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. Εισαγωγή 4](#_Toc187845501)

[1.1. Σκοπός 4](#_Toc187845502)

[1.2. Πεδίο Εφαρμογής 4](#_Toc187845503)

[2. Πολιτική Διαχείρισης Συμβάντων και Περιστατικών 5](#_Toc187845504)

[2.1. Ετοιμότητα και εντοπισμός συμβάντων και περιστατικών (ΕΙΜ1) 5](#_Toc187845505)

[2.2. Ανάλυση και αξιολόγηση συμβάντων και περιστατικών (ΕΙΜ2) 6](#_Toc187845506)

[2.2.1. Ταξινόμηση Περιστατικών 6](#_Toc187845507)

[2.3. Περιορισμός και ανάκτηση από συμβάντα και περιστατικά (ΕΙΜ3) 7](#_Toc187845508)

[2.3.1. Ομάδα Αντιμετώπισης Περιστατικών Ασφαλείας Πληροφοριών 8](#_Toc187845509)

[2.4. Δραστηριότητες μετά το συμβάν και το περιστατικό (ΕΙΜ4) 9](#_Toc187845510)

[2.5. Ρυθμιστικές υποχρεώσεις κοινοποίησης συμβάντος και συνεργασίας (ΕΙΜ5) 10](#_Toc187845511)

[2.6. Επικοινωνία με ενδιαφερόμενους φορείς για συμβάντα και περιστατικά (ΕΙΜ6): 11](#_Toc187845512)

[3. Αναθεώρηση 11](#_Toc187845513)

[4. Αναφορές 12](#_Toc187845514)

# Εισαγωγή

# Σκοπός

Η ορθή προετοιμασία καθώς και η άμεση ανταπόκριση σε περιστατικά ασφάλειας πληροφοριών/κυβερνοασφάλειας είναι η στρατηγική που χρησιμοποιείται ώστε ο [Όνομα Οργανισμού] να είναι σε ετοιμότητα και να βρίσκεται σε θέση να διαχειριστεί και να αντιμετωπίσει το οποιοδήποτε περιστατικό ασφάλειας συμβεί με τις ελάχιστες επιπτώσεις στη λειτουργία του.

Πιο συγκεκριμένα ο σκοπός της παρούσας πολιτικής περιλαμβάνει τους τρείς (3) πιο κάτω ενδεικτικούς όρους πολιτικής:

1. To καθορισμό μίας δομημένης προσέγγισης για την αποτελεσματική διαχείριση συμβάντων και περιστατικών ασφαλείας, ώστε να ελαχιστοποιηθούν οι επιπτώσεις στη λειτουργία του [Όνομα Οργανισμού].
2. Την εξασφάλιση ότι όλα τα περιστατικά ασφάλειας πληροφοριών/ κυβερνοασφάλειας καταγράφονται, αναλύονται, και αντιμετωπίζονται σύμφωνα με τις βέλτιστες πρακτικές και τις ισχύουσες νομικές και άλλες κανονιστικές απαιτήσεις (π.χ. Απόφαση Κ.Δ.Π. 39/2022)
3. Την προστασία των δεδομένων , των συστημάτων, καθώς και της φήμης του [Όνομα Οργανισμού] μέσω μιας συντονισμένης αντίδρασης με τη δημιουργία μιας αποτελεσματικής ομάδας Αντιμετώπισης Περιστατικών Ασφαλείας Πληροφορικής για διαχείριση περιστατικών και συμβάντων, προάγοντας την ασφάλεια και ελαχιστοποιώντας την επανάληψη παρόμοιων περιστατικών.

# Πεδίο Εφαρμογής

Η Πολιτική Διαχείρισης Συμβάντων και Περιστατικών του [Όνομα Οργανισμού] αναφέρεται σε όλα τα συμβάντα και τα περιστατικά που ενδέχεται να επηρεάσουν την ασφάλεια, τη λειτουργικότητα και τη φήμη του [Όνομα Οργανισμού], ανεξάρτητα από την προέλευση ή τη φύση τους. Εφαρμόζεται σε όλα τα τμήματα, τις λειτουργίες και τα επίπεδα του οργανισμού και πιο συγκεκριμένα σε:

* όλο το προσωπικό, προμηθευτές, και εξωτερικούς συνεργάτες που έχουν πρόσβαση στα συστήματα του [Όνομα Οργανισμού].
* Όλα τα πληροφοριακά συστήματα και υποδομές, τις βάσεις δεδομένων, τα δίκτυα, του [Όνομα Οργανισμού].
* σε όλα τα κτήρια, υποκαταστήματα, τις λειτουργικές μονάδες και τις φυσικές εγκαταστάσεις του [Όνομα Οργανισμού], ανεξαρτήτως γεωγραφικής τοποθεσίας.

Η Πολιτική καλύπτει όλα τα είδη περιστατικών όπως κυβερνοεπιθέσεις, παραβιάσεις δεδομένων, τεχνικές αστοχίες, και φυσικές καταστροφές και αποτελεί αναπόσπαστο μέρος της στρατηγικής διαχείρισης κινδύνων του [Όνομα Οργανισμού].

# Πολιτική Διαχείρισης Συμβάντων και Περιστατικών

# Ετοιμότητα και εντοπισμός συμβάντων και περιστατικών (ΕΙΜ1)

Ο [Όνομα Οργανισμού] είναι έτοιμος να εντοπίσει και να αντιδράσει σε περίπτωση σοβαρού συμβάντος ή περιστατικού που αφορά την ασφάλεια πληροφοριών ενεργοποιώντας τις αντίστοιχες διαδικασίες. Αυτές οι διαδικασίες πρέπει να είναι ευθυγραμμισμένες με τις γενικές δυνατότητες παρακολούθησης και τις ειδικές λειτουργίες παρακολούθησης της ασφάλειας του [Όνομα Οργανισμού] (π.χ. υπηρεσίες ανίχνευσης και πρόληψης εισβολών.

Ο [Όνομα Οργανισμού] διαθέτει και διατηρεί ένα σχέδιο διαχείρισης και αντιμετώπισης συμβάντων και περιστατικών, εγκεκριμένο από την διοίκηση του [Όνομα Οργανισμού], το οποίο πρέπει να:

* Παρέχει στον [Όνομα Οργανισμού] καθοδήγηση για την ανάπτυξη της ικανότητας απόκρισης σε συμβάντα και περιστατικά.
* Περιγράφει τη δομή και την οργάνωση της ικανότητας απόκρισης σε συμβάντα και περιστατικά.
* Παρέχει μία γενική προσέγγιση για το πώς η ικανότητα απόκρισης σε συμβάντα και περιστατικά ενσωματώνεται στον [Όνομα Οργανισμού].
* Πληροί τις μοναδικές απαιτήσεις του [Όνομα Οργανισμού] που σχετίζονται με την αποστολή, το μέγεθος, τη δομή και τις λειτουργίες του.
* Ορίζει τα περιστατικά ασφάλειας για τα οποία πρέπει να υποβάλλονται σχετικές αναφορές.
* Παρέχει δείκτες απόδοσης (KPI) για τη μέτρηση της ικανότητας απόκρισης σε συμβάντα και περιστατικά εντός του [Όνομα Οργανισμού].
* Καθορίζει τους πόρους και την διοικητική υποστήριξη που απαιτούνται για την αποτελεσματική διατήρηση και ανάπτυξη της ικανότητας απόκρισης σε συμβάντα και περιστατικά.

Ο [Όνομα Οργανισμού] διανέμει αντίγραφα του σχεδίου/πλάνου διαχείρισης συμβάντων και περιστατικών σε όλους τους σχετικούς εμπλεκόμενους, τόσο εσωτερικούς όσο και εξωτερικούς, και διατηρεί μια λίστα με αυτούς. Θα πρέπει να επικοινωνείτε οποιαδήποτε νέα έκδοση του σχεδίου/πλάνου σε όλους τους εμπλεκόμενους σε περίπτωση αλλαγής/αναβάθμισης του.

# 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. Η ανάλυση και η αξιολόγηση των συμβάντων και των περιστατικών αποτελούν κρίσιμα στοιχεία της διαδικασίας διαχείρισης περιστατικών του [Όνομα Οργανισμού].

Κατά το βήμα αυτό, ο [Όνομα Οργανισμού] εφαρμόζει και διατηρεί διαδικασίες που επιτρέπουν την ανάλυση και την αξιολόγηση συμβάντων και περιστατικών, ώστε να λαμβάνει αιτιολογημένες αποφάσεις σχετικά με τις δράσεις και τα μέτρα για την αντιμετώπιση ή την αποκατάσταση από συμβάντα και περιστατικά που αφορούν την ασφάλεια.

Κατά την ανάλυση και αξιολόγηση των συμβάντων και περιστατικών, εξετάζεται ο αντίκτυπος στα υποκείμενα δεδομένων, στις επιχειρηματικές δραστηριότητες, στα εξωτερικά μέρη και στο οικοσύστημα του [Όνομα Οργανισμού].

Ο [Όνομα Οργανισμού] καταγράφει τα αποτελέσματα της ανάλυσης και της αξιολόγησης των εκάστοτε συμβάντων ή περιστατικών.

Η ανάλυση και η αξιολόγηση συμβάντων και περιστατικών πρέπει να διεκπεραιώνεται σε συνεννόηση με την ανώτατη διοίκηση για την σύνδεση συμβάντων και περιστατικών με σενάρια υψηλού κινδύνου.

# Ταξινόμηση Περιστατικών

Τα συμβάντα ασφάλειας πληροφοριών πρέπει να ταξινομούνται ανάλογα την κρισιμότητα τους σε:

* **Πληροφορία:** κανένας αντίκτυπος, αλλά η ανάλυση θα μπορούσε να χρησιμοποιηθεί για τη βελτίωση των πολιτικών, διαδικασιών ή ελέγχων ασφάλειας πληροφοριών.
* **Προειδοποίηση:** χαμηλός αντίκτυπος.
* **Κρίσιμο περιστατικό**: μέτριος αντίκτυπος.
* **Έκτακτη ανάγκη**: σοβαρός αντίκτυπος.

Επιπλέον τα περιστατικά ασφάλειας πληροφορίων θα πρέπει να ταξινομούνται σε 4 κατηγορίες:

* **Πολύ σοβαρά περιστατικά**: είναι αυτά που ενεργούν σε κρίσιμα συστήματα πληροφοριών και οδηγούν σε ιδιαίτερα σοβαρή επιχειρησιακή απώλεια, ή οδηγούν σε ιδιαίτερα σημαντικό κοινωνικό αντίκτυπο.
* **Σοβαρά περιστατικά** : είναι αυτά που ενεργούν σε κρίσιμα συστήματα πληροφοριών ή σημαντικά συστήματα πληροφοριών και οδηγούν σε σοβαρή επιχειρησιακή απώλεια ή οδηγούν σε σημαντικό κοινωνικό αντίκτυπο.
* **Λιγότερο σοβαρά περιστατικά** : είναι αυτά που ενεργούν σε σημαντικά συστήματα πληροφοριών ή συστήματα πληροφοριών που δεν έχουν μεγάλο αντίκτυπο για τον [Όνομα Οργανισμού] και οδηγούν σε σημαντική επιχειρησιακή απώλεια, ή οδηγούν σε σημαντικό κοινωνικό αντίκτυπο.
* **Μικρά περιστατικά** : είναι αυτά που ενεργούν σε συστήματα πληροφοριών που δεν έχουν μεγάλο αντίκτυπο για τον [Όνομα Οργανισμού] και οδηγούν σε μικρή επιχειρησιακή απώλεια ή καμία επιχειρησιακή απώλεια, ή οδηγούν σε μικρό κοινωνικό αντίκτυπο ή χωρίς κοινωνικό αντίκτυπο.

Κάθε συμβάν ασφάλειας πληροφοριών πρέπει να αξιολογείται χρησιμοποιώντας τη συμφωνημένη κλίμακα ταξινόμησης περιστατικών και να έχει οριστεί υπεύθυνος ο οποίος αποφασίζει εάν το συμβάν πρέπει να ταξινομηθεί ως περιστατικό ασφάλειας πληροφοριών.

Η αξιολόγηση και η απόφαση ενός περιστατικού ή/και συμβάντος για επιβεβαίωση ή επανεκτίμηση ανάλογα με τη σοβαρότητα θα πρέπει να διαβιβάζεται.

# Περιορισμός και ανάκτηση από συμβάντα και περιστατικά (ΕΙΜ3)

Θα πρέπει να εξασφαλίζεται 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 του [Όνομα Οργανισμού]. Η Απόφαση 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.

Προς τούτο, ο [Όνομα Οργανισμού] διαθέτει ομάδα αντιμετώπισης περιστατικών ασφάλειας πληροφοριών (είτε εσωτερικά είτε εξωτερικά μέσω συνεργασίας με πάροχο υπηρεσιών για την διαχείριση περιστατικών) για την ανάλυση, αξιολόγηση, εκτίμηση και έρευνα των συμβάντων και περιστατικών, με σκοπό την κατανόηση των μεθόδων και των στόχων της επίθεσης( βλέπε παράγραφος 2.3.1). Η ομάδα εφαρμόζει και διατηρεί διαδικασίες για τον περιορισμό και την αποκατάσταση (ανάκαμψη) 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 του.

Η αποκατάσταση από συμβάντα και περιστατικά στον [Όνομα Οργανισμού] εξετάζεται με γνώμονα τον στόχο του σημείου ανάκτησης (RPO) και τον χρόνο αποκατάστασης (RTO). Αυτό είναι απαραίτητο για να καθοριστεί η απαιτούμενη διάρκεια και το επίπεδο των υπηρεσιών που πρέπει να αποκατασταθούν για να επανέλθει η επιχειρηματική διαδικασία μετά από ένα περιστατικό.

Τα σχέδια του [Όνομα Οργανισμού] που περιγράφουν το τρόπο λειτουργίας, τα μέτρα και τα βήματα σε περίπτωση συγκεκριμένων περιστατικών να βασίζονται στην αντίστοιχη αξιολόγηση κινδύνων και να καλύπτουν τα κυριότερα είδη απειλών και επιθέσεων, σύμφωνα με διεθνείς αναφορές και δεδομένα. Τουλάχιστον, αυτά τα σχέδια πρέπει να περιλαμβάνουν σενάρια/περιπτώσεις όπως:

* Ransomware.
* Malware.
* Κοινωνική μηχανική επίθεση (Social engineering attack).
* Επίθεση άρνησης υπηρεσίας (Denial of Service).
* Επίθεση στην αλυσίδα εφοδιασμού (Supply chain availability attack).
* Επίθεση στην φυσική ασφάλεια (Physical security attack).
* Κλοπή μέσων / συσκευών / πληροφοριών.

Τα πιο πάνω σενάρια θα πρέπει να ανανεώνονται σε τακτική βάση ανάλογα και με το τοπίο κυβερνοαπειλών (Threat Landscape) τόσο σε τοπικό όσο και σε Ευρωπαϊκό επίπεδο.

Οι ενέργειες για τον περιορισμό των επιπτώσεων στον [Όνομα Οργανισμού] πρέπει να προσαρμόζονται ανάλογα με τη σοβαρότητα του περιστατικού και τις πληροφορίες ή λειτουργίες που επηρεάζονται ή μπορεί να επηρεαστούν. Στο πλαίσιο του περιορισμού και της ανταπόκρισης, ο [Όνομα Οργανισμού] δύναται να ζητήσει βοήθεια από τις αρμόδιες αρχές όπως την Αρχή Ψηφιακής Ασφάλειας

# 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, έχει δημιουργήσει μια ομάδα Αντιμετώπισης Περιστατικών Ασφαλείας Πληροφοριών (Security Incident Response Team). Η εν λόγω ομάδα καθορίζεται από την Γενική Διεύθυνση και τα αρμόδια εμπλεκόμενα Τμήματα π.χ. Ανθρώπινου Δυναμικού, Πληροφορικής κτλ..

Όπως αναφέρθηκε και πιο πάνω η ομάδα, 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 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 έχει επικοινωνία και να συνεργάζεται (όπου προκύπτει ανάγκη) με άλλα τρίτα μέρη και εξωτερικούς συνεργάτες όπως:

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

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

* Τις Εποπτικές Αρχές.
* Το Γραφείο Επίτροπου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα), σε συνεργασία με τον Υπεύθυνος Προστασίας Δεδομένων(ΥΠΠ) του [Όνομα Οργανισμού].
* Τις αρμόδιες διωκτικές αρχές (Αστυνομία Κύπρου). Η διερεύνηση των εν λόγω περιστατικών ενδέχεται να γίνεται σε συνεργασία με τις εν λόγω αρχές.

Η 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.

# Δραστηριότητες μετά το συμβάν και το περιστατικό (ΕΙΜ4)

Ο [Όνομα Οργανισμού] εφαρμόζει και διατηρεί διαδικασίες για μετά την εκδήλωση συμβάντων και περιστατικών, προκειμένου να αποτυπωθούν τα διδάγματα που προκύπτουν από αυτά και να καθορίζεται εάν χρειάζεται να ληφθούν πρόσθετα μέτρα ασφαλείας για την πρόληψη παρόμοιων συμβάντων και περιστατικών στο μέλλον.

Για τη φάση των διδαγμάτων, πραγματοποιούνται οι εξής δραστηριότητες, οι οποίες πρέπει να είναι καταγεγραμμένες στη διαδικασία:

● Εντοπισμός των διδαγμάτων που προέκυψαν από συμβάντα και αδυναμίες στην ασφάλεια πληροφοριών.

● Αναγνώριση, επανεξέταση και υλοποίηση βελτιώσεων στα μέτρα ασφάλειας πληροφοριών.

● Επανεξέταση και βελτίωση της αξιολόγησης κινδύνου για την ασφάλεια των πληροφοριών.

● Εξέταση της αποτελεσματικότητας των διαδικασιών, των πολιτικών, των εμπλεκομένων με το περιστατικό (π.χ. Ομάδα ανταπόκρισης), της ανάλυσης και της ανάκτησης από το περιστατικό, καθώς και της αντιμετώπισης των αδυναμιών στην ασφάλεια πληροφοριών.

Με βάση τα διδάγματα που αντλήθηκαν, πρέπει να εντοπίζονται και να εφαρμόζονται βελτιώσεις στο σχέδιο διαχείρισης συμβάντων ασφάλειας πληροφοριών. Οι πληροφορίες που προκύπτουν από την αξιολόγηση των συμβάντων ή περιστατικών ασφάλειας πληροφοριών πρέπει να χρησιμοποιούνται για την αντιμετώπιση επαναλαμβανόμενων ή υψηλού αντίκτυπου περιστατικών.

Εξετάζεται η καθιέρωση μιας διαδικασίας μετά το περιστατικό, η οποία περιλαμβάνει συνάντηση με τους ιδιοκτήτες του συστήματος, τους διαχειριστές δεδομένων και άλλα εμπλεκόμενα μέρη που συμμετείχαν στην αντιμετώπιση του περιστατικού, με σκοπό την ανταλλαγή διδαγμάτων και τον προσδιορισμό προληπτικών μέτρων.

Συστήνεται όπως στις εκπαιδεύσεις του προσωπικού γίνεται χρήση πληροφοριών από πραγματικά περιστατικά ασφάλειας πληροφοριών.

# Ρυθμιστικές υποχρεώσεις κοινοποίησης συμβάντος και συνεργασίας (ΕΙΜ5)

Ο [Όνομα Οργανισμού] εφαρμόζει και διατηρεί διαδικασίες της συμμόρφωσης με ρυθμιστικές και νομοθετικές απαιτήσεις όσον αφορά την κοινοποίηση περιστατικών καθώς και διασφαλίζει ότι υπάρχουν επαρκείς διαδικασίες κοινοποίησης και υποβολής εκθέσεων για συμβάντα και περιστατικά ασφάλειας πληροφοριών στις αρμόδιες ρυθμιστικές αρχές.

Ο [Όνομα Οργανισμού] ενημερώνει τα σχετικά ενδιαφερόμενα μέρη στην περίπτωση συμβάντων ή περιστατικών ασφάλειας, όπως περιγράφεται σε νομικές και ρυθμιστικές υποχρεώσεις π.χ. βάσει της Απόφασης 39/2022. 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 (Γραφείο Επιτρόπου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα).

Προς αυτό το σκοπός, οι αρμοδιότητες και ευθύνες για την κοινοποίηση περιστατικών στις ρυθμιστικές αρχές έχουν καθοριστεί και έχουν ανατεθεί εγγράφως στα αντίστοιχα άτομα ή ρόλους. Αυτές οι αρμοδιότητες περιλαμβάνουν και τις υποχρεώσεις του Υπεύθυνου Ασφάλειας Δικτύων και Πληροφοριών.

Συστήνεται όπως σχεδιαστούν και πραγματοποιούνται σε προκαθορισμένα χρονικά διαστήματα ασκήσεις προσομοίωσης περιστατικών ασφαλείας. Επιπλέον για κάθε κοινοποίηση συμβάντος συστήνεται όπως ο [Όνομα Οργανισμού] διατηρεί πρότυπες φόρμες που συμπληρώνονται από το αρμόδιο προσωπικό για κάθε είδος περιστατικού και για την αντίστοιχη αρμόδια αρχή.

# 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 Αρχή Ψηφιακής Ασφάλειας (ΑΨΑ) και άλλες αρμόδιες αρχές ή υπηρεσίες έκτακτης ανάγκης.

Προς αυτό το σκοπό ο [Όνομα Οργανισμού] εφαρμόζει και να διατηρεί διαδικασίες για τη διασφάλιση σχετικής επικοινωνίας όσον αφορά συμβάντα και περιστατικά ασφάλειας πληροφοριών προς εξωτερικούς και εσωτερικούς αποδέκτες. Σε αυτές διατηρείται λίστα με τα σχετικά στοιχεία επικοινωνίας και τα ενδιαφερόμενα μέρη τα οποία πρέπει να ενημερωθούν στην περίπτωση συμβάντων ή περιστατικών ασφάλειας. Στη λίστα έχει καταγραφεί επίσης το χρονικό διάστημα στο οποίο πρέπει να γίνει η ενημέρωση, το είδος του περιστατικού που αφορά η ενημέρωση και το υπεύθυνο άτομο από τη πλευρά του [Όνομα Οργανισμού].

# Αναθεώρηση

Τα έγγραφα σχετικά με τη Πολιτική Διαχείρισης Συμβάντων και Περιστατικών και άλλες συναφείς διαδικασίες θα πρέπει να επανεξετάζονται και να αναθεωρούνται τουλάχιστον ετησίως ή σε περίπτωση σημαντικών περιστατικών ή συμβάντων του [Όνομα Οργανισμού] με στόχο να διασφαλίζεται ότι παραμένει επικαιροποιημένη, αποτελεσματική και ευθυγραμμισμένη με τις ανάγκες του οργανισμού, τυχόν νομικές/κανονιστικές απαιτήσεις και άλλες τεχνολογικές εξελίξεις όπως νέες αναδυόμενες απειλές, ή κατόπιν εσωτερικών ή εξωτερικών ελέγχων ή αξιολογήσεις κινδύνου κτλ.)

# Αναφορές

|  |  |  |  |
| --- | --- | --- | --- |
| **Κατηγορία** | **ID** | **Μέτρο** | **Στόχος Μέτρου** |
| Διαχείριση Συμβάντων Και Περιστατικών | EIM1 | Ετοιμότητα και εντοπισμός συμβάντων και περιστατικών | Να διασφαλίζει ότι ο οργανισμός είναι σε θέση να εντοπίζει συμβάντα και περιστατικά που ενδέχεται να συνιστούν απειλή για τους στόχους της ασφάλειας πληροφοριών του οργανισμού και να ενεργοποιεί τις αντίστοιχες διαδικασίες αντιμετώπισης περιστατικών. |
| Διαχείριση Συμβάντων Και Περιστατικών | EIM2 | Ανάλυση και αξιολόγηση συμβάντων και περιστατικών | Να διασφαλιστεί ότι ο οργανισμός 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. |
| Διαχείριση Συμβάντων Και Περιστατικών | EIM3 | Περιορισμός και ανάκτηση από συμβάντα και περιστατικά | Να εξασφαλιστεί επαρκής περιορισμός και αποκατάσταση από συμβάντα και περιστατικά ασφάλειας που επηρεάζουν αρνητικά τους στόχους ασφάλειας πληροφοριών του οργανισμού. |
| Διαχείριση Συμβάντων Και Περιστατικών | EIM4 | Δραστηριότητες μετά το συμβάν και το περιστατικό. | Να διασφαλιστεί ότι ο οργανισμός μαθαίνει από συμβάντα και περιστατικά ασφάλειας, προκειμένου να αποτρέπονται παρόμοια συμβάντα και περιστατικά στο μέλλον. |
| Διαχείριση Συμβάντων Και Περιστατικών | EIM5 | Ρυθμιστικές υποχρεώσεις κοινοποίησης συμβάντος και συνεργασίας. | Να διασφαλίσει ότι ο οργανισμός ενημερώνει τα σχετικά ενδιαφερόμενα μέρη στην περίπτωση συμβάντων ή περιστατικών ασφάλειας, όπως περιγράφεται σε νομικές και ρυθμιστικές υποχρεώσεις. |
| Διαχείριση Συμβάντων Και Περιστατικών | EIM6 | Επικοινωνία με ενδιαφερόμενους φορείς για συμβάντα και περιστατικά. | Να εξασφαλίζει ότι ο οργανισμός κοινοποιεί πληροφορίες σχετικά με συμβάντα και περιστατικά ασφάλειας δικτύων και πληροφοριών σε εσωτερικούς και εξωτερικούς ενδιαφερόμενους φορείς. |