Όνομα Οργανισμού

Πολιτική & 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](#_Toc190433384)

[1.1. Σκοπός 5](#_Toc190433385)

[1.2. Πεδίο Εφαρμογής 5](#_Toc190433386)

[2. Πολιτική Διαχείρισης Κινδύνων 6](#_Toc190433387)

[2.1. Κατάλογος Στοιχείων Ενεργητικού 6](#_Toc190433388)

[2.2. Μητρώο Κινδύνων 7](#_Toc190433389)

[2.3. Ανάλυση και Αξιολόγηση Κινδύνων 8](#_Toc190433390)

[2.4. Σχέδια Αντιμετώπισης Κινδύνων 9](#_Toc190433391)

[3. Αναθεώρηση 10](#_Toc190433392)

[4. Αναφορές 11](#_Toc190433393)

[5. ΠΑΡΑΡΤΗΜΑ Α – Μεθοδολογία Διαχείρισης Κινδύνου 13](#_Toc190433394)

[5.1. Ορισμός Πεδίου Εφαρμογής 13](#_Toc190433395)

[5.2. Σκοπός της Εκτίμησης Κινδύνων 13](#_Toc190433396)

[5.3. Καθορισμός Ρόλων και Αρμοδιότητων 13](#_Toc190433397)

[5.4. Προσδιορισμός Στοιχείων Ενεργητικού 14](#_Toc190433398)

[5.5. Προσδιορισμός Πιθανών Ευπαθειών 14](#_Toc190433399)

[5.6. Προσδιορισμός Πιθανών Κινδύνων 15](#_Toc190433400)

[5.7. Προσδιορισμός Τύπων Κινδύνων 15](#_Toc190433401)

[5.8. Προσδιορισμός Ιδιοκτητών Κινδύνων 16](#_Toc190433402)

[5.9. Προσδιορισμός Υφιστάμενων Δικλείδων Ασφαλείας 16](#_Toc190433403)

[5.10. Κριτήρια Ανάλυσης Κινδύνου 16](#_Toc190433404)

[5.10.1. Κριτήρια Πιθανότητας 16](#_Toc190433405)

[5.10.2. Κριτήρια Επιπτώσεων 16](#_Toc190433406)

[6. Κριτήρια Βαθμολόγησης Κινδύνου 18](#_Toc190433407)

[7. Διαδικασία Ανάλυσης / Αξιολόγησης Κινδύνων 20](#_Toc190433408)

[7.1. Συλλογή πληροφοριών 20](#_Toc190433409)

[7.2. Αξιολόγηση της πιθανότητας 20](#_Toc190433410)

[7.3. Αξιολόγηση των επιπτώσεων 20](#_Toc190433411)

[8. Αντιμετώπιση Κινδύνου 20](#_Toc190433412)

[8.1. Κριτήρια Αποδοχής Κινδύνων 21](#_Toc190433413)

[8.2. Πολιτική Ανάληψης Κινδύνων 21](#_Toc190433414)

[8.3. Στρατηγικές Αντιμετώπισης Κινδύνου 22](#_Toc190433415)

[8.4. Επιλογή Μέτρων Αντιμετώπισης Κινδύνου 22](#_Toc190433416)

[8.5. Σχέδιο εφαρμογής για τα μέτρα ασφάλειας δικτύων και πληροφοριών (Action Plan) 22](#_Toc190433417)

[8.5.1. Ενέργειες που θα πρέπει να περιλαμβάνει το σχέδιο δράσης 23](#_Toc190433418)

[8.5.2. Απαίτηση σε πόρους 23](#_Toc190433419)

[8.5.3. Ανάθεση ρόλων και αρμοδιοτήτων 23](#_Toc190433420)

[8.5.4. Παρακολούθηση αποτελεσματικότητας και Αναφορά 23](#_Toc190433421)

[8.5.5. Αξιολόγηση και αναθεώρηση του σχεδίου αντιμετώπισης κινδύνων 24](#_Toc190433422)

[8.5.6. Υποβολή εκθέσεων και συνεχής βελτίωση 24](#_Toc190433423)

[8.6. Δήλωση Εφαρμογής Πλαισίου (Statement of Applicability) 24](#_Toc190433424)

[9. Διαδικασία Εκτίμησης και Αντιμετώπισης Κινδύνου 25](#_Toc190433425)

[9.1. Διάγραμμα διαδικασίας 25](#_Toc190433426)

[Παράρτημα Β – Κατάλογος Στοιχείων Ενεργητικού 26](#_Toc190433427)

[Παράρτημα Γ – Κατάλογος Απειλών 29](#_Toc190433428)

[Παράρτημα Δ – Κατάλογος Ευπαθειών 31](#_Toc190433429)

[Παράρτημα Ε – Κριτήρια Επιπτώσεων Κινδύνων 37](#_Toc190433430)

# Εισαγωγή

# Σκοπός

Το παρόν έγγραφο περιλαμβάνει ενδεικτικούς Όρους Πολιτικής για τη διαχείριση κινδύνων που αφορούν στους πόρους και τα δεδομένα του [Όνομα Οργανισμού] σύμφωνα με τις πρόνοιες της περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών (Μέτρα Ασφάλειας Φορέων Εκμετάλλευσης Βασικών Υπηρεσιών και Φορέων Κρίσιμων Υποδομών Πληροφοριών) Απόφασης του 2020 (Κ.Δ.Π. 389/2020) και της περί Ασφάλειας Δικτύων και Συστημάτων Πληροφοριών (Έλεγχοι Ωριμότητας Κυβερνοασφάλειας) Απόφασης του 2024 (Κ.Δ.Π. 245/2024).

Σκοπός του παρόντος εγγράφου είναι:

* Η θέσπιση μίας δομημένης προσέγγισης 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 ενίσχυση της οργανωτικής ανθεκτικότητας, ελαχιστοποιώντας την έκθεση σε κινδύνους ασφάλειας πληροφοριών/κυβερνοασφάλειας.
* Η διασφάλιση της ευθυγράμμισης της διαχείρισης κινδύνων με τους στρατηγικούς στόχους και τις κανονιστικές υποχρεώσεις του οργανισμού.
* Ο καθορισμός ρόλων και αρμοδιοτήτων για τις δραστηριότητες σχετικές με τη διαχείριση κινδύνων.
* Η υποστήριξη λήψης αποφάσεων με την παροχή δομημένης μεθοδολογίας για την αξιολόγηση και την αντιμετώπιση των κινδύνων.
* Η προώθηση μιας κουλτούρας με επίγνωση των κινδύνων ασφάλειας πληροφοριών/κυβερνοασφάλειας μέσω συνεχούς παρακολούθησης, κατάρτισης και βελτίωσης.

# Πεδίο Εφαρμογής

Η Πολιτική και Μεθοδολογία Διαχείρισης Κινδύνων εφαρμόζεται σε όλα τα τμήματα και τις λειτουργίες του [Όνομα Οργανισμού], ανεξαρτήτως γεωγραφικής τοποθεσίας. Περιλαμβάνει την αναγνώριση, αξιολόγηση, αντιμετώπιση, παρακολούθηση και επικοινωνία όλων των κινδύνων που μπορεί να επηρεάσουν την επίτευξη των στόχων του [Όνομα Οργανισμού]. Πιο συγκεκριμένα το πεδίο εφαρμογής καλύπτει:

* όλες τις κρίσιμες δραστηριότητες, πληροφοριακά συστήματα, υποδομές, περιουσιακά στοιχεία και προσωπικό που είναι απαραίτητα για την αδιάλειπτη και ασφαλή λειτουργία του [Όνομα Οργανισμού].
* Όλες οι οργανωτικές μονάδες, τα τμήματα και το προσωπικό που εμπλέκονται στη λήψη αποφάσεων σχετικά με τους κινδύνους.
* Προμηθευτές και συνεργάτες τρίτων που χειρίζονται ή επεξεργάζονται ευαίσθητα δεδομένα ή παρέχουν κρίσιμες υπηρεσίες.
* Θέματα συμμόρφωσης με κανονιστικές απαιτήσεις.

# Πολιτική Διαχείρισης Κινδύνων

Ο [Όνομα Οργανισμού] διατηρεί μία μεθοδολογία διαχείρισης κινδύνων (Βλέπε Παράρτημα Α), η οποία περιλαμβάνει την διαδικασία διαχείρισης κινδύνων ασφάλειας πληροφοριών και δικτύων, προσδιορίζει τα κριτήρια ανάλυσης της πιθανότητας και των επιπτώσεων των κινδύνων και τη στρατηγική αντιμετώπιση τους (μείωση, μεταφορά, αποφυγή, αποδοχή κινδύνου) σύμφωνα με την διάθεση ανάληψης κινδύνου (risk appetite) του [Όνομα Οργανισμού] και εφαρμόζεται τουλάχιστον ετησίως. Η μεθοδολογία συμφωνείται και υποστηρίζεται από τη Ανώτατη Διοίκηση και άλλους σχετικούς φορείς εντός του [Όνομα Οργανισμού]. Σε αυτήν:

* Έχουν καθοριστεί σαφείς ρόλοι, αρμοδιότητες και κριτήρια για την διενέργεια της διαχείρισης κινδύνων, καθώς και τα σχετικά αρχεία που πρέπει να τηρούνται.
* Έχουν καθοριστεί τα κριτήρια αποδοχής κινδύνων, τα οποία πρέπει να λαμβάνουν υπόψη τους στόχους, το πλαίσιο λειτουργίας και την στρατηγική του.
* Ο [Όνομα Οργανισμού] καταγράφει τα αποτελέσματα της διαδικασίας διαχείρισης κινδύνων ασφάλειας πληροφοριών και δικτύων και να παρέχει τα αποτελέσματα στις αρμόδιες Αρχές ετησίως ή και κατόπιν αιτήματος.
* Οι αναγνωρισμένοι κίνδυνοι προτεραιοποιούνται σύμφωνα με τον αντίκτυπο που μπορεί να έχουν στον [Όνομα Οργανισμού] ως προς την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των πόρων που επηρεάζουν.
* Ακολουθεί τις βέλτιστες πρακτικές και αποτελείται από διακριτές φάσεις και αναλυτικά βήματα (πλαίσιο λειτουργίας, αξιολόγηση κινδύνων (που αποτελείται από αναγνώριση κινδύνων, ανάλυση κινδύνων και αποτίμηση κινδύνων), αντιμετώπιση κινδύνων, καταγραφή και αναφορά των κινδύνων, επικοινωνία, παρακολούθηση και ανασκόπηση κινδύνων) για την αποτελεσματική διεξαγωγή ασκήσεων αξιολόγησης κινδύνων.
* Ο [Όνομα Οργανισμού] όπου είναι δυνατό θεσπίζει και παρακολουθεί συγκεκριμένους δείκτες απόδοσης σχετικά με την διαχείριση κινδύνων.
* Οπού είναι δυνατό και εφαρμόζεται θα πρέπει να ακολουθεί την ευρύτερη μεθοδολογία διαχείρισης επιχειρησιακών κινδύνων (Enterprise Risk Management) και να την τροφοδοτεί σύμφωνα με τα αποτελέσματά της.
* Συστήνεται όπως ο [Όνομα Οργανισμού] ορίσει έναν υπεύθυνο για την συνολική διαχείριση και παρακολούθηση της μεθοδολογίας διαχείρισης κινδύνων.
* Ο [Όνομα Οργανισμού] οφείλει να ενημερώνει σχετικά με την μεθοδολογία διαχείρισης κινδύνων, όλα τα εμπλεκόμενα μέρη (εσωτερικά ή/και εξωτερικά του [Όνομα Οργανισμού]) των οποίων η δραστηριότητα τους σχετίζεται με τους κινδύνους του Οργανισμού.

# Κατάλογος Στοιχείων Ενεργητικού

Στα πλαίσια της μεθοδολογία διαχείρισης κινδύνων θα πρέπει να προηγηθεί ο προσδιορισμός των Στοιχείων Ενεργητικού μέσω δημιουργίας ενός καταλόγου συστημάτων και διαδικασιών και άλλων σημαντικών πόρων εντός του [Όνομα 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 η εκτίμηση κινδύνου. Η σαφής αποτύπωση του πλαισίου θα επιτρέψει τον καλύτερο εντοπισμό των κινδύνων.

Παραδείγματα Στοιχείων Ενεργητικού περιλαμβάνονται στο Παράρτημα Β του παρόντος εγγράφου.

Σκοπός του Καταλόγου Στοιχείων Ενεργητικού είναι η συνεχής παρακολούθηση της κατάστασης των στοιχείων / εξοπλισμού των δικτύων, συστημάτων πληροφοριών και ουσιωδών υπηρεσιών ως προς τη λειτουργική τους δυνατότητα και τις πιθανές βλάβες και η εφαρμογή τυχόν πολιτικών που σχετίζονται με το εκάστοτε είδος που βρίσκεται στο κατάλογο.

Ένα βασικό μέρος της διαδικασίας εκτίμησης κινδύνου είναι ο προσδιορισμός της αξίας ενός στοιχείου ενεργητικού με στόχο να γνωρίζουμε τον αντίκτυπο σε περίπτωση απώλειας του. Έλλειψη της αξίας ενός στοιχείου ενεργητικού, καθιστά πιο δύσκολο το έργο υπολογισμού των κινδύνων που σχετίζονται με ένα στοιχείο ενεργητικού.

Για περισσότερες πληροφορίες μπορείτε να ανατρέξετε στη «Πολιτική Διαχείρισης Στοιχείων Ενεργητικού».

# Μητρώο Κινδύνων

Ο [Όνομα Οργανισμού] τηρεί, και ενημερώνει τακτικά, ένα μητρώο απειλών, ευπαθειών και κινδύνων για κάθε στοιχείο ενεργητικού, συμπεριλαμβανομένων των απειλών που προέρχονται από εσωτερικά πρόσωπα, με σκοπό την αποτελεσματική αναγνώριση, καταγραφή και παρακολούθηση των κινδύνων, σύμφωνα με τις διεθνείς βέλτιστες πρακτικές.

Για κάθε κίνδυνο που αναγνωρίζεται, υπάρχει τουλάχιστον ένας υπεύθυνος ιδιοκτήτης κινδύνου.

Το μητρώο κινδύνων πρέπει να συμπεριλαμβάνει κινδύνους που προκύπτουν από:

* τον ανθρώπινο παράγοντα,
* τυχαία ή παράνομη καταστροφή,
* απώλεια,
* αλλοίωση,
* άνευ αδείας κοινοποίηση ή πρόσβαση σε πληροφορίες που διαβιβάζονται, αποθηκεύονται ή υποβάλλονται σε επεξεργασία.
* άλλοι κίνδυνοι που θα μπορούσαν δυνητικά να επηρεάσουν ουσιώδεις οικονομικές και κοινωνικές λειτουργίες.
* απειλές όπως remote spying, theft of equipment, theft of information or media, retrieval of recycled or discarded media, data input from untrustworthy sources, incorrect use of devices, illegal processing of data, sending or distributing of malware, abuse of rights.
* αντίστοιχα περιλαμβάνονται αδυναμίες όπως είναι ελλιπείς πόροι προσωπικού, προσωπικό που διενεργεί ενέργειες με conflict of interest / απουσία διαχωρισμού καθηκόντων, έλλειψη παρακολούθησης και εποπτείας, μερικός ορισμός πολιτικών, αδυναμία εφαρμογής τεχνικών μέτρων επιβολής πολιτικών και διαδικασιών, κ.α.

Οι κίνδυνοι πρέπει να καλύπτουν όλες τις πιθανές κατηγορίες πηγών κινδύνων (risk sources), ανεξάρτητα από το αν είναι υπό τον έλεγχο του [Όνομα Οργανισμού]. Ειδικά για τα πολύπλοκα και κρίσιμα σενάρια κινδύνων, η μεθοδολογία πρέπει να επαναλαμβάνεται (iterations), αρχικά σε υψηλό επίπεδο (high level) και στη συνέχεια με μεγαλύτερη ανάλυση (drilling down) σε περισσότερες λεπτομέρειες, μέχρι να αναγνωριστεί η ορθή ρίζα του προβλήματος (root cause).

Όπου έχουν γίνει παραδοχές και ομαδοποιήσεις, πρέπει να υπάρχει σχετική καταγραφή που τεκμηριώνει πώς προκύπτουν οι σχετικές παραδοχές και ομαδοποιήσεις και ότι αυτά είναι προσαρμοσμένα με το ευρύτερο πλαίσιο λειτουργίας του [Όνομα Οργανισμού].

Σε περίπτωση που απειλές, ευπάθειες ή/και κίνδυνοι αναγνωριστούν ως μη εφαρμόσιμοι στο τρέχον περιβάλλον του [Όνομα Οργανισμού], τα εμπλεκόμενα μέρη πρέπει να επικαιροποιούν το σχετικό μητρώο. Πρέπει να υποδεικνύουν ότι η αντίστοιχη εγγραφή δεν είναι πλέον ενεργή, για λόγους ιστορικότητας.

Το μητρώο απειλών, ευπαθειών και κινδύνων πρέπει να επικαιροποιείται λαμβάνοντας πληροφορίες από την διαδικασία καταγραφής και αναφοράς ευπαθειών.

Η αναγνώριση των απειλών, ευπαθειών και κινδύνων στους οποίους είναι εκτεθειμένος ο [Όνομα Οργανισμού] πρέπει να γίνεται με τη συμμετοχή όσο το δυνατόν μεγαλύτερου αριθμού εσωτερικών μερών.

Ο [Όνομα Οργανισμού] συστήνεται όπως διαθέτει διαδικασία, η οποία πρέπει να έχει κοινοποιηθεί στο προσωπικό, για την παροχή στοιχείων αναγνώρισης απειλών, ευπαθειών και κινδύνων, στους οποίους είναι εκτεθειμένος ο [Όνομα Οργανισμού], από το προσωπικό σε ad-hoc βάση.

Πρέπει να γίνεται τακτικός έλεγχος πληρότητας των στοιχείων του μητρώου απειλών, ευπαθειών και κινδύνων έναντι διεθνών έγκυρων πηγών.

# Ανάλυση και Αξιολόγηση Κινδύνων

Η ανάλυση και η αξιολόγηση των κινδύνων αποτελούν ουσιώδη στοιχεία του πλαισίου διαχείρισης κινδύνων του [Όνομα Οργανισμού]. Η διαδικασία αυτή περιλαμβάνει τον εντοπισμό, την αξιολόγηση και την ιεράρχηση των κινδύνων με βάση την πιθανότητα και τις πιθανές επιπτώσεις σε στοιχεία ενεργητικού σε σχέση με την Εμπιστευτικότητα, Ακεραιότητα, Διαθεσιμότητα και Αυθεντικότητα των πληροφοριών και λειτουργιών τους.

Ο [Όνομα Οργανισμού] πραγματοποιεί ανάλυση των κινδύνων για την ασφάλεια πληροφοριών όσον αφορά τα στοιχεία ενεργητικού, λαμβάνοντας υπόψη τις διαφορετικές πιθανότητες και τις βαθμολογίες των επιπτώσεων.

Ο κίνδυνος πρέπει να προσδιορίζεται και να βαθμολογείται για την αξιολόγηση της κατάλληλης στρατηγικής μετριασμού.

Τα αποτελέσματα της ανάλυσης και της αξιολόγησης κινδύνου πρέπει να καταγράφονται στο μητρώο απειλών, ευπαθειών και κινδύνων που διατηρεί ο [Όνομα Οργανισμού].

Πρέπει να καθορίζονται κατάλληλες και επαρκείς στρατηγικές για την αντιμετώπιση των κινδύνων που αναλύονται, συμπεριλαμβανομένων των μέτρων για την πρόληψη, τον εντοπισμό και την παρακολούθηση των επιθέσεων από εσωτερικά πρόσωπα, από άγνοια, αμέλεια, ή κακόβουλες ή επαγγελματικές προθέσεις.

Κατά την εκτίμηση της πιθανότητας και της σχετικής επίπτωσης, πρέπει να λαμβάνεται υπόψη η υλοποίηση ανεξάρτητων και εξαρτημένων γεγονότων.

Συστήνεται όπως υλοποιούνται μέθοδοι και προβλέψεις για τον προσδιορισμό των cascading κινδύνων και των επιπτώσεων τους.

Η ανάλυση των κινδύνων στους οποίους είναι εκτεθειμένος ο [Όνομα Οργανισμού] πρέπει να γίνεται με τη συμμετοχή όσο το δυνατόν μεγαλύτερου αριθμού εσωτερικών μερών.

Ο [Όνομα Οργανισμού] πρέπει να διαθέτει διαδικασία, η οποία είναι γνωστή στο προσωπικό, για την ενημέρωση του αρμόδιου προσωπικού σε περίπτωση αναγνώρισης λάθους ή παράλειψης στην ανάλυση κινδύνων.

Για τον προσδιορισμό της πιθανότητας και της επίπτωσης των αναγνωρισμένων κινδύνων, πρέπει να λαμβάνεται υπόψη η υλοποίηση σχετικών μέτρων αντιμετώπισης (controls), εφόσον υπάρχουν.

Οι πιθανές και επιλεγμένες στρατηγικές πρέπει να ανασκοπούνται περιοδικά από τα κατάλληλα εξουσιοδοτημένα ενδιαφερόμενα μέρη, προκειμένου να εξεταστεί κατά πόσο εξακολουθούν να είναι κατάλληλες και αποτελεσματικές για τη διαχείριση των σχετικών κινδύνων για τον [Όνομα Οργανισμού]. Αλλαγές σε σχέση με την τεχνολογία, τις υπηρεσίες ή νέες στρατηγικές συνεργασίες πρέπει επίσης να οδηγούν στην ανασκόπηση των σχετικών στρατηγικών και αποφάσεων.

Ο ιδιοκτήτης του κάθε κινδύνου, πρέπει να δίνει την έγκριση του, σχετικά με την αποδοχή του υπολειπόμενου κινδύνου (residual risk) και της επιλεγμένης στρατηγικής αντιμετώπισης κινδύνου.

# Σχέδια Αντιμετώπισης Κινδύνων

Ο [Όνομα Οργανισμού] καθορίζει μέσα από υλοποίηση συγκεκριμένων σχεδίων, τις ενέργειες που απαιτούνται για την αντιμετώπιση των εντοπισμένων κινδύνων, διασφαλίζοντας ότι η διαχείριση τους ευθυγραμμίζεται με τους οργανωτικούς στόχους και άλλες απαιτήσεις συμμόρφωσης. Το έγγραφο αυτό περιγράφει λεπτομερώς τις επιλεγμένες επιλογές αντιμετώπισης των κινδύνων -όπως ο μετριασμός, η αποδοχή, η μεταφορά ή η αποφυγή- μαζί με τις ανατεθείσες αρμοδιότητες, τα χρονοδιαγράμματα και τους απαραίτητους πόρους. Με τη συστηματική εφαρμογή μέτρων αντιμετώπισης κινδύνων, οι οργανισμοί μπορούν να ενισχύσουν την ανθεκτικότητα, να διατηρήσουν τη λειτουργική συνέχεια και να ανταποκριθούν στις κανονιστικές υποχρεώσεις.

Προς αυτό το σκοπό:

* Ο [Όνομα Οργανισμού] καθορίζει κατάλληλα και επαρκή μέτρα αντιμετώπισης του κινδύνου στα πλαίσια της εφαρμογής της στρατηγικής αντιμετώπισης κινδύνων που καθορίζεται στη διαδικασία αξιολόγησης των κινδύνων, λαμβάνονται υπόψη προληπτικά μέτρα, μέτρα εντοπισμού και μέτρα αντίδρασης από διοικητική, τεχνολογική και φυσική άποψη, προκειμένου να διασφαλίζεται, κατά περίπτωση, μια πολυεπίπεδη άμυνα.
* Τα σχέδια αντιμετώπισης κινδύνων λαμβάνουν υπόψη τα μέτρα ασφάλειας που περιγράφονται στην σχετική νομοθεσία.
* Οι ενέργειες αντιμετώπισης κινδύνων καταγράφονται σε σχετικό αρχείο το οποίο περιέχει περιγραφή των μέτρων που λαμβάνονται, μέχρι πότε ισχύουν, ποιος είναι ο υπεύθυνος κάθε μέτρου ασφάλειας, ποιοι είναι οι πόροι που απαιτούνται, με ποιόν τρόπο θα ελεγχθεί η αποτελεσματικότητα των ενεργειών, καθώς και το υπολειπόμενο επίπεδο κινδύνου μετά την εφαρμογή των ενεργειών.
* Το αποτέλεσμα της αντιμετώπισης κινδύνων καταγράφεται στο σχέδιο αντιμετώπισης κινδύνων του [Όνομα Οργανισμού].
* Τα σχέδια αντιμετώπισης κινδύνων πρέπει να παρακολουθούνται για τον έλεγχο της αποτελεσματικότητας των μέτρων αντιμετώπισης που έχει υλοποιήσει ο [Όνομα Οργανισμού]. Το χρονικό διάστημα στο οποίο ο οργανισμός πρέπει να υλοποιήσει τις σχετικές ενέργειες καθορίζεται σύμφωνα με την κρισιμότητα του κινδύνου όπως αποτυπώνεται και στην σχετική διαδικασία.
* Προκειμένου να αξιολογηθεί η πληρότητα των επιλεγμένων μέτρων, πρέπει να γίνεται σε τακτική βάση σύγκριση με οργανωμένες λίστες ενεργειών (π.χ. ISO 27002, ISO 27001 Annex A, ISO 27017, ISO 27011, κ.α.). Σε περίπτωση που αναγνωριστεί κάποια ενέργεια η οποία μπορεί να υλοποιηθεί, ο [Όνομα Οργανισμού] πρέπει να προβαίνει σε κατάλληλη αξιολόγηση διενεργώντας τα βήματα της διαχείρισης κινδύνου με πεδίο τους κινδύνους που μπορεί να καλύψει η συγκεκριμένη ενέργεια.

# Αναθεώρηση

Τα έγγραφα σχετικά με την Διαχείριση Κινδύνων θα πρέπει να επανεξετάζονται και να αναθεωρούνται σε τακτικές προγραμματισμένες αναθεωρήσεις τουλάχιστον ετησίως ή σε περίπτωση σημαντικών αλλαγών στο περιβάλλον του [Όνομα Οργανισμού] με στόχο να διασφαλίζεται η ευθυγράμμιση με τους εξελισσόμενους κινδύνους και τις οργανωτικές αλλαγές. Επιπρόσθετα συστήνεται όπως επανεξάγεται στο πλαίσιο εισηγήσεων μετά από εσωτερικούς ελέγχους σε συνδυασμό με τις ετήσιες αξιολογήσεις κινδύνων ή άλλους ελέγχους συμμόρφωσης ή της εισαγωγής νεών κανονισμών ή σχετικά πρότυπα

Τέλος συστήνεται όπως αναθεωρείτε μετά από σημαντικά περιστατικά ασφάλειας ή παραβιάσεις και αλλαγές στο τοπίο κυβερνοασφάλειας λόγω αναδυόμενων απειλών, γεωπολιτικών αλλαγών ή τεχνολογικών εξελίξεων.

# Αναφορές

|  |  |  |  |
| --- | --- | --- | --- |
| **Κατηγορία** | **ID** | **Μέτρο** | **Στόχος Μέτρου** |
| Διαχείριση Κίνδυνων | RM1 | Μεθοδολογία | Να θεσπιστεί μεθοδολογία διαχείρισης κινδύνων, η οποία αντικατοπτρίζει τη διαδικασία εκτίμησης κινδύνου του οργανισμού, τα κριτήρια ανάλυσης κινδύνου, τα κριτήρια αποδοχής κινδύνων και την πολιτική ανάληψης κινδύνων. |
| Διαχείριση Κίνδυνων | RM2 | Πλαίσιο | Να καταρτιστεί κατάλογος στοιχείων ενεργητικού, συστημάτων και διαδικασιών εντός του οργανισμού. |
| Διαχείριση Κίνδυνων | RM3 | Εντοπισμός κινδύνων | Να εντοπιστούν οι απειλές, ευπάθειες και κίνδυνοι στους οποίους εκτίθενται τα στοιχεία ενεργητικού, τα συστήματα και οι διαδικασίες του οργανισμού. |
| Διαχείριση Κίνδυνων | RM4 | Ανάλυση κινδύνου | Να αναλυθούν οι κίνδυνοι για την ασφάλεια πληροφοριών στο πλαίσιο των στοιχείων ενεργητικού ανάλογα με τις διάφορες πιθανότητες και επιπτώσεις. |
| Διαχείριση Κίνδυνων | RM5 | Αξιολόγηση κινδύνων | Να αξιολογηθούν οι κίνδυνοι για την ασφάλεια πληροφοριών με βάση την πολιτική ανάληψης κινδύνων του οργανισμού και να καθοριστούν οι κατάλληλες στρατηγικές αντιμετώπισης. |
| Διαχείριση Κίνδυνων | RM6 | Αντιμετώπιση κινδύνων | Να καθοριστούν οι δράσεις για την αντιμετώπιση των κινδύνων για την ασφάλεια πληροφοριών. |
| Ασφάλεια Ανθρώπινων Πόρων | HRS5 | Προστασία από απειλές που προέρχονται από εσωτερικά πρόσωπα | Να εξασφαλιστεί η προστασία από απειλές κατά της ασφάλειας δικτύων και πληροφοριών από το εσωτερικό του οργανισμού. |

*Σημείωση: το μέρος πιο κάτω αφορά τη Μεθοδολογία Διαχείρισης Κινδύνου που σκοπό έχει την υποστήριξη της Πολιτικής που καταγράφεται στις πιο πάνω παραγράφους. Η Μεθοδολογία αυτή δύναται να είναι σε ξεχωριστό έγγραφο από τη Πολιτική Διαχείρισης Κινδύνου.*

# ΠΑΡΑΡΤΗΜΑ Α – Μεθοδολογία Διαχείρισης Κινδύνου

# Ορισμός Πεδίου Εφαρμογής

Σαν Πρώτο βήμα θα γίνεται προσδιορισμός και ο ορισμός του πεδίου εφαρμογής της εκτίμησης κινδύνου. Συνήθως, ο ορισμός πεδίου εφαρμογής περιλαμβάνει, τα τμήματα του [Όνομα Οργανισμού] και άλλες επιχειρησιακές μονάδες του [Όνομα Οργανισμού] που πρόκειται να συμπεριληφθούν, με βάση την επιχειρησιακό αντικείμενο, 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.

# Καθορισμός Ρόλων και Αρμοδιότητων

|  |  |
| --- | --- |
| Ρόλος | Αρμοδιότητα |
| Υπεύθυνος Ασφάλειας Δικτύων και Συστημάτων 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 του [Όνομα Οργανισμού] | • 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. |

**Υποσημείωση:** Ο κάθε οργανισμός δύναται να καθορίσει μόνο τους ρόλους οι οποίοι ευθυγραμμίζονται με τις ανάγκες και την δομή του και να απαλείψει ή τροποποιήσει τους ρόλους οι οποίοι δεν εφαρμόζονται σε κάθε περίπτωση. Επιπρόσθετα, ανάλογα με το μέγεθος του κάθε οργανισμού, θα υπάρχουν περιπτώσεις κατά τις οποίες δεν θα είναι εφικτός ο διορισμός ξεχωριστών ατόμων για τον κάθε ρόλο. Σε μια τέτοια περίπτωση ο οργανισμός δύναται να καθορίσει πέραν του ενός ρόλου σε ένα άτομο, νοουμένου ότι δεν θα προκύπτει σύγκρουση συμφέροντος μεταξύ των ρόλων αυτών.

# Προσδιορισμός Στοιχείων Ενεργητικού

Ο προσδιορισμός των Στοιχείων Ενεργητικού μέσω δημιουργίας ενός καταλόγου συστημάτων και διαδικασιών και άλλων σημαντικών πόρων εντός του [Όνομα Οργανισμού] όπως καταγράφεται και στη Πολιτική Διαχείρισης στοιχείων Ενεργητικού.

Ο προσδιορισμός πιθανών απειλών αποτελεί βασικό συστατικό στοιχείο των μεθοδολογιών κινδύνου, με στόχο την αναγνώριση πηγών κινδύνου που θα μπορούσαν να εκμεταλλευτούν τρωτά σημεία και να επηρεάσουν τα περιουσιακά στοιχεία του οργανισμού. Για κάθε στοιχείο ενεργητικού, εντοπίζονται οι απειλές που εύλογα αναμένεται να ισχύουν για αυτό και που έχουν τη δυνατότητα να το βλάψουν. Οι απειλές μπορεί να είναι εσωτερικές ή εξωτερικές και να προέρχονται από κυβερνοεπιθέσεις, αποτυχίες συστημάτων, ανθρώπινα λάθη, φυσικές καταστροφές ή κανονιστικές αλλαγές

Μια αρχική λίστα τυπικών απειλών περιλαμβάνεται στο Παράρτημα Γ του παρόντος εγγράφου αλλά και σε άλλα πρότυπα του αντικειμένου όπως ISO 27005 κτλ.

# Προσδιορισμός Πιθανών Ευπαθειών

Η διαδικασία αυτή περιλαμβάνει την αξιολόγηση τεχνικών, επιχειρησιακών και οργανωτικών πτυχών για τον εντοπισμό κενών στους ελέγχους ασφαλείας, στις διαμορφώσεις του συστήματος, στις διαδικασίες και στους ανθρώπινους παράγοντες. Για κάθε στοιχείο ενεργητικού, εντοπίζονται και προσδιορίζονται οι περιστάσεις ή τα χαρακτηριστικά ενός περιστατικού στοιχείου που μπορεί να ενεργοποιηθεί 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 Δ του παρόντος εγγράφου.

# Προσδιορισμός Πιθανών Κινδύνων

Ο προσδιορισμός των δυνητικών κινδύνων περιλαμβάνει την ανάλυση της αλληλεπίδρασης μεταξύ απειλών και τρωτών σημείων για τον προσδιορισμό των δυνητικών αρνητικών επιπτώσεων σε ουσιώδεις λειτουργίες και υπηρεσίες που παρέχονται από τον Οργανισμό. Οι κίνδυνοι προκύπτουν όταν μια απειλή εκμεταλλεύεται μια ευπάθεια. Σε αυτό το στάδιο 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.

# 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:

Κίνδυνοι εμπιστευτικότητας - Απειλές που θέτουν σε κίνδυνο το απόρρητο ευαίσθητων δεδομένων, επιτρέποντας μη εξουσιοδοτημένη πρόσβαση.

* Παραδείγματα: Παραβιάσεις δεδομένων, εσωτερικές απειλές, αδύναμη κρυπτογράφηση και μη ασφαλής αποθήκευση.

Κίνδυνοι ακεραιότητας - Κίνδυνοι που επηρεάζουν την ακρίβεια, τη συνέπεια και την αξιοπιστία των δεδομένων και των συστημάτων.

* Παραδείγματα: Διαφθορά δεδομένων, μη εξουσιοδοτημένες τροποποιήσεις, κακόβουλο λογισμικό (π.χ. ransomware) και επιθέσεις στην αλυσίδα εφοδιασμού λογισμικού(supply chain).
* Κίνδυνοι διαθεσιμότητας - Απειλές που διαταράσσουν την πρόσβαση σε συστήματα, δίκτυα ή υπηρεσίες, οδηγώντας σε διακοπή λειτουργίας.

Κίνδυνοι διαθεσιμότητας - Απειλές που διαταράσσουν την πρόσβαση σε συστήματα, δίκτυα ή υπηρεσίες, οδηγώντας σε διακοπή λειτουργίας.

* Παραδείγματα: Επιθέσεις DDoS, βλάβες συστημάτων, ransomware, δυσλειτουργίες υλικού και ανεπαρκής πλεονασμός.

Κίνδυνοι Αυθεντικότητας - Κίνδυνοι που παρεμποδίζουν την γνησιότητα της πληροφορίες, την ιχνηλασιμότητα, τον έλεγχο και την επιβολή των πολιτικών ασφαλείας

Παραδείγματα: Ανεπαρκείς πρακτικές καταγραφής, έλλειψη ελέγχων πρόσβασης, αδύναμοι μηχανισμοί ελέγχου ταυτότητας και ανεπαρκείς δυνατότητες forensics.

# Προσδιορισμός Ιδιοκτητών Κινδύνων

Ο οργανισμός προχωρεί σε προσδιορισμό των υπευθύνων κινδύνων κυβερνοασφάλειας, διασφαλίζοντας τη λογοδοσία και τον αποτελεσματικό μετριασμό των κινδύνων. Ιδιοκτήτης κινδύνου είναι το άτομο ή η ομάδα που είναι υπεύθυνη για τη διαχείριση ενός συγκεκριμένου κινδύνου, την επίβλεψη των ενεργειών αντιμετώπισης και μετριασμού και τη διασφάλιση της συμμόρφωσης με τις πολιτικές ασφαλείας

# 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, καθορίζοντας τους παράγοντες που χρησιμοποιούνται για την αξιολόγηση και την ιεράρχηση των κινδύνων κυβερνοασφάλειας. 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

Τα κριτήρια επιπτώσεων χρησιμοποιούνται για το καθορισμό της έκτασης των συνεπειών που μπορεί να έχει προκύψει από ένα κίνδυνο κυβερνοασφάλειας. Τα κριτήρια αυτά βοηθούν στην αξιολόγηση της σοβαρότητας ενός κινδύνου με βάση τις πιθανές επιπτώσεις με βάση τις περιοχές επιπτώσεων που παρουσιάζονται παρακάτω:

* Επίδραση στη λειτουργία
* Οικονομικό κόστος
* Βλάβη στη φήμη / Εμπιστοσύνη
* Νομική, συμβατική και οργανωτική Συμμόρφωση
* Υγεία και ασφάλεια

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Επίπεδο επιπτώσεων** | | **Περιοχές επιπτώσεων** | | | | |
| **Αξιολόγηση επιπτώσεων** | **Γενική περιγραφή** | **Επίδραση στη λειτουργία** | **Οικονομικό κόστος** | **Βλάβη στη φήμη/Εμπιστοσύνη** | **Νομική, συμβατική και οργανωτική Συμμόρφωση** | **Υγεία και ασφάλεια** |
| 1 | Αμελητέα | Καμία επίδραση | Πολύ λίγο ή καθόλου | Καμία ζημία στη φήμη. | Καμία νομική ή κανονιστική επίπτωση. | Καμία επίδραση στην υγεία και ασφάλεια. |
| 2 | Ελάχιστη | Κάποια τοπική διαταραχή στις κανονικές επιχειρηματικές λειτουργίες | Μερικό | Περιορισμένη επίδραση, εύκολη αποκατάσταση. | Μικρή παράβαση με δυνατότητα διόρθωσης. | Μικρός κίνδυνος χωρίς μακροχρόνιες επιπτώσεις. |
| 3 | Μέτρια | Μπορεί ακόμα να παραδώσει προϊόν/υπηρεσία με κάποια δυσκολία | Ανεπιθύμητο αλλά υποφερτό | Δημοσιογραφική κάλυψη, κάποια απώλεια εμπιστοσύνης. | Παράβαση που μπορεί να οδηγήσει σε πρόστιμα ή έρευνες. | Πιθανότητα τραυματισμού ή σοβαρού άγχους. |
| 4 | Υψηλή | Οι επιχειρήσεις είναι ακρωτηριασμένες σε βασικούς τομείς | Σοβαρές επιπτώσεις στο εισόδημα ή/και στα κέρδη | Εκτεταμένη δημοσιότητα, σοβαρή μείωση εμπιστοσύνης. | Σοβαρή παράβαση που μπορεί να οδηγήσει σε νομικές ενέργειες. | Σοβαρή επίδραση στην ασφάλεια ατόμων. |
| 5 | Πολύ υψηλή | Εκτός λειτουργείας, καμία εξυπηρέτηση στους πελάτες | μη βιώσιμο χρέος, ο οργανισμός θα σταματήσει να λειτουργεί | Καταστροφική ζημία στη φήμη, απώλεια βασικών πελατών/εταίρων. | Νομικές κυρώσεις που επηρεάζουν τη λειτουργία του οργανισμού. | Άμεσος κίνδυνος για τη ζωή ή σοβαρές σωματικές επιπτώσεις. |

Η επίπτωση αξιολογείται με βάση τις πιο πάνω κατηγορίες 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.

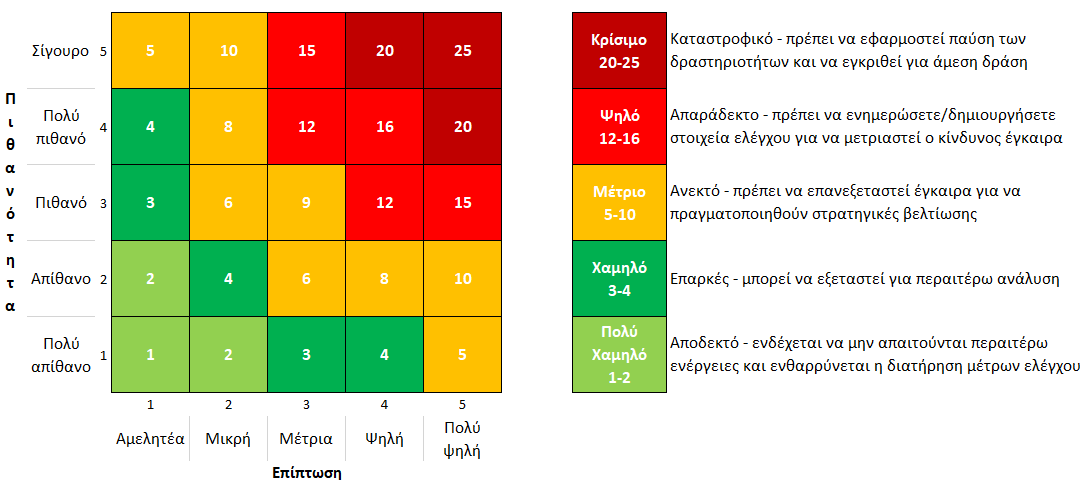
Το επίπεδο επιπτώσεων θα λάβει βαθμολογία με βάση τον συνδυασμό των 5 περιοχών καθώς και την επίπτωση που θα έχει ένα στοιχείο ενεργητικού εάν διακυβευτεί η εμπιστευτικότητα, η ακεραιότητα, η διαθεσιμότητα και η αυθεντικότητα του.

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

# Κριτήρια Βαθμολόγησης 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 χάρτης θερμότητας κινδύνων (heat map). ω είναι ένα οπτικό εργαλείο που χρησιμοποιείται στη διαχείριση κινδύνων για την αξιολόγηση και την κοινοποίηση της πιθανότητας και του αντίκτυπου των εντοπισμένων κινδύνων με τρόπο εύληπτο και κατανοητό. Απεικονίζει τους κινδύνους σε έναν πίνακα, συνήθως με την πιθανότητα στον ένα άξονα και τον αντίκτυπο στον άλλο, χρησιμοποιώντας χρωματική κωδικοποίηση για να υποδηλώσει τη σοβαρότητα κάθε κινδύνου με στόχο την ιεράρχηση των κινδύνων με βάση την πιθανότητα εμφάνισης τους και τις πιθανές συνέπειες που μπορεί να έχουν στον οργανισμό.

Ο χάρτης θερμότητας κινδύνων (heat map) που παρουσιάζεται παρακάτω απεικονίζει τις κλίμακες και μας επιτρέπει να ιεραρχήσουμε τους κινδύνους του οργανισμού, ώστε να μπορούν να αντιμετωπιστούν αποτελεσματικότερα.



Ο πίνακας χωρίζεται σε τμήματα Άξονα Χ: Πιθανότητα και Άξονας Υ: Επίπτωση (π.χ., πολύ χαμηλό έως Κρίσιμο).

Ο πίνακας χωρίζεται σε τμήματα με βάση αυτές τις κατηγορίες, με αποτέλεσμα να προκύπτουν κελιά που αντιπροσωπεύουν συνδυασμούς επιπέδων πιθανότητας και επιπτώσεων. Η τομή της πιθανότητας και των επιπτώσεων παρέχει το συνολικό επίπεδο κινδύνου(risk score) με βάση αυτές τις κατηγορίες, με αποτέλεσμα να προκύπτουν κελιά που αντιπροσωπεύουν συνδυασμούς επιπέδων πιθανότητας και επιπτώσεων.

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

* ΚΡΙΣΙΜΟ – 20 έως 25 συμπεριλαμβανομένων
* ΨΗΛΟ – 12 έως 16 συμπεριλαμβανομένων
* ΜΕΤΡΙΟ – 5 έως 10 συμπεριλαμβανομένων
* ΧΑΜΗΛΟ – 3 έως 4 συμπεριλαμβανομένων
* ΠΟΛΥ ΧΑΜΗΛΟ – 1 έως 2 συμπεριλαμβανομένων

όπου

**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 ενός σχεδίου δράσης 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) ή άλλο σώμα Ανώτατης Διοίκησης π.χ. Διευθύνουσα Επιτροπή Ασφάλειας Πληροφοριών (Information Security Steering Committee) |

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 την Απόφαση 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 αντιμετώπισης κινδύνου. Τα μέτρα αυτά δύναται να κατηγοριοποιούνται σε διοικητικά, οργανωτικά, τεχνολογικά ή μέτρα φυσικής ασφάλειας

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

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

Me την ολοκλήρωση της αξιολόγησης κινδύνου θα πρέπει να ετοιμάζεται ένα λεπτομερές σχέδιο δράσης για την εφαρμογή των μέτρων ασφάλειας πληροφοριών ως μέρος του σχεδίου αντιμετώπισης κινδύνων. Αυτό περιλαμβάνει χρονοδιαγράμματα, κατανομή πόρων και ρόλων. Το σχέδιο αυτό αποτελεί μέρος μιας ευρύτερης διαδικασίας διαχείρισης κινδύνων και διασφαλίζει ότι η ασφάλειας πληροφοριών του οργανισμού ευθυγραμμίζεται με τους εντοπισμένους κινδύνους και τα τρωτά σημεία.

# Ενέργειες που θα πρέπει να περιλαμβάνει το σχέδιο δράσης

1. Δημιουργία ενός καταλόγου ενεργειών για κάθε στρατηγική αντιμετώπισης κινδύνων.
2. Για κάθε αναγνωρισμένο μέτρο ασφαλείας, θα πρέπει να προσδιοριστούν τα εξής:
   * 1. Ποιες ενέργειες απαιτούνται; (π.χ. εγκατάσταση firewall, εκπαίδευση των εργαζομένων)
     2. Υπεύθυνος υλοποίησης; (π.χ. τμήμα πληροφορικής, ανθρώπινο δυναμικό, εξωτερικοί συνεργάτες)
     3. Χρονοδιάγραμμα υλοποίησης της δράσης; (π.χ. εντός 3 μηνών)
     4. Απαίτηση σε πόρους; (π.χ. προϋπολογισμός για την αγορά λογισμικού ή/και υλισμικού, κόστος κατάρτισης εργαζομένων, κόστος αγοράς υπηρεσιών)
     5. Τρόπος επικύρωσης της δράσης; (π.χ. δοκιμές διείσδυσης, αξιολογήσεις ευπάθειας)

# Απαίτηση σε πόρους

Για την κατανομή πόρων και άλλου προϋπολογισμού θα πρέπει:

* να εκτιμηθεί το κόστος που απαιτείται για εργαλεία, τεχνολογίες, εκπαίδευση και τυχόν τρίτους προμηθευτές.
* Να διατεθούν οι ανθρώπινους πόρους με τις κατάλληλες δεξιότητες για την εκτέλεση των μέτρων ασφαλείας.
* Να εξασφαλιστεί η απαραίτητη υποστήριξης από την Ανώτατη Διοίκηση για συνεχή χρηματοδότηση συμπεριλαμβανομένης και της μακροπρόθεσμης συντήρησης και παρακολούθηση των μέτρων που εφαρμόζονται ανά περίπτωση.

# Ανάθεση ρόλων και αρμοδιοτήτων

Για την ανάθεση συγκεκριμένων ρόλων και αρμοδιοτήτων σε άτομα ή ομάδες για διασφάλιση της υπευθυνότητας της κάθε δράσης θα πρέπει:

* Να οριστεί ένας επικεφαλής της δράσης ή μια ομάδα διαχείρισης κινδύνων υπεύθυνη για την επίβλεψη της υλοποίησης.
* Για πιο συγκεκριμένα και εξειδικευμένα καθήκοντα να ανατεθούν ειδικούς σε θέματα ασφάλειας, σε προσωπικό πληροφορικής ή σε εξωτερικούς συνεργάτες.
* Να καθοριστεί μία διαδικασία αναφοράς και κλιμάκωσης σε περίπτωση προβλημάτων.

# Παρακολούθηση αποτελεσματικότητας και Αναφορά

Μετά την εφαρμογή των μέτρων ασφαλείας, η συνεχής παρακολούθηση και ο έλεγχος είναι ουσιώδης σημασίας για να διασφαλιστεί η αποτελεσματικότητά τους και η ελαχιστοποίηση των υπολειπόμενων κινδύνων. Προς αυτό το σκοπό θα πρέπει:

* Να μελετηθεί η εγκατάσταση εργαλείων παρακολούθησης της ασφάλειας (π.χ. συστήματα διαχείρισης πληροφοριών και συμβάντων ασφάλειας - SIEM).
* Να διεξάγονται σε τακτική βάση αξιολογήσεις τρωτότητας(vulnerability assessments), δοκιμές διείσδυσης (penetration testing) και ελέγχους ασφαλείας (IT Audits).
* Να παρακολουθείτε η απόδοση των εφαρμοζόμενων ελέγχων ώστε να επιβεβαιώνεται η ορθή λειτουργία.

# Αξιολόγηση και αναθεώρηση του σχεδίου αντιμετώπισης κινδύνων

Ο [Όνομα Οργανισμού] είναι υπεύθυνος να αξιολογεί την αποτελεσματικότητα των εφαρμοζόμενων μέτρων με βάση την Απόφαση Κ.Δ.Π. 389/2020. Ο [Όνομα Οργανισμού] θα πρέπει να διεξάγεται τακτική επανεξέταση και επικαιροποίηση του σχεδίου αντιμετώπισης κινδύνων για να διασφαλιστεί ότι παραμένει αποτελεσματικό στην αντιμετώπιση νέων και εξελισσόμενων και αναδυόμενων κινδύνων και απειλών καθώς και άλλων επιχειρησιακών αναγκών.

Επιπλέον, Θα πρέπει να παρέχετε ανατροφοδότηση στα ενδιαφερόμενα μέρη και το σχέδιο να προσαρμόζεται ανάλογα με τις ανάγκες ώστε να παραμένει ευθυγραμμισμένο με τους στόχους.

# Υποβολή εκθέσεων και συνεχής βελτίωση

Θα πρέπει να προωθηθεί μία κουλτούρα συνεχούς βελτίωσης, βελτιώνοντας τις πολιτικές, τις διαδικασίες και τις τεχνικές λύσεις με βάση την ανατροφοδότηση και τις αναδυόμενες τάσεις του τοπίου απειλών. Αυτό επιτυγχάνεται μέσω της τακτικής υποβολής εκθέσεων προς τα στελέχη της Ανώτατης Διοίκησης του Οργανισμού σχετικά με την αντιμετώπιση των κινδύνων και την εφαρμογή των μέτρων ασφαλείας και της συνεχούς βελτίωσης ώστε να εξασφαλίσετε μακροπρόθεσμη ανθεκτικότητα στην ασφάλεια.

# Δήλωση Εφαρμογής Πλαισίου

Η δήλωση εφαρμογής θα καθορίζει τους ελέγχους από το Παράρτημα ΙΙΙ της Απόφασης Κ.Δ.Π. 389/2020 που έχουν επιλεγεί θα προσδιορίζει λεπτομερώς εκείνους που έχουν εφαρμοστεί με μια περιγραφή του τρόπου υλοποίησης και άλλης υποστηρικτικής πληροφορίας. Σε πολύ σπάνιες περιπτώσεις ενδέχεται να υπάρχουν έλεγχοι έχουν αποκλειστεί για κάποιο λόγο ή δεν εφαρμόζονται στον Οργανισμό. Σε τέτοια περίπτωση θα πρέπει επίσης στη Δήλωση Εφαρμογής Πλαισίου να καταγράφεται τεκμηριωμένα οι λόγοι αποκλεισμού.

# Διαδικασία Εκτίμησης και Αντιμετώπισης Κινδύνου

# Διάγραμμα διαδικασίας



# Παράρτημα Β – 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/σΤοποθεσία |  | 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 Γ – 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 Δ – 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 Ε – Κριτήρια Επιπτώσεων Κινδύνων

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Επίπεδο επίπτωσης** | | **Περιοχές επιπτώσεων** | | | | |
| **Εκτίμηση επιπτώσεων** | **Γενική Περιγραφή** | **Α.1 Επίδραση στη λειτουργία** | **Α2. Οικονομικό κόστος** | **Α3. Βλάβη στη φήμη** | **Α4. Νομική, συμβατική και οργανωτική Συμμόρφωση** | **A.5 Υγεία και ασφάλεια** |
| 5 | **Πολύ υψηλή** | **Πλήρης διακοπή λειτουργίας, σοβαρές επιπτώσεις σε ένα Οργανισμό ή την κρίσιμη υποδομή. Η ανάκαμψη απαιτεί εκτεταμένες διαδικασίες αποκατάστασης.**  **Π.χ - Οργανισμός αδυνατεί να λειτουργήσει λόγω κυβερνοεπίθεσης (π.χ. ransomware).**  **- Διείσδυση σε κρίσιμες υποδομές (ηλεκτρικό δίκτυο, υγεία, χρηματοπιστωτικά ιδρύματα).** | **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).** **π.χ κυβερνοεπίθεση που πιθανό να οδηγήσει σε κατάρρευση του Οργανισμού.** | **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.**  **Π.χ. Διεθνής παραβίαση δεδομένων με υψηλά πρόστιμα και νομικές αγωγές.** | **Ακραία επίδραση στην υγεία και ασφάλεια, με πιθανή απώλεια ζωών ή μαζικούς τραυματισμούς. Οι επιπτώσεις είναι μη αναστρέψιμες και επηρεάζουν μεγάλο πληθυσμό. Π.χ**  - Ransomware επίθεση που μπλοκάρει ζωτικής σημασίας ιατρικό εξοπλισμό (π.χ., μηχανές ανάνηψης, χειρουργικά ρομπότ), με αποτέλεσμα απώλεια ζωών.  - Παραβίαση συστήματος ελέγχου βιομηχανίας, προκαλώντας ανεξέλεγκτη διαρροή τοξικών ή επικίνδυνων ουσιών.  - Κυβερνοεπίθεση σε υποδομές ενέργειας, με αποτέλεσμα εκτεταμένη διακοπή ρεύματος που επηρεάζει νοσοκομεία, οδηγώντας σε απώλεια ανθρώπινων ζωών. |
| 4 | **Υψηλή** | **Σημαντική διακοπή κρίσιμων λειτουργιών, με ευρύ αντίκτυπο στην παραγωγικότητα και τις υπηρεσίες.**  **.**  **Π.χ αδυναμία πρόσβασης σε βασικά πληροφοριακά συστήματα για μεγάλο μέρος του οργανισμού.**  **- Σοβαρή κυβερνοεπίθεση που επηρεάζει κρίσιμα δεδομένα ή υπηρεσίες.** | **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).**  **Π.χ. νέα για κυβερνοεπίθεση με απώλεια δεδομένων πελατών.** | **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.**  **Π.χ. Απώλεια προσωπικών δεδομένων χιλιάδων πολιτών.** | **Σημαντική επίδραση στην υγεία και ασφάλεια, πιθανός σοβαρός τραυματισμός ή ασθένεια. Το περιστατικό απαιτεί επείγουσα παρέμβαση.Π.χ**  **- Κυβερνοεπίθεση που μπλοκάρει την πρόσβαση σε ηλεκτρονικούς ιατρικούς φακέλους, προκαλώντας καθυστερήσεις στη διάγνωση και θεραπεία ασθενών.**  **- Παραβίαση βιομηχανικού συστήματος, οδηγώντας σε υπερθέρμανση μηχανημάτων και αυξημένο κίνδυνο εργατικών ατυχημάτων.**  **- Επίθεση σε δίκτυο μεταφορών, προκαλώντας προβλήματα στις φωτεινές σηματοδοτήσεις, αυξάνοντας τον κίνδυνο ατυχημάτων.** |
| 3 | **Μέτρια** | **Μέτρια διακοπή που επηρεάζει μεμονωμένους χρήστες ή τμήματα. Μερική μείωση παραγωγικότητας**  **Π.χ - Διακοπή ενός πληροφοριακού συστήματος με αντίκτυπο σε συγκεκριμένες ομάδες εργαζομένων.**  **- Περιορισμένη διακοπή υπηρεσίας email ή του ERP συστήματος.**  **.** | **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 / άλλους ενδιαφερόμενους.** | **Μέτρια επίδραση, που μπορεί να προκαλέσει σωματική ή ψυχολογική επιβάρυνση. Ίσως απαιτείται ιατρική παρακολούθηση ή ανάκαμψη.** |
| 2 | **Ελάχιστη** | **Μικρή διακοπή λειτουργίας, αλλά το σύστημα παραμένει λειτουργικό. Εύκολη αποκατάσταση με μικρή καθυστέρηση** | **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.** | **Μικρή ήπια επίδραση, χωρίς σοβαρές ή μόνιμες επιπτώσεις στην υγεία. Η επίδραση είναι περιορισμένη και αναστρέψιμη.** |
| 1 | **Αμελητέα** | **Καμία επίδραση στη λειτουργία. Δεν επηρεάζονται οι κρίσιμες διαδικασίες.** | **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 ή ελάχιστη επίδραση στην υγεία και ασφάλεια. Δεν προκύπτει κίνδυνος τραυματισμού ή ασθένειας.** |