεδομένων.
- **Card skimming(place physical shims (skimmers) on a card reader in order to read information directly from the magnetic stripe) :** Απειλούνται τα δεδομένα των λογαριασμών από τη τοποθέτηση ειδικών συσκευών ανάγνωσης στους αναγνώστες καρτών του ATM.
- **Retrieval of paper documents from garbage bins in order to gain access to personal information :** Ανάκτηση εγγράφων από τους κάδους απορριμμάτων.
- **Theft of documents :** Κλοπή εγγράφων, η οποία μπορεί να οδηγήσει σε διαρροή ευαίσθητων δεδομένων.
- **Insider Employee gets backup tapes :** Κλοπή από υπάλληλο της τράπεζας.
- **Theft of backup tapes :** Κλοπή των ταινιών backup.
- **Fire :** Φωτιά στις κτηριακές εγκαταστάσεις του οργανισμού.
- **Use of software by unathorized user :** Χρήση του λογισμικού που είναι εγκατεστημένο στους υπολογιστές του κύριου χώρου από μη εξουσιοδοτημένο χρήστη.
- **Insertion of CDs, DVDs, or USB thumb drives into the organization's computers from unauthorized user (Main area) :** Απειλή παρεμβολής στις διαδικασίες του οργανισμού μέσω της σύνδεσης εξωτερικής συσκευής στους υπολογιστές της τράπεζας.
- **Network access by unauthorized persons via a single Ethernet cable insertion :** Μη εξουσιοδοτημένη πρόσβαση στο δίκτυο.
- **Damage to the device :** Απειλείται να υποστεί ζημιά η συσκευή που βρίσκεται στον κύριο χωρο (βανδαλισμός).
- **The EPSON Network utility included with some older Epson printers installs a binary code with weak permissions :** Το network utility που υπάρχει σε παλιές συσκευές της εταιρίας EPSON επιτρέπει την εγκατάσταση κώδικα, επιτυχής εκμετάλλευση της μπορεί να οδηγήσει στην απώλεια του ελέγχου της συσκευής.
- **Brute force attack by third parties and taking control of the system :** Εξαντλητική δοκιμή κωδικών για την είσοδο στη συσκευή με αποτέλεσμα την απώλεια ελέγχου της.
- **Malicious software that corrupts packages :** Εγκατάσταση κακόβουλου λογισμικού το οποίο προκαλεί την διακοπή των πακέτων με συνέπεια την τροποποίηση ή διαρροή ευαίσθητων δεδομένων.
- **Social engineering :** Προσπάθεια εξαπάτησης των υπαλλήλων για την αποκάλυψη εμπιστευτικών πληροφοριών. Οι πληροφορίες που λαμβάνονται στη συνέχεια χρησιμοποιούνται για την απόκτηση πρόσβασης σε συστήματα και υπάρχει κίνδυνος ενέργειων εις βάρος του προσώπου ή του οργανισμού του οποίου τα δεδομένα έχουν αποκαλυφθεί.
- **Damage to communication lines/cables :** Απειλείται η διαθεσιμότητα της κάμερας και του Database Server από καταστροφή των επικοινωνιακών γραμμών.
- **MAC Flooding :** Απειλή η οποία στοχεύει στην αποστολή εμπιστευτικών πληροφοριών σε τμήματα του δικτύου που κανονικά δεν θα αποστέλλονταν,

πλημμυρίζοντας τον πίνακα MAC διευθύνσεων του switch με ψεύτικες διευθύνσεις.

- **Unathorised access to the bank's whole network. Due to that the firewall fails to provide protection to the rest of the system :** Εκμετάλλευση των ασυνεπειών του firewall και απόκτηση πρόσβασης στο δίκτυο της τράπεζας από μη εξουσιοδοτημένα άτομα.
- **Installation of malicious software (eg. Viruses,worms, Trojan horses) :** Απειλούνται άμεσα οι συσκευές και το λογισμικό της τράπεζας, όπως και τα δεδομένα τους από την εγκατάσταση κακόβουλου λογισμικού.
- **Former employee or contractor has access to the system :** Απειλούνται ευαίσθητα δεδομένα από πρώην υπάλληλους της τράπεζας που εξακολουθούν να έχουν ενεργό λογαριασμό και συνεπώς πρόσβαση στο σύστημα της τράπεζας.
- **Insider Employee gets employee personal data :** Απειλή αποκάλυψης ή τροποποίησης δεδομένων που αφορούν το προσωπικό της τράπεζας από υπάλληλο της εταιρίας .
- **Software failure :** Απειλείται η εύρυθμη λειτουργία των συσκευών που χρησιμοποιούν το συγκεκριμένο λογισμικό.
- **Abuse of cashier's privileges :** Κατάχρηση των δικαιωμάτων του ταμεία παρακρατώντας χρήματα και μη καταγράφοντας τις συναλλαγές με τους πελάτες.
- **Remote eavesdropping :** Απομακρυσμένη παρακολούθηση των τηλεπικοινωνιακών κλήσεων .

Α3.3 Ευπάθειες που εντοπίστηκαν

Οι ευπάθειες παρατίθενται με τη σειρά που παρουσιάστηκαν τα αγαθά .

- **Rules not appropriately configured :** Οι κανόνες εισαγωγής εντολών (input field) στην βάση δεδομένων δεν έχουν οριστεί πλήρως.
- **Poor password management :** Κακή διαχείριση των συνθηματικών που επιτρέπουν την πρόσβαση στην υπηρεσία.
- **Not properly handle authentication-header packets :** Ακατάλληλη επικύρωση της ταυτότητας όπου προέρχονται τα πακέτα.
- **Incomplete package sender authentication :**Πρόβλημα στην επικύρωση ανολοκλήρωτων πακέτων που αποστέλνονται μέσω του δικτύου.
- **Unstable power grid, susceptibility of equipment to voltage variations :** Η ύπαρξη ασταθούς ηλεκτρικού ρεύματος ή η ευαισθησία του εξοπλισμού σε μεταβολές τάσεις μπορεί να οδηγήσει σε αδυναμία εκτέλεσης των διαδικασιών της τράπεζας.
- **Out-of-date software versions(Windows XP) :** Παλιές εκδόσεις λογισμικού.
- **Insufficient protection of communication with peripherals :** Η ανεπαρκής προστασία της σύνδεσης περιφερειακών συσκευών προσφέρει τη δυνατότητα στους επιτιθέμενους να παρέμβουν στις συναλλαγές.
- **"OpenType Font Parsing Vulnerability" :** Πρόκειται για μια ευπάθεια του λειτουργικού συστήματος (Windows Server 2008 R2) ,επιτυχής εκμετάλλευση της μπορεί να επιτρέψει την απομακρυσμένη εκτέλεση κώδικα.
- **Running unnecessary services :** Ευπάθεια του Web Server, η οποία υπάρχει εξαιτίας της εκτέλεσης από τον server μη αναγκαίων για τον οργανισμό υπηρεσιών.
- **Lack of input's parsing :** Έλλειψη ελέγχου των δεδομένων που εισάγονται στο σύστημα.

- **Uncontrolled downloading and using software :** Λήψη εφαρμογών ή αρχείων χωρίς περιορισμούς.
- **Lack of security awareness :** Έλλειψη ενημέρωσης του προσωπικού για θέματα ασφάλειας.
- **Kernel Code Vulnerability :** Ευπάθεια του λειτουργικού συστήματος(MAC-OS) όπου επιτυχής εκμετάλλευση της μπορεί να οδηγήσει στην αδυναμία εισόδου στη συσκευή σε εξουσιοδοτημένους χρήστες.
- **Bluetooth pairing vulnerability :** Ευπάθεια των MacBook. Απειλούνται τα προσωπικά δεδομένα που περιέχονται στο laptop.
- **Outdated firmware :** Παλιές εκδόσεις λογισμικού.
- **Stack or static buffer overflow :** Ευπάθεια του εκτυπωτή που μπορεί να επιτρέψει την εγκατάσταση κακόβουλου αρχείου.
- **Failure to perform data encryption and authentication at card data:** Αποτυχία κρυπτογράφησης των δεδομένων που φέρουν οι κάρτες.
- **Lack of security awareness or inappropriate shredding process :** Έλλειψη ενημέρωσης του προσωπικού για θέματα ασφάλειας ή ακατάλληλη διαδικασία τεμαχισμού των εγγράφων.
- **Insufficient protection of stored documents :** Ανεπαρκής προστασία των εγγράφων που είναι αποθηκευμένα στους χώρους της τράπεζας.
- **Not encrypted :** Τα backup της τράπεζας δεν είναι κρυπτογραφημένα.
- **Insufficient protection of backup tapes :** Ανεπαρκής προστασία των ταινιών backup.
- **Lack of fire measures(smoking inside the building, installation of equipment near flammable materials) :** Έλλειψη κανόνων πυρασφάλειας.
- **Lack of identification and authentication mechanisms or no 'logout' when leaving the workstation :** Έλλειψη μηχανισμών αυθεντικοποίησης ή μη αποσύνδεση των χρηστών από τους υπολογιστές.
- **Insufficient protection of communication with peripherals :** Ανεπαρκής προστασία σύνδεσης περιφερειακών συσκευών στους υπολογιστές του κυρίου χώρου.
- **Lack of policies for the correct use of telecommunications media and messaging (unprotected switch at the main area room) :** Η συσκευή switch που βρίσκεται στον κύριο χώρο βρίσκεται σε κοινή θεά και αυτό μπορεί να έχει ως αποτέλεσμα την καταστροφή της ή την παρεμβολή στο δίκτυο από κάποιον μη εξουσιοδοτημένο χρήστη.
- **Missing updates and patches :** Οφείλεται στη μη λήψη των ενημερώσεων λογισμικού του εκτυπωτή.
- **Maintain default usernames and passwords :** Ευπάθεια που οφείλεται στην διατήρηση των προκαθορισμένων από τον κατασκευαστή όνομα χρήστη και συνθηματικού.
- **Uncontrolled download from the internet :** Ανεξέλεγκτη λήψη εφαρμογών και αρχείων από το διαδίκτυο.
- **Inadequate training / education of employees on safety issues :** Ανεπαρκής εκπαίδευση του προσωπικού σε θέματα ασφάλειας.
- **Shared connection line from switch to camera and to the server :** Κοινη γραμμη συνδεσης της καμερας και του database server στο switch.
- **Inadequate network management :** Ανεπαρκής διαχείριση του δικτύου.

- **Configuration Mistakes :** Λάθη στις ρυθμίσεις της συσκευής αποτελούν απειλή για την λειτουργία των διαδικασιών της τράπεζας καθώς και την καθιστούν επιρρεπή σε επιθέσεις.
- **Missed Security Patches :** Οφείλεται στη μη λήψη των ενημερώσεων λογισμικού.
- **Wrong allocation of access rights :** Λανθασμένη κατανομή των δικαιωμάτων πρόσβασης από τον διαχειριστή.
- **Database not encrypted :** Η βάση δεδομένων δεν είναι κρυπτογραφημένη και αυτό έχει ως αποτέλεσμα την άμεση πρόσβαση στα δεδομένα.
- **Jet Database Engine Remote Code Execution :** Η ευπάθεια αυτή προσφέρει την δυνατότητα εκτέλεσης απομακρυσμένου κώδικα όταν το Windows Jet Database Engine χειρίζεται εσφαλμένα αντικείμενα στη μνήμη.
- **Unsupervised work of bank staff :** Οι εργασίες των υπαλλήλων δεν επιβλέπονται και η εκμετάλλευση αυτής της ευπάθειας μπορεί να οδηγήσει σε αυθαιρεσίες των υπαλλήλων.
- **Connections not encrypted :** Η σύνδεση του τηλεφώνου δεν κρυπτογραφείται.

Α3.4 Αποτελέσματα αποτίμησης

Ακολουθεί ενδεικτικός πίνακας της αποτίμησης των επιπτώσεων(Impacts),που μπορεί να προκαλέσει ένα αγαθό σε περίπτωση που παραβιαστεί,ως προς την διαθεσιμότητα την ακεραιότητα και την εμπιστευτικότητα.Παρατηρούμε ότι η βαθμολογία των Impacts μπορεί να φτάσει από την ελάχιστη τιμή (1),στην οποία η τράπεζα δεν διατρέχει κάποιο σοβαρό κίνδυνο, μέχρι και την μέγιστη τιμή (10),όπου η τράπεζα βρίσκεται σε μια κρίσιμη κατάσταση.

	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	Αποποίηση αποστολέα	Αποποίηση παραλήπτη	Άρνηση αποστολής ή παραλαβής	Παρεμβολή λανθασμένων μηνυμάτων	Λανθασμένη δρομολόγηση	Παρακολούθηση κίνησης	Μη παράδοση	Απώλεια ακολουθίας μηνυμάτων
Database Server	4	5	5	6	8	9	10	10	7	9	3	9	2	5	8	3	6	6	6	7	7	7	7	4
Router	2	2	3	5	7	7	8	9	3	5	4	5	1	3	4	3	3	3	3	4	5	6	4	3
Automated Teller Machine (ATM)	1	1	2	3	4	5	6	7	3	5	2	6	2	5	7	2	3	3	4	4	5	6	5	2
Web Server (AMSRV001)	3	3	3	4	5	6	7	7	5	5	3	6	3	5	7	3	3	3	4	5	5	7	6	4
Bank Customer Data	1	1	2	3	5	5	6	7	7	7	5	7	5	6	7	5	6	6	6	7	7	7	6	4
Laptop (AMLPS001)	2	2	3	4	5	5	8	9	6	8	4	7	4	7	9	3	4	5	5	7	7	9	5	4
Printer (AMPR0001)	1	1	2	2	3	4	5	6	3	6	3	5	3	5	6	2	2	2	4	6	6	5	4	4
Printer (AMPR0002)	1	1	2	2	3	4	5	6	3	6	3	5	3	4	6	2	2	2	4	6	6	5	4	4
Paper Documents	1	2	2	3	4	5	6	7	5	7	3	7	4	6	7									
Backup tapes	3	3	4	4	6	6	7	9	5	8	4	7	3	7	9	5	6	6	6	8	7	9	8	5
Facilities	4	4	4	5	6	6	8	9	3	7	2	9	2	6	9									
Workstations	1	1	2	3	4	5	5	6	3	6	2	5	2	5	6	3	4	4	4	6	4	6	5	4
Switch (M.A)	2	2	3	5	7	7	8	8	4	7	4	7	3	7	8	3	4	4	5	7	7	8	6	5

Scanner	1	1	2	3	5	5	6	6	2	6	2	4	2	5	6	2	2	2	3	6	6	6	4	4
Camera	1	1	2	2	3	3	4	5	3	5	3	5	2	4	5	2	3	3	3	4	5	5	4	4
Switch (D.O)	2	2	3	5	7	7	8	8	4	8	4	7	4	7	8	3	4	4	5	7	7	8	6	5
New Account Opening Process	1	2	3	5	5	6	7	7	4	7	4	7	2	5	7	2	3	3	4	6	5	7	5	6
Switch (C.R)	3	3	4	5	7	7	8	8	5	8	5	8	3	7	8	3	4	4	5	7	7	8	6	5
Firewall	5	6	7	7	7	8	9	10	6	10	7	8	5	9	10	6	5	5	6	6	7	8	5	5
Workstation C.R	2	2	3	4	5	5	6	7	3	7	2	5	2	5	7	2	4	4	4	5	6	7	5	3
Bank Employee Data	5	5	6	6	7	7	8	9	7	9	6	7	3	7	9	5	6	6	6	7	9	8	6	5
Windows 10 Pro	1	2	2	2	4	5	6	8	5	7	3	6	2	5	8	2	3	3	3	5	6	7	5	4
Money deposit	2	2	3	3	5	5	5	6	3	6	5	6	2	5	6	2	3	3	5	5	6	5	4	4
VoIP Phone	2	2	3	4	5	5	6	7	3	7	4	6	2	6	7	2	3	3	4	5	6	7	5	5
Money Withdrawal from ATM	2	2	4	4	5	5	7	7	4	7	4	6	4	6	7	2	4	4	4	4	6	7	6	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 της Τράπεζας.

Α1 Προσωπικό – Προστασία Διαδικασιών Προσωπικού

- (A-0017 , A-0024) Διεξαγωγή σεμιναρίων για το προσωπικό με σκοπό την ευαισθητοποίηση τους όσον αφορά θέματα ασφάλειας του λογισμικού.

- (Backup tapes , A-0019) Να υπάρχουν εσωτερικοί κανονισμοί και πολιτικές για τους υπαλλήλους με σκοπό την αποφυγή πρόσβασης κάποιου υπαλλήλου σε ευαίσθητα δεδομένα της τράπεζας και πιθανή διάρρευση τους.

- (Facilities) Διεξαγωγή προγραμμάτων για εκπαίδευση σχετικά με την αντιμετώπιση πυρκαγιάς και λήψη μέτρων για την πρόληψη και αντιμετώπιση της.

- (Paper documents) Να υπάρχουν εσωτερικοί κανονισμοί και πολιτικές για τους υπαλλήλους με σκοπό την αποφυγή πρόσβασης κάποιου υπαλλήλου σε ευαίσθητα δεδομένα της τράπεζας και πιθανή διάρρευση τους αλλά και θέσπιση αυστηρών πολιτικών και διαδικασιών για την αντιμετώπιση του προβλήματος.

- (A-0013) Θέσπιση πολιτικής που θα δηλώνει πως ο εταιρικός εξοπλισμός θα χρησιμοποιείται μόνο για σκοπούς της επιχείρησης και για τίποτα άλλο με σκοπό να μην εκτεθεί το σύστημα σε εξωτερικές απειλές.

- (A-0023) Επίβλεψη των ενεργειών των εργαζομένων με σκοπό να μην καταχραστούν τα δικαιώματα τους εις βάρος της τράπεζας.

A2 Ταυτοποίηση και αυθεντικοποίηση

- (A-0010) Έλεγχος και επικύρωση του πεδίου εισόδου στον server της βάσης δεδομένων ώστε να αποφευχθεί το μπλοκάρισμα του συστήματος και η μη πραγματοποίηση οποιασδήποτε συναλλαγής.

- (A-0010) Θέσπιση πολιτικής που θα λέει να εφαρμόζονται κωδικοί υψηλής ασφάλειας στους λογαριασμούς των πελατών για να αποφευχθεί η πρόσβαση κάποιου εξωτερικού ατόμου στην βάση δεδομένων της τράπεζας.

- (A-0002 , A-0003 , A-0004) Εφαρμογή πολιτικής αναγνώρισης και ελέγχου ταυτότητας του χρήστη για να μην είναι εφικτό να χρησιμοποιηθεί το σύστημα από χρήστη που δεν έχει την ανάλογη άδεια.

- (A-0008) Αλλαγή των προεπιλεγμένων usernames και passwords των καμερών ώστε να μην μπορεί με ευκολία να αποκτήσει κάποιος τρίτος πρόσβαση σε αυτές.

A3 Έλεγχος προσπέλασης και χρήσης πόρων

- (A-0025) Χρήση τοπικών πολιτικών και έλεγχος όλων των συσκευών για να περιοριστεί μια πιθανή σύνδεση περιφερειακής συσκευής στο ATM.

- (A-0007) Να επιτρέπεται η πρόσβαση στο σύστημα των εκτυπωτών μόνο σε εξουσιοδοτημένες διευθύνσεις IP, μηχανές και/ή χρήστες για να μην υπάρξει αλλοίωση δεδομένων μέσα από την εγκατάσταση κακόβουλου λογισμικού στα συγκεκριμένα μηχανήματα.

- (A-0002 , A-0003 , A-0004) Απενεργοποίηση όλων των CD, DVD και USB θυρών και ενεργοποίηση ελέγχου από antivirus για κάθε εξωτερική συσκευή που συνδέεται σε αυτές τις θύρες ώστε να μην είναι εφικτή η σύνδεση στο σύστημα κάποιας συσκευής από κάποιον τρίτο που θέλει να υποκλέψει πληροφορίες.

- (A-0015) Ορισμός συγκεκριμένων πολιτικών με ελάχιστα δικαιώματα με σκοπό να μειωθούν οι πιθανότητες πτώσης του τραπεζικού συστήματος εξαιτίας αδυναμίας του firewall να το προστατεύσει.

- (A-0001) Δημιουργία διαδικασίας με την οποία θα ανακαλείται η πρόσβαση του χρήστη στον λογαριασμό του μετά την λήξη της συνεργασίας του με την τράπεζα. Με αυτόν τον τρόπο αποφεύγεται η πιθανότητα ως πρώην υπάλληλος της τράπεζας να έχει ακόμα πρόσβαση στα δεδομένα της.

- (A-0014 , A-0009 , A-0017 , A-0018 , A-0006 , A-0007 , Backup tapes , A-0002 , A-0003 , A-0004 , A-0012 , A-0005 , A-0008 , A-0013 , A-0011 , A-0015 , A-0001 , A-0019 , A-0016) Παρακολούθηση των στοιχείων καταγραφής της τράπεζας με σκοπό να υπάρχουν καταγεγραμμένες όλες οι δράσεις της τράπεζας και να μπορεί να γίνει καλύτερη διαχείριση των όποιων προβλημάτων προκύψουν.

- (A-0025 , A-0002 , A-0003 , A-0004) Καταγραφή και παρακολούθηση των γεγονότων ασφάλειας για τη διαχείριση ανάλογων προβλημάτων.

A4 Διαχείριση εμπιστευτικών δεδομένων

- (A-0022) Κρυπτογράφηση των στοιχείων συναλλαγής με τον σαρωτή της κάρτας ώστε να μην υπάρξει υποκλοπή αυτών των δεδομένων κατά την εισαγωγή της στο ATM.

- (Backup tapes) Αύξηση της φυσικής ασφάλειας και εφαρμογή του κανόνα ''3-2-1 Backup Rule''. Αυτός ο κανόνας δηλώνει πως πρέπει να κρατάμε τουλάχιστον 3 αντίγραφα των δεδομένων , να αποθηκεύουμε 2 backup αντίγραφα σε διαφορετικά μέσα αποθήκευσης και το ένα από αυτά να μην βρίσκεται στον χώρο της τράπεζας.

- (A-0022) Αποστολή SMS στον πελάτη με τα στοιχεία των τραπεζικών του συναλλαγών ώστε σε περίπτωση υποκλοπής των στοιχείων της κάρτας του να γίνει άμεση αναφορά στην τράπεζα για την λήψη των ανάλογων μέτρων.

A5 Προστασία από τη χρήση υπηρεσιών από τρίτους

- (A-0007) Να επιτρέπεται η πρόσβαση στο σύστημα των εκτυπωτών μόνο σε εξουσιοδοτημένες διευθύνσεις IP, μηχανές και/ή χρήστες για να μην υπάρξει αλλοίωση δεδομένων μέσα από την εγκατάσταση κακόβουλου λογισμικού στα συγκεκριμένα μηχανήματα.

- (A-0001) Δημιουργία διαδικασίας με την οποία θα ανακαλείται η πρόσβαση του χρήστη στον λογαριασμό του μετά την λήξη της συνεργασίας του με την τράπεζα. Με αυτόν τον τρόπο αποφεύγεται η πιθανότητα ως πρώην υπάλληλος της τράπεζας να έχει ακόμα πρόσβαση στα προσωπικά δεδομένα της.

- (A-0005) Αναδιαμόρφωση του συστήματος απομακρύνοντας τις πλέον μη απαραίτητες για την τράπεζα υπηρεσίες ώστε να μην υπάρξει επίθεση από μια υπηρεσία που δεν χρησιμοποιείται πια και δεν μπορεί να εντοπιστεί εύκολα.

- (A-0014) Honeypots. Μηχανισμός ο οποίος εντοπίζει , εκτρέπει και σε ορισμένες περιπτώσεις εμποδίζει την επίθεση στο σύστημα από μη εξουσιοδοτημένους χρήστες.

A6 Προστασία λογισμικού

- (A-0014) Honeypots. Μηχανισμός ο οποίος εντοπίζει , εκτρέπει και σε ορισμένες περιπτώσεις εμποδίζει την επίθεση στο σύστημα από μη εξουσιοδοτημένους χρήστες.

- (A-0025 , A-0015 , A-0017 , A-0021) Τακτικά updates των εφαρμογών και του λειτουργικού συστήματος ώστε να είναι ενημερωμένο το σύστημα και συνεπώς πιο ανθεκτικό σε επιθέσεις.

- (A-0006) Συχνά updates στο firmware του εκτυπωτή ώστε να μην υπάρξει πρόσβαση στην μνήμη της συσκευής μέσω κάποιας παλιάς και πιο αδύναμης έκδοσης.

- (A-0005) Αναβάθμιση στην τελευταία έκδοση λογισμικού της EPSON για τον σαρωτή καθώς οι παλαιότερες αναφέρονται και σε παλιότερα μοντέλα και συνεπώς οι άδειες που δίνονται είναι πιο ευάλωτες σε επίθεση.

- (A-0010) Έλεγχος λαθών από τον server της βάσης δεδομένων για να μπλοκαριστεί η πρόσβαση στην βάση από μη εξουσιοδοτημένους χρήστες.

A7 Διαχείριση ασφάλειας δικτύου

- (A-0007) Mandatory access control: Διαδικασία ελέγχου πρόσβασης με την οποία το σύστημα του router περιορίζει τη δυνατότητα σε κάποιον τρίτο να αποκτήσει πρόσβαση στο δίκτυο του και σε αυτό ολόκληρης της τράπεζας.

- (A-0014) Τοποθέτηση ενός UPS στο ρούτερ ή διαχωρισμός του δικτύου σε υποδίκτυα με διαφορετικά ρούτερ ώστε να μην δημιουργηθεί πρόβλημα σε ολόκληρο το σύστημα σε περίπτωση που δεν υπάρχει ηλεκτρική τροφοδότηση του κεντρικού ρούτερ.

- (A-0012) Απομάκρυνση των σημαντικότερων συσκευών δικτύου από τον κύριο χώρο ώστε να μην είναι εκτεθειμένα και συνεπώς ευάλωτα σε κάποιον πολυσύχναστο χώρο.

- (A-0011) Ξεχωριστές γραμμές επικοινωνίας από το switch προς τις συσκευές για να μην υπάρχει κοινή σύνδεση μεταξύ ξεχωριστών συσκευών, γεγονός που κάνει το σύστημα πιο ευάλωτο σε επίθεση.

- (A-0011) Διαμόρφωση των θυρών ασφάλειας του switch με τέτοιο τρόπο που να μην είναι δυνατή η υπερχείλιση της MAC διεύθυνσης του δικτύου.

- (A-0016) Συχνές αναβαθμίσεις του εργαλείου που προστατεύει το δίκτυο των VoIP Phones από τυχόν επίθεση.

A8 Προστασία από ιομορφικό λογισμικό

- (A-0014) Honeypots. Μηχανισμός ο οποίος εντοπίζει , εκτρέπει και σε ορισμένες περιπτώσεις εμποδίζει την επίθεση στο σύστημα από μη εξουσιοδοτημένους χρήστες.

- (A-0025 , A-0015 , A-0017) Τακτικά updates των εφαρμογών και του λειτουργικού συστήματος ώστε να είναι ενημερωμένο το σύστημα και συνεπώς πιο ανθεκτικό σε επιθέσεις.

- (A-0009) Εγκατάσταση της τελευταίας μη μολυνσμένης από ιό έκδοσης λογισμικού για την ανθεκτικότητα του συστήματος σε τυχόν επιθέσεις.

- (A-0006) Συχνά updates στο firmware του εκτυπωτή ώστε να μην υπάρξει πρόσβαση στην μνήμη της συσκευής μέσω κάποιας παλιάς και πιο αδύναμης έκδοσης.

- (A-0009) Εγκατάσταση του antivirus Kaspersky για να μην βρεθεί εκτεθειμένος ο web server.

A9 Ασφαλής χρήση διαδικτυακών υπηρεσιών

- (A-0013 , A-0017) Θέσπιση πολιτικής που θα δηλώνει πως ο εταιρικός εξοπλισμός θα χρησιμοποιείται μόνο για σκοπούς της επιχείρησης και για τίποτα άλλο με σκοπό να μην εκτεθεί το σύστημα σε εξωτερικές απειλές.

- (A-0015) Ορισμός συγκεκριμένων πολιτικών με ελάχιστα δικαιώματα με σκοπό να μειωθούν οι πιθανότητες πτώσης του τραπεζικού συστήματος εξαιτίας αδυναμίας του firewall να το προστατεύσει.

A10 Ασφάλεια εξοπλισμού

- (A-0014) Τοποθέτηση ενός UPS στο ρούτερ ή διαχωρισμός του δικτύου σε υποδίκτυα με διαφορετικά ρουτέρ ώστε να μην δημιουργηθεί πρόβλημα σε ολόκληρο το σύστημα σε περίπτωση που δεν υπάρχει ηλεκτρική τροφοδότηση του κεντρικού ρούτερ.

- (A-0012) Απομάκρυνση των σημαντικότερων συσκευών δικτύου από τον κύριο χώρο ώστε να μην είναι εκτεθειμένα και συνεπώς ευάλωτα σε κάποιον πολυσύχναστο χώρο.

- (Paper documents) Βελτίωση φυσικής ασφάλειας με την επανατοποθέτηση του εξοπλισμού και των φωτοαντίγραφων σε ασφαλές σημείο.

- (Backup tapes) Τακτικός έλεγχος των backup για την αποφυγή κλοπής τους.

A11 Φυσική ασφάλεια κτιριακής εγκατάστασης

- (Facilities) Διεξαγωγή προγραμμάτων για εκπαίδευση σχετικά με την αντιμετώπιση πυρκαγιάς και λήψη μέτρων για την πρόληψη και αντιμετώπιση της.

- (Facilities) Τοποθέτηση ανιχνευτών καπνού για την πρόληψη τυχόν πυρκαγιάς.

Α4. ΣΥΝΟΨΗ ΠΙΟ ΚΡΙΣΙΜΩΝ ΑΠΟΤΕΛΕΣΜΑΤΩΝ

Παρακάτω παρουσιάζονται τα πιο σημαντικά ευρήματα που χρήζουν άμεσης αντιμετώπισης.

- Στο **Firewall** εντοπίστηκε η ευπάθεια Configuration Mistakes, η οποία καθιστά το δίκτυο της τράπεζας, επιρρεπή σε επιθέσεις.Η εκμετάλλευση αυτής της ευπάθειας από κάποιον άλλο χρήστη,μπορεί να έχει ως αποτέλεσμα την μη εξουσιοδοτημένη πρόσβαση στο δίκτυο αυτό.Συνέπεια της παραπάνω απειλής μπορεί να είναι η μείωση των επιδόσεων του δικτύου σε ορισμένες περιπτώσεις καθώς και η τροποποίηση ή ακόμα και η διαρροή των δεδομένων της τράπεζας.

- Στις **Εγκαταστάσεις (Facilities)** η ευπάθεια που παρατηρήθηκε είναι η έλλειψη κανόνων πυρασφάλειας.'Ετσι σε περιπτωση πυρκαγιάς υπάρχει σοβαρός κίνδυνος μερικής ή ολικής καταστροφής των συστημάτων, καθώς και σοβαρός κίνδυνος ανθρώπινης απώλειας.

- Στα **Windows 10 Pro** εντοπίστηκε η ευπάθεια Jet Database Engine Remote Code Execution,η οποία σε ορισμένες περιπτώσεις δίνει την δυνατότητα εκτέλεσης απομακρυσμένου κώδικα σε εξωτερικούς χρήστες, με αποτέλεσμα να απειλείται η εύρυθμη λειτουργία των συσκευών που χρησιμοποιούν το συγκεκριμένο λογισμικό.Άμεση συνέπεια αυτού, είναι η πλήρης απώλεια προστασίας του συστήματος, δηλαδή η έκθεσή του σε διαφόρων ειδών κινδύνους.

ΠΗΓΕΣ:

https://www.cvedetails.com/?fbclid=IwAR3a27saZEZXF0zl3uCW3zVm_2N_C_OtZdT9i9-jJ2bUCHeYkLMjB6afz8U

https://www.ptsecurity.com/ww-en/analytics/atm-vulnerabilities-2018/?fbclid=IwAR1FJNrUVFNdOVqw4xMBU8eJ7vkkrJEYo4KfAZXh-JOK-NDQ-s6ZpOeJOZU

https://epson.com/support

https://advisera.com/27001academy/knowledgebase/threats-vulnerabilities/