ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΚΑΙ ΚΡΙΣΙΜΩΝ ΥΠΟΔΟΜΩΝ

ΣΧΕΔΙΟ ΑΣΦΑΛΕΙΑΣ

ΕΡΓΑΣΙΑ ΧΕΙΜΕΡΙΝΟΥ ΕΞΑΜΗΝΟΥ 2019

Contents

1. ΕΙΣΑΓΩΓΗ

1.1. Περιγραφή Εργασίας

Το παρόν αρχείο αποτελεί ένα σχέδιο ασφαλείας για την ανάλυση και διαχείριση επικινδυνότητας σε περιβάλλον τραπέζης (AUEB BANK) στα πλαίσια του μαθήματος "Ασφάλεια πληροφοριακών συστημάτων" του Οικονομικού πανεπιστημίου Αθηνών. Σκοπός είναι η καταγραφή όλων των αγαθών που χρήζουν προστασίας, των απειλών αλλά και η παράθεση μέτρων προστασίας.

1.2. Δομή παραδοτέου

Στην 2.1 καταγράφονται τα υφιστάμενα πληροφοριακά συστήματα της τράπεζας τα οποία χρειάζεται να ελεγχθούν ως προς τυχόν ευπάθειες και τις σχετικές απειλές. Στην 3.1 καταγράφονται τα αγαθά εκείνα που θα παρουσιάσουν απειλές και στην 3.2 αναλύονται οι απειλές αυτές. Στη συνέχεια, στην 3.3 απαριθμούνται οι ευπάθειες και στην 3.4 εμφανίζονται τα αποτελέσματα της αποτίμησης σε πίνακα για κάθε ένα αγαθό. Στην ενότητα Β2 αναλύονται προτεινόμενα μέτρα ασφάλειας τα οποία εντάσσονται σε 11 κατηγορίες και τέλος, στην ενότητα Α4 συνοψίζονται τα πιο κρίσιμα αποτελέσματα.

2. ΜΕΘΟΔΟΛΟΓΙΑ ΜΕΛΕΤΗΣ ΑΣΦΑΛΕΙΑΣ

Για τη Διαχείριση Επικινδυνότητας της τράπεζας (AUEB BANK) χρησιμοποιήθηκε παραμετροποιημένη μέθοδος του ISO27001K. 1Επιλέχθηκε 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 *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
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*

2.1. Περιγραφή Πληροφοριακού Συστήματος (ΠΣ) υπό έλεγχο

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

2.1.1. Υλικός εξοπλισμός (hardware)

Inventory ID	Asset Name	Type
A-0001	AMCWS001	Workstation
A-0002	AMCWS002	Workstation
A-0003	AMCWS003	Workstation
A-0004	AMCWS004	Workstation
A-0005	AMSC0001	Scanner

Inventory ID	Asset Name	Type
A-0006	AMPR0001	Printer
A-0007	AMPR0002	Printer
A-0008	AMCAM001	Camera
A-0009	AMSRV001	Server
A-0010	AMSRV002	Server
A-0017	AMLPS001	Laptop
A-0025	Automated Teller Machine (ATM)	Automated Teller Machine
A-0028	Profindustry CL	Counterfeit money detector

2.1.2. Λογισμικό και εφαρμογές

Inventory ID	Asset Name	Type
A-0015	Fortinet-Fortigate-400D	Firewall
A-0021	Windows 10 Pro	Software
A-0026	Customer web application	Web application
A-0027	Employee web application	Web application

2.1.3. Δίκτυο

Inventory ID	Asset Name	Type
A-0011	AMCSW001	Switch
A-0012	AMCSW002	Switch
A-0013	AMCSW003	Switch
A-0014	AMCRT001	Router
A-0016	VIPH0001	VoIP Phone

2.1.4. Δεδομένα

Inventory ID	Asset Name	Type
A-0018	Bank Customer Data	Data
A-0019	Bank Employee Data	Data

2.1.5. Διαδικασίες

Inventory ID	Asset Name	Type
A-0022	Money Withdrawal from ATM	Process
A-0023	Money Deposit	Process
A-0024	New Account Opening	Process

3. ΑΠΟΤΙΜΗΣΗ ΠΣ ΚΑΙ ΕΓΚΑΤΑΣΤΑΣΕΩΝ ΤΡΑΠΕΖΑΣ

3.1. Αγαθά που εντοπίστηκαν

Inventory ID	Asset Name	Type
A-0001	AMCWS001	Workstation
A-0002	AMCWS002	Workstation
A-0003	AMCWS003	Workstation
A-0004	AMCWS004	Workstation
A-0005	AMSC0001	Scanner
A-0006	AMPR0001	Printer
A-0007	AMPR0002	Printer
A-0009	AMSRV001	Server
A-0010	AMSRV002	Server
A-0011	AMCSW001	Switch
A-0012	AMCSW002	Switch
A-0013	AMCSW003	Switch
A-0014	AMCRT001	Router
A-0016	VIPH0001	VoIP Phone
A-0017	AMLPS001	Laptop
A-0018	Bank Customer Data	Data
A-0019	Bank Employee Data	Data

Inventory ID	Asset Name	Type
A-0021	Windows 10 Pro	Software
A-0022	Money Withdrawal from ATM	Process
A-0023	Money Deposit	Process
A-0024	New Account Opening	Process
A-0025	Automated Teller Machine (ATM)	Automated Teller Machine
A-0026	Customer web application	Web application
A-0027	Employee web application	Web application
A-0028	Profindustry CL	Counterfeit money detector

3.2. Απειλές που εντοπίστηκαν

- Phising attack, δηλαδή ο επιτιθέμενος θα οδηγήσει τον πελάτη της τράπεζας σε κάποιο ψεύτικο site το οποίο μοιάζει με το αυθεντικό site της τράπεζας στέλνοντάς του ένα link. Ο χρήστης πατώντας πάνω στο link θα οδηγηθεί στο ψεύτικο site όπου ο επιτιθέμενος θα μπορέσει να του κλέψει τα προσωπικά δεδομένα.
- DoS attack. Αυτού του είδους οι απειλές στέλνουν χιλιάδες αιτήματα τραυτόχρονα από διαφορετικές IP διευθύνσεις σε ένα site με αποτέλεσμα να αυξάνεται η κίνηση στην ιστοσελίδα της τράπεζας και ο server να μην μπορεί να ανταποκριθεί σε όλα αυτά τα αιτήματα. Κατά συνέπεια ο χρόνος ανταπόκρισης της ιστοσελίδας να γίνεται πολυ αργός και οι χρήστες να μην μπορούν να εκτελέσουν τις επιθυμητές ενέργειες σωστά. Επιπλέον υπάρχει και ο κίνδυνος η ιστοσελίδα να μην είναι καθόλου διαθέσιμη στους χρήστες για ένα αρκετά μεγάλο χρονικό διάστημα, από κάποια λεπτά έως και ώρες.
- Domain Name System Hijacking. Σε αυτόν τον τύπο επίθεσης αλλάζονται από ρυθμίσεις DNS με αποτέλεσμα η κίνηση που θα στέλνονταν στον web server της τράπεζας να στέλνεται στον web server του χάκερ και έτσι εκείνος να αποσπά σημαντικές πληροφορίες.
- Cross-Site Request Forgery ή CSRF επιθέσεις γίνονται όταν οι χρήστες πατούν πάνω σε κάποιο link που του στάλθηκε ή κατεβάζουν αρχεία και οι επιτιθέμενοι αναγκάζουν τον χρήστη να εκτελέσει ανεπιθύμητες ενέργειες όπως για παράδειγμα αλλαγή κωδικών ή μεταφορά χρημάτων. Έτσι κλονίζεται η εμπιστοσύνη που έχουν οι πελάτες στην τράπεζα.
- Επιθέσεις SQL Injection. Σε αυτού του είδους τις επιθέσεις οι χάκερς πληκτρολογούν SQL κώδικα ερωτήματος σε μια φόρμα και η εφαρμογή που επεξεργάζεται αυτόν τον κώδικα δεν τον ελέγχει σωστά και τον επικυρώνει επιτρέποντας με αυτόν τον τρόπο στον εισβολέα να δώσει εντολές στην βάση δεδομένων.
- Κάποιος υπάλληλος μπορεί να διαγράψει ή να τροποποιήσει τα δεδομένα που βρίσκονται αποθηκευμένα στον data server.

- Καθώς κάποιος υπάλληλος της τράπεζας συνδέεται στο internet ή συνδέει στον υπολογιστή κάποια άλλη συσκευή (π.χ usb) ο υπολογιστή μπορεί να προσβληθεί από κακόβουλο λογισμικό που βρίσκεται ήδη εγκατεστημένο στην συσκευή. Αν το ιομορφικό λογισμικό δεν έχει ενημερωθεί με την πιο πρόσφατη έκδοση δεν μπορεί να εντοπίσει το επικίνδυνο malware και να το αντιμετωπίσει. Έτσι αυτό εγκαθίσταται στον υπολογιστή και ίσως οδηγήσει σε απώλεια αρχείων και δεδομένων.
- Καθώς εγκαθίσταται λογισμικό από μη έγκυρη πηγή είναι πολύ πιθανό να έχει μολυνθεί από malware, το οποίο θα εγκατασταθεί στον υπολογιστή της τράπεζας μαζί με το λογισμικό. Αυτό έχει ως αποτέλεσμα όχι μόνο να επηρεάσει και να οδηγήσει στην απώλειά τους αλλά και να δώσει πρόσβαση και έλεγχο του υπολογιστή σε κάποιον τρίτο.
- Κάποιος μη εξουσιοδοτημένος υπάλληλος της τράπεζας μπορεί να αποκτήσει πρόσβαση σε αρχεία που περιέχουν ευαίσθητα προσωπικά δεδομένα των πελατών και να χρησιμοποιήσει για προσωπικό όφελος είτε να τα πουλήσει σε τρίτους.
- Η μη κρυπτογραφημένη κίνηση του VoIP phone στο δίκτυο δίνει την δυνατότητα σε κάποιον που θα αποκτήσει πρόσβαση στο δίκτυο να ‘’ακούσει’’ τις πληροφορίες που μεταφέρονται μέσω αυτού και έτσι να αποκτήσει πρόσβαση στα προσωπικά δεδομένα τόσο των υπαλλήλων της τράπεζας όσο και των πελατών της.
- Κάποιος εισβολέας αποκτώντας πρόσβαση στο VoIP phone μπορεί να υποδυθεί κάποιον υπάλληλο της τράπεζας και να επικοινωνήσει με κάποιον πελάτη. Ο πελάτης νομίζοντας ότι μιλάει με κάποιον νόμιμο υπάλληλο της τράπεζας και να του δώσει όσα στοιχεία του ζητηθούν.
- Δίνεται η δυνατότητα σε κακόβουλα, μη πιστοποιημένα φυσικά πρόσωπα να αποκτήσουν πρόσβαση σε όλα τα επιθυμητά αρχεία του υπολογιστή, να τροποποιήσουν, να αλλοιώσουν, να αντιγράψουν, να διαγράψουν ακόμη και να στείλουν προσωπικά δεδομένα και αρχεία, εφόσον η οθόνη παραμένει σε κατάσταση αδράνειας και όχι κλειδώματος μετά την απομάκρυνση του αρμοδίου υπαλλήλου.
- Κάποιοι επιτιθέμενοι μπορούν να αποκτήσουν πρόσβαση στις ευαίσθητες πληροφορίες των κατόχων καρτών τραπέζης εφόσον η κάρτα, κατά την διαδικασία ανάληψης ή κατάθεσης χρημάτων σε ένα ATM ,παραμείνει στο εσωτερικό αυτού για ανεξήγητα μεγάλο χρονικό διάστημα.
- Κακόβουλοι απομακρυσμένοι χρήστες, αποκτώντας πρόσβαση σε ένα ATM, μπορούν να αλλάζουν τα στοιχεία κατάθεσης χρημάτων και να τα στέλνουν σκόπιμα σε δικούς τους λογαριασμούς .Αυτό πολλές φόρες είναι δύσκολο να γίνει αντιληπτό από τους κάτοχους των καρτών καθώς οι περισσότεροι εμπιστεύονται τυφλά το σύστημα και δεν πραγματοποιούν έλεγχο ορθότητας με βάση την απόδειξη συναλλαγής.

3.3. Ευπάθειες που εντοπίστηκαν

- Τρωτά σημεία και λάθος ρύθμιση των server.Για παράδειγμα διατήρηση των προεπιλεγμένων ρυθμίσεων.
- Εγκατάσταση λογισμικού από μη έγκυρη πηγή.
- Μη κρυπτογραφημένη κίνηση του VoIP phone στο δίκτυο.
- Διατήρηση προεπιλεγμένων ρυθμίσεων.
- Έλλειψη θέσπισης πολιτικών και διαδικασιών ασφαλείας.

- Η αυτόματη ενημέρωση εφαρμογών, λειτουργικού συστήματος και ιομοφρικού λογισμικού είναι απενεργοποιημένη.
- Υπάρχουν bugs στο λειτουργικό σύστημα και στους servers τα οποία μπορεί να επιτρέψουν στους επιτιθέμενους να λάβουν τον πλήρη έλεγχό τους.
- Μη χρήση ή χρήση πολύ εύκολων κωδικών.
- Στα πλαίσια ενός γραφείου οι εργαζόμενοι ίσως, μη λαμβάνοντας υπόψιν τους κινδύνους που ελλοχεύουν, κατά την απομάκρυνσή τους από τους προσωπικούς τους υπολογιστές, αφήνουν ανοιχτές τις οθόνες αυτών ή ακόμη και καθώς πατούν το κουμπί αναστολής/αδράνειας και δεν γνωρίζουν ότι η οθόνη παραμένει ξεκλείδωτη.
- Πολλοί χρήστες αγνοούν το ότι πρέπει να χρησιμοποιούν την μπαταριά τύπου CMOS και εμμένουν στην χρησιμοποίηση της κύριας μπαταρίας των προσωπικών τους υπολογιστών.
- Οι επιτιθέμενοι χρήστες έχουν την δυνατότητα να κάνουν κατάχρηση μιας συγκεκριμένης ευπάθειας διαδρομής χρησιμοποιώντας το πρωτόκολλο SCP.Οι επιτιθέμενοι εκμεταλλευόμενοι αυτό το ελάττωμα μπορούν επίσης να αποκτήσουν πρόσβαση σε απομακρυσμένη εκτέλεση κώδικα δημιουργώντας ένα ωφέλιμο φορτίο που καταχράται τη λειτουργία εντολής SITE.
- Η ευπάθεια της παράκαμψης της ταυτότητας στο διαδίκτυο επιτρέπει σε απομακρυσμένο εισβολέα να ανακτήσει την διαμόρφωση της συσκευής κάτι που καθίσταται ιδιαιτέρως επικίνδυνο ειδικά αν αυτή η συσκευή πρόκειται για παράδειγμα για το router,τον printer ή τον scanner.
- Οι ευπάθειες του λογισμικού θα μπορούσαν να επιτρέψουν σε έναν απομακρυσμένο εισβολέα, που δεν έχει ταυτοποιηθεί, να παρακάμψει τα φίλτρα ρύθμισης που έχουν διαμορφωθεί στην συσκευή. Έτσι, θα αποκτήσουν πρόσβαση στα συνημμένα e-mails, τόσο των υπαλλήλων όσο και των πελατών της τράπεζας, με σκοπό την παράνομη χρήση των προσωπικών τους δεδομένων

3.4 Αποτελέσματα αποτίμησης

	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
Workstation	3	3	4	4	7	7	10	10	6	8	3	7	4	5	8	3			4			7		
Server	7	7	8	9	9	10	10	10	8	7	3	6	6	6	10				10	7	8	10	8	5
Printer	1	2	3	3	6	6	6	9	5	5	2	5	3	3	6	6	4	4	4	4	6	6	4	4
VoIP phone	3	4	5	5	7	7	9	9	6	7	3	6	5	6	9	5	5	5	5	7	8	9	5	4
Scanner	2	3	4	4	5	5	7	7	6	6	2	5	3	3	6	6	5	5	6	8	6	6	4	5
Laptop	3	3	5	5	6	9	10	10	6	8	3	6	4	4	7	3			4					
Switch	4	5	7	7	9	9	10	10	8	9	5	8	5	6	7					6	8	8	5	5
ATM	4	6	7	8	8	10	10	10	8	9	6	8	7	6	8	8	7	7	7	7	8	9	7	5
Process	3	3	5	6	7	8	10	10	6	7	6	9	6	6	7									
Router	6	7	9	9	10	10	10	10	10	9	8	9	6	7	7	7	6		7	7	9	9	6	5
Software	4	5	5	6	8	9	10	8	6	8	4	5												
Data	4	4	6	6	8	8	10	10	10	10	7	8	9		10									
Counterfeit money detector	4	4	5	6	7	9	10	10	7	8	4	6												
Customers Web Application	5	6	7	7	7	7	8	8	8	6	4	6	7	6	8	5	7	7	6	6	8	8	6	6

Employees Web Application	5	6	7	7	7	7	8	8	8	6	4	6	6	7	8	8	5	7	8	6	7	8	6	6

Β2. ΠΡΟΤΕΙΝΟΜΕΝΑ ΜΕΤΡΑ ΑΣΦΑΛΕΙΑΣ

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

1. Προσωπικό – Προστασία Διαδικασιών Προσωπικού
2. Ταυτοποίηση και αυθεντικοποίηση
3. Έλεγχος προσπέλασης και χρήσης πόρων
4. Διαχείριση εμπιστευτικών δεδομένων
5. Προστασία από τη χρήση υπηρεσιών από τρίτους
6. Προστασία λογισμικού
7. Διαχείριση ασφάλειας δικτύου
8. Προστασία από ιομορφικό λογισμικό
9. Ασφαλής χρήση διαδικτυακών υπηρεσιών
10. Ασφάλεια εξοπλισμού
11. Φυσική ασφάλεια κτιριακής εγκατάστασης

Τα μέτρα έχουν εφαρμογή στο ΠΣ της AUEB BANK

1. Προσωπικό – Προστασία Διαδικασιών Προσωπικού

- Χρήση ισχυρών προσωπικών κωδικών ασφαλείας για την εισαγωγή των εξουσιοδοτημένων προσώπων και μη γνωστοποίηση αυτών σε τρίτους.
- Αποφυγή αποθήκευσης προσωπικών και ευαίσθητων πληροφοριών στον υπολογιστή. Αντιθέτως, αποθήκευση αυτών σε κάποιο USB, ώστε να προστατευθούν από τρίτους.
- Τακτική παρακολούθηση σεμιναρίων κυβερνοασφαλείας κα πρόληψης από το προσωπικό της τράπεζας.
- Κλείδωμα οθονών(και όχι αδρανοποίηση αυτών) κατά της απομάκρυνση του χρήστη του προσωπικού υπολογιστή από αυτόν.
- Αποφυγή αποθήκευσης κωδικών ασφαλείας στους υπολογιστές.
- Αποφυγή σύνδεσης του υπολογιστή της εργασίας σε δωρεάν δίκτυο Wi-Fi.
- Προσεκτική διατήρηση και ασφάλιση συσκευών όπως υπολογιστές, VoIP phones και γενικότερα συσκευών παροχής προσωπικών πληροφοριών.
- Χρήση εφαρμογών που τραβούν φωτογραφία όταν κάποιος θα επιχειρήσει το ξεκλείδωμα κινητού(ή οποιασδήποτε άλλης προσωπικής συσκευής) και ταυτόχρονα αποστολή τοποθεσίας του επιτηδείου.

2. Ταυτοποίηση και αυθεντικοποίηση

- Να γίνει υποχρεωτική η χρήση ισχυρών κωδικών πρόσβασης κατά την εκκίνηση του υπολογιστή. Οι κωδικοί θα πρέπει να είναι γνωστοί μόνο στους αρμόδιους υπαλλήλους.
- Χρήση κωδικών πρόσβασης ακόμα και όταν ο υπολογιστή χρησιμοποιείται ξανά μετά από αδρανή κατάσταση.
- Κλείδωμα οθόνης έπειτα από ασφαλές χρονικό διάστημα που θα ορίσει ο χρήστης.
- Αποφυγή αποθήκευσης κωδικών ασφαλείας στους υπολογιστές.
- Χρήση εφαρμογών ειδοποίησης ασφαλείας, κατά την διάρκεια που κάποιος εισαχθεί ή προσπαθεί να εισαχθεί στον υπολογιστή/ σύστημα.

- Προστασία κωδικών πρόσβασης.

- Αποφυγή γραφής ή αποθήκευσης κωδικών πρόσβασης σε διάφορα έγγραφα ή άλλα μέσα, προκειμένου να μην υπάρξει πρόβλημα θύμησης αυτών.

- Χρήση ελέγχου ταυτότητας δυο παραγόντων.
- Χρήση διαφορετικών συνθηματικών για κάθε λογαριασμό.
- Δημιουργία ενός κεντρικού συνθηματικού (που θα είναι μεν πολύπλοκο αλλά εύκολο στην απομνημόνευση) ώστε γίνεται μόνο προσωπική προσπέλαση και χρησιμοποίηση οποιοδήποτε άλλου συνθηματικού για οποιοδήποτε άλλο λογαριασμό στον υπολογιστή.

3. Έλεγχος προσπέλασης και χρήσης πόρων

- Έλεγχος προσώπων που χρησιμοποιούν τις συσκευές της τράπεζας.

- Σύνδεση συσκευών εξυπηρέτησης(π.χ. εκτυπωτών,scanner κ.α.) μόνο με υπολογιστές που βρίσκονται στις υπηρεσίες της τράπεζας.

- Εμφάνιση ουράς διεργασιών για την σωστή και ταχύτερη εξυπηρέτηση.

4. Διαχείριση εμπιστευτικών δεδομένων

- Να γίνεται καθημερινά backup των αρχείων.
- Χρήση συσκευών αποθήκευσης(π.χ. USB) και αποφυγή αποθήκευσης αρχείων στον υπολογιστή.
- Χρησιμοποίηση ενός συστήματος δημόσιου-ιδιωτικού κλειδιού που χρησιμοποιεί τον αλγόριθμο Διεθνούς Αλγόριθμου κρυπτογράφησης δεδομένων (IDEA) για την κρυπτογράφηση αρχείων και μηνυμάτων ηλεκτρονικού ταχυδρομείου
- Χρήση ψηφιακών υπογραφών.

5. Προστασία από τη χρήση υπηρεσιών από τρίτους

- Χρήση κωδικών στα αρχεία με ευαίσθητα και σημαντικά δεδομένα.

- Έλεγχος προσωπικού παροχής υπηρεσιών.

- Συνεργασία με αξιόπιστους συνεργάτες.

- Κρυπτογράφηση αρχείων και ευαίσθητων δεδομένων

- Χρήση ψηφιακών υπογραφών και πιστοποιημένων εγγράφων.
- Χρήση πρωτόκολλου ελέγχου ταυτότητας δικτύου που χρησιμοποιεί κρυπτογράφηση μυστικού κλειδιού και διευκολύνει την ενιαία σύνδεση

6. Προστασία λογισμικού

- Να γίνεται συχνά εγκατάσταση των ενημερώσεων.
- Χρήση κατάλληλου λογισμικού που παρακολουθεί την κίνηση μια ιστοσελίδας ώστε να αποφευχθεί μια επίθεση DoS.
- Χρήση firewall.
- Αποφυγή ανοίγματος ύποπτων συνημμένων τα οποία μπορεί να εμφανίζονται σε email, tweet, δημοσιεύσεις, διαφημίσεις στο Internet, μηνύματα ή συνημμένα και, ορισμένες φορές, προσποιούνται ότι προέρχονται από γνωστές και αξιόπιστες πηγές.
- Καταργήστε την εγκατάσταση του παραπλανητικού λογισμικού ασφαλείας με μη αυτόματο τρόπο.
- Πραγματοποίηση λήψης προγραμμάτων μόνο από αξιόπιστες τοποθεσίες Web.
- Προσεκτική ανάγνωση σε όλες τις προειδοποιήσεις ασφάλειας, τις άδειες χρήσης και τις δηλώσεις προστασίας προσωπικών δεδομένων που συσχετίζονται με το λογισμικό.
- Χρησιμοποίηση ενός τυπικού λογαριασμού χρήστη αντί ενός λογαριασμού διαχειριστή.

7. Διαχείριση ασφάλειας δικτύου

- Κρυπτογράφηση των καναλιού που βρίσκεται το VoIP phone.
- Χρήση ασφαλών πρωτοκόλλων
- Χρήση firewall.
- Έλεγχος γνησιότητας της ταυτότητας των χρηστών , των προγραμμάτων ή των μηχανημάτων καθώς και των εξουσιοδοτήσεων που αυτά διαθέτουν για την προσπέλαση των προστατευμένων πόρων του συστήματος.
- Αποφυγή τοποθέτησης δεδομένων σε σημεία οπού δεν είναι κατανοητά.
- Χρησιμοποίηση πρωτοκόλλων ασφαλείας.
- Ενημερώσεις δικτιού.

8. Προστασία από ιομορφικό λογισμικό

- Χρήση προγράμματος προστασίας από ιομορφικό λογισμικό.
- Χρήση firewall.
- Αποφυγή ανοίγματος οποιουδήποτε συνημμένου αρχείου που μπορεί να βρεθεί στο e-mail είτε κατά τη διάρκεια πλοήγησης στο διαδίκτυο.
- Δημιουργία αντιγράφων ασφαλείας των αρχείων σε τακτά χρονικά διαστήματα, σε εξωτερικό μέσο αποθήκευσης και διατήρησής τους εκτός δικτύου, έτσι ώστε να είναι δυνατή η αποκατάστασή τους.

- Πληκτρολόγηση διευθύνσεων των ιστοσελίδων στον φυλλομετρητή ιστοσελίδων, αντί χρήσης υπερσυνδέσμων.
- Απενεργοποίηση εκτέλεσης μακροεντολών και JavaScript στις εφαρμογές με τις οποίες ανοίγουν αρχεία τύπου .docx και .pdf.
- Έλεγχος ενημερώσεων εκδόσεων του λειτουργικού συστήματος.

9. Ασφαλής χρήση διαδικτυακών υπηρεσιών

- Να μην ανοίγονται link και να μην εγκαθίστανται στον υπολογιστή αρχεία που προέρχονται από αναξιόπιστες πηγές.
- Αποφυγή χρήσης διαφόρων site που δεν εξυπηρετούν τους σκοπούς της τράπεζας.
- Απόρριψη και έλεγχος ισοτόπων που χρησιμοποιούν προσωπικά δεδομένα και θεωρούνται αναξιόπιστοι.
- Χρήση του Secure Electronic Transmission (SET) (που είναι ένα πρότυπο πρωτόκολλο που αναπτύχθηκε από τη MasterCard, την VISA και άλλους), για να επιτρέπει στους χρήστες να πραγματοποιούν ασφαλείς συναλλαγές μέσω του Διαδικτύου. Διαθέτει ψηφιακά πιστοποιητικά και ψηφιακές υπογραφές.

10. Ασφάλεια εξοπλισμού

- Χρήση antivirus.
- Συνειδητή και όχι ανεξέλεγκτη χρήση εξοπλισμού.
- Εγκατάσταση προγραμμάτων προστασίας από ιούς.
- Ενημέρωση ή και αλλαγή εξοπλισμού ανά τακτά χρονικά διαστήματα.

11. Φυσική ασφάλεια κτιριακής εγκατάστασης

- Εγκατάσταση συσκευών πυρόσβεσης και ανίχνευσης φωτιάς.
- Χρήση πορτών ασφαλείας.
- Χρήση συναγερμών κλοπής, φωτιάς και πλημμύρας.

Α4. ΣΥΝΟΨΗ ΠΙΟ ΚΡΙΣΙΜΩΝ ΑΠΟΤΕΛΕΣΜΑΤΩΝ

Τα δύο αγαθά με την υψηλότερη επικινδυνότητα είναι ο database Server και το ATM.

Ο database Server στην ουσία είναι στημένος με τέτοιον τρόπο ώστε να κάνει πράγματα σχετικά με τις βάσεις δεδομένων που έχει μέσα του. Για παράδειγμα όταν τον καλέσει μια ιστοσελίδα. Όταν λοιπόν μπει κάποιος επισκέπτης σε κάποιο προϊόν, τότε η ιστοσελίδα θα ζητήσει από τον database Server να της δώσει όλα τα δεδομένα για το προϊόν αυτό ώστε να τα μορφοποιήσει και να τα δείξει στον επισκέπτη. Στην τράπεζα συγκεκριμένα χρησιμοποιείται για να αποθηκεύσει δεδομένα συναλλαγών, προσωπικά δεδομένα πελατών, στοιχεία λογαριασμών, αρχεία δανείων κ.α. Κρίνεται επομένως σκόπιμη η προστασία του από ανεπιθύμητες απειλές. Η πιο σύνηθες επίθεση είναι η τύπου DoS. Συγκεκριμένα, στέλνονται από διαφορετικές IP χιλιάδες διαφορετικά αιτήματα προς εξυπηρέτηση μια δεδομένη χρονική στιγμή, με αποτέλεσμα την αποτυχία ανταπόκρισης του Server σε αυτά. Αυτό έχει ως αποτέλεσμα , ο χρόνος απόκρισης του site να αυξάνεται σημαντικά, καθιστώντας το σύστημα εκτός λειτουργίας για αρκετό χρονικό διάστημα. Ακόμη μια σημαντική επίθεση είναι η SQL Injection. Οι SQL injection επιθέσεις είναι ο πιο συνηθισμένος τρόπος που οι χάκερ χρησιμοποιούν για να αποκτήσουν πρόσβαση σε ιστοσελίδες και για να κλέψουν ευαίσθητα δεδομένα, εκμεταλλευόμενοι τα τρωτά σημεία που υπάρχουν στις εφαρμογές Web που διασυνδέονται με βάσεις δεδομένων στο υπόβαθρο. Για παράδειγμα στην περίπτωση της τράπεζας, ένας χρήστης μπορεί να ζητήσει από το site να του επιστρέψει μια λίστα με τις τελευταίες του συναλλαγές. Αν το site έχει μια SQL ευπάθεια, ωστόσο, ένας εισβολέας μπορεί να εισάγει μια ειδικά δημιουργημένη σειρά με εντολές σε κώδικα στο πλαίσιο αναζήτησης, που θα μπορούσε να παράγει μια λίστα με όλα τα περιεχόμενα της βάσης δεδομένων, τα προσωπικά στοιχεία των πελατών αλλά και τους αριθμούς πιστωτικών καρτών όλων αυτών. Αυτές οι δύο είναι οι πιο σημαντικές επιθέσεις από τις οποίες μπορεί να προσβληθεί ένας Server, ωστόσο υπάρχει πληθώρα απειλών και ευπαθειών.

Χρησιμοποιώντας ένα ATM, οι πελάτες μπορούν να έχουν πρόσβαση στους τραπεζικούς λογαριασμούς τους, προκειμένου να κάνουν αναλήψεις μετρητών (με τη χρήση καρτών ανάληψης ή χρεωστικών καρτών), έλεγχο στις κινήσεις του λογαριασμού τους ή ακόμα και πληρωμές υπολοίπων πιστωτικών καρτών τους. Μια σημαντική απειλή που μπορεί να αντιμετωπίσει ένα ATM είναι να προσβληθεί από κακόβουλο λογισμικό. Με αυτό τον τρόπο μη εξουσιοδοτημένοι απομακρυσμένοι χρήστες μπορούν να αποκτήσουν πρόσβαση στις συναλλαγές ενός πελάτη, αποσπώντας σημαντικά χρηματικά ποσά, προσωπικές πληροφορίες λογαριασμών καθώς επίσης και ενημερωμένο αρχείο καταθέσεων. Επιπλέον, οι επιτιθέμενοι είναι σε θέση να αλλάξουν τα υπόλοιπα λογαριασμών και τα τείχη προστασίας αυτών. Με τη σειρά του, αυτό επιτρέπει τη διαθεσιμότητα απεριόριστων κεφαλαίων κατά τις συναλλαγές εκταμίευσης ATM.