

Διοίκηση Ασφάλειας ΠΣ - Παραδοτέο 4

Ομάδα 2 - Κωνσταντίνος Γαρείος - inf2021036

Μάιος 2025

Υποθετική Μελέτη Περίπτωσης - Σύστημα ΑΙΟΛΟΣ

Contents

1	Εισαγωγή	2
2	Κατάλογος Πληροφοριακών Πόρων	3
2.1	Σχήμα ΑΙΟΛΟΣ	4
2.2	Τύποι δεδομένων	4
2.3	Οντότητες εφαρμογών	5
3	Μελέτη Ασφάλειας του συστήματος	5
3.1	Πλαίσιο κινδύνου	5
3.2	Σχέδιο ασφάλειας: Προτεινόμενα αντίμετρα	6
3.3	Αποδεκτές απειλές	6
4	Ανάλυση επικινδυνότητας	7
4.1	PTA	7
4.2	SimpleRisk	23
5	Υποθέσεις	27

1 Εισαγωγή

Η ανάλυση επικινδυνότητας αφορά τα εργαλεία **PTA** και **SimpleRisk**.

Αναλαμβάνω την ανάλυση επικινδυνότητας του **λογισμικού μισθοδοσίας** και της **βάσης δεδομένων Oracle** του συστήματος "ΑΙΟΛΟΣ", ένα θυγατρικό σύστημα της δημόσιας υποδομής G-Cloud της ΓΓΠΣΔΔ.

Το σύστημα ΑΙΟΛΟΣ αποκλειστικά διαχειρίζεται το υπουργείο Ναυτιλίας της Ελλάδας και των εφαρμογών της Γενικής Διεύθυνσης. Βρίσκεται σε διαφορετικό χώρο από το υπόλοιπο G-Cloud στην οδό Χάνδρη 1 και Θεσσαλονίκης στην Καλλιθέα.

Εμπλεκόμενες τεχνολογίες:

1. Software
2. Hardware
3. Linux
4. Oracle Databases
5. Local Servers
6. Virtual Machines

2 Κατάλογος Πληροφοριακών Πόρων

Πληροφοριακός Πόρος	Κατηγορία	Σημειώσεις
Κεντρικό Κτήριο G-Cloud	Κτήριο	Καλλιθέα Αττικής
Παράρτημα ΑΙΟΛΟΣ	Κτήριο	Καλλιθέα Αττικής
Εξυπηρετής αποκλειστικής χρήσης	Hardware	Κτήριο ΑΙΟΛΟΣ
Hypervisor Εξυπηρετητής ESXi	Hardware	Κτήριο ΑΙΟΛΟΣ
Red Hat Linux OS	Software	Server - (Web Server)
USB ports, DVD Recorder	Hardware	Server - (Web Server)
Λογισμικό Μισθοδοσίας Υπουργείου	Software	Server - (VM Server)
HRMS - Λογισμικό διαχείρισης HR	Software	Server - (VM Server)
Virtual Storage	Software	Server - (VM Server)
Database Infrastructure	Hardware	DC - EXADATA
EXADATA Oracle Database	Software	DC - EXADATA
Φυσικής μορφής συμβόλαια	Physical papers	Ερμάριο
Μαγνητικές κασέτες backup	Hardware	Ερμάριο
CD/DVD εφαρμογών	Hardware	Ερμάριο

2.1 Σχήμα ΑΙΟΛΟΣ

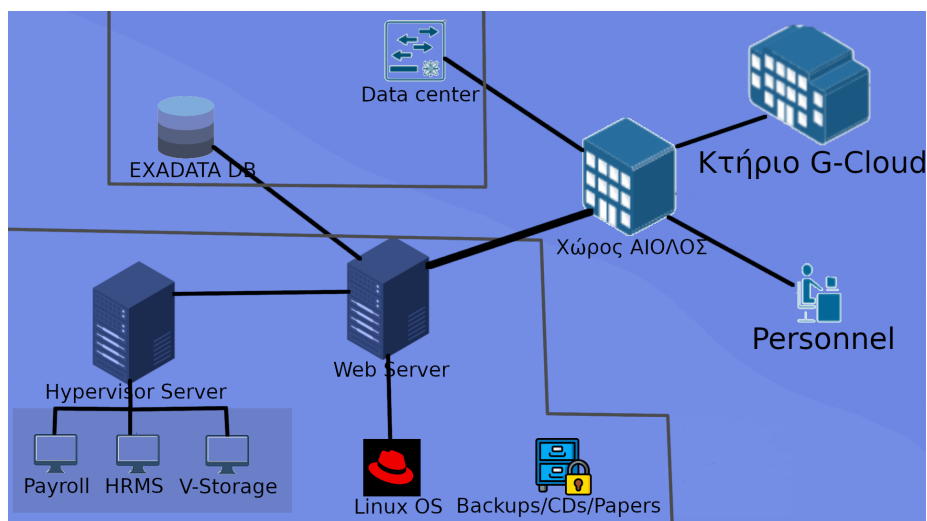


Figure 1: Οπτικοποίηση του συστήματος (Την υλοποίησα με GIMP)

2.2 Τύποι δεδομένων

Σύστημα	Βάση/Υπηρεσία	Τύπος δεδομένων
HRMS	Local VM	Προσωπικά Δεδομένα Υπαλλήλων
Payroll	Local VM	Δεδομένα Μισθοδοσίας Υπαλλήλων
Virtual Storage	Local VM	Δεδομένα αποθήκευσης
Μαγνητικές Κασέτες	Physical	Backups των Προσωπικών Δεδομένων των πολιτών
Συμβόλαια	Physical	Αρχεία αγορών app, server, etc.
CD εφαρμογών	Physical	CDs για την λειτουργία εφαρμογών

2.3 Οντότητες εφαρμογών

Πληροφοριακός Πόρος	IP	Στέγαση
Web Server	10.2.0.1	Κτήριο ΑΙΟΛΟΣ
Hypervisor Server	10.2.1.4	Κτήριο ΑΙΟΛΟΣ
Εφαρμογή Payroll	10.2.1.10	Hypervisor Server
Εφαρμογή HRMS	10.2.1.20	Hypervisor Server
EXADATA Database	10.2.1.30	DC Server
Oracle External Database	10.5.0.1	Κτήριο ΑΙΟΛΟΣ
Κάμερα καταγραφής	10.3.0.1	Κτήριο ΑΙΟΛΟΣ
Αισθητήρες Θερμοκρασίας	10.3.0.3	Κτήριο ΑΙΟΛΟΣ
Αισθητήρες Υγρασίας	10.3.0.2	Κτήριο ΑΙΟΛΟΣ
Συναγερμός Παραβίασης	10.3.0.4	Κτήριο ΑΙΟΛΟΣ

3 Μελέτη Ασφάλειας του συστήματος

3.1 Πλαίσιο κινδύνου

Για το σύστημα ΑΙΟΛΟΣ, παρατηρούνται πιθανές απειλές με μέτριο έως σημαντικό αντίκτυπο τόσο στο λογισμικό μισθοδοσίας, όσο και στην Oracle βάση δεδομένων..

Η υποδομή ΒΔ Oracle **δεν** επεξεργάζεται ευαίσθητα προσωπικά δεδομένα κατά ορισμό ΓΚΠΔ, με αποτέλεσμα ο αντίκτυπος παραβίασής τους να μην είναι μέγιστης επικινδυνότητας.

Και τα δύο αυτά αγαθά παρέχονται από εξωτερικό χώρο του συστήματος, γι' αυτό δεν χάνεται το ποσό της αρχικής επένδυσης σε αυτά υπό καμία συνθήκη εντός του ελέγχου μας. Σε περίπτωση απώλειας των αγαθών του χώρου, το λογισμικό επανεγκαθίσταται και η φυσική μορφή της βάσης δεδομένων λειτουργεί ανεξάρτητα.

Απειλούνται τα δεδομένα καθώς αποστέλονται και διαβάζονται ως προς C/I/A, η ζωντανή χρήση των εφαρμογών ως προς A και τα δεδομένα backup της δομής Oracle ως προς C/I/A (Λόγω της ασφάλειας ερμάριου και του χώρου, θεωρείται κυρίως I/A).

3.2 Σχέδιο ασφάλειας: Προτεινόμενα αντίμετρα

Virtual Firewall

Είναι κρίσιμο πρόβλημα ότι δεν παρέχεται επαγγελματικό Firewall στο σύστημα, το οποίο το καθιστά ευάλωτο σε κυβερνοεπιθέσεις που απειλούν την εμπιστευτικότητα και ακεραιότητα των δεδομένων της βάσης και του λογισμικού μισθοδοσίας, καθώς και την ολική διαθεσιμότητα των εφαρμογών. Προτείνεται η παροχή ενός επαγγελματικού Virtual Firewall λόγω της VM δομής.

Long-life HDD

Οι κασέτες backup έχουν μεγάλη αβεβαιότητα ως προς τον χρόνο ζωής λόγω της απομαγνητοποίησης του υλικού, θέτοντας σε υψηλό κίνδυνο την ακεραιότητα και διαθεσιμότητα των δεδομένων backup. Να σημειώνεται ότι το πρωτόκολλο backup συμβάλλει σημαντικά στην φήμη του οργανισμού. Επομένως, συστήνεται η χρήση μακροχρόνιων εταιρικών HDD, κατασκευασμένοι για αποθήκευση backup δεδομένων. Συμπληρωματικά, θα ακολουθείται πλάνο περιοδικών ελέγχων και διατήρησης των δίσκων.

UPS system

Το σύστημα βρίσκεται σε διεύθυνση που ενδέχεται να παρουσιάσει διακοπές ρεύματος μέχρι δεκάδες φορές τον χρόνο. Θεωρείται σκόπιμο να στηθεί σύστημα UPS που θα παρέχει 24ωρη ενέργεια σε περίπτωση διακοπής. Είναι απαραίτητο για την ακεραιότητα δεδομένων σε περίπτωση διακοπής αλλά και της διαθεσιμότητας του συστήματος για διαδικασίες μισθοδοσίας.

Σύστημα πυρόσβεσης αερίου Novec 1230

Οι χώροι πληροφοριακών συστημάτων είναι απαγορευτικό να λειτουργούν με σύστημα πυρόσβεσης νερού, το οποίο είναι η προκειμένη περίπτωση. Σε λειτουργία προκαλεί βραχυκύκλωμα επηρεάζοντας την πρόσφατη ακεραιότητα δεδομένων αλλά και την διαθεσιμότητα των συστημάτων μισθοδοσίας και βάσης δεδομένων. Οφείλει να γίνει επένδυση σε μοντέρνο σύστημα πυρόσβεσης αερίου. Συστήνεται λόγω τιμής και αποτελεσματικότητας το Novec 1230 που προσφέρει υπηρεσίες στην Ελλάδα.

3.3 Αποδεκτές απειλές

- Υλική φυσική κλοπή: Χαμηλό ρίσκο, ακολουθούνται αποτελεσματικά πρωτόκολλα φυσικής ασφάλειας ήδη. (Αξιολόγηση: Χαμηλή)
- Πλημμύρα: Υπάρχει υψηλό ρίσκο λόγω της παραθαλάσσιας περιοχής. Ωστόσο, το υπόγειο κτήριο είναι ήδη διαφυλασσόμενο σωστά από πλημμύρα. (Αξιολόγηση: Μέτρια-Χαμηλή)
- Βλάβη Hardware: Το υλικό είναι υψηλής ποιότητας, η βλάβη δεν είναι αρκετά πιθανή. Προγραμματίζονται ήδη έλεγχοι μηνιαία για την διατήρησή του. (Αξιολόγηση: Χαμηλή)

- Σοβαρός σεισμός: Η Καλλιθέα έχει υψηλή σεισμική δραστηριότητα, ωστόσο η υποδομή του κτιρίου είναι μοντέρνα και αντιστέκεται, καθώς και το Hardware είναι σχετικά ασφαλώς στημένο για ανθεκτικότητα σε σεισμούς. (Αξιολόγηση: Μέτρια)

4 Ανάλυση επικινδυνότητας

4.1 PTA

Τα Screenshots είναι επίσης συνημμένα στο .zip αρχείο
Αξιοποιήθηκε το πρότυπο ISO 27005

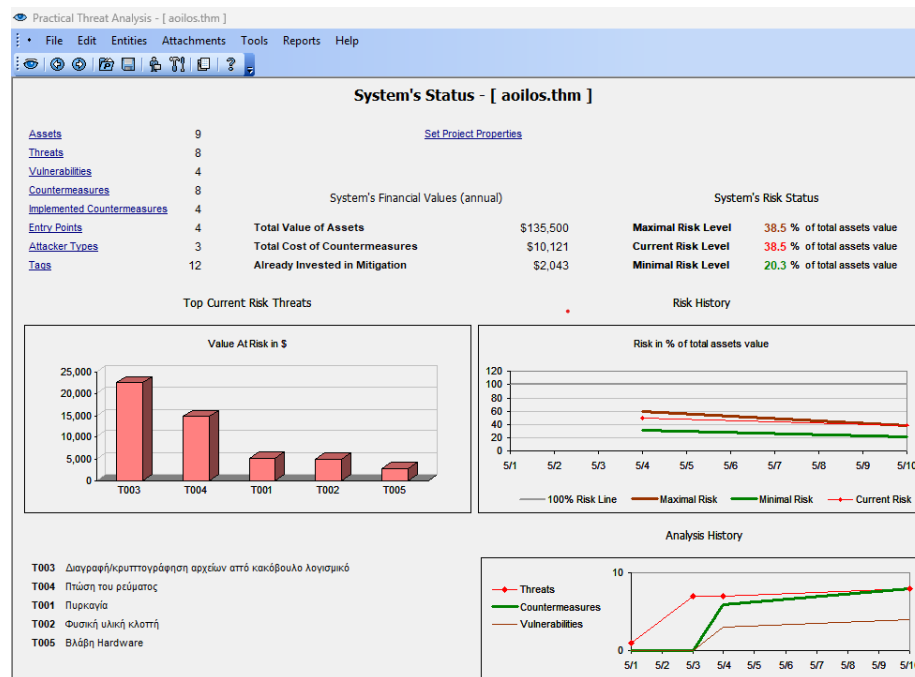


Figure 2: System's Status

Mitigation Simulator Results

This report presents the results of the current simulation session performed with the Mitigation Simulator tool. The main output is a list of countermeasures which form a mitigation plan that should be implemented in order to reduce the system's risk to a specified target level. For each of the countermeasures in the simulated mitigation plan, the report displays basic information as well as the countermeasure's annual implementation cost. For more information click the 'Help on Current Screen' button.

Sort By

Countermeasure Cost

Simulated Risk Status		
(in % of total system assets value)		
Maximal Risk Level	38.5	%
Current Risk Level	38.5	%
Minimal Risk Level	20.3	%
Simulated Risk Level	20.3	%
System's Financial Values (annual)		
Total Value of Assets	\$135,500	
Total Cost of Countermeasures	\$10,121	
Already Invested in Mitigation	\$2,043	
Simulated Mitigation Cost	\$8,078	
Simulated Mitigation Level (in %)	18.2	

C003 Σύστημα παροχής ρεύματος (UPS)

Implementation Cost : \$3,700

C007 Σύστημα πυρόσβεσης Novec 1230 (αερίου)

Implementation Cost : \$2,411

C006 Χρήση Virtual Firewall

Implementation Cost : \$1,500

Saturday, May 10, 2025

Page 1 of 2

C008 Enterprise HDD backups

Implementation Cost : \$467

Figure 3: Mitigation Simulator Results

Optimized Risk Reduction Plan

This analysis report presents a recommended sequence of mitigation steps that will reduce the system's risk to a given target level in the most cost-effective way. Each step in the plan is comprised of countermeasures that should be implemented in order to achieve the step's contribution to risk reduction. For more information click the 'Help on Current Screen' button.

System's Risk Status		
(in % of total system assets value)		
Maximal Risk Level	38.5	%
Current Risk Level	38.5	%
Minimal Risk Level	20.3	%

1

List of countermeasures that should be implemented in step: 1

C006 Χρήση Virtual Firewall

Costs

Countermeasure Implementation :	\$1,500
Accumulated per Step :	\$1,500
Accumulated per Plan :	\$1,500

Risk remaining after implementation of step's countermeasures: 30.4 %

2

List of countermeasures that should be implemented in step: 2

C008 Enterprise HDD backups

Costs

Countermeasure Implementation :	\$467
Accumulated per Step :	\$467
Accumulated per Plan :	\$1,967

Figure 4: Optimized Risk Reduction Plan (1/2)

Risk remaining after implementation of step's countermeasures: 29.6 %

3

List of countermeasures that should be implemented in step: 3

C007 Σύστημα πυρόσβεσης Novec 1230 (αερίου)

Costs

Countermeasure Implementation : \$2,411

Accumulated per Step : \$2,411

Accumulated per Plan : \$4,378

Risk remaining after implementation of step's countermeasures: 25.8 %

4

List of countermeasures that should be implemented in step: 4

C003 Σύστημα παροχής ρεύματος (UPS)

Costs

Countermeasure Implementation : \$3,700

Accumulated per Step : \$3,700

Accumulated per Plan : \$8,078

Risk remaining after implementation of step's countermeasures: 20.3 %

Figure 5: Optimized Risk Reduction Plan (2/2)

Detailed Threats

This report presents a list of all system's threats which meet Tags Filter criteria, sorted according to the specified Sort By field. The report shows all assets, vulnerabilities, countermeasures, entry points, attacker types and tags associated with each threat. In addition, it displays the relevant calculative parameters such as level of damage and mitigation. For more information click the 'Help on Current Screen' button.

Tags Filter	No Filter
Sort By	Current Risk Level

T003	Διαγραφή/κρυπτογράφηση αρχείων από κακόβουλο λογισμικό
Description:	
Μέσω ανθρώπινου λάθους, επίθεσης στο δίκτυο ή σκόπιμης φυσικής επίθεσης, ένα κακόβουλο λογισμικό όπως Ransomware, καταστρέφει τα αρχεία.	
Risk	
Current:	16.6 %
Maximal:	16.6 %
Minimal:	8.5 %
Probability:	3.00
Damage:	5.5 % of total assets value
Maximal Mitigation Available:	49.0 %
Threatened Assets:	
A006 Oracle Database	
Level of Damage : 33 %	
A005 Λογισμικό μισθοδοσίας	
Level of Damage : 100 %	
Exploited Vulnerabilities:	
V003 Έλλειψη ασφάλειας από τροποποίηση/διαγραφή αρχείων	
Δεν υπάρχουν μέτρα για να αντιμετωπίσουν την σκόπιμη/ακούσια τροποποίηση αρχείων	
Recommended Countermeasures:	
C004 Backups Βάσης δεδομένων μαγνητικών κασετών	
62 backups για το τελευταίο τρίμηνο. Σε περίπτωση που χαθούν πρόσφατα αρχεία, μπορούμε να τα επαναφέρουμε.	
Included in Mitigation Set V	
C005 Μέτρα εξουσιοδότησης για τροποποίηση των λογισμικών DB/Payroll	
Αναλυτική παροχή μέτρων που εξουσιοδοτούν σε συγκεκριμένους υπαλλήλους να τροποποιούν δεδομένα στην βάση δεδομένων.	
Included in Mitigation Set V	

Figure 6: Detailed Threats 1/11

C006 Χρήση Virtual Firewall

Ένα εύρωστο virtual firewall εγγυάται την ασφαλή λειτουργία των VM που επικοινωνούν με την βάση δεδομένων. Οδηγώντας στην ασφάλεια του συστήματος από Ransomware επιθέσεις και μη εξουσιοδοτημένη τροποποίηση των δεδομένων μέσω του δικτύου.

Included in Mitigation Set V

Entry Points:

E003 Άνοιγμα κακόβουλου λογισμικού από Phishing επίθεση

Attacker Types:

K003 Επιτηθέμενος hacker/ απαταιώνας phishing

Tags:

G005 Crucial availability

G011 Crucial Integrity

G010 High likelihood

Figure 7: Detailed Threats (2/11)

T004 Πτώση του ρεύματος

Description:

Αποσυνδέεται το ρεύμα για μία περίοδο, διακόπτοντας την λειτουργία των αγαθών.

Risk Current: **11.0 %**
 Maximal: **11.0 %**
 Minimal: **5.5 %**

Probability: 5.00

Damage: 2.2 % of total assets value

Maximal Mitigation Available: 50.0 %

Threatened Assets:

A006 Oracle Database
 Level of Damage : 16 %

A005 Λογισμικό μισθοδοσίας
 Level of Damage : 16 %

Exploited Vulnerabilities:

V002 Αστάθεια δικτύου ρεύματος

Το δίκτυο ρεύματος στην περιοχή είναι ασταθές και δημιουργεί προβλήματα διαθεσιμότητας των υπηρεσιών.

Recommended Countermeasures:

C003 Σύστημα παροχής ρεύματος (UPS)

Το τροφοδοτικό αδιάληπτης παροχής ενέργειας μπορεί να διατηρήσει ένα τοπικό δίκτυο ρεύματος στην περίπτωση που πέσει το δίκτυο της περιοχής/τοπικής περιφέρειας.

Included in Mitigation Set V

Entry Points:

Attacker Types:

Tags:

G010 High likelihood

G005 Crucial availability

Figure 8: Detailed Threats (3/11)

T001 Πυρκαγιά

Description:

Η παρουσίαση πυρκαγιάς στον χώρο των αγαθών.

Risk Current: 3.8 %
 Maximal: 3.8 %
 Minimal: 0.0 %

Probability: 0.33

Damage: 11.5 % of total assets value

Maximal Mitigation Available: 100.0 %

Threatened Assets:

A006 Oracle Database
 Level of Damage : 82 %
A005 Λογισμικό μισθοδοσίας
 Level of Damage : 100 %

Exploited Vulnerabilities:

V001 Απουσία ασφαλούς συστήματος πυρανίχνευσης
 Δεν υπάρχει ή υπολειπεται φτωχό σύστημα πυρανίχνευσης, με αποτέλεσμα να μην προστατεύει τα αγαθά από πυρκαγιά.

Recommended Countermeasures:

C001 Σύστημα πυρανίχνευσης/καπνού
 Υπάρχει και διατηρείται ένα αξιόπιστο σύστημα πυρανίχνευσης στον χώρο των αγαθών
 Included in Mitigation Set
C002 Αυτόματο σύστημα πυρόσβεσης νερού
 Σύστημα που αυτόματα προειδοποιεί και σβήνει την φωτιά έγκαιρα. (Μειωμένο κόστος, προϋποθέτοντας ότι υπάρχει εγκατάσταση πυρανίχνευσης.
 Included in Mitigation Set
C007 Σύστημα πυρόσβεσης Novec 1230 (αερίου)
 Εγκατάσταση συστήματος απόσβεσης της φωτιάς με Novec 1230, φιλικό σε ηλεκτρονικές συσκευές.
 Included in Mitigation Set V

Entry Points:

E001 Υψηλή θερμοκρασία και εύλεκτος χώρος

Attacker Types:

K001 Περιβάλλον

Figure 9: Detailed Threats (4/11)

T002 Φυσική υλική κλοπή**Description:**

Η φυσική κλοπή του υλικού από κλέφτη στον χώρο.

Risk Current: 3.6 %
 Maximal: 3.6 %
 Minimal: 3.6 %

Probability: 0.33

Damage: 11.0 % of total assets value

Maximal Mitigation Available: 0.0 %

Threatened Assets:

A006 Oracle Database
 Level of Damage : 82 %
A005 Λογισμικό μισθοδοσίας
 Level of Damage : 66 %

Exploited Vulnerabilities:**Recommended Countermeasures:****Entry Points:****Attacker Types:****Tags:**

G005 Crucial availability
G012 Crucial confidentiality
G011 Crucial Integrity
G009 Rare occurrence

Figure 10: Detailed Threats 5/11

T005 Βλάβη Hardware**Description:**

Δυσλειτουργία του Hardware υλικού, είτε για λόγους συντήρησης, είτε γενικά.

Risk Current: 2.0 %
 Maximal: 2.0 %
 Minimal: 2.0 %

Probability: 0.33

Damage: 6.1 % of total assets value

Maximal Mitigation Available: 0.0 %

Threatened Assets:

A006 Oracle Database
 Level of Damage : 50 %
A005 Λογισμικό μισθοδοσίας
 Level of Damage : 0 %

Exploited Vulnerabilities:**Recommended Countermeasures:****Entry Points:****Attacker Types:****Tags:**

G005 Crucial availability
G011 Crucial Integrity

Figure 11: *Detailed Threats (6/11)*

T005 Βλάβη Hardware**Description:**

Δυσλειτουργία του Hardware υλικού, είτε για λόγους συντήρησης, είτε γενικά.

Risk Current: 2.0 %
 Maximal: 2.0 %
 Minimal: 2.0 %

Probability: 0.33

Damage: 6.1 % of total assets value

Maximal Mitigation Available: 0.0 %

Threatened Assets:

A006 Oracle Database
 Level of Damage : 50 %
A005 Λογισμικό μισθοδοσίας
 Level of Damage : 0 %

Exploited Vulnerabilities:**Recommended Countermeasures:****Entry Points:****Attacker Types:****Tags:**

G005 Crucial availability
G011 Crucial Integrity

Figure 12: Detailed Threats (7/11)

T008 Απομαγνητισμός κασετών backups**Description:**

Οι κασέτες των backup δεδομένων της βάσης δεδομένων πρόκειται να απομαγνητοποιηθούν με την πάροδο του χρόνου. Οδηγώντας σε κρίσιμο κίνδυνο να χαθούν όλα τα δεδομένα backup.

Risk Current: 1.0 %
 Maximal: 1.0 %
 Minimal: 0.2 %

Probability: 0.50

Damage: 2.0 % of total assets value

Maximal Mitigation Available: 82.0 %

Threatened Assets:

A006 Oracle Database
Level of Damage : 16 %

Exploited Vulnerabilities:

V004 Χρήση μαγνητικών κασετών αντί για άλλα αξιόπιστα συστήματα/υλικό
Η χρήση μαγνητικών κασετών είναι μικράς χρονικής ζωής.

Recommended Countermeasures:

C008 Enterprise HDD backups
Η χρήση long-term επιβίωσης δίσκων για backup. (Τύπου BackupChain)
Included in Mitigation Set V

Entry Points:

E004 Απομαγνητοποίηση της κασέτας

Attacker Types:

K001 Περιβάλλον

Tags:

G010 High likelihood
G005 Crucial availability
G011 Crucial Integrity

Figure 13: Detailed Threats (8/11)

T007 Σοβαρός σεισμός

Description:

Ένας σεισμός υψηλού ριχτερ διαταράσσει την λειτουργία ή προκαλεί ζημιά στο υλικό.

Risk Current: 0.4 %
 Maximal: 0.4 %
 Minimal: 0.4 %

Probability: 0.10

Damage: 4.3 % of total assets value

Maximal Mitigation Available: 0.0 %

Threatened Assets:

A005 Λογισμικό μισθοδοσίας
Level of Damage : 16 %

A006 Oracle Database
Level of Damage : 33 %

Exploited Vulnerabilities:

Recommended Countermeasures:

Entry Points:

Attacker Types:

Tags:

G005 Crucial availability
G011 Crucial Integrity
G009 Rare occurrence

Figure 14: Detailed Threats (9/11)

T006 Πλημμύρα**Description:**

Πλημμύρα στον χώρο διαταράσσει την λειτουργία των αγαθών και πιθανό δημιουργεί ζημιά σε αυτά.

Risk Current: 0.1 %
 Maximal: 0.1 %
 Minimal: 0.1 %

Probability: 0.01

Damage: 6.2 % of total assets value

Maximal Mitigation Available: 0.0 %

Threatened Assets:

 A005 Λογισμικό μισθοδοσίας
 Level of Damage : 16 %
 A006 Oracle Database
 Level of Damage : 49 %

Exploited Vulnerabilities:**Recommended Countermeasures:****Entry Points:****Attacker Types:****Tags:**

 G009 Rare occurrence
 G005 Crucial availability
 G011 Crucial Integrity

Figure 15: Detailed Threats (10/11)

T006 Πλημμύρα**Description:**

Πλημμύρα στον χώρο διαταράσσει την λειτουργία των αγαθών και πιθανό δημιουργεί ζημιά σε αυτά.

Risk Current: 0.1 %
 Maximal: 0.1 %
 Minimal: 0.1 %

Probability: 0.01

Damage: 6.2 % of total assets value

Maximal Mitigation Available: 0.0 %

Threatened Assets:

 A005 Λογισμικό μισθοδοσίας
 Level of Damage : 16 %
 A006 Oracle Database
 Level of Damage : 49 %

Exploited Vulnerabilities:**Recommended Countermeasures:****Entry Points:****Attacker Types:****Tags:**

 G009 Rare occurrence
 G005 Crucial availability
 G011 Crucial Integrity

Figure 16: Detailed Threats (11/11)

Model Completeness

This self-diagnosing report is intended to help in assessing the completeness and robustness of the current PTA threat model. For each of the model's entity types (Threats, Assets, Vulnerabilities and Countermeasures) it displays a table with a checklist of conditions which the entity should fulfill in order to be part of a 'well behaved' threat model. Entities conditions which are not fulfilled, and hence may weaken the model's productivity, are marked in red. For more information click the 'Help on Current Screen' button.

Model Entities	
Threats	8
Assets	9
Vulnerabilities	4
Countermeasures	8

Threats

ID	Has Unique Name	Exploits Vulnerabilities	Threatens Assets	Causes Damage	Occurs
T001	Yes	Yes	Yes	Yes	Yes
T002	Yes	No	Yes	Yes	Yes
T003	Yes	Yes	Yes	Yes	Yes
T004	Yes	Yes	Yes	Yes	Yes
T005	Yes	No	Yes	Yes	Yes
T006	Yes	No	Yes	Yes	Yes
T007	Yes	No	Yes	Yes	Yes
T008	Yes	Yes	Yes	Yes	Yes

Assets

ID	Has Unique Name	Threatened by Threats	Is Damaged	Has Value
A005	Yes	Yes	Yes	Yes
A006	Yes	Yes	Yes	Yes

Figure 17: Model Competitiveness (1/2)

Vulnerabilities

ID	Has Unique Name	Exploited by Threats	Has Countermeasures
V001	Yes	Yes	Yes
V002	Yes	Yes	Yes
V003	Yes	Yes	Yes
V004	Yes	Yes	Yes





















Countermeasures

ID	Has Unique Name	Mitigates Vulnerabilities	Mitigates Threats	Has Cost
C001	Yes	Yes	Yes	Yes
C002	Yes	Yes	Yes	Yes
C003	Yes	Yes	Yes	Yes
C004	Yes	Yes	Yes	Yes
C005	Yes	Yes	Yes	Yes
C006	Yes	Yes	Yes	Yes
C007	Yes	Yes	Yes	Yes
C008	Yes	Yes	Yes	Yes

Figure 18: Model Completeness (2/2)

4.2 SimpleRisk

Η ανάλυση SimpleRisk υλοποιήθηκε από το Docker Image του. Αξιοποιήθηκε η πολιτική NIST 800-171 στην αυτοαξιολόγηση του συστήματος και το πρότυπο ISO 27005.

Actions	Asset Name	IP Address	Asset Valuation	Site/Location	Team	Asset Details	Tags
	Asset Name	IP Address	Asset Valuation	Site/Location	Team	Asset Details	Tags
 	Backup cassette		\$0 to \$10,000	Εργασια	Data Center & Storage	60 μηχανικές κοπτικές ημερήσιων backups και 2 κοπτικές μηνιαίων backups.	Add tags View tags
 	CD/DVDs in use		\$0 to \$10,000	Εργασια	Data Center & Storage	Υποστηρικτικοί δίσκοι που υποστηρίζουν εφαρμογές του οργανισμού.	Add tags View tags
 	ESX Hypervisor Server	10.2.1.4	\$40,001 to \$50,000	Κτήρια AIDHCE	Web Systems	Ο LAN εξυπηρετητής που υποστηρίζει όλα τα VMs.	Critical Involability High cost Information Server
 	EXADATA Oracle Database	10.5.0.1	\$0 to \$10,000	Εξυπηρετησι Oracle DC	Database	Αποκεντρωμένη εξυπηρετησι βάση δεδομένων για το σύστημα μεγάλης κλίμακας.	Critical Involability High cost Information Software
 	HR Management System	10.2.1.20	\$0 to \$10,000	Κτήρια AIDHCE	IT Systems Management	Το λογισμικό HRMS που εκτελείται σε διακομιστή, υποστηρίζει κρίσιμες λειτουργίες.	Software
 	Playvid Software	10.2.1.10	\$0 to \$10,000	Κτήρια AIDHCE	IT Systems Management	Το λογισμικό που εκτελείται σε διακομιστή που υποστηρίζει τις διαδικασίες μεθοδεύσεις.	Software
 	Red Hat Enterprise Linux (OS)		\$0 to \$10,000	Κτήρια AIDHCE	Unix	Αποκεντρωμένη πύλη του οργανισμού, βασικά για διαδικασίες ασφαλείας, είναι αναγκαία για την εκτέλεση της 9.2.	Software
 	Server physical contracts		\$0 to \$10,000	Εργασια	Data Center & Storage	Φυσική συμβολή από την εγκατάσταση του εξυπηρετητή.	Add tags View tags
 	Server αποδοτικότητα χρήσης	10.2.0.1	\$30,001 to \$40,000	Κτήρια AIDHCE	Web Systems	Ο εξυπηρετητής που διατηρεί την διαθεσιμότητα των εφαρμογών κατά την επικοινωνία τους με την εξυπηρετησι βάση.	Critical Involability High cost Information Server
 	Ασφάλεια Κινηματογράφου	10.3.0.3	\$0 to \$10,000	Κτήρια AIDHCE	Network	Σύστημα ασφαλείας για έλεγχο της εισερχόμενης θερμοκρασίας.	Physical Security

Showing 1 to 10 of 13 entries

First Previous 1 2 Next Last Show All

Manage Assets

Verified Assets

Unverified Assets

Delete All

10 entries per page

Actions

Asset Name

IP Address

Asset Valuation

Site/Location

Team

Asset Details

Tags

Asset Name

IP Address

Asset Valuation

Site/Location

Team

Asset Details

Tags

	Ασφάλεια Κινηματογράφου	10.3.0.2	\$0 to \$10,000	Κτήρια AIDHCE	Network	Σύστημα ασφαλείας για καταγραφή της υφιστάμενης του εκτελεστικού χώρου.	[Physical Security](#)
	Κινηματογράφος εγκατάστασης		\$40,001 to \$100,000			Η εγκατάσταση του κτιρίου.	[High cost](#) [Information](#)
	Συνταγματική Προστασία	10.3.0.4	\$0 to \$10,000	Κτήρια AIDHCE	Network	Συνταγματική προστασία δεδομένων με επί ασφαλείας.	[Physical Security](#)

Showing 11 to 13 of 13 entries

Delete All

First Previous 1 2 Next Last Show All

Figure 19: Assets

Review Regularly

Below is the list of all risks sorted by Unreviewed, Past Due, and Next Review Date.

10▼

entries per page

ID	Status	Subject	Inherent Risk (Current)	Days Open	Next Review Date
1004	Mgmt Reviewed	Πίσση του πείρατος	7	4	08/16/2025
1001	Mgmt Reviewed	Παραγωγή	6.5	5	11/14/2025
1003	Mgmt Reviewed	Διατροφή/κυκλοφορήση αρχείων από κοινόβουλο λογισμικό	6.5	4	11/14/2025
1008	Mgmt Reviewed	Απομακρυντικός κωδικών backup	6	4	11/14/2025
1002	Mgmt Reviewed	Υψος φυσική αλληλ	5.75	4	11/14/2025
1006	Mgmt Reviewed	Πλημμύρα	5	4	11/14/2025
1005	Mgmt Reviewed	Βλάβη Hardware	4	4	11/14/2025
1007	Mgmt Reviewed	Συβαρής ασφαλείας	3.5	4	05/13/2026

Showing 1 to 8 of 8 entries

FirstPrevious1NextLastShow All

Figure 20: review plans for threats

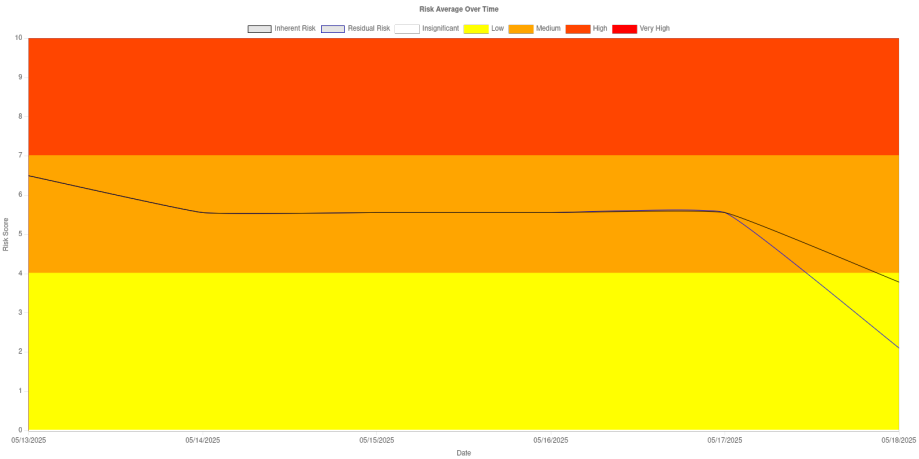


Figure 21: risk average over time

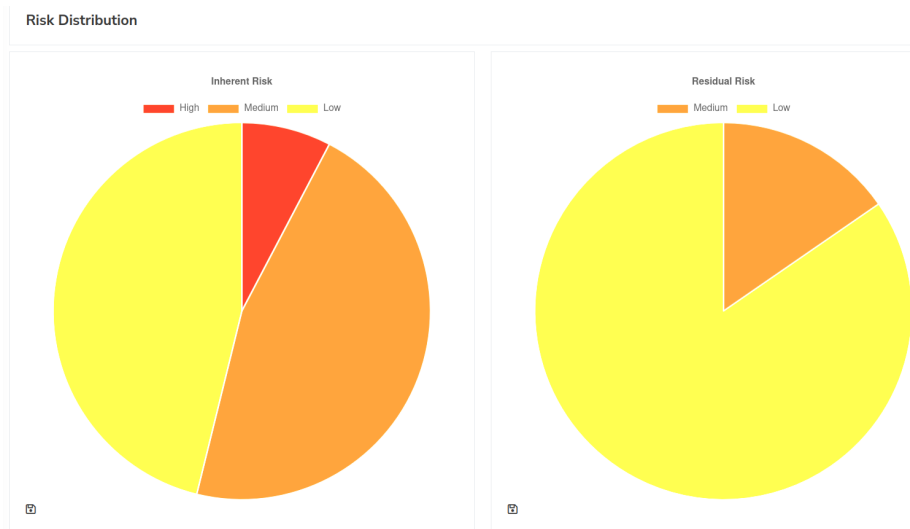


Figure 22: Risk distribution

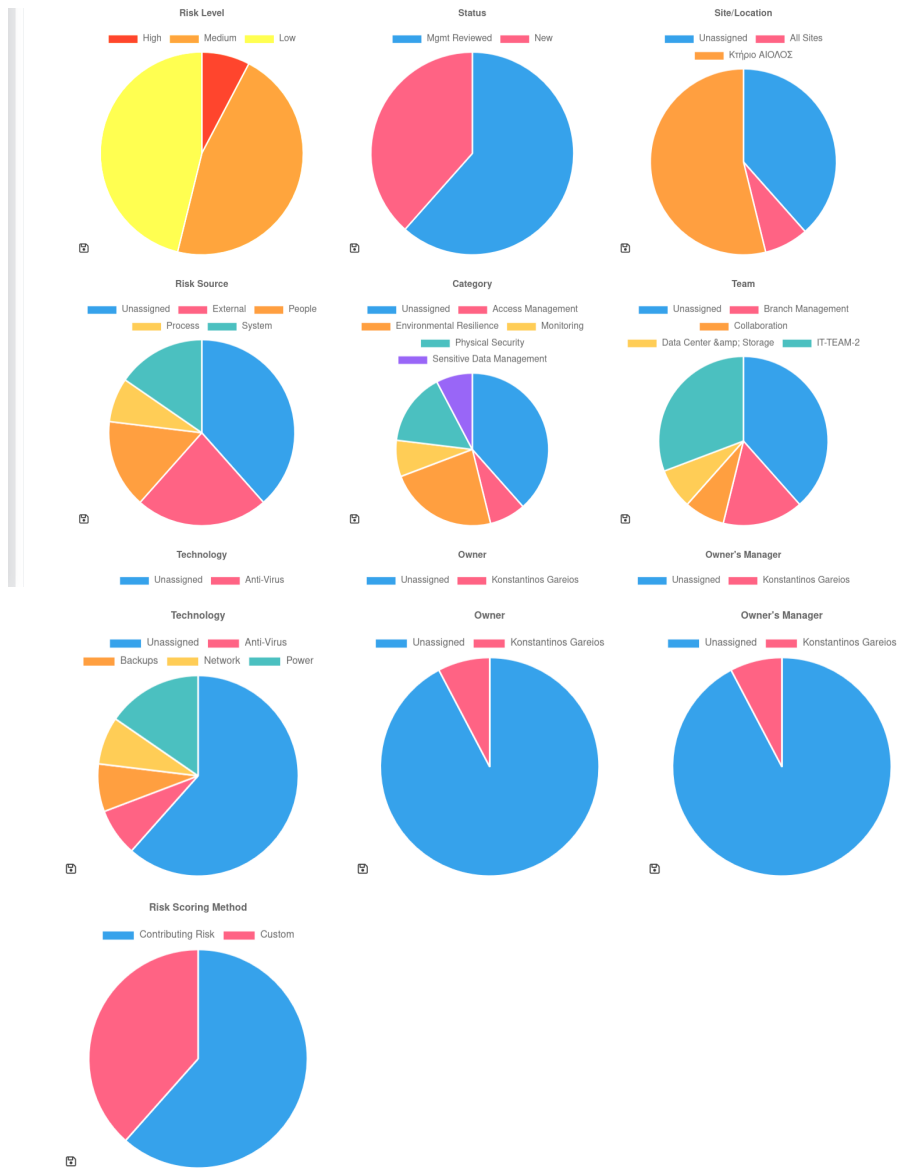


Figure 23: Pie charts

5 Υποθέσεις

- Ο Server αποκλειστικής χρήσης δρα ως Web Server.
- Απουσιάζει επαγγελματικό Firewall (εφόσον δεν αναφέρεται)
- Το σύστημα e-prescription είναι ανεξάρτητο από την βάση δεδομένων της ΓΓΠΣΔΔ που αξιοποιεί το παρόν σύστημα.
- Το κτήριο ΑΙΟΛΟΣ έχει χτιστεί με ισχυρή υποδομή για να αντιμετωπίζει πλημμύρες, λόγω της περιοχής. Δεν πλημμυρίζεται το εσωτερικό υλικό.
- Τηρούνται ήδη τακτικά ελέγχοι για το Hardware.
- Υπάρχει καλή ανθεκτικότητα του συστήματος για σεισμούς και το προσωπικό γνωρίζει να ακολουθεί αντισεισμικά πρωτόκολλα.