ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΚΑΙ ΚΡΙΣΙΜΩΝ ΥΠΟΔΟΜΩΝ

ΣΧΕΔΙΟ ΑΣΦΑΛΕΙΑΣ

ΣΥΓΓΡΑΦΕΙΣ:

ΜΑΤΘΑΙΟΥ ΚΩΝΣΤΑΝΤΙΝΑ 3170260

ΝΙΚΟΛΟΥΤΣΟΣ ΚΩΝΣΤΑΝΤΙΝΟΣ 3170122

ΣΙΑΧΑΜΗΣ ΝΙΚΟΣ 3170143

ΕΡΓΑΣΙΑ ΧΕΙΜΕΡΙΝΟΥ ΕΞΑΜΗΝΟΥ 2020-21

Περιεχόμενα

1. ΕΙΣΑΓΩΓΗ

Στόχος της παρούσας εργασίας είναι να γίνει μια ολοκληρωμένη μελέτη ασφάλειας των πληροφοριακών συστημάτων και των κρίσιμων υποδομών της δοσμένης βιομηχανίας, όπου θα αναπτυχθεί ένα σχέδιο ασφάλειας (template) και τρόποι προστασίας για τον έλεγχο των υποδομών, διαδικασιών και λογισμικού του πληροφοριακού συστήματος μιας εταιρείας που εξειδικεύεται σε θέματα τραπεζών για επεξεργασία προσωπικών δεδομένων, αφού πρώτα εντοπιστούν πιθανές απειλές και ευπάθειες. Στο πληροφοριακό σύστημα πρέπει να τηρείται η ακεραιότητα, η εμπιστευτικότητα και η διαθεσιμότητα (C.I.A.).

1.1.Περιγραφή Εργασίας

Στην εργασία καλούμαστε να κάνουμε ανάλυση επικινδυνότητας μιας βιομηχανίας που πραγματεύεται απομακρυσμένες αγοροπωλησίες μέσω του διαδικτύου. Πρώτα, γίνεται αναφορά στη μεθοδολογία μελέτης και στους λόγους που επιλέχτηκε αυτή για την επιχείρηση που μας απασχολεί, αλλά και στα στάδια και βήματα της ανάλυσης και διαχείρισης επικινδυνότητας.Έπειτα, περιγράφονται τα υφιστάμενα πληροφοριακά συστήματα του ξενοδοχείου, που αφορούν στον υλικό εξοπλισμό, στο λογισμικό, στις εφαρμογές, στο δίκτυο, στα δεδομένα και στις διαδικασίες. Εν συνεχεία, γίνεται η αποτίμηση τους με βάση την κρισιμότητά τους για τη βιομηχανία, δηλαδή τις επιπτώσεις που προκύπτουν από τη φθορά τους για το σύστημα και παρουσιάζονται οι απειλές, οι ευπάθειες και τα αποτελέσματα αποτίμησης με τη βοήθεια πίνακα. Στην πορεία, προτείνονται έντεκα κατηγορίες αποτελεσματικών μέτρων ασφάλειας των πληροφοριακών συστημάτων ως τρόποι αντιμετώπισης των απειλών. Τέλος, συνοψίζονται τα πιο κρίσιμα αποτελέσματα με την υψηλότερη επικυνδυνότητα, δίνοντας έμφαση στην αξιολόγηση του impact κάθε αγαθού όσον αφορά την ακεραιότητα, διαθεσιμότητα και εμπιστευτικότητα.

1.2.Δομή παραδοτέου

Στην 1η ενότητα παρουσιάζουμε επιγραμματικά τις ενότητες της εργασίας και τι θα αναλύσουμε κατά την μελέτη μας. Στην 2η ενότητα παρουσιάζεται η μεθοδολογία που ακολουθήσαμε, στην 3η ενότητα περιγράφονται τα κυριότερα στοιχεία από την μελέτη και την ανάλυση επικινδυνότητας που εκπονήθηκε. Εν συνεχεία, στην 4η ενότητα περιγράφουμε τα μέτρα ασφαλείας και στην 5η ενότητα μια εκτεταμένη περιγραφή των πιο κρίσιμων σημείων της ανάλυσης επικινδυνότητας για την βιομηχανία.

2. ΜΕΘΟΔΟΛΟΓΙΑ ΜΕΛΕΤΗΣ ΑΣΦΑΛΕΙΑΣ

Για τη Διαχείριση Επικινδυνότητας της βιομηχανίας ΣΤΕΡΓΙΟΠΟΥΛΟΣ Α.Ε. χρησιμοποιήθηκε παραμετροποιημένη μέθοδος του ISO27001K1. 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.

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 βιομηχανίας ΣΤΕΡΓΙΟΠΟΥΛΟΣ Α.Ε., τα οποία με το πέρας της μελέτης θα επικαιροποιηθούν, αναβαθμιστούν ή σε κάποιες περιπτώσεις αντικατασταθούν.

2.1.1. Υλικός εξοπλισμός (hardware)

- Server
- Switch
- Router
- Printer
- Tablet
- VOIP phone
- Workstation
- Access Point
- Wireless Controller

2.1.2. Λογισμικό και εφαρμογές

Λογισμικό (Software) είναι η συλλογή από προγράμματα υπολογιστών, διαδικασίες και οδηγίες που εκτελούν συγκεκριμένες εργασίες σε ένα υπολογιστικό σύστημα. Στο σύστημά μας συνυπάρχουν διαφόρων ειδών λογισμικά στις διάφορες συσκευές καθώς και στα διάφορα υποδίκτυα. Πιο αναλυτικά υπάρχουν τα ακόλουθα:

- Windows 10 Pro (Στο υποδίκτυο Sales & IT Departments στα workstations PC3 και PC5 καθώς και στο υποδίκτυο Director's Office στο Laptop1)
- Windows 7 (Στο υποδίκτυο Sales & IT Departments στα workstations PC4 και PC6)
- Windows XP (Στο υποδίκτυο Accounting & HR Departments στα workstations PC1 και PC2)
- Cisco proprietary software (Στα switches SW-FLOOR1, SW-FLOOR2, SW-FLOOR3, SW-FLOOR4.1 και SW-FLOOR4.2 των Accounting & HR Departments, Sales & IT Departures, Director's Office και Computer Room αντίστοιχα. Στα routers EDGE-ROUTER, ROUTER1, ROUTER2, ROUTER3 και ROUTER4 του Main Building. Επίσης, στο ACCESS POINT και το WIRELESS-LAN-CONTROLLER1 του Director's Office όπως και στο VOIP-PHONE1 του Sales & IT Departures.)
- FortiGate proprietary software (Στο FIREWALL που υπάρχει στο Main Building)
- Windows Server 2008 (Στους HRM SERVER, CRM SERVER και DOMAIN CONTROLLER/ FILE SERVER που βρίσκονται στο Computer Room)
- Ubuntu 16.04.7 LTS (Στους RADIUS/SNMP SERVER, EMAIL SERVER και APPLICATION SERVER που βρίσκονται στο Computer Room)
- Ubuntu 12.04.5 LTS (Στο DNS/DHCP SERVER που βρίσκονται στο Computer Room)
- Android 9 Pie (API 28) (Στο TABLET-PC1 στο Director's Office)
- Epson proprietary software (Στον PRINTER1 στο Accounting & IT Departures)

2.1.3. Δίκτυο

Δίκτυο είναι ένα σύνολο από δύο ή περισσότερους υπολογιστές που είναι συνδεδεμένοι μεταξύ τους ώστε να μπορούν να ανταλλάσσουν δεδομένα και να μοιράζονται διάφορες συσκευές.

Στο σύστημά μας παρατηρούμε ότι το γενικό δίκτυο χωρίζεται τρία κύρια υποδίκτυα, το Accounting & HR Departures και Sales & IT Departures, το Director's Office και το Computer Room. Υπάρχουν τέσσερις routers για πιο αποδοτική δρομολόγηση μεταξύ των υποδικτύων. Τέλος, υπάρχει ένας router και ένα firewall που συνδέουν το εταιρικό δίκτυο μέσω του παρόχου στο Internet.

2.1.4. Δεδομένα

Πληροφοριακά δεδομένα είναι ένα σύνολο στοιχείων, μία συλλογή που αποτυπώνει τιμές επί αντικειμένων, προσώπων και γεγονότων. Στο σύστημά μας υπάρχουν Industry Customer Data και Industry Employee Data όπου κρατιούνται τα δεδομένα των πελατών και των υπαλλήλων σε βάση δεδομένων.

2.1.5. Διαδικασίες

Διαδικασίες είναι μια σειρά από συγκεκριμένες εκτελούμενες πράξεις από τους ανθρώπους και τα συστήματα με τέτοιο τρόπο ώστε να επιτευχθεί ένα συγκεκριμένο αποτέλεσμα.

Στο σύστημά μας εντοπίζονται οι ακόλουθες διαδικασίες:

- Create New Customer που χρησιμοποιείται από το Sales & IT Departments
- Create New Order (Local) που χρησιμοποιείται από το Sales & IT Departments
- Create New Order (Remotely) που χρησιμοποιείται από τον οποιοδήποτε και του τομέα των πωλήσεων μέσω κάποιου smartphone
- Customer Support που χρησιμοποιείται από το Accounting & HR Departments

3. ΑΠΟΤΙΜΗΣΗ ΠΣ ΚΑΙ ΕΓΚΑΤΑΣΤΑΣΕΩΝ ΒΙΟΜΗΧΑΝΙΑΣ

Κάθε επιχείρηση και κατ' επέκταση κάθε πληροφοριακό σύστημα, απαρτίζεται από μια μεγάλη ποικιλία από αγαθά. Μπορεί ένα φαινομενικά ασήμαντο αγαθό να αποτελέσει την αιτία για μια σοβαρή απειλή για το σύστημά μας και να προκαλέσει σοβαρά προβλήματα σε αυτό. Γι' αυτό τον λόγο είναι σημαντικό να βρούμε και να καταγράψουμε κάθε πιθανό αγαθό.

3.1.Αγαθά που εντοπίστηκαν

Τα αγαθά που εντοπίστηκαν και χρήζουν προστασίας είναι τα εξής :

- **Industry Customer Data:** αφορούν τα προσωπικά δεδομένα όλων των πελατών της βιομηχανίας (π.χ ονοματεπώνυμο, κατοικία,παραγγελίες λογαριασμού κλπ.).
- **Industry Employee Data:** αφορούν τα προσωπικά δεδομένα όλων των εργαζομένων της βιομηχανίας (π.χ ονοματεπώνυμο, κατοικία, διοικητική θέση κ.α.).
- **Windows 10 Pro:** αποτελεί ένα λειτουργικό σύστημα υπολογιστών που κατασκευάστηκε από την Microsoft.
- **Windows 7:** αποτελεί ένα λειτουργικό σύστημα υπολογιστών που κατασκευάστηκε από την Microsoft.
- **Laptop:** φορητός υπολογιστής σχεδιασμένος για τεχνικές ή επιστημονικές εφαρμογές ή ο οποίος περιέχει κάποια στοιχεία της εταιρείας.
- **Tablet:** φορητή συσκευή σχεδιασμένη για τεχνικές ή επιστημονικές εφαρμογές σε συνεργασία με σταθερό υπολογιστή.
- **Workstation:** είναι ειδικός σταθερός υπολογιστής σχεδιασμένος για τεχνικές ή επιστημονικές εφαρμογές.
- **CRM server:** σύστημα διαχείρισης και ανάλυσης στοιχείων προερχόμενα από την εμπορική κινητικότητα και αλληλεπίδραση με τους πελάτες.
- **HRM server:** σύστημα σχεδιασμένο για την αυτοματοποίηση των διαδικασιών που αφορούν το τμήμα ανθρώπινου δυναμικού π.χ πληρωμές κ.ο.κ.
- **RADIUS/SNMP server:** συσκευή δικτύου που χρησιμοποιείται για την εξακρίβωση/ αυθεντικοποίηση των χρηστών.
- **Email server:** αφοσιώνεται στο να δέχεται και να προωθεί μηνύματα ηλεκτρονικού ταχυδρομείου.
- **DNS/DHCP server:** χρησιμοποιούνται για να αντιστοιχίσουν domain στην ip διεύθυνση και ip διεύθυνση στο δίκτυο.
- **Application server:** λαμβάνει τα http request και αλληλεπιδρά με τον CRM αυτοματοποιώντας διεργασίες απομακρυσμένων πωλήσεων (remote sales).
- **Domain Controller/File server:** χρησιμοποιείται για την εξακρίβωση των χρηστών του δικτύου και την φύλαξη δεδομένου μεγάλης αξίας.
- **Router:** Είναι μια συσκευή δικτύωσης η οποία συνδέει την συσκευή με την οποία ενώνεται στο διαδίκτυο.
- **Edge-Router:** Είναι μια συσκευή δικτύωσης η οποία συνδέει το εσωτερικό δίκτυο της βιομηχανίας με τον έξω κόσμο,δηλαδή το διαδίκτυο.
- **VOIP phone:** Είναι μία τεχνολογία που μετατρέπει την φωνή του χρήστη σε ψηφιακό σήμα και του επιτρέπει να κάνει "τηλεφωνήματα" μέσω υπολογιστή και χρησιμοποιείται από το τμήμα υποστήριξης και επικοινωνίας πελατών.
- **Wireless-Lan-controller:** διαχειρίζεται τις ασύρματες συνδέσεις και επιτρέπει σε φορητές συσκευές να συνδεθούν στο δίκτυο.
- **Printer:** Είναι η συσκευή η οποία μετατρέπει τις πληροφορίες του συστήματος σε έντυπη μορφή.

- **Switch:** Είναι υλικό δικτύωσης που συνδέει συσκευές σε ένα δίκτυο.
- Access point:
- **Create New Customer:** δημιουργία νέου λογαριασμού για έναν πελάτη της βιομηχανίας
- **Create New Order (Local):** δημιουργία νέας παραγγελίας πελάτη τοπικά,δηλαδή μέσω υπαλλήλου του καταστήματος.
- **Create New Order (Remotely):** δημιουργία νέας παραγγελίας πελάτη απομακρυσμένα,δηλαδή ο ίδιος ο πελάτης συμπληρώνει την φόρμα και παραθέτει την παραγγελία μέσω προσωπικής συσκευής.
- **Customer Support:** τεχνική υποστήριξη στους πελάτες από τους υπαλλήλους της βιομηχανίας

3.2.Απειλές που εντοπίστηκαν

ASSETS	THREATS
Edge Router	1. Edge router can be easily shut down on flood attacks 2. Access to the network of unauthorized user
Domain Controller/File server	1. Excessive Privilege Abuse 2. server fails
Application server	1. SQL Injection.Cross Site Scripting. 2. Man In The Middle attack 3. Unauthorized user will get access to server via SSH (bruteforce)
Industry Customer Data	1. Password can be easily decrypted 2. Loss of data
Industry Employee Data	Employee spies on other employee's data
Router	Unauthorized access to router gateway configuration
Windows 7	Remote malware attack
Create New Customer	1. Fraud 2. unauthorized access by third person to account
Windows 10 Pro	1. Remote code execution 2. Employees are able to see other employee's data

Email server	1. Unauthorized access to your emails and data leakage. 2. SPAM Bombard
Create New Order(Remotely)	Customer unaware of extra invalid charges
VOIP Phone	1. Remote eavesdropping (lead to communication and security breaches) 2. VOIP station SPAM
CRM server	Unauthorized access to automated sales processes or data
Customer Support	Spam bombarding
RADIUS/SNMP server	Allow an unauthenticated, remote attacker to be authorized as a subscriber
HRM server	Unauthorized access to HR data and actions
Workstation	1. Unauthorized physical access 2. USB malware code execution (USB Rubber ducky)
Access point	Unauthorized hosts use your network
DNS/DHCP server	TCP SYN Flood Attacks
Wireless-Lan-Controller	Unauthenticated, remote attacker to cause a denial of service (DoS overflow)
Switch	Technical failures
Printer	Unauthorized access to printer
Laptop	Easy to be stolen
Tablet	SIM Hijacking
Create New Order(Local)	Ongoing data is lost

3.3.Ευπάθειες που εντοπίστηκαν

ASSETS	VULNERABILITY
Edge Router	Poor performance of product
Domain Controller/File server	1. Rules not appropriately configured 2. No backup server
Application server	1. No access control policy (e.g .htaccess for Apache) 2. Not encrypting traffic with https (TLS) 3. Not using ssh keys for connecting
Industry Customer Data	1. Deprecated password hash 2. Not having backup files
Industry Employee Data	Database not encrypted
Router	Not changing default credentials for router interface gateway
Windows 7	Microsoft stop releasing updates
Create New Customer	1. Inadequate authentication measures 2. Weak password
Windows 10 Pro	2. Bad Windows firewall configuration 3. Bad active directory configuration
Email server	1. No spam filtering 2. Email traffic is not encrypted. And rules not appropriately configured. And weak email passwords
Create New Order(Remotely)	Inadequate order confirmation policy
VOIP Phone	1. Unencrypted connections 2. Not having black-list
CRM server	Deprecated version of software
Customer Support	No spam restriction measures
RADIUS/SNMP server	Incorrect RADIUS user credential validation
HRM server	Deprecated version of software
Workstation	1. USB port 2. Weak password
Access point	Weak passwords
DNS/DHCP server	Inadequate firewalls rules (iptables)

Wireless-Lan-Controller	Insufficient validation of CAPWAP packets
Switch	Cheap material protection
Printer	Allow connection to outside of work computers
Laptop	Portability and high cost
Tablet	Old SIM version
Create New Order(Local)	No network and no caching orders

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	Παρόχου Υπηρεσιών	Εξωτερικούς	Επανάληψη μηνυμάτων	Αποποίηση αποστολέα	Αποποίηση παραλήπτη	Άρνηση αποστολής ή παραλαβής	Παρεμβολή λανθασμένων μηνυμάτων	Λανθασμένη δρομολόγηση	Παρακολούθηση κίνησης	Μη παράδοση	Απώλεια ακολουθίας μηνυμάτων
Windows 10 pro	3	3	5	5	5	6	6	7	5	7	3	7	2	4	7	2				4	5	8	4	5
Windows 7	3	3	5	5	5	6	6	7	5	7	3	7	2	4	7	2				4	5	8	4	5
Laptop1	3	4	5	5	6	6	7	7	6	8	6	8	5	4	9	4				3	5	8	3	5
PC1	3	4	5	5	6	6	7	8	5	8	6	8	5	4	9	4				3	5	8	3	5
PC2	3	4	5	5	6	6	7	8	5	8	6	8	5	4	9	4				3	5	8	3	5
PC3	3	4	5	6	7	7	8	8	6	8	6	8	5	4	9	4				4	6	8	4	5
PC4	3	4	5	6	7	7	8	8	6	8	6	8	5	4	9	4				4	6	8	4	5
PC5	3	4	5	6	7	7	8	8	6	8	6	8	5	4	9	4				4	6	8	4	5
PC6	3	4	5	6	7	7	8	8	6	8	6	8	5	4	9	4				4	6	8	4	5
Tablet- PC1	2	3	3	3	4	4	5	6	4	5	3	5	2	4	6	2				2	4	6	3	4
Printer1	2	3	4	4	5	5	5	5	5	7	3	5	2	4	7	2	2	1		2	5	7	3	2
Router1	6	7	8	8	9	9	9	9	7	7	5	7	3	5	8	5	4	4	2	6	9	9	6	3
Router2	6	7	8	8	9	9	9	9	7	6	5	6	3	5	7	4	4	4	2	5	8	8	5	3

Router3	4	5	6	7	8	8	8	9	6	6	4	6	3	5	7	4	4	4	2	5	8	8	5	3
Router4	6	8	9	9	9	9	9	9	7	7	5	6	3	6	8	5	4	4	2	6	9	9	6	3
Edge-Router	6	7	8	8	9	10	10	10	8	7	5	7	3	5	9	5	4	4	2	6	10	10	6	3
Wireless-Lan-Controller1	2	3	4	4	5	5	5	6	4	5	3	5	2	3	5	4	4	4	2	3	5	6	4	3
VoIP-Phone1	4	5	6	6	7	7	7	8	6	7	4	6	2	4	6	6	4	4	2	6	7	8	5	5
CRM Server	3	4	5	5	6	6	7	8	5	7	4	6	2	4	6	2			2	4	6	8	4	4
RADIUS / SNMP Server	3	4	5	6	6	7	7	8	5	7	5	7	2	4	7	3			2	4	6	8	4	4
Email Server	2	3	4	5	6	6	7	8	5	8	4	6	3	5	8	2			3	5	7	8	6	6
DNS / DHCP Server	2	3	5	6	7	7	7	8	5	7	6	8	2	4	6	3			2	5	7	8	6	6
HRM Server	2	3	3	4	5	5	5	6	4	6	4	6	2	4	6	2			2	4	5	7	4	4
Application Server	3	5	6	7	8	8	9	9	6	7	6	8	2	5	7	3			3	5	8	9	4	6
Domain Controller / File Server	4	5	6	8	9	9	9	10	8	8	7	10	3	5	8	3			3	5	8	10	6	6
SW-Floor1	4	5	5	6	7	7	8	8	6	6	3	6	2	4	6	3			3	4	6	7	5	3
SW-Floor2	5	6	6	7	7	8	8	9	7	6	3	6	2	4	7	4			3	4	7	8	5	3
SW-Floor3	4	5	5	6	7	7	8	8	6	6	3	6	2	4	6	3			3	4	6	7	5	3
SW-Floor4.1	6	7	8	9	9	9	9	9	7	6	3	6	2	4	7	5			3	4	7	9	5	3

SW-Floor4.2	4	5	6	7	8	8	9	9	6	6	4	6	2	4	7	4			3	4	7	8	5	3
Access Point	2	3	4	4	5	5	5	6	4	5	3	5	2	3	5	3			3	3	5	5	4	2
Industry Customer Data	3	4	5	6	7	7	8	8	5	8	5	8	4	6	8							8		5
Industry Employee Data	2	3	4	6	6	7	7	8	4	7	5	7	2	5	8							8		5
Create New Customer	3	3	4	6	8	9	9	9	6	8	3	6	2	4	6									
Create New Order (Local)	3	3	4	6	7	8	8	8	5	7	3	6	1	4	7									
Create New Order (Remotely)	3	4	5	6	7	8	8	8	5	7	3	6	1	4	7									
Customer Support	4	5	5	6	7	7	7	7	4	6	3	7	1	4	7									

4. 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 του/της **ΣΤΕΡΓΙΟΠΟΥΛΟΣ Α.Ε**.

4.1.Προσωπικό – Προστασία Διαδικασιών Προσωπικού

ASSETS	Preventive controls
Windows 7 & 10 pro	Agents should not download from unknown sources
Workstation	Agents should not plug in unknown USBs
Industry Employee Data	Internal Employee Rules and Procedures available
Workstation	Change password frequently and use strong passwords

4.2.Ταυτοποίηση και αυθεντικοποίηση

ASSETS	Preventive controls
Email Server	Strong passwords or 2-factor authentication, restrict ip (allow only work VPN connections),
Access point	Use strong Wifi password to avoid packet sniffing from unauthorized users.
Create new customer	Add authentication methods such as phone, email verification
Create New Order (Remotely)	Authenticate order with OTP (one-time password)

4.3.Έλεγχος προσπέλασης και χρήσης πόρων

ASSETS	Preventive controls
Domain Controller / File Server	Strict and grant database access base on the user roles requirements
Printer	Control usage based on priority of employees
Windows 10 pro	Enable windows active directories and harness their power

4.4.Διαχείριση εμπιστευτικών δεδομένων

ASSETS	Preventive controls
Industry Customer Data	Avoid losing data by using cloud storage (google drive, dropbox, amazon)
Create New Order (Local)	When Network is down save orders data locally and upload when network is restored
Domain Controller / File Server	Use of Clustering servers (Kubernetes, Docker, Ansible) to make sure at least 1 file server/domain controller is always online

4.5.Προστασία από τη χρήση υπηρεσιών από τρίτους

ASSETS	Preventive controls
Application Server	Use certificate from trusted CA for using TLS protocol (Google, Sertico, Comondo)
Industry Customer Data	Avoid using deprecated hashes for passwords like md5!

4.6.Προστασία λογισμικού

ASSETS	Preventive controls
Application Server	Always update software version to the latest if possible
HRM Server	Bump software version to latest
RADIUS/SNMP Server	Don't use deprecated version (This is what cisco advises)

4.7.Διαχείριση ασφάλειας δικτύου

ASSETS	Preventive controls
Edge-Router	Mandatory Access Control
Router	Change default gateway credentials. And change them with stronger password
Edge-Router	Avoid dos attacks by banning IPs that shows malicious behaviour. (firewall)
Wireless Lan Controller	Update to latest version (cisco's solution) to fix known vulnerabilities

4.8.Προστασία από ιομορφικό λογισμικό

ASSETS	Preventive controls
Application Server	Sanitizing input fields to avoid SQL, XSS attacks. Install antivirus to remove malwares (malwarebytes)
Windows 7 & 10 pro	Enable windows firewall and install trusted antivirus
Email Server	Use ML algorithms to detect emails with harmful content (Gmail filtering).

4.9.Ασφαλής χρήση διαδικτυακών υπηρεσιών

ASSETS	Preventive controls
DNS/DHCP Server	Have a fallback server, or use 8.8.8.8 which is google DNS
Tablet	Buy SIM card from trusted providers to avoid getting hijacked
VOIP-phone	Use NAT to speak behind it. Use symmetric key encryption RSA and secure websockets to avoid Man In The Middle Attacks
VOIP-phone	Add a spam filter to avoid telephone line congestion. Which means agents will not be able to work properly.
Customer Support	Filtering customer support tasks by adding spam filters.

4.10.Ασφάλεια εξοπλισμού

ASSETS	Preventive controls
Switch	Material protection of switcher

4.11.Φυσική ασφάλεια κτιριακής εγκατάστασης

ASSETS	Preventive controls
Laptop	Security guards and alarms in the building and have insurance for laptops
Workstation	Use air conditioner to avoid system overheat and possible hardware damages

5. ΣΥΝΟΨΗ ΠΙΟ ΚΡΙΣΙΜΩΝ ΑΠΟΤΕΛΕΣΜΑΤΩΝ

Με βάση τα στοιχεία που παρουσιάζονται στο risk assessment spreadsheet το 5% των ευρημάτων περιορίζεται στα εξής τρία πιο κρίσιμα αποτελέσματα:

1. **Edge Router :**

   Είναι ζωτικής σημασίας πόρος καθώς σχετίζεται σε μεγάλο βαθμό,ίσως τον μεγαλύτερο από κάθε άλλο πόρο του συστήματος, με την διασύνδεση της βιομηχανίας με τον έξω κόσμο δηλαδή με το διαδίκτυο. Οι πωλήσεις εξ' αποστάσεως μέσω διαδικτύου αποτελούν μεγάλο ποσοστό των κερδών της βιομηχανίας και έτσι μια επίθεση πλημμύρας στον πόρο αυτό θα πάγωνε όχι μόνο την δημιουργία παραγγελιών από την πλευρά των πελατών αλλά και κάθε παραγωγική διαδικασία εντός της βιομηχανίας αφού πλέον κάθε παραγωγή σχετίζεται με το διαδίκτυο (λογιστικά,παραλαβή πρώτης ύλης κτλ). Δεδομένου αυτού χρήζει μεγάλης προσοχής η απόκτηση σύγχρονου και καλής ποιότητας εξοπλισμού όπου θα μπορεί να ανταπεξέρχεται σε μεγάλο φόρτο εργασίας και δεν θα κινδυνεύει η βιομηχανία να αποκοπεί. Επιπλέον σημαντική ευπάθεια αποτελεί και η έλλειψη ολοκληρωμένης ταυτοποίησης παραλήπτη πακέτων που διέρχονται από τον πόρο. Υπάρχει ο κίνδυνος, έτσι να αποκτήσουν πρόσβαση σε σημαντικά δεδομένα μη εξουσιοδοτημένοι χρήστες στα δεδομένα του συστήματος. Εάν συμβεί αυτό, τότε μπορεί να γίνει υποκλοπή εμπιστευτικών δεδομένων και να καταλήξουν σε άτομα που δεν πρέπει. Για να ξεφύγουμε από τέτοιες επιθέσεις, μπορούμε να χρησιμοποιήσουμε κατάλληλα μέτρα όπως το mandatory access control όπου περιορίζει τις δυνατότητες-δικαιώματα των χρηστών με βάση την πολιτική που έχει ορίσει ο βασικός διαχειριστής.

2. **Domain Controller/File server:**

   Είναι από τα σημαντικότερα κομμάτια της βιομηχανίας καθώς περιέχει τα ηλεκτρονικά αρχεία και δεδομένα της εταιρείας. Ο File server εχει ενα δικό του σύστημα αποθήκευσης και χρησιμοποιείτε ως storage για τους clients του.

   Από την άλλη, ο Domain Controller ταυτοποιεί τους χρήστες και έτσι διαθέτει σε αυτούς τα δεδομένα που τους αντιστοιχούν με τα βάση τα δικαιώματά τους(active directories).

- Η διαθεσιμότητα των δεδομένων είναι σημαντική για κάθε εταιρεία. Γι' αυτόν τον λόγο επινοήθηκαν τα **cluster server** τα οποία αποτελούν τόσο εφεδρικούς server σε περίπτωση που απενεργοποιηθεί κάποιος όσο και λύση για καλύτερο διαμοιρασμό του φόρτου γνωστό και ώς load balancing. Έτσι λοιπόν μειώνουμε δραστικά τις πιθανότητες για την προσωρινή, αλλά και μερικές φορές την μόνιμη, απώλεια δεδομένων.
- Είναι πολύ σημαντικό να ρυθμίσουμε τους κανονισμούς του fileserver σε ευαίσθητα δεδομένα ετσι ώστε να αποφύγουμε πιθανές προσπελάσεις σε αυτά από μη-εξουσιοδοτημένους χρήστες.

3. Application server:

Ο Application Server έχει την σημαντική δουλειά να παρέχει στους clients πρόσβαση στο business logic,δηλαδή την στρατηγική και πολιτική διαχείριση της πληροφορίας της εταιρείας(π.χ το Tomcat).

Ο Application server αποτελεί πολύτιμο αγαθό κάθε εταιρείας γιαυτο θα πρέπει να προστατευτεί τόσο από γνωστές επιθέσεις όπως SQL injection, XSS scripting οσο και απο πιο προχωρημένες επιθέσεις όπως man in the middle και exploitation απο security misconfigurations.

- Για να αποφύγουμε επιθέσεις όπως το SQL injection αρκεί ο software engineer να κάνει input sanitization τόσο στο Frontend οσο και το Backend. Με αυτο τον τρόπο το sql injection string θά γίνεται encoded και δεν θα εκτελείται από το server.
- Από την άλλη, η αποφυγή του XSS scripting μπορεί να έχει λυθεί σε μεγάλο βαθμό από τους σημερινούς browsers. Ωστόσο, θα πρέπει η ομάδα υλοποίησης του λογισμικού να κάνει πάλι input sanitization ώστε να αποφύγει άσχημα περιστατικά όπως υποκλοπή δεδομένων.
- Επιπρόσθετα θα πρέπει να ενισχυθεί το επίπεδο αυθεντικοποίησης των πελατών (application, web server κ.α) καθώς και ασφαλούς μεταφοράς δεδομένων σε αυτούς. Για το πρώτο, αρκεί να χρησιμοποιηθούν γνωστές τακτικες όπως JWT καθώς και ssh keys τα όποια θα χρειάζονται κάθε φορά που χρειάζεται να γίνει σύνδεση με protocol ssh στον σερβερ. Για το δεύτερο, αρκεί να εγκατασταθεί ενα certificate απο trusted CA (Δωρεάν με FreeSSL) το οποίο απαιτείται για να γίνει η σύνδεση https και να χρησιμοποιείτε το TLS protocol. Έτσι λοιπόν θα είναι σχεδόν αδύνατο για οποιονδήποτε man in the middle να αναγνωρίσει τα δεδομένα.

6. ΒΙΒΛΙΟΓΡΑΦΙΑ

- https://www.infoblox.com/wp-content/uploads/2016/04/infoblox-whitepaper-top5-dns-security-attack-risks-how-to-avoid-them_0.pdf
- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180207-cps#:~:text=A%20vulnerability%20in%20the%20RADIUS,incorrect%20RADIUS%20user%20credential%20validation
- https://github.com/JBalanza/USBBlocker
- https://www.softwaretestinghelp.com/default-router-username-and-password-list/#:~:text=%231)%20The%20default%20username%20and,the%20maker%20of%20the%20router
- https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wlc-capwap-dos-Y2sD9uEw#:~:text=A%20vulnerability%20in%20the%20Control,condition%20on%20an%20affected%20device
- https://www.pandasecurity.com/en/mediacenter/security/sim-hijacking-explained/