ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΚΑΙ ΚΡΙΣΙΜΩΝ ΥΠΟΔΟΜΩΝ

ΣΧΕΔΙΟ ΑΣΦΑΛΕΙΑΣ

ΣΥΓΓΡΑΦΕΙΣ: Άγγελος Τσελές(3170160),Ανδρέας Πολυχρονάκης(3170140),Ιωάννης Ματσούκας(3170106)

ΕΡΓΑΣΙΑ ΧΕΙΜΕΡΙΝΟΥ ΕΞΑΜΗΝΟΥ 2020-21

Contents

1. ΕΙΣΑΓΩΓΗ

Η εργασία εκπονήθηκε στα πλαίσια του μαθήματος της Ασφάλειας Πληροφοριακών Συστημάτων του 7ου εξαμήνου για το ακαδημαϊκό έτος 2020-2021.

1.1. Περιγραφή Εργασίας

Η παρούσα εργασία αποτελεί μία πρόταση ενός πλάνου ασφαλείας του Πληροφοριακού Συστήματος μιας εταιρείας η οποία έχει δημιουργήσει μια εφαρμογή. Στα πλαίσια λοιπόν του συγκεκριμένου project θα ασχοληθούμε με την παράδοση ενός σχεδίου ασφαλείας στο οποίο θα αναφέρονται εκτενώς όλα τα απαραίτητα βήματα της ανάλυσης επικινδυνότητας δηλαδή όλα τα μέτρα που απαιτούνται για την καλύτερη δυνατή διαχείριση της επικινδυνότητας λαμβάνοντας πάντα υπόψιν μας πιθανούς κινδύνους αλλά και αδυναμίες του συστήματος που έχουν εντοπιστεί.

1.2. Δομή παραδοτέου

Αναλυτικότερα, στην ενότητα 2 θα παρουσιάσουμε την μεθοδολογία που ακολουθήσαμε μαζί και με τα αντίστοιχα βήματα. Ακόμη, θα γίνει μια λεπτομερής καταγραφή των Πληροφοριακών Συστημάτων της εταιρείας τα οποία πέραν της μελέτης θα πρέπει να τα επεξεργαστούμε. Στην ενότητα 3,περιγράφονται τα αποτελέσματα τόσο από την μελέτη όσο και από την ανάλυση επικινδυνότητας που εκπονήθηκε προηγουμένως. Συνεχίζοντας, στην ενότητα 4 θα γίνει μία αναφορά στα προτεινόμενα μέτρα ασφαλείας που θεωρούμε ότι μπορούν να βοηθήσουν σημαντικά στην αντιμετώπιση των κινδύνων που προαναφέρθηκαν. Τέλος, στην ενότητα 5 θα πραγματοποιηθεί μια σύνοψη των πιο κρίσιμων αποτελεσμάτων που εντοπίστηκαν κατά την διάρκεια της μελέτης.

2. ΜΕΘΟΔΟΛΟΓΙΑ ΜΕΛΕΤΗΣ ΑΣΦΑΛΕΙΑΣ

Για τη Διαχείριση Επικινδυνότητας της bet365 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 *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*

2.1. Περιγραφή Πληροφοριακού Συστήματος (ΠΣ) υπό έλεγχο

Στην ενότητα αυτή, καταγράφονται τα υφιστάμενα πληροφοριακά συστήματα της bet365, τα οποία με το πέρας της μελέτης θα επικαιροποιηθούν, αναβαθμιστούν ή σε κάποιες περιπτώσεις αντικατασταθούν.

2.1.1. Υλικός εξοπλισμός (hardware)

Παρακάτω παρατίθενται όλος ο υλικός εξοπλισμός hardware του Πληροφοριακού Συστήματος. Το ΠΣ αποτελείται από servers ,συσκευές δικτύου(routers,switches,access point,WLAN controller) και συσκευές που χρησιμοποιούν το δίκτυο όπως υπολογιστές,laptop,εκτυπωτή,tablet και voIP τηλέφωνο. Οι συσκευές αυτές χρησιμοποιούν το δίκτυο μέσω των συσκευών δικτύου ώστε να πραγματοποιηθούν όλες οι εργασίες που απαιτούνται. Πιο συγκεκριμένα, οι συσκευές δικτύου μοιράζουν το σήμα του δικτύου μεταξύ των servers και των υπόλοιπων συσκευών που βρίσκονται σε διαφορετικό όροφο.

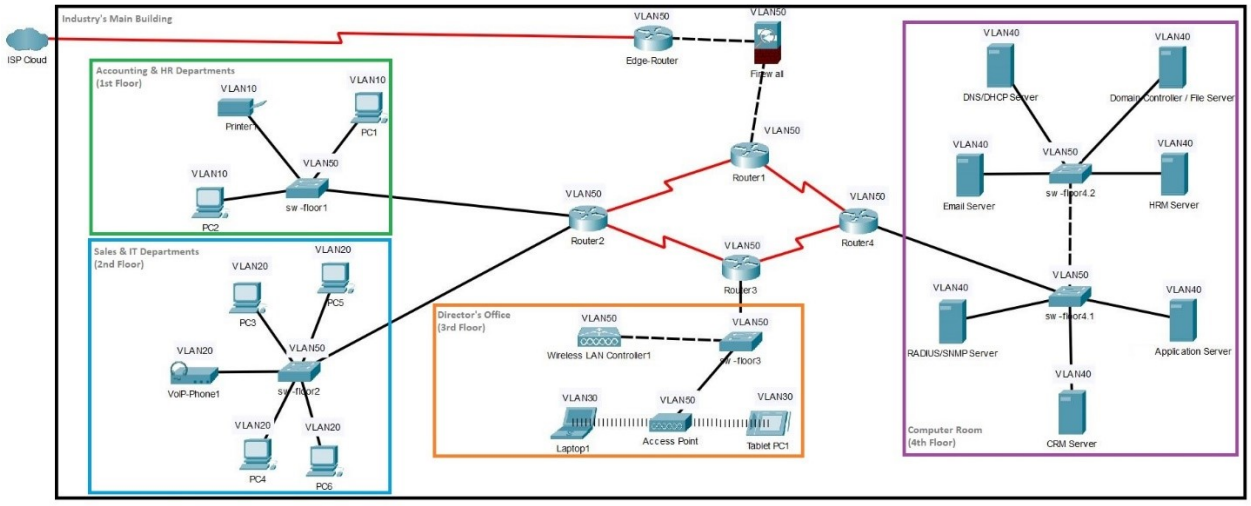
Asset Name	
LAPTOP1	SW-FLOOR4.1
PC5	ROUTER1
CRM SERVER	SW-FLOOR4.2
RADIUS/SNMP SERVER	ROUTER4
ROUTER2	APPLICATION SERVER
VOIP-PHONE1	PC3
ROUTER3	PC1
WIRELESS-LAN-CONTROLLER1	PC2
TABLET-PC1	DOMAIN CONTROLLER/FILE SERVER
EMAIL SERVER	SW-FLOOR2
PC4	ACCESS POINT
PC6	SW-FLOOR1
PRINTER1	SW-FLOOR3
EDGE-ROUTER	
DNS/DHCP SERVER	
HRM SERVER	
SW-FLOOR4.1	

2.1.2. Λογισμικό και εφαρμογές

- Windows 10 Pro
- Windows 7
- Windows Server 2008
- Windows XP
- Ubuntu 16.04.7 LTS
- Ubuntu 12.04.5 LTS
- Cisco proprietary software
- FortiGate proprietary software
- Android 9 Pie(API 28)
- Epson proprietary software

2.1.3. Δίκτυο

Παρακάτω φαίνεται η τοπολογία του δικτύου και το πως επικοινωνούν οι συσκευές hardware μεταξύ τους όπως εξηγήσαμε παραπάνω.



2.1.4. Δεδομένα

Asset Name
Industry Customer Data
Industry Employee Data

2.1.5. Διαδικασίες

Asset Name
Create New Customer
Create New Order (Local)
Create New Order (Remotely)
Customer Support

3. ΑΠΟΤΙΜΗΣΗ ΠΣ ΚΑΙ ΕΓΚΑΤΑΣΤΑΣΕΩΝ ΒΙΟΜΗΧΑΝΙΑΣ

Στην ενότητα αυτή αναφέρονται όλα τα αγαθά που εντοπίστηκαν καθώς και οι απειλές και οι ευπάθειες τους. Στο τέλος αναφέρονται τα αποτελέσματα αποτίμησης για κάθε αγαθό ξεχωριστά.

3.1. Αγαθά που εντοπίστηκαν

Inventory ID	Asset Name
CI-A-1000	Industry Customer Data
CI-A-1001	Industry Employee Data
CI-A-1002	Create New Customer
CI-A-1003	Create New Order (Local)
CI-A-1004	Create New Order (Remotely)
CI-A-1005	Customer Support
CI-A-1006	Windows 10 Pro
CI-A-1007	Windows 7
CI-A-1008	LAPTOP1
CI-A-1009	PC5
CI-A-1010	CRM SERVER
CI-A-1011	RADIUS/SNMP SERVER
CI-A-1012	ROUTER2
CI-A-1013	VOIP-PHONE1
CI-A-1015	ROUTER3
CI-A-1016	WIRELESS-LAN-CONTROLLER1
CI-A-1017	TABLET-PC1
CI-A-1018	EMAIL SERVER
CI-A-1019	PC4
CI-A-1020	PC6
CI-A-1021	PRINTER1
CI-A-1022	EDGE-ROUTER
CI-A-1023	DNS/DHCP SERVER
CI-A-1024	HRM SERVER
CI-A-1025	SW-FLOOR4.1
CI-A-1026	ROUTER1
CI-A-1027	SW-FLOOR4.2
CI-A-1028	ROUTER4
CI-A-1029	APPLICATION SERVER
CI-A-1030	PC3
CI-A-1031	PC1
CI-A-1032	PC2
CI-A-1033	DOMAIN CONTROLLER/FILE SERVER
CI-A-1034	SW-FLOOR2
CI-A-1035	ACCESS POINT
CI-A-1036	SW-FLOOR1
CI-A-1037	SW-FLOOR3

3.2. Απειλές που εντοπίστηκαν

Potential Threats
Excessive Privilege Abuse
Insider Employee gets employee personal data
Access to the network of unauthorized user
Cross Side Scripting(XSS)
Order is compromised
Social engineering
Brute force attack
RCE Attack
Ransomware
Man-in-the-middle attack
Threat of Data leakage
DNS tunneling
Data Breach
SQL Injection Attack
Routing Table Poisoning
Denial of Service
Packet Mistreating Attacks
Hit and Run
Shadow IT
Rootkit
Phishing
Spyware
Computer Virus
Adware
Keylogger
Computer worm
Rogue Access Points
Remote eavesdropping
Unauthorized changes to settings
Saved copies on the internal storage
Evil Twin Attacks
CDP Manipulation
STP Attacks
Against The VTY Lines Attacks
MAC Flooding
Trojan
Scareware
Cryptojacking
Fleeceware
ARP spoofing

3.3. Ευπάθειες που εντοπίστηκαν

Vulnerabilities
Rules not appropriately configured
Database not encrypted
Incomplete package sender authentication
No validation or encoding user input
There is no security policy within industry

No sufficient investment in high quality equipment/software which provide security
Employees' network at home is not as secure as industry's network
Personal devices are usually unprotected
Human Factor
Weak credentials
Remote code execution vulnerability(Windows Jet Database Engine improperly handles objects in memory)
Lack of technical support and updates from Microsoft
Inherently Insecure Services(FTP, Telnet)
SNMP messages are not encrypted
Unprotected communication channels and lack of encryption(SSL/TLS encryption in SMTP,POP3,IMAP protocols)
DNS relays query information from internal workstations to outside servers
Stolen credentials (by phising)
Missing or failed updates
Without correct protection and encryption, the routing table of the router can become extremely vulnerable.
If an attacker floods the routers networks with message requests, the router simply cannot handle the sheer volume of the requests at one time.
The router may be vulnerable against harmful packages within the routing process.
Router is vulnerable to massive attacks at one time
Google Play Store cannot protect users from apps that use the method of hidden charges.
Director may prefer different apps than those IT recommends.
Insufficient security protection
Insufficient Staff awareness training
Individuals within companies may have taken it upon themselves to set up an authorized access point, without informing the network administrator.
Unrestricted Remote Access
Unsecured Document Storage
Poor Administrative Security
Director may be unsuspected to potential phising/scam threats and connect to a fake wireless access point which is identical to the legitimate one.
CDP packets are enabled on all interfaces by default on Cisco switches and they are transmitted in clear text.
Switch is vulnerable to spoofing the root bridge in the topology.
Telnet transmits packets in clear text
The switch cannot handle an unlimited amount of MAC addresses.
Switch can get fooled by an attacker and any traffic meant for the IP address of a device is be sent to the attacker instead.
Unencrypted connections
SQL injection

3.4. Αποτελέσματα αποτίμησης

Στον παρακάτω πίνακα γίνεται αποτίμηση του Impact για κάθε αγαθό του Asset Inventory, ως προς την διαθεσιμότητα, ακεραιότητα, εμπιστευτικότητα.

	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
Domain Controller / File Server	1	5	8	9	10	10	10	10	8	8	5	8	2	5	8								
Industry Employee Data	1	2	3	5	8	9	9	8	5	6	2	6	4	4	4	5	5	5	5	5	4	4	5	5
Edge-Router	1	2	3	4	5	7	8	8	5	5	2	5	2	6	6	4	4	4	4	4	6	6	4	4
Laptop1	1	2	3	4	5	6	7	8	5	5	2	5	3	6	6									
PC1	2	3	4	4	5	6	7	7	4	4	3	5	3	5	6									
PC2	2	3	4	5	6	7	8	8	5	5	3	6	3	5	7									
PC3	1	2	4	5	6	7	8	8	5	5	2	6	3	5	7									
PC4	1	2	4	5	5	6	6	6	4	4	2	4	3	5	5									
PC5	1	2	3	4	4	4	5	5	3	3	2	4	3	5	5									
PC6	1	2	4	5	6	6	7	7	3	3	2	4	3	5	5									
Tablet-PC1	1	2	2	3	3	4	4	4	2	3	2	3	3	4	4									
Access Point	1	2	3	4	5	6	7	7	4	5	2	4	2	5	5	4	5	5	6	5	7	7	5	5
VOIP-Phone1	1	2	3	4	5	7	7	7	4	5	2	5	3	5	5	5	5	5	6	6	5	7	5	5
Printer1	1	2	3	4	4	5	6	6	3	4	2	4	2	4	4									

Wireless-LAN-Controller1	1	2	3	4	5	6	7	7	4	4	2	5	2	5	6	4	5	5	6	5	6	6	5	5
Windows 10 Pro	2	3	5	7	8	8	9	9	6	6	3	6	3	5	7									
Windows 7	2	3	5	7	8	8	9	9	6	6	3	6	3	5	7									
SW-Floor1	2	3	4	5	6	6	6	6	4	4	2	5	2	5	5	4	5	5	6	5	6	6	5	4
SW-Floor2	2	3	4	5	6	7	7	7	4	4	2	4	2	5	5	4	5	5	6	5	6	7	6	5
SW-Floor3	1	2	3	4	5	6	7	7	4	4	2	4	2	5	5	5	5	5	6	7	6	7	5	4
SW-Floor4.1	3	4	5	6	7	7	8	8	6	6	3	5	2	6	6	5	6	6	8	7	6	8	5	5
SW-Floor4.2	3	4	5	6	6	7	7	7	6	6	3	5	2	6	6	5	6	6	7	6	6	7	5	5
Router1	3	4	5	6	7	8	9	9	6	6	3	6	3	6	7	5	6	6	7	7	9	8	6	6
Router2	2	3	4	5	6	7	8	8	5	5	2	5	3	6	6	5	6	6	8	7	7	7	6	5
Router3	1	2	3	4	5	6	7	8	5	5	2	5	3	6	6	5	4	4	6	7	7	8	6	5
Router4	3	4	5	5	6	7	8	8	5	5	3	6	3	6	7	5	5	5	7	7	8	7	7	6
CRM Server	3	4	5	6	7	8	10	10	8	8	5	8	3	5	7									
Radius/SNMP Server	3	4	5	6	7	8	8	8	6	6	4	7	4	6	7	5	6	6	7	6	6	7	6	6
Email Server	2	3	4	5	7	7	8	8	6	6	5	7	3	5	7	5	4	4	6	6	5	7	6	5
DNS/DHCP Server	2	3	4	5	6	7	8	9	7	7	4	6	2	5	6	3	4	4	5	3	4	5	4	3
HRM Server	2	3	4	5	6	7	8	8	6	6	5	7	5	5	6									
Application Server	4	6	6	8	8	9	9	9	8	8	5	8	4	7	8	5	6	6	7	7	7	8	6	6
Create New Customer	2	3	5	6	7	7	8	8	6	5	4	7	2	6	7	5	5	5	5	4	4	6	6	5

Create New Order (Local)	2	3	4	5	6	7	7	7	5	5	4	7	3	6	7										
Customer Support	2	3	5	7	8	9	10	10	8	7	6	8	3	6	8	5	4	4	4	6	5	8	6	7	
Industry Customer Data	1	2	3	5	8	8	9	9	6	7	2	6	3	5	8	5	5	5	5	5	4	4	5	5	
Create New Order (Remotely)	2	3	4	5	6	7	7	7	5	5	4	6	3	6	7	4	5	5	6	5	5	6	6	5	

Ο πίνακας του Impact Assessment χωρίζεται σε 4 υποκατηγορίες(Απώλεια Διαθεσιμότητας, Απώλεια Ακεραιότητας, Αποκάλυψη , Αστοχίες και λάθη στην τηλεπικοινωνιακή μετάδοση).

Σχετικά με την Απώλεια Διαθεσιμότητας ,βλέπουμε ότι το impact εξαιτίας της απώλειας κάθε αγαθού είναι χαμηλό για τις πρώτες 3 με 12 ώρες. Όσο όμως η απώλεια μεγαλώνει, το impact αυξάνεται σημαντικά. Ιδιαίτερα, αν η απώλεια ενός αγαθού διαρκέσει πάνω από 1 εβδομάδα οι συνέπειες γίνονται όλο και χειρότερες για την επιχείρηση και μπορούν να βλάψουν σε τεράστιο βαθμό την λειτουργία και την φήμη της προς τα έξω.

Σχετικά με την Απώλεια Ακεραιότητας, η Ολική Καταστροφή, όπως είναι λογικό, σημαίνει ότι το αγαθό δεν μπορεί να χρησιμοποιηθεί, οπότε το impact είναι το μέγιστο δυνατό .Στην μερική απώλεια και στην σκόπιμη αλλοίωση ,το impact είναι μέτριο συνήθως αλλά δεν πρέπει να υποτιμηθεί σε καμία περίπτωση, διότι αν πολλά αγαθά ταυτόχρονα έχουν μερική απώλεια τότε οι συνέπειες μπορεί να είναι ολέθριες για την επιχείρηση. Στα λάθη μικρής κλίμακας, το impact είναι χαμηλό προς μέτριο ενώ στα λάθη μεγάλης κλίμακας είναι μέτριο προς υψηλό.

Σχετικά με την Αποκάλυψη, στην περίπτωση που αυτή είναι εσωτερική το impact είναι χαμηλό προς μέτριο. Αν η αποκάλυψη γίνει προς τους παρόχους υπηρεσιών, το impact είναι μέτριο καθώς οι περισσότεροι πάροχοι είναι σχετικά αξιόπιστοι. Παρόλα αυτά, όταν η αποκάλυψη είναι εξωτερική ,το impact είναι υψηλό, καθώς ευαίσθητα δεδομένα και πληροφορίες ενδεχομένως διαρρεύσουν ,ενώ χάκερς μπορεί να επιχειρήσουν να επιτεθούν σε αγαθά της επιχείρησης. Ο κίνδυνος, δηλαδή, είναι αρκετά αυξημένος στην περίπτωση αυτή και είναι κάτι που πρέπει να λάβει σοβαρά η επιχείρηση.

Τέλος, σχετικά με πιθανές αστοχίες και σφάλματα στην τηλεπικοινωνιακή μετάδοση, παρατηρούμε ότι ορισμένα αγαθά δεν συμμετέχουν σε αυτήν, οπότε δεν επηρεάζονται. Για τα υπόλοιπα αγαθά, μπορούμε εύλογα να συμπεράνουμε ότι συγκεκριμένα σφάλματα(π.χ. άρνηση αποστολής ή παραλαβής, παρακολούθηση χρήσης κτλ.) έχουν υψηλότερο impact σε σύγκριση με άλλα σφάλματα που έχουν σαφώς χαμηλότερη επίδραση στον τρόπο λειτουργίας της επιχείρησης.

4. ΠΡΟΤΕΙΝΟΜΕΝΑ ΜΕΤΡΑ ΑΣΦΑΛΕΙΑΣ

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

A1. Προσωπικό – Προστασία Διαδικασιών Προσωπικού

A2. Ταυτοποίηση και αυθεντικοποίηση

A3. Έλεγχος προσπέλασης και χρήσης πόρων

A4. Διαχείριση εμπιστευτικών δεδομένων

A5. Προστασία από τη χρήση υπηρεσιών από τρίτους

A6. Προστασία λογισμικού

A7. Διαχείριση ασφάλειας δικτύου

A8. Προστασία από μορφικό λογισμικό

A9. Ασφαλής χρήση διαδικτυακών υπηρεσιών

A10. Ασφάλεια εξοπλισμού

A11. Φυσική ασφάλεια κτιριακής εγκατάστασης

Τα μέτρα έχουν εφαρμογή στο ΠΣ της bet365.

4.1. Προσωπικό – Προστασία Διαδικασιών Προσωπικού

Detective Controls	Inventory ID
Notify IT Support	CI-A-1005
Consult with a cybersecurity expert	CI-A-1000 CI-A-1024
Staff should act according to the general instructions they have been advised	CI-A-1028 CI-A-1017
Notify local authorities	CI-A-1000 CI-A-1007

Preventive Controls	Inventory ID
Internal Employee Rules and Procedures available	CI-A-1001
Secure employees' home WiFi Network	CI-A-1004
Staff should be trained accordingly to recognize and detect potential threats	CI-A-1008 CI-A-1009 CI-A-1019 CI-A-1020 CI-A-1030 CI-A-1031 CI-A-1032 CI-A-1021 CI-A-1017
Open dialogue between employees and IT staff about the types of apps being used, especially public cloud services	CI-A-1017
Develop a security policy	CI-A-1003 CI-A-1008 CI-A-1009 CI-A-1019 CI-A-1020 CI-A-1030 CI-A-1031 CI-A-1032 CI-A-1021

4.2. Ταυτοποίηση και αυθεντικοποίηση

Preventive Controls	Inventory ID
Enforcing strong credentials and multi-factor authentication	CI-A-1024
Use a 2-Step Verification	CI-A-1008 CI-A-1009 CI-A-1019 CI-A-1020 CI-A-1030 CI-A-1031 CI-A-1032

Detective Controls	Inventory ID
Checking for proper page authentication	CI-A-1010

4.3. Έλεγχος προσπέλασης και χρήσης πόρων

Preventive Controls	Inventory ID
Strict and grant database access base on the user roles requirements	CI-A-1033
Mandatory Access Control	CI-A-1022
CSS encode and validation	CI-A-1002
Stored procedures	CI-A-1029

Detective Controls	Inventory ID
Log Monitoring	CI-A-1001

4.4. Διαχείριση εμπιστευτικών δεδομένων

Preventive Controls	Inventory ID
Know where sensitive data resides	CI-A-1000
High-grade encryption	CI-A-1000 CI-A-1010 CI-A-1024 CI-A-1008 CI-A-1009 CI-A-1019 CI-A-1020 CI-A-1030 CI-A-1031 CI-A-1032
Encryption of both incoming and outgoing emails	CI-A-1018
Input validation	CI-A-1029

Parametrized queries	CI-A-1029

4.5. Προστασία από τη χρήση υπηρεσιών από τρίτους

Preventive Controls	Inventory ID
Use cloud-based VoIP provider that encrypts calls before they are sent.	CI-A-1013

4.6. Προστασία λογισμικού

Preventive Controls	Inventory ID
Invest in quality threat detection software	CI-A-1006
Keep both operating systems and third-party software fully updated	
Upgrade to windows 10 or an advanced edition of windows 7 such as Professionals	CI-A-1007

4.7. Διαχείριση ασφάλειας δικτύου

Preventive Controls	Inventory ID
Deploy VPN	CI-A-1004 CI-A-1010 CI-A-1016 CI-A-1026 CI-A-1027
Set up a firewall	CI-A-1011 CI-A-1023
Network Encryption	CI-A-1027
Use the services of a networking engineer	CI-A-1012
Ensure the router and network are secure	CI-A-1015
Provide ongoing testing	
Install wireless intrusion prevention systems to monitor the radio spectrum for unauthorized access points	CI-A-1035
Disable CDP on non-management interfaces	CI-A-1036
Root guard	CI-A-1034

Detective Controls	Inventory ID
BPDU skew (latency) detection	CI-A-1034
Check Command prompt	CI-A-1027
Use Wireshark	

Loop guard	CI-A-1034
BPDU guard	CI-A-1034
Avoid Telnet	CI-A-1037
Use SSH as possible	
Configuring Port Security	CI-A-1025
Port Base Authentication	
Static ARP entries	CI-A-1027

4.8. Προστασία από ιομορφικό λογισμικό

Preventive Controls	Inventory ID
Use reputable antivirus software	CI-A-1008 CI-A-1009 CI-A-1019 CI-A-1020 CI-A-1030 CI-A-1031 CI-A-1032
Static analysis	
Get antispyware software	

Detective Controls	Inventory ID
Use anti-spyware removal tools	CI-A-1008 CI-A-1009 CI-A-1019 CI-A-1020 CI-A-1030 CI-A-1031 CI-A-1032
Use virus removal tools	
Use an adware removal tool	
Full Malware Scan	
Disable the keylogger program in Task Manager	
Uninstall any suspicious program	

4.9. Ασφαλής χρήση διαδικτυακών υπηρεσιών

Preventive Controls	Inventory ID
Set your spam filters to high	CI-A-1005
Delete any request for personal information or passwords	
Install an ad-blocking or anti-cryptomining extension on web browsers	CI-A-1008 CI-A-1009 CI-A-1019 CI-A-1020 CI-A-1030 CI-A-1031 CI-A-1032

4.10. Ασφάλεια εξοπλισμού

Preventive Controls	Inventory ID
Invest in high quality assets	CI-A-1003
Protect personal devices	CI-A-1004

Detective Controls	Inventory ID
Rebuild the compromised computer	CI-A-1008 CI-A-1009 CI-A-1019 CI-A-1020 CI-A-1030 CI-A-1031 CI-A-1032

Separate the wireless network from the organizational wired network	CI-A-1026
Replacing old printers with new printers	CI-A-1021

4.11. Φυσική ασφάλεια κτιριακής εγκατάστασης

Δεν υπάρχει κάποιο προτεινόμενο μέτρο ασφάλειας που να εντάσσεται σε αυτή την κατηγορία.

5. ΣΥΝΟΨΗ ΠΙΟ ΚΡΙΣΙΜΩΝ ΑΠΟΤΕΛΕΣΜΑΤΩΝ

1) Man-in-the-middle attack

Αγαθό που απειλεί: Αυτή του είδους επίθεση απειλεί τον CRM Server. Ο CRM Server διαχειρίζεται την αλληλεπίδραση της βιομηχανίας με τους πελάτες της αυτοματοποιώντας διεργασίες πωλήσεων που πραγματοποιούνται στο χώρο της βιομηχανίας.

Ευπάθεια που εκμεταλλεύεται: Η απειλή αυτή εκμεταλλεύεται την εκ φύσεως αδυναμία των services όπως του FTP και του Telnet. Ο κράκερ με αυτόν τον τρόπο παρεμποδίζει την νόμιμη επικοινωνία μεταξύ των δύο μερών και ελέγχει την ροή επικοινωνίας.

Πιθανή Συνέπεια: Ο κράκερ μπορεί να αποκτήσει πρόσβαση ευαίσθητα δεδομένα και στοιχεία των πελατών της βιομηχανίας, χωρίς να γίνει αντιληπτό ούτε στον διαχειριστή ούτε στην λειτουργία του server.

Αξιολόγηση Συνέπειας: Το γεγονός ότι ένας μη εξουσιοδοτημένος χρήστης μπορεί να αποκτήσει πρόσβαση σε απόρρητα και ευαίσθητα δεδομένα ενδέχεται να έχει καταστροφικές επιπτώσεις για την βιομηχανία. Πέρα από τις πληροφορίες και τα δεδομένα, είναι σχεδόν βέβαιο ότι θα κλονιστεί η αξιοπιστία των πελατών απέναντι στην βιομηχανία και η φήμη της θα πέσει δραματικά. **10/10**

Αξιολόγηση Πιθανότητας: Η επίθεση Man-in-the-middle είναι μία από τις πιο δημοφιλής επιθέσεις στον κλάδο των επιχειρήσεων. Οι επιτιθέμενοι προσπαθούν να αποκτήσουν πρόσβαση σε ευαίσθητα δεδομένα είτε λόγω χρηματικών κινήτρων είτε επειδή κάποια ανταγωνιστική επιχείρηση θέλει να πλήξει την βιομηχανία. **9/10**

Μέτρα Πρόληψης: Ένα μέτρο πρόληψης που προτείνεται είναι η χρήση ενός δικτύου VPN(Virtual Private Network). Ένα VPN δίκτυο συνήθως απαιτεί από τους απομακρυσμένους χρήστες του δικτύου πιστοποίηση, και συχνά ασφαλίζει τα δεδομένα με τεχνολογίες κρυπτογράφησης για να εμποδιστεί η διάδοση των ιδιωτικών πληροφοριών σε μη εξουσιοδοτημένους τρίτους. Ένα άλλο μέτρο είναι η υψηλού βαθμού κρυπτογράφηση των δεδομένων ώστε να μην μπορούν να τα εκμεταλλευτούν μη εξουσιοδοτημένοι χρήστες.

Μέτρα Ανίχνευσης: Ο χρήστης πρέπει να ελέγχει αν η σελίδα που ανοίγει είναι αυθεντικοποιημένη. Εάν δεν είναι, πρέπει οπωσδήποτε να αποχωρίσει από αυτήν άμεσα αλλιώς θα εκτεθεί σε κίνδυνο.

Αξιολόγηση Ευπάθειας: Η ευπάθεια αυτή είναι πολύ σοβαρή και η επιχείρηση σίγουρα πρέπει να την λάβει υπόψιν της. Η απειλή μπορεί να εκμεταλλευτεί την ευπάθεια αυτή και να προκαλέσει μεγάλες ζημιές .Παρόλα αυτά, η επιχείρηση μπορεί να πάρει τα κατάλληλα μέτρα(κυρίως στο επίπεδο της πρόληψης) ώστε ο κίνδυνος να αντιμετωπιστεί όσο γίνεται. **9/10**

RPN: **810**

2) SQL Injection Attack

Αγαθό που απειλεί: Αυτή η είδους επίθεση απειλεί τον Application Server. Ο Application Server διαχειρίζεται τις αλληλεπιδράσεις της βιομηχανίας με τους πελάτες αυτοματοποιώντας διεργασίες απομακρυσμένων πωλήσεων. Λαμβάνει τα HTTP requests και αλληλεπιδρά με τον CRM Server για την διεκπεραίωση μιας πώλησης.

Ευπάθεια που εκμεταλλεύεται: Το SQL injection είναι μια ευπάθεια που αφορά την ασφάλεια του ιστού. Επιτρέπει στον επιτιθέμενο να παρεμβάλει στις επερωτήσεις(queries) που κάνει η εφαρμογή στην βάση δεδομένων της.

Πιθανή Συνέπεια: Ο επιτιθέμενος μπορεί να αποκτήσει πρόσβαση σε ευαίσθητες πληροφορίες και δεδομένα, να τα τροποποιήσει ακόμα και να τα διαγράψει. Αυτό μπορεί να προκαλέσει ζημιές και καταστροφές στις λειτουργίες της εφαρμογής και στη συμπεριφορά της, οι οποίες πολύ πιθανό είναι να περάσουν και απαρατήρητες.

Αξιολόγηση Συνέπειας: Οι συνέπειες μπορεί να είναι καταστροφικές για την βιομηχανία ,καθώς διαρρέουν πολύτιμες πληροφορίες και δεδομένα σε μη εξουσιοδοτημένους χρήστες και επίσης η λειτουργία και η αξιοπιστία της εφαρμογής κλονίζονται σε μεγάλο βαθμό. **9/10**

Αξιολόγηση Πιθανότητας: Το SQL Injection Attack είναι μια πολύ συνηθισμένη επίθεση που κυρίως πραγματοποιείται με σκοπό την απόκτηση απόρρητων πληροφοριών. Είναι βέβαιο ότι η βιομηχανία θα δεχτεί τέτοιες επιθέσεις και θα πρέπει να είναι σε θέση να τις προλαμβάνει και να τις αντιμετωπίζει. **9/10**

Μέτρα Πρόληψης: Προτείνονται 3 μέτρα πρόληψης. Το πρώτο είναι το input validation,το οποίο εξασφαλίζει ότι μόνο συγκεκριμένα δεδομένα μπαίνουν στην ροή εργασίας σε ένα Πληροφοριακό Σύστημα και με αυτόν τον τρόπο δεδομένα που θέλουν να βλάψουν το σύστημα δεν μπορούν να εισέλθουν. Το δεύτερο μέτρο είναι να χρησιμοποιούνται παραμετροποιημένες επερωτήσεις(parameterized queries). Οι επερωτήσεις αυτές απαιτούν τουλάχιστον μία παράμετρο προκειμένου να εκτελεστούν. Αυτή η παράμετρος περνιέται στην επερώτηση με μία ξεχωριστή δήλωση. Το τρίτο μέτρο είναι η χρήση αποθηκευμένων διαδικασιών(stored procedures).

Οι αποθηκευμένες διαδικασίες είναι έτοιμα κομμάτια κώδικα που μπορούν να αποθηκευτούν και έτσι ο κώδικας να χρησιμοποιηθεί όποτε απαιτείται.

Μέτρα Ανίχνευσης: Ως μέτρο ανίχνευσης προτείνεται η ενεργοποίηση του firewall το οποίο μπορεί να ανιχνεύσει πιθανές επιθέσεις SQL Injection.

Αξιολόγηση Ευπάθειας: Η ευπάθεια αυτή είναι πολύ σοβαρή και ο επιτιθέμενος μπορεί να εκμεταλλευτεί πιθανά κενά ασφαλείας και να αποκτήσει πρόσβαση σε εμπιστευτικά δεδομένα, προκαλώντας σοβαρές έως και ανεπανόρθωτες ζημιές για την βιομηχανία. Υπάρχουν ορισμένα μέτρα που μπορούν να βοηθήσουν στην αντιμετώπιση αυτής της επίθεσης έως ένα βαθμό. **9/10**

RPN: **729**

References

Adware. (n.d.). Retrieved from www.malwarebytes.com: https://www.malwarebytes.com/adware/

Anderson, S. (2020, March 22). *10 Latest (MOST DANGEROUS) Virus & Malware Threats in 2020*. Retrieved from www.safetydetectives.com: https://www.safetydetectives.com/blog/most-dangerous-new-malware-and-security-threats/

Application server. (n.d.). Retrieved from en.wikipedia.org: https://en.wikipedia.org/wiki/Application_server

Casey, B. (2013, December). *Identifying and preventing router, switch and firewall vulnerabilities*. Retrieved from searchsecurity.techtarget.com: https://searchsecurity.techtarget.com/tip/Identifying-and-preventing-router-switch-and-firewall-vulnerabilities

Cryptojacking – What is it? (n.d.). Retrieved from www.malwarebytes.com: https://www.malwarebytes.com/cryptojacking/

Fu, A. (2017, December 5). *Secure Print: 5 Print Security Threats to Watch Out For*. Retrieved from www.uniprint.net: https://www.uniprint.net/en/secure-print-5-print-security-threats/

How Data Breaches Happen. (n.d.). Retrieved from www.kaspersky.com: https://www.kaspersky.com/resource-center/definitions/data-breach

HP. (2018, July 2). *How to prevent cyber attacks on your work printers*. Retrieved from www.stuff.co.nz: https://www.stuff.co.nz/business/better-business/105107047/how-to-prevent-cyber-attacks-on-your-work-printers

Human resource management system. (n.d.). Retrieved from en.wikipedia.org: https://en.wikipedia.org/wiki/Human_resource_management_system

Keyloggers - What is a keystroke logger? (n.d.). Retrieved from www.malwarebytes.com: https://www.malwarebytes.com/keylogger/

McCraw, C. (2020, May 6). *12 VoIP Security Vulnerabilities and How to Fix Them*. Retrieved from getvoip.com: https://getvoip.com/blog/2020/05/06/voip-security/

Mokadem, H. E. (n.d.). *Switch Attacks and Countermeasures*. Retrieved from www.cisco.com: https://www.cisco.com/c/dam/en_us/training-events/le31/le46/cln/promo/share_the_wealth_contest/finalists/Hany_EL_Mokadem_Switch_Attacks_and_Countermeasures.pdf

Nadeau, M. (2020, July 9). *What is cryptojacking? How to prevent, detect, and recover from it*. Retrieved from www.csoonline.com: https://www.csoonline.com/article/3253572/what-is-cryptojacking-how-to-prevent-detect-and-recover-from-it.html

NEWMAN, L. H. (2020, January 5). *Hacker Lexicon: What Is Fleeceware, and How Can You Protect Yourself?* Retrieved from www.wired.com: https://www.wired.com/story/what-is-fleeceware-protect-yourself/

NortonLifeLock. (2019, August 28). *What is a computer worm, and how does it work?* Retrieved from us.norton.com/: https://us.norton.com/internetsecurity-malware-what-is-a-computer-worm.html

Nuggets, M. -T. (2018, November 19). *5 Threats to Your Email Server*. Retrieved from www.cbtnuggets.com: https://www.cbtnuggets.com/blog/certifications/microsoft/5-threats-to-your-email-server

Petters, J. (2020, October 8). *What is a Man-in-the-Middle Attack: Detection and Prevention Tips*. Retrieved from www.varonis.com: https://www.varonis.com/blog/man-in-the-middle-attack/

Pressley, A. (2017, October 16). *The 5 most common router attacks on a network*. Retrieved from www.intelligentcio.com: https://www.intelligentcio.com/eu/2017/10/16/the-5-most-common-router-attacks-on-a-network/

PREVENTING XSS. (n.d.). Retrieved from www.veracode.com: https://www.veracode.com/security/preventing-xss

Researcher, M. A. (2006, June 29). *The Ten Most Critical Wireless and Mobile Security Vulnerabilities*. Retrieved from www.helpnetsecurity.com: https://www.helpnetsecurity.com/2006/06/29/the-ten-most-critical-wireless-and-mobile-security-vulnerabilities/

ROOTKIT: WHAT IS A ROOTKIT? (n.d.). Retrieved from www.veracode.com: https://www.veracode.com/security/rootkit

Samarati, M. (2020, September 4). *Phishing attacks: 6 reasons why we keep taking the bait*. Retrieved from www.itgovernance.co.uk: https://www.itgovernance.co.uk/blog/6-reasons-phishing-is-so-popular-and-so-successful

Security, P. (2019, March 25). *What is Adware? Tips for Preventing and Removing*. Retrieved from www.pandasecurity.com: https://www.pandasecurity.com/en/mediacenter/panda-security/what-is-adware/

SPYWARE. (n.d.). Retrieved from www.veracode.com: https://www.veracode.com/security/spyware

SQL injection. (n.d.). Retrieved from portswigger.net: https://portswigger.net/web-security/sql-injection

Stas Ignatenko, D. R. (2019, March 22). Retrieved from apriorit: https://www.apriorit.com/qa-blog/428-mail-server-security-testing

Trojan horse (computing). (n.d.). Retrieved from en.wikipedia.org: https://en.wikipedia.org/wiki/Trojan_horse_(computing)

VoIP vulnerabilities. (n.d.). Retrieved from en.wikipedia.org: https://en.wikipedia.org/wiki/VoIP_vulnerabilities

What is a Computer Virus and What Does It Do? (n.d.). Retrieved from www.webroot.com: https://www.webroot.com/au/en/resources/tips-articles/computer-security-threats-computer-viruses

What is a DHCP Server? (n.d.). Retrieved from www.infoblox.com: https://www.infoblox.com/glossary/dhcp-server/

What is a DNS Server? (n.d.). Retrieved from www.cloudflare.com: https://www.cloudflare.com/learning/dns/what-is-a-dns-server/

WHAT IS SQL INJECTION. (n.d.). Retrieved from www.veracode.com: https://www.veracode.com/security/what-sql-injection

Wilkins, S. (2020, July 10). *Be Aware of These 7 Common Wireless Network Threats*. Retrieved from www.pluralsight.com: https://www.pluralsight.com/blog/it-ops/wireless-lan-security-threats

Επίθεση man-in-the-middle. (n.d.). Retrieved from el.wikipedia.org: https://el.wikipedia.org/wiki/%CE%95%CF%80%CE%AF%CE%B8%CE%B5%CF%83%CE%B7_man-in-the-middle