ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ ΚΑΙ ΚΡΙΣΙΜΩΝ ΥΠΟΔΟΜΩΝ

ΣΧΕΔΙΟ ΑΣΦΑΛΕΙΑΣ

ΣΥΓΓΡΑΦΕΙΣ:

Θεμελίνα Κουζούμπαση, 3170076

Κωνσταντίνα Σουβατζιδάκη, 3170149

Φοίβος Χαραλαμπάκος, 3170175

ΕΡΓΑΣΙΑ ΧΕΙΜΕΡΙΝΟΥ ΕΞΑΜΗΝΟΥ 2020-21

Contents

1. ΕΙΣΑΓΩΓΗ

Το παρόν έγγραφο είναι ένα **σχέδιο ασφάλειας** που δημιουργήθηκε στα πλαίσια της εξαμηνιαίας εργασίας του μαθήματος **Ασφάλεια Πληροφοριακών Συστημάτων**, το οποίο αφορά το Πληροφοριακό Σύστημα μιας **Βιομηχανίας** για την αποτελεσματική καταγραφή και εξυπηρέτηση των πελατών της.

1.1. Περιγραφή Εργασίας

Το **σχέδιο ασφάλειας** είναι το έγγραφο που προκύπτει από **την Ανάλυση Επικινδυνότητας**. Συγκεκριμένα στην παρούσα εργασία, με δεδομένη τη λίστα αγαθών της εταιρείας, πραγματοποιείται εντοπισμός των πιθανών απειλών και ευπαθειών, καθώς και αποτίμηση των επιπτώσεων για κάθε ένα από αυτά. Επιπρόσθετα, προτείνονται μέτρα προστασίας, χωρισμένα σε κατηγορίες ως προς την φύση τους. Τέλος, συνοψίζονται τα πιο κρίσιμα αποτελέσματα που προκύπτουν από την ανάλυση επικινδυνότητας, δηλαδή τα αγαθά που έχουν σοβαρότερο ρόλο στην ασφάλεια της Βιομηχανίας.

1.2. Δομή παραδοτέου

Το παρόν έγγραφο χωρίζεται σε ενότητες ως εξής: Σε πρώτη φάση, **στην Ενότητα 2**, περιγράφονται όλα τα αγαθά του συστήματος αναλυτικά και κατηγοριοποιούνται σε αγαθά υλικού, λογισμικού, δεδομένων και σε διαδικασίες. Ύστερα, **η Ενότητα 3**, ξεκινά με μια ταξινόμηση των αγαθών ως προς την κρισιμότητά τους για την ασφάλεια της εταιρίας, και στην συνέχεια παρουσιάζονται αναλυτικά οι απειλές, οι ευπάθειες και οι επιπτώσεις που αντιστοιχούν στο κάθε ένα από αυτά. Ακόμα, δίνεται ένας πίνακας με την αξιολόγηση των επιπτώσεων που φέρει κάθε αγαθό στην διαθεσιμότητα, την εμπιστευτικότητα και την ακεραιότητα του Πληροφοριακού Συστήματος. Έπειτα, **στην Ενότητα 4**, παρουσιάζονται τα προτεινόμενα μέτρα προστασίας για την βελτιστοποίηση της ασφάλειας των αγαθών της Βιομηχανίας. Σε τελική φάση, **στην Ενότητα 5**, δίνονται τα κρισιμότερα αποτελέσματα που προκύπτουν από το παρόν έγγραφο, δηλαδή τα 4 αγαθά που θεωρείται πως έχουν μεγαλύτερη επίδραση στο εάν το σύστημα θα είναι ασφαλές ή όχι, με μια σύντομη αιτιολόγηση.

2. ΜΕΘΟΔΟΛΟΓΙΑ ΜΕΛΕΤΗΣ ΑΣΦΑΛΕΙΑΣ

Για τη Διαχείριση Επικινδυνότητας της Βιομηχανίας 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 α-σφάλειας 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 Βιομηχανίας, τα οποία με το πέρας της μελέτης θα επικαιροποιηθούν, αναβαθμιστούν ή σε κάποιες περιπτώσεις αντικατασταθούν.

2.1.1. Υλικός εξοπλισμός (hardware)

Πρόκειται για όλες τις συσκευές υλικού, δηλαδή τις φυσικές συσκευές που χρησιμοποιούνται από τον οργανισμό, όπως οι υπολογιστές, οι servers,τα laptops,το υλικό δικτύου, κ.α. Δίνεται ένας πίνακας με όλα τα αγαθά υλικού εξοπλισμού:

Inventory ID	Όνομα	Περιγραφή
CI-A-1008	Laptop	Φορητός υπολογιστής στο γραφείο του διευθυντή που βρίσκεται συνδεδεμένος στο υπό-δίκτυο ασύρματα.
CI-A-1010	CRM Server	Εξυπηρετητής υπεύθυνος για την αλληλεπίδραση μεταξύ πελατών και βιομηχανίας, διαχειρίζεται τις πωλήσεις που πραγματοποιούνται τοπικά. Βρίσκεται στον όροφο με τους servers (Computer room).
CI-A-1011	RADIUS/SNMP Server	Εξυπηρετητής που αναλαμβάνει τον έλεγχο των χρηστών του δικτύου. Παρέχει έλεγχο ταυτότητας, εξουσιοδότηση και υπηρεσίες παρακολούθησης χρηστών. Βρίσκεται στον όροφο με τους servers (Computer room).
CI-A-1012 CI-A-1015 CI-A-1026 CI-A-1028	Router 1-4	Συσκευές που συνδέουν τα διαφορετικά VLANs του δικτύου μεταξύ τους. Καθορίζουν την κατάλληλη διαδρομή που πρέπει να ακολουθεί κάθε πακέτο ανάλογα με τις διευθύνσεις πηγής και προορισμού, ώστε αυτό να μεταδοθεί σωστά. Βρίσκονται στο κεντρικό κτήριο της εταιρίας. Ένα από αυτά συνδέεται με το firewall.
CI-A-1022	Edge Router	Ο κεντρικός δρομολογητής της εταιρίας που συνδέει το τοπικό της δίκτυο με το Internet. Αναλαμβάνει την μετάδοση των πακέτων από το εξωτερικό δίκτυο στο εσωτερικό, και συνδέεται μέσω του firewall με το 1ο εσωτερικό router.

CI-A-1013	VoIP Phone	Συσκευή μετάδοσης φωνής μέσω του Internet. Χρησιμοποιείται για δημιουργία κλήσεων στο Διαδίκτυο και βρίσκεται στο τμήμα Sales & IT της βιομηχανίας.
CI-A-1016	WLAN Controller	Ελεγκτής του ασύρματου τοπικού δικτύου, αναλαμβάνει την διαχείριση των σημείων πρόσβαση, και επιτρέπει ή αποτρέπει ασύρματες συσκευές από το να συνδεθούν σε αυτό. Βρίσκεται στο γραφείο του Διευθυντή.
CI-A-1017	Tablet PC	Φορητή συσκευή - ταμπλέτα στο γραφείο του Διευθυντή. Πιθανότατα χρησιμοποιείται ως προσωπική συσκευή του Διευθυντή για επικοινωνία με συναδέλφους ή και άτομα εκτός του εργασιακού του περιβάλλοντος.
CI-A-1018	Email Server	Εξυπηρετητής που διαχειρίζεται την ανταλλαγή email μεταξύ των χρηστών του δικτύου της εταιρίας με το Διαδίκτυο. Βρίσκεται στον όροφο με τους servers (Computer room).
CI-A-1021	Printer	Συσκευή που χρησιμοποιείται από τους υπαλλήλους του Λογιστηρίου για εκτύπωση εγγράφων. Συνδέεται μέσω δικτύου με τους υπολογιστές του συγκεκριμένου VLAN.
CI-A-1023	DNS/DHCP Server	Εξυπηρετητής που αναλαμβάνει την απόδοση διευθύνσεων IP στις συσκευές του δικτύου, την απόδοση ονομάτων, και την αποστολή των απαραίτητων πληροφοριών στις συσκευές ώστε να μπορούν να επικοινωνούν μεταξύ τους. Βρίσκεται στον όροφο με τους servers (Computer room).
CI-A-1024	HRM Server	Εξυπηρετητής που προσφέρει ολοκληρωμένη παρακολούθηση όλου του εργασιακού κύκλου, όπως προσέλκυση νέων υπαλλήλων και ταχεία ένταξη αυτών στην παραγωγική διαδικασία. Βρίσκεται στον όροφο με τους servers (Computer room).
CI-A-1025 CI-A-1027 CI-A-1034 CI-A-1036 CI-A-1037	Switch 1-5	Συνδέουν μεταξύ τους τις διαφορετικές συσκευές εντός ενός VLAN και αναλαμβάνουν την μεταγωγή των πακέτων ανάμεσα σε αυτές. Βρίσκονται από ένα στο Λογιστήριο, το τμήμα πωλήσεων και το γραφείο του Διευθυντή, καθώς και 2 ακόμα στον όροφο με τους servers.
CI-A-1029	Application Server	Εξυπηρετητής που διαχειρίζεται τις αλληλεπιδράσεις της βιομηχανίας με τους πελάτες αυτοματοποιώντας την διεργασία των απομακρυσμένων πωλήσεων, λαμβάνοντας HTTP αιτήματα των πελατών και αλληλοεπιδρώντας με τον CRM server. Βρίσκεται στον όροφο με τους servers (Computer room).
CI-A-1033	Domain Controller – File Server	Εξυπηρετητής που παρέχει έλεγχο ταυτότητας στους χρήστες ενός τομέα καθώς και τα δικαιώματα που έχουν για πρόσβαση σε αρχεία, φακέλους, πόρους κτλ. Επιπλέον αποτελεί κεντρική αποθήκη δεδομένων και αρχείων. Βρίσκεται στον όροφο με τους servers (Computer room).
CI-A-1035	Access Point	Συσκευή η οποία επιτρέπει σε ασύρματες συσκευές να συνδεθούν στο ενσύρματο δίκτυο. Βρίσκεται στο γραφείο του Διευθυντή.
CI-A-1031 CI-A-1032	PC 1-2 (Accounting & HR)	Ειδικοί υπολογιστές σχεδιασμένοι για τεχνικές ή επιστημονικές εφαρμογές. Χρησιμοποιούνται από τους υπαλλήλους του Λογιστηρίου και εκτελούν την διεργασία εξυπηρέτησης πελατών.
CI-A-1009 CI-A-1019 CI-A-1020 CI-A-1030	PC 3-6 (Sales & IT)	Όμοιοι με τους παραπάνω, όμως χρησιμοποιούνται από τους υπαλλήλους του τμήματος Πωλήσεων και εκτελούν τις διεργασίες δημιουργίας πελατών και παραγγελιών τοπικά.

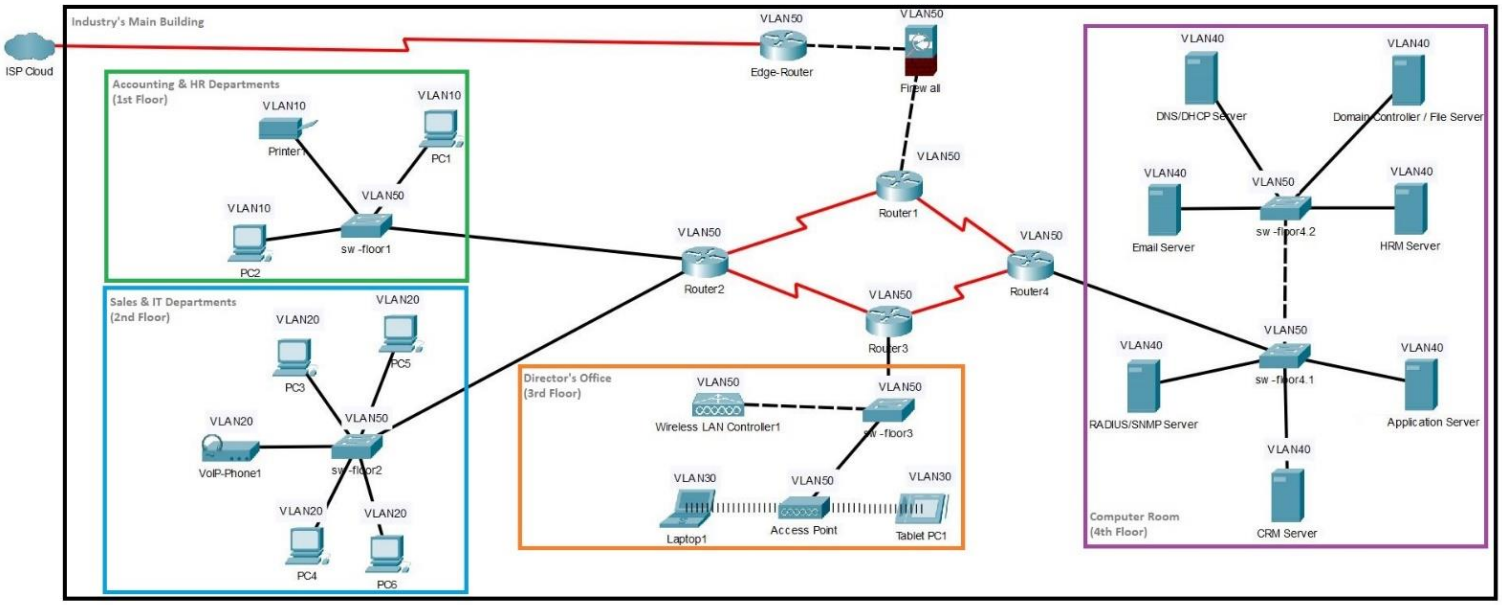
2.1.2. Λογισμικό και εφαρμογές

Πρόκειται για τα λειτουργικά συστήματα που τρέχουν στα workstations του οργανισμού:

Inventory ID	Όνομα	Περιγραφή
CI-A-1006	Windows 10 Pro	Η νεότερη και δημοφιλέστερη έκδοση των Microsoft Windows
CI-A-1007	Windows 7	Πρόγονος των Windows 10, επίσης δημοφιλές λειτουργικό σύστημα.

2.1.3. Δίκτυο

Στην ακόλουθη εικόνα φαίνεται η τοπολογία του δικτύου του οργανισμού, το οποίο χωρίζεται σε 4 διαφορετικά VLANS, που επικοινωνούν μεταξύ τους μέσω 4 κεντρικών δρομολογητών. Όλο το δίκτυο συνδέεται με το Διαδίκτυο μέσω του edge router.



2.1.4. Δεδομένα

Πρόκειται για τα δεδομένα τα οποία αποθηκεύει η εταιρία σε βάση δεδομένων εντός των server της.

Inventory ID	Όνομα	Περιγραφή
CI-A-1000	Industry Customer Data	Τα δεδομένα των πελατών της εταιρίας, βρίσκονται αποθηκευμένα σε Database Server.
CI-A-1001	Industry Employee Data	Τα δεδομένα των υπαλλήλων της εταιρίας, βρίσκονται αποθηκευμένα σε Database Server.

2.1.5. Διαδικασίες

Οι ακόλουθες είναι οι βασικές επιχειρησιακές διεργασίες της Βιομηχανίας, οι οποίες πραγματοποιούνται από τους υπαλλήλους της σε κάποια από τα μηχανήματα υλικού της.

Inventory ID	Όνομα	Περιγραφή
CI-A-1002	Create New Customer	Η διαδικασία δημιουργίας ενός νέου πελάτη για την εταιρία. Λαμβάνει χώρα στους υπολογιστές του τμήματος Sales & IT, και ότι αλληλοεπιδράει με τα δεδομένα των πελατών της εταιρίας που υπάρχουν σε βάση δεδομένων.
CI-A-1003	Create New Order(Local)	Η διαδικασία δημιουργίας μιας νέας παραγγελίας ενός πελάτη τοπικά, λαμβάνει χώρα στους υπολογιστές του τμήματος Sales & IT, και διεκπεραιώνεται από τον CRM server.
CI-A-1004	Create New Order(Remotely)	Η διαδικασία δημιουργίας μιας νέας παραγγελίας ενός πελάτη εξ αποστάσεως. Οι remote παραγγελίες πελατών στέλνονται στον Application server, ο οποίος τις επεξεργάζεται αλληλοεπιδρώντας με τον CRM server.
CI-A-1005	Customer Support	Η διαδικασία εξυπηρέτησης πελατών, λαμβάνει χώρα στους υπολογιστές του τμήματος Accounting & HR.

3. ΑΠΟΤΙΜΗΣΗ ΠΣ ΚΑΙ ΕΓΚΑΤΑΣΤΑΣΕΩΝ ΒΙΟΜΗΧΑΝΙΑΣ

Σε αυτή την ενότητα παρουσιάζονται τα πιο κρίσιμα από τα **αγαθά** της Βιομηχανίας, τα οποία κρίνεται πως έχουν ορισμένες **ευπάθειες** τις οποίες μπορούν να εκμεταλλευτούν **απειλές**, με αποτέλεσμα να προκληθούν σοβαρές **επιπτώσεις** στην ασφάλεια.

3.1. Αγαθά που εντοπίστηκαν

Τα ακόλουθα είναι τα αγαθά της Βιομηχανίας, με φθίνουσα σειρά ως προς την κρισιμότητα τους για την ασφάλεια. Στην αξιολόγηση ενός αγαθού ως πιο κρίσιμο συνυπολογίζονται η σοβαρότητα των επιπτώσεων τους, καθώς και η πιθανότητα να εμφανιστούν οι απειλές που τα αφορούν, όπως φαίνεται και στο έγγραφο ***«ISO27k FMEA – Risk Assessment Spreadsheet 2020.xls"***

	Inventory ID	Όνομα		Inventory ID	Όνομα
1	CI-A-1029	Application Server	15	CI-A-1007	Windows 7
2	CI-A-1009 CI-A-1019 CI-A-1020 CI-A-1030	PC 3-6 (Sales & IT)	16	CI-A-1012 CI-A-1015 CI-A-1026 CI-A-1028	Router 1-4
3	CI-A-1031 CI-A-1032	PC 1-2 (Accounting & HR)	17	CI-A-1025 CI-A-1027	Switch4.1,4.2 (Computer Room)
4	CI-A-1033	Domain Controller – File Server	18	CI-A-1034 CI-A-1036 CI-A-1037	Switch 1 (Accounting & HR) Switch 2 (Sales & IT) Switch 3 (Director)
5	CI-A-1011	RADIUS/SNMP Server	19	CI-A-1002	Create New Customer
6	CI-A-1000	Industry Customer Data	20	CI-A-1003	Create New Order (Local)
7	CI-A-1001	Industry Employee Data	21	CI-A-1005	Customer Support
8	CI-A-1023	DNS/DHCP Server	22	CI-A-1010	CRM Server
9	CI-A-1016	WLAN Controller	23	CI-A-1008	Laptop
10	CI-A-1004	Create New Order (Remote)	24	CI-A-1017	Tablet PC
11	CI-A-1018	Email Server	25	CI-A-1024	HRM Server
12	CI-A-1035	Access Point	26	CI-A-1021	Printer
13	CI-A-1013	VoIP Phone	27	CI-A-1006	Windows 10 Pro
14	CI-A-1022	Edge Router			

Στην συνέχεια παρουσιάζονται αναλυτικά οι απειλές, ευπάθειες, και επιπτώσεις που πιθανόν θα φέρει καθένα από τα παραπάνω αγαθά στην ασφάλεια της Βιομηχανίας.

3.2. Απειλές που εντοπίστηκαν

Ο ακόλουθος πίνακας περιέχει τις **απειλές** που εντοπίστηκαν **ανά αγαθό** ή κατηγορία αγαθού:

Inventory ID	Όνομα	Απειλές
CI-A-1029	Application Server	• Distributed DoS - TCP SYN/UDP Flood Attacks (δημιουργία πολλών συνδέσεων TCP ή αποστολή πολλών πακέτων UDP σε όλες τις πύλες του server, προκαλώντας ένα ολοένα αυξανόμενο πλήθος μη ολοκληρωμένων συνδέσεων ή εισερχόμενων πακέτων). • Λογισμικό το οποίο στην πραγματικότητα δεν χρειαζόμαστε εγκαθίσταται και τρέχει στον server.
CI-A-1009 CI-A-1019 CI-A-1020 CI-A-1030 CI-A-1031 CI-A-1032	PC 3-6 (Sales & IT) PC 1-2 (Accounting & HR)	• Μη εξουσιοδοτημένος χρήστης έχει πρόσβαση στο workstation • Εγκατάσταση κακόβουλου λογισμικού - επιθέσεις που βασίζονται σε ανθρώπινο λάθος ή αφέλεια όπως οι social engineering επιθέσεις (phishing)/τα worms/η απάτη(εγκατάσταση λογισμικού που φαίνεται να είναι κάτι άλλο) • Επιθέσεις στα BIOS(πχ BIOS rootkit – αντικατάσταση BIOS με κακόβουλο κώδικα)
CI-A-1033	Domain Controller – File Server	• Κατάχρηση των δικαιωμάτων χρήσης • Απειλές και ιοί από τους οποίους το λειτουργικό δεν υποστηρίζει προστασία πλέον (όλες οι απειλές που δημιουργήθηκαν μετά τον 01/2020)
CI-A-1011	RADIUS/SNMP Server	• Μη εξουσιοδοτημένος βλέπει τα πακέτα που στέλνονται (packet spoofing). • Μη εξουσιοδοτημένος αποκτά το κλειδί κρυπτογράφησης.
CI-A-1000 CI-A-1001	Industry Customer Data Industry Employee Data	• Μη εξουσιοδοτημένη πρόσβαση στα προσωπικά δεδομένα πελατών ή υπαλλήλων • Database injection attacks (SQL Injection - Προσθήκη κακόβουλου κώδικα σε SQL queries)
CI-A-1023	DNS/DHCP Server	• Cache poisoning/DNS Spoofing/MITM (αντικατάσταση ιστοσελίδας με πιστό αντίγραφο σε server του attacker και προώθηση αυτής στους χρήστες)
CI-A-1016	WLAN Controller	• Αποστολή ενός ειδικά κατασκευασμένου frame και υπερχείλιση στοίβας/εκτέλεση κακόβουλου κώδικα (buffer overflow)
CI-A-1004	Create New Order (Remote)	• Attackers αποκτούν πρόσβαση σε λογαριασμούς χρηστών
CI-A-1018	Email Server	• Σπάσιμο κωδικών πρόσβασης χρηστών email και εισβολή hackers • Denial of Service attack (DoS/DDoS)

CI-A-1035	Access Point	• Μη εξουσιοδοτημένος χρήστης στέλνει αιτήματα αυθεντικοποίησης από πολλαπλούς πελάτες/ συσκευές • UDP Flood attack • Χρήστης συνδεδεμένος σε κοντινό ασύρματο δίκτυο παρεμβάλλει την κίνηση του ασύρματου δικτύου της εταιρίας.
CI-A-1013	VoIP Phone	• Παρεμβολές από κακόβουλο χρήστη • Eavesdropping – ο επιτιθέμενος αποκτά πρόσβαση και παρακολουθεί τα σήματα και περιεχόμενα που ανταλλάζονται ανάμεσα στους νόμιμους χρήστες
CI-A-1022	Edge Router	• Οι κανόνες χρήσης δεν έχουν διαμορφωθεί σωστά • Το λειτουργικό του σύστημα δεν υποστηρίζει ενημερώσεις ασφαλείας από την Microsoft από τον 01/2020
CI-A-1007	Windows 7	• Απειλές και ιοί από τους οποίους το λειτουργικό δεν υποστηρίζει προστασία πλέον (όλες οι απειλές που δημιουργήθηκαν μετά τον 01/2020)
CI-A-1012 CI-A-1015 CI-A-1026 CI-A-1028	Router 1-4	• Κακόβουλος χρήστης με πρόσβαση στο λειτουργικό σύστημα μιας συσκευής του δικτύου αποκτά πρόσβαση με δικαιώματα admin σε ολόκληρο το ευάλωτο σύστημα • Μη εξουσιοδοτημένος χρήστης έχει πρόσβαση στο περιεχόμενο των CDP πακέτων
CI-A-1025 CI-A-1027 CI-A-1034 CI-A-1036 CI-A-1037	Switch4.1,4.2 (Computer Room) Switch 1 (Accounting & HR) Switch 2 (Sales & IT) Switch 3 (Director)	• Εισβολέας που έχει έλεγχο συσκευής εντός του δικτύου στέλνει πολλαπλές ψεύτικες MAC διευθύνσεις μέχρι η CAM μνήμη να υπερχειλίσει (MAC flooding attack) • Ένας υπολογιστής στο VLAN συνδέεται με το switch και παίρνει όλες τις πληροφορίες για την τοπολογία του LAN (switch spoofing)
CI-A-1002	Create New Customer	• Κακόβουλος χρήστης έχει την δυνατότητα να δημιουργήσει μια καινούρια entry πελάτη (αποθηκεύεται σε database – customer data) • Εισαγωγή κακόβουλου SQL κώδικα στα πεδία εισαγωγής στοιχείων πελάτη (SQL Injection) (πχ κώδικας που στέλνει όλα τα δεδομένα της βάσης στον attacker)
CI-A-1003	Create New Order (Local)	• Μέλη του προσωπικού διαρρέουν δεδομένα πωλήσεων σε τρίτους με σκοπό το προσωπικό τους συμφέρον ή το συμφέρον του τρίτου
CI-A-1005	Customer Support	• Καθώς μεταφέρονται από την πηγή τους στην εφαρμογή, διαρροή των δεδομένων μέσω του δικτύου. • Μέλη του προσωπικού διαρρέουν δεδομένα σε τρίτους με σκοπό το προσωπικό τους συμφέρον ή το συμφέρον του τρίτου.
CI-A-1010	CRM Server	• Μη εξουσιοδοτημένη πρόσβαση στις διεργασίες
CI-A-1008	Laptop	• Μη εξουσιοδοτημένος χρήστης αποκτά πρόσβαση στο laptop • Fake access point attack (σύνδεση της συσκευής σε σημείο πρόσβασης που δημιουργεί ο attacker με σκοπό να διαβάσει τα δεδομένα όσων συνδέονται). • Παρεμβολές στο ασύρματο δίκτυο. • Κλοπή

CI-A-1017	Tablet PC	• Οποιοδήποτε πρόσωπο έχει στα χέρια του την φυσική συσκευή μπορεί να αποκτήσει πρόσβαση ή να παραβιάσει τον κωδικό πρόσβασης • Εγκατάσταση ιομορφικού λογισμικού μετά από πρόσβαση στο διαδίκτυο
CI-A-1024	HRM Server	• SQL injection attack • Επιτιθέμενος αποκτά πρόσβαση σε δεδομένα απόδοσης των υπαλλήλων της εταιρείας**,** ή τις οδηγίες για τους νέους υπαλλήλους
CI-A-1021	Printer	• Παρεμβολή κακόβουλου λογισμικού/χρηστών στην μεταφορά των δεδομένων προς εκτύπωση
CI-A-1006	Windows 10 Pro	• Απειλές και ιοί τους οποίους ο πάροχος του λειτουργικού συστήματος έχει διαχειριστεί μετά την τελευταία ενημέρωση.

3.3. Ευπάθειες που εντοπίστηκαν

Ο ακόλουθος πίνακας περιέχει τις **ευπάθειες** που εντοπίστηκαν **ανά αγαθό** ή κατηγορία αγαθού:

Inventory ID	Όνομα	Ευπάθειες
CI-A-1029	Application Server	• λαμβάνει HTTP αιτήματα από μη επικυρωμένες πηγές/πελάτες • Για κάθε αίτημα αναθέτει μνήμη στη σύνδεση με την πηγή πριν ολοκληρωθεί το TCP three – way handshake (πριν λάβει το ACK μήνυμα απ' την πηγή) • Εγκατάσταση λογισμικού χωρίς έλεγχο.
CI-A-1009 CI-A-1019 CI-A-1020 CI-A-1030 CI-A-1031 CI-A-1032	PC 3-6 (Sales & IT) PC 1-2 (Accounting & HR)	• Αδύναμος κωδικός πρόσβασης • Μη ελεγμένη εγκατάσταση λογισμικού από εξουσιοδοτημένο υπάλληλο , έλλειψη ενημέρωσης υπαλλήλων σχετικά με τους κινδύνους του Internet, χρήστες που δεν γνωρίζουν πως να χρησιμοποιούν έναν υπολογιστή • Πολλοί υπολογιστές σε ένα VLAN • Τα BIOS του υπολογιστή είναι erasable (πχ flash)/κανένας έλεγχος πρόσβασης στα BIOS
CI-A-1033	Domain Controller – File Server	• Οι κανόνες χρήσης δεν έχουν διαμορφωθεί σωστά • Το λειτουργικό του σύστημα δεν υποστηρίζει ενημερώσεις ασφαλείας από την Microsoft από τον 01/2020
CI-A-1011	RADIUS/SNMP Server	• Χρησιμοποιεί UDP πρωτόκολλο το οποίο είναι stateless και connectionless. • Χρήση συμμετρικής κρυπτογράφησης και μη ασφαλούς MD5 συνάρτησης κατακερματισμού για το κλειδί. • Επιτρέπει την χρήση του ίδιου κλειδιού κρυπτογράφησης σε πολλούς χρήστες.
CI-A-1000 CI-A-1001	Industry Customer Data Industry Employee Data	• Τα δεδομένα είναι αποθηκευμένα σε μη κρυπτογραφημένη μορφή • Απουσία ελέγχου SQL queries πριν την εκτέλεση

CI-A-1023	DNS/DHCP Server	• Ανεπαρκές configuration • Ευπάθειες του πρωτοκόλλου DNS και της μνήμης cache του server
CI-A-1016	WLAN Controller	• Το λογισμικό τρέχει κώδικα στην μνήμη χωρίς έλεγχο ορίων μνήμης κατά την εγγραφή και ανάγνωση • Σφάλματα κατά την επεξεργασία frames
CI-A-1004	Create New Order (Remote)	• Κακή υλοποίηση της αυθεντικοποίησης χρήστη στην εφαρμογή και της διαχείρισης συνεδρίας (session management)
CI-A-1018	Email Server	• Αδύναμες τεχνικές authentication χρηστών/αδύναμοι κωδικοί πρόσβασης • Έλλειψη ελέγχου για υπερβολικά μεγάλες ροές εισερχόμενων πακέτων
CI-A-1035	Access Point	• Λανθασμένη διαχείριση των χρηστών που προσπαθούν να συνδεθούν • Λανθασμένη διαχείριση των πόρων όσο επεξεργάζεται UDP πακέτα • Δυνατότητα παρεμβολής στα ασύρματα δίκτυα
CI-A-1013	VoIP Phone	• Έλλειψη κρυπτογράφησης δεδομένων που μεταδίδονται • Default (προεπιλεγμένοι) κωδικοί
CI-A-1022	Edge Router	• Μη αποτροπή μεγάλων ροών εισερχομένων πακέτων • Ανεπαρκής αυθεντικοποίηση αποστολέα πακέτων
CI-A-1007	Windows 7	• Δεν υποστηρίζει ενημερώσεις ασφαλείας από την Microsoft από τον 01/2020
CI-A-1012 CI-A-1015 CI-A-1026 CI-A-1028	Router 1-4	• Μη ενημέρωση του λογισμικού του router • Χρήση hard-coded hashes κωδικών χρηστών • Μη κρυπτογραφημένα frames του πρωτοκόλλου CDP (Cisco Discovery Protocol) (πρωτόκολλο επιπέδου 2 που παρέχει πληροφορίες για την τοπολογία όλων των Cisco συσκευών δικτύου στο LAN, by default enabled)
CI-A-1025 CI-A-1027 CI-A-1034 CI-A-1036 CI-A-1037	Switch4.1,4.2 (Computer Room) Switch 1 (Accounting & HR) Switch 2 (Sales & IT) Switch 3 (Director)	• Περιορισμένο πλήθος MAC διευθύνσεων χωράνε στον πίνακα CAM του switch. • Καμία ρύθμιση (configuration) σχετικά με τις MAC διευθύνσεις που μπορούν να στέλνουν frames • Αυτόματη ανάθεση port για την δημιουργία trunk συνδέσμων των συσκευών του δικτύου με το switch
CI-A-1002	Create New Customer	• Ανεπαρκές authentication του χρήστη που εκτελεί την διεργασία δημιουργίας πελάτη • Η εφαρμογή δημιουργίας πελάτη δεν κάνει type checking στα fields για την εισαγωγή στοιχείων πελάτη (που θα αποθηκευτούν στην βάση!)
CI-A-1003	Create New Order (Local)	• Το προσωπικό του τμήματος πωλήσεων μέσω της διεργασίας έχει πρόσβαση σε όλα τα δεδομένα πωλήσεων
CI-A-1005	Customer Support	• Για την σωστή εξυπηρέτηση πελατών απαιτείται πρόσβαση σε προσωπικά δεδομένα πελατών, συχνά είναι ευαίσθητα προσωπικά δεδομένα. • Η διεργασία εξυπηρέτησης έχει πρόσβαση σε όλα τα δεδομένα πελατών χωρίς φίλτρο.

CI-A-1010	CRM Server	• Έλλειψη verification(επαλήθευσης) χρηστών (πελατών και υπαλλήλων) • Outdated λογισμικό/ έλλειψη ενημερώσεων
CI-A-1008	Laptop	• Αδύναμος κωδικός πρόσβασης • Είναι φορητή συσκευή • Συνδέεται ασύρματα στο δίκτυο, αυτόματη σύνδεση στο πρώτο διαθέσιμο access point.
CI-A-1017	Tablet PC	• Αδύναμος ή ανύπαρκτος κωδικός πρόσβασης • Κανένα προ εγκατεστημένο λογισμικό προστασίας από ιούς και συχνή άγνοια χρηστών της ανάγκης εγκατάστασης του • Το tablet βρίσκεται συνδεδεμένο στο ίδιο δίκτυο με τις υπόλοιπες σημαντικότερες συσκευές της εταιρίας (υπολογιστές, server) και είναι πολύ πιο ευάλωτο σε επιθέσεις από αυτές • Παραβίαση του τοπικού δικτύου μέσω του tablet
CI-A-1024	HRM Server	• Απουσία ελέγχου SQL queries πριν την εκτέλεση • Τα δικαιώματα χρηστών δεν είναι σωστά καταχωρημένα/ρυθμισμένα
CI-A-1021	Printer	• Μετάδοση των δεδομένων προς εκτύπωση σε μη κρυπτογραφημένη μορφή • Κανένας έλεγχος πρόσβασης στον εκτυπωτή μέσω του δικτύου
CI-A-1006	Windows 10 Pro	• Δεν έχει εγκατασταθεί η νεότερη ενημέρωση του λειτουργικού συστήματος.

3.4. Αποτελέσματα αποτίμησης

Ο ακόλουθος πίνακας περιέχει τις **επιπτώσεις** που μπορεί να προκύψουν σε κάθε **αγαθό** ή κατηγορία αγαθού:

Inventory ID	Όνομα	Επιπτώσεις
CI-A-1029	Application Server	• Η υπηρεσία απορρίπτεται στους νόμιμους χρήστες, τους πελάτες της εταιρίας • Ο εξυπηρετητής δυσλειτουργεί ή παύει να λειτουργεί
CI-A-1009 CI-A-1019 CI-A-1020 CI-A-1030 CI-A-1031 CI-A-1032	PC 3-6 (Sales & IT) PC 1-2 (Accounting & HR)	• Κακόβουλο λογισμικό στέλνει προσωπικά δεδομένα σε άγνωστη πηγή (διαρροή προσωπικών δεδομένων) • Ο υπολογιστής παύει να λειτουργεί – καταστρέφεται • Μη εξουσιοδοτημένος χρήστης τροποποιεί/διαγράφει/καταστρέφει δεδομένα • Πρόσβαση στο VLAN και αχρήστευση συσκευών
CI-A-1033	Domain Controller – File Server	• Αδυναμία ταυτοποίησης των χρηστών στο δίκτυο • Αδυναμία στην πρόσβαση των δεδομένων • Μη εξουσιοδοτημένος χρήστης αποκτά τον έλεγχο ολόκληρου του δικτύου • Καταστροφή του συστήματος αρχείων του ΠΣ
CI-A-1011	RADIUS/SNMP Server	• Κλοπή δεδομένων του δικτύου, κωδικών πρόσβασης χρηστών (υπαλλήλων/πελατών).

CI-A-1000 CI-A-1001	Industry Customer Data Industry Employee Data	• Αδυναμία πρόσβασης στα δεδομένα • Μη εξουσιοδοτημένη πρόσβαση και τροποποίηση προσωπικών δεδομένων
CI-A-1023	DNS/DHCP Server	• Κλοπή δεδομένων • Κατάρρευση του server - διακοπή υπηρεσιών δικτύου - αποτροπή χρηστών από το να συνδεθούν
CI-A-1016	WLAN Controller	• Διαρροή δεδομένων και πρόσβαση σε ευαίσθητες πληροφορίες • Το ασύρματο δίκτυο δυσλειτουργεί, καθυστερεί ή παύει να λειτουργεί
CI-A-1004	Create New Order (Remote)	• Διαρροή προσωπικών δεδομένων πελατών • Δημιουργία ψεύτικων παραγγελιών
CI-A-1018	Email Server	• Πρόσβαση σε προσωπικά δεδομένα και δεδομένα της εταιρίας/διαρροή προσωπικών δεδομένων • Αχρήστευση του email server, αδύνατη η λήψη και αποστολή ηλεκτρονικού ταχυδρομείου • Ανεπιθύμητη κίνηση στο δίκτυο, υπερφόρτωση δικτύου • Επιπλέον τρόποι εισόδου για μη εξουσιοδοτημένους κακόβουλους χρήστες
CI-A-1035	Access Point	• Προσωρινή διακοπή της σύνδεσης των συνδεδεμένων συσκευών με το δίκτυο (προσωρινή αδυναμία λειτουργίας)
CI-A-1013	VoIP Phone	• Διαρροή συζητήσεων ή προσωπικών δεδομένων • Χρήση των πληροφοριών των συζητήσεων για μελλοντικές επιθέσεις • Καθυστερήσεις στις κλήσεις
CI-A-1022	Edge Router	• Κακόβουλοι χρήστες/που δεν έχουν δικαιώματα αποκτούν πρόσβαση στο δίκτυο και επομένως στις συσκευές του. • Ο router παύει να μεταδίδει πακέτα γιατί μπλοκάρεται
CI-A-1007	Windows 7	• Ο υπολογιστής που τρέχει Windows 7 δεν είναι πλέον προστατευμένος από ιούς • Από κλοπή δεδομένων μέχρι ολική καταστροφή του μηχανήματος
CI-A-1012 CI-A-1015 CI-A-1026 CI-A-1028	Router 1-4	• Κλοπή δεδομένων • Κακόβουλος χρήστης αποκτά πληροφορίες για όλη την τοπολογία του δικτύου • Έλεγχος των πακέτων που κινούνται στο δίκτυο • Πλήρης αχρήστευση του δικτύου (το δίκτυο βρίσκεται στα χέρια του επιτιθέμενου)
CI-A-1025 CI-A-1027 CI-A-1034 CI-A-1036 CI-A-1037	Switch4.1,4.2 (Computer Room) Switch 1 (Accounting & HR) Switch 2 (Sales & IT) Switch 3 (Director)	• Ο μεταγωγέας/switch είναι πιο ευάλωτος σε επερχόμενες επιθέσεις ακόμη και μετά την ολοκλήρωση της επίθεσης MAC flooding (πχ ARP spoofing και άλλες επιθέσεις τύπου active sniffing) • Παρακολούθηση όλης της κίνησης του συγκεκριμένου VLAN • Αδυναμία λειτουργίας • VLAN hopping (η συσκευή αποκτά πρόσβαση σε VLANS εκτός από το δικό του)

CI-A-1002	Create New Customer	• Κλοπή δεδομένων • Unauthorized τροποποίηση δεδομένων
CI-A-1003	Create New Order (Local)	• Διαρροή σημαντικών δεδομένων μέσα από τα δεδομένα πωλήσεων (πχ τραπεζικοί λογαριασμοί, στατιστικά, δεδομένα πελατών)
CI-A-1005	Customer Support	• Για την σωστή εξυπηρέτηση πελατών απαιτείται πρόσβαση σε προσωπικά δεδομένα πελατών, συχνά είναι ευαίσθητα προσωπικά δεδομένα. • Η διεργασία εξυπηρέτησης έχει πρόσβαση σε όλα τα δεδομένα πελατών χωρίς φίλτρο.
CI-A-1010	CRM Server	• Καθυστερήσεις, αδυναμία εκτέλεσης συναλλαγών • Διαρροή και καταστροφή δεδομένων • Δημιουργία ψεύτικων παραγγελιών
CI-A-1008	Laptop	• Δυσλειτουργία ή καταστροφή της συσκευής • Μη εξουσιοδοτημένη τροποποίηση, διαρροή δεδομένων. • Κλοπή κωδικών, logins και συνθηματικών.
CI-A-1017	Tablet PC	• Διαρροή προσωπικών δεδομένων του διευθυντή • Αχρήστευση της συσκευής • Από μόλυνση της φορητής συσκευής επιτυγχάνεται είσοδος σε άλλες συσκευές του δικτύου
CI-A-1024	HRM Server	• Απώλεια ή διαρροή των δεδομένων απόδοσης των υπαλλήλων • Δυσλειτουργία του server (παροχή εσφαλμένων δεδομένων ή οδηγιών)
CI-A-1021	Printer	• Διαρροή εμπιστευτικών δεδομένων
CI-A-1006	Windows 10 Pro	• Ο υπολογιστής που τρέχει Windows 10 δεν είναι προστατευμένος από τους νεότερους ιούς • Από κλοπή δεδομένων μέχρι ολική καταστροφή του μηχανήματος

Παρακάτω δίνεται ένας πίνακας αποτίμησης των επιπτώσεων, για κάθε ένα από τα παραπάνω αγαθά ως προς την διαθεσιμότητα, την ακεραιότητα, την εμπιστευτικότητα , και τυχών αστοχίες και λάθη στην τηλεπικοινωνιακή μετάδοση. Χρησιμοποιήθηκε η κλίμακα αξιολόγησης του Impact του συστήματος ISO27001.

	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	Αποποίηση	Άρνηση αποστολής ή παραλαβής	Παρεμβολή λογισμικών μηνυμάτων	Λανθασμένη δρομολόγηση	Παρακολούθηση κίνησης	Μη παράδοση	Απώλεια ακολουθίας μηνυμάτων
Application Server	8	8	8	9	9	9	10	10	7	6	7	5	1	1	1	1	1	1	10	1	1	8	8	8
PC 3-6 (Sales & IT) PC 1-2 (Accounting & HR)	8	8	8	9	9	10	10	7	7	6	6	6	1	6	7	1	6	1	8	1	1	7	1	1
Domain Controller – File Server	7	8	8	8	9	10	10	10	8	8	6	6	5	1	8	1	1	1	10	1	1	2	8	2
RADIUS/SNMP Server	7	8	8	9	10	10	10	9	9	9	6	6	8	2	10	1	1	1	1	6	1	7	1	5
Industry Customer Data	1	1	1	2	2	2	2	8	6	7	5	7	7	1	8	1	1	1	1	1	1	1	1	1
Industry Employee Data	1	1	1	2	2	2	2	8	6	7	5	7	6	1	8	1	1	1	1	1	1	1	1	1
DNS/DHCP Server	5	6	6	7	7	8	8	8	6	8	4	3	1	1	7	2	8	1	7	1	8	3	6	6
WLAN Controller	6	6	6	6	7	8	9	2	2	2	2	2	1	5	7	6	1	1	8	8	5	8	8	7

Create New Order (Remote)	1	1	1	1	1	1	1	7	6	7	5	7	1	1	7	1	6	1	1	6	1	6	1	1
Email Server	6	6	7	7	7	8	8	8	6	4	2	2	1	1	7	5	1	1	8	7	1	5	8	8
Access Point	7	7	7	7	8	8	8	1	1	1	1	1	4	1	7	7	1	1	8	7	1	7	8	8
VoIP Phone	7	7	7	7	8	9	9	1	1	1	1	1	2	4	8	1	1	1	7	5	1	10	1	3
Edge Router	7	7	8	8	8	8	8	1	1	1	1	1	1	6	8	6	7	7	8	8	8	7	8	8
Windows 7	4	5	6	6	7	8	8	8	6	7	4	6	1	1	8	1	7	1	1	1	1	1	1	1
Router 1-4	7	7	8	8	8	8	8	1	1	1	1	1	1	6	8	6	7	7	8	8	8	7	8	8
Switch4.1,4.2 (Computer Room)	7	7	8	8	8	8	8	1	1	1	1	1	1	1	7	3	1	1	7	5	7	7	8	7
Switch 1 (Accounting & HR) Switch 2 (Sales & IT) Switch 3 (Director)	7	7	8	8	8	8	8	1	1	1	1	1	1	1	1	3	1	1	8	4	7	7	8	7
Create New Customer	1	1	1	1	1	1	1	8	6	8	4	5	2	1	8	1	5	1	1	1	1	1	1	1
Create New Order (Local)	1	1	1	1	1	1	1	1	1	1	1	1	7	1	7	1	1	1	1	1	1	1	1	1
Customer Support	1	1	1	1	1	1	1	1	1	1	1	1	7	1	7	1	1	1	1	1	1	1	1	1

CRM Server	6	6	7	7	7	8	8	8	8	7	5	7	4	1	6	1	6	1	2	1	1	1	1	1
Laptop	3	3	4	5	6	7	9	7	6	7	5	6	7	1	7	1	1	1	1	1	7	1	1	1
Tablet PC	1	1	1	1	1	1	1	2	2	1	2	2	1	1	7	1	1	1	1	6	6	6	1	1
HRM Server	3	4	4	5	5	6	7	7	5	6	3	6	2	1	7	1	1	1	1	1	1	1	1	1
Printer	1	1	1	1	1	1	1	1	1	1	1	1	5	2	7	1	4	1	1	7	6	7	1	1
Windows 10 Pro	2	2	3	4	5	5	6	6	5	6	2	3	1	1	6	1	1	1	1	1	1	1	1	1

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 ιομορφικό λογισμικό

A9. Ασφαλής χρήση διαδικτυακών υπηρεσιών

A10. Ασφάλεια εξοπλισμού

A11. Φυσική ασφάλεια κτιριακής εγκατάστασης

Τα μέτρα έχουν εφαρμογή στο ΠΣ της Βιομηχανίας η οποία μελετάται στην παρούσα εργασία.

Παρακάτω παρουσιάζονται όλα τα μέτρα που εντοπίστηκαν, χωρισμένα στις παραπάνω 11 κατηγορίες, σε συνδυασμό με τα IDs και τα ονόματα των αγαθών τα οποία προστατεύει το κάθε μέτρο.

4.1. Προσωπικό – Προστασία Διαδικασιών Προσωπικού

Inventory ID	Όνομα	Μέτρο Προστασίας
CI-A-1031 CI-A-1032 CI-A-1009 CI-A-1019 CI-A-1020 CI-A-1030 CI-A-1008 CI-A-1018	PC 1-6, Laptop, Tablet , Email Server	Κατάλληλη εκπαίδευση των υπαλλήλων για χρήση ισχυρών κωδικών πρόσβασης
CI-A-1031 CI-A-1032 CI-A-1009 CI-A-1019 CI-A-1020 CI-A-1030	PC 1-6	Ενημέρωση του προσωπικού για συχνά σφάλματα χρήσης υπολογιστών και τις social engineering επιθέσεις.

4.2. Ταυτοποίηση και αυθεντικοποίηση

Inventory ID	Όνομα	Μέτρο Προστασίας
CI-A-1031 CI-A-1032 CI-A-1009 CI-A-1019 CI-A-1020 CI-A-1030 CI-A-1008 CI-A-1017 CI-A-1018	PC 1-6, Laptop, Tablet, Email Server	Χρήση ισχυρών κωδικών πρόσβασης στους υπολογιστές και τους λογαριασμούς email.
CI-A-1017	Tablet	Χρήση βιομετρικών μεθόδων ταυτοποίησης όπως πχ το αποτύπωμα.
CI-A-1018 CI-A-1004	Email Server Create New Order (Remote)	Χρήση 2 factor authentication
CI-A-1011	RADIUS/SNMP Server	Ανάθεση χρονικού ορίου για κάθε προσπάθεια σύνδεσης - αυθεντικοποίησης
CI-A-1033 CI-A-1000 CI-A-1001 CI-A-1010	Domain Controller – File Server, Industry Customer Data, Industry Employee Data, CRM Server	Χρήση ψηφιακών πιστοποιητικών για την αυθεντικοποίηση χρηστών που επιθυμούν πρόσβαση σε ευαίσθητα δεδομένα.

4.3. Έλεγχος προσπέλασης και χρήσης πόρων

Inventory ID	Όνομα	Μέτρο Προστασίας
CI-A-1033 CI-A-1000 CI-A-1001	Domain Controller – File Server, Industry Customer Data, Industry Employee Data	Τακτική ενημέρωση των δικαιωμάτων πρόσβασης των συσκευών των υπαλλήλων στο σύστημα αρχείων και την βάση δεδομένων της εταιρίας, για παράδειγμα 1 φορά τον μήνα.
CI-A-1002 CI-A-1003 CI-A-1005	Customer Support, Create New Order (Local), Create New Customer	Περιορισμός του όγκου δεδομένων πωλήσεων στα οποία έχει πρόσβαση η διεργασία.

4.4. Διαχείριση εμπιστευτικών δεδομένων

Inventory ID	Όνομα	Μέτρο Προστασίας
CI-A-1033 CI-A-1000 CI-A-1001	Domain Controller – File Server, Industry Customer Data, Industry Employee Data	Διατήρηση αντιγράφων ασφαλείας (backups) όλων των κρίσιμων προσωπικών δεδομένων.
CI-A-1033 CI-A-1000 CI-A-1001 CI-A-1018	Domain Controller – File Server, Industry Customer Data, Industry Employee Data, Email Server	Σωστή και ασφαλής κρυπτογράφηση των ευαίσθητων δεδομένων που βρίσκονται αποθηκευμένα στην βάση δεδομένων και άλλους servers της εταιρίας, όπως για παράδειγμα ο email server.
CI-A-1003 CI-A-1005	Customer Support, Create New Order (Local)	Χρήση συστήματος που προειδοποιεί την διεύθυνση της εταιρίας όταν κάποιος υπάλληλος στα πλαίσια μιας επιχειρησιακής διεργασίας χρησιμοποιεί εμπιστευτικά δεδομένα τα οποία δεν χρειάζεται για την εργασία αυτή.
CI-A-1013	VoIP Phone	Κρυπτογράφηση των δεδομένων που μεταδίδονται κατά την δημιουργία κλήσεων με Voice over IP
CI-A-1021	Printer	Εγκατάσταση λογισμικού για κρυπτογράφηση των δεδομένων πρώτού σταλούν για εκτύπωση
CI-A-1003 CI-A-1005	Customer Support, Create New Order (Local)	Μεταφορά των δεδομένων σε κρυπτογραφημένη μορφή για την χρήση τους από την διεργασία.
CI-A-1000 CI-A-1001	Industry Customer Data, Industry Employee Data	Δημιουργία πολιτικής για το απόρρητο των προσωπικών δεδομένων και καθορισμός των νομικών συνεπειών υπαλλήλου σε περίπτωση διαρροής τους από αυτόν.

4.5. Προστασία από τη χρήση υπηρεσιών από τρίτους

Inventory ID	Όνομα	Μέτρο Προστασίας
CI-A-1012 CI-A-1015 CI-A-1026 CI-A-1028 CI-A-1022	Edge Router, Router 1-4	Χρήση VPN ώστε να παραμένει κρυφή η διεύθυνση IP της εταιρίας καθώς και να είναι ελεγχόμενη η πρόσβαση και κίνηση εντός του τοπικού δικτύου.
	Όλα τα αγαθά που βρίσκονται στο **Computer Room**	Εγκατάσταση ενός επιπλέον firewall στον όροφο του Computer Room, για ελεγχόμενη μετάβαση αιτημάτων στους διακομιστές.
CI-A-1021	Printer	Αποσύνδεση του εκτυπωτή από τον μεταγωγέα δικτύου και απευθείας σύνδεση του σε θύρες των συσκευών που τον χρησιμοποιούν (PCs).

4.6. Προστασία λογισμικού

Inventory ID	Όνομα	Μέτρο Προστασίας
CI-A-1000 CI-A-1001 CI-A-1024	Industry Customer Data, Industry Employee Data, HRM Server	Διόρθωση του κώδικα εφαρμογών για χρήση παραμετροποιημένων SQL ερωτημάτων (queries)
CI-A-1000, CI-A-1001	Industry Customer Data, Industry Employee Data	Χρήση Database firewall που εντοπίζει τα SQL Injections
CI-A-1031 CI-A-1032 CI-A-1009 CI-A-1019 CI-A-1020 CI-A-1030 CI-A-1008	PC 1-6, Laptop	Συνεχής εγκατάσταση των τελευταίων ενημερώσεων λογισμικού για όλες τις εφαρμογές.
CI-A-1031 CI-A-1032 CI-A-1009 CI-A-1019 CI-A-1020 CI-A-1030	PC 1-6	Χρήση non-writeable τεχνολογίας μνήμης για τα BIOS
CI-A-1031 CI-A-1032 CI-A-1009 CI-A-1019 CI-A-1020 CI-A-1030	PC 1-6	Υλοποίηση ψηφιακής υπογραφής για αποφυγή της εξ αποστάσεως unauthorized πρόσβασης στα BIOS

4.7. Διαχείριση ασφάλειας δικτύου

Inventory ID	Όνομα	Μέτρο Προστασίας
CI-A-1012 CI-A-1015 CI-A-1026 CI-A-1028 CI-A-1022 CI-A-1016 CI-A-1025 CI-A-1027 CI-A-1034 CI-A-1036 CI-A-1037 CI-A-1035	Router 1-4, Edge Router, WLAN Controller, Switch 1, 2, 3, 4.1,4.2, Access Point	Συνεχής εγκατάσταση των τελευταίων ενημερώσεων λογισμικού στις συσκευές δικτύου όπως οι routers, τα switches, και ο ελεγκτής ασύρματου δικτύου.
CI-A-1016	WLAN Controller	Χρήση πρωτοκόλλου WPA (WiFi protected access)
CI-A-1012 CI-A-1015 CI-A-1026 CI-A-1028	Router 1-4	Αποθήκευση των εγγραφών του CDP πίνακα στο configuration αρχείο της συσκευής και απενεργοποίηση του πρωτοκόλλου CDP.

CI-A-1035	Access Point	Επιλογή νέου ασύρματου καναλιού χωρίς παρεμβολές, ή ρύθμιση της επιλογής καναλιού Wi-Fi στο «Αυτόματο» ώστε να επιλέγεται συνεχώς το κανάλι με τις λιγότερες παρεμβολές.
CI-A-1035	Access Point	Μετακίνηση του access point ή μείωση της δύναμης του σήματος του Wi-Fi , έτσι ώστε να φτάνει μόνο μέχρι τα σύνορα του χώρου στον οποίο το ασύρματο δίκτυο είναι χρήσιμο για την εταιρία.
CI-A-1012 CI-A-1015 CI-A-1026 CI-A-1028 CI-A-1022	Router 1-4, Edge Router	Χρήση ισχυρού κωδικού πρόσβασης στους routers.
CI-A-1011	RADIUS/SNMP Server	Χρήση ασφαλούς συνάρτησης κατακερματισμού SHA-1 για την κρυπτογράφηση κλειδιών, και επιλογή κατάλληλου κλειδιού ώστε να είναι δύσκολο να βρεθεί
CI-A-1011	RADIUS/SNMP Server	Χρήση πρωτοκόλλου TCP έναντι UDP
CI-A-1016 CI-A-1035	WLAN Controller, Access Point	Χρήση ενός firewall στο γραφείο του διευθυντή που να ελέγχει αποκλειστικά την κίνηση του ασύρματου δικτύου.
CI-A-1025 CI-A-1027 CI-A-1034 CI-A-1036 CI-A-1037	Switch 1, 2, 3, 4.1,4.2	Χρήση Secure Shell 2 (SSH2) (πρωτόκολλο για ασφαλείς (κρυπτογραφημένες) συνδέσεις συσκευών με το switch)
CI-A-1025 CI-A-1027 CI-A-1034 CI-A-1036 CI-A-1037	Switch 1, 2, 3, 4.1,4.2	Τακτική επανασύνδεση των συσκευών στο switch σε διαφορετικές θύρες ώστε να αλλάζουν τα ζεύγη MAC address – port . Απενεργοποίηση των θυρών που δεν χρησιμοιούνται.
CI-A-1025 CI-A-1027 CI-A-1034 CI-A-1036 CI-A-1037	Switch 1, 2, 3, 4.1,4.2	Καθορισμός του μέγιστου πλήθους ή των συγκεκριμένων διευθύνσεων MAC που μπορούν να συνδεθούν στο switch. "Κλείδωμα" των MAC διευθύνσεων στις θύρες (επιλογή του port security).
CI-A-1025 CI-A-1027 CI-A-1034 CI-A-1036 CI-A-1037	Switch 1, 2, 3, 4.1,4.2	Hard code την θύρα που χρησιμοποιείται για δημιουργία trunk συνδέσμων.

4.8. Προστασία από ιομορφικό λογισμικό

Inventory ID	Όνομα	Μέτρο Προστασίας
CI-A-1006	Windows 10	Ενεργοποίηση αυτόματης εγκατάστασης ενημερώσεων λειτουργικού συστήματος
CI-A-1033 CI-A-1007	Domain Controller – File Server, Windows 7	Αγορά πακέτου extended security updates.

CI-A-1033, CI-A-1007	Domain Controller – File Server, Windows 7	Αντικατάσταση με πιο μοντέρνο λειτουργικό σύστημα το οποίο λαμβάνει τακτικά ενημερώσεις λογισμικού.
CI-A-1029	Application Server	Απεγκατάσταση λογισμικού που έχει εγκατασταθεί χωρίς εξουσιοδότηση ή που δεν το χρειάζεται η εταιρία.
CI-A-1031 CI-A-1032 CI-A-1009 CI-A-1019 CI-A-1020 CI-A-1030	PC 1-6	Χρήση εικονικών μηχανών και αντικατάστασή τους σε περίπτωση που κάποιο μηχάνημα μολυνθεί από ιομορφικό λογισμικό.
CI-A-1031 CI-A-1032 CI-A-1009 CI-A-1019 CI-A-1020 CI-A-1030 CI-A-1007 CI-A-1006	PC 1-6 Windows 7 Windows 10	Επιστροφή σε κάποιο σημείο πριν από μόλυνση του συστήματος (restore point)

4.9. Ασφαλής χρήση διαδικτυακών υπηρεσιών

Inventory ID	Όνομα	Μέτρο Προστασίας
CI-A-1029	Application Server	Ανάθεση μνήμης ανά σύνδεση μόνο εφόσον ο χρήστης που κάνει ένα HTTP αίτημα έχει εξακριβωθεί, πχ μέσω hashing με χρήση IP, θύρας και άλλων πληροφοριών του αποστολέα (SYN cookies).
CI-A-1029 CI-A-1031 CI-A-1032 CI-A-1009 CI-A-1019 CI-A-1020 CI-A-1030	Application Server, PC 1-6	Χρήση ασφαλούς πρωτοκόλλου HTTPS για περιήγηση στο διαδίκτυο.
CI-A-1017	Tablet	Χρήση 3G/4G για πρόσβαση στο Διαδίκτυο από το tablet, ώστε αυτό να μην βρίσκεται συνδεδεμένο στο ίδιο δίκτυο με τις άλλες, σημαντικότερες συσκευές.
CI-A-1022	Edge Router	Προσθήκη φίλτρων για απόρριψη πακέτων που προέρχονται προφανώς με σκοπό την επίθεση DoS (πχ πολλά συνεχόμενα πακέτα από ίδιες IP/MAC)
CI-A-1029 CI-A-1000 CI-A-1001	Application Server, Industry Customer Data, Industry Employee Data	Μετάβαση σε ασφαλείς υπηρεσίες cloud, οι οποίες παρέχουν σημαντική προστασία από επιθέσεις μέσω του Διαδικτύου, αντί για διατήρηση του εξυπηρετητή εντός του κτηρίου της Βιομηχανίας.
CI-A-1023	DNS/DHCP Server	Αντικατάσταση του πρωτοκόλλου DNS με το ασφαλέστερο πρωτόκολλο DNSSEC το οποίο καταπολεμά τις ευπάθειες του DNS, παρέχει κρυπτογράφηση και ισχυρότερη αυθεντικοποίηση

4.10. Ασφάλεια εξοπλισμού

Inventory ID	Όνομα	Μέτρο Προστασίας
CI-A-1031 CI-A-1032 CI-A-1009 CI-A-1019 CI-A-1020 CI-A-1030 CI-A-1008	PC 1-6, Laptop	Εγκατάσταση κλειστού κυκλώματος τηλεόρασης (κάμερες ασφαλείας) για 24ωρή παρακολούθηση των χώρων της εταιρίας και επομένως της μη εξουσιοδοτημένης πρόσβασης σε PC και Laptops.
CI-A-1008	Laptop	Χρήση αλυσίδας Kensington για προστασία από κλοπή.
CI-A-1000 CI-A-1001	Industry Customer Data, Industry Employee Data	Χρήση συστοιχίας RAID για την διατήρηση φυσικών αντιγράφων των σκληρών δίσκων της εταιρίας και αντικατάσταση σε περίπτωση καταστροφής.
	Όλος ο **υλικός εξοπλισμός** της εταιρίας.	Χρήση συστημάτων uninterruptible power supply (UPS).

4.11. Φυσική ασφάλεια κτιριακής εγκατάστασης

Inventory ID	Όνομα	Μέτρο Προστασίας
	Όλα τα αγαθά που βρίσκονται στο **Computer Room**	Εγκατάσταση συστήματος κλιματισμού στον 4ο όροφο όπου βρίσκεται το δωμάτιο των διακομιστών με σκοπό να προστατευτούν αυτοί από πιθανή υπερθέρμανση
	Όλος ο **υλικός εξοπλισμός** της εταιρίας.	Ασφάλιση του κτηρίου για είσπραξη αποζημίωσης σε περίπτωση φυσικών καταστροφών.

5. ΣΥΝΟΨΗ ΠΙΟ ΚΡΙΣΙΜΩΝ ΑΠΟΤΕΛΕΣΜΑΤΩΝ

Όπως φαίνεται και από τον πίνακα με τα αγαθά στην ενότητα 3.1, τα 4 αγαθά που θεωρούνται πιο κρίσιμα για την ασφάλεια της Βιομηχανίας μετά το πέρας της ανάλυσης επικινδυνότητας, λαμβάνοντας υπ' όψην τόσο την σοβαρότητα των επιπτώσεων τους, όσο και άλλους παράγοντες όπως την ευκολία εκμετάλλευσης των ευπαθειών τους και την πιθανότητα να πετύχει μια επίθεση εις βάρος τους είναι τα εξής :

1) **Application Server**

   Από τους σημαντικότερους εξυπηρετητές για την Βιομηχανία, αλλά και ο πιο ευάλωτος στο να δεχτεί επίθεση από απομακρυσμένα μηχανήματα μέσω του Διαδικτύου, καθώς αυτοματοποιεί την διεργασία **της δημιουργίας παραγγελίας εξ αποστάσεως**. Επιθέσεις όπως Distributed Denial of Service και TCP Flood Attack, μπορούν να δημιουργηθούν οδηγώντας τον server σε κατάρρευση, και κατά συνέπεια την εταιρία σε μια σοβαρή απώλεια λειτουργικότητας. Ακόμα, η εύκολη πρόσβαση σε αυτόν μέσω της δημιουργίας παραγγελίας, άλλα και η ευκολία εγκατάστασης λογισμικού σε αυτόν, τον κάνει εύκολο στόχο για κακόβουλους που θέλουν να «σπάσουν» άλλα σημαντικά μηχανήματα της εταιρίας που συνδέονται μαζί του.

2) **PCs**

   Τα μηχανήματα αυτά αποτελούν πολύτιμα αγαθά για την Βιομηχανία καθώς εκτελούν βασικές διεργασίες όπως η τοπική δημιουργία παραγγελίας και η εξυπηρέτηση πελατών. Οι διεργασίες αυτές έχουν άμεση πρόσβαση σε ευαίσθητα δεδομένα, και εκτελούνται από προσωπικό που δεν εξειδικεύεται σε θέματα πληροφορικής και ασφάλειας. Επομένως υπάρχει μεγάλη πιθανότητα ένας υπολογιστής να δεχτεί επιθέσεις, συχνά λόγω ανθρώπινου λάθους, οι οποίες θα στοχεύσουν στα δεδομένα ή άλλα σημαντικά αγαθά της εταιρίας όπως servers.

3) **Domain Controller – File Server**

   Ο εξυπηρετητής αυτός είναι ιδιαίτερης σημασίας αγαθό, καθώς περιέχει το σύστημα αρχείων και την βάση δεδομένων της εταιρίας, και αναλαμβάνει τον έλεγχο προσπέλασης στα δεδομένα που βρίσκονται αποθηκευμένα εκεί. Με μια επίθεση σε αυτόν μπορεί κανείς να αποκτήσει πρόσβαση ή να τροποποιήσει αυτά τα πολύτιμα δεδομένα, κάτι το οποίο θα ήταν τεράστιο πλήγμα για την Βιομηχανία. Το απαρχαιωμένο του λειτουργικό σύστημα κάνει αυτόν τον εξυπηρετητή ακόμα πιο ευάλωτο σε επιθέσεις.

4) **RADIUS/SNMP Server**

   Από τους σημαντικότερους εξυπηρετητές της Βιομηχανίας, καθώς αναλαμβάνει τη συνολική διαχείριση του τοπικού δικτύου. Παρέχει έλεγχο ταυτότητας, εξουσιοδότηση και υπηρεσίες παρακολούθησης όλων των χρηστών – συσκευών του δικτύου, γι' αυτό και παραβιάζοντας τον εξυπηρετητή αυτόν μπορεί ο επιτιθέμενος να αποκτήσει τον πλήρη έλεγχο του δικτύου.

ΠΗΓΕΣ

MAC flooding attack

https://digitalfortresslk.wordpress.com/2018/03/22/common-attack-types-on-switches/
https://www.wisegeek.com/what-is-mac-flooding.htm
https://www.interserver.net/tips/kb/mac-flooding-prevent/
https://en.wikipedia.org/wiki/SSH_(Secure_Shell)#Vulnerabilities
https://www.differencebetween.com/difference-between-ssh1-and-vs-ssh2/
https://www.ciscopress.com/articles/article.asp?p=2181836&seqNum=7
https://www.cisco.com/c/en/us/products/collateral/switches/business-250-series-smart-switches/nb-06-bus250-smart-switch-ds-cte-en.html

Switch spoofing attack
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

https://www.omnisecu.com/ccna-security/what-is-switch-spoofing-attack-how-to-prevent-switch-spoofing-attack.php

BIOS rootkit attack
https://www.lenovo.com/us/en/desktops-and-all-in-ones/thinkcentre/m-series-towers/ThinkCentre-M90t/p/11TC1MDM90T
https://www.lenovopartnernetwork.com/us/thinkshield/
https://searchcloudsecurity.techtarget.com/definition/BIOS-rootkit-attack

SYN flood attack

https://www.imperva.com/learn/ddos/syn-flood/

Access point's vulnerabilities (specific product)

https://www.cisco.com/c/en/us/support/wireless/business-240ac-access-point/model.html
https://www.cisco.com/c/en/us/support/docs/csa/cisco-sa-aironet-dos-h3DCuLXw.html

https://www.cisco.com/c/en/us/support/docs/csa/cisco-sa-aironet-dos-VHr2zG9y.html

Network interference

https://how2do.org/how-to-avoid-interference-on-wifi-from-neighbors-networks/

https://www.cisco.com/c/en/us/support/docs/smb/wireless/CB-Wireless-Mesh/2073-interferers.html

CDP unencrypted packet vulnerability

http://www.networkpcworld.com/2018/06/types-of-layer-2switch-security-attacks.html

https://howdoesinternetwork.com/2011/cdp-attack
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2_46_se/configuration/guide/scg1/swcdp.pdf

https://learningnetwork.cisco.com/s/article/cisco-discovery-protocol-cdp-x
https://www.computernetworkingnotes.com/ccna-study-guide/cdp-cisco-discovery-protocol-guide-with-examples.html

Unauthorized privilege access through router
https://cwe.mitre.org/data/definitions/798.html
https://www.cybersecurity-help.cz/vdb/SB2019090511

DDOS attack on edge router
https://www.ccexpert.us/scnd/threats-to-and-attacks-on-routers.html#:~:text=Some%20general%20threats%20to%20routers,%2C%20eavesdropping%2C%20and%20information%20theft

Buffer overflow attack on WLAN Controller

https://cwe.mitre.org/data/definitions/119.html
https://www.cybersecurity-help.cz/vdb/SB2020041604

Password cracking and DDOS attack on Email server
https://www.cbtnuggets.com/blog/certifications/microsoft/5-threats-to-your-email-server

Transmission interference
https://blog.symquest.com/4-common-printer-security-vulnerabilities-to-fix-today

Cache poisoning – DNS spoofing attack
Infoblox, *Top Five DNS Security Attack Risks and How to Avoid Them*, https://www.infoblox.com/wp-content/uploads/2016/04/infoblox-whitepaper-top5-dns-security-attack-risks-how-to-avoid-them_0.pdf , 2016

https://www.imperva.com/learn/application-security/dns-spoofing/

Portable device vulnerabilities
European Union Agency For Cybersecurity, *Hardware Threat Landscape and Good Practice Guide*, ENISA, https://www.enisa.europa.eu/publications/hardware-threat-landscape, 2017

SQL injection attack

https://en.wikipedia.org/wiki/SQL_injection

https://dzone.com/articles/what-is-the-sql-injection-vulnerability-amp-how-to
https://www.getfilecloud.com/blog/2018/06/identifying-the-top-10-most-common-database-security-vulnerabilities/

Radius cryptographic key and hashing

https://en.wikipedia.org/wiki/RADIUS

Customer Relationship Management security

https://www.toolbox.com/tech/enterprise-software/blogs/4-common-mistakes-in-crm-security-101514/

User authentication and session management

Michaels, Ross & Cole ltd, *Solving the Top 10 Application Security Threats*, MRC/M – Power , https://www.mrc-productivity.com/research/solving-application-security.pdf

Customer support security

http://techgenix.com/customer-service-department/

Windows 7

https://www.microsoft.com/en-us/windows/windows-7-end-of-life-support-information

Windows Server 2008

https://support.microsoft.com/en-us/help/4456235/end-of-support-for-windows-server-2008-and-windows-server-2008-r2

https://docs.microsoft.com/el-gr/lifecycle/faq/extended-security-updates