ΔΗΜΟΣ ΚΙΛΚΙΣ

Διαδικασία Αντιμετώπισης Περιστατικών της Ασφάλειας Πληροφοριών

Information Security Incident Response Procedure

ΔΗΜΟΣ ΚΙΛΚΙΣ

Διαδικασία Αντιμετώπισης Περιστατικών της Ασφάλειας Πληροφοριών

Information Security Incident Response Procedure

Ταξινόμηση Εγγράφου:	**Εσωτερικό Έγγραφο**
Έγγραφο Ανάφ.	**GDPR-DOC-15**
Έκδοση:	1
Χρονολογημένο:	**29 Νοεμβρίου 2018**
Συντάκτης Εγγράφου:	**Proset I.K.E**

Ιστορικό Αλλαγών

Έκδοση	Ημερομηνία	Σύνοψη αλλαγών

Έγκριση

Όνομα	Θέση	Υπογραφή	Ημερομηνία

Περιεχόμενα

Κατάλογος Σχημάτων

Κατάλογος Πινάκων

1 Εισαγωγή

Το παρόν έγγραφο προορίζεται να χρησιμοποιηθεί όταν έχει συμβεί κάποιο είδος περιστατικού που επηρεάζει την ασφάλεια των πληροφοριών του «Δήμου Κιλκίς», συμπεριλαμβανομένων εκείνων που ενδεχομένως επηρεάζουν τα προσωπικά δεδομένα για τα οποία ο οργανισμός είναι υπεύθυνος. Σκοπός του είναι να εξασφαλίσει μια γρήγορη, αποτελεσματική και τακτική ανταπόκριση στην παραβίαση της ασφάλειας των πληροφοριών.

Οι διαδικασίες που ορίζονται στο παρόν έγγραφο πρέπει να χρησιμοποιούνται μόνο ως καθοδήγηση κατά την ανταπόκριση σε ένα περιστατικό. Η ακριβής φύση ενός περιστατικού και ο αντίκτυπός του δεν μπορούν να προβλεφθούν με κανένα βαθμό βεβαιότητας και, ως εκ τούτου, είναι σημαντικό να χρησιμοποιείται ένας καλός βαθμός κοινής λογικής όταν αποφασίζονται οι ενέργειες που πρέπει να γίνουν.

Ωστόσο, προβλέπεται ότι οι δομές που παρουσιάζονται εδώ θα αποδειχθούν χρήσιμες για να καταστεί δυνατή η ταχύτερη λήψη των ορθών ενεργειών και η παροχή ακριβέστερων πληροφοριών.

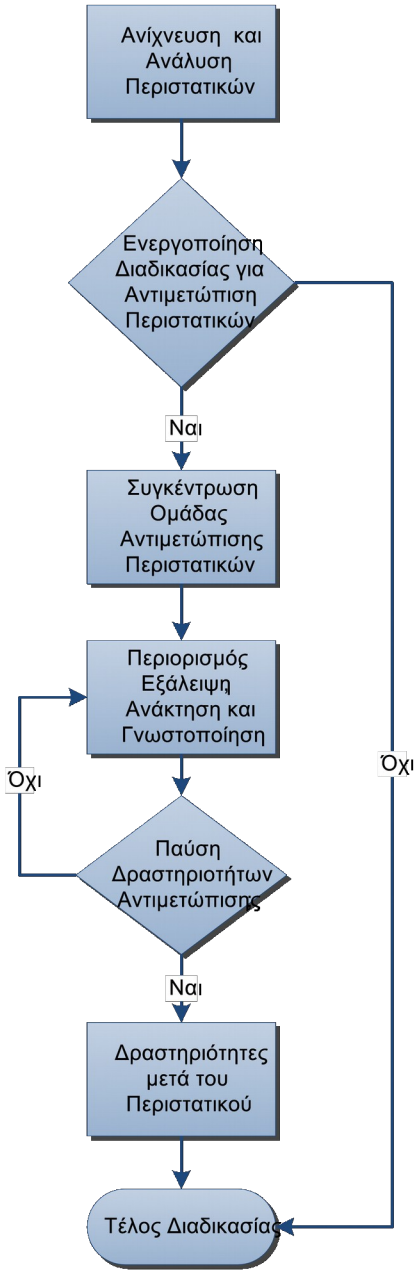
Οι στόχοι αυτής της διαδικασίας αντιμετώπισης περιστατικών είναι:

- παροχή μιας συνοπτικής επισκόπησης του τρόπου με τον οποίο ο «Δήμος Κιλκίς» θα ανταποκριθεί σε ένα περιστατικό
- ορισμός του ποιος θα ανταποκριθεί σε ένα περιστατικό και τους ρόλους και τις ευθύνες του
- περιγραφή των εγκαταστάσεων που υπάρχουν για να βοηθήσετε στη διαχείριση του συμβάντος
- καθορισμός του τρόπου με τον οποίο θα ληφθούν αποφάσεις σχετικά με την ανταπόκρισή μας σε ένα περιστατικό
- να εξηγεί πώς θα γίνεται η επικοινωνία εντός του οργανισμού και με τα εξωτερικούς φορείς
- να παρέχει στοιχεία επικοινωνίας για τους βασικούς ανθρώπους και τις εξωτερικές υπηρεσίες
- καθορισμός του τι θα συμβεί όταν επιλυθεί το περιστατικό και θα σταματήσουν οι ενέργειες αντιμετώπισης του

Όλα τα μέλη του προσωπικού που αναφέρονται σε αυτό το έγγραφο θα λάβουν ένα αντίγραφο το οποίο πρέπει να έχουν στη διάθεσή τους όταν απαιτείται.
Τα στοιχεία επικοινωνίας θα ελέγχονται και θα ενημερώνονται τουλάχιστον δύο φορές το χρόνο. Οι αλλαγές στις επαφές ή άλλες σχετικές λεπτομέρειες που προκύπτουν εκτός αυτών των προγραμματισμένων ελέγχων θα πρέπει να αποστέλλονται στη διεύθυνση ……. το συντομότερο δυνατό μετά την πραγματοποίηση της αλλαγής.
Όλες οι προσωπικές πληροφορίες που συλλέγονται στο πλαίσιο της διαδικασίας αντιμετώπισης περιστατικών και περιλαμβάνονται στο παρόν έγγραφο θα χρησιμοποιηθούν αποκλειστικά για τους σκοπούς της διαχείρισης περιστατικών ασφάλειας πληροφοριών και υπόκεινται σε σχετική νομοθεσία για την προστασία των δεδομένων

2 Διάγραμμα Ροής της Διαδικασίας Αντιμετώπισης Περιστατικών

Η ροή της διαδικασίας αντιμετώπισης περιστατικών φαίνεται στο παρακάτω διάγραμμα.



Σχήμα1–Διάγραμμα ροής της διαδικασίας αντιμετώπισης περιστατικών

Αυτά τα βήματα εξηγούνται λεπτομερέστερα στην υπόλοιπη διαδικασία.

3 Ανίχνευση και Ανάλυση Περιστατικών

Ένα περιστατικό μπορεί να εντοπιστεί αρχικά με μεγάλη ποικιλία τρόπων και μέσω διαφόρων πηγών, ανάλογα με τη φύση και τη θέση του περιστατικού. Ορισμένα περιστατικά μπορεί να ανιχνευθούν από τα εργαλεία λογισμικού που χρησιμοποιούνται στο «Δήμο Κιλκίς» ή από τους υπαλλήλους που παρατηρούν ασυνήθιστη δραστηριότητα. Άλλοι μπορεί να ειδοποιηθούν από τρίτους, όπως ο πελάτης, ο προμηθευτής ή η υπηρεσία επιβολής του νόμου, που έχει λάβει γνώση παραβίασης, ίσως επειδή οι κλεμμένες πληροφορίες χρησιμοποιήθηκαν με κάποιο τρόπο για κακόβουλους σκοπούς.

Δεν είναι ασυνήθιστο να υπάρξει καθυστέρηση μεταξύ της προέλευσης του περιστατικού και της πραγματικής ανίχνευσής του. Ένας από τους στόχους μιας προληπτικής προσέγγισης για την ασφάλεια των πληροφοριών είναι η μείωση αυτής της χρονικής περιόδου. Ο σημαντικότερος παράγοντας είναι ότι η διαδικασία αντιμετώπισης περιστατικών πρέπει να ξεκινήσει το συντομότερο δυνατόν μετά την ανίχνευση, ώστε να μπορεί να δοθεί αποτελεσματική αντιμετώπιση.

Μόλις εντοπιστεί το περιστατικό, πρέπει να διενεργηθεί αρχική εκτίμηση του αντικτύπου, προκειμένου να αποφασιστεί η κατάλληλη αντιμετώπιση.

Αυτή η εκτίμηση αντικτύπου πρέπει να εκτιμά:

- Την έκταση των επιπτώσεων στην υποδομή πληροφορικής, συμπεριλαμβανομένων υπολογιστών, δικτύων, εξοπλισμού και καταλύματος
- Τα περιουσιακά στοιχεία των πληροφοριών (συμπεριλαμβανομένων των προσωπικών δεδομένων) που ενδέχεται να κινδυνεύουν ή να διακυβεύονται
- Την πιθανή διάρκεια του περιστατικού, δηλαδή όταν μπορεί να έχει αρχίσει
- Τις υπηρεσιακές μονάδες που επηρεάζονται και η έκταση των επιπτώσεων σε αυτές
- Για τις παραβιάσεις που αφορούν τα προσωπικά δεδομένα, το βαθμό κινδύνου για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων
- Την αρχική ένδειξη της πιθανής αιτίας του περιστατικού

Αυτές οι πληροφορίες θα πρέπει να τεκμηριώνονται έτσι ώστε να είναι διαθέσιμη για τρέχουσα χρήση και μετέπειτα αναθεώρηση μια σαφής κατανόηση της κατάστασης ως προς το χρόνο, όπως εμφανίζεται.

Πρέπει να δημιουργηθεί ένας κατάλογος των πληροφοριακών περιουσιακών στοιχείων (συμπεριλαμβανομένων των δεδομένων προσωπικού χαρακτήρα), των υπηρεσιακών δραστηριοτήτων, των προϊόντων, των υπηρεσιών, των ομάδων και των διαδικασιών υποστήριξης που ενδέχεται να έχουν επηρεαστεί από το περιστατικό, μαζί με μια εκτίμηση της έκτασης των επιπτώσεων.

Ως αποτέλεσμα αυτής της αρχικής ανάλυσης, οποιοδήποτε μέλος της ομάδας διαχείρισης έχει την εξουσία να επικοινωνεί με τον Αρχηγό της ομάδας αντιμετώπισης περιστατικών ανά πάσα στιγμή, για να του ζητήσει να αξιολογήσει εάν πρέπει να ενεργοποιηθεί η διαδικασία αντιμετώπισης περιστατικών.

4 Ενεργοποίηση της Διαδικασίας Αντιμετώπισης Περιστατικών

Ο Υπεύθυνος της Ομάδας, μόλις ειδοποιηθεί για ένα περιστατικό, πρέπει να αποφασίσει εάν η κλίμακα και οι πραγματικές ή πιθανές επιπτώσεις του περιστατικού δικαιολογούν την ενεργοποίηση της Ομάδας Αντιμετώπισης Περιστατικών.

Εάν κάποια από τις ακόλουθες περιστάσεις ισχύουν για ένα συγκεκριμένο περιστατικό, το οποίο αποτελεί ευθύνη του Υπεύθυνου της Ομάδας,

- Υπάρχει σημαντική πραγματική ή δυνητική απώλεια διαβαθμισμένων πληροφοριών, συμπεριλαμβανομένων των προσωπικών δεδομένων
- Υπάρχει σημαντική πραγματική ή ενδεχόμενη διακοπή των υπηρεσιακών δραστηριοτήτων
- Υπάρχει σημαντικός κίνδυνος για τη φήμη των υπηρεσιών
- Οποιαδήποτε άλλη κατάσταση που μπορεί να έχει σημαντικές επιπτώσεις στον οργανισμό

Σε περίπτωση διαφωνίας ή αβεβαιότητας σχετικά με το εάν θα ενεργοποιηθεί ή όχι μια διαδικασία αντιμετώπισης περιστατικών, η απόφαση του Υπεύθυνου της Ομάδας θα είναι η οριστική.

Εάν αποφασιστεί να μην ενεργοποιηθεί η διαδικασία, τότε θα πρέπει να δημιουργηθεί ένα σχέδιο που να επιτρέπει μια ανταπόκριση χαμηλότερου επιπέδου στο περιστατικό μέσα στους κανονικούς διαύλους της διαχείρισης. Αυτό μπορεί να συνεπάγεται την επίκληση σχετικών διαδικασιών σε τοπικό επίπεδο.

Εάν το περιστατικό εγγυάται την ενεργοποίηση της διαδικασίας αντιμετώπισης περιστατικών, ο Υπεύθυνος της Ομάδας θα αρχίσει να συγκεντρώνει την εν λόγω ομάδα.

5 Συγκέντρωση της Ομάδας Αντιμετώπισης Περιστατικών (ΟΑΠ)

Μόλις ληφθεί η απόφαση για την ενεργοποίηση της διαδικασίας αντιμετώπισης περιστατικών, ο Υπεύθυνος της ομάδας (ή ο αναπληρωτής) θα εξασφαλίσει ότι όλοι οι κάτοχοι ρόλων (ή οι αναπληρωτές τους εάν οι κύριοι κάτοχοι δεν είναι σε επαφή) έρχονται σε επαφή, ενημερώνονται για τη φύση του συμβάντος και συγκεντρώνονται σε μια κατάλληλη τοποθεσία.

Η εξαίρεση είναι ο Σύνδεσμος Περιστατικών, ο οποίος θα κληθεί να παρακολουθήσει τη θέση/τοποθεσία του συμβάντος (αν είναι διαφορετικός) προκειμένου να αρχίσει να συγκεντρώνει πληροφορίες για την εκτίμηση περιστατικών που θα διεξαγάγει η ομάδα, ώστε να μπορεί να προσδιοριστεί η κατάλληλη αντιμετώπιση.

5.1 Μέλη της Ομάδας Αντιμετώπισης Περιστατικών

Η Ομάδα Αντιμετώπισης Περιστατικών θα αποτελείται γενικά από τους παρακάτω ανθρώπους στους καθορισμένους ρόλους και τους αναφερόμενους αναπληρωτές, αν και η **ακριβής σύνθεση της ομάδας θα ποικίλει ανάλογα με τη φύση του συμβάντος**.

Ρόλος / Υπηρεσιακός Τομέας	Κύριος Κάτοχος του Ρόλου	Αναπληρωτής
Υπεύθυνος- Συντονιστής της Ομάδας		
Σύνδεσμος Περιστατικών		
Πληροφορικός		
Υπηρεσιακές Λειτουργίες		
Ανθρώπινο Δυναμικό		
Δημόσιες Σχέσεις		
Νομικός Σύμβουλος		

Πίνακας1 – Μέλη της ομάδας αντιμετώπισης περιστατικών

Τα στοιχεία επικοινωνίας για τα παραπάνω αναφέρονται στο Παράρτημα Α του παρόντος εγγράφου.

5.2 Ρόλοι και Ευθύνες

Οι ευθύνες των ρόλων εντός της ομάδας αντιμετώπισης περιστατικών είναι οι εξής:

Υπεύθυνος -Συντονιστής Ομάδας

- Αποφασίζει εάν θα ξεκινήσει ή όχι μια διαδικασία αντιμετώπισης
- Συγκεντρώνει την ομάδα αντιμετώπισης περιστατικών
- Διαχειρίζεται συνολικά την ομάδα αντιμετώπισης περιστατικών
- Πράττει ως διεπαφή με το διοικητικό συμβούλιο και άλλους ενδιαφερόμενους υψηλού επιπέδου
- Τελικός λήπτης αποφάσεων σε περιπτώσεις διαφωνίας
- Υποστηρίζει την ομάδα αντιμετώπισης περιστατικών
- Συντονίζει πόρους μέσα στο κέντρο διοίκησης
- Προετοιμάζεται για συναντήσεις και καταγράφει ενέργειες και αποφάσεις
- Ενημερώνει τα μέλη της ομάδας για την τελευταία κατάσταση κατά την επιστροφή τους στο κέντρο διοίκησης
- Διευκολύνει την επικοινωνία μέσω ηλεκτρονικού ταχυδρομείου, φαξ, τηλεφώνου ή άλλων μεθόδων
- Παρακολουθεί εξωτερικές πηγές πληροφοριών όπως ειδήσεις

Σύνδεσμος Περιστατικών

- Παρακολουθεί τον τόπο του περιστατικού το συντομότερο δυνατόν
- Αξιολογεί την έκταση και τον αντίκτυπο του περιστατικού
- Παρέχει μέσω της άμεσης εμπειρίας του για την κατάσταση, ενημέρωση στην ομάδα αντιμετώπισης περιστατικών
- Συνδέεται με την ομάδα σε συνεχή βάση για την παροχή ενημερώσεων και την απάντηση σε οποιεσδήποτε ερωτήσεις που απαιτούνται για τη λήψη αποφάσεων από την ομάδα

Πληροφορικός

- Παρέχει πληροφορίες σχετικά με ζητήματα που σχετίζονται με την τεχνολογία
- Βοηθά στην εκτίμηση αντικτύπου

Υπηρεσιακές Λειτουργίες

- Συμβάλλει στη λήψη αποφάσεων που βασίζονται στη γνώση των υπηρεσιών
- Ενημερώνει άλλα μέλη της ομάδας για υπηρεσιακά ζητήματα
- Βοηθά στην αξιολόγηση πιθανών επιπτώσεων στους πολίτες του Δήμου
- Ασχολείται με θέματα φυσικής ασφάλειας και πρόσβασης
- Παρέχει παρουσία ασφαλείας, εάν απαιτείται

Ανθρώπινο Δυναμικό

- Εκτιμά τον κίνδυνο για τη ζωή και την σωματική ακεραιότητα του συμβάντος
- Εξασφαλίζει ότι οι νομικές ευθύνες για την υγεία και την ασφάλεια πληρούνται ανά πάσα στιγμή
- Συνδέεται με υπηρεσίες έκτακτης ανάγκης όπως η αστυνομία, η πυρκαγιά και η ιατρική
- Θεωρεί περιβαλλοντικά ζητήματα σχετικά με το περιστατικό

- Αξιολογεί και συμβουλεύει το Ανθρώπινο Δυναμικό για θέματα πολιτικών για και συμβάσεων εργασίας
- Αντιπροσωπεύει τα συμφέροντα των εργαζομένων του οργανισμού
- Συμβουλεύει για θέματα ικανότητας και πειθαρχίας

Δημόσιες Σχέσεις

- Υπεύθυνος για τη διασφάλιση ότι οι εσωτερικές επικοινωνίες είναι αποτελεσματικές
- Αποφασίζει το επίπεδο, τη συχνότητα και το περιεχόμενο των επικοινωνιών με εξωτερικά μέρη, όπως τα μέσα ενημέρωσης
- Καθορίζει την προσέγγιση για την ενημέρωση των επηρεαζόμενων μερών πχ. πελάτες, μετόχους

Νομικός Σύμβουλος

- Συμβουλεύει τι πρέπει να γίνει για να διασφαλιστεί η συμμόρφωση με τους σχετικούς νόμους και κανονιστικά πλαίσια, τον GDPR
- Αξιολογεί τις πραγματικές και πιθανές νομικές επιπτώσεις του περιστατικού και των επακόλουθων ενεργειών

5.3 Διαχείριση, Παρακολούθηση και Ανακοίνωση Περιστατικού

Μόλις προσδιοριστεί η κατάλληλη αντίδραση στο περιστατικό, η Ομάδα Αντιμετώπισης Περιστατικών πρέπει να είναι σε θέση να διαχειριστεί τη συνολική ανταπόκριση, να παρακολουθήσει την κατάσταση του περιστατικού και να διασφαλίσει την αποτελεσματική ανακοίνωση σε όλα τα επίπεδα.

Θα πρέπει να διεξάγονται τακτικές συνεδριάσεις της ΟΑΠ με την κατάλληλη συχνότητα που αποφασίζεται από τον αρχηγό της ομάδας. Πρότυπο ημερήσιας διάταξης για αυτές τις συνεδριάσεις περιλαμβάνεται στο Παράρτημα Γ. Σκοπός αυτών των συνεδριάσεων είναι να διασφαλιστεί ότι οι πόροι διαχείρισης περιστατικών διαχειρίζονται αποτελεσματικά και ότι οι βασικές αποφάσεις λαμβάνονται έγκαιρα, με βάση επαρκείς πληροφορίες. Κάθε συνάντηση θα καταγράφεται από τον Συντονιστή της Ομάδας.

Ο Σύνδεσμος Περιστατικών θα παρέχει ενημερώσεις στην ΟΑΠ σε συχνότητα που αποφασίζεται από τον Αρχηγό Ομάδας. Αυτές οι ενημερώσεις θα πρέπει να συνδυάζονται με τις συνεδριάσεις της ΟΑΠ, έτσι ώστε να είναι διαθέσιμες οι πιο πρόσφατες πληροφορίες για κάθε συνεδρίαση.

5.4 Διαδικασίες Ανακοίνωσης/Επικοινωνίας

Είναι ζωτικής σημασίας να διατηρούνται αποτελεσματικές επικοινωνίες μεταξύ όλων των εμπλεκόμενων στην αντιμετώπιση περιστατικών.

Ο κύριος τρόπος επικοινωνίας κατά τη διάρκεια ενός περιστατικού θα είναι αρχικά πρόσωπο με πρόσωπο και τηλέφωνο, σταθερό και κινητό. Το ηλεκτρονικό ταχυδρομείο δεν πρέπει να χρησιμοποιείται, εκτός εάν έχει δοθεί άδεια από την ΟΑΠ.

Οι ακόλουθες οδηγίες πρέπει να τηρούνται σε όλες τις επικοινωνίες:

- Να είστε ήρεμοι και να αποφύγετε μακρά συνομιλία
- Να συμβουλεύσετε τα μέλη της εσωτερικής ομάδας για την ανάγκη υποβολής αιτήσεων πληροφοριών στην ΟΑΠ
- Εάν η κλήση απαντηθεί από κάποιον άλλο εκτός της επαφής:
    - Ρωτήστε εάν η επαφή είναι διαθέσιμη αλλού
    - Εάν δεν μπορούν να επικοινωνήσουν, αφήστε ένα μήνυμα για να επικοινωνήσουν μαζί σας σε ένα συγκεκριμένο αριθμό
    - Μην παρέχετε λεπτομέρειες σχετικά με το Περιστατικό
- Πάντα να τεκμηριώνετε τις λεπτομέρειες του χρόνου κλήσης, τις απαντήσεις και τις ενέργειες

Όλες οι ανακοινώσεις θα πρέπει να καταγράφονται σαφώς και με ακρίβεια, καθώς ενδέχεται να χρειαστούν αρχεία στο πλαίσιο μιας νομικής δράσης σε μεταγενέστερη ημερομηνία.

5.4.1 Γνωστοποίηση στην Εποπτική Αρχή Προστασίας των Δεδομένων

Ο GDPR απαιτεί τα περιστατικά που αφορούν τα δεδομένα προσωπικού χαρακτήρα και ενδέχεται να θέσουν σε κίνδυνο τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων πρέπει να αναφέρονται χωρίς καθυστέρηση στην εποπτική αρχή προστασίας δεδομένων εντός 72 ωρών από τη στιγμή που το γνωρίζουν. Η *GDPR-DOC-18Διαδικασία Γνωστοποίησης Παραβίασης Προσωπικών Δεδομένων* πρέπει να χρησιμοποιείται για το σκοπό αυτό. Σε περίπτωση που δεν επιτευχθεί ο στόχος των 72 ωρών, πρέπει να δοθούν λόγοι για την καθυστέρηση.

Τα στοιχεία επικοινωνίας με την εποπτική αρχή προστασίας δεδομένων παρατίθενται στο Παράρτημα Β.

5.4.2 Ανακοίνωση στα Υποκείμενα των Δεδομένων

Σε περίπτωση που ένα περιστατικό αφορά δεδομένα προσωπικού χαρακτήρα, η ΟΑΠ πρέπει να λάβει απόφαση σχετικά με την έκταση, το χρονοδιάγραμμα και το περιεχόμενο της ανακοίνωσης στα υποκείμενα των δεδομένων. OGDPR απαιτεί η ανακοίνωση να πραγματοποιείται «χωρίς αδικαιολόγητη καθυστέρηση» εάν η παραβίαση ενδέχεται να οδηγήσει σε «υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων».
Η *GDPR-DOC-18Διαδικασία Γνωστοποίησης Παραβίασης Προσωπικών Δεδομένων* πρέπει να χρησιμοποιείται για το σκοπό αυτό.

5.4.3 Άλλη Εξωτερική Επικοινωνία

Ανάλογα με το περιστατικό μπορεί να υπάρξει μια ποικιλία εξωτερικών μερών με τα οποία θα επικοινωνούν κατά τη διάρκεια της ανταπόκρισης. Είναι σημαντικό οι πληροφορίες που διατίθενται σε τρίτους να διαχειρίζονται έτσι ώστε να είναι έγκαιρες και ακριβείς.

Οι κλήσεις που δεν προέρχονται από οργανισμούς που εμπλέκονται άμεσα στην αντιμετώπιση περιστατικών (όπως τα μέσα ενημέρωσης) θα πρέπει να διαβιβάζονται στο μέλος της ΟΑΠ που είναι αρμόδιο για τις επικοινωνίες.

Μπορεί να υπάρχουν ορισμένοι εξωτερικοί φορείς οι οποίοι, αν και δεν εμπλέκονται άμεσα με το περιστατικό, ενδέχεται να επηρεαστούν από αυτό και πρέπει να ειδοποιηθούν για το γεγονός αυτό. Αυτοί μπορεί να περιλαμβάνουν:

- Πολίτες
- Εποπτική αρχή

Το μέλος της ΟΑΠ των Επικοινωνιών πρέπει να καταρτίσει έναν κατάλογο με τα ενδιαφερόμενα μέρη και να καθορίσει το μήνυμα που πρέπει να τους δοθεί. Κατάλογο ορισμένων εξωτερικών υπηρεσιών παρέχεται στο Παράρτημα Β.

Τα ενδιαφερόμενα μέρη που δεν έχουν ειδοποιηθεί από την ΟΑΠ μπορούν να καλέσουν για να λάβουν πληροφορίες σχετικά με το περιστατικό και τα αποτελέσματά του. Αυτές οι κλήσεις πρέπει να καταγράφονται σε ένα αρχείο καταγραφής μηνυμάτων και να διαβιβάζονται στο μέλος επικοινωνίας της ΟΑΠ.
.

5.4.4 Επικοινωνία με τα ΜΜΕ

Σε γενικές γραμμές, η επικοινωνιακή στρατηγική σε σχέση με τα μέσα ενημέρωσης θα είναι η έκδοση ενημερώσεων, μέσω της ανώτατης διοίκησης. Κανένας υπάλληλος δεν θα πρέπει να δίνει συνέντευξη στα μέσα μαζικής ενημέρωσης, εκτός εάν αυτό έχει προηγουμένως εγκριθεί από την ΟΑΠ.

Η προτιμώμενη διεπαφή με τα μέσα μαζικής ενημέρωσης είναι η έκδοση προειδοποιητικών δελτίων τύπου. Σε εξαιρετικές περιπτώσεις, θα διεξαχθεί συνέντευξη τύπου για να απαντηθούν ερωτήσεις σχετικά με το περιστατικό και τα αποτελέσματά του. Είναι ευθύνη του μέλους Επικοινωνιών της ΟΑΠ να οργανώσει τον τόπο διεξαγωγής των εκδηλώσεων και να επικοινωνήσει με τον Τύπο που πιθανόν επιθυμεί να παρευρεθεί.

Κατά τη σύνταξη μιας δήλωσης για τα μέσα ενημέρωσης θα πρέπει να τηρηθούν οι ακόλουθες οδηγίες:

- Οι προσωπικές πληροφορίες πρέπει να προστατεύονται ανά πάσα στιγμή
- Εμείνετε στα γεγονότα και μην κάνετε εικασίες σχετικά με το περιστατικό ή την αιτία του

- Εξασφαλίστε τη λήψη νομικών συμβουλών προτού εκδοθούν οποιεσδήποτε δηλώσεις
- Προσπαθήστε να προκαταλάβετε τις ερωτήσεις που μπορεί εύλογα να ζητηθούν
- Υπογραμμίστε ότι έχει ενεργοποιηθεί μια προετοιμασμένη αντιμετώπιση και ότι γίνονται τα πάντα

Τα ακόλουθα μέλη του προσωπικού θα διοριστούν εκπρόσωποι του Δήμου εάν πρόκειται να εκδοθούν περαιτέρω πληροφορίες, πχ. σε συνέντευξη Τύπου:

Όνομα	Ρόλος	Έκταση Περιστατικού
ΠρόσωποΑ	Τμήμα Δημοσίων Σχέσεων	Χαμηλή - Μέτρια
ΠρόσωποΒ	Προϊστάμενος	Υψηλή

Πίνακας1–Εκπρόσωποι στα ΜΜΕ

Ο καταλληλότερος εκπρόσωπος θα εξαρτηθεί από την έκταση του συμβάντος και την επίδρασή του στους πελάτες, τον προμηθευτή, το κοινό και άλλους ενδιαφερόμενους.

6 Περιορισμός, Εξάλειψη, Ανάκαμψη και Γνωστοποίηση Περιστατικών

6.1 Περιορισμός

Το πρώτο βήμα θα είναι να προσπαθήσετε να σταματήσετε το περιστατικό από το να χειροτερέψει, δηλαδή να το διατηρήσετε. Σε περίπτωση ενός ιού, αυτό μπορεί να συνεπάγεται την αποσύνδεση των επηρεαζόμενων τμημάτων του δικτύου.Για μια επίθεση hacking μπορεί να περιλαμβάνει την απενεργοποίηση ορισμένων προφίλ ή θύρες στο τείχος προστασίας ή ίσως ακόμη και την αποσύνδεση του εσωτερικού δικτύου από το Internet εντελώς. Οι συγκεκριμένες ενέργειες που πρέπει να εκτελεστούν θα εξαρτηθούν από τις περιστάσεις του συμβάντος.

Σημείωση: εάν κριθεί πιθανό ότι θα χρειαστεί να συγκεντρωθούν ψηφιακά αποδεικτικά στοιχεία που θα χρησιμοποιηθούν στη συνέχεια στο δικαστήριο, πρέπει να ληφθούν προφυλάξεις για να εξασφαλιστεί ότι τα εν λόγω αποδεικτικά στοιχεία παραμένουν αποδεκτά. Αυτό σημαίνει ότι τα σχετικά δεδομένα δεν πρέπει να αλλάζονται ούτε σκόπιμα ούτε κατά λάθος, πχ. με την εκκίνηση ενός φορητού υπολογιστή. Συνιστάται η παροχή ειδικών συμβουλών σε αυτό το σημείο - βλ. Επαφές στο Παράρτημα Β.

Ιδιαίτερα (αλλά όχι αποκλειστικά) εάν υπάρχει υποψία για **ύποπτες ενέργειες** στο περιστατικό, πρέπει να τηρούνται ακριβή αρχεία των ενεργειών που έχουν αναληφθεί και των αποδεικτικών στοιχείων που συλλέγονται σύμφωνα με τις κατευθυντήριες οδηγίες **ψηφιακής εγκληματολογίας**. Οι βασικές αρχές αυτών των κατευθυντήριων γραμμών είναι οι εξής:

Αρχή 1 - Μην αλλάζετε κανένα στοιχείο. Εάν γίνει κάτι που έχει ως αποτέλεσμα την αλλοίωση των δεδομένων του σχετικού συστήματος με οποιονδήποτε τρόπο, τότε αυτό θα επηρεάσει κάθε μεταγενέστερη δικαστική υπόθεση.

Αρχή 2 - Προσπελάστε τα αρχικά δεδομένα μόνο σε εξαιρετικές περιπτώσεις. Ένας εξειδικευμένος ειδικός θα χρησιμοποιήσει εργαλεία για να πάρει ένα κομμάτι των δεδομένων που διατηρούνται στη μνήμη, είτε πρόκειται για σκληρό δίσκο, μνήμη flash είτε για κάρτα SIM σε τηλέφωνο. Όλες οι αναλύσεις θα περιληφθούν, στη συνέχεια, στο αντίγραφο και το πρωτότυπο δεν θα πρέπει ποτέ να αγγιχτεί παρά μόνο σε εξαιρετικές περιπτώσεις πχ. ο χρόνος είναι ουσιαστικής σημασίας και η απόκτηση πληροφοριών για την πρόληψη ενός περαιτέρω εγκλήματος είναι πιο σημαντική από τη διατήρηση των αποδεικτικών στοιχείων αποδεκτά.

Αρχή 3 - Διατηρήστε πάντα μια διαδρομή ελέγχου για όσα έχουν γίνει. Τα εγκληματολογικά εργαλεία θα το κάνουν αυτόματα, αλλά αυτό ισχύει και για τους πρώτους ανθρώπους που αντιμετωπίζουν το περιστατικό. Η λήψη φωτογραφιών και βίντεο ενθαρρύνεται όσο δεν τίποτα δεν έχει αγγιχτεί.

Αρχή 4 - Ο υπεύθυνος πρέπει να διασφαλίσει ότι ακολουθούνται οι οδηγίες.

Πριν από την άφιξη ενός ειδικού, πρέπει να συγκεντρωθούν βασικές πληροφορίες.

Αυτές μπορεί να περιλαμβάνουν:

- Φωτογραφίες ή βίντεο σχετικών μηνυμάτων ή πληροφοριών
- Χειρόγραφα αρχεία της χρονολογίας του συμβάντος
- Πρωτότυπα έγγραφα, συμπεριλαμβανομένων αρχείων για το ποιος τα βρήκε, πού και πότε
- Λεπτομέρειες για κάθε μάρτυρα

Μόλις συγκεντρωθούν, τα αποδεικτικά στοιχεία θα φυλάσσονται σε ασφαλές μέρος όπου δεν μπορεί να παραβιαστεί και να καθιερωθεί επίσημη αλυσίδα επιμέλειας.

Τα αποδεικτικά στοιχεία μπορεί να απαιτηθούν:

- Για μεταγενέστερη ανάλυση της αιτίας του περιστατικού
- Ως εγκληματολογικά αποδεικτικά στοιχεία για ποινικές ή αστικές διαδικασίες
- Για την υποστήριξη τυχόν διαπραγματεύσεων αποζημίωσης με προμηθευτές λογισμικού ή υπηρεσιών

Στη συνέχεια, πρέπει να καθοριστεί μια σαφής εικόνα του τι συνέβη. Η έκταση του περιστατικού και ο αντίκτυπος των επιπτώσεων θα πρέπει να εξακριβωθεί πριν να ληφθούν οποιαδήποτε μέτρα περιορισμού.

Τα αρχεία καταγραφής ελέγχου μπορούν να εξεταστούν για να ταξινομηθεί η ακολουθία των γεγονότων. Θα πρέπει να ληφθεί μέριμνα ώστε να χρησιμοποιούνται μόνο ασφαλή αντίγραφα αρχείων που δεν έχουν αλλοιωθεί.

6.2 Εξάλειψη

Οι ενέργειες για την αποκατάσταση των ζημιών που προκλήθηκαν από το περιστατικό, όπως η διαγραφή κακόβουλου λογισμικού, πρέπει να τεθούν μέσω της διαδικασίας διαχείρισης αλλαγών (ως επείγουσα αλλαγή εάν είναι απαραίτητο). Αυτές οι ενέργειες θα πρέπει να στοχεύουν στον καθορισμό της τρέχουσας αιτίας και στην αποτροπή επανάληψης του περιστατικού. Πρέπει να εντοπιστούν τυχόν ευπάθειες που έχουν αξιοποιηθεί ως μέρος του συμβάντος.

Ανάλογα με τον τύπο του συμβάντος, η εξάλειψη μπορεί μερικές φορές να είναι περιττή.

6.3 Ανάκαμψη

Κατά τη διάρκεια της φάσης ανάκαμψης, τα συστήματα θα πρέπει να αποκατασταθούν στην κατάσταση προ της εμφάνισης του περιστατικού, αν και θα πρέπει να πραγματοποιηθούν οι απαραίτητες ενέργειες για την αντιμετώπιση τυχόν τρωτών σημείων που χρησιμοποιήθηκαν ως μέρος του περιστατικού. Αυτό μπορεί να περιλαμβάνει δραστηριότητες όπως η εγκατάσταση επιδιορθώσεων, η αλλαγή των κωδικών πρόσβασης, η ενίσχυση των server και οι διαδικασίες τροποποίησης.

6.4 Γνωστοποίηση

Η γνωστοποίηση ενός περιστατικού ασφάλειας πληροφοριών και η απώλεια δεδομένων που προκύπτει είναι ένα ευαίσθητο θέμα το οποίο πρέπει να αντιμετωπιστεί προσεκτικά και με πλήρη έγκριση της διοίκησης ακολουθώντας τις οδηγίες στο έγγραφο ***GDPR-DOC-18 Διαδικασία Γνωστοποίησης Παραβίασης Προσωπικών Δεδομένων***. Η ΟΑΠ θα αποφασίσει, βάσει νομικών συμβουλών και άλλων συμβουλών από εμπειρογνώμονες και με όσο το δυνατόν πληρέστερη κατανόηση των επιπτώσεων του συμβάντος, ποια ειδοποίηση απαιτείται και τη μορφή που θα πάρει.

Ο «Δήμος Κιλκίς» θα συμμορφώνεται πάντοτε πλήρως με τις ισχύουσες νομικές και κανονιστικές απαιτήσεις του GDPR σχετικά με την κοινοποίηση περιστατικών και θα αξιολογεί προσεκτικά τις προσφορές που πρέπει να γίνουν στα μέρη που ενδέχεται να επηρεαστούν από το συμβάν, όπως είναι οι υπηρεσίες παρακολούθησης πιστώσεων.

Τα αρχεία που συλλέγονται στο πλαίσιο της ανταπόκρισης στο περιστατικό ενδέχεται να απαιτηθούν στο πλαίσιο οποιασδήποτε διεξαγόμενης έρευνας από τα αρμόδια ρυθμιστικά όργανα και ο «Δήμος Κιλκίς» θα συνεργαστεί πλήρως με αυτές τις διαδικασίες.

7 Δραστηριότητα Μετά το Περιστατικό

Ο Υπεύθυνος της Ομάδας θα αποφασίσει, με βάση τις τελευταίες πληροφορίες από τον Σύνδεσμο Περιστατικών και άλλα μέλη της ομάδας, το σημείο στο οποίο πρέπει να σταματήσουν οι δραστηριότητες ανταπόκρισης και να σταματήσει η ΟΑΠ. Σημειώστε ότι η ανάκτηση και η εκτέλεση των σχεδίων μπορεί να συνεχιστεί πέρα από αυτό το σημείο αλλά υπό λιγότερο τυπικό έλεγχο διαχείρισης.

Η απόφαση αυτή θα εξαρτηθεί από την κρίση του Υπεύθυνου της Ομάδας αλλά θα πρέπει να βασίζεται στα ακόλουθα κριτήρια:

- Η κατάσταση έχει επιλυθεί πλήρως ή είναι αρκετά σταθερή
- Ο ρυθμός αλλαγής της κατάστασης έχει επιβραδυνθεί σε ένα σημείο όπου απαιτούνται λίγες αποφάσεις
- Η κατάλληλη αντίδραση είναι σε εξέλιξη και τα σχέδια αποκατάστασης προχωρούν στο να προγραμματιστούν
- Ο βαθμός κινδύνου για την υπηρεσία έχει μειωθεί σε ένα αποδεκτό σημείο
- Έχουν εκπληρωθεί οι άμεσες νομικές και ρυθμιστικές αρμοδιότητες

Εάν η ανάκαμψη από το περιστατικό συνεχίζεται, ο Υπεύθυνος της Ομάδας πρέπει να ορίσει τις επόμενες ενέργειες που πρέπει να αναληφθούν. Αυτά μπορεί να περιλαμβάνουν:

- Λιγότερο συχνές συνεδριάσεις της ΟΑΠ, πχ. εβδομαδιαία ανάλογα με τις περιστάσεις
- Ενημέρωση όλων των εμπλεκομένων μερών ότι η ΟΑΠ αποσύρεται
- Εξασφάλιση της ασφάλειας όλων των εγγράφων του συμβάντος
- Ζητώντας από το όλο το προσωπικό που δεν εμπλέκεται σε περαιτέρω εργασία να επιστρέψει στα κανονικά καθήκοντα

Πρέπει να καταγράφονται όλες οι ενέργειες που πραγματοποιούνται στο πλαίσιο της απόσυρσης.

Μετά την απόσυρση της ΟΑΠ, ο Υπεύθυνος της Ομάδας θα διεξάγει μια ενημέρωση όλων των μελών ιδανικά εντός 24 ωρών. Τα σχετικά αρχεία του περιστατικού θα εξεταστούν από την ΟΑΠ για να διασφαλιστεί ότι αντικατοπτρίζουν πραγματικά γεγονότα και αντιπροσωπεύουν πλήρη και ακριβή καταγραφή του συμβάντος.

Οποιαδήποτε άμεσα σχόλια από την ομάδα θα καταγραφούν.

Μια πιο επίσημη αναθεώρηση μετά το περιστατικό θα διεξάγεται κάθε φορά που θα αποφασιστεί από την ανώτατη διοίκηση ανάλογα με το μέγεθος και τη φύση του συμβάντος.

8 ΠΑΡΑΡΤΗΜΑΑ – Φύλλο Επαφής Αρχικής Ανταπόκρισης

Ο παρακάτω πίνακας θα πρέπει να χρησιμοποιείται για την καταγραφή επιτυχημένης και ανεπιτυχούς αρχικής επαφής με μέλη της ΟΑΠ:

Όνομα	Ρόλος στο Σχέδιο	Αριθμός Γραφείου	Αριθμός Σπιτιού	Αριθμός Κινητού	Ημ/νία-Ώρα	Αποτέλεσμα (Έγινε Επικοινωνία / Καμία Απάντηση / Αφέθηκε Μήνυμα / Απρόσιτο)	Χρόνος (σε περίπτωση επικοινωνίας)
Πρόσωπο Α	Υπεύθυνος-Συντονιστής της Ομάδας	Χxx xxxxxx	Χxx xxxxxx	Χxx xxxxxx			
Πρόσωπο Β	Σύνδεσμος Περιστατικών	Χxx xxxxxx	Χxx xxxxxx	Χxx xxxxxx			
Πρόσωπο Γ	Πληροφορικός	Χxx xxxxxx	Χxx xxxxxx	Χxx xxxxxx			
Πρόσωπο Δ	Υπηρεσιακές Λειτουργίες	Χxx xxxxxx	Χxx xxxxxx	Χxx xxxxxx			
Πρόσωπο Ε	Ανθρώπινο Δυναμικό	Χxx xxxxxx	Χxx xxxxxx	Χxx xxxxxx			
Πρόσωπο ΣΤ	Δημόσιες Σχέσεις	Χxx xxxxxx	Χxx xxxxxx	Χxx xxxxxx			
Πρόσωπο Ζ	Νομικός Σύμβουλος	Χxx xxxxxx	Χxx xxxxxx	Χxx xxxxxx			

ΠΑΡΑΡΤΗΜΑΒ – Χρήσιμες Εξωτερικές Επαφής

Ο παρακάτω πίνακας εμφανίζει τα στοιχεία επικοινωνίας τρίτων που μπορεί να είναι χρήσιμα ανάλογα με τη φύση του περιστατικού:

Οργανισμός	Επαφή	Αριθμός Τηλεφώνου	Email
Εποπτική Αρχή Προστασίας Δεδομένων			
Προμηθευτής Λογισμικού Ασφαλείας			
Προμηθευτής Λογισμικού Οργάνωσης Δήμου			
Προμηθευτής Υπηρεσιών Τεχνικής υποστήριξης ΤΠΕ (ICT)			
Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος		11188, fax: 213-1527471	ccu@cybercrimeunit.gov.gr
Πάροχος Υπηρεσιών Διαδικτύου			
Μέσα Μαζικής ενημέρωσης			
Ένωση που ανήκει ο Δήμος			
Φορείς που αναφέρεται ο Δήμος			

9 ΠΑΡΑΡΤΗΜΑΓ–Πρότυπη Ημερήσια Διάταξη της Συνεδρίασης της ΟΑΠ

Συνιστάται η ακόλουθη βασική ατζέντα να χρησιμοποιείται για συνεδριάσεις της ομάδας αντιμετώπισης περιστατικών.

Ατζέντα

Συμμετέχοντες: Όλα τα μέλη της ομάδας αντιμετώπισης περιστατικών

Τοποθεσία: Κέντρο διοίκησης

Συχνότητα: Κάθε 4 ώρες

Πρόεδρος: Υπεύθυνος Ομάδας

1. Ενέργειες προηγούμενης συνεδρίασης
2. Ενημέρωση της κατάστασης του περιστατικού
3. Απαιτούμενες αποφάσεις
4. Κατανομή καθηκόντων
5. Εσωτερικές επικοινωνίες
6. Εξωτερικές επικοινωνίες
7. Απόσυρση
8. Όποιες άλλες εργασίες