Όνομα Οργανισμού

Μεθοδολογία Διαχείρισης Κινδύνου

|  |  |
| --- | --- |
| **Περιεχόμενο:** | Μεθοδολογία Διαχείρισης Κινδύνου |
| **Δημιουργός:** |  |
| **Έκδοση:** | 1.0 |
| **Ημερομηνία Έκδοσης:** | ηη/μμ/χχχχ |
| **Εμπιστευτικότητα:** |  |
| **Ιδιοκτήτης:** |  |

Διανομή

| Ρόλος | Όνομα | Οργανισμός | Τοποθεσία | Αριθμός Αντιτύπων |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Καταγραφή Τροποποιήσεων

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Κατάσταση Έκδοσης | Έκδοση | Ημερομηνία | Ενέργειες από | Περιγραφή |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Αναφορές

|  |  |  |
| --- | --- | --- |
| **Αρ.** |  | **Αναφορά Εγγράφου** |
| 1 |  |  |
| 2 |  |  |
| 3 |  |  |

Υποστηρικτικό Υλικό

|  |  |
| --- | --- |
| **Αρ.** | **Αναφορά** |
| 1 |  |
| 2 |  |
| 3 |  |

Ειδικό Λεξιλόγιο

Οι όροι και συντμήσεις ορίζονται πιο κάτω:

| Όροι και συντμήσεις | Περιγραφή |
| --- | --- |
|  |  |
|  |  |
|  |  |

Πίνακας Περιεχομένων

[1. Εισαγωγή 5](#_Toc155250106)

[1.1. Ορισμός Πεδίου Εφαρμογής Εκτίμησης Κινδύνου 5](#_Toc155250107)

[2. Σκοπός της Εκτίμησης Κινδύνων 5](#_Toc155250108)

[3. Ρόλοι και Αρμοδιότητες 6](#_Toc155250109)

[4. Προσδιορισμός Στοιχείων Ενεργητικού 6](#_Toc155250110)

[4.1. Κατάλογος Στοιχείων Ενεργητικού 6](#_Toc155250111)

[5. Προσδιορισμός Πιθανών Απειλών 8](#_Toc155250112)

[6. Προσδιορισμός Πιθανών Ευπαθειών 8](#_Toc155250113)

[7. Προσδιορισμός Πιθανών Κινδύνων 8](#_Toc155250114)

[8. Προσδιορισμός Τύπων Κινδύνων 8](#_Toc155250115)

[8.1. Προσδιορισμός Ιδιοκτητών Κινδύνων 9](#_Toc155250116)

[8.2. Προσδιορισμός Υφιστάμενων Δικλείδων Ασφαλείας 9](#_Toc155250117)

[9. Κριτήρια Ανάλυσης Κινδύνου 9](#_Toc155250118)

[10. Κριτήρια Πιθανότητας 9](#_Toc155250119)

[11. Κριτήρια Επιπτώσεων 9](#_Toc155250120)

[12. Κριτήρια Βαθμολογίας Κινδύνου 10](#_Toc155250121)

[13. Διαδικασία Ανάλυσης / Αξιολόγησης Κινδύνων 11](#_Toc155250122)

[13.1. Συλλογή πληροφοριών 11](#_Toc155250123)

[13.2. Αξιολόγηση της πιθανότητας 12](#_Toc155250124)

[13.3. Αξιολόγηση των επιπτώσεων 12](#_Toc155250125)

[14. Αντιμετώπιση Κινδύνου 12](#_Toc155250126)

[15. Κριτήρια Αποδοχής Κινδύνων 12](#_Toc155250127)

[16. Πολιτική Ανάληψης Κινδύνων 13](#_Toc155250128)

[16.1. Στρατηγικές Αντιμετώπισης Κινδύνου 13](#_Toc155250129)

[17. Επιλογή Μέτρων Αντιμετώπισης Κινδύνου 13](#_Toc155250130)

[17.1. Μητρώο Κινδύνων 14](#_Toc155250131)

[17.2. Σχέδιο εφαρμογής για τα μέτρα ασφάλειας δικτύων και πληροφοριών (Action Plan) 14](#_Toc155250132)

[17.3. Δήλωση Εφαρμογής Πλαισίου (Statement of Applicability) 14](#_Toc155250133)

[18. Διαδικασία Εκτίμησης και Αντιμετώπισης Κινδύνου 15](#_Toc155250134)

[18.1. Διάγραμμα διαδικασίας 15](#_Toc155250135)

[18.2. Αναθεώρηση Αξιολόγησης Κινδύνων 16](#_Toc155250136)

[18.3. Διαδικασία Αξιολόγησης της Αποτελεσματικότητας των Εφαρμοζόμενων Μέτρων 16](#_Toc155250137)

[Παράρτημα Α – Κατάλογος Στοιχείων Ενεργητικού 17](#_Toc155250138)

[Παράρτημα Β – Κατάλογος Απειλών 20](#_Toc155250139)

[Παράρτημα Γ – Κατάλογος Ευπαθειών 22](#_Toc155250140)

[Παράρτημα Δ – Κριτήρια Επιπτώσεων Κινδύνων 28](#_Toc155250141)

# Εισαγωγή

Σκοπός του παρόντος εγγράφου είναι να θεσπιστεί η μεθοδολογία για τη διαχείριση κινδύνων μέσω του καθορισμού της διαδικασίας εκτίμησης κινδύνων, των κριτηρίων ανάλυσης κινδύνου, των κριτηρίων αποδοχής κινδύνων και της πολιτικής ανάληψης κινδύνων από τον οργανισμό.

Η μεθοδολογία διαχείρισης κινδύνου επιτρέπει στον οργανισμό να αξιολογεί τους κινδύνους για την ασφάλεια πληροφοριών που αντιμετωπίζει, και να εφαρμόσει τα κατάλληλα μέτρα για την αντιμετώπιση ή τον μετριασμό τους.

Στο έγγραφο αυτό καθορίζεται ο τρόπος με τον οποίο εκτελείται η διαδικασία διαχείρισης και εκτίμησης κινδύνου, έτσι ώστε να εντοπίζονται, να αξιολογούνται, να αντιμετωπίζονται και να διαχειρίζονται τους κινδύνους του οργανισμού, με βάση το Κ.Δ.Π 389/2020.

# Ορισμός Πεδίου Εφαρμογής Εκτίμησης Κινδύνου

Ο προσδιορισμός και ο ορισμός του πεδίου εφαρμογής της εκτίμησης κινδύνου. Συνήθως, ο ορισμός πεδίου εφαρμογής περιλαμβάνει, ποια τμήματα του οργανισμού πρόκειται να συμπεριληφθούν, με βάση την επιχειρηματική μονάδα, την υπηρεσία, τη γραμμή, τη γεωγραφία, τη δομή του οργανισμού ή άλλα μέσα.

# Σκοπός της Εκτίμησης Κινδύνων

Ο σκοπός ή οι λόγοι για τους οποίους θα πρέπει να διενεργείται εκτίμηση κινδύνου, είναι για να βοηθήσει τον [Όνομα Οργανισμού] να καταλάβει το εύρος της επικινδυνότητας των ρίσκων και να μπορέσει να τον διαχειριστεί. Επιπρόσθετα, μετριάζοντας τα ρίσκα που αναδειχθήκαν κατά την διάρκεια της αξιολόγησης, θα αποτρέψει και θα μειώσει τα δαπανηρά συμβάντα ασφάλειας και τις παραβιάσεις δεδομένων και θα αποφύγει ζητήματα κανονιστικών ρυθμίσεων και συμμόρφωσης.

# Ρόλοι και Αρμοδιότητες

|  |  |
| --- | --- |
| Ρόλος | Αρμοδιότητα |
| Υπεύθυνος Ασφάλειας Πληροφοριών | Διατηρεί ενημερωμένο μητρώο κινδύνων ασφάλειας πληροφοριών και σχεδίου μεταχείρισης, για λογαριασμό του οργανισμού. |
| Υπεύθυνος Κινδύνου | • Ένας κατάλληλος διευθυντής θα διοριστεί ως υπεύθυνος για κάθε κίνδυνο.• Θα παρέχει διασφάλιση ότι ο κίνδυνος εκτιμάται με ακρίβεια.• Θα παρέχει διασφάλιση ότι προτείνονται τα κατάλληλα μέτρα αντιμετώπισης.• Θα παρέχει διασφάλιση ότι ο κίνδυνος κοινοποιείται στα κατάλληλα μέρη. • Θα είναι υπεύθυνος για τη διασφάλιση ότι η υλοποίηση των μέτρων αντιμετώπισης των κινδύνων πραγματοποιείται εντός των συμφωνημένων χρονικών ορίων.• Αναμετάδοση ενημερώσεων. |
| Ανώτατη Διοίκηση | • Είναι υπεύθυνη για την αναθεώρηση των κινδύνων ασφαλείας πληροφοριών που θεωρούνται σημαντικοί ή κρίσιμοι (ώστε να επιβεβαιωθεί ότι εφαρμόζονται κατάλληλα μέτρα αντιμετώπισης).• Είναι υπεύθυνη για τη διασφάλιση ότι οι απαραίτητοι πόροι είναι διαθέσιμοι για την υποστήριξη αυτών των ενεργειών. |
| Υπάλληλοι | • Υποχρεούνται να ειδοποιούν τον Υπεύθυνο Ασφάλειας Πληροφοριών για τυχόν ζητήματα που αντιλαμβάνονται και ενδέχεται να αποτελούν, να υποδεικνύουν ή να προκαλούν κίνδυνο ασφάλειας πληροφοριών.• Απαιτείται να υποστηρίζουν την εφαρμογή όλων των μέτρων αντιμετώπισης κινδύνων που έχουν κριθεί απαραίτητα από τον Υπεύθυνο Κινδύνου ή την Ανώτερη Διοίκηση. |

# Προσδιορισμός Στοιχείων Ενεργητικού

Προσδιορισμός των Στοιχείων Ενεργητικού (Κατάλογος), συστημάτων και διαδικασιών εντός του οργανισμού και καταγραφή των εξαρτήσεων και αλληλεξαρτήσεων μεταξύ αυτών των στοιχείων ενεργητικού, των συστημάτων και των διαδικασιών με σκοπό τη σαφή αποτύπωση του πλαισίου / περιβάλλοντος στο οποίο θα πραγματοποιηθεί εκτίμηση κινδύνου. Η σαφής εικόνα του πλαισίου του οργανισμού θα επιτρέψει τον εντοπισμό των κινδύνων εντός του οργανισμού.

Παραδείγματα Στοιχείων Ενεργητικού περιλαμβάνονται στο Παράρτημα Α του παρόντος εγγράφου.

# Κατάλογος Στοιχείων Ενεργητικού

Σκοπός του Καταλόγου Στοιχείων Ενεργητικού είναι η παρακολούθηση της κατάστασης των στοιχείων / εξοπλισμού των δικτύων, συστημάτων πληροφοριών και ουσιωδών υπηρεσιών ως προς τη λειτουργική τους δυνατότητα και τις πιθανές βλάβες.

Ένα βασικό μέρος μιας εκτίμησης κινδύνου είναι ο προσδιορισμός της αξίας ενός στοιχείου ενεργητικού. Ελλείψει της αξίας ενός στοιχείου ενεργητικού, είναι πιο δύσκολο να υπολογιστούν οι κίνδυνοι που σχετίζονται με ένα στοιχείο ενεργητικού. Χωρίς μια γνωστή αποτίμηση, είναι δύσκολο να γνωρίζουμε τον αντίκτυπο της απώλειας.

Ο στόχος της αποτίμησης στοιχείων ενεργητικού είναι να καθορίσει ποια στοιχεία ενεργητικού έχουν μεγαλύτερη αξία από άλλα. Δίνει στον οργανισμό τη δυνατότητα να δει ποια στοιχεία ενεργητικού έχουν μεγαλύτερη αξία και ποια έχουν μικρότερη αξία. Αυτό είναι πολύ χρήσιμο για τον οργανισμό που έχει πολλά στοιχεία ενεργητικού, καθώς παρέχει μια άποψη για τα υψηλής αξίας στοιχεία ενεργητικού χωρίς τον «θόρυβο» των στοιχείων ενεργητικού χαμηλότερης αξίας.

Επίπεδα Αποτίμησης Στοιχείων Ενεργητικού:

* Χαμηλό
* Μέτριο
* Ψηλό

Τα κριτήρια / παράμετροι βάσει των οποίων ιεραρχούνται τα στοιχεία του δικτύου ως προς την κρισιμότητα / σημασία τους αναφορικά με το ρόλο τους στην υποστήριξη των ουσιωδών υπηρεσιών είναι τα εξής:

**Κόστος αντικατάστασης**

Εάν το στοιχείο ενεργητικού είναι στοιχείο ενεργητικού της κατηγορίας «Εξοπλισμός», η αποτίμησή του μπορεί να προσδιοριστεί ως το κόστος αγοράς (και εγκατάστασης) ενός ανταλλακτικού. Εάν το στοιχείο ενεργητικού είναι μια βάση δεδομένων, το κόστος του μπορεί να προσδιοριστεί ως το λειτουργικό κόστος για την επαναφορά του από τη δημιουργία αντιγράφων ασφαλείας ή το κόστος για την ανάκτησή του από την πηγή του, όπως ένας πάροχος υπηρεσιών.

**Λογιστική Αξία**

Αντιπροσωπεύει την αξία ενός στοιχείου ενεργητικού στο χρηματοοικονομικό σύστημα του οργανισμού, συνήθως την τιμή αγοράς μείον τις αποσβέσεις.

**Καθαρή παρούσα αξία**

Εάν το στοιχείο ενεργητικού δημιουργεί άμεσα ή έμμεσα έσοδα, μπορεί να χρησιμοποιηθεί αυτή η μέθοδος αποτίμησης.

**Κόστος Αναδιάταξης**

Εάν το στοιχείο ενεργητικού είναι μια εικονική μηχανή, η αποτίμηση του μπορεί να προσδιοριστεί ως το κόστος της εκ νέου εγκατάστασης του. Αυτό είναι συνήθως ένα χαμηλό κόστος εάν έχει συσταθεί από εσωτερικό προσωπικό, αλλά θα μπορούσε να είναι δύσκολο εάν μια άλλη εταιρεία προσληφθεί για την αναδιάταξη του.

**Κόστος δημιουργίας ή επανάκτησης**

Εάν το στοιχείο είναι μια βάση δεδομένων, το κόστος του μπορεί να προσδιοριστεί ως το κόστος της εκ νέου δημιουργίας του. Εάν το στοιχείο ενεργητικού είναι πνευματική ιδιοκτησία, όπως πηγαίος κώδικας λογισμικού, η αποτίμηση του μπορεί να προσδιοριστεί ως η προσπάθεια των προγραμματιστών να το δημιουργήσουν ξανά.

**Επακόλουθο χρηματοοικονομικό κόστος**

Εάν το στοιχείο ενεργητικού είναι μια βάση δεδομένων που περιέχει ευαίσθητα δεδομένα, η αποτίμησή τους μπορεί να μετρηθεί με τη μορφή χρηματοοικονομικού κόστους που προκύπτει από την κλοπή ή τον συμβιβασμό του. Ενώ το κόστος ανάκτησης αυτής της βάσης δεδομένων μπορεί να είναι σχετικά χαμηλό, οι συνέπειες του συμβιβασμού της θα μπορούσαν να κοστίσουν εκατοντάδες ευρώ ανά εγγραφή. Αυτό είναι ένα τυπικό κόστος κατά τη μέτρηση του συνόλου των επιπτώσεων μιας παραβίασης.

Η αξία του κάθε στοιχείου ενεργητικού λαμβάνεται υπόψη κατά την ανάλυση κινδύνου. Επίσης, λαμβάνει υπόψη την επιχειρηματική κρισιμότητα της κάθε διαδικασίας του οργανισμού η οποία εξαρτάται από το αντίστοιχο στοιχείο ενεργητικού.

Ο Κατάλογος Στοιχείων Ενεργητικού βρίσκεται στην Εργαλειοθήκη Αξιολόγησης Κινδύνου.

# Προσδιορισμός Πιθανών Απειλών

Για κάθε στοιχείο ενεργητικού, εντοπίζονται οι απειλές που εύλογα αναμένεται να ισχύουν για αυτό και που έχουν τη δυνατότητα να το βλάψουν.

Μια αρχική λίστα τυπικών απειλών περιλαμβάνεται στο Παράρτημα Β του παρόντος εγγράφου.

# Προσδιορισμός Πιθανών Ευπαθειών

Για κάθε στοιχείο ενεργητικού, εντοπίζονται και προσδιορίζονται οι περιστάσεις ή τα χαρακτηριστικά ενός περιστατικού στοιχείου που μπορεί να κεφαλαιοποιηθεί από οποιαδήποτε συγκεκριμένη απειλή. Μια ευπάθεια δεν προκαλεί ζημιά, αλλά η παρουσία της μπορεί να επιτρέψει σε ένα γεγονός απειλής να βλάψει ένα περιουσιακό στοιχείο.

Μια αρχική λίστα τυπικών ευπαθειών περιλαμβάνεται στο Παράρτημα του παρόντος εγγράφου.

# Προσδιορισμός Πιθανών Κινδύνων

Λαμβάνονται υπόψη κίνδυνοι που προκύπτουν από τυχαία ή παράνομη καταστροφή, απώλεια, αλλοίωση, άνευ αδείας κοινοποίηση ή πρόσβαση σε πληροφορίες που διαβιβάζονται, αποθηκεύονται ή υποβάλλονται κατ’ άλλο τρόπο σε επεξεργασία. Επίσης, λαμβάνονται υπόψη οι κίνδυνοι που παρουσιάζονται οι οποίοι θα μπορούσαν να επιδράσουν δυνητικά σε ουσιώδεις οικονομικές και κοινωνικές λειτουργίες και υπηρεσίες που παρέχονται από τον οργανισμό (Αξιολόγηση κινδύνων σχετικά με την Επιχειρησιακή Συνέχεια).

Μια αρχική λίστα πιθανών κινδύνων περιλαμβάνεται στο Παράρτημα Δ του παρόντος εγγράφου.

# Προσδιορισμός Τύπων Κινδύνων

Οι τύποι κινδύνων που θα προκύψουν για κάθε εντοπισμένη απειλή εναντίον κάθε στοιχείου ενεργητικού θα πρέπει να λαμβάνονται υπόψη κατά την αξιολόγηση κινδύνου. Οι τύποι κινδύνων μπορεί να είναι η απώλεια εμπιστευτικότητας, ακεραιότητας, διαθεσιμότητας ή αυθεντικότητας οποιουδήποτε στοιχείου ενεργητικού. Ανάλογα με τη φύση του στοιχείου ενεργητικού, οι συνέπειες μπορεί να λάβουν πολλές μορφές, συμπεριλαμβανομένης της διακοπής ή της υποβάθμισης των υπηρεσιών, της μείωσης της ποιότητας των υπηρεσιών, της απώλειας επιχειρήσεων, της βλάβης της φήμης ή των χρηματικών κυρώσεων, συμπεριλαμβανομένων των προστίμων.

Πιο κάτω φαίνονται οι τύποι κινδύνων μαζί με τις επεξηγήσεις τους:

Εμπιστευτικότητα: Διασφάλιση ότι οι πληροφορίες δεν είναι προσβάσιμες σε μη εξουσιοδοτημένους χρήστες, διαδικασίες ή άλλες οντότητες.

Ακεραιότητα: Διασφάλιση της συνέπειας, της ακρίβειας και της αξιοπιστίας των δεδομένων.

Διαθεσιμότητα: Διασφάλιση ότι οι πληροφορίες ή οι υπηρεσίες είναι προσβάσιμες όταν μια εξουσιοδοτημένη οντότητα απαιτεί πρόσβαση.

Αυθεντικότητα: Διασφάλιση ότι οι πληροφορίες είναι γνήσιες, έμπιστες και μπορούν να επαληθευτούν.

# Προσδιορισμός Ιδιοκτητών Κινδύνων

Ο οργανισμός πρέπει να εκχωρεί μεμονωμένους κινδύνους σε μεμονωμένους ανθρώπους, συνήθως μεσαίους έως ανώτερους ηγέτες διοίκησης. Οι ηγέτες αυτοί θα πρέπει να έχουν την κυριότητα των ελέγχων που λειτουργούν στο πλαίσιο του ελέγχου τους, καθώς και των πόρων που χρησιμοποιούνται σε καθημερινές επιχειρηματικές δραστηριότητες, όπως ο προϋπολογισμός, το προσωπικό και άλλα. Οι ιδιοκτήτες κινδύνων είναι τα άτομα που είναι υπεύθυνα για τις αποφάσεις κινδύνου, συμπεριλαμβανομένης της αντιμετώπισης κινδύνου.

# Προσδιορισμός Υφιστάμενων Δικλείδων Ασφαλείας

Οι δικλείδες ασφαλείας ή τα μέτρα ασφαλείας που υπάρχουν ήδη εντοπίζονται και εξετάζονται με σκοπό την διαπίστωση κατά πόσον είναι αποτελεσματικές. Τα κριτήρια για την εξέταση μιας δικλείδας ασφαλείας ή ενός μέτρου ασφαλείας περιλαμβάνουν εάν μειώνει την πιθανότητα ή τον αντίκτυπο ενός συμβάντος απειλής. Τα αποτελέσματα αυτής της εξέτασης καταλήγουν στο συμπέρασμα εάν ο έλεγχος είναι αποτελεσματικός, αναποτελεσματικός ή περιττός.

# Κριτήρια Ανάλυσης Κινδύνου

Για να αξιολογεί τον κίνδυνο για ένα στοιχείο ενεργητικού και να καθορίζει την κατάλληλη μεταχείριση, ο οργανισμός εξετάζει τις απειλές, τις ευπάθειες, την πιθανότητα να λάβει χώρα η απειλή και την επίπτωσή της σε περίπτωση που συμβεί. Χρησιμοποιείται κλίμακα 5 σημείων για να περιγράψει την πιθανότητα να λάβει χώρα ένας κίνδυνος και να περιγράψει την επίπτωση που είναι πιθανό να έχει.

# Κριτήρια Πιθανότητας

Η κλίμακα των 5 σημείων για την πιθανότητα κυμαίνεται από 1 = πολύ απίθανο έως 5 = σίγουρο, όπως φαίνεται πιο κάτω:

|  |  |  |
| --- | --- | --- |
| **Πιθανότητα** | **Περιγραφή** | **Περίληψη** |
| 1 | Πολύ απίθανο | Δεν έχει συμβεί ποτέ πριν και δεν υπάρχει λόγος να πιστεύουμε ότι είναι πιο πιθανό τώρα |
| 2 | Απίθανο | Υπάρχει πιθανότητα να συμβεί, αλλά μάλλον δεν θα συμβεί |
| 3 | Πιθανό | Συνολικά, ο κίνδυνος είναι πιο πιθανό να συμβεί παρά όχι |
| 4 | Πολύ πιθανό | Θα ήταν έκπληξη εάν ο κίνδυνος δεν εμφανιζόταν είτε με βάση τη συχνότητα του παρελθόντος είτε τις τρέχουσες συνθήκες |
| 5 | Σίγουρο | Είτε συμβαίνει ήδη τακτικά είτε υπάρχει κάποιος λόγος να πιστεύουμε ότι είναι σχεδόν επικείμενο |

# Κριτήρια Επιπτώσεων

Η επίπτωση αξιολογείται με βάση τις περιοχές επιπτώσεων που παρουσιάζονται παρακάτω,

* Αποφάσεις Διοίκησης
* Οικονομική / Άμεση Απώλεια Εσόδων / Κόστος
* Φήμη / Εμπιστοσύνη / Εικόνα
* Νομική / Κανονιστική Ευθύνη
* Απάτη

καθώς και το επίπεδο που θα επηρεαστούν αυτές οι περιοχές σε περίπτωση που διακυβευτεί η εμπιστευτικότητα, η ακεραιότητα, η διαθεσιμότητα και η αυθεντικότητα ενός στοιχείου ενεργητικού αντίστοιχα (Εκτίμηση επιπτώσεων).

Η υψηλότερη βαθμολογία εμπιστευτικότητας, ακεραιότητας, διαθεσιμότητας και αυθεντικότητας περιοχής αντίκτυπου θεωρείται ότι αξιολογεί την κρισιμότητα κάθε στοιχείου ενεργητικού, το οποίο είναι και πάλι η υψηλότερη βαθμολογία επιπτώσεων. Στη συνέχεια, η υψηλότερη βαθμολογία επιπτώσεων της αξιολόγησης της κρισιμότητας χρησιμοποιείται στην εκτίμηση επικινδυνότητας.

Το επίπεδο επιπτώσεων θα λάβει βαθμολογία με βάση τον συνδυασμό των 5 περιοχών καθώς και την επίπτωση που θα έχει ένα στοιχείο ενεργητικού εάν διακυβευτεί η εμπιστευτικότητα, η ακεραιότητα, η διαθεσιμότητά και η αυθεντικότητά του.

Κάθε μία από τις 5 περιοχές θα είναι ένας παρονομαστής για την εμπιστευτικότητα, την ακεραιότητα, τη διαθεσιμότητα και την αυθεντικότητα κάθε στοιχείου ενεργητικού και μια βαθμολογία θα παρέχεται χρησιμοποιώντας την κλίμακα 5 σημείων.

Η υψηλότερη βαθμολογία εμπιστευτικότητας, ακεραιότητας, διαθεσιμότητας και αυθεντικότητας περιοχής επιπτώσεων θεωρείται ότι αξιολογεί την κρισιμότητα κάθε στοιχείου ενεργητικού όπου η υψηλότερη από τις τρεις βαθμολογίες θεωρείται ως η τελική βαθμολογία επιπτώσεων.

Τα κριτήρια επιπτώσεων κινδύνων περιλαμβάνονται στο Παράρτημα Δ του παρόντος εγγράφου.

# Κριτήρια Βαθμολογίας Κινδύνου

Η ταξινόμηση κινδύνου που χρησιμοποιείται θα είναι η βαθμολογία που προκύπτει από τον πολλαπλασιασμό της πιθανότητας εμφάνισης του κινδύνου και της επίπτωσης που είναι πιθανό να έχει. Και οι δύο κλίμακες κυμαίνονται από το 1 έως το 5, επομένως η ελάχιστη βαθμολογία θα είναι 1 και η μέγιστη βαθμολογία θα είναι 25 όπως φαίνεται στον παραπάνω πίνακα.

Σε κάθε κίνδυνο θα αποδίδεται ταξινόμηση με βάση τη βαθμολογία του ως εξής:

* ΚΡΙΣΙΜΟ – 20 έως 25 συμπεριλαμβανομένων
* ΨΗΛΟ – 10 έως 16 συμπεριλαμβανομένων
* ΜΕΤΡΙΟ – 8 έως 9 συμπεριλαμβανομένων
* ΧΑΜΗΛΟ – 5 έως 6 συμπεριλαμβανομένων
* ΠΟΛΥ ΧΑΜΗΛΟ – 1 έως 4 συμπεριλαμβανομένων

Ο πίνακας κινδύνου που παρουσιάζεται παρακάτω απεικονίζει τις κλίμακες και μας επιτρέπει να ιεραρχήσουμε τους κινδύνους μας, ώστε να μπορούν να αντιμετωπιστούν αποτελεσματικότερα.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 5 | **5** | **10** | **15** | **20** | **25** |  | **Κρίσιμο** |
| 4 | **4** | **8** | **12** | **16** | **20** |  | **Ψηλό** |
| 3 | **3** | **6** | **9** | **12** | **15** |  | **Μέτριο** |
| 2 | **2** | **4** | **6** | **8** | **10** |  | **Χαμηλό** |
| 1 | **1** | **2** | **3** | **4** | **5** |  | **Πολύ Χαμηλό** |
|  | 1 | 2 | 3 | 4 | 5 |  |  |

**Κρίσιμο**: Καταστροφικό – πρέπει να εφαρμοστεί παύση των δραστηριοτήτων και να εγκριθεί για άμεση δράση

**Ψηλό**: Απαράδεκτο – πρέπει να ενημερώσετε / δημιουργήσετε στοιχεία ελέγχου για να μετριαστεί ο κίνδυνος

**Μέτριο**: Ανεκτό – πρέπει να επανεξεταστεί έγκαιρα για να πραγματοποιηθούν στρατηγικές βελτίωσης

**Χαμηλό**: Επαρκές – μπορεί να εξεταστεί για περαιτέρω ανάλυση

**Πολύ Χαμηλό**: Αποδεκτό – ενδέχεται να μην απαιτούνται περαιτέρω ενέργειες και ενθαρρύνεται η διατήρηση μέτρων ελέγχου

Το σκεπτικό για την ένδειξη της πιθανότητας και των αξιολογήσεων επιπτώσεων που θα απονεμηθούν θα δοθεί έτσι ώστε αυτές να μπορούν να αξιολογηθούν σε μεταγενέστερη ημερομηνία για να διαπιστωθεί εάν έχουν αλλάξει ουσιαστικά. Αυτό θα βοηθήσει επίσης στη διασφάλιση της συνέπειας και της επαναληψιμότητας στις εκτιμήσεις κινδύνου.

Ο παραπάνω πίνακας δείχνει τις ταξινομήσεις κινδύνου, όπου το πράσινο υποδεικνύει αποδεκτό όριο, καθώς η πιθανότητα είναι ελάχιστη ή/και η επίπτωση είναι ελάχιστη.

Το πορτοκαλί υποδηλώνει ότι το όριο κινδύνου είναι μεσαίο/μέτριο, καθώς ο κίνδυνος είναι μεγαλύτερος, όπως και η επίπτωση. Επομένως, ο περιορισμός αυτών των κινδύνων είναι πιο σημαντικός από την αντιμετώπιση των κινδύνων που βρίσκονται στο πράσινο.

Η κόκκινη περιοχή υποδεικνύει τους κινδύνους που είναι υψίστης προτεραιότητας, καθώς τόσο η επίπτωση όσο και ο κίνδυνος είναι σχετικά υψηλοί, επομένως τα μέτρα για τον περιορισμό τους πρέπει να είναι ύψιστης προτεραιότητας και, εάν δεν μπορούν να μειωθούν, τότε πρέπει να υπάρχουν αντίμετρα για αυτούς τους κινδύνους.

Η συνολική πρόθεση της αξιολόγησης κινδύνου και των προτεινόμενων αντιμετωπίσεων είναι να μειωθεί η ταξινόμηση των κινδύνων σε ένα ελάχιστο αποδεκτό επίπεδο, π.χ. ΠΟΛΥ ΨΗΛΟ, ΨΗΛΟ ΚΑΙ ΜΕΣΑΙΟ ΜΕΧΡΙ ΤΟ ΧΑΜΗΛΟ και το ΠΟΛΥ ΧΑΜΗΛΟ. Αυτό δεν είναι πάντα εφικτό, καθώς μερικές φορές, αν και η βαθμολογία μειώνεται, παραμένει στην ίδια ταξινόμηση, π.χ. η μείωση της βαθμολογίας από 16 σε 10 σημαίνει ότι εξακολουθεί να παραμένει κίνδυνος ΨΗΛΟΥ επιπέδου. Ο οργανισμός μπορεί να αποφασίσει να αποδεχθεί αυτούς τους κινδύνους, παρόλο που παραμένουν σε υψηλή βαθμολογία.

Οι προτεραιότητες των στοιχείων του Σχεδίου Συνεχούς Βελτίωσης καθορίζονται από την υψηλότερη προτεραιότητα των στοιχείων της εκτίμησης κινδύνου που αντιμετωπίζονται, π.χ. εάν 3 στοιχεία αντιμετωπίζονται με μία ενέργεια και ένα ΜΕΣΑΙΟ και δύο ΧΑΜΗΛΟ, τότε η προτεραιότητα της ενέργειας θα είναι ΜΕΣΑΙΑ.

# Διαδικασία Ανάλυσης / Αξιολόγησης Κινδύνων

# Συλλογή πληροφοριών

Ο Υπεύθυνος Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών συγκεντρώνει έναν σημαντικό όγκο πληροφοριών, έτσι ώστε η ανάλυση κινδύνου να είναι πολύτιμη και ολοκληρωμένη, μέσω των πιο κάτω διαθέσιμων πηγών:

* Συνεντεύξεις με ιδιοκτήτες διαδικασιών
* Συνεντεύξεις με ιδιοκτήτες στοιχείων ενεργητικού
* Συνεντεύξεις με προγραμματιστές εφαρμογών
* Συνεντεύξεις με προσωπικό ασφαλείας
* Συνεντεύξεις με εξωτερικούς ειδικούς σε θέματα ασφάλειας
* Αρχεία συμβάντων ασφαλείας
* Ανάλυση περιστατικών που συμβαίνουν σε άλλους οργανισμούς
* Προηγούμενες εκτιμήσεις κινδύνου
* Κλπ.

# Αξιολόγηση της πιθανότητας

Πρέπει να γίνει εκτίμηση της πιθανότητας εμφάνισης της απειλής. Αυτό θα πρέπει να εξετάσει εάν έχει συμβεί στο παρελθόν είτε σε αυτόν τον οργανισμό είτε σε παρόμοιους οργανισμούς στον ίδιο κλάδο ή τοποθεσία και αν υπάρχουν επαρκή κίνητρα, ευκαιρίες και ικανότητα για να γίνει η απειλή πραγματική.

# Αξιολόγηση των επιπτώσεων

Τέλος, θα πρέπει να δοθεί μια εκτίμηση της επίπτωσης που θα μπορούσε να έχει η απώλεια εμπιστευτικότητας, ακεραιότητας, διαθεσιμότητας ή αυθεντικότητας του περιουσιακού στοιχείου στον οργανισμό. Ο τρόπος αξιολόγησης του αντικτύπου περιγράφεται στην ενότητα Κριτήρια Αξιολόγησης Κινδύνου αυτής της διαδικασίας.

Η αξιολόγηση / Ανάλυση Κινδύνων διενεργείται σε τακτά χρονικά διαστήματα.

# Αντιμετώπιση Κινδύνου

Για τους κινδύνους που κρίνονται ότι υπερβαίνουν το όριο αποδοχής (με βάση τα κριτήρια αποδοχής κινδύνου που προσδιορίζονται) από τον οργανισμό, στη συνέχεια θα διερευνηθούν οι επιλογές αντιμετώπισης.

# Κριτήρια Αποδοχής Κινδύνων

Καθορισμός της μεθόδου που ο οργανισμός χρησιμοποιεί για τον προσδιορισμό της αποδοχής κινδύνου. Η αποδοχή κινδύνου ορίζεται ως μια απόφαση με την οποία ο οργανισμός θεωρεί ότι η παρουσία ενός κινδύνου είναι αποδεκτή και ότι δεν απαιτεί μείωση ή μετριασμό.

Ο οργανισμός επιλέγει να αποδεχτεί ένα κίνδυνο με βάση τις πιο κάτω προϋποθέσεις:

* Το κόστος του μετριασμού του κινδύνου είναι μεγαλύτερο από την αξία του περιουσιακού στοιχείου που προστατεύεται
* Ο αντίκτυπος του συμβιβασμού είναι χαμηλός ή η αξία ή η ταξινόμηση του περιουσιακού στοιχείου είναι χαμηλή

Πλαίσιο αποδοχής κινδύνου:

|  |  |
| --- | --- |
| **Επίπεδο Κινδύνου** | **Επίπεδο που απαιτείται για αποδοχή** |
| Πολύ Χαμηλό | Υπεύθυνος για την Ασφάλεια Δικτύων και Συστημάτων Πληροφοριών |
| Χαμηλό | Υπεύθυνος για την Ασφάλεια Δικτύων και Συστημάτων Πληροφοριών |
| Μέτριο | Υπεύθυνος για την Ασφάλεια Δικτύων και Συστημάτων Πληροφοριών |
| Ψηλό | Διευθυντής ή Επικεφαλής Λειτουργιών (CEO ή COO) |
| Πολύ Ψηλό | Διοικητικό Συμβούλιο (Board of Directors) |

Όταν ο οργανισμός αποδέχεται έναν κίνδυνο, εξακολουθεί να επανεξετάζει τον κίνδυνο τουλάχιστον ετησίως. Λόγοι για την επανεξέταση ενός αποδεκτού κινδύνου είναι οι εξής:

* Η αξία του περιουσιακού στοιχείου μπορεί να έχει αλλάξει κατά τη διάρκεια του έτους
* Η αξία της επιχειρηματικής δραστηριότητας που σχετίζεται με το περιουσιακό στοιχείο ενδέχεται να έχει αλλάξει κατά τη διάρκεια του έτους
* Η ισχύς των απειλών ενδέχεται να έχει αλλάξει κατά τη διάρκεια του έτους οδηγώντας ενδεχομένως σε υψηλότερο βαθμό κινδύνου
* Το κόστος του μετριασμού μπορεί να έχει αλλάξει κατά τη διάρκεια του έτους, οδηγώντας δυνητικά σε μεγαλύτερη σκοπιμότητα για μετριασμό του κινδύνου ή μεταφορά

# Πολιτική Ανάληψης Κινδύνων

Risk appetite - Το επίπεδο κινδύνου που ο οργανισμός είναι διατεθειμένος να δεχτεί κατά την επιδίωξη της αποστολής, της στρατηγικής και των στόχων του και πριν απαιτηθεί δράση για την αντιμετώπιση του κινδύνου.

Risk capacity – Το αντικειμενικό ποσό απώλειας που μπορεί να ανεχτεί ο οργανισμός χωρίς να τίθεται υπό αμφισβήτηση η συνεχής ύπαρξη του.

# Στρατηγικές Αντιμετώπισης Κινδύνου

Οι ακόλουθες στρατηγικές μπορούν να εφαρμοστούν για την αντιμετώπιση των εντοπισμένων μη αποδεκτών κινδύνων:

Μείωση / Μετριασμός: Εφαρμογή κατάλληλων ελέγχων για τη μείωση της πιθανότητας ή/και του αντίκτυπου του κινδύνου

Αποφυγή: Διακόψτε τη δραστηριότητα που σχετίζεται με τον κίνδυνο

Μεταφορά: Μεταβίβαση του κινδύνου σε άλλο μέρος, π.χ. ασφαλιστή ή προμηθευτή

Θα χρησιμοποιηθεί κριτική στην απόφαση σχετικά με την πορεία δράσης που θα ακολουθήσει, με βάση την καλή γνώση των περιστάσεων που περιβάλλουν τον κίνδυνο, π.χ.

* Επιχειρηματική στρατηγική
* Ρυθμιστικά και νομοθετικά ζητήματα
* Τεχνικά ζητήματα
* Εμπορικά και συμβατικά ζητήματα

Ο διαχειριστής κινδύνων διασφαλίζει ότι ζητείται η γνώμη όλων των μερών που έχουν συμφέρον ή επηρεάζουν την αντιμετώπιση του κινδύνου.

# Επιλογή Μέτρων Αντιμετώπισης Κινδύνου

Σύμφωνα με τον Κανονισμό Κ.Δ.Π. 389/2020, το Παράρτημα ΙΙΙ του εν λόγω εγγράφου θα χρησιμοποιηθεί ως αφετηρία για τον προσδιορισμό των κατάλληλων και επαρκών μέτρων για την αντιμετώπιση των απαιτήσεων αντιμετώπισης του κινδύνου που προσδιορίζονται στο πλαίσιο της διαδικασίας εκτίμησης κινδύνου.

Κατά τον καθορισμό των μέτρων, ο οργανισμός λαμβάνει υπόψη προληπτικά μέτρα, μέτρα εντοπισμού και μέτρα αντίδρασης από διοικητική, τεχνολογική και φυσική άποψη.

Σε περίπτωση που τα μέτρα που ορίζονται στο Παράρτημα ΙΙΙ δεν ανταποκρίνονται σε όλες τις απαιτήσεις, τότε μπορούν να εφαρμοστούν πρόσθετα μέτρα.

Σχέδιο Εφαρμογής Μέτρων Ασφάλειας Δικτύων και Πληροφοριών (Action Plan)

Οι Στρατηγικές Αντιμετώπισης Κινδύνων σε συνδυασμό με τα Μέτρα Αντιμετώπισης απαρτίζουν το Σχέδιο Αντιμετώπισης Κινδύνων του οργανισμού.

# Μητρώο Κινδύνων

Επισκόπηση ανάλυσης κινδύνου και της εκτίμησης κινδύνου

# Σχέδιο εφαρμογής για τα μέτρα ασφάλειας δικτύων και πληροφοριών (Action Plan)

Το σχέδιο εφαρμογής (μεθοδολογία διαχ. κινδ.) για τα μέτρα ασφάλειας δικτύων και πληροφοριών περιγράφεται στα βήματα που θα ακολουθηθούν.

1) Ανάλυση Κινδύνων

* Αξιολόγηση των δυνητικών κινδύνων και απειλών για τα δίκτυα και τις πληροφορίες του Οργανισμού.
* Καταγραφή των ευαίσθητων περιοχών και κρίσιμων διαδικασιών.

2) Σχεδίαση Ασφάλειας Δικτύου

* Ανάπτυξη πολιτικών ασφαλείας για τον περιορισμό των προσβάσεων και τον έλεγχο των αρμοδιοτήτων.
* Εφαρμογή μέτρων ασφαλείας, όπως firewall, antivirus, intrusion detection και encryption.

3) Εκπαίδευση Προσωπικού

* Διοργάνωση σεμιναρίων για την εκπαίδευση του προσωπικού σχετικά με τις βασικές αρχές ασφαλείας και πρακτικές.
* Εκπαίδευση σχετικά μεθόδους επίθεσης.
* Εκπαίδευση για τη διαχείριση ασφαλείας πληροφοριών και την αντίδραση σε περιστατικά.

 4) Καταγραφή, Παρακολούθηση και Αναφορά

* Εγκατάσταση συστήματος καταγραφής και παρακολούθησης για τον έλεγχο των δραστηριοτήτων στο δίκτυο.
* Άμεση αναφορά περιστατικών και εκτέλεση έρευνας.

5) Ετοιμότητα και Αντίδραση

* Ανάπτυξη σχεδίου αντίδρασης σε περίπτωση επίθεσης ή παραβίασης ασφαλείας.
* Εφαρμογή τακτικών δοκιμών αντίδρασης (incident response drills).

6) Συνεχής Βελτίωση

* Καθορισμός μετρήσεων αποτελεσματικότητας και αναθεώρηση του σχεδίου ανά τακτά χρονικά διαστήματα.
* Εφαρμογή βελτιώσεων βασιζόμενες στα αποτελέσματα των αναθεωρήσεων.

# Δήλωση Εφαρμογής Πλαισίου (Statement of Applicability)

Η δήλωση εφαρμογής θα καθορίζει τους εν λόγω ελέγχους από το Παράρτημα ΙΙΙ του Κ.Δ.Π. 389/2020 που έχουν επιλεγεί και τους λόγους της επιλογής τους. Θα προσδιορίζει επίσης λεπτομερώς εκείνους που έχουν εφαρμοστεί και θα προσδιορίζει όποιους έχουν αποκλειστεί ρητά μαζί με έναν λόγο για τον εν λόγω αποκλεισμό.

# Διαδικασία Εκτίμησης και Αντιμετώπισης Κινδύνου

# Διάγραμμα διαδικασίας



# Αναθεώρηση Αξιολόγησης Κινδύνων

Η αναθεώρηση της Αξιολόγησης Κινδύνων διενεργείται λαμβάνοντας υπόψη:

* Το πλαίσιο λειτουργίας του οργανισμού
* Την αποτελεσματικότητα των εφαρμοζόμενων μέτρων
* Την αναγνώριση νέων απειλών
* Οργανωτικές ή τεχνολογικές αλλαγές
* Άλλα γεγονότα που θα έθεταν καινούρια δεδομένα τα οποία οφείλουν να λάβουν υπόψη

# Διαδικασία Αξιολόγησης της Αποτελεσματικότητας των Εφαρμοζόμενων Μέτρων

Ο [Όνομα Οργανισμού] είναι υπεύθυνος να αξιολογεί την αποτελεσματικότητα των εφαρμοζόμενων μέτρων με βάση το Κ.Δ.Π. 389/2020. Ο [Όνομα Οργανισμού] θα πρέπει να χρησιμοποιεί διάφορες μεθόδους αξιολόγησης, όπως audits, gap assessments, κλπ.

# Παράρτημα Α – Κατάλογος Στοιχείων Ενεργητικού

| **Κατηγορία Στοιχείου Ενεργητικού** | **Υπο - Κατηγορία** | **Στοιχείο Ενεργητικού** |
| --- | --- | --- |
| Πληροφορίες | Εταιρικές | Προϋπολογισμοί |
| Εταιρικά σχέδια |
| Εταιρικές πολιτικές |
| Υπηρεσίες υγείας | Αρχεία ασθενών - ονόματα, διευθύνσεις, επαφές |
| Αλληλογραφία και παράπονα ασθενών |
| Ανθρώπινο δυναμικό | Αρχεία υπαλλήλων - διεύθυνση, Ημερομηνία Γέννησης, Αριθμοί Ασφάλισης |
| Απαιτήσεις δαπανών εργαζομένων |
| Πληροφορίες μισθοδοσίας, συμπεριλαμβανομένων τραπεζικών στοιχείων |
| Αρχεία εκπαιδεύσεων |
| Πληροφορίες πρόσληψης |
| Πληροφορίες άδειας/ελέγχου ασφαλείας |
| Παράπονα εργαζομένων/πειθαρχικά αρχεία |
| Μητρώα ασθένειας/υγείας στην εργασία |
| Σύμβαση Εργασίας |
| Χρηματοδότηση | Λογιστικά αρχεία - τιμολόγια, λογαριασμοί |
| Τραπεζικά στοιχεία επαγγελματικού λογαριασμού |
| Αγοράς | Στοιχεία επικοινωνίας προμηθευτών |
| Σχέδια αγοράς |
| Εμπορικοί όροι |
| Νομικές | Συμβάσεις προμηθευτών |
| Έντυπο συγκατάθεσης ασθενών (διανυκτέρευση) |
| Μισθώσεις ακινήτων |
| Πιστωτικές συμβάσεις |
| Ασφαλιστήρια συμβόλαια |
| Λειτουργίες | Εγχειρίδια για τη σωστή χρήση ιατρικού εξοπλισμού |
| Προδιαγραφές προϊόντος και τιμολόγια υλικών |
| Διαδικασία και διαδικαστική τεκμηρίωση |
| Πνευματική Ιδιοκτησία ειδικά για τον οργανισμό |
| Σχέδια πόρων |
| Έλεγχος και Συμμόρφωση | Αρχεία εσωτερικού ελέγχου |
| Αρχεία εξωτερικού ελέγχου |
| Εκτιμήσεις κινδύνων |
|   |
| Λογισμικό |   | Ηλεκτρονική Διεύθυνση |
| Λογιστικά |
| Κατάσταση μισθοδοσίας |
| Λογισμικό κατά παραγγελία |
| Intranet |
| Ιστότοπος |
| Σχεδιασμός |
| Εφαρμογές γραφείου |
| Εμπορία |
| Εφαρμογές ειδικές για τον κλάδο |
|   |
| Εξοπλισμός |   | Διακομιστές υπολογιστών |
| Εξοπλισμός δικτύωσης |
| Προσωπικοί Υπολογιστές |
| Οι φορητές συσκευές |
| Κινητά τηλέφωνα |
|   |
| Κτίρια/Τοποθεσία |   | Κτίρια |
| Αίθουσες διακομιστή, συμπεριλαμβανομένων κλιματιστικών και μονάδων ισχύος |
| Μηχανήματα |
| Stock |
| Οχήματα |
|   |
| Υπηρεσίες |   | Παροχή Ηλεκτρισμού |
| Παροχή φυσικού αερίου |
| Νερό |
| Υπηρεσίες δικτύου |
| Τηλεφωνικές υπηρεσίες |
|   |
| Άνθρωποι | Βασικοί πόροι | Ιδιοκτήτης / Διευθύνων Σύμβουλος |
| Διευθυντές |
| Μηχανικοί |
| Κάτοχοι γνώσης |
|   |
| Άλλα |   |   |
|   |   |
|   |

# Παράρτημα Β – Κατάλογος Απειλών

Ο ακόλουθος κατάλογος μπορεί να χρησιμοποιηθεί ως σημείο εκκίνησης για τη δημιουργία σχετικού καταλόγου απειλών που ενδέχεται να ισχύουν για τα περιουσιακά στοιχεία πληροφοριών που προσδιορίζονται στο απόθεμα.

| **Κατηγορία απειλής** | **Απειλή** | **Παράδειγμα** |
| --- | --- | --- |
| Ανθρώπινος     | Κακόβουλος ξένος | Κάποιος ξεκινά μια επίθεση άρνησης υπηρεσίας στον ιστότοπό ηλεκτρονικού εμπορίου σας |
| Κακόβουλος εσωτερικά | Ένας υπάλληλος ή ένα αξιόπιστο τρίτο μέρος αποκτά πρόσβαση σε πληροφορίες με μη εξουσιοδοτημένο τρόπο μέσα από το δίκτυό σας |
| Απώλεια βασικού προσωπικού | Ένα ή περισσότερα άτομα με βασικές δεξιότητες ή γνώσεις δεν είναι διαθέσιμα ίσως λόγω εκτεταμένης ασθένειας |
| Ανθρώπινο λάθος | Ένας υπάλληλος διαγράφει κατά λάθος τη βάση δεδομένων πελατών |
| Τυχαία απώλεια | Ένας υπεύθυνος χάνει ένα memory stick με τα στοιχεία πελατών της τράπεζας σε αυτό |
| Φυσικός     | Φωτιά | Το κεντρικό γραφείο σας καίγεται λόγω ηλεκτρικής βλάβης |
| Πλημμύρα | Ο κοντινός ποταμός σπάει τις όχθες του και το κεντρικό γραφείο σας έχει πλημμυρίσει σοβαρά |
| Έντονα καιρικά φαινόμενα | Κανείς δεν μπορεί να μπει στο γραφείο λόγω του καιρού. |
| Σεισμός | Η περιοχή του κεντρικού γραφείου σας επηρεάζεται από ένα σεισμό που βλάπτει όλους τους διακομιστές σας |
| Αστραπή | Όλοι οι διακομιστές σας έχουν καεί από κεραυνό στο κτίριο του κέντρου δεδομένων |
| Τεχνικός   | Αποτυχία υλικού | Ένας σημαντικός διακομιστής έχει αποτυχία επεξεργαστή |
| Αποτυχία λογισμικού | Το χρηματοπιστωτικό σας σύστημα επεξεργάζεται τα τιμολόγια εσφαλμένα λόγω σφάλματος |
| Ιός/κακόβουλος κώδικας | Ένας ιός εξαπλώνεται σε όλο το δίκτυό σας εμποδίζοντας την πρόσβαση στα δεδομένα σας |
| Σωματικός   | Δολιοφθορά | Ένας δυσαρεστημένος πρώην υπάλληλος παίρνει ένα τσεκούρι στο δωμάτιο του διακομιστή σας |
| Κλοπή | Έρχεσαι τη Δευτέρα το πρωί για να βρεις ότι όλοι οι υπολογιστές σου έχουν κλαπεί |
| Εμπρησμός | Κάποιος με μνησικακία εναντίον του οργανισμού σας ανάβει φωτιά κατά τη διάρκεια της νύχτας |
| Περιβαλλοντικός   | Επικίνδυνα απόβλητα | Ένα φορτηγό που μεταφέρει επικίνδυνα απόβλητα έχει ένα ατύχημα έξω από το γραφείο σας |
| Διακοπή ρεύματος | Ο υποσταθμός που τροφοδοτεί την περιοχή σας έχει καταρρεύσει |
| Βλάβη παροχής αερίου | Υπάρχει μια ύποπτη διαρροή και όλες οι προμήθειες είναι απενεργοποιημένες |
| Λειτουργικός  | Σφάλμα διεργασίας | Η νέα διαδικασία μεταφοράς δεδομένων δεν καλύπτει μη αναμενόμενες περιστάσεις και τα δεδομένα χάνονται ή αποστέλλονται σε λάθος προορισμό |
| Έγκλημα | Ένα έγκλημα συμβαίνει μέσα ή κοντά στο γραφείο σας και η περιοχή σφραγίζεται από την αστυνομία |

# Παράρτημα Γ – Κατάλογος Ευπαθειών

|  |  |  |
| --- | --- | --- |
| **Τύπος** | **Παραδείγματα ευπαθειών** | **Παραδείγματα απειλών** |
| Υλικό | Ανεπαρκής συντήρηση/ ελαττωματική εγκατάσταση μέσων αποθήκευσης | Παραβίαση του πληροφοριακού συστήματος συντήρησης |
| Έλλειψη συστημάτων περιοδικής αντικατάστασης | Καταστροφή εξοπλισμού ή μέσων |
| Ευαισθησία στην υγρασία, τη σκόνη, τη ρύπανση | Σκόνη, διάβρωση, κατάψυξη |
| Ευαισθησία στην ηλεκτρομαγνητική ακτινοβολία | Ηλεκτρομαγνητική ακτινοβολία |
| Έλλειψη αποτελεσματικού ελέγχου αλλαγής διαμόρφωσης | Σφάλμα κατά τη χρήση |
| Ευαισθησία σε διακυμάνσεις τάσης | Απώλεια παροχής ηλεκτρικού ρεύματος |
| Ευαισθησία στις διακυμάνσεις της θερμοκρασίας | Μετεωρολογικό φαινόμενο |
| Μη προστατευμένος χώρος αποθήκευσης | Κλοπή μέσων ή εγγράφων |
| Έλλειψη φροντίδας κατά τη διάθεση | Κλοπή μέσων ή εγγράφων |
| Ανεξέλεγκτη αντιγραφή | Κλοπή μέσων ή εγγράφων |
| Λογισμικό | Καμία ή ανεπαρκής δοκιμή λογισμικού | Κατάχρηση δικαιωμάτων |
| Γνωστά ελαττώματα στο λογισμικό | Κατάχρηση δικαιωμάτων |
| Δεν γίνεται «αποσύνδεση» κατά την απομάκρυνση από το σταθμό εργασίας | Κατάχρηση δικαιωμάτων |
| Απόρριψη ή επαναχρησιμοποίηση μέσων αποθήκευσης χωρίς κατάλληλη διαγραφή | Κατάχρηση δικαιωμάτων |
| Έλλειψη ιχνών ελέγχου | Κατάχρηση δικαιωμάτων |
| Εσφαλμένη κατανομή των δικαιωμάτων πρόσβασης | Κατάχρηση δικαιωμάτων |
| Ευρέως διανεμημένο λογισμικό | Αλλοίωση δεδομένων |
| Εφαρμογή προγραμμάτων εφαρμογών σε λάθος δεδομένα από την άποψη του χρόνου | Αλλοίωση δεδομένων |
| Περίπλοκο περιβάλλον εργασίας χρήστη | Σφάλμα κατά τη χρήση |
| Έλλειψη τεκμηρίωσης | Σφάλμα κατά τη χρήση |
| Εσφαλμένη ρύθμιση παραμέτρων | Σφάλμα κατά τη χρήση |
| Εσφαλμένες ημερομηνίες | Σφάλμα κατά τη χρήση |
| Έλλειψη μηχανισμών αναγνώρισης και ελέγχου ταυτότητας, όπως ο έλεγχος ταυτότητας χρήστη | Σφυρηλάτηση δικαιωμάτων |
| Μη προστατευμένοι πίνακες κωδικών πρόσβασης | Σφυρηλάτηση δικαιωμάτων |
| Κακή διαχείριση κωδικών πρόσβασης | Σφυρηλάτηση δικαιωμάτων |
| Δεν είναι δυνατή η ενεργοποίηση των υπηρεσιών που δεν είναι ενεργοποιημένες | Παράνομη επεξεργασία δεδομένων |
| Ανώριμο ή νέο λογισμικό | Δυσλειτουργία λογισμικού |
| Ασαφείς ή ελλιπείς προδιαγραφές για προγραμματιστές | Δυσλειτουργία λογισμικού |
| Έλλειψη αποτελεσματικού ελέγχου αλλαγών | Δυσλειτουργία λογισμικού |
| Ανεξέλεγκτη λήψη και χρήση λογισμικού | Αλλοίωση λογισμικού |
| Έλλειψη αντιγράφων | Αλλοίωση λογισμικού |
| Έλλειψη φυσικής προστασίας του κτιρίου, των θυρών και των παραθύρων | Κλοπή μέσων ή εγγράφων |
| Μη παραγωγή εκθέσεων διαχείρισης | Μη εξουσιοδοτημένη χρήση εξοπλισμού |
| Τέλος Ζωής / Τέλος Υποστήριξης | Παραβίαση του πληροφοριακού συστήματος διατήρησης |
| Δίκτυο | Έλλειψη απόδειξης αποστολής ή λήψης μηνύματος | Άρνηση ενεργειών |
| Μη προστατευμένες γραμμές επικοινωνίας | Υποκλοπές |
| Απροστάτευτη ευαίσθητη κυκλοφορία | Υποκλοπές |
| Κακή καλωδίου αρθρώσεων | Βλάβη τηλεπικοινωνιακού εξοπλισμού |
| Ενιαίο σημείο αποτυχίας | Βλάβη τηλεπικοινωνιακού εξοπλισμού |
| Έλλειψη αναγνώρισης και εξακρίβωσης της ταυτότητας του αποστολέα και του παραλήπτη | Σφυρηλώντας δικαιώματα |
| Ανασφαλής αρχιτεκτονική δικτύου | Απομακρυσμένη κατασκοπεία |
| Σαφής μεταφορά κωδικών πρόσβασης | Απομακρυσμένη κατασκοπεία |
| Ανεπαρκής διαχείριση δικτύου (ανθεκτικότητα της δρομολόγησης) | Κορεσμός του πληροφοριακού συστήματος |
| Μη προστατευμένες συνδέσεις δημόσιου δικτύου | Μη εξουσιοδοτημένη χρήση εξοπλισμού |
| Προσωπικό | Απουσία προσωπικού | Παραβίαση της διαθεσιμότητας προσωπικού |
| Ανεπαρκείς διαδικασίες πρόσληψης | Καταστροφή εξοπλισμού ή μέσων |
| Ανεπαρκής εκπαίδευση ασφάλειας | Σφάλμα κατά τη χρήση |
| Εσφαλμένη χρήση λογισμικού και υλικού | Σφάλμα κατά τη χρήση |
| Έλλειψη επίγνωσης της ασφάλειας | Σφάλμα κατά τη χρήση |
| Έλλειψη μηχανισμών παρακολούθησης | Παράνομη επεξεργασία δεδομένων |
| Εργασία χωρίς επίβλεψη από το εξωτερικό προσωπικό ή το προσωπικό καθαρισμού | Κλοπή μέσων ή εγγράφων |
| Έλλειψη πολιτικών για τη σωστή χρήση των τηλεπικοινωνιακών μέσων και των μηνυμάτων | Μη εξουσιοδοτημένη χρήση εξοπλισμού |
| Τοποθεσία | Ανεπαρκής ή απρόσεκτη χρήση του φυσικού ελέγχου πρόσβασης σε κτίρια και δωμάτια | Καταστροφή εξοπλισμού ή μέσων |
| Τοποθεσία σε περιοχή επιρρεπή σε πλημμύρες | Πλημμύρα |
| Ασταθές δίκτυο ηλεκτρικής ενέργειας | Απώλεια παροχής ηλεκτρικού ρεύματος |
| Έλλειψη φυσικής προστασίας του κτιρίου, των θυρών και των παραθύρων | Κλοπή εξοπλισμού |
| Οργανισμός | Έλλειψη επίσημης διαδικασίας εγγραφής και διαγραφής χρηστών | Κατάχρηση δικαιωμάτων |
| Έλλειψη επίσημης διαδικασίας για την επανεξέταση του δικαιώματος πρόσβασης (εποπτεία) | Κατάχρηση δικαιωμάτων |
| Έλλειψη ή ανεπαρκής διάταξη (όσον αφορά την ασφάλεια) στις συμβάσεις με πελάτες ή/και τρίτους | Κατάχρηση δικαιωμάτων |
| Έλλειψη διαδικασίας παρακολούθησης των εγκαταστάσεων επεξεργασίας πληροφοριών | Κατάχρηση δικαιωμάτων |
| Έλλειψη τακτικών ελέγχων (εποπτεία) | Κατάχρηση δικαιωμάτων |
| Έλλειψη διαδικασιών προσδιορισμού και αξιολόγησης του κινδύνου | Κατάχρηση δικαιωμάτων |
| Έλλειψη αναφορών σφαλμάτων που καταγράφονται στα αρχεία καταγραφής διαχειριστή και χειριστή | Κατάχρηση δικαιωμάτων |
| Ανεπαρκής απόκριση συντήρησης υπηρεσίας | Παραβίαση της δυνατότητας διατήρησης του πληροφοριακού συστήματος |
| Έλλειψη ή ανεπαρκής συμφωνία επιπέδου εξυπηρέτησης | Παραβίαση της δυνατότητας διατήρησης του πληροφοριακού συστήματος |
| Έλλειψη διαδικασίας ελέγχου αλλαγών | Παραβίαση της δυνατότητας διατήρησης του πληροφοριακού συστήματος |
| Έλλειψη επίσημης διαδικασίας για τον έλεγχο τεκμηρίωσης ISMS | Αλλοίωση των δεδομένων |
| Έλλειψη επίσημης διαδικασίας για την εποπτεία των αρχείων ISMS | Αλλοίωση των δεδομένων |
| Έλλειψη επίσημης διαδικασίας για την έγκριση διαθέσιμων στο κοινό πληροφοριών | Δεδομένα από αναξιόπιστους πηγές |
| Έλλειψη κατάλληλης κατανομής των αρμοδιοτήτων ασφάλειας των πληροφοριών | Άρνηση ενεργειών |
| Έλλειψη σχεδίων συνέχειας | Βλάβη εξοπλισμού |
| Έλλειψη πολιτικής χρήσης ηλεκτρονικού ταχυδρομείου | Σφάλμα κατά τη χρήση |
| Έλλειψη διαδικασιών για την εισαγωγή λογισμικού σε λειτουργικά συστήματα | Σφάλμα κατά τη χρήση |
| Έλλειψη εγγραφών στα αρχεία καταγραφής διαχειριστή και τελεστή | Σφάλμα κατά τη χρήση |
| Έλλειψη διαδικασιών για τον διαβαθμισμένο χειρισμό πληροφοριών | Σφάλμα κατά τη χρήση |
| Έλλειψη ευθυνών για την ασφάλεια των πληροφοριών στις περιγραφές θέσεων εργασίας | Σφάλμα κατά τη χρήση |
| Έλλειψη ή ανεπαρκής διάταξη (σχετικά με την ασφάλεια των πληροφοριών) στις συμβάσεις με εργαζομένους | Παράνομη επεξεργασία δεδομένων |
| Έλλειψη καθορισμένης πειθαρχικής διαδικασίας σε περίπτωση συμβάντος ασφάλειας πληροφοριών | Κλοπή εξοπλισμού |
| Έλλειψη επίσημης πολιτικής για τη χρήση κινητών υπολογιστών | Κλοπή εξοπλισμού |
| Έλλειψη ελέγχου των περιουσιακών στοιχείων εκτός προϋπόθεσης | Κλοπή εξοπλισμού |
| Ελλιπής ή ανεπαρκής πολιτική «σαφές γραφείο και σαφής οθόνη» | Κλοπή μέσων ή εγγράφων |
| Έλλειψη άδειας εγκαταστάσεων επεξεργασίας πληροφοριών | Κλοπή μέσων ή εγγράφων |
| Έλλειψη καθιερωμένων μηχανισμών παρακολούθησης για παραβιάσεις της ασφάλειας | Κλοπή μέσων ή εγγράφων |
| Έλλειψη τακτικών αξιολογήσεων διαχείρισης | Μη εξουσιοδοτημένη χρήση εξοπλισμού |
| Έλλειψη διαδικασιών για την αναφορά αδυναμιών ασφάλειας | Μη εξουσιοδοτημένη χρήση εξοπλισμού |
| Έλλειψη διαδικασιών συμμόρφωσης με τα πνευματικά δικαιώματα | Χρήση πλαστού ή αντιγραμμένου λογισμικού |

# Παράρτημα Δ – Κριτήρια Επιπτώσεων Κινδύνων

|  |  |
| --- | --- |
| **Επίπεδο επίπτωσης** | **Περιοχές επιπτώσεων** |
| **Εκτίμηση επιπτώσεων** | **Γενική Περιγραφή** | **Α.1 Αποφάσεις διοίκησης** | **Α2. Οικονομική / Άμεση Απώλεια Εσόδων / Κόστος** | **Α3. Φήμη / Εμπιστοσύνη / Εικόνα** | **Α4. Νομική / Κανονιστική Ευθύνη** | **A.5 Απάτη** |
| 5 | **Πολύ υψηλός** | **Η διαδικασία λήψης αποφάσεων της διοίκησης διαταράχθηκε σημαντικά****Σημειώθηκε σημαντική αποτυχία στην εκτέλεση της διαδικασίας. Η διαδικασία ενδέχεται να μην εκτελεστεί ή να απαιτεί μη διαχειρίσιμες καθυστερήσεις πριν από την ενδεχόμενη εκτέλεση.**  | **Δημιουργία θέματος βιωσιμότητας και κεφαλαιακής επάρκειας****Απώλεια εσόδων / αποτέλεσμα κόστους με αποτέλεσμα τη δημιουργία ζητήματος βιωσιμότητας και κεφαλαιακής επάρκειας του οργανισμού που απαιτεί τη συμμετοχή του Διοικητικού Συμβουλίου και των ρυθμιστικών αρχών**  | **Όλες οι Ομάδες που σχετίζονται με τον Οργανισμό επηρεάζονται** **Σημαντική υποβάθμιση της εμπιστοσύνης / εικόνας που προκύπτει από την αλλαγή της στάσης της φήμης προς όλες τις σχετικές ομάδες (π.χ. Όλους τους Πελάτες / Υποψήφιους Πελάτες / Ρυθμιστικές Αρχές / Τρίτα Μέρη).** | **Επιχειρηματικές και μελλοντικές απειλητικές υποχρεώσεις** **Είναι σε ισχύ οι υποχρεώσεις που απειλούν σημαντικά την ύπαρξη του Οργανισμού και την ικανότητά του να συνεχίσει να παρέχει υπηρεσίες.** | **Εκτεταμένη απάτη****Η δραστηριότητα απάτης έχει εξαπλωθεί σε διάφορες (πολλαπλές) οντότητες και γεωγραφικές τοποθεσίες. Τα πρόσθετα μέτρα που απαιτούνται για τον μετριασμό της κατάστασης και την ανάκτηση των χαμένων κεφαλαίων ενδέχεται να μην είναι δυνατή.** |
| 4 | **Ψηλός** | **Η διαδικασία λήψης αποφάσεων της διοίκησης παρεμποδίστηκε σοβαρά** **Έχει σημειωθεί αποτυχία κατά την εκτέλεση της διαδικασίας. Απαιτούνται εναλλακτικές διαδικασίες για την εκτέλεση της διαδικασίας και ο Οργανισμός αντιμετωπίζει σημαντικές καθυστερήσεις.**  | **Τα οικονομικά αποτελέσματα επηρέασαν σοβαρά** **τα οικονομικά****Τα οικονομικά αποτελέσματα ή το κόστος του οργανισμού επηρεάζονται σοβαρά με έναν αριθμό τμημάτων που επηρεάζονται από την απώλεια εσόδων / υψηλό κόστος και απαιτείται συμμετοχή του Διοικητικού Συμβουλίου** | **Πολλαπλές Ομάδες σχετικές με τον Οργανισμό****Σοβαρή υποβάθμιση της εμπιστοσύνης / εικόνας που προκύπτει από την αλλαγή της στάσης της φήμης προς ορισμένες σχετικές ομάδες (π.χ. Ιδιώτες Πελάτες και Εταιρικοί Πελάτες).** | **Υποχρεώσεις που έχουν ως αποτέλεσμα τον επιχειρηματικό αντίκτυπο που απαιτεί ειδικό χειρισμό** **Υφίστανται υποχρεώσεις που απαιτούν ιδιαίτερη προσοχή, χειρισμό εκτός των τυπικών διαδικασιών και αν δεν αντιμετωπιστούν εγκαίρως και η βασική αιτία παραμένει, μπορεί να οδηγήσουν σε σημαντικές απώλειες (π.χ. μέσω κυρώσεων) ή / και να αναδειχθεί σε "Σημαντικό" απειλώντας έτσι την ύπαρξη του Οργανισμού και την ικανότητά του να συνεχίσει να παρέχει υπηρεσίες.** | **Κατανεμημένη απάτη σε αριθμούς ή / και όγκο****Η δραστηριότητα απάτης διανέμεται αλλά δεν είναι ακόμη ευρέως διαδεδομένη. Ωστόσο, ο αριθμός των δόλιων συναλλαγών ή / και ο όγκος της δραστηριότητας απάτης είναι αυξημένος από τον μέσο όρο. Πρόσθετα μέτρα απαιτούνται για τον μετριασμό της κατάστασης. Η ανάκτηση ορισμένων χαμένων κεφαλαίων ενδέχεται να μην είναι δυνατή.** |
| 3 | **Μέτριος** | **Η διαδικασία λήψης αποφάσεων από τη διοίκηση επηρεάστηκε αλλά ισχύει****Η διαδικασία εκτελείται, αλλά αντιμετωπίζονται διαταραχές που απαιτούν εκ νέου επεξεργασία ή εκ νέου εργασία με αποτέλεσμα διαχειρίσιμες καθυστερήσεις.** | **Αδυναμία κάλυψης της ζημίας από τον** **υφιστάμενο προϋπολογισμό****Απώλεια / Κόστος που οδηγεί σε αδυναμία του τμήματος να καλύψει από τον υφιστάμενο προϋπολογισμό και απαιτείται έγκριση από τα ανώτερα διοικητικά στελέχη** | **Συγκεκριμένη ομάδα σχετική με τον Οργανισμό που επηρεάζεται****Υποβάθμιση της εμπιστοσύνης / εικόνας που προκύπτει από την αλλαγή της στάσης της φήμης προς μια συγκεκριμένη σχετική ομάδα (π.χ. Εταιρικοί Πελάτες ή Υποψήφιοι Ιδιώτες Πελάτες). Αυτό μπορεί να ανυψωθεί σε "Σοβαρό" ανάλογα με το μέγεθος του ομίλου που επηρεάζεται.** | **Υποχρεώσεις που διακανονίζονται μέσω των υφιστάμενων διαδικασιών****Ισχύουν υποχρεώσεις που αντιμετωπίζονται με τυπικές διαδικασίες, αλλά μπορεί να οδηγήσουν σε ορισμένες απώλειες (π.χ. κυρώσεις) και μπορεί να παρεμποδίσουν περαιτέρω τις σχέσεις με τρίτους / Πελάτες.** | **Περιπτώσεις απάτης που εντοπίζονται και επιλύονται μέσω υφιστάμενων** **διαδικασιών****Η δραστηριότητα απάτης είναι περιορισμένη, αλλά ο αριθμός των δόλιων συναλλαγών ή/και ο όγκος της δραστηριότητας απάτης είναι αυξημένος από τον μέσο όρο. Οι υποθέσεις μπορούν να διεκπεραιωθούν μέσω των υφιστάμενων διαδικασιών παρακολούθησης και διαχείρισης της απάτης.**  |
| 2 | **Ελάχιστος** | **Η διαδικασία λήψης αποφάσεων της διοίκησης επηρεάζεται έμμεσα** **Η διαδικασία εκτελείται με περιστασιακές έμμεσες και ελάχιστες διακοπές που απαιτούν περιορισμένες καθυστερήσεις.** | **Διαχειρίζεται από τον υπάρχοντα προϋπολογισμό** **Ζημιά / Κόστος που αντιμετωπίζεται μέσω των υφιστάμενων χορηγήσεων στον ετήσιο προϋπολογισμό** | **Ατομική Οντότητα σχετική με τον επηρεαζόμενο Οργανισμό** **Υποβάθμιση εμπιστοσύνης / εικόνας που προκύπτει από την αλλαγή της στάσης της φήμης προς μια συγκεκριμένη οντότητα μόνο (π.χ. ιδιώτης πελάτης ή εταιρικός πελάτης).** | **Περιορισμένες υποχρεώσεις** **Είναι σε ισχύ οι υποχρεώσεις που αντιμετωπίζονται με τυπικές διαδικασίες. Οι απώλειες είναι περιορισμένες (π.χ. ελάχιστες κυρώσεις) και δεν εμποδίζουν τις σχέσεις με Τρίτους / Πελάτες.** | **Περιπτώσεις απάτης αλλά περιορισμένες σε αριθμούς ή / και** **όγκο****Η δραστηριότητα απάτης απομονώνεται. Οι υποθέσεις μπορούν να διεκπεραιωθούν μέσω των υφιστάμενων διαδικασιών παρακολούθησης και διαχείρισης της απάτης.** |
| 1 | **Αμελητέος** | **Καμία** **επιρροή****Δεν υπάρχουν διαταραχές ή δυσκολίες.**  | **Δεν υπάρχει άμεση απώλεια /** **κόστος****Δεν υπάρχει άμεση απώλεια εσόδων ή δεν υπάρχει άμεσο κόστος για τη διόρθωση οποιασδήποτε ζημιάς** | **Καμία άμεση επίδραση σε έναν Όμιλο ή** **μια οντότητα****Καμία υποβάθμιση της εμπιστοσύνης / εικόνας προς οποιεσδήποτε ομάδες ή οντότητες.** | **Δεν υπάρχουν άμεσες** **υποχρεώσεις****Δεν υπάρχουν υποχρεώσεις.** | **Καμία άμεση** **απάτη****Δεν εντοπίστηκε σχετική δραστηριότητα απάτης.** |