Όνομα Οργανισμού

Πολιτική Διαχείρισης Συμβάντων και Περιστατικών

|  |  |
| --- | --- |
| **Περιεχόμενο:** | Πολιτική Διαχείρισης Συμβάντων και Περιστατικών |
| **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. Σκοπός 4](#_Toc155083226)

[2. Ομάδα Αντιμετώπισης Περιστατικών Ασφαλείας Πληροφοριών 4](#_Toc155083227)

[3. Πολιτική Διαχείρισης Περιστατικών Ασφαλείας 5](#_Toc155083228)

[4. Πλαίσιο Διαχείρισης Περιστατικών Ασφαλείας 6](#_Toc155083229)

[4.1. Κανόνες Διαχείρισης Περιστατικών Ασφαλείας 6](#_Toc155083230)

[4.2. Προετοιμασία και Προγραμματισμός Αντιμετώπισης Περιστατικών 9](#_Toc155083231)

[4.2.1 Χρήστες 9](#_Toc155083238)

[4.2.2 Διαχειριστές και Διαχείριση Συστημάτων 9](#_Toc155083239)

[4.2.3 Προκαθορισμένα σενάρια Περιστατικών Ασφαλείας 9](#_Toc155083240)

[4.3. Αναγνώριση, Αναφορά και Καταγραφή Περιστατικών 10](#_Toc155083241)

[4.3.1 Αναφορά περιστατικών από τους Χρήστες 10](#_Toc155083243)

[4.3.2 Αναφορά περιστατικών από συστήματα 10](#_Toc155083244)

[4.4. Διερεύνηση Περιστατικών 10](#_Toc155083245)

[4.5. Αξιολόγηση και Διαβάθμιση Περιστατικών 12](#_Toc155083246)

[4.6. Αντιμετώπιση και Μετριασμός Περιστατικών 12](#_Toc155083247)

[4.7. Αναφορά, Ανασκόπηση και Βελτίωση Ασφαλείας 12](#_Toc155083248)

[Παράρτημα Α – Φόρμα Συλλογής Πληροφοριών 14](#_Toc155083249)

# Σκοπός

Η σωστή προετοιμασία καθώς και η άμεση ανταπόκριση σε περιστατικά ασφάλειας είναι η στρατηγική που χρησιμοποιείται ούτως ώστε ένας οργανισμός να είναι σε ετοιμότητα και να βρίσκεται σε θέση να διαχειριστεί και να αντιμετωπίσει το οποιοδήποτε περιστατικό ασφάλειας συμβεί.

Σκοπός της Πολιτικής Διαχείρισης Συμβάντων και Περιστατικών είναι να καθορίσει τις απαιτήσεις για τη δημιουργία μιας αποτελεσματικής ομάδας Αντιμετώπισης Περιστατικών Ασφαλείας Πληροφορικής, καθώς και ενός ενιαίου πλαισίου για τη διαχείριση των περιστατικών ασφαλείας για τον [Όνομα Οργανισμού]. Επιπρόσθετα, σκοπός της παρούσας Πολιτικής, είναι να καθορίσει τις απαιτήσεις και ανάγκες καθώς και να περιγράψει τις κατευθυντήριες γραμμές για την υλοποίηση σχεδίου/σχεδίων άμεσης ανταπόκρισης περιστατικών ασφαλείας.

Η Πολιτική Διαχείρισης Συμβάντων και Περιστατικών Ασφάλειας απευθύνεται στο προσωπικό του [Όνομα Οργανισμού], στους προμηθευτές, και σε τρίτους που δραστηριοποιούνται εκ μέρους του [Όνομα Οργανισμού].

# Ομάδα Αντιμετώπισης Περιστατικών Ασφαλείας Πληροφοριών

Ο [Όνομα Οργανισμού], προκειμένου να βρίσκεται σε θέση να μπορεί να διαχειρίζεται κρίσιμα περιστατικά ασφαλείας ή/και περιστατικά μείζονος καταστροφής, καθώς και να προστατεύει τόσο τα πληροφοριακά συστήματα και τις πληροφορίες του, όσο και τη συνέχιση των εργασιών του, πρέπει να διαθέτει μια εσωτερική ομάδα Αντιμετώπισης Περιστατικών Ασφαλείας Πληροφοριών (Security Incident Response Team). Η εν λόγω ομάδα καθορίζεται από την Γενική Διεύθυνση και [αρμόδιο τμήμα Ανθρώπινου Δυναμικού].

Η εσωτερική ομάδα, πρέπει να παρέχει υπηρεσίες, με σκοπό να περιορίζει, να μετριάζει και να αποτρέπει το εύρος ζημίας στα περιστατικά ασφαλείας, καθώς και να προστατεύει τόσο τα πληροφοριακά συστήματα και τις πληροφορίες τους, όσο και την συνέχιση των εργασιών της [Όνομα Οργανισμού]. Η εν λόγω ομάδα πρέπει να εμπλέκεται σε κρίσιμα περιστατικά ασφαλείας σε περιστατικά μείζονος καταστροφής, καθώς και σε οποιαδήποτε άλλα περιστατικά κρίνεται ότι η εμπλοκή της είναι απαραίτητη. Επιπρόσθετα η ομάδα δύναται να συνεργάζεται με άλλα τρίτα μέρη. Συγκεκριμένα η εν λόγω ομάδα πρέπει να συνεργάζεται και να έχει επικοινωνία (όπου προκύπτει ανάγκη) με τρίτα μέρη όπως:

* Τον πάροχο δικτύου (ISP)
* Τους προμηθευτές συστήματος (όπου εμπλέκονται σε περιστατικό)
* Άλλες ομάδες CSIRT (π.χ. Ομάδα CSIRT της ΚΤΚ, Εθνική Ομάδα CSIRT, ΓΕΡΗΕΤ κ.τ.λ.)

Περαιτέρω, σε περιπτώσεις ακραίων περαστικών ασφάλειας, συμπεριλαμβανομένων των παραβιάσεων των δεδομένων, η εν λόγω ομάδα, όπου απαιτείται πρέπει να ενημερώνει:

* Την Εποπτική Αρχή
* Το Γραφείο Επίτροπου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα), σε συνεργασία με τον ΥΠΔ
* τις αρμόδιες διωκτικές αρχές (Αστυνομία Κύπρου). Η διερεύνηση των εν λόγω περιστατικών ενδέχεται να γίνεται σε συνεργασία με τις εν λόγω αρχές.

Η εσωτερική Ομάδα Αντιμετώπισης Περιστατικών Ασφαλείας Πληροφοριών πρέπει να στελεχώνεται από άτομα διαφορετικών αρμοδιοτήτων και εξειδίκευσης. Επίσης η εν λόγω ομάδα πρέπει να είναι καταγεγραμμένη σε πίνακα που να περιλαμβάνει το ρόλο και τα στοιχεία επικοινωνίας για το κάθε μέλος.

# Πολιτική Διαχείρισης Περιστατικών Ασφαλείας

Ο Κανονισμός Κ.Δ.Π. 389/2020 διαθέτει έναν πυλώνα ΑΝΤΑΠΟΚΡΙΣΗ (RESPOND) που έχει ως στόχο να διασφαλίσει ότι οι φορείς είναι σε θέση να ανταποκρίνονται σε συμβάντα και περιστατικά που ενδέχεται να επηρεάσουν την εμπιστευτικότητα, την ακεραιότητα, τη διαθεσιμότητα ή την αυθεντικότητα πληροφοριών. Συγκεκριμένα προτείνει:

1. Ετοιμότητα και εντοπισμός συμβάντων και περιστατικών [ΕΙΜ1]:

Ο [Όνομα Οργανισμού] να είναι έτοιμος να εντοπίσει και να αντιδράσει σε περίπτωση σοβαρού συμβάντος ή περιστατικού που αφορά την ασφάλεια πληροφοριών ενεργοποιώντας τις αντίστοιχες διαδικασίες αντιμετώπισης περιστατικών, με γενικές δυνατότητες παρακολούθησης και ειδικές λειτουργίες παρακολούθησης της ασφάλειας, όπως τις υπηρεσίες ανίχνευσης και πρόληψης εισβολών.

1. Ανάλυση και αξιολόγηση συμβάντων και περιστατικών [ΕΙΜ2]:

Ο [Όνομα Οργανισμού] να είναι σε θέση να αναλύει και να αξιολογεί συμβάντα και περιστατικά που αφορούν την ασφάλεια πληροφοριών, ούτως ώστε να ενεργοποιεί κατάλληλες διαδικασίες περιορισμού και ανάκτησης. Λαμβάνει αιτιολογημένες αποφάσεις σχετικά με τις δράσεις και τα μέτρα που πρέπει να ληφθούν για την αντιμετώπιση ή την αποκατάσταση από συμβάντα και περιστατικά. Εξετάζει τον αντίκτυπο στα υποκείμενα δεδομένων, στις επιχειρηματικές δραστηριότητες, στα εξωτερικά μέρη και στο οικοσύστημα των φορέων. Διασφαλίζει ότι η ανάλυση και αξιολόγηση συμβάντων και περιστατικών διεκπεραιώνεται σε συνεννόηση με την ανώτατη διοίκηση για τη σύνδεση συμβάντων και περιστατικών με σενάρια υψηλού κινδύνου.

1. Περιορισμός και ανάκτηση από συμβάντα και περιστατικά [ΕΙΜ3]:

Να εξασφαλιστεί επαρκής περιορισμός και αποκατάσταση από συμβάντα και περιστατικά, ώστε να περιορίζονται στο ελάχιστο οι επιπτώσεις στα συστήματα, τις εφαρμογές, τα δίκτυα και τα δεδομένα, καθώς και να διασφαλίζονται, στο μέτρο του δυνατού, οι κρίσιμες λειτουργίες της [Όνομα Οργανισμού].

1. Δραστηριότητες μετά το συμβάν και το περιστατικό [ΕΙΜ4]:

Θέσπιση, εφαρμογή και διατήρηση διαδικασιών μετά την εκδήλωση συμβάντων και περιστατικών, προκειμένου να αποτυπωθούν τα διδάγματα που έχουν αντληθεί από τα συμβάντα και περιστατικά ασφάλειας πληροφοριών και να προσδιορίζουν κατά πόσον πρέπει να θεσπιστούν πρόσθετα μέτρα ασφάλειας για την πρόληψη παρόμοιων συμβάντων και περιστατικών. Ο [Όνομα Οργανισμού] εξετάζει το ενδεχόμενο θέσπισης εκ των υστέρων διαδικασίας, η οποία περιλαμβάνει συνάντηση για την αξιολόγηση του συμβάντος ή περιστατικού με τους επηρεαζόμενους ιδιοκτήτες του συστήματος, τους διαχειριστές δεδομένων και άλλα ενδιαφερόμενα μέρη που συμμετείχαν στην αντιμετώπιση του περιστατικού, με σκοπό την ανταλλαγή διδαγμάτων και τον προσδιορισμό προληπτικών μέτρων.

1. Ρυθμιστικές υποχρεώσεις κοινοποίησης συμβάντος και συνεργασίας [ΕΙΜ5]:

Ο [Όνομα Οργανισμού] ενημερώνει τα σχετικά ενδιαφερόμενα μέρη στην περίπτωση συμβάντων ή περιστατικών ασφάλειας, όπως περιγράφεται σε νομικές και ρυθμιστικές υποχρεώσεις. Στο πλαίσιο των δεδομένων προσωπικού χαρακτήρα, ο οργανισμός διασφαλίζει τη συμμόρφωση με τις σχετικές νομοθετικές και ρυθμιστικές διατάξεις που αφορούν την προστασία των δεδομένων προσωπικού χαρακτήρα και επικοινωνεί, όπου είναι απαραίτητο, με την αρμόδια αρχή προστασίας δεδομένων.

1. Επικοινωνία με ενδιαφερόμενους φορείς για συμβάντα και περιστατικά [ΕΙΜ6]:

Ο [Όνομα Οργανισμού] κοινοποιεί πληροφορίες σχετικά με συμβάντα και περιστατικά ασφάλειας δικτύων και πληροφοριών σε εσωτερικούς και εξωτερικούς ενδιαφερόμενους φορείς, προκειμένου να ελαχιστοποιούνται οι σχετικές επιπτώσεις και οι εκ των υστέρων δραστηριότητες προκειμένου να καθορίζονται προληπτικά μέτρα, όπως με την ΑΨΑ και τις υπηρεσίες έκτακτης ανάγκης.

# Πλαίσιο Διαχείρισης Περιστατικών Ασφαλείας

Ο [Όνομα Οργανισμού] πρέπει να διαθέτει ένα πλαίσιο Διαχείρισης Περιστατικών Ασφάλειας, προκειμένου να εξασφαλίζεται τόσο η συνεχής βελτίωση της ασφάλειας των Πληροφοριακών Συστημάτων και Πληροφοριών του [Όνομα Οργανισμού], όσο και η έγκαιρη και αποτελεσματική ανταπόκριση σε περιστατικά ασφαλείας. Το εν λόγω πλαίσιο πρέπει να αποτελείται από μια συνεχή διαδικασία (continues cycle) που να περιλαμβάνει τουλάχιστο τα στάδια που απεικονίζονται πιο κάτω. Σημειώνεται πως ο [Όνομα Οργανισμού] πρέπει να διανέμει αντίγραφα του σχεδίου αντιμετώπισης συμβάντων σε όλους τους εμπλεκόμενους για να είναι σε ετοιμότητα ανά πάσα στιγμή και για να είναι ενημερωμένοι σε περίπτωση περιστατικού.

# Κανόνες Διαχείρισης Περιστατικών Ασφαλείας

1. Αναφορά Περιστατικών

* Όλοι οι υπεύθυνοι των περιουσιακών αγαθών του [Όνομα Οργανισμού], οι διαχειριστές περιουσιακών αγαθών, οι χρήστες καθώς επίσης και τα τρίτα μέρη (προμηθευτές, συνεργάτες, κλπ.), έχουν την ευθύνη να αναφέρουν τυχόν περιστατικά που επηρεάζουν ή ενδέχεται να επηρεάσουν το επίπεδο ασφάλειας του [Όνομα Οργανισμού].
* Ο [Όνομα Οργανισμού] διασφαλίζει ότι διατίθενται επαρκείς πόροι για την αποτελεσματική διαχείριση και αντιμετώπιση περιστατικών ασφαλείας.
* Θα πρέπει να υπάρχει επίσημα καταγεγραμμένη Διαδικασία Διαχείρισης Περιστατικών προκειμένου να αντιμετωπίζονται τα περιστατικά ασφάλειας πληροφοριών έγκαιρα και αποτελεσματικά, αναφέροντας τυχόν παραβιάσεις, συμβάντα, ή αδυναμίες στο τμήμα πληροφορικής το συντομότερο δυνατό.
* Η Διαδικασία Διαχείρισης Περιστατικών θα πρέπει να δοκιμάζεται τουλάχιστον μία φορά το χρόνο.
* Ο Υπεύθυνος Ασφάλειας Πληροφοριών πρέπει να διασφαλίζει ότι όλοι οι εργαζόμενοι και τα σχετικά τρίτα μέρη γνωρίζουν τη διαδικασία.
* Ο [Όνομα Οργανισμού] διασφαλίζει ότι όλοι οι χρήστες είναι εκπαιδευμένοι για να εντοπίζουν και να αναφέρουν περιστατικά ασφάλειας πληροφοριών. Παραδείγματα περιστατικών ασφάλειας πληροφοριών είναι:
* Κακόβουλο λογισμικό (π.χ. virus/worm/ trojan/ κλπ.),
* Κοινωνική Μηχανική (Social Engineering),
* Μη εξουσιοδοτημένη αποκάλυψη ευαίσθητων πληροφοριών,
* Κλοπή περιουσιακών στοιχείων (π.χ. φορητός υπολογιστής, κινητό, ευαίσθητα έγγραφα κλπ.),
* Ύποπτα μηνύματα ηλεκτρονικού ταχυδρομείου (π.χ. spam, phishing emails),
* Κατάχρηση συστημάτων από υπαλλήλους ή τρίτα μέρη,
* Βλάβες συστήματος λόγω ύποπτης κακόβουλης πράξης,
* Φυσικές καταστροφές (π.χ. σεισμός, πλημμύρα, πυρκαγιά, κλπ.),
* Παραβίαση πολιτικών και διαδικασιών ασφάλειας πληροφοριών.

1. Απόκριση σε Περιστατικά

* Θα πρέπει να συγκροτηθεί μία Ομάδα Απόκρισης σε Περιστατικά (ΟΑΠ) προκειμένου να συντονίσει τις δραστηριότητες διαχείρισης των περιστατικών ασφαλείας, η οποία θα περιλαμβάνει τα ακόλουθα μέλη:
* Υπεύθυνος Ασφάλειας Πληροφοριών,
* Υπεύθυνος πληροφοριακού αγαθού (κατά περίπτωση),
* Τεχνικό, εξειδικευμένο προσωπικό (ανάλογα με τη φύση του συμβάντος).
* Ο Υπεύθυνος Ασφάλειας Πληροφοριών μπορεί να αλλάξει τη σύνθεση των μελών της ομάδας λαμβάνοντας υπόψη την κρισιμότητα και τον τύπο του συμβάντος.
* Τα περιστατικά πρέπει να ιεραρχηθούν και να κατηγοριοποιηθούν σύμφωνα με τη Διαδικασία Διαχείρισης Περιστατικών, λαμβάνοντας υπόψη την κρισιμότητα των πληροφοριών/ πόρων οι οποίοι επηρεάστηκαν από το συμβάν.
* Οι χρήστες δεν θα παρεμβαίνουν στα συστήματα τα οποία επηρέασε το περιστατικό για σκοπούς διαχείρισης ή επίλυσης προβλημάτων, εκτός εάν έχουν εξουσιοδοτηθεί καταλλήλως. Μόνο η Ομάδα Απόκρισης σε Περιστατικά αναλαμβάνει την επαναφορά των συστημάτων στην κανονική λειτουργία.
* Οι χρήστες δεν θα εκμεταλλεύονται τις αδυναμίες ή τα περιστατικά ώστε να αποκτούν πρόσβαση σε μη εξουσιοδοτημένες πληροφορίες.
* Όλο το προσωπικό και τα τρίτα μέρη θα πρέπει να συνεργάζονται πλήρως με τη διερεύνηση περιστατικών ασφάλειας πληροφοριών.
* Τα συστήματα τα οποία συνδέονται με τα παραβιασμένα συστήματα πρέπει να ελέγχονται προκειμένου να εντοπίζονται πιθανές ευπάθειες ασφαλείας που θα μπορούσαν να διευρύνουν τις επιπτώσεις του περιστατικού.
* Όλοι οι ενδιαφερόμενοι (π.χ. χρήστες, πελάτες, διοίκηση, κλπ.) πρέπει να ενημερώνονται σχετικά με την πρόοδο των περιστατικών, όπως είναι απαραίτητο και όταν χρειάζεται.
* Ο [Όνομα Οργανισμού] πρέπει να χρησιμοποιήσει τα συμβάντα τα οποία είναι αποτέλεσμα αδυναμιών της υποδομή ασφαλείας του για να διασφαλίσει την προληπτική αντιμετώπιση περιστατικών. Η υποδομή ασφαλείας περιλαμβάνει, μεταξύ άλλων:
* Τείχος Προστασίας (Firewall),
* Συστήματα ανίχνευσης/ πρόληψης εισβολής (IPS/ IDS),
* Σύστημα αντιμετώπισης κακόβουλου λογισμικού (Antivirus).

1. Συλλογή Τεκμηρίωσης

* Ο [Όνομα Οργανισμού] συλλέγει αποδεικτικά στοιχεία που σχετίζονται με περιστατικά ασφάλειας πληροφοριών.
* Όλα τα αρχεία και τα αποδεικτικά στοιχεία που συλλέγονται σχετικά με περιστατικά ασφάλεiας πρέπει να διασφαλίζονται για ανάλυση μετά το συμβάν.
* Η συλλογή και διάδοση των σχετικών αποδεικτικών στοιχείων συμβάντων ασφάλειας πληροφοριών θα πρέπει να είναι σύμφωνη με τους ισχύοντες τοπικούς νόμους και κανονιστικά πλαίσια ώστε διασφαλίζεται η ακεραιότητά τους.

1. Ανάλυση και Διορθωτικές Ενέργειες (Μετά από Περιστατικό)

* Η απόκριση σε περιστατικά περιλαμβάνει την υποβολή επίσημης έκθεσης που περιγράφει το συμβάν καθώς και τις κατάλληλες διορθωτικές ενέργειες που έχουν ληφθεί.
* Η αναφορά περιστατικών ασφάλειας πληροφοριών κατατάσσεται, από προεπιλογή, ως Εμπιστευτική, ανεξάρτητα από τη σοβαρότητα ή την αξιολόγηση του συμβάντος.
* Ο [Όνομα Οργανισμού] θα διεξάγει ανάλυση αιτίας των περιστατικών ασφάλειας και θα προσδιορίζει προληπτικά μέτρα που πρέπει να ληφθούν για την αποφυγή παρόμοιων συμβάντων στο μέλλον.
* Τα «μαθήματα» που αντλήθηκαν από περιστατικά (δηλ. βάση γνώσεων) πρέπει να τεκμηριώνονται και να διατίθενται στο προσωπικό του τμήματος πληροφορικής για τη διαχείριση μελλοντικών περιστατικών.
* Η Διευθύνουσα Επιτροπή Ασφάλειας Πληροφοριών θα ενημερώνεται για τον όγκο, τις τάσεις και τους τύπους περιστατικών ασφάλειας πληροφοριών, προκειμένου να αποφασίζει για περαιτέρω βελτιώσεις στην ασφάλεια των πληροφοριών ώστε να μειωθεί η πιθανότητα μελλοντικών συμβάντων.
* Το αποτέλεσμα της ανάλυσης περιστατικών ενδέχεται να οδηγήσουν σε αναθεώρηση των υφιστάμενων πολιτικών, στην ανάπτυξη πρόσθετων δικλείδων ασφάλειας και στη πραγματοποίηση προγραμμάτων ευαισθητοποίησης των χρηστών.

# Προετοιμασία και Προγραμματισμός Αντιμετώπισης Περιστατικών

Ο [Όνομα Οργανισμού] πρέπει πάντα να βρίσκεται σε ετοιμότητα, προκειμένου να μπορεί τόσο να ανιχνεύει ένα περιστατικό το οποίο ενδέχεται να λάβει χώρα οποιαδήποτε στιγμή, όσο και να το διαχειρίζεται.



### Χρήστες

Ως εκ τούτου, οι χρήστες που δραστηριοποιούνται εκ μέρους του [Όνομα Οργανισμού], πρέπει να τυγχάνουν σχετικής και συνεχής ενημέρωσης/επαγρύπνησης/εκπαίδευσης σχετικά με το πώς να ανιχνεύουν, να επιλύουν (όπου είναι εφικτό), αλλά και να αναφέρουν ένα περιστατικό ασφαλείας.

### Διαχειριστές και Διαχείριση Συστημάτων

Περαιτέρω, οι διαχειριστές των συστημάτων, πρέπει να λαμβάνουν τα απαραίτητα μέτρα ελέγχου καθώς και να καθορίζουν τις απαραίτητες δικλίδες ασφαλείας, σύμφωνα με την Πολιτική Ασφάλειας, τις διαδικασίες, τις οδηγίες, τις βέλτιστες πρακτικές, τις αξιολογήσεις επικινδυνότητας, τις αναφορές ελέγχου κλπ. Επίσης, τα «γνωστά» περιστατικά ασφαλείας τα οποία έλαβαν χώρα στο παρελθόν, πρέπει να λαμβάνονται υπόψη από τους διαχειριστές, προκειμένου να καθορίσουν κανόνες ανίχνευσης ή/και αποτροπής περιστατικών παρόμοιας φύσης που πιθανόν να λάβουν χώρα στο μέλλον.

### Προκαθορισμένα σενάρια Περιστατικών Ασφαλείας

Ο [Όνομα Οργανισμού] πρέπει να αναπτύξει προκαθορισμένα σενάρια περιστατικών ασφαλείας και σχέδια επιχειρηματικής συνέχειας για κάθε πληροφορικό σύστημα ή/και υπηρεσία. Τα εν λόγω σχέδια είναι απαραίτητα, προκειμένου ο [Όνομα Οργανισμού], να είναι σε ετοιμότητα να αντιμετωπίσει αποτελεσματικά το οποιοδήποτε περιστατικό δύναται να συμβεί. Η ομάδα Αντιμετώπισης Περιστατικών Ασφαλείας Πληροφοριών, πρέπει να αναπτύξει τέτοια σχέδια τόσο για τα διάφορα συστήματα και υπηρεσίες του [Όνομα Οργανισμού], όσο και για τις διάφορες απειλές που μπορούν να λάβουν χώρα.

Για παράδειγμα τα σενάρια απειλών που αντιμετωπίζουν τα πληροφοριακά συστήματα ή/και οι υπηρεσίες του [Όνομα Οργανισμού] θα πρέπει να περιλαμβάνουν τουλάχιστο τα ακόλουθα

* Φυσικά φαινόμενα (π.χ. σεισμός, πλημύρα)
* Πυρκαγιά
* Επιθέσεις τύπου DDoS
* Εισβολή από κακόβουλους χρήστες/μη εξουσιοδοτημένη πρόσβαση
* Μόλυνση συστημάτων από κακόβουλα λογισμικά
* Διαρροή προσωπικών δεδομένων πελατών του [Όνομα Οργανισμού]
* Κατασκοπία
* Πόλεμος
* Απάτη (εσωτερική και εξωτερική)
* Operating system and software failure
* Hardware Failure
* Παραβίαση κανονιστικού πλαισίου που διέπει τη λειτουργία του [Όνομα Οργανισμού]

# Αναγνώριση, Αναφορά και Καταγραφή Περιστατικών

Ο [Όνομα Οργανισμού] πρέπει να διαθέτει κατάλληλες διαδικασίες για την έγκαιρη αναγνώριση και αναφορά οποιονδήποτε αναφορών περιστατικών ασφάλειας. Επιπρόσθετα ο [Όνομα Οργανισμού] πρέπει να διαθέτει ένα κεντρικό Μητρώο αναφοράς και διαχείρισης περιστατικών ασφάλειας, προκειμένου να συμβάλει στη βελτίωση της ασφάλειας των πληροφοριακών συστημάτων, πληροφοριών και υπηρεσιών, του [Όνομα Οργανισμού]. Στο εν λόγω Μητρώο πρέπει να εξασφαλίζεται ότι καταγράφονται, συλλέγονται, αποθηκεύονται, προστατεύονται και αναλύονται όλα τα περιστατικά σχετικά με την ασφάλεια των πληροφοριακών συστημάτων και πληροφοριών. Διασφαλίζεται επίσης πως σε καμία περίπτωση δεν θα έχει πρόσβαση στο μητρώο τρίτο πρόσωπο ή άτομο το οποίο δεν είναι μέλος της Ομάδας Αντιμετώπισης Περιστατικών. Το μητρώο αυτό πρέπει να αναθεωρείται και να επικαιροποιείται αν τακτά διαστήματα και να είναι κρυπτογραφημένο. Πιθανοί τρόποι εντοπισμού περιστατικών:

* Από χρήστες
* Από ενημέρωση πελατών
* Από Σύστημα Παρακολούθησης
* Από εξωτερικούς συνεργάτες
* Από ελέγχους ασφάλειας

### Αναφορά περιστατικών από τους Χρήστες

Όλο το προσωπικό του [Όνομα Οργανισμού], έχει υποχρέωση να αναφέρει το οποιοδήποτε περιστατικό (δραστηριότητα ή ανησυχία ή υποψία) μπορεί να βλάψει έμμεσα ή άμεσα την ασφάλεια των πληροφοριακών συστημάτων ή/και των πληροφοριών του [Όνομα Οργανισμού]. Για την αναφορά των περιστατικών από τους χρήστες, πρέπει να ακολουθείται σχετική διαδικασία για «αναφορά περιστατικών ασφάλειας», ούτως ώστε οι χρήστες να μπορούν να αναφέρουν και να περιγράψουν το περιστατικό έγκαιρα και με ακρίβεια. Η διαδικασία πρέπει να περιλαμβάνει διεργασία αναφοράς του περιστατικού στο κεντρικό μητρώο αναφοράς περιστατικών. Νοείται ότι οι χρήστες των πληροφοριακών συστημάτων, πρέπει να είναι ενημερωμένοι με την σχετική διαδικασία και τον τρόπο αναφοράς του οποιοδήποτε περιστατικού ή/και ανησυχία σχετική με την ασφάλεια.

### Αναφορά περιστατικών από συστήματα

Τα ημερολόγια των συστημάτων του [Όνομα Οργανισμού] πρέπει να συσσωρεύονται, προκειμένου να αποφεύγονται περιστατικά και να επιτυγχάνεται η άμεση ανταπόκριση των ευπαθειών ή της κακόβουλης εισβολής στα πληροφοριακά συστήματα και πληροφορίες.

# Διερεύνηση Περιστατικών

Ο [Όνομα Οργανισμού] πρέπει να στελεχώνεται με λειτουργό διερεύνησης περιστατικών ασφάλειας. Ο λειτουργός διερεύνησης περιστατικών, πρέπει να ενημερώνεται για το πιθανό περιστατικό. Σε περίπτωση που ενημερωθεί τηλεφωνικός, ο εν λόγω λειτουργός, θα πρέπει να αναφέρει το γεγονός ώστε να καταγραφεί το περιστατικό στο μητρώο αναφοράς περιστατικών.

Συγκεκριμένα ο εν λόγω λειτουργός αρχικά πρέπει να συλλέγει και να αναλύει τις απαραίτητες πληροφορίες ώστε να διερευνήσει και να προχωρήσει σε προκαταρτική αξιολόγηση. Οι απαραίτητες πληροφορίες πρέπει να περιλαμβάνουν τουλάχιστο τα πιο κάτω:

* Γενική περιγραφή του περιστατικού.
* Ημερομηνία και ώρα αρχικής αναφοράς Περιστατικού.
* Πρόσωπο/Υπάλληλος/Σύστημα που εντόπισε/αναγνώρισε το περιστατικό.
* Εάν το περιστατικό και συνεπακόλουθες συνέπειες που μπορεί να προκληθούν συνεχίζονται ή τερματίστηκαν.
* Εκτιμώμενη χρονική περίοδος διάρκειας περιστατικού.
* Επηρεαζόμενα συστήματα πληροφορικής ή άλλες φανερές συνέπειες.
* Άλλες λειτουργικές ή επιζήμιες συνέπειες.
* Συλλογή άλλων επιπρόσθετων πληροφοριών (logs, evidences, κλπ.)

Σχετική φόρμα υπάρχει στο Παράρτημα Α του παρόντος εγγράφου.

Ο εν λόγω λειτουργός πρέπει αρχικά να διερευνήσει το περιστατικό. Η διερεύνηση πρέπει να περιλαμβάνει τουλάχιστο τα ακόλουθα.

* Συσχετισμό περιστατικού με Σύστημα/Υπηρεσία: Το περιστατικό θα πρέπει να συσχετίζεται με το σύστημα ή/και την υπηρεσία που αντιμετωπίζει το τρέχον περιστατικό.
* Κατηγοριοποίηση περιστατικού:
* Διαβάθμιση περιστατικού: Το περιστατικό πρέπει να αξιολογείται και να διαβαθμίζεται σύμφωνα με το βαθμό σημαντικότητα του
  + Κρίσιμης σημαντικότητας
  + Υψηλής σημαντικότητας
  + Μέτριας σημαντικότητας
  + Χαμηλής σημαντικότητας
  + Ψευδές θετικό (False positive)

Σε περίπτωση που το περιστατικό διαβαθμιστεί ως:

* “Ψευδές Θετικό (false positive)” ο λειτουργός διερεύνησης περιστατικών πρέπει να ενημερώνει για επικύρωση.
* Κρίσιμης σημαντικότητας περιστατικό ή/και περιστατικό που ενδέχεται να επιφέρει σημαντικές ή/και καταστροφικές συνέπειες στον [Όνομα Οργανισμού], ο λειτουργός διερεύνησης περιστατικών ειδοποιεί άμεσα την ομάδα Αντιμετώπισης Περιστατικών Ασφαλείας Πληροφοριών για περαιτέρω χειρισμό του εν λόγω περιστατικού.
* Υψηλής, Μέτριας ή Χαμηλής σημαντικότητας ο λειτουργός διερεύνησης περιστατικών αποστέλλει/αναθέτει το περιστατικό σε λειτουργό επίλυσης/διόρθωσης περιστατικών, ανάλογα με τον τύπο και είδος του περιστατικού, για περαιτέρω χειρισμό.

# Αξιολόγηση και Διαβάθμιση Περιστατικών

Στην περίπτωση που ένα περιστατικό ανατεθεί στον λειτουργό επίλυσης/διόρθωσης περιστατικών, πρέπει να επαναξιολογηθεί. Η διερεύνηση θα πρέπει να περιλαμβάνει τουλάχιστο τα ακόλουθα:

* Συσχετισμός περιστατικού με Σύστημα/Υπηρεσία: Το περιστατικό θα πρέπει να συσχετίζεται με το σύστημα ή/και την υπηρεσία που αντιμετωπίζει το τρέχον περιστατικό.
* Κατηγοριοποίηση περιστατικού
* Διαβάθμιση περιστατικού: Το περιστατικό θα πρέπει να αξιολογείται και να διαβαθμίζεται σύμφωνα με το βαθμό σημαντικότητας του:
  + Κρίσιμης σημαντικότητας
  + Υψηλής σημαντικότητας
  + Μέτριας σημαντικότητας
  + Χαμηλής σημαντικότητας
  + Ψευδές θετικό (False positive)

Σημειώνεται ότι στην περίπτωση όπου υπάρχει προκαθορισμένο σενάριο/σχέδιο επιχειρηματικής συνέχειας για την αντιμετώπιση ενός περιστατικού, πρέπει αυτό να εκτελείται/εφαρμόζεται άμεσα και παράλληλα να ενημερώνεται η ομάδα Αντιμετώπισης Περιστατικών Ασφαλείας Πληροφοριών.

Επιπρόσθετα, στην περίπτωση που λειτουργός επίλυσης, διαβαθμίσει το περιστατικό ως κρίσιμης σημαντικότητας, ή κρίνει ότι το περιστατικό ενδέχεται να επιφέρει σημαντικές ή/και καταστροφικές συνέπειες στον [Όνομα Οργανισμού], πρέπει άμεσα να ειδοποιείται η ομάδα Αντιμετώπισης Περιστατικών Ασφαλείας Πληροφοριών για τον περαιτέρω χειρισμό του εν λόγω περιστατικού.

# Αντιμετώπιση και Μετριασμός Περιστατικών

Στην συνέχεια εφόσον το περιστατικό έχει διαβαθμιστεί, ο λειτουργός επίλυσης, πρέπει να λάβει τις ανάλογες ενέργειες προκειμένου το περιστατικό να αντιμετωπιστεί λαμβάνοντας υπόψη και τον στόχο του σημείου ανάκτησης (RPO) και τον χρόνο αποκατάστασης (RTO)Σημειώνεται ότι, σε περιπτώσεις όπου απαιτείται δαπάνη (κόστος) για να αντιμετωπιστεί το περιστατικό, ο εν λόγω λειτουργός σε συνεργασία με τον Επιχειρησιακό Ιδιοκτήτη του συστήματος που αντιμετωπίζει το περιστατικό, πρέπει να εξασφαλίσουν σχετική έγκριση από το αρμόδιο εγκριτικό τμήμα.

# Αναφορά, Ανασκόπηση και Βελτίωση Ασφαλείας

Στη συνέχεια εφόσον ο λειτουργός επίλυσης περιστατικού προβεί στις ανάλογες ενέργειες για την επίλυση του περιστατικού, ο [Υπεύθυνος Ασφάλειας Πληροφοριών] πρέπει να επικυρώσει ότι το περιστατικό έχει τύχει κατάλληλου χειρισμού.

Στην περίπτωση όπου το περιστατικό δεν έχει επιλυθεί, πρέπει να αποστέλλεται πίσω στο στάδιο «Αναγνώριση, Αναφορά και Καταγραφή Περιστατικών» για περαιτέρω διερεύνηση και ορθότερη επίλυση. Στην αντίθετη περίπτωση, όπου το περιστατικό έχει κατάλληλα επιλυθεί, ο εν λόγω επικεφαλής ή/και εκπρόσωπος του, θα πρέπει να αναφέρει το περιστατικό για καταγραφή του στο Μητρώο Γεγονότων της Ασφάλειας Πληροφοριών και στο Μητρώο Γεγονότων Λειτουργικού Κινδύνου.

Περαιτέρω, όλα τα περιστατικά θα πρέπει να είναι διαθέσιμα και να λαμβάνονται υπόψη στο αρχικό στάδιο του πλαισίου διαχείρισης περιστατικών ασφάλειας «Προετοιμασία και Προγραμματισμός Αντιμετώπισης Περιστατικών». Πιο συγκεκριμένα:

* Τα περιστατικά πρέπει να καταγράφονται και να αρχειοθετούνται για μελλοντική αναφορά και χρήση.
* Τα καταγεγραμμένα περιστατικά πρέπει να λαμβάνονται υπόψη κατά τη διάρκεια της υλοποίησης διαδικασιών, οδηγιών και τεχνικών λύσεων ασφάλειας συστημάτων και πληροφοριών.

# Παράρτημα Α – Φόρμα Συλλογής Πληροφοριών

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Μητρώο Περιστατικού | | | | | |
| Όνομα: |  |  |  | Ημερομηνία: |  |
| Επίθετο: |  |  |  | Ώρα: |  |
| Τμήμα: |  |  |  | Διάρκεια: |  |
|  |  |  |  |  |  |
| Ποιος εντόπισε/αναγνώρισε το περιστατικό; | | | | | |
|  | | | | | |
| Περιγραφή περιστατικού | | | | | |
|  | | | | | |
| Συνεπακόλουθες συνέπειες; | | | | | |
|  | | | | | |
| Επηρεαζόμενα Συστήματα | | | | | |
|  | | | | | |
| Άλλες λειτουργικές ή επιζήμιες συνέπειες; | | | | | |
|  | | | | | |