Δήμος Περάματος 07/01/2025
Α. Π.: 133

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΔΗΜΟΣ ΠΕΡΑΜΑΤΟΣ
ΤΜΗΜΑ ΟΡΓΑΝΩΣΗΣ ,
ΠΡΟΓΡΑΜΜΑΤΙΣΜΟΥ
ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗΣ
Λ. Δημοκρατίας 28 – Πέραμα
Τηλ – 2132037212
It-program@perama.gr

ΠΡΟΣ:

1) Όλες Υπηρεσίες/Διευθύνσεις

ΕΝΙΑΙΑ ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ ΣΥΣΤΗΜΑΤΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ

Κωδικός Διαδικασίας	1.0	**Έκδοση**	1.0	**Σχετικά Πρότυπα**	*Ν. 4961/2022, ISO/IEC 27001:2013, Γενικός Κανονισμός, Προστασίας Δεδομένων, ENISA (Consumerization of IT), Οδηγίες της ΑΠΔΠΧ*
Σχετικές Απαιτήσεις	*Συμμόρφωση του Δήμου Περάματος με τον Ν. 4961/2022*				

Περιεχόμενα

Κωδικός Διαδικασίας	1.0	**Έκδοση**	1.0	**Σχετικά Πρότυπα**	*Ν. 4961/2022, ISO/IEC 27001:2013, Γενικός Κανονισμός, Προστασίας Δεδομένων, ENISA (Consumerization of IT), Οδηγίες της ΑΠΔΠΧ*
Σχετικές Απαιτήσεις	*Συμμόρφωση του Δήμου Περάματος με τον Ν. 4961/2022*				

1. Εισαγωγή

Ο νέος νόμος Ν. 4961/2022, δημοσιεύθηκε στις 27 Ιουλίου 2022 στο ΦΕΚ 146/Α/27-07-2022 και αφορά στις αναδυόμενες τεχνολογίες πληροφορικής και επικοινωνιών, την ενίσχυση της ψηφιακής διακυβέρνησης. Με τον νέο νόμο θεσπίζονται οριζόντιες και τομεακές υποχρεώσεις για φορείς του δημοσίου που παράγουν, διανέμουν, εκμεταλλεύονται και κάνουν χρήση προηγμένων τεχνολογιών. Ο Νόμος αναπτύσσεται σε τέσσερα μέρη, τα οποία αφορούν την ψηφιακή αναβάθμιση της δημόσιας διοίκησης και έχει ως σκοπό τη δημιουργία του κατάλληλου θεσμικού υποβάθρου για τη θεμιτή και ασφαλή αξιοποίηση νέων τεχνολογιών από φορείς του δημοσίου καθώς και την ενίσχυση της ανθεκτικότητας της δημόσιας διοίκησης απέναντι σε απειλές στον κυβερνοχώρο.

Στο πλαίσιο εξυπηρέτησης του σκοπού αυτού, ο Νόμος 4961/2022, εισάγει διατάξεις και ιδρύει ρόλους για την θεσμική ενίσχυση της ασφάλειας πληροφοριών και της προστασίας προσωπικών δεδομένων.

Η παρούσα Ενιαία Πολιτική Ασφαλείας Συστημάτων Πληροφορικής και Επικοινωνιών συντάσσεται κατ' απαίτηση του άρθρου 20 § 2 του Ν. 4961/2022, σύμφωνα με το οποίο κάθε φορέας κεντρικής κυβέρνησης καταρτίζει και τηρεί ενιαία πολιτική ασφαλείας συστημάτων πληροφορικής και επικοινωνιών. Ως εκ τούτου, ο Δήμος Περάματος (εφεξής «Φορέας» ή «Οργανισμός»), οφείλει να εναρμονίζεται με τις νέες νομοθετικές διατάξεις και να επιδιώκει την ενίσχυση της ασφάλειας πληροφοριών.

Με την παρούσα Πολιτική Ασφάλειας Πληροφοριών η Διοίκηση του Οργανισμού εκφράζει ρητά τη βούλησή της για τη διασφάλιση των πληροφοριών και των πληροφοριακών πόρων που υποστηρίζουν τις δραστηριότητές της και παρέχει τις βασικές κατευθύνσεις για τη διαχείριση της ασφάλειας των πληροφοριών.

Η διασφάλιση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών και συστημάτων της, σύμφωνα με την κρισιμότητά τους, είναι ουσιαστικής σημασίας για την επίτευξη των επιχειρησιακών στόχων και λειτουργειών του Οργανισμού, καθώς και της συμμόρφωσής του με το ισχύον νομοθετικό και ρυθμιστικό πλαίσιο. Επιπροσθέτως, η προστασία των δεδομένων και ιδιαίτερα των Δεδομένων Προσωπικού Χαρακτήρα (εφεξής: ΔΠΧ) σε έναν Οργανισμό αναδεικνύεται σε μια σημαντική, οργανωμένη και επιμελή καθημερινή δραστηριότητα. Τα ΔΠΧ αποτελούν ένα ουσιώδες κεφάλαιο για κάθε Οργανισμό και θα πρέπει να συλλέγονται, επεξεργάζονται, διακινούνται, φυλάσσονται, προστατεύονται με την εφαρμογή των κατάλληλων πρακτικών, διαδικασιών, πολιτικών και εργαλείων.

Κωδικός Διαδικασίας	1.0	**Έκδοση**	1.0	**Σχετικά Πρότυπα**	*Ν. 4961/2022, ISO/IEC 27001:2013, Γενικός Κανονισμός, Προστασίας Δεδομένων, ENISA (Consumerization of IT), Οδηγίες της ΑΠΔΠΧ*
Σχετικές Απαιτήσεις	*Συμμόρφωση του Δήμου Περάματος με τον Ν. 4961/2022*				

Με την παρούσα Πολιτική η Διοίκηση του Οργανισμού εκφράζει ρητά τη βούλησή για τη συμμόρφωσής της με το ισχύον νομοθετικό και ρυθμιστικό πλαίσιο και τη διασφάλιση των πληροφοριών και των πληροφοριακών πόρων που υποστηρίζουν τις δραστηριότητές του.

Στόχος της Πολιτικής είναι η ενίσχυση της ανθεκτικότητάς του Οργανισμού απέναντι σε απειλές στον κυβερνοχώρο και η προσαρμογή με τις κανονιστικές απαιτήσεις του Νόμου 4691/2022, συγκεκριμένα του άρθρου 20 § 2 με το οποίο θεσπίζεται η υποχρέωση τήρησης της παρούσας Ενιαίας Πολιτικής Ασφάλειας Συστημάτων Πληροφορικής και Επικοινωνιών.

Ο Οργανισμός επιδιώκει την παροχή των Υπηρεσιών σύμφωνα με το ισχύον Νομικό και Κανονιστικό πλαίσιο και τις λοιπές συμβατικές υποχρεώσεις του με τρόπο που να προστατεύονται τα πληροφοριακά δεδομένα από εκούσια ή ακούσια κλοπή, καταστροφή, ή χρήση κατά παράβαση των Νόμων και των Κανονιστικών Διατάξεων. Η ενίσχυση της ασφάλειας πληροφοριών είναι ουσιαστικής σημασίας για την επίτευξη των επιχειρησιακών στόχων και λειτουργειών του Οργανισμού, καθώς και της συμμόρφωσής του με το ισχύον νομοθετικό και ρυθμιστικό πλαίσιο.

Ο σκοπός της ασφάλειας της πληροφορίας είναι να διασφαλίσει την επιχειρησιακή συνέχεια του Οργανισμού και να ελαχιστοποιήσει τους κινδύνους που επαπειλούν τα δεδομένα, αποφεύγοντας περιστατικά ασφαλείας και μειώνοντας τις επιπτώσεις που μπορεί να έχουν τα περιστατικά αυτά. Παράλληλα με την Πολιτική αυτή διασφαλίζονται και τα Δικαιώματα των Υποκειμένων των δεδομένων, όπως ορίζονται από την ισχύουσα νομοθεσία.

Σκοπός της παρούσας Πολιτικής είναι επιπλέον, να προστατέψει τα πληροφοριακά δεδομένα και τις πληροφοριακές υποδομές του Οργανισμού από όλες τις εσωτερικές, εξωτερικές, εκούσιες ή ακούσιες απειλές. Περαιτέρω, στόχος της Πολιτικής είναι να διαχειριστεί ο Οργανισμός αποτελεσματικά, οποιαδήποτε περιστατικά σχετίζονται με την παραβίαση ιδιωτικότητας ή ασφάλειας, να περιορίσει την πιθανή ζημιά, να συνδράμει στην ταχύτερη και αποτελεσματικότερη αντιμετώπιση του περιστατικού (και των πιθανών δυσχερών αποτελεσμάτων του), να ικανοποιήσει τις νομικές υποχρεώσεις, και να περιορίσει (ή δυνατόν αποτρέψει) διοικητικές ή/και ποινικές κυρώσεις, που απορρέουν από την ισχύουσα νομοθεσία.

Ειδικότερα και, προς συμμόρφωση του Οργανισμού με τις απαιτήσεις του άρθρου 20 του Ν. 4961/2022, η παρούσα πολιτική περιλαμβάνει:

α) τους στόχους ασφάλειας του φορέα και την προσέγγιση διαχείρισής τους,

β) τον τρόπο διαχείρισης των απαιτήσεων που δημιουργούνται από:

βα) την επιχειρησιακή στρατηγική του φορέα,

ββ) τις νομοθετικές, κανονιστικές και συμβατικές υποχρεώσεις του,
βγ) το διεθνές περιβάλλον κυβερνοαπειλών,

γ) την ανάθεση γενικών και ειδικών ρόλων και αντίστοιχων ευθυνών για τη διαχείριση της ασφάλειας πληροφοριακών συστημάτων,

δ) διαδικασίες για τον χειρισμό αποκλίσεων και εξαιρέσεων,

καθώς και την παραπομπή σε επιμέρους θεματικές ενότητες (παραπομπές σε ειδικότερες Πολιτικές) οι οποίες μνημονεύονται στη συνέχεια του παρόντος.

Η Πολιτική μπορεί να επικαιροποιείται όταν υπάρχουν αλλαγές στις διεργασίες της Διεύθυνσης ή αλλαγές στα συστήματά της.

Η Πολιτική αυτή αφορά σε και πρέπει να προσαρμοστούν σε αυτή όλες οι οργανικές μονάδες του Οργανισμού. Η Ενιαία Πολιτική εφαρμόζεται από όλες τις Διευθύνσεις / Τμήματα / Γραφεία του Οργανισμού.

Η παρούσα Πολιτική Ασφαλείας αφορά όλους τους πληροφοριακούς πόρους του Οργανισμού, οι οποίοι υποστηρίζουν τη διεξαγωγή των επιχειρηματικών δραστηριοτήτων του. Κατά συνέπεια, καλύπτει το σύνολο των πληροφοριών/δεδομένων που διακινούνται, αποθηκεύονται και γενικά επεξεργάζονται στον Οργανισμό, είτε αυτές βρίσκονται σε ηλεκτρονική είτε σε έντυπη μορφή.

Η Πολιτική Ασφάλειας απευθύνεται σε όλο το προσωπικό και στους συνεργάτες οι οποίοι αποκτούν πρόσβαση στα συστήματα, στις πληροφορίες, στις υπηρεσίες και στις εγκαταστάσεις του Οργανισμού. Όλο το προσωπικό και οι εξωτερικοί συνεργάτες (όταν αυτό απαιτείται) είναι υποχρεωμένοι να εφαρμόζουν την Ενιαία Πολιτική και τα επιμέρους Παραρτήματά της, που διέπουν τη λειτουργία του Οργανισμού και εμπίπτουν στο πεδίο των δραστηριοτήτων τους.

Προϋπόθεση για την τροποποίηση και εφαρμογή της είναι, κατ' αρχήν ο έλεγχος των αλλαγών από τον Υπεύθυνο Προστασίας Δεδομένων του Φορέα και κατόπιν η έγκρισή της από τη Διοίκηση του.

Η πολιτική αποτελείται από δύο (2) διακριτά στοιχεία τα οποία είναι:

Α) Η Ενιαία Πολιτική Ασφαλείας Συστημάτων Πληροφορικής και Επικοινωνιών

Β) Τα παραρτήματα με τις ειδικές πολιτικές ασφαλείας ήτοι

1. Πολιτική Ασφάλειας Δικτύων
2. Πολιτική Ορθής Χρήσης
3. Πολιτική Διαχείρισης Ταυτότητας και Ελέγχου Πρόσβασης
4. Πολιτική Αντιγράφων Ασφαλείας
5. Πολιτική Διαχείρισης Περιστατικών και Επιχειρησιακής Συνέχειας
6. Πολιτική Φυσικής Ασφάλειας

2. Στόχοι Ασφάλειας του Οργανισμού

Οι στόχοι της Ενιαίας Πολιτικής Ασφαλείας Συστημάτων Πληροφορικής και Επικοινωνιών επικεντρώνονται στη διασφάλιση της ασφάλειας και της προστασίας των πληροφοριακών συστημάτων και των τηλεπικοινωνιακών υποδομών του Οργανισμού. Οι κύριοι στόχοι που περιλαμβάνουν:

Προστασία των Δεδομένων των Πολιτών: Ο Οργανισμός πρέπει να διασφαλίσει ότι τα προσωπικά δεδομένα των πολιτών που χρησιμοποιούν τις υπηρεσίες του (πολιτών, εργαζομένων, συναλλασσόμενων κλπ.) είναι ασφαλή και προστατευμένα από παράνομη πρόσβαση ή διαρροή.

Προστασία των Υπηρεσιών και των Δικτύων: Διασφάλιση της ασφάλειας των πληροφοριακών συστημάτων, των εφαρμογών και των δικτύων που χρησιμοποιούνται για την παροχή δημόσιων υπηρεσιών.

Πρόληψη Κυβερνοεπιθέσεων: Ανάπτυξη μέτρων πρόληψης και αντιμετώπισης κυβερνοεπιθέσεων που μπορεί να απειλήσουν την ασφάλεια του Οργανισμού.

Συμμόρφωση με τους Νόμους και τους Κανονισμούς: Εφαρμογή και τήρηση των νόμων και των κανονισμών που αφορούν την κυβερνοασφάλεια και την προστασία των δεδομένων.

Εκπαίδευση και Ευαισθητοποίηση: Εκπαίδευση του προσωπικού του Οργανισμού και ευαισθητοποίηση των χρηστών σχετικά με τις ασφαλείς πρακτικές και τους κινδύνους της κυβερνοασφάλειας.

Εφαρμογή Καλών Πρακτικών: Εφαρμογή βέλτιστων πρακτικών στον τομέα της κυβερνοασφάλειας για την προστασία των συστημάτων και των δεδομένων.

Ετοιμότητα για Κρίσεις: Προετοιμασία για τη διαχείριση κρίσεων κυβερνοασφάλειας και την αποκατάσταση των υπηρεσιών μετά από επεισόδια.

Η προσέγγιση των στόχων κυβερνοασφάλειας του Οργανισμού απαιτεί συνολικό σχεδιασμό και εφαρμογή εκτεταμένων πρακτικών ασφάλειας που να καλύπτουν την πληροφοριακή υποδομή, τις διαδικασίες, το προσωπικό και τους χρήστες. Τα βήματα προσέγγισης των ως άνω στόχων μπορούν να διαμορφωθούν ως εξής:

- Καθορισμός σαφών στόχων κυβερνοασφάλειας, οι οποίοι είναι συμβατοί με την αποστολή και τα καθήκοντα του Οργανισμού.
- Ανάλυση των κινδύνων, για την αναγνώριση πιθανών απειλών και ευκαιριών για την ασφάλεια της πληροφοριακής υποδομής και των δεδομένων.
- Δημιουργία και εφαρμογή πολιτικών και διαδικασιών ασφάλειας που να καλύπτουν θέματα όπως η πρόσβαση, η αποθήκευση και η ανάκτηση δεδομένων.
- Εφαρμογή μέτρων ασφαλείας όπως πχ. προηγμένα λογισμικά ασφαλείας και κρυπτογράφηση δεδομένων.
- Παρακολούθηση και αντιμετώπιση περιστατικών με σκοπό την άμεση ανίχνευση και αντιμετώπιση ενδεχόμενων κυβερνοεπιθέσεων.
- Ανάπτυξη σχεδίων ετοιμότητας και αποκατάστασης για τη διαχείριση κρίσεων και την επαναφορά των υπηρεσιών μετά από επιθέσεις.
- Τακτική επισκόπηση και αξιολόγηση των πολιτικών και των μέτρων ασφαλείας και προσαρμογή τους ανάλογα με τις εκάστοτε απαιτήσεις.

Η κυβερνοασφάλεια δεν είναι στατική, και η προστασία του Οργανισμού από τις κυβερνοαπειλές απαιτεί συνεχή προσπάθεια και προσαρμογή.

3. Διαχείριση απαιτήσεων ασφάλειας

3.1. Επιχειρησιακή στρατηγική

Η επιχειρησιακή στρατηγική του Οργανισμού, αποτελείται από ένα σύνολο προτεραιοτήτων και δράσεων που καθορίζουν τον τρόπο με τον οποίο ο Οργανισμός θα επιδιώξει τους στόχους του και θα ανταποκριθεί στις διάφορες προκλήσεις που ενδέχεται να αντιμετωπίσει. Οι στόχοι και ο ρόλος του Οργανισμού είναι κρίσιμοι αφενός για την αποτελεσματική λειτουργία του και αφετέρου για την παροχή αποτελεσματικών υπηρεσιών που ανταποκρίνονται στις ανάγκες της τοπικής κοινωνίας.

Ειδικότερα, η επιχειρησιακή στρατηγική του Οργανισμού, επικεντρώνεται στους εξής τομείς:

1) **Βελτίωση των υποδομών:** Μέσω της ανάπτυξης και συντήρησης του οδικού δικτύου, των πάρκων, των αθλητικών εγκαταστάσεων και των λοιπών κοινόχρηστων χώρων, της αναβάθμισης των δικτύων ύδρευσης και αποχέτευσης, της ενεργειακής αναβάθμισης δημοτικών κτιρίων

2) **Προαγωγή της Κοινωνικής Ευημερίας:** Μέσω της παροχής ποιοτικών κοινωνικών υπηρεσιών, της στήριξης των ευπαθών κοινωνικών ομάδων και της προώθησης της κοινωνικής συνοχής και αλληλεγγύης.
3) **Οικονομική Ανάπτυξη:** Μέσω της ενίσχυσης της τοπικής οικονομίας και της απασχόλησης, της υποστήριξης των τοπικών επιχειρήσεων και της προώθησης της επιχειρηματικότητας και της προσέλκυσης επενδύσεων.
4) **Προστασία τους περιβάλλοντος:** Μέσω της εφαρμογής προγραμμάτων ανακύκλωσης και μείωσης αποβλήτων, της προστασίας και ανάδειξης φυσικών πόρων και πράσινων χώρων και της αντιμετώπισης της κλιματικής αλλαγής και προώθησης της βιώσιμης ανάπτυξης.
5) **Πολιτιστική και εκπαιδευτική ανάπτυξη:** Μέσω της προώθησης του πολιτισμού και της παράδοσης μέσω εκδηλώσεων, μουσείων και πολιτιστικών κέντρων, της στήριξης της εκπαίδευσης και της διά βίου μάθησης και της ενίσχυσης αθλητικών και πολιτιστικών δραστηριοτήτων.
6) **Βελτίωση της ποιότητας ζωής των δημοτών:** Μέσω της ανάπτυξης και συντήρησης πάρκων, παιδότοπων, χώρων αναψυχής, της προώθησης της δημόσιας ασφάλειας και της προστασίας των πολιτών και της διασφάλισης της καθαριότητας και της υγιεινής της πόλης.
7) **Καλή διακυβέρνηση και διαφάνεια:** Μέσω της ενίσχυσης της διαφάνειας και της λογοδοσίας στη διοίκηση του Δήμου, της βελτίωσης των υπηρεσιών προς τους πολίτες μέσω της ηλεκτρονικής διακυβέρνησης και της ενίσχυσης της συμμετοχής των πολιτών στη λήψη αποφάσεων.
8) **Προετοιμασία και αντιμετώπιση έκτακτων αναγκών:** Μέσω της ανάπτυξης σχεδίων έκτακτης ανάγκης για φυσικές καταστροφές, υγειονομικές κρίσεις κλπ. και της ενημέρωσης και εκπαίδευσης των πολιτών για την αντιμετώπιση κρίσεων.

Ωστόσο, η επιχειρησιακή στρατηγική του Οργανισμού, πρέπει να αναθεωρείται τακτικά και να προσαρμόζεται στις εκάστοτε συνθήκες.

3.2. Νομικό και Κανονιστικό πλαίσιο της πολιτικής Ασφάλειας του Οργανισμού

Το Νομικό και Κανονιστικό πλαίσιο προσδιορίζεται από:

- Νόμος 4961/2022 (ΦΕΚ 146/Α/27-7-2022) «Αναδυόμενες τεχνολογίες πληροφορικής και επικοινωνιών, ενίσχυση της ψηφιακής διακυβέρνησης και άλλες διατάξεις», όπως τροποποιήθηκε και ισχύει, δυνάμει του Ν. 5039/2023.
- Οδηγία (ΕΕ) 2022/2555 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 14ης Δεκεμβρίου 2022 σχετικά με μέτρα για υψηλό κοινό επίπεδο κυβερνοασφάλειας σε

ολόκληρη την Ένωση, την τροποποίηση του κανονισμού (ΕΕ) αριθ. 910/2014 και της οδηγίας (ΕΕ) 2018/1972, και για την κατάργηση της οδηγία (ΕΕ) 2016/1148 (οδηγία NIS 2).

- Νόμος 4577/2018, Ενσωμάτωση στην ελληνική νομοθεσία της Οδηγίας 2016/1148/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση και άλλες διατάξεις.
- Νόμος 5002/2022, Διαδικασία άρσης του απορρήτου των επικοινωνιών, κυβερνοασφάλεια και προστασία προσωπικών δεδομένων πολιτών
- Νόμος 4624/2019 (Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 και άλλες διατάξεις"
- Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών.
- Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Ιουλίου 2002, σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών (οδηγία για την προστασία ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες)
- Οδηγία (ΕΕ) 2015/1535 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 9ης Σεπτεμβρίου 2015, για την καθιέρωση μιας διαδικασίας πληροφόρησης στον τομέα των τεχνικών προδιαγραφών και των κανόνων σχετικά με τις υπηρεσίες της κοινωνίας των πληροφοριών.
- Απόφαση ΑΔΑΕ 165/2011 Κανονισμός για τη Διασφάλιση του Απορρήτου των Ηλεκτρονικών Επικοινωνιών
- Ν.2121 ΦΕΚ 25 Α / 04-03-1993 Νόμος περί προστασίας και αποφυγής κλοπής πνευματικής ιδιοκτησίας
- Ν.3741/2006 Νόμος για την προστασία δεδομένων προσωπικού χαρακτήρα και ιδιωτικής ζωής στον τομέα των ηλεκτρονικών

3.2 Διεθνές περιβάλλον κυβερνοαπειλών

Το διεθνές περιβάλλον κυβερνοαπειλών αναφέρεται στο σύνολο των κυβερνοαπειλών και κινδύνων που προέρχονται από διεθνείς πηγές και απειλούν την κυβερνοασφάλεια των χωρών, των οργανισμών και των ατόμων. Αυτό το περιβάλλον είναι δυναμικό και εξελίσσεται διαρκώς, καθώς οι κυβερνοαπειλές προσαρμόζονται στις νέες τεχνολογίες και στις γεωπολιτικές εξελίξεις.

Από απειλές που προέρχονται από μεμονωμένους εγκληματίες , μέχρι επιθέσεις φερόμενες ως απόρροια ενεργειών τρίτων κρατών, το περιβάλλον κυβερνοαπειλών είναι διαρκώς μεταβαλλόμενο, οδηγώντας σε μια εγγενή αδυναμία άμεσης προστασίας του. Οι εν λόγω συνθήκες επιβεβαιώνουν την ανάγκη για μια περιοδικά αναθεωρούμενη στρατηγική, η οποία θα θέτει τους κανόνες αντιμετώπισης ή μετριασμού του αντίκτυπου των εν λόγω απειλών.

Σε ευρωπαϊκό επίπεδο, η Ευρωπαϊκή Ένωση αναγνωρίζει ότι κρίσιμοι τομείς, όπως οι μεταφορές, η ενέργεια, η υγεία και ο χρηματοοικονομικός κλάδος, εξαρτώνται όλο και περισσότερο από τις ψηφιακές τεχνολογίες για την άσκηση των βασικών δραστηριοτήτων τους. Οι κυβερνοεπιθέσεις και τα κυβερνοεγκλήματα πολλαπλασιάζονται σε όλη την Ευρώπη, ενώ οι μέθοδοι που χρησιμοποιούνται στις ενέργειες αυτές εξελίσσονται συνεχώς. Κατέστη, επομένως, σαφής, η ανάγκη για ανάπτυξη ισχυρότερης δράσης στο πεδίο της κυβερνοασφάλειας με στόχο να οικοδομηθεί ένας ανοικτός και ασφαλής κυβερνοχώρος.

Η πράξη της ΕΕ για την κυβερνοασφάλεια τέθηκε σε ισχύ τον Ιούνιο του 2019 και θέσπισε ένα σύστημα πιστοποίησης σε επίπεδο ΕΕ και μια νέα και ισχυρότερη εντολή για τον Οργανισμό της ΕΕ για την Κυβερνοασφάλεια.

Τον Δεκέμβριο του 2020, η Ευρωπαϊκή Επιτροπή και η Ευρωπαϊκή Υπηρεσία Εξωτερικής Δράσης (ΕΥΕΔ) παρουσίασαν μια νέα στρατηγική της ΕΕ για την κυβερνοασφάλεια. Στόχος της στρατηγικής αυτής είναι να ενισχυθεί η ανθεκτικότητα της Ευρώπης απέναντι στις κυβερνοαπειλές και να μπορέσουν να ωφεληθούν πλήρως όλοι οι πολίτες και οι επιχειρήσεις από έγκυρες και αξιόπιστες υπηρεσίες και ψηφιακά εργαλεία. Η στρατηγική περιλαμβάνει συγκεκριμένες προτάσεις για τη χρήση κανονιστικών και επενδυτικών μέσων καθώς και μέσων άσκησης πολιτικής.

Η οδηγία για την ασφάλεια των συστημάτων δικτύου και πληροφοριών (NIS) θεσπίστηκε το 2016 και αποτελεί το πρώτο νομοθετικό μέτρο ενωσιακής εμβέλειας με στόχο την ενίσχυση της συνεργασίας μεταξύ των κρατών μελών όσον αφορά το κρίσιμο ζήτημα της κυβερνοασφάλειας. Θεσπίζει υποχρεώσεις ασφάλειας για τους φορείς εκμετάλλευσης βασικών υπηρεσιών (σε ζωτικούς τομείς όπως η ενέργεια, οι μεταφορές, η υγεία και ο χρηματοοικονομικός κλάδος) και για τους παρόχους ψηφιακών υπηρεσιών (διαδικτυακές αγορές, μηχανές αναζήτησης και υπηρεσίες υπολογιστικού νέφους).

Κωδικός Διαδικασίας	1.0	**Έκδοση**	1.0	**Σχετικά Πρότυπα**	*Ν. 4961/2022, ISO/IEC 27001:2013, Γενικός Κανονισμός, Προστασίας Δεδομένων, ENISA (Consumerization of IT), Οδηγίες της ΑΠΔΠΧ*
Σχετικές Απαιτήσεις	*Συμμόρφωση του Δήμου Περάματος με τον Ν. 4961/2022*				

Η ΕΕ εξέδωσε το 2022 αναθεωρημένη οδηγία για τα NIS (NIS2) προς αντικατάσταση της οδηγίας του 2016. Οι νέοι κανόνες διασφαλίζουν υψηλό κοινό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση, ανταποκρινόμενοι στο εξελισσόμενο τοπίο των απειλών και λαμβάνοντας υπόψη τον ψηφιακό μετασχηματισμό, ο οποίος επιταχύνθηκε με την πανδημία COVID-19. Έτσι, με τη νέα νομοθεσία της ΕΕ θεσπίζονται νέοι ελάχιστοι κανόνες για ρυθμιστικό πλαίσιο, προβλέπονται μηχανισμοί για την αποτελεσματική συνεργασία μεταξύ των αρμόδιων αρχών σε κάθε χώρα της ΕΕ και επικαιροποιείται ο κατάλογος των τομέων και δραστηριοτήτων που υπόκεινται σε υποχρεώσεις κυβερνοασφάλειας. Η οδηγία NIS2 τέθηκε σε ισχύ στις 16 Ιανουαρίου 2023.

Σε εθνικό επίπεδο, έχει συσταθεί Γενική Διεύθυνση Κυβερνοασφάλειας με τις εξής αρμοδιότητες:

- Διατυπώνει την πολιτική ασφάλειας συστημάτων ΤΠΕ για το δημόσιο τομέα και προωθεί την εφαρμογή της
- Ορίζει απαιτήσεις και κανόνες ασφάλειας, που αποτελούν αναπόσπαστο μέρος κάθε έργου ΤΠΕ του δημοσίου και ενσωματώνονται σε αυτά από τη φάση της σχεδίασης, ως απαραίτητη προϋπόθεση των αρχών του ενιαίου σχεδιασμού
- Συνεργάζεται με τις αρμόδιες Ανεξάρτητες και Ρυθμιστικές Αρχές, τον Ευρωπαϊκό Οργανισμό για την Ασφάλεια Δικτύων και Πληροφοριών και ακαδημαϊκούς φορείς για την υιοθέτηση ενιαίων πολιτικών ασφαλείας στο πλαίσιο της δημόσιας διοίκησης
- Συνεργάζεται με την Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων και την Τεχνικής Φύσεως Αρχή Ασφάλειας Πληροφοριών της Εθνικής Υπηρεσίας Πληροφοριών, καθώς επίσης και με τα CERTs που δραστηριοποιούνται στην Ελλάδα για θέματα αρμοδιότητας του Τμήματος
- Προωθεί δράσεις εκπαίδευσης και ενημέρωσης του προσωπικού που διαχειρίζεται και υποστηρίζει κρίσιμα συστήματα και υποδομές του Δημοσίου

Παράλληλα, θεσπίστηκε η Εθνική Στρατηγική Κυβερνοασφάλειας 2020-2025 προκειμένου να αξιολογηθεί η υφιστάμενη κατάσταση κυβερνοαπειλών στη χώρα μας, να αναγνωρισθούν οι νέες προκλήσεις και να διαμορφωθεί ένα κατάλληλο στρατηγικό πλαίσιο άμεσης εφαρμογής.

Στην Ευρωπαϊκή Ένωση έχουν παρατηρηθεί επιθέσεις οι οποίες είχαν ποικίλους στόχους. Ήδη με βάση τα τελευταία στοιχεία του ENISA (ETL 2020, List of top 15 threats, enisa.europa.eu):

– οι επιθέσεις τύπου phishing έχουν ήδη ανέλθει στην 3η θέση, με τα web application attacks να κατεβαίνουν στην 4η

– οι επιθέσεις spam ανέβηκαν στην 5η θέση και οι επιθέσεις DDoS κατέβηκαν στην 6η θέση

– οι επιθέσεις identity theft ανέβηκαν από τη 13η στην 7η θέση

– η περίπτωση των botnets βρίσκεται πλέον στη 10η θέση

– η περίπτωση physical manipulation, damage, theft and loss κατέβηκε στην 11η θέση

– ομοίως η περίπτωση information leakage κατέβηκε στη 12η θέση

– στη 13η θέση ανήλθαν τα ransomware

– στη 14η θέση ανήλθαν οι περιπτώσεις cyberespionage

– στη 15η θέση βρίσκονται οι περιπτώσεις cryptojacking

Κωδικός Διαδικασίας	1.0	**Έκδοση**	1.0	**Σχετικά Πρότυπα**	*Ν. 4961/2022, ISO/IEC 27001:2013, Γενικός Κανονισμός, Προστασίας Δεδομένων, ENISA (Consumerization of IT), Οδηγίες της ΑΠΔΠΧ*
Σχετικές Απαιτήσεις	*Συμμόρφωση του Δήμου Περάματος με τον Ν. 4961/2022*				

Ορισμοί:

Ασφάλεια Δεδομένων: Παραδοσιακά, ο όρος ασφάλεια Πληροφορίας/δεδομένων (information/data security) χρησιμοποιείται για να περιγράψει τη μεθοδολογία, καθώς και τις μεθόδους και τεχνικές που ακολουθούνται προκειμένου να επιτευχθούν οι εξής στόχοι:

- Εμπιστευτικότητα (confidentiality): Οι πληροφορίες/δεδομένα δεν πρέπει να αποκαλύπτονται σε μη εξουσιοδοτημένα άτομα.
- Ακεραιότητα (integrity): Οι πληροφορίες/δεδομένα πρέπει να είναι ακριβή, ακέραια και γνήσια – όχι εσφαλμένα, αλλοιωμένα ή μη ενημερωμένα.
- Διαθεσιμότητα (availability): Οι πληροφορίες/δεδομένα πρέπει να είναι στη διάθεση των χρηστών όποτε απαιτείται η χρήση τους.

Στο χώρο της πληροφορικής και κατ' επέκταση του διαδικτύου/κυβερνοχώρου, οι όροι «συμβάν» και «περιστατικό» χρησιμοποιούνται για την περιγραφή περιστατικών τα οποία λαμβάνουν χώρα ή επηρεάζουν ένα δίκτυο υπολογιστών.

Συμβάν: Ένα συμβάν αποτελεί οποιαδήποτε ενέργεια σε συστήματα πληροφορικής η οποία είτε ηθελημένα (π.χ. στα πλαίσια δοκιμών, ενημερώσεων, ελέγχων) είτε όχι ,μπορεί να θέσει σε κίνδυνο την ορθή λειτουργία ή να έχει ως συνέπεια την μερική ή την πλήρη κατάρρευση των συστημάτων πληροφορικής, των δικτύων, των βάσεων δεδομένων και εν γένει την λειτουργία ενός Οργανισμού. Ο αριθμός των καθημερινών συμβάντων εξαρτάται από το μέγεθος, δηλαδή το οικονομικό μέγεθος και τον αριθμό των εργαζομένων και συνεργατών και την επιχειρηματική δραστηριότητα του Οργανισμού. Κάθε οργανισμός μπορεί να αντιμετωπίσει εκατοντάδες γεγονότα που προκαλούνται από διάφορους λόγους, όπως κυβερνοεπιθέσεις, ενέργειες εργαζομένων, κακόβουλο λογισμικό το οποίο είναι είτε συνημμένο σε μήνυμα ηλεκτρονικού ταχυδρομείου, είτε διεισδύει από μολυσμένη συσκευή, κακή χρήση του χρήστη κ.λπ.

Περιστατικό: Κάθε περιστατικό αποτελεί γεγονός ενώ κάθε γεγονός δεν χαρακτηρίζεται απαραίτητα ως περιστατικό. Ως εκ τούτου, περιστατικό νοείται οποιαδήποτε ενέργεια συνίσταται σε παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, άνευ άδειας κοινολόγηση ή πρόσβαση δεδομένων ανεξάρτητα αν είναι δεδομένα προσωπικού χαρακτήρα ή όχι που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία και κατά συνέπεια παραβιάζει το απόρρητο, την ακεραιότητα ή τη διαθεσιμότητα των δεδομένων προσβάλλοντας ή θέτοντας σε κίνδυνο την ιδιωτική ζωή των υποκειμένων και των περιουσιακών στοιχείων του Οργανισμού σύμφωνα και με τις πολιτικές ασφάλειας. Για παράδειγμα, η ύπαρξη και ο καθυστερημένος εντοπισμός στον καθορισμό οποιασδήποτε ευπάθειας στο δίκτυο υπολογιστών ή στο λογισμικό των συστημάτων του Οργανισμού είναι ένα

συμβάν. Όταν όμως εντοπιστεί και διαπιστωθεί (από την ομάδα διαχείρισης και αντιμετώπισης περιστατικών) ότι από αυτό το κενό ή την ευπάθεια έχει προκύψει παραβίαση των υπολογιστικών συστημάτων και άρα και της ασφάλειας των δεδομένων, τότε αυτό χαρακτηρίζεται ως περιστατικό.

Μερικές από τις πιο συνηθισμένες ενδείξεις περιστατικού ασφαλείας είναι οι εξής:

- Κακόβουλο λογισμικό (malicious software)
- Επιθέσεις από το διαδίκτυο (web based attacks)
- Phishing
- Επιθέσεις σε διαδικτυακές εφαρμογές
- Ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου
- Επιθέσεις άρνησης υπηρεσίας (Denial of service-DoS attacks)
- Κλοπή ταυτότητας χρήστη (identity theft)
- Παραβιάσεις προσωπικών δεδομένων
- Εσωτερικές απειλές (insider threat)
- Botnets
- Φυσικές απειλές
- Διαρροή δεδομένων
- Λογισμικό λύτρων (ransomware)
- Ηλεκτρονική κατασκοπεία
- Cryptojacking

3.3 Διαχείριση απαιτήσεων του Οργανισμού

Βάσει του ανωτέρω νομοθετικού πλαισίου, των κινδύνων που προκύπτουν από το διεθνές περιβάλλον κυβερνοαπειλών και της επιχειρησιακής στρατηγικής του Οργανισμού, δημιουργούνται συγκεκριμένες απαιτήσεις ασφαλείας.

Η διαχείριση των απαιτήσεων απαιτεί συγκεκριμένο σχεδιασμό και την υλοποίηση συγκεκριμένων βημάτων, με σκοπό την ορθή λειτουργία του Οργανισμού και την κάλυψη των αναγκών του. Συνεπώς, αρχικά απαιτείται η συλλογή και η λεπτομερής καταγραφή των απαιτήσεων και στη συνέχεια η κατάταξή τους σε κατηγορίες ανάλογα με βάση την προτεραιότητά τους, καθορίζοντας μέσω ενός συστήματος προτεραιότητας, ποιες απαιτήσεις είναι πιο επείγουσες ή πιο σημαντικές. Στη συνέχεια, πρέπει να διενεργηθεί αξιολόγηση εφικτότητας υλοποίησης κάθε απαίτησης, κατόπιν ελέγχου των διαθέσιμων πόρων. Υψίστης σημασίας βήμα, αποτελεί η χάραξη συγκεκριμένης στρατηγικής η οποία μπορεί να εφαρμοστεί μέσω της ενημέρωσης και της συνεργασίας των εμπλεκόμενων προσώπων. Τέλος, κρίνεται απαραίτητη η συνεχής αξιολόγηση

και παρακολούθηση της προόδου της στρατηγικής, προκειμένου να διασφαλίζεται ότι επιτυγχάνονται οι στόχοι που έχουν τεθεί.

Όπως αναφέρθηκε ανωτέρω, οι κύριες δραστηριότητες του Οργανισμού, αφορούν διάφορους άξονες για την βέλτιστη παροχή υπηρεσιών υγείας προς τους πολίτες. Κατά την υλοποίηση της επιχειρησιακής του στρατηγικής, διαχειρίζεται μεγάλο όγκο πληροφοριών και δεδομένων προσωπικού χαρακτήρα, που αφορούν εργαζόμενους του Οργανισμού, ασθενείς αλλά και πολίτες (πχ. διαχείριση δεδομένων προσωπικού χαρακτήρα εργαζομένων για τη χορήγηση αναρρωτικών αδειών σε εργαζομένους του Φορέα). Κατά τη διενέργεια των εκάστοτε διαδικασιών, ο Οργανισμός προβαίνει σε επεξεργασία τόσο απλών δεδομένων όσο και δεδομένων ειδικών κατηγοριών (άρθρο 9 ΓΚΠΔ), ενώ για την επεξεργασία αυτή χρησιμοποιούνται και ηλεκτρονικά μέσα (ηλεκτρονικοί υπολογιστές, πληροφοριακά συστήματα, βάσεις δεδομένων κλπ.).

Επομένως, προκειμένου ο Οργανισμός να συμμορφώνεται πλήρως με το ανωτέρω νομοθετικό και κανονιστικό πλαίσιο και να τηρούνται όλες οι προϋποθέσεις ασφάλειας, προβαίνει στις εξής ενέργειες:

- Στην περιγραφή των κανόνων και των διαδικασιών που πρέπει να ακολουθούνται για την προστασία των πληροφοριακών συστημάτων,
- Στην ικανοποίηση των κανονιστικών και νομοθετικών απαιτήσεων όπως απορρέουν από τις οικείες διατάξεις (Νόμος 4961/2022, Νόμος 4624/2019, Κανονισμός (ΕΕ) 2016/679 κ.ά.),
- Στον καθορισμό των συγκεκριμένων ρόλων και αρμοδιοτήτων που απαιτούνται για την υλοποίηση της ενιαίας πολιτικής ασφαλείας,
- Στη διασφάλιση της ομαλής λειτουργίας των πληροφοριακών πόρων,
- Στην άμεση αντιμετώπιση περιστατικών Ασφάλειας Πληροφοριών και την ταχεία ανταπόκριση σε κάθε συμβάν που αναφέρεται ή εντοπίζεται και ενδέχεται να υποδεικνύει παραβίαση της εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας,
- Στη συνεχή βελτίωση του επιπέδου Ασφάλειας Πληροφοριών,
- Στην περιοδική αξιολόγηση των κινδύνων που σχετίζονται με την ασφάλεια πληροφοριών και την κυβερνοασφάλεια,
- Στον χρονοπρογραμματισμό των απαραίτητων ενεργειών και δέσμευσης των κατάλληλων πόρων που απαιτούνται για τη διασφάλιση των πληροφοριακών συστημάτων,

Κωδικός Διαδικασίας	1.0	**Έκδοση**	1.0	**Σχετικά Πρότυπα**	*Ν. 4961/2022, ISO/IEC 27001:2013, Γενικός Κανονισμός, Προστασίας Δεδομένων, ENISA (Consumerization of IT), Οδηγίες της ΑΠΔΠΧ*
Σχετικές Απαιτήσεις	*Συμμόρφωση του Δήμου Περάματος με τον Ν. 4961/2022*				

- Στην αύξηση του βαθμού επίγνωσης του προσωπικού σε κινδύνους που απειλούν την Ασφάλεια Πληροφοριών και η συνεχής ενημέρωση για τις βέλτιστες πρακτικές που πρέπει να ακολουθούνται για την ελαχιστοποίηση της πιθανότητας εμφάνισής τους,
- Στην απόκτηση κοινής αντίληψης και γνώσης για την ανάγκη προστασίας και τους στόχους ασφάλειας του Οργανισμού, προκειμένου να δημιουργηθούν κοινές πρακτικές και πεποιθήσεις που αφορούν στην ανάγκη και τους τρόπους προστασίας των πληροφοριακών συστημάτων,
- Στην αναγνώριση των διαφορετικών εμπλεκομένων, των συμφερόντων και των δικαιωμάτων τους,
- Στη διασφάλιση των δικαιωμάτων των φυσικών προσώπων που λαμβάνουν υπηρεσίες από τον Οργανισμό καθώς και των εργαζομένων και συνεργατών της.

Για την επίτευξη των παραπάνω στόχων έχουν ήδη αναπτυχθεί και εφαρμόζονται επιμέρους Τεχνικά Μέτρα, Πολιτικές Ασφαλείας και Διαδικασίες, όπου περιγράφονται και όλες οι σχετικές αρμοδιότητες του προσωπικού και οι οποίες διασφαλίζουν και αποδεικνύουν ότι η διαχείριση των πληροφοριακών δεδομένων διενεργείται σύμφωνα με το Νόμο κανονιστικό Πλαίσιο.

Τα εν λόγω Μέτρα, Πολιτικές και Διαδικασίες επανεξετάζονται και επικαιροποιούνται όταν κρίνεται απαραίτητο, όπως για παράδειγμα μετά από εκτεταμένες αλλαγές στα πληροφοριακά συστήματα, βασικές αλλαγές στα προγράμματα (software), κλπ., και κατ' ελάχιστο ανά έτος. Υπεύθυνος για την επικαιροποίηση είναι ο Υπεύθυνος Ασφάλειας Συστημάτων Πληροφορικής και Επικοινωνιών του Οργανισμού, σε συνεργασία με τους Προϊσταμένους των Διευθύνσεων και ειδικότερα το Τμήμα Πληροφορικής.

Όλο το προσωπικό και οι εξωτερικοί συνεργάτες (όταν αυτό απαιτείται) είναι υποχρεωμένοι να εφαρμόζουν τις Πολιτικές Ασφαλείας που διέπουν τη λειτουργία του Οργανισμού και εμπίπτουν στο πεδίο των δραστηριοτήτων τους.

Η Διοίκηση δεσμεύεται για την παροχή όλων των απαραίτητων πόρων και μέσων για την εφαρμογή της παρούσας και των επιμέρους Πολιτικών Ασφαλείας.

4. Γενικοί και ειδικοί ρόλοι για τη διαχείριση της ασφάλειας πληροφοριακών συστημάτων

Υπεύθυνος Ασφάλειας Συστημάτων Πληροφορικής και Επικοινωνιών

Ο Οργανισμός υποχρεούται να ορίσει Υπεύθυνο Ασφάλειας Συστημάτων Πληροφορικής και Επικοινωνιών (ΥΑΣΠΕ), βάσει του άρθρου 18 του Ν. 4961/2022. Τα καθήκοντα του ΥΑΣΠΕ, όπως αναλύονται στο άρθρο 19 Ν. 4961/2022 είναι τα εξής:

α) η διαρκής μέριμνα για την ασφάλεια των συστημάτων δικτύου και πληροφοριών του φορέα κατά την έννοια της περ. 2 του άρθρου 3 του ν. 4577/2018 (Α' 199),

β) η συνεργασία με τους αρμόδιους φορείς στον τομέα της κυβερνοασφάλειας και η μέριμνα για την εφαρμογή των κατευθυντήριων οδηγιών, απαιτήσεων και μέτρων ασφαλείας που εκδίδουν,

γ) η τήρηση μητρώου του φορέα με τις υποδομές πληροφορικής και επικοινωνιών, το λογισμικό και τα πληροφοριακά αγαθά,

δ) η συμμετοχή στη διενέργεια ελέγχων σε συστήματα πληροφορικής και επικοινωνιών του φορέα για τη διακρίβωση του υφιστάμενου επιπέδου ασφάλειας,

ε) η εποπτεία της τήρησης της πολιτικής ασφάλειας συστημάτων πληροφορικής και επικοινωνιών του φορέα,

στ) η παρακολούθηση και αξιοποίηση νέων τεχνολογιών και εργαλείων ασφάλειας συστημάτων πληροφορικής και επικοινωνιών για την ενίσχυση του επιπέδου κυβερνοασφάλειας του φορέα και

ζ) η διενέργεια αξιολογήσεων του επιπέδου κυβερνοασφάλειας του φορέα σε συνεργασία με τις κατά περίπτωση αρμόδιες αρχές.

Επιπλέον, ο ΥΑΣΠΕ είναι υπεύθυνος για την κατάρτιση και την τήρηση σχεδίου ανάλυσης κινδύνου καθώς και της ενιαίας πολιτικής ασφάλειας συστημάτων πληροφορικής και επικοινωνιών.

Ο ΥΑΣΠΕ μπορεί, επίσης να αναλαμβάνει την ευθύνη για την παρακολούθηση των συστημάτων και των δικτύων, την ανίχνευση απειλών και την αντίδραση σε περιστατικά ασφαλείας.

Παράλληλα, πρέπει να δημιουργούνται και να ελέγχονται αυστηρά, τα προνομιακά δικαιώματα πρόσβασης, όπως αυτά που σχετίζονται με τους λογαριασμούς διαχειριστή συστημάτων ή δικτύων. Ο ΥΑΣΠΕ δύναται να είναι υπεύθυνος για την πρόσβαση με διαχειριστικά δικαιώματα (πχ. σε εξυπηρετητές, σταθμούς εργασίας, firewall, router, βάσεις δεδομένων, εφαρμογές).

Τέλος, είναι υπεύθυνος για τον συντονισμό και την εκτέλεση του σχεδίου ανάκαμψης.

Κωδικός Διαδικασίας	1.0	**Έκδοση**	1.0	**Σχετικά Πρότυπα**	*Ν. 4961/2022, ISO/IEC 27001:2013, Γενικός Κανονισμός, Προστασίας Δεδομένων, ENISA (Consumerization of IT), Οδηγίες της ΑΠΔΠΧ*
Σχετικές Απαιτήσεις	*Συμμόρφωση του Δήμου Περάματος με τον Ν. 4961/2022*				

Υπεύθυνος Προστασίας Δεδομένων

Καθήκον του Υπευθύνου Προστασίας Δεδομένων είναι να διασφαλίζει ότι ο Οργανισμός τηρεί τις απαιτήσεις που ορίζονται από το οικείο νομοθετικό και κανονιστικό πλαίσιο. Ειδικότερα:

α) ενημερώνει και συμβουλεύει τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία και τους υπαλλήλους που επεξεργάζονται τις υποχρεώσεις τους που απορρέουν από τον παρόντα κανονισμό και από άλλες διατάξεις της Ένωσης ή του κράτους μέλους σχετικά με την προστασία δεδομένων,

β) παρακολουθεί τη συμμόρφωση με τον Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR), με άλλες διατάξεις της Ένωσης ή του κράτους μέλους σχετικά με την προστασία δεδομένων και με τις πολιτικές του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία σε σχέση με την προστασία των δεδομένων προσωπικού χαρακτήρα, συμπεριλαμβανομένων της ανάθεσης αρμοδιοτήτων, της ευαισθητοποίησης και της κατάρτισης των υπαλλήλων που συμμετέχουν στις πράξεις επεξεργασίας, και των σχετικών ελέγχων,

γ) παρέχει συμβουλές, όταν ζητείται, όσον αφορά την εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων και παρακολουθεί την υλοποίησή της σύμφωνα με το άρθρο 35,

δ) συνεργάζεται με την εποπτική αρχή,

ε) ενεργεί ως σημείο επικοινωνίας για την εποπτική αρχή για ζητήματα που σχετίζονται με την επεξεργασία, περιλαμβανομένης της προηγούμενης διαβούλευσης που αναφέρεται στο άρθρο 36, και πραγματοποιεί διαβουλεύσεις, ανάλογα με την περίπτωση, για οποιοδήποτε άλλο θέμα.

Κατά την εκτέλεση των καθηκόντων του, ο υπεύθυνος προστασίας δεδομένων λαμβάνει δεόντως υπόψη τον κίνδυνο που συνδέεται με τις πράξεις επεξεργασίας, συνεκτιμώντας τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας.

Ομάδα Διαχείρισης Περιστατικών

Η δημιουργία Ομάδας Διαχείρισης Περιστατικών (εφεξής: Ομάδα) είναι το πρωταρχικό βήμα για την αντιμετώπιση περιστατικών ασφαλείας. Η βασική αρχή λειτουργίας της Ομάδας αυτής είναι η καταγραφή, η ανάλυση, η αξιολόγηση διαδικασιών και λειτουργιών, η πληροφόρηση και η ενημέρωση μεταξύ των μελών, ο σχεδιασμός, η βελτίωση με βάση την εμπειρία που αποκτάται.

Η Ομάδα πρέπει να είναι αντιπροσωπευτική το σύνολο των επιμέρους τμημάτων του Οργανισμού, που, μεταξύ άλλων, θα πρέπει να περιλαμβάνει μέλη από:

- Τον επικεφαλής της Ομάδας (μέλος της Διοίκησης)
- Τον Υπεύθυνο Προστασίας Δεδομένων (ΥΠΔ/DPO) του Οργανισμού.
- Την πληροφορική (IT).
- Την Νομική υπηρεσία (ή εξωτερικό συνεργάτη πάροχο νομικών υπηρεσιών).
- Το τμήμα Ανθρώπινου Δυναμικού

Επικεφαλής ομάδας

Το μέλος του Διοικητικού Συμβουλίου θα εξασφαλίσει ότι όλα τα μέλη της ομάδας επικοινωνούν αποτελεσματικά, συνεργάζονται και συντονίζονται με στόχο την γρήγορη και πλήρη ανάκαμψη.

Υπεύθυνος Ερευνών

Ο προϊστάμενος του τμήματος τεχνικής υποστήριξης (IT) θα συλλέξει, θα αναλύσει όλα τα αποδεικτικά στοιχεία, θα καθορίσει την αιτία, θα κατευθύνει τους υπόλοιπους αναλυτές ασφαλείας και θα εφαρμόσει ένα πλάνο για την ταχεία ανάκαμψη των συστημάτων και των υπηρεσιών.

Συντονιστής Επικοινωνίας

Ο υπεύθυνος Διαχείρισης Ανθρώπινου Δυναμικού θα αναλάβει την επικοινωνία με όλους τους εμπλεκόμενους υπαλλήλους ή τρίτους εντός ή εκτός του Οργανισμού (π.χ. αρχές, υποκείμενα, συνεργάτες κ.λπ.).

Υπεύθυνος Τεκμηρίωσης και τήρησης χρονοδιαγραμμάτων

Ο Υπεύθυνος Προστασίας Δεδομένων θα βεβαιωθεί ότι όλες οι δραστηριότητες της Ομάδας είναι τεκμηριωμένες ή θα τεκμηριωθούν στο τέλος των ενεργειών, συμπεριλαμβανομένων των ενεργειών κατά την διερεύνηση, ανακάλυψη και αποκατάστασης και θα φροντίσει για την θέση σε εφαρμογή ενός αξιόπιστου χρονοδιαγράμματος για κάθε στάδιο του περιστατικού.

Υπεύθυνος Διαχείρισης Εργαζομένων/Νομική Υποστήριξη

Η Νομική Υπηρεσία του Οργανισμού θα βοηθήσει στην νομική υποστήριξη και καθοδήγηση του υπευθύνου Διαχείρισης Ανθρώπινου Δυναμικού.

Συντονιστής Ασφαλείας Πληροφοριακών Συστημάτων

Ο Συντονιστής ασφάλειας πληροφοριακών συστημάτων είναι ο υψηλότερος υπεύθυνος για την κυβερνοασφάλεια στον Οργανισμό. Αναπτύσσει και υλοποιεί τη στρατηγική ασφαλείας και διαχειρίζεται τον προϋπολογισμό ασφαλείας. Ο ρόλος αυτός μπορεί να αποδοθεί στον Υπεύθυνο Πληροφορικής και Διαχείρισης Δεδομένων του Φορέα.

5. Διαδικασίες χειρισμού αποκλίσεων και εξαιρέσεων

Οι διαδικασίες χειρισμού των αποκλίσεων και εξαιρέσεων είναι ζωτικής σημασίας για τη διατήρηση της ασφάλειας των πληροφοριακών συστημάτων και των δεδομένων του Οργανισμού. Οι διαδικασίες που διεξάγει ο Οργανισμός κατά την αντιμετώπιση αποκλίσεων και εξαιρέσεων στην ασφάλεια δικτύων περιλαμβάνουν:

Καταγραφή και τεκμηρίωση

Ο Οργανισμός διενεργεί αναλυτική καταγραφή και τεκμηρίωση για κάθε απόκλιση από τις πρακτικές ασφάλειας. Ειδικότερα, προς τον σκοπό αυτό, έχει συνταχθεί, κατόπιν μελέτης, για τον Οργανισμό, Report συνολικού κινδύνου. Το Report συνολικού κινδύνου, το οποίο συντάσσεται βάσει απαιτήσεων του άρθρου 20 του Ν. 4961/2022, αποτελεί καταγραφή των απειλών, των ευπαθειών και των κινδύνων που αφορούν τον Οργανισμό.

Ο Οργανισμός καταγράφει όλες τις γνωστές κυβερνοαπειλές που ενδέχεται να τον επηρεάσουν, τις ευπαθείς περιοχές των πληροφοριακών συστημάτων και των δικτύων του και τα σημεία που είναι περισσότερο πιθανό να αποτελέσουν στόχο για κυβερνοεπιθέσεις. Απαιτείται, επιπλέον, καταγραφή προηγούμενων περιστατικών ασφαλείας ή επιθέσεων που έχουν επηρεάσει τον Οργανισμό.

Περεταίρω, αξιολογείται η τρέχουσα κατάσταση ασφάλειας των πληροφοριακών συστημάτων, των δικτύων και των διαδικασιών του Οργανισμού.

Αξιολόγηση των κινδύνων

Μετά την καταγραφή και τεκμηρίωση των απειλών και των ευπαθειών του Οργανισμού, ακολουθεί η αξιολόγηση του κινδύνου που ενέχουν. Πρέπει να αξιολογηθεί, ιδιαιτέρως, το πιθανό κόστος και οι επιπτώσεις των κυβερνοαπειλών για τον Οργανισμό, καθώς και ποια δεδομένα ή υπηρεσίες ενδέχεται να επηρεαστούν. Η διακοπή κάποιων από τις επιχειρησιακές διεργασίες του Οργανισμού μπορεί να έχει σημαντικές επιπτώσεις στη λειτουργία του. Για το λόγο αυτό, ο Οργανισμός οφείλει να εκτιμήσει το βαθμό εξάρτησης κάθε διεργασίας από τα περιουσιακά του στοιχεία και στη συνέχεια τους κινδύνους που τα απειλούν.

Η μεθοδολογία που ακολουθείται για την εκτίμηση των κινδύνων είναι η εξής: εκτιμάται η πιθανότητα να συμβεί κάποιο από τα περιστατικά που περιγράφονται στο Report Συνολικού Κινδύνου, σε σχέση με τις επιπτώσεις που θα έχει για τον οργανισμό ένα τέτοιο περιστατικό. Βάσει των εκτιμήσεων επί των κινδύνων, ο Οργανισμός προχωράει στη λήψη μέτρων που θα εξασφαλίσουν όσο το δυνατόν χαμηλότερο επίπεδο κινδύνου για τα δεδομένα και τις επιχειρησιακές του λειτουργίες γενικά.

Ο κίνδυνος χαρακτηρίζεται ως υψηλός, μέτριος ή αποδεκτός αναλόγως του αντικτύπου που ενδέχεται να επιφέρει στην ασφάλεια των πληροφοριακών συστημάτων του Οργανισμού και του μεγέθους της απειλής. Ολική διακοπή λειτουργίας του Οργανισμού με την έννοια της αδυναμίας

εξυπηρέτησης των πολιτών της πέραν του ορισμένου διαστήματος αυτού καθώς και αδυναμία συνολικής λειτουργίας του Οργανισμού πέραν ορισμένου διαστήματος συνεπάγεται πολύ σημαντικές συνέπειες τόσο για τους ανθρώπους που εξυπηρετεί, όσο και για τη φήμη του Οργανισμού και του Ελληνικού Δημοσίου. Αντιθέτως, ως αποδεκτό επίπεδο κινδύνου, ορίζεται το σημείο αυτό που θα επιτρέπει στον Οργανισμό να επαναφέρει τις επιχειρησιακές του λειτουργίες, δίχως να αντιμετωπίσει επιπτώσεις στη φήμη του και στους ανθρώπους που εξυπηρετεί.

Κατανόηση των αιτιών

Ο Οργανισμός οφείλει να διεξάγει την ως άνω αξιολόγηση με ιδιαίτερη προσοχή ως προς την αιτία που προκαλεί την συγκεκριμένη απειλή. Με τον τρόπο αυτό προκύπτουν τα προβλήματα που υπάρχουν καθώς και το αν αυτά αφορούν τις διαδικασίες, τον τεχνολογικό εξοπλισμό ή την ανθρώπινη δράση.

Λήψη μέτρων

Με σκοπό την βελτίωση της ασφάλειας των πληροφοριακών συστημάτων και την αποφυγή επανάληψης προβλημάτων και βάσει των απειλών και των ευπαθειών που έχουν καταγραφεί, ο Οργανισμός λαμβάνει τα κατάλληλα τεχνικά και οργανωτικά μέτρα.

Ο Οργανισμός έχει καταρτίσει Σχέδιο Ανάκαμψης από Καταστροφή ή DRP (Disaster Recovery Plan), στο οποίο περιγράφονται τα βήματα αντιμετώπισης και διαχείρισης των έκτακτων συμβάντων που απειλούν την επιχειρησιακή συνέχεια των διεργασιών του.

Μετά τη λήψη και την εφαρμογή των μέτρων ασφαλείας, ο Οργανισμός προβαίνει σε συνεχή επαλήθευση προκειμένου να εξασφαλίσει ότι λειτουργούν αποτελεσματικά. Οφείλει, επίσης, να μεριμνά για την συνεχή εκπαίδευση του προσωπικού του σχετικά με την ασφάλεια των πληροφοριακών συστημάτων, τις βέλτιστες πρακτικές και την αντίδραση σε πιθανές απειλές.

Επιπλέον, ο Οργανισμός οργανώνει και αναπτύσσει σχέδια για την αντιμετώπιση πιθανών κυβερνοεπιθέσεων και περιστατικών ασφαλείας.

Τέλος, παρακολουθεί την κατάσταση ασφαλείας καταγράφοντας ανωμαλίες και απειλές και καταρτίζοντας αναφορές για κάθε περιστατικό ασφαλείας.

Με σκοπό τη βελτίωση της ασφάλειας των πληροφοριακών συστημάτων και την αποφυγή επανάληψης προβλημάτων και βάσει των απειλών

Συνεχής ανάλυση και βελτίωση των πρακτικών,

Ο Οργανισμός πρέπει να εξετάζει συνεχώς τα μέτρα του και να τα βελτιώνει σύμφωνα με τις εξελίξεις στον τομέα της κυβερνοασφάλειας.

6. Επιμέρους Πολιτικές

6.1. Πολιτική Ασφάλειας Δικτύων

Εισαγωγή

Κάθε χρήστης των Πληροφοριακών Συστημάτων (Π.Σ.) του Δήμου Περάματος (εφεξής «Οργανισμός» ή Φορέας) θα πρέπει να συνεισφέρει στην ασφάλεια πληροφοριών και των υποδομών με την ορθή χρήση των πόρων τους και να τηρεί θεμελιώδεις κανόνες ορθής χρήσης και δεοντολογίας.

Σκοπός

Στόχος της συγκεκριμένης πολιτικής είναι να καθορίσει τον τρόπο με τον οποίο πρέπει να σχεδιαστεί και να διαχειρίζεται το δίκτυο του Οργανισμού.

Έχοντας ως στόχο την αντιμετώπιση των δυσμενέστερων σεναρίων, η δημιουργία και εφαρμογή της Πολιτικής Ασφάλειας Δικτύων (εφεξής: Πολιτική) αποτελεί μία από τις προϋποθέσεις συμμόρφωσης με την κείμενη νομοθεσία περί ασφάλειας πληροφοριών και προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΔΠΧ) συγκεκριμένα:

- *τις διατάξεις του Ν. 4961/2022 (ΦΕΚ Α' 146/27.07.2022)*[1]
- *τις διατάξεις του Κανονισμού (ΕΕ) 2016/679 (GDPR/ΓΚΠΔ)* [2],
- *τις διατάξεις του Ν. 4624/2019 (ΦΕΚ Α' 137/29.08.2019)* [3]

Τα πλεονεκτήματα από την υιοθέτηση και εφαρμογή της παρούσας Πολιτικής είναι πολλαπλά και μακροπρόθεσμα ωφέλιμα για τον Οργανισμό. Ειδικότερα, η εφαρμογή της Πολιτικής:

---

[1] Νόμος υπ' αριθμ. 4961/2022 Τεύχος Α' 146/27.07.2022: Αναδυόμενες τεχνολογίες πληροφορικής και επικοινωνιών, ενίσχυση της ψηφιακής διακυβέρνησης και άλλες διατάξεις.

[2] Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων).

[3] Νόμος υπ' αριθμ. 4624 Τεύχος Α' 137/29.08.2019, Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 και άλλες διατάξεις.

- Περιορίζει τη νομική έκθεση του Οργανισμού και τον προστατεύει από νομικές ενέργειες που τυχόν ασκηθούν εναντίον του, παρέχοντας στο προσωπικό εκ των προτέρων ειδοποίηση για τους κανονισμούς και τις πολιτικές που πρέπει να ακολουθούνται.
- Περιορίζει την ατομική και ιδία χρήση των πόρων και των υποδομών που παρέχονται από τον Οργανισμό.
- Συμβάλλει στη διαχείριση του κόστους μειώνοντας την ποσότητα των πόρων που χρησιμοποιούνται, όπως η αποθήκευση και το εύρος ζώνης.
- Συμβάλλει στην προστασία των πόρων και των δεδομένων των υπολογιστών ενός οργανισμού από κυβερνοεπιθέσεις και άλλες μορφές κλοπής ή διαρροής δεδομένων.
- Βοηθά στην πρόληψη παραβιάσεων συμμόρφωσης με ισχύοντες κανονισμούς και νομοθεσίες.
- Χρησιμεύει για την προστασία του Οργανισμού από τις σκόπιμες ή τυχαίες δραστηριότητες του εργατικού δυναμικού του.

Πεδίο εφαρμογής

Η συγκεκριμένη πολιτική πρέπει να εφαρμόζεται σε όλα τα συστήματα, διαδικασίες και χρήστες του Οργανισμού, περιλαμβανομένων Διευθυντών, Προϊσταμένων, υπαλλήλων, προμηθευτών και λοιπών τρίτων που έχουν πρόσβαση στα ΠΣ του Οργανισμού.

Σχεδιασμός ασφάλειας δικτύων

Ο σχεδιασμός των δικτύων είναι μια περίπλοκη διαδικασία που απαιτεί καλή γνώση των δικτυακών αρχών και της τεχνολογίας. Κάθε σχεδιασμός δικτύου είναι πιθανό να είναι διαφορετικός, με βάση ένα συγκεκριμένο σύνολο απαιτήσεων που καθορίζονται στο πρώιμο στάδιο της διαδικασίας αυτής. Αυτή η πολιτική δεν επιχειρεί να προσδιορίσει πώς τα μεμονωμένα δίκτυα πρέπει να σχεδιαστούν και να υλοποιηθούν, αλλά παρέχει καθοδήγηση για τα πρότυπα δομικά στοιχεία που πρέπει να χρησιμοποιούνται.

Απαιτήσεις

Ο σχεδιασμός του δικτύου πρέπει να βασίζεται στον σαφή ορισμό των απαιτήσεων και να περιλαμβάνει τους εξής παράγοντες, που σχετίζονται με την ασφάλεια και την προστασία των δεδομένων προσωπικού χαρακτήρα:

- Τη διαβάθμιση των πληροφοριών που μεταφέρονται σε όλο το δίκτυο, καθώς και τον έλεγχο της πρόσβασης των δικτύων.
- Την αξιολόγηση των κινδύνων και των πιθανών απειλών των δικτύων, λαμβάνοντας υπόψη τυχόν εγγενείς ευπάθειες.
- Το επίπεδο εμπιστοσύνης μεταξύ των διαφόρων συστατικών του δικτύου ή/και των συστημάτων ή/και των φορέων που θα αλληλοσυνδεθούν.
- Τα επίπεδα διαθεσιμότητας και ανθεκτικότητας που απαιτούνται από το δίκτυο.
- Τη γεωγραφική εξάπλωση του δικτύου.
- Τα μέτρα προστασίας που πρέπει να ισχύουν σε τοποθεσίες από τις οποίες θα υπάρχει πρόσβαση στο δίκτυο.
- Τις δυνατότητες ασφάλειας των υφιστάμενων υπολογιστών ή συσκευών που θα χρησιμοποιούνται για την πρόσβαση στο δίκτυο του Οργανισμού.

Οι απαιτήσεις πρέπει να καταγράφονται και να υπάρχει συμφωνία πριν από την έναρξη των εργασιών σχεδιασμού.

Διαχωρισμός δικτύων

Πρέπει να υιοθετηθεί η αρχή, ότι ένα δίκτυο οφείλει να αποτελείται από ένα σύνολο μικρότερων δικτύων διαχωρισμένα το ένα από το άλλο, με βάση τα επίπεδα εμπιστοσύνης ή τα οργανωτικά - επιχειρησιακά όρια (ή και τα δύο).

Ένα κατάλληλο επίπεδο εμπιστοσύνης πρέπει να διαμορφωθεί στο επίπεδο του τομέα δικτύου (domain level) και οι περίμετροι του τομέα πρέπει να ασφαλίζονται με ένα τείχος προστασίας, όπου αυτό ενδείκνυται.

Μέσα στα δίκτυα, πρέπει να χρησιμοποιούνται Εικονικά Τοπικά Δίκτυα (VLAN) για να διαχωρίσουν τις οργανωτικές μονάδες.

Οι servers πρέπει να βρίσκονται σε δικό τους, ξεχωριστό VLAN, διαχωρισμένο από τα PC των χρηστών και προστατευμένο από το firewall.

Περιμετρική ασφάλεια

Σε όλες τις περιμέτρους μεταξύ του εσωτερικού δικτύου και ενός εξωτερικού δικτύου (όπως το Διαδίκτυο) πρέπει να τεθούν σε εφαρμογή αποτελεσματικά μέτρα για να διασφαλίσουν ότι μόνο η εξουσιοδοτημένη κίνηση στο δίκτυο επιτρέπεται.

Δημόσια δίκτυα

Όταν οι πληροφορίες πρόκειται να μεταφερθούν μέσω ενός δημόσιου δικτύου, όπως το Διαδίκτυο, τότε πρέπει να χρησιμοποιείται ισχυρή κρυπτογράφηση μέσω SSL, για τη διασφάλιση της εμπιστευτικότητας των δεδομένων που διαβιβάζονται. Συγκεκριμένα, πρέπει να εγκατασταθούν έμπιστα πιστοποιητικά στους δικτυακούς ιστότοπους του Οργανισμού με μέγεθος κλειδιού τουλάχιστον 2048 bits.

Ασύρματα δίκτυα

Όλες οι ασύρματες συσκευές οι οποίες συνδέονται ή παρέχουν πρόσβαση στο δίκτυο του Οργανισμού πρέπει να ακολουθούν τους παρακάτω κανόνες:

- Χρησιμοποιούν πρωτόκολλα TKIP ή Advanced Encryption System (AES) με ελάχιστο μήκος κλειδιού τα 128 bit.
- Εγκαθίστανται, υποστηρίζονται και συντηρούνται από μια εγκεκριμένη ομάδα υποστήριξης.
- Χρησιμοποιούν τα εγκεκριμένα πρωτόκολλα και υποδομές πιστοποίησης του Οργανισμού.
- Διατηρούν μια φυσική διεύθυνση (διεύθυνση MAC) που μπορεί να καταχωρηθεί και να παρακολουθηθεί.
- Όλες οι συσκευές Bluetooth πρέπει να χρησιμοποιούν Secure Simple Pairing με ενεργοποιημένη την κρυπτογράφηση.
- Πρέπει να εγκατασταθεί ένα τείχος προστασίας μεταξύ του ασύρματου δικτύου και του κύριου τοπικού δικτύου (LAN).
- Εάν απαιτείται η χρήση ασύρματου δικτύου για τους επισκέπτες του Οργανισμού, τότε αυτό πρέπει να διαχωρίζεται από όλα τα εσωτερικά δίκτυα (συμπεριλαμβανομένων των εσωτερικών ασύρματων δικτύων) και να διασφαλίζεται με τη χρήση ενός τείχους προστασίας.
- Η πρόσβαση στα ΠΣ του Οργανισμού απαγορεύεται ρητώς από συσκευές, οι οποίες είναι ταυτόχρονα συνδεδεμένες στο ασύρματο δίκτυο και στο δίκτυο του Οργανισμού.

Όλες οι οικιακές ασύρματες συσκευές, οι οποίες παρέχουν πρόσβαση στο δίκτυο του Οργανισμού πρέπει να ακολουθούν τους παρακάτω κανόνες:

- Ενεργοποιήστε το WiFi Protected Access 2 (WPA2). Όταν ενεργοποιείτε το WPA2, διαμορφώστε ένα σύνθετο κοινόχρηστο μυστικό κλειδί (τουλάχιστον 20 χαρακτήρων) στον ασύρματο υπολογιστή-πελάτη και στο σημείο ασύρματης πρόσβασης.
- Απενεργοποιήστε την εκπομπή SSID.

- Αλλάξτε το προεπιλεγμένο όνομα SSID.
- Αλλάξτε το προεπιλεγμένο όνομα χρήστη και κωδικό πρόσβασης.

Φυσική ασφάλεια

Ο κύριος και κεντρικός εξοπλισμός του δικτύου πρέπει να στεγάζεται σε κατάλληλα ντουλάπια που κλειδώνουν ή σε ικριώματα (racks) σε ένα ασφαλές Computer Room στο οποίο μόνο εξουσιοδοτημένο προσωπικό υποστήριξης θα έχει πρόσβαση.

Απομακρυσμένη πρόσβαση

Η απομακρυσμένη πρόσβαση θα χορηγείται μόνο όταν είναι αναγκαία και έπειτα από την έγγραφη έγκριση του Υπεύθυνου Προστασίας Δεδομένων ή του Υπεύθυνου Ασφάλειας και όχι για όλους τους χρήστες από προεπιλογή.

Βασικές αρχές ασφάλειας δικτύων

Οι ακόλουθες βασικές αρχές, πρέπει να υιοθετηθούν για τη διαμόρφωση του δικτύου:

Υλικό δικτύων

Οι θύρες μεταγωγέων (Switch ports), συμπεριλαμβανομένων των διαγνωστικών θυρών θα ρυθμίζονται, ώστε να είναι απενεργοποιημένες και θα ανοίγουν μόνο όταν υπάρχει ανάγκη από τους διαχειριστές και μετά από έγκριση του Υπεύθυνου Ασφάλειας ή/και του Υπεύθυνου Προστασίας Δεδομένων. Δεν θα χρησιμοποιούνται διανομείς (Hubs), λόγω των εγγενών αδυναμιών της ασφάλειάς τους.

Α. Υπηρεσίες με περιορισμένη χρήση
Η χρήση των ακόλουθων υπηρεσιών πρέπει να παρακολουθείται και να γίνεται σε συγκεκριμένα συστήματα (είτε servers είτε workstations). Συγκεκριμένα, πρέπει να είναι από προεπιλογή απενεργοποιημένες και να ενεργοποιούνται μόνο έπειτα από την έγκριση του Υπεύθυνου Ασφάλειας ή/και του Υπεύθυνου Προστασίας Δεδομένων.

Πίνακας 4 – Περιορισμένες θύρες

Θύρα (port)	Υπηρεσία (Service)
20 (TCP)	ftpdata
21 (TCP)	ftp
22 (TCP)	ssh
23 (TCP)	telnet
25 (TCP)	smtp

53 (TCP / UDP)	domain
80 (TCP)	http
88 (TCP)	kerberos
110 (TCP)	pop3
119 (TCP)	nntp
123 (TCP)	ntp
143 (TCP)	imap
179 (TCP)	bgp
389 (TCP / UDP)	ldap
443 (TCP)	ssl
1080 (TCP)	socks
3128 (TCP)	squid
8000 (TCP)	http
8080 (TCP)	http
8888 (TCP)	http

Β. Επιτρεπόμενα Μηνύματα ICMP

Μόνο οι συγκεκριμένοι τύποι μηνυμάτων ICMP που παρουσιάζονται στον πίνακα που ακολουθεί μπορούν να επιτραπούν. Όλα τα υπόλοιπα πρέπει να απαγορεύονται.

Για τις συγκεκριμένες περιπτώσεις που χαρακτηρίζονται ως «Optional» στον παρακάτω πίνακα, από προεπιλογή δεν θα επιτρέπονται, αλλά αν κριθεί αναγκαίο θα επιτρέπονται μόνο έπειτα από την έγκριση του Υπεύθυνου Ασφάλειας ή και Υπεύθυνου Προστασίας Δεδομένων.

Πίνακας 5 – Μηνύματα ICMP

Τύπος	Περιγραφή	Inbound	Outbound
0	echo reply	Optional	Deny
3	destination unreachable	Allow	Deny
4	source quench	Allow	Allow
8	echo request (ping)	Optional	Allow
11	time exceeded	Optional	Optional
12	parameter problem	Deny	Deny

Διευθυνσιοδότηση (IP Addressing)

Θα χρησιμοποιείται IPv4 για τα εσωτερικά δίκτυα.

Το εσωτερικό εύρος διευθύνσεων IP που χρησιμοποιείται θα είναι καταγεγραμμένο και θα τηρείται ενημερωμένο στο έγγραφο με την αρχιτεκτονική του δικτύου του Οργανισμού.

Η ανάθεση και η χρήση των υπό-δικτύων πρέπει να παρακολουθείται προσεκτικά.

Πρωτόκολλα δικτύων

Το πρωτόκολλο που θα χρησιμοποιείται σε όλα τα δίκτυα θα είναι το TCP/IP.

Μόνο τα πρωτόκολλα και οι θύρες που απαιτούνται για έναν συγκεκριμένο εξυπηρετητή πρέπει να είναι ενεργοποιημένα από προεπιλογή, προκειμένου να

μειωθούν οι πάσης φύσεως επιθέσεις.

Διαχείριση ασφάλειας δικτύων

Από τη στιγμή που τα δίκτυα έχουν σχεδιαστεί και υλοποιηθεί με βάση ένα σαφές σύνολο απαιτήσεων ασφάλειας, υπάρχει μια συνεχιζόμενη ευθύνη για τη διαχείριση και τον έλεγχο του ασφαλούς περιβάλλοντος δικτύωσης για την προστασία των πληροφοριών του οργανισμού σε συστήματα και εφαρμογές. Αυτό πρέπει να επιτευχθεί μέσω των κατάλληλων ελέγχων στους ακόλουθους τομείς:

Καταγραφή και παρακολούθηση

Τα επίπεδα καταγραφής σχετικά με τις συσκευές του δικτύου πρέπει να διαμορφώνονται σύμφωνα με την πολιτική του οργανισμού και τα αρχεία καταγραφής να ελέγχονται σε τακτική βάση (περισσότερα στην Πολιτική Καταγραφής και Παρακολούθησης Ενεργειών Χρήσης). Συγκεκριμένα, τα εξής αρχεία καταγραφής πρέπει να ελέγχονται σε καθημερινή βάση από τον Υπεύθυνο Πληροφορικής:

- Αρχεία καταγραφής του συστήματος τείχους προστασίας.
- Αρχεία καταγραφής ασφαλείας τείχους προστασίας.
- Αρχεία καταγραφής των ΠΣ του Οργανισμού.

Τα παραπάνω αρχεία καταγραφής είναι σύμφωνα με την Πολιτική Καταγραφής και Παρακολούθησης Ενεργειών Χρήσης.

Ταυτόχρονα, τα αρχεία καταγραφής αποτελούν στοιχεία του εσωτερικού ελέγχου μέσω των οποίων θα γίνει η επιβεβαίωση της ορθής εφαρμογής των προδιαγραφόμενων μέτρων προστασίας (περισσότερα στη Διαδικασία Εσωτερικού Ελέγχου).

Έλεγχος αδυναμιών

Πρέπει να πραγματοποιούνται τεχνικοί έλεγχοι αδυναμιών σε επίπεδο δικτύου και υποδομών τουλάχιστον μία (1) φορά το χρόνο.

Αντικός (Antivirus) έλεγχος

Όλες οι συσκευές του Οργανισμού (φορητοί υπολογιστές, σταθεροί υπολογιστές, εξυπηρετητές) προστατεύονται από κακόβουλο λογισμικό. Για το σκοπό αυτό χρησιμοποιούνται αντιικά προγράμματα (antivirus), καθώς και προγράμματα τειχών ασφαλείας (firewall). Τόσο το antivirus, όσο και το firewall πρέπει να διαθέτουν ανά πάσα στιγμή τις πλέον πρόσφατες ενημερώσεις.

Τα αντιικά προγράμματα σαρώνουν τις συσκευές τις οποίες προστατεύουν: (α) περιοδικά (σε εβδομαδιαία βάση), (β) σε πραγματικό χρόνο σαρώνοντας (i) κάθε αρχείο που λαμβάνεται από το δίκτυο, (ii) κάθε αρχείο που ανοίγεται από τυχόν συνδεόμενο φορητό αποθηκευτικό μέσο πριν το άνοιγμα του αρχείου, (iii) κάθε συνδεόμενο φορητό αποθηκευτικό μέσο κατά τη σύνδεσή του, (iv) επισυναπτόμενα αρχεία ηλ. ταχυδρομείου και λήψεις από το διαδίκτυο (κατά την είσοδό τους στο δίκτυο, κατά την αποθήκευσή τους σε διακομιστές ηλεκτρονικού ταχυδρομείου και σε υπολογιστές) και (v) ιστοσελίδες.

Η σάρωση των αρχείων θα γίνεται με χρήση τόσο υπογραφών όσο και heuristics, ενώ δεν πρέπει να εξαιρούνται της σάρωσης τυχόν συμπιεσμένα αρχεία.

Αλλαγές δικτύων

Όλες οι αλλαγές στις συσκευές του δικτύου θα υπόκεινται σε Διαδικασία Διαχείρισης Αλλαγών και έπειτα από την κατάλληλη αξιολόγηση του κινδύνου (risk assessment) και τον απαραίτητο προγραμματισμό, θα τίθενται σε εφαρμογή.

Περιστατικά ασφάλειας δικτύων

Τα γεγονότα που θεωρούνται περιστατικά ασφάλειας του δικτύου πρέπει να καταγράφονται και να διαχειρίζονται σύμφωνα με την Πολιτική Διαχείρισης Περιστατικών και Επιχειρησιακής Συνέχειας.

6.2 Πολιτική Ορθής Χρήσης

Εισαγωγή

Κάθε χρήστης των Πληροφοριακών Συστημάτων (Π.Σ.) του Δήμου Περάματος (εφεξής «Οργανισμός» ή Φορέας) θα πρέπει να συνεισφέρει στην ασφάλεια πληροφοριών και των υποδομών με την ορθή χρήση των πόρων τους και να τηρεί θεμελιώδεις κανόνες ορθής χρήσης και δεοντολογίας.

Σκοπός

Ο σκοπός της παρούσας Πολιτικής, είναι να εγκαθιδρύσει και καθιερώσει την ορθή χρήση των πληροφοριακών υποδομών, των υπολογιστών, των συστημάτων δικτύωσης καθώς και της διαχείρισης πληροφοριών και δεδομένων του Οργανισμού. Η προστασία των δεδομένων και των πληροφοριακών συστημάτων σε έναν Οργανισμό αναδεικνύεται σε μια σημαντική, οργανωμένη και επιμελή καθημερινή δραστηριότητα.

Έχοντας ως στόχο την αντιμετώπιση των δυσμενέστερων σεναρίων, η δημιουργία και εφαρμογή της Πολιτικής Ορθής Χρήσης (εφεξής: Πολιτική) αποτελεί μία από τις προϋποθέσεις συμμόρφωσης με την κείμενη νομοθεσία περί ασφάλειας πληροφοριών και προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΔΠΧ) συγκεκριμένα:

- *τις διατάξεις του Ν. 4961/2022 (ΦΕΚ Α' 146/27.07.2022)*[4]
- *τις διατάξεις του Κανονισμού (ΕΕ) 2016/679 (GDPR/ΓΚΠΔ)* [5]*,*
- *τις διατάξεις του Ν. 4624/2019 (ΦΕΚ Α' 137/29.08.2019)* [6]

[4] Νόμος υπ' αριθμ. 4961/2022 Τεύχος Α' 146/27.07.2022: Αναδυόμενες τεχνολογίες πληροφορικής και επικοινωνιών, ενίσχυση της ψηφιακής διακυβέρνησης και άλλες διατάξεις.
[5] Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων).
[6] Νόμος υπ' αριθμ. 4624 Τεύχος Α' 137/29.08.2019, Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων

Τα πλεονεκτήματα από την υιοθέτηση και εφαρμογή της παρούσας Πολιτικής είναι πολλαπλά και μακροπρόθεσμα ωφέλιμα για τον Οργανισμό. Ειδικότερα, η εφαρμογή της Πολιτικής Ορθής Χρήσης:

- Περιορίζει τη νομική έκθεση του Οργανισμού και τον προστατεύει από νομικές ενέργειες που τυχόν ασκηθούν εναντίον του, παρέχοντας στο προσωπικό εκ των προτέρων ειδοποίηση για τους κανονισμούς και τις πολιτικές που πρέπει να ακολουθούνται.
- Περιορίζει την ατομική και ιδία χρήση των πόρων και των υποδομών που παρέχονται από τον Οργανισμό.
- Συμβάλλει στη διαχείριση του κόστους μειώνοντας την ποσότητα των πόρων που χρησιμοποιούνται, όπως η αποθήκευση και το εύρος ζώνης.
- Συμβάλλει στην προστασία των πόρων και των δεδομένων των υπολογιστών ενός οργανισμού από κυβερνοεπιθέσεις και άλλες μορφές κλοπής ή διαρροής δεδομένων.
- Βοηθά στην πρόληψη παραβιάσεων συμμόρφωσης με ισχύοντες κανονισμούς και νομοθεσίες.
- Χρησιμεύει για την προστασία του Οργανισμού από τις σκόπιμες ή τυχαίες δραστηριότητες του εργατικού δυναμικού του.

Βασικός στόχος της Πολιτικής είναι να εγκαθιδρυθεί στον Οργανισμό μία κουλτούρα ορθής και ασφαλούς χρήσης των πληροφοριακών συστημάτων, η οποία θα υιοθετηθεί από το σύνολο του εργατικού δυναμικού και κάθε εξουσιοδοτημένο χρήστη. Με τον τρόπο αυτό επιτυγχάνεται ο περιορισμός των περιστατικών που σχετίζονται με την παραβίαση ιδιωτικότητας ή ασφάλειας αύξηση της εμπιστοσύνης των υποκειμένων των δεδομένων προς τον Οργανισμό η συμμόρφωση με τις νομικές υποχρεώσεις και συνακόλουθα η βελτίωση της φήμης του Οργανισμού.

Πεδίο εφαρμογής

προσωπικού χαρακτήρα και ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 και άλλες διατάξεις.

Η Πολιτική Ορθής χρήσης αφορά όλα τα συστήματα πληροφορικής, τους υπολογιστές, τις συσκευές, τα συστήματα δικτύωσης, τα δεδομένα και τις πληροφορίες του Οργανισμού, καθώς και τους χρήστες και τις συσκευές τους μέσα στον Οργανισμό.

Πολιτική Ορθής Χρήσης

Ο Οργανισμός είναι υπεύθυνος για τον έλεγχο, τη διαχείριση και την απονομή δικαιωμάτων πρόσβασης σε χρήστες και εξουσιοδοτημένα πρόσωπα. Ο Οργανισμός θα πρέπει να εξασφαλίζει ότι όσοι έχουν πρόσβαση στις πληροφοριακές υποδομές, τις συσκευές, τα συστήματα και τα δεδομένα του Οργανισμού, έχουν νόμιμη ανάγκη να τα χρησιμοποιούν. Επίσης ο Οργανισμός πρέπει να μεριμνά ώστε κάθε χρήστης έχει κατανοήσει τις απαιτήσεις ασφαλείας για τη χρήση των συστημάτων πληροφορικής, των υπολογιστών και των συσκευών του Οργανισμού.

Συνακόλουθα, κάθε εργαζόμενος ή εξουσιοδοτημένος χρήστης των συστημάτων πληροφορικής, των υπολογιστών και των συσκευών του Οργανισμού, *οφείλει να τηρεί τις ακόλουθες οδηγίες:*

Α. ΕΥΘΥΝΗ ΠΡΟΣΒΑΣΗΣ

Κάθε εξουσιοδοτημένο πρόσωπο που χρησιμοποιεί τους πόρους και τα συστήματα πληροφορικής του Οργανισμού (εφεξής καλούμενος και «χρήστης») είναι υπεύθυνος για τη συμμόρφωση με αυτή την Πολιτική. Οι ειδικότερες ευθύνες πρόσβασης περιλαμβάνουν αλλά δεν περιορίζονται σε:

- Προϋποθέσεις πρόσβασης

Κάθε χρήστης οφείλει να έχει λάβει γνώση της Πολιτικής Προστασίας Προσωπικών Δεδομένων και είναι υπεύθυνος για την τήρηση των όρων της.

Κάθε χρήστης είναι υπεύθυνος για την προστασία των συστημάτων και των δεδομένων στα οποία έχει πρόσβαση. Η ευθύνη του καλύπτει τόσο τις μηχανογραφικές όσο και τις μη μηχανογραφικές συσκευές πληροφορικής και τεχνολογίας πληροφοριών που βρίσκονται στην κατοχή του Οργανισμού. Οι χρήστες

αναμένεται να μάθουν και να συμμορφωθούν με όλες τις πολιτικές του Οργανισμού σχετικά με την προστασία των πληροφοριών.

- Ευθύνη για τη διατήρηση του απορρήτου των κωδικών πρόσβασης

Οι κωδικοί πρόσβασης που σχετίζονται με τον υπηρεσιακό λογαριασμό ενός χρήστη ή άλλο αναγνωριστικό του Οργανισμού δεν πρέπει να κοινοποιούνται. Οι παραβιασμένοι κωδικοί πρόσβασης ενδέχεται να επηρεάσουν όχι μόνο το άτομο, αλλά και άλλους χρήστες πόρων και συστημάτων πληροφορικής του Οργανισμού.

- Παραβιάσεις

Κάθε χρήστης αποδέχεται την ευθύνη για όλες τις παραβιάσεις που προκύπτουν από ένα σύστημα υπολογιστή (υπηρεσιακό ή ιδιωτικό) κατά τη χρήση οποιωνδήποτε πόρων και συστημάτων πληροφορικής του Οργανισμού συμπεριλαμβανομένων, ενδεικτικά, των περιπτώσεων που το σύστημα είναι συνδεδεμένο σε δίκτυο του Οργανισμού ή χρησιμοποιώντας τον υπηρεσιακό λογαριασμό του χρήστη.

- Αναφορά παραβιάσεων

Κάθε χρήστης οφείλει να αναφέρει στον Οργανισμό κάθε είδους παραβίαση, εσφαλμένη χρήση ή πιθανότητα παραβίασης της ασφάλειας των συστημάτων πληροφορικής, συσκευών ή δεδομένων του Οργανισμού. Οποιοδήποτε περιστατικό που μπορεί να οδηγήσει σε παραβίαση ή αποτελεί παραβίαση πρέπει να γνωστοποιείται στον Οργανισμό το συντομότερο δυνατό, ενδεικτικά εντός διαστήματος είκοσι τεσσάρων (24) ωρών από τη στιγμή που γίνεται αντιληπτό από κάποιον χρήστη.

Β. ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑ

Κάθε χρήστης οφείλει να γνωρίζει και να τηρεί τις ακόλουθες οδηγίες της Πολιτικής Ορθής Χρήσης, προκειμένου να διασφαλίζεται η εμπιστευτικότητα των πληροφοριών του Οργανισμού:

- Να τηρεί εχεμύθεια για θέματα που χαρακτηρίζονται ως απόρρητα από τις κείμενες διατάξεις[7] ή όταν αυτό επιβάλλεται από την κοινή πείρα και λογική, για γεγονότα ή πληροφορίες των οποίων λαμβάνει γνώση ή επεξεργάζεται κατά την εκτέλεση των καθηκόντων του.

- Να περιορίζεται μόνο στην πρόσβαση/επεξεργασία των πληροφοριών που είναι απαραίτητες για την εκτέλεση των καθηκόντων του.

- Να γνωρίζει ότι οποιαδήποτε ενέργεια (δηλ. καταχώρηση, μεταβολή, διαγραφή, εμφάνιση ή εκτύπωση στοιχείων) που πραγματοποιείται στα πληροφοριακά συστήματα του Οργανισμού, δύναται να καταγράφεται και μπορεί να αποδοθεί στον υπάλληλο που την πραγματοποίησε.

- Να λαμβάνει μέριμνα για την όσο το δυνατόν καθαρότερη επιφάνεια εργασίας χωρίς να εκτίθενται απροστάτευτα έντυπα ή ηλεκτρονικά υπηρεσιακά δεδομένα.

Γ. ΟΡΘΗ ΧΡΗΣΗ ΔΙΑΔΙΚΤΥΟΥ / ΗΛΕΚΤΡΟΝΙΚΟΥ ΥΠΗΡΕΣΙΑΚΟΥ ΤΑΧΥΔΡΟΜΕΙΟΥ

Η πλοήγηση στο Διαδίκτυο μέσω των πληροφοριακών συστημάτων και συστημάτων του Οργανισμού εγκυμονεί τους περισσότερους κινδύνους για την ασφάλεια των υποδομών και των δεδομένων του Οργανισμού. Η τήρηση των ακόλουθων πρακτικών ατομικά, από κάθε χρήστη, ελαχιστοποιεί τους κινδύνους που μπορούν να προκύψουν από τη μη ορθή χρήση του Διαδικτύου.

Ειδικότερα, κάθε χρήστης είναι κρίσιμο να κατανοήσει και οφείλει να ακολουθεί τις κάτωθι οδηγίες όταν συνδέεται στο Διαδίκτυο κάνοντας χρήση είτε των συστημάτων δικτύου είτε των ηλεκτρονικών πόρων (συσκευών) του Οργανισμού.

[7] Ν. 4624/2019: Προστασία των προσωπικών δεδομένων, Ν. 3471/06: Προστασία των προσωπικών δεδομένων στον τομέα των ηλεκτρονικών επικοινωνιών, Ν.3842/2010: Κώδικας Φορολογίας και Εισοδήματος - Άρθρο 11, Ν.2960/2001: Εθνικός Τελωνειακός Κώδικας - Άρθρο 11

Ορθή Χρήση του Διαδικτύου

Ένα από τα κύρια στοιχεία της Πολιτικής Ορθής Χρήσης, είναι ο καθορισμός της κατάλληλης και αντίστοιχα της μη αποδεκτής χρήσης του Διαδικτύου.

Ενδεικτικά, οι χρήστες πρέπει να αποφεύγουν την πλοήγηση σε ιστοσελίδες με το ακόλουθο περιεχόμενο:

- Λογαριασμοί μέσων κοινωνικής δικτύωσης
- Πλατφόρμες ροής σε πραγματικό χρόνο (streaming platforms)
- Ηλεκτρονικές αγορές
- Ειδήσεις
- Προσωπικό ηλεκτρονικό ταχυδρομείο ή άλλες προσωπικές επικοινωνίες
- Πορνογραφία
- Τυχερά παιχνίδια
- Παράνομη δραστηριότητα

Επίσης συστήνεται σε όλους τους χρήστες να μην εισέρχονται στο δίκτυο του Οργανισμού ή να χρησιμοποιούν υπηρεσιακές συσκευές, μέσω δημόσιου Wi-Fi.

Ορθή Χρήση του Ηλεκτρονικού Υπηρεσιακού Ταχυδρομείου

Κατά τη χρήση του υπηρεσιακού ηλεκτρονικού ταχυδρομείου του Οργανισμού, κάθε εξουσιοδοτημένος χρήστης οφείλει:

- Να μη γίνεται χρήση του διαδικτύου και του υπηρεσιακού ηλεκτρονικού ταχυδρομείου με τρόπο που να αντιβαίνει τον υπηρεσιακό ρόλο του χρήστη και μπορεί να προσβάλλει το κύρος του Οργανισμού.

- Να μη διακινεί μηνύματα ηλεκτρονικού ταχυδρομείου με παράνομο ή άσεμνο περιεχόμενο και με κακόβουλο λογισμικό.

- Να μην αποστέλλει σε άλλους χρήστες, ανεπιθύμητα ηλεκτρονικά μηνύματα (unsolicited mails ή junk mails) ή άλλου διαφημιστικού ή προωθητικού περιεχομένου (spams).

- Να μην αποστέλλει μη υπηρεσιακά δεδομένα/αρχεία μέσω του υπηρεσιακού ηλεκτρονικού ταχυδρομείου.

- Να μην αποστέλλει υπηρεσιακά δεδομένα/αρχεία μέσω μη υπηρεσιακού ηλεκτρονικού ταχυδρομείου.

- Να μη διακινεί εμπιστευτικές ή απόρρητες πληροφορίες και προσωπικά δεδομένα εργαζομένων στον Οργανισμό ή πολιτών, μέσω ηλεκτρονικού ταχυδρομείου ή του διαδικτύου χωρίς τη λήψη μέτρων που καθιστούν ασφαλή τη μετάδοση της πληροφορίας (πχ κρυπτογράφηση).

- Να μην ανοίγει ή αποθηκεύει επισυνημμένα αρχεία και να μην ανοίγει συνδέσμους (links) που περιέχονται σε μηνύματα ηλεκτρονικού ταχυδρομείου από άγνωστους αποστολείς ή ακόμη και από γνωστούς αποστολείς όταν φαίνεται ότι αποστέλλουν μηνύματα που δεν ανέμενε να λάβει.

- Να επικοινωνεί άμεσα προς ενημέρωση του αρμοδίου υπεύθυνου του Οργανισμού (π.χ. Τμήμα Πληροφορικής ή Διοικητικό Τμήμα) το αργότερο εντός είκοσι τεσσάρων (24) ωρών από τη στιγμή που ήρθε σε γνώση του ή εντόπισε οποιοδήποτε ύποπτο μήνυμα ηλεκτρονικού ταχυδρομείου.

Δ. ΟΡΘΗ ΧΡΗΣΗ ΣΤΑΘΕΡΩΝ ΚΑΙ ΦΟΡΗΤΩΝ ΥΠΟΛΟΓΙΣΤΙΚΩΝ ΜΕΣΩΝ

Ως σταθερές υπολογιστικές συσκευές ορίζονται οι σταθεροί ηλ. υπολογιστές (desktop PCs) και οι συνδεδεμένες με αυτούς περιφερειακές συσκευές (εκτυπωτές, αντιγραφικά, σαρωτές εγγράφων κλπ) που χρησιμοποιεί το προσωπικό του Οργανισμού στην εργασία του.

Ως φορητές υπολογιστικές συσκευές ορίζονται, όχι περιοριστικά, οι παρακάτω:

- Φορητοί υπολογιστές (laptops)
- Φορητές συσκευές αποθήκευσης (usb sticks, εξωτερικοί σκληροί δίσκοι)
- Συσκευές Tablet
- Έξυπνα τηλέφωνα (smartphones)

Η ορθή χρήση σταθερών και φορητών υπολογιστικών μέσων αφορά μέτρα προστασίας που πρέπει να υπάρχουν κατά τη χρήση σταθερών και φορητών ηλ. συσκευών στον Οργανισμό, με στόχο τον μετριασμό των ακόλουθων κινδύνων:

- Απώλεια ή κλοπή των συσκευών, συμπεριλαμβανομένων και των δεδομένων τους.
- Εισαγωγή ιών και κακόβουλου λογισμικού στο δίκτυο.
- Διαρροή διαβαθμισμένων πληροφοριών, μέσω κακόβουλης αντιγραφής ή της παρατήρησης σε δημόσια θέα.

Τα μέτρα αυτά, πρέπει να τηρούνται ανά πάσα στιγμή, κατά τη χρήση του συνόλου των συσκευών και τη μεταφορά των φορητών συσκευών και πρέπει να εφαρμόζονται σε όλα τα συστήματα και τις διαδικασίες από το σύνολο των χρηστών των συσκευών

του Κέντρου, συμπεριλαμβανομένων των μελών της διοίκησης, των διευθυντικών στελεχών, των υπαλλήλων, των προμηθευτών, των εθελοντών και λοιπών τρίτων που έχουν πρόσβαση στα προσωπικά δεδομένα του Κέντρου.

Τα μέτρα ορθής χρήσης σταθερών και φορητών υπολογιστικών μέσων είναι τα εξής:

- Μην αφαιρείτε αναγνωριστικά σημάδια της συσκευής, όπως η ετικέτα παγίου αγαθού του Κέντρου ή ο σειριακός αριθμός.

- Βεβαιωθείτε ότι η φορητή συσκευή αποθηκεύεται σε ασφαλές σημείο, όταν δεν χρησιμοποιείται και ότι το κλειδί δεν είναι εύκολα προσβάσιμο.

- Βλάβες σχετικά με τις συσκευές πρέπει να καταγράφονται και να κοινοποιούνται στο αρμόδιο τμήμα.

- Μην προσθέτετε περιφερειακό εξοπλισμό στη συσκευή χωρίς την έγκριση του αρμόδιου τμήματος.

- Δεν επιτρέπεται να μεταφέρετε εκτός του χώρου εργασίας σας τις φορητές συσκευές που παρέχονται από το Κέντρο. Εξαίρεση σε αυτό τον κανόνα θα δίνεται μόνο, έπειτα από έγκριση της Διοίκησης του Κέντρου.

- Στην περίπτωση που η συσκευή μεταφέρεται εκτός χώρου εργασίας σας (έπειτα από έγκριση της Διοίκησης), πρέπει να βεβαιωθείτε ότι η συσκευή μεταφέρεται σε μια προστατευτική θήκη ώστε να μην εκτίθεται σε καταστάσεις στις οποίες μπορεί να πάθει ζημιά.

- Στην περίπτωση που η συσκευή μεταφέρεται εκτός χώρου εργασίας σας (έπειτα από έγκριση της Διοίκησης), δεν πρέπει να την αφήνετε χωρίς επιτήρηση σε δημόσια θέα.

Έλεγχοι πρόσβασης

- Πρέπει να εφαρμόζετε πλήρη κρυπτογράφηση δίσκου στις συσκευές που χρησιμοποιείτε.

- Δεν πρέπει να αποθηκεύετε διαβαθμισμένες πληροφορίες σε φορητή συσκευή, εκτός εάν αυτό έχει εγκριθεί και έχουν τεθεί κατάλληλοι έλεγχοι (π.χ. κρυπτογράφηση) σε εφαρμογή.

- Μην κρατάτε τα διακριτικά πρόσβασης, Προσωπικούς Αριθμούς Αναγνώρισης ή άλλα στοιχεία ασφαλείας μαζί με τη συσκευή.

- Βεβαιωθείτε ότι κλειδώνει η οθόνη της συσκευής μετά από ένα σύντομο χρονικό διάστημα στο οποίο δεν χρησιμοποιείται και απαιτεί έναν κωδικό πρόσβασης για να ξεκλειδώσει.

- Οι κωδικοί που χρησιμοποιούνται πρέπει να είναι ισχυροί και να είναι δύσκολο να τους μαντέψει κάποιος.

- Δεν πρέπει να ρυθμιστούν μη ασφαλείς συνδέσεις (δηλαδή εκείνες που δεν απαιτούν κωδικό πρόσβασης).

- Οι σταθερές και φορητές συσκευές του Κέντρου προορίζονται μόνο για επαγγελματική χρήση. Δεν πρέπει να τις μοιράζεστε με την οικογένεια ή τους φίλους σας ή να χρησιμοποιούνται για τις προσωπικές σας δραστηριότητες.

- Μπορεί να σας ζητηθεί να επιστρέψετε τη συσκευή στο Γραφείο Ολοκληρωμένου Πληροφοριακού Συστήματος, ανά πάσα στιγμή, για επιθεώρηση και έλεγχο.

- Δεν πρέπει να εγκαταστήσετε οποιοδήποτε μη εξουσιοδοτημένο λογισμικό στη συσκευή, χωρίς τη συμβουλή του αρμόδιου τμήματος.

- Δεν πρέπει αλλάξετε τη διαμόρφωση ή την εγκατάσταση της συσκευής, χωρίς τη συμβουλή του αρμόδιου τμήματος.

Μη ‘’έμπιστο’’ λογισμικό

- Πρέπει να εγκαθίσταται μόνο ‘’έμπιστο’’ λογισμικό στη συσκευή και μόνο μετά την έγκριση του αρμόδιου τμήματος.

- Πρέπει να εφαρμόσετε λίστα με άδειες χρήσης, για να επιτρέψετε την εγκατάσταση μόνο εγκεκριμένων εφαρμογών, επαληθεύοντας ότι οι εφαρμογές λαμβάνουν μόνο τα απαραίτητα δικαιώματα στη φορητή συσκευή ή εφαρμόζοντας ένα ασφαλή χώρο στη συσκευή, που απομονώνει τα δεδομένα και τις εφαρμογές του Κέντρου από όλα τα υπόλοιπα δεδομένα και τις εφαρμογές της φορητής συσκευής.

- Πρέπει να συμβουλεύεστε το αρμόδιο τμήμα σε περίπτωση που θέλετε να εγκαταστήσετε μη-''έμπιστο'' λογισμικό και αυτό το λογισμικό πρέπει πρώτα να εγκριθεί από τον Υπεύθυνο Προστασίας Προσωπικών Δεδομένων.

- Πρέπει να εφαρμόζετε όλες τις αυτόματες ενημερώσεις και τις διορθώσεις ασφάλειας του κατασκευαστή.

Τεχνικές κρυπτογράφησης

- Η συσκευή πρέπει να ασφαλίζεται, έτσι ώστε όλα τα δεδομένα της να είναι κρυπτογραφημένα (τουλάχιστον με τη δυνατότητα κρυπτογράφησης του ίδιου του λειτουργικού συστήματος) και έτσι να είναι προσβάσιμα τα δεδομένα μόνο εάν ο κωδικός πρόσβασης είναι γνωστός.

- Εάν η συσκευή παρέχεται με κρυπτογράφηση, μην την απενεργοποιήσετε.

Προστασία από Ιούς

- Πρέπει να εγκαθίσταται λογισμικό προστασίας από ιούς στη συσκευή.

- Βεβαιωθείτε ότι η συσκευή συνδέεται με το δίκτυο σε τακτική βάση για την ενημέρωση και τον έλεγχο αναφορικά με τους ιούς και λοιπό κακόβουλο λογισμικό.

- Μην απενεργοποιείτε την προστασία από ιούς στη συσκευή.

- Πρέπει να κάνετε αυτόματη επαλήθευση και λήψη ενημερώσεων καθημερινά.

- Πραγματοποιήστε σάρωση σε πραγματικό χρόνο από κάθε αρχείο, όπως αυτό λήφθηκε, ανοίχθηκε ή εκτελέστηκε.

- Πραγματοποιήστε σάρωση όλων των σκληρών δίσκων και των αφαιρούμενων μέσων, ανά τακτικά χρονικά διαστήματα.

Σύνδεση δικτύου

- Η συσκευή πρέπει να συνδέεται μόνο στο προβλεπόμενο δίκτυο για τη χρήση του Κέντρου.

- Η συσκευή δεν πρέπει να συνδέεται σε μη-έμπιστα δίκτυα (όπως εξωτερικά ασύρματα δίκτυα).

- Εάν πρέπει να συνδεθεί σε ένα μη-έμπιστο δίκτυο, τότε πρέπει να χρησιμοποιείται ένα VPN, ώστε να διασφαλιστεί η εμπιστευτικότητα και η ακεραιότητα της πληροφορίας που θα μεταδοθεί.

- Δεν πρέπει να γίνονται αλλαγές στις ρυθμίσεις δικτύου της συσκευής χωρίς την έγκριση του αρμόδιου τμήματος.

Χρήση μη-έμπιστων φορητών συσκευών

- Όλες οι φορητές συσκευές θεωρούνται μη-έμπιστες, εκτός εάν το Κέντρο έχει φροντίσει για την εφαρμογή κατάλληλων ρυθμίσεων ασφάλειας και παρακολουθεί συνεχώς την ασφάλειά τους.

- Μην προσπαθήσετε να παρακάμψετε ή να διαγράψετε τις αρχικές ρυθμίσεις της φορητής συσκευής.

Επίβλεψη

- Όταν βρίσκεστε σε δημόσιους χώρους ή χώρους γραμματείας - υποδοχής του Κέντρου, βεβαιωθείτε ότι τοποθετείτε τη συσκευή με τέτοιο τρόπο, ώστε μη εξουσιοδοτημένα άτομα να μην μπορούν να δουν ή φωτογραφίσουν ή βιντεοσκοπήσουν την οθόνη.

Ε. ΔΙΑΧΕΙΡΙΣΗ ΚΩΔΙΚΩΝ ΠΡΟΣΒΑΣΗΣ

Κάθε εξουσιοδοτημένος χρήστης των συσκευών και των πληροφοριακών συστημάτων του Οργανισμού, των οποίων η πρόσβαση είναι δυνατή με τη χρήση κωδικών, θα πρέπει να λαμβάνει υπόψιν και τηρεί τα κάτωθι:

- Να τηρεί μυστικά τα στοιχεία του προσωπικού λογαριασμού του (όνομα χρήστη και κωδικός) και να ειδοποιεί άμεσα τον προϊστάμενο του για τυχόν διαρροή τους.

- Να μη κοινοποιεί σε κανέναν τρίτο (ούτε τηλεφωνικά ούτε με ηλεκτρονικό ταχυδρομείο) τους προσωπικούς κωδικούς πρόσβασης του. Επίσης να μην τους σημειώνει σε μέρη όπου μπορούν να αποκαλυφθούν (π.χ. σε εκτεθειμένα χαρτιά ή αρχεία)

- Να λαμβάνει μέριμνα ώστε να τους αλλάζει περιοδικά (ενδεικτικά ανά έξι μήνες, με εντολή του αρμόδιου προϊσταμένου του)

- Να κλειδώνει με μυστικό προσωπικό κωδικό την επιφάνεια εργασίας του προσωπικού του υπολογιστή όταν απουσιάζει από το γραφείο

Καταρχάς, ο ίδιος ο Οργανισμός οφείλει να μεριμνά:

- Για την εγκατάσταση ισχυρών και αυξημένης ασφάλειας κωδικών πρόσβασης
- Για την περιοδική και συχνή αλλαγή των κωδικών (ενδεικτικά κάθε τρεις ή έξι μήνες)

ΣΤ. ΠΟΛΙΤΙΚΕΣ ΚΑΙ ΠΡΑΚΤΙΚΕΣ ΧΡΗΣΤΗ ΕΠΙΣΚΕΠΤΗ

Στην περίπτωση που οι χρήστες ή οι εργαζόμενοι του φορέα υποχρεούνται να επιτρέψουν την πρόσβαση **χρήστη - επισκέπτη** σε συσκευή ή το δίκτυο του Οργανισμού, οφείλουν να τους ενημερώνουν εκ των προτέρων και να παρακολουθούν ότι οι προσωρινοί χρήστες - επισκέπτες τηρούν τις πρακτικές και τις πολιτικές προστασίας πληροφοριών που εφαρμόζονται από τον Οργανισμό.

Ειδικότερα, οφείλουν να καθιστούν σαφές ότι οι προσωρινοί επισκέπτες – χρήστες δεν έχουν αδιάληπτη πρόσβαση στους υλικούς, τεχνολογικούς και πληροφοριακούς πόρους του Οργανισμού και να οριοθετούν την πρόσβαση αποκλειστικά για το σκοπό και το χρονικό διάστημα που κρίνεται αναγκαίο για την διεκπεραίωση της εργασίας του προσωρινού επισκέπτη. Προτείνεται επίσης η επιτήρηση του επισκέπτη – χρήστη καθ' όλη τη διάρκεια χρήσης τυχόν συσκευής ή δικτύου του Οργανισμού, από αρμόδιο εξουσιοδοτημένο άτομο που θα υποδεικνύει ο Φορέας.

Ζ. ΕΥΘΥΝΗ ΤΟΥ ΟΡΓΑΝΙΣΜΟΥ ΩΣ ΠΡΟΣ ΤΗ ΧΡΗΣΗ ΛΟΓΙΣΜΙΚΟΥ ΚΑΙ ΕΞΟΠΛΙΣΜΟΥ

Ο Οργανισμός, ως Υπεύθυνος Επεξεργασίας κατά τον ορισμό του Γενικού Κανονισμού Προστασίας Δεδομένων (ΓΚΠΔ ή GDPR - Κανονισμός (ΕΕ) 2016/679), αλλά και προς συμμόρφωση με το Νόμο 4961/2022 οφείλει:

- Να χρησιμοποιεί μόνο νόμιμο λογισμικό και μόνο κατόπιν έγκρισης από την αρμόδια υπηρεσία ή Τμήμα του Οργανισμού και εν γένει να προστατεύει τα πνευματικά δικαιώματα και την πνευματική ιδιοκτησία.

- Να μην επιτρέπει την χρήση του εξοπλισμού που του έχει διατεθεί σε μη εξουσιοδοτημένα πρόσωπα.

6.3 Πολιτική Πρόσβασης

Εισαγωγή

Κάθε χρήστης των Πληροφοριακών Συστημάτων (Π.Σ.) του Δήμου Περάματος (εφεξής «Οργανισμός» ή Φορέας) θα πρέπει να συνεισφέρει στην ασφάλεια πληροφοριών και των υποδομών με την ορθή χρήση των πόρων τους και να τηρεί θεμελιώδεις κανόνες ορθής χρήσης και δεοντολογίας.

Σκοπός

Σκοπός της συγκεκριμένης πολιτικής είναι να καθορίσει τους κατάλληλους κανόνες (τεχνικά και οργανωτικά μέτρα), προκειμένου να διασφαλιστεί ότι η πρόσβαση στα δεδομένα και τις υπηρεσίες του Οργανισμού, επιτρέπεται μόνο σε εξουσιοδοτημένους χρήστες και ότι τα κατάλληλα δικαιώματα έχουν οριστεί, εφαρμόζονται και αναθεωρούνται επαρκώς.

Έχοντας ως στόχο την αντιμετώπιση των δυσμενέστερων σεναρίων, η δημιουργία και εφαρμογή της Πολιτικής Πρόσβασης (εφεξής: Πολιτική) αποτελεί μία από τις προϋποθέσεις συμμόρφωσης με την κείμενη νομοθεσία περί ασφάλειας πληροφοριών και προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΔΠΧ) συγκεκριμένα:

- *τις διατάξεις του Ν. 4961/2022 (ΦΕΚ Α' 146/27.07.2022)*[8]
- *τις διατάξεις του Κανονισμού (ΕΕ) 2016/679 (GDPR/ΓΚΠΔ)* [9]*,*
- *τις διατάξεις του Ν. 4624/2019 (ΦΕΚ Α' 137/29.08.2019)* [10]

[8] Νόμος υπ' αριθμ. 4961/2022 Τεύχος Α' 146/27.07.2022: Αναδυόμενες τεχνολογίες πληροφορικής και επικοινωνιών, ενίσχυση της ψηφιακής διακυβέρνησης και άλλες διατάξεις.
[9] Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων).
[10] Νόμος υπ' αριθμ. 4624 Τεύχος Α' 137/29.08.2019, Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 και άλλες διατάξεις.

Τα πλεονεκτήματα από την υιοθέτηση και εφαρμογή της παρούσας Πολιτικής είναι πολλαπλά και μακροπρόθεσμα ωφέλιμα για τον Οργανισμό. Ειδικότερα, η εφαρμογή της Πολιτικής:

- Περιορίζει τη νομική έκθεση του Οργανισμού και τον προστατεύει από νομικές ενέργειες που τυχόν ασκηθούν εναντίον του, παρέχοντας στο προσωπικό εκ των προτέρων ειδοποίηση για τους κανονισμούς και τις πολιτικές που πρέπει να ακολουθούνται.
- Περιορίζει την ατομική και ιδία χρήση των πόρων και των υποδομών που παρέχονται από τον Οργανισμό.
- Συμβάλλει στη διαχείριση του κόστους μειώνοντας την ποσότητα των πόρων που χρησιμοποιούνται, όπως η αποθήκευση και το εύρος ζώνης.
- Συμβάλλει στην προστασία των πόρων και των δεδομένων των υπολογιστών ενός οργανισμού από κυβερνοεπιθέσεις και άλλες μορφές κλοπής ή διαρροής δεδομένων.
- Βοηθά στην πρόληψη παραβιάσεων συμμόρφωσης με ισχύοντες κανονισμούς και νομοθεσίες.
- Χρησιμεύει για την προστασία του Οργανισμού από τις σκόπιμες ή τυχαίες δραστηριότητες του εργατικού δυναμικού του.

Πεδίο Εφαρμογής

Η συγκεκριμένη πολιτική πρέπει να εφαρμόζεται σε όλα τα συστήματα, διαδικασίες και χρήστες του Οργανισμού συμπεριλαμβανομένων των Διευθυντών, των Προϊσταμένων, των υπαλλήλων, των προμηθευτών και λοιπών τρίτων που έχουν πρόσβαση στα ΠΣ του Οργανισμού.

Διαχείριση πρόσβασης χρήστη

Οι τυπικές διαδικασίες ελέγχου πρόσβασης χρήστη για κάθε σύστημα του Οργανισμού πρέπει να είναι τεκμηριωμένες, να εφαρμόζονται και να τηρούνται συνεχώς ενημερωμένες ώστε να εξασφαλιστεί η εξουσιοδοτημένη πρόσβαση των χρηστών και η αποτροπή μη εξουσιοδοτημένης πρόσβασης.

Πρέπει να καλύπτουν όλα τα στάδια του κύκλου ζωής της πρόσβασης των χρηστών, από την αρχική καταχώρηση των νέων χρηστών μέχρι το τελικό στάδιο

της διαγραφής των λογαριασμών χρηστών για τους οποίους δεν απαιτείται πλέον πρόσβαση.

Τα δικαιώματα πρόσβασης των χρηστών πρέπει να επανεξετάζονται σε τακτά χρονικά διαστήματα, ώστε να διασφαλιστεί ότι διατίθενται τα κατάλληλα δικαιώματα στους κατάλληλους χρήστες. Λογαριασμοί διαχείρισης των συστημάτων πρέπει να παρέχονται μόνο σε εξειδικευμένους χρήστες που απαιτούνται για την εκτέλεση εργασιών διαχείρισης του συστήματος.

Εγγραφή και διαγραφή - απενεργοποίηση χρήστη

Γραπτή αίτηση για την πρόσβαση στα δίκτυα και τα επιμέρους συστήματα του Οργανισμού πρέπει να υποβληθεί στον άμεσο προϊστάμενο κάθε υπαλλήλου και να εγκριθεί από τον Υπεύθυνο Ασφάλειας. Όλες οι αιτήσεις πρέπει να πρωτοκολλώνται και να υποβάλλονται σε επεξεργασία σύμφωνα με μια τυπική διαδικασία ώστε να διασφαλίζεται ότι διενεργούνται οι κατάλληλοι έλεγχοι ασφάλειας και δίνεται η κατάλληλη εξουσιοδότηση, πριν τη δημιουργία ενός λογαριασμού χρήστη.

Η αρχή του διαχωρισμού των αρμοδιοτήτων πρέπει να εφαρμόζεται έτσι, ώστε η δημιουργία του λογαριασμού χρήστη και η εκχώρηση των δικαιωμάτων να εκτελείται από διαφορετικούς υπαλλήλους.

Κάθε χρήστης πρέπει να έχει ένα μοναδικό όνομα χρήστη (username) που δεν θα μοιράζεται με οποιονδήποτε άλλο χρήστη και θα συνδέεται με ένα συγκεκριμένο άτομο (δεν θα συνδέεται δηλαδή με ρόλο, αλλά απευθείας με το χρήστη). Δεν πρέπει να δημιουργούνται λογαριασμοί γενικής χρήσης, δεδομένου ότι παρέχουν ανεπαρκή κατανομή ευθυνών.

Κατά την αρχική δημιουργία του λογαριασμού πρέπει να παράγεται ένας αρχικός ισχυρός κωδικός πρόσβασης και να γνωστοποιείται στο χρήστη μέσω ασφαλών μέσων. Ο χρήστης υποχρεούται να αλλάξει τον κωδικό πρόσβασης κατά την πρώτη χρήση του λογαριασμού του.

Κατά την δημιουργία ενός λογαριασμού χρήστη πρέπει να πραγματοποιηθεί η αποδοχή των πολιτικών ασφάλειας του Οργανισμού και των αρμοδιοτήτων του συγκεκριμένου ρόλου.

Η ενεργοποίηση ενός λογαριασμού δεν θα πραγματοποιείται πριν από την επίσημη αποδοχή του χρήστη (μέσω αποδοχής της πολιτικής ασφάλειας) και την επίσημη έγκριση του λογαριασμού από τον Κάτοχο του Συστήματος.

Όταν ένας εργαζόμενος αποχωρήσει υπό κανονικές συνθήκες από τον Οργανισμό, η πρόσβασή του στα πληροφοριακά συστήματα και τα δεδομένα του Οργανισμού πρέπει να ανασταλεί κατά το κλείσιμο των εργασιών της τελευταίας εργάσιμης ημέρας του. Είναι ευθύνη του άμεσα προϊσταμένου του να ζητήσει την αναστολή των δικαιωμάτων πρόσβασης.

Σε εξαιρετικές περιπτώσεις, όπου υπάρχουν βάσιμες υποψίες ότι ο εργαζόμενος μπορεί να δράσει κακόβουλα, πριν ή κατά τη λήξη της σύμβασής του, το αίτημα για την άρση της πρόσβασης μπορεί να εγκριθεί άμεσα, πριν από την ενημέρωση για αποχώρηση του χρήστη, σε συνεργασία με τη νομική υπηρεσία του Οργανισμού. Αυτή η επιλογή πρέπει να ακολουθείται ιδιαίτερα, στην περίπτωση που ο υπάλληλος προς αποχώρηση έχει δικαιώματα προνομιακής πρόσβασης π.χ. διαχειριστής τομέα.

Για τη διαγραφή ενός νέου χρήστη του Οργανισμού πρέπει να λαμβάνονται υπόψη οι εξής οδηγίες:

- Οι λογαριασμοί χρηστών που δεν χρησιμοποιούνται, πρέπει να διαγράφονται άμεσα.
- Οι λογαριασμοί των υπαλλήλων που απολύονται ή συνταξιοδοτούνται ή μεταφέρονται σε άλλη υπηρεσία, πρέπει να απενεργοποιούνται, άμεσα, τη μέρα της απόφασης απόλυσης ή το αργότερο κατά την ημέρα της απόλυσης.
- Μετά την απόλυση ενός υπαλλήλου, πρέπει να ενημερώνεται η λίστα χρηστών του Οργανισμού.
- Μετά την απόλυση ενός χρήστη, το συγκεκριμένο User ID δεν πρέπει να δίνεται σε άλλον χρήστη/υπάλληλο.

Πρόσβαση χρήστη

Πρέπει να κατανέμονται σε κάθε χρήστη, δικαιώματα και προνόμια πρόσβασης, ανάλογα με τα καθήκοντα που καλείται να εκτελέσει.

Οι ρόλοι χρηστών πρέπει να τηρούνται σύμφωνα με τις επιχειρησιακές απαιτήσεις και τυχόν μεταβολές τους πρέπει να εγκρίνονται επίσημα και να ελέγχονται μέσω Διαδικασίας Πρόσβασης Χρηστών.

Δεν πρέπει να χορηγούνται πρόσθετα δικαιώματα στους λογαριασμούς των χρηστών, εκτός του ρόλου της ομάδας στην οποία ανήκουν. Αν είναι απαραίτητη η εκχώρηση επιπλέον δικαιωμάτων, τότε θα γίνεται επίσημα μέσω της Διαδικασίας Πρόσβασης Χρηστών.

Οι Διαχειριστές Συστήματος δεν πρέπει να έχουν τη δυνατότητα εγγραφής ή τροποποίησης όλων των δεδομένων του κρίσιμων ΠΣ του Οργανισμού. Σε περίπτωση που προκύψει κάποια ανάγκη για τροποποίηση δεδομένων (π.χ. διόρθωση δεδομένων), αυτό πρέπει να πραγματοποιείται μόνο έπειτα από κατάλληλη έγκριση από τον Προϊστάμενο Διεύθυνσης Πληροφορικής και Διαχείρισης Δεδομένων του Οργανισμού.

Ταυτόχρονα, πρέπει να υπάρχει καταγραφή των χρηστών που έχουν πρόσβαση σε δεδομένα προσωπικού χαρακτήρα ειδικών κατηγοριών του Οργανισμού, καθώς και τα δικαιώματα εγγραφής/τροποποίησης/- προβολής που έχουν σε αυτά.

Αφαίρεση ή τροποποίηση δικαιωμάτων πρόσβασης

Σε περίπτωση που απαιτείται η αφαίρεση ή η τροποποίηση των δικαιωμάτων πρόσβασης ενός χρήστη λόγω αλλαγής επιχειρησιακού ρόλου ή εσωτερικής αναδιοργάνωσης (π.χ. αλλαγή στη δομή του Οργανισμού), πρέπει να ελεγχθούν τα συνολικά δικαιώματα πρόσβασης του χρήστη και να ολοκληρωθεί η διαδικασία σύμφωνα με τη Διαδικασία Πρόσβασης Χρηστών.

Σε περίπτωση που ένας χρήστης αποκτά ένα νέο ρόλο, εκτός από τους ήδη υπάρχοντες, τότε ένας νέος σύνθετος ρόλος πρέπει να αιτηθεί προς δημιουργία μέσω της Διαδικασίας Πρόσβασης Χρηστών. Πρέπει να δοθεί η δέουσα προσοχή, για τυχόν προβλήματα διαχωρισμού καθηκόντων.

Κατά την αλλαγή ενός λογαριασμού χρήστη, πρέπει να πραγματοποιηθεί η αποδοχή των πολιτικών ασφαλείας του Οργανισμού και των αρμοδιοτήτων του συγκεκριμένου ρόλου.

Μόνο οι εξουσιοδοτημένοι χρήστες (π.χ. διαχειριστές συστήματος), θα είναι σε θέση να δουν ή να ενημερώσουν τα δικαιώματα κάποιου χρήστη του Οργανισμού, έπειτα από την κατάλληλη έγκριση από τον Προϊστάμενο Διεύθυνσης Πληροφορικής του Οργανισμού.

Η αλλαγή των δικαιωμάτων πρόσβασης των χρηστών με ειδικά προνόμια (π.χ. root users, διαχειριστές εφαρμογών, λογαριασμοί διαχείρισης βάσης δεδομένων), πρέπει να ακολουθεί την ίδια διαδικασία (όπως περιγράφεται πιο πάνω).

Δεν πρέπει να επιτρέπεται στους διαχειριστές, να αλλάζουν τους δικούς τους λογαριασμούς ή τα δικαιώματα πρόσβασής τους.

Διαχείριση προνομιακών δικαιωμάτων πρόσβασης

Πρέπει να δημιουργούνται και να ελέγχονται αυστηρά, τα προνομιακά

δικαιώματα πρόσβασης, όπως αυτά που σχετίζονται με τους λογαριασμούς διαχειριστή συστημάτων ή δικτύων.

Οι διαχειριστές των συστημάτων δεν πρέπει να κάνουν καθημερινή χρήση των λογαριασμών με προνομιακή πρόσβαση και ξεχωριστοί προνομιακοί λογαριασμοί (admin accounts), πρέπει να δημιουργούνται και να χρησιμοποιούνται, μόνο όταν απαιτούνται τα επιπλέον προνόμια.

Η πρόσβαση με διαχειριστικά δικαιώματα πρέπει να διατεθεί μόνο σε άτομα των οποίων οι ρόλοι το απαιτούν και οι οποίοι έχουν λάβει επαρκή εκπαίδευση για να κατανοήσουν τις επιπτώσεις της χρήσης τέτοιου είδους λογαριασμών.

Πρέπει να πραγματοποιούνται έλεγχοι (τουλάχιστον κάθε έξι (6) μήνες) στα προφίλ των χρηστών με ειδικά προνόμια (π.χ. root, users, διαχειριστές εφαρμογών, λογαριασμοί διαχείρισης βάσης δεδομένων).

Πρέπει να υπάρχει διαχωρισμός μεταξύ των διαχειριστών συστημάτων και εφαρμογών.

Ενδεικτικοί ρόλοι:

- Ρόλος με δικαιώματα διαχείρισης σε εξυπηρετητές, σταθμούς εργασίας (Διαχειριστές Συστημάτων - System Administrators)
- Ρόλος με δικαιώματα διαχείρισης σε firewall, router (Διαχειριστές Δικτύων – Network Administ- rators)
- Ρόλος με δικαιώματα διαχείρισης στις βάσεις δεδομένων (Διαχειριστές Βάσεων Δεδομένων – Data base Administrators)
- Ρόλος με δικαιώματα διαχείρισης στις εφαρμογές του Οργανισμού (Διαχειριστές Εφαρμογών – Application Administrators)

Πρέπει να χορηγείται μόνο ο ελάχιστος αριθμός προνομίων, ο οποίος κρίνεται απαραίτητος για τη διενέργεια των λειτουργιών.

Οι χρήστες πρέπει να έχουν πρόσβαση σε συστήματα που χρησιμοποιούν μόνο μέσω του προσωπικού τους λογαριασμού και δεν πρέπει για κανένα λόγο να χρησιμοποιούν άλλους λογαριασμούς ή να αποκαλύπτουν τους λογαριασμούς τους σε άλλους.

Οι λογαριασμοί χρηστών δεν πρέπει να αποθηκεύονται σε χώρους που είναι προσιτοί από άλλους (π.χ. σε ένα χαρτί κάτω από το πληκτρολόγιο).

Ο χρήστης είναι υπεύθυνος για τυχόν ενέργειες που έγιναν με τη χρήση του λογαριασμού του.

Πρέπει να αποφεύγεται κατά το δυνατόν η χρήση των λογαριασμών με προνομιακή πρόσβαση σε αυτοματοποιημένες ρουτίνες. Όπου αυτό είναι αναπόφευκτο τότε ο κωδικός που χρησιμοποιείται πρέπει να προστατεύεται και να αλλάζει σε τακτά χρονικά διαστήματα (τουλάχιστον μία φορά το εξάμηνο).

Πρέπει να τηρείται μια ενημερωμένη λίστα με τα συνολικά δικαιώματα των χρηστών του Οργανισμού. Υπεύθυνος για την συντήρηση της συγκεκριμένης λίστας είναι ο Υπεύθυνος Ασφάλειας του Οργανισμού.

Αυθεντικοποίηση χρήστη για εξωτερικές συνδέσεις

Σύμφωνα με την Πολιτική Ασφάλειας Δικτύων, η χρήση εξοπλισμού ο οποίος δεν ανήκει στον Οργανισμό, μπορεί να θέσει σε σοβαρό κίνδυνο την ασφάλεια του δικτύου του.

Πρέπει να ληφθεί ειδική έγκριση, από τον Υπεύθυνο Ασφάλειας πριν από τη σύνδεση οποιουδήποτε εξοπλισμού στο δίκτυο του Οργανισμού.

Όπου απαιτείται απομακρυσμένη πρόσβαση στο δίκτυο του Οργανισμού μέσω VPN, πρέπει πρώτα να εγκριθεί από τον Υπεύθυνο Ασφάλειας, τόσο το απαιτούμενο λογισμικό, όσο και η ανάγκη απομακρυσμένης πρόσβασης.

Πρόσβαση προμηθευτών

Δεν πρέπει να δίνονται λεπτομέρειες στους συνεργάτες ή τους προμηθευτές του Οργανισμού για τον τρόπο πρόσβασης στο δίκτυο και τα συστήματά του, χωρίς την γραπτή άδεια από τον Υπεύθυνο Ασφάλειας.

Οποιεσδήποτε αλλαγές στις συνδέσεις ενός προμηθευτή (π.χ. κατά τη λήξη της σύμβασης) πρέπει να αποστέλλονται αμέσως στον Υπεύθυνο Ασφάλειας έτσι ώστε η πρόσβαση να ενημερωθεί ή να τερματιστεί.

Όλα τα δικαιώματα και οι μέθοδοι πρόσβασης πρέπει να ελέγχονται από τον Υπεύθυνο Πληροφορικής και να επανεξετάζονται από τον Υπεύθυνο Ασφάλειας.

Οι συνεργάτες ή οι προμηθευτές του Οργανισμού, πρέπει να επικοινωνήσουν με τον Υπεύθυνο Ασφάλειας, σε κάθε περίπτωση, ώστε να ζητήσουν άδεια σύνδεσης στο δίκτυο του Οργανισμού και πρέπει να τηρηθεί ένα αρχείο καταγραφής αυτών των δραστηριοτήτων.

Τα λογισμικά απομακρυσμένης πρόσβασης που επιτρέπεται να χρησιμοποιούνται για λόγους εργασιών πρέπει να είναι εγκεκριμένα από τον Υπεύθυνο Ασφάλειας. Για την ενεργοποίηση απομακρυσμένης πρόσβασης πρέπει να δίνεται η

κατάλληλη έγκριση του Υπεύθυνου Ασφάλειας, βάσει της Διαδικασίας Πρόσβασης Χρηστών (βάσει της Φόρμας Αίτησης Υπηρεσίας). Αντίστοιχα, πρέπει να απενεργοποιείται η σύνδεση όταν δεν είναι σε χρήση και να τηρείται ιστορικό στο Αρχείο Χρηστών Απομακρυσμένης Πρόσβασης.

Ανασκόπηση δικαιωμάτων πρόσβασης

Πρέπει να επανεξετάζονται τα δικαιώματα πρόσβασης των χρηστών σε τακτά χρονικά διαστήματα (τουλάχιστον μια (1) φορά κάθε ένα (1) χρόνο). Η ανασκόπηση αυτή έχει ως στόχο να εντοπιστούν:

Άτομα που δεν πρέπει να έχουν πρόσβαση στα ΠΣ του Οργανισμού (π.χ. άτομα που έχουν απολυθεί/παραιτηθεί ή έχουν αλλάξει διεύθυνση).

Οι λογαριασμοί χρηστών με μεγαλύτερη πρόσβαση από εκείνη που απαιτεί ο ρόλος.

Οι λογαριασμοί χρηστών που δεν παρέχουν επαρκή προσδιορισμό π.χ. γενικοί ή κοινοί-διαμοιραζόμενοι λογαριασμοί

Οποιαδήποτε άλλα θέματα που δεν συμμορφώνονται με αυτήν την πολιτική

Ο έλεγχος των δικαιωμάτων των διαχειριστών πρέπει να πραγματοποιείται σε μικρότερα χρονικά διαστήματα (μια φορά κάθε έξι (6) μήνες) σύμφωνα με τη Διαδικασία Πρόσβασης Χρηστών.

Αν κατά την διάρκεια ελέγχου των δικαιωμάτων πρόσβασης παρατηρηθούν διαφορές μεταξύ των πραγματικών και των εγκεκριμένων δικαιωμάτων, τότε πρέπει να ξεκινάει η Διαδικασία Διαχείρισης Περιστατικών, να ενημερώνεται άμεσα ο Κάτοχος του Συστήματος και να εφαρμόζεται η κατάλληλη διορθωτική ενέργεια (π.χ. διαγράφονται άμεσα τα επιπλέον δικαιώματα, αφού έχουν συλλεχθεί τα απαραίτητα ψηφιακά πειστήρια).

Η ανασκόπηση αυτή θα πραγματοποιείται σύμφωνα με την επίσημη Διαδικασία Πρόσβασης Χρηστών και τυχόν διορθωτικές ενέργειες θα εντοπίζονται, θα καταγράφονται και θα υλοποιούνται.

Αυθεντικοποίηση χρήστη και πολιτική κωδικού πρόσβασης

Στην Πολιτική Κωδικών Πρόσβασης καταγράφονται οι οδηγίες και οι γενικές αρχές για την δημιουργία και ορθή χρήση των κωδικών πρόσβασης των χρηστών του Οργανισμού.

Αρμοδιότητες χρηστών

Ο ρόλος που παίζει ο κάθε χρήστης είναι ζωτικής σημασίας για την προστασία των στοιχείων πρόσβασης των λογαριασμών του, καθώς και για την διασφάλιση ότι ο λογαριασμός του, δεν χρησιμοποιείται για να βλάψει τον Οργανισμό.

Προκειμένου να μεγιστοποιηθεί η ασφάλεια των πληροφοριών, κάθε χρήστης:

- Πρέπει να χρησιμοποιεί έναν ισχυρό κωδικό πρόσβασης, δηλαδή έναν κωδικό που είναι συμβατός με τους κανόνες που ορίζονται στην Πολιτική Κωδικών Πρόσβασης.
- Να μην αποκαλύπτει ποτέ σε κανέναν τον κωδικό πρόσβασης ή να επιτρέπει σε κάποιον άλλο χρήστη να χρησιμοποιήσει τον λογαριασμό του.
- Δεν πρέπει να καταγράψει τον κωδικό πρόσβασης εγγράφως ή με ηλεκτρονικά μέσα, π.χ. σε ένα έγγραφο ή σε ένα e-mail.
- Πρέπει να αποφεύγει τη χρήση του ίδιου κωδικού πρόσβασης για άλλους λογαριασμούς χρηστών, είτε προσωπικούς είτε σχετικούς με τον Οργανισμό.
- Πρέπει να βεβαιώνεται ότι οποιοδήποτε μηχάνημα (PC, workstation), σε περίπτωση απουσίας του, είναι κλειδωμένο ή έχει αποσυνδεθεί.
- Δεν πρέπει να αφήνει τίποτα στην οθόνη, που μπορεί να περιέχει πληροφορίες πρόσβασης, όπως ονόματα χρήστη και κωδικούς πρόσβασης.
- Πρέπει να αποσυνδέεται από τον σταθμό εργασίας του (να ενεργοποιείται το screen saver και να απαιτείται συνθηματικό για την πρόσβαση), σε περίπτωση απουσίας τους από την θέση εργασίας του. Η μέγιστη περίοδος για την ενεργοποίηση του screen saver πρέπει να είναι δεκαπέντε (15) λεπτά.
- Πρέπει να ενημερώνει τον Υπεύθυνο Πληροφορικής για τυχόν αλλαγές στις απαιτήσεις του ρόλου και της πρόσβασής του.
- Η μη συμμόρφωση με τις απαιτήσεις αυτές μπορεί να οδηγήσει στην λήψη πειθαρχικών μέτρων κατά του εν λόγω ατόμου.

Πρόσβαση σε συστήματα και εφαρμογές

Η πρόσβαση σε όλα τα συστήματα του Οργανισμού πρέπει να ελέγχεται για να περιοριστεί η πρόσβαση σε εξουσιοδοτημένους χρήστες, μεταξύ άλλων με ασφαλείς διαδικασίες time-out log-on και session time- out, όπως περιγράφεται στη συνέχεια.

Ταυτόχρονα, πρέπει να τεθεί σε ισχύ ένα ολοκληρωμένο μοντέλο ασφαλείας το

οποίο περιλαμβάνει υποστήριξη για τα ακόλουθα:

- Δημιουργία ατομικών λογαριασμών χρηστών.
- Αποσαφήνιση ρόλων και ομάδων. Πρέπει να υπάρχουν προκαθορισμένοι ρόλοι, στους οποίους θα δίνονται συγκεκριμένα δικαιώματα ανάλογα με το είδος πρόσβασης που απαιτείται από τις υπηρεσιακές ανάγκες της θέσης κάθε υπαλλήλου, με στόχο την ορθότερη διαχείριση πρόσβασης (π.χ. παρακολούθηση δικαιωμάτων σε περίπτωση παραίτησης χρήστη ή μετάθεσής του σε άλλη διεύθυνση/υπηρεσία). Προτείνεται ο διαχωρισμός των δικαιωμάτων να γίνεται ανάλογα με την ιεραρχία κάθε διεύθυνσης και των υπηρεσιακών αναγκών της. Όταν για λόγους επιχειρησιακούς ή έλλειψης ανθρώπινου δυναμικού αυτό δεν είναι εφικτό και υπάρχει η ανάγκη για ανάθεση περισσότερων ρόλων σε κάποιον υπάλληλο του Οργανισμού, πρέπει να υπάρχει έγγραφη τεκμηρίωση της εξαίρεσης από τον προϊστάμενο του εκάστοτε τμήματος και έγκριση από τον Υπεύθυνο Ασφάλειας του Οργανισμού.
- Χορήγηση δικαιωμάτων πρόσβασης σε αντικείμενα (π.χ. αρχεία, προγράμματα, μενού) διαφόρων τύπων (π.χ. ανάγνωση, εγγραφή, διαγραφή, εκτέλεση) από υποκείμενα (λογαριασμοί χρηστών και ομάδων).
- Διαχείριση λογαριασμών χρηστών, συμπεριλαμβανομένης της ικανότητας να απενεργοποιηθούν και να διαγραφούν λογαριασμοί.
- Διαχείριση κωδικών πρόσβασης, με:
  - Δυνατότητα να αλλάξει ο χρήστης τον κωδικό πρόσβασης.
  - Δυνατότητα ελέγχων για τον αποδεκτό κωδικό πρόσβασης.
  - Δυνατότητα λήξης του κωδικού πρόσβασης.
  - Δυνατότητα hashed/κρυπτογραφημένης αποθήκευσης και διαβίβασης του κωδικού πρόσβασης.

Διαδικασία ασφαλούς σύνδεσης

Η διαδικασία σύνδεσης στα συστήματα του Οργανισμού πρέπει να ακολουθεί τους εξής κανόνες:

- Η οθόνη δεν πρέπει να εμφανίζει κανένα αναγνωριστικό του συστήματος ή της εφαρμογής μέχρι να ολοκληρωθεί με επιτυχία η σύνδεση.
- Στην οθόνη σύνδεσης πρέπει να περιλαμβάνεται μια τυπική ανακοίνωση για να ενημερώνει τους χρήστες, ότι ο πόρος αυτός είναι μόνο για εταιρική χρήση.

- Πρέπει να εμφανίζονται μόνο περιορισμένα βοηθητικά μηνύματα σχετικά με τη διαδικασία, έτσι ώστε να μην παρέχει πληροφορίες και να βοηθά τους μη εξουσιοδοτημένους χρήστες.
- Να επιτρέπεται ένας συγκεκριμένος αριθμός ανεπιτυχών προσπαθειών πρόσβασης (τρεις (3) φορές).
- Το σύστημα επικυρώνει τα στοιχεία σύνδεσης μόνο μετά την ολοκλήρωση της εισόδου και στη συνέχεια, εάν υπάρχει κάποιο λάθος, το σύστημα απαιτεί από το χρήστη να προσπαθήσει ξανά. Συγκεκριμένα, τα μηνύματα σφάλματος που εμφανίζονται πρέπει να είναι γενικά όπως π.χ. ανεπιτυχής πρόσβαση, δοκιμάστε ξανά.
- Οι πληροφορίες που καταχωρούνται από τον χρήστη κατά τη διάρκεια μιας προσπάθειας σύνδεσης, πρέπει να επικυρώνονται μόνον ως ένα πλήρες σύνολο. Εάν παρουσιαστεί σφάλμα, το σύστημα δεν πρέπει να δώσει καμία ένδειξη για το ποιο μέρος των πληροφοριών είναι σωστό ή λανθασμένο (το User ID ή ο κωδικός πρόσβασης κτλ.).
- Παροχή πληροφοριών σχετικά με τον αριθμό των αποτυχημένων προσπαθειών σύνδεσης, καθώς και της τελευταίας επιτυχημένης εισόδου στο σύστημα.
  - Περιορισμοί βάσει ημερομηνίας και ώρας εισόδου.
  - Περιορισμοί βάσει συσκευών και τοποθεσίας.

Λήξη συνεδρίας (session time-out)

Όλοι οι χρήστες του Οργανισμού απαιτείται να αποσυνδέονται από τις ενεργές συνεδρίες όταν ολοκληρώσουν την εργασίας τους.

Μετά από ένα ρυθμιζόμενο χρονικό διάστημα αδράνειας του χρήστη, η προστασία οθόνης με κωδικό πρόσβασης ενεργοποιείται. Το μέγιστο χρονικό διάστημα για την ενεργοποίηση της προφύλαξης οθόνης πρέπει να είναι δεκαπέντε (15) λεπτά.

Μετά από ένα ρυθμιζόμενο χρονικό διάστημα αδράνειας του χρήστη σε συνεδρία (session) στα ΠΣ του Οργανισμού ο χρήστης πρέπει να πιστοποιείται ξανά. Η μέγιστη περίοδος για την απενεργοποίηση της συνεδρίας (session time-out) πρέπει να είναι τριάντα (30) λεπτά.

Χρήση βοηθητικών προγραμμάτων

Η πρόσβαση σε βοηθητικά προγράμματα, τα οποία ενδέχεται να παρέχουν μια μέθοδο παράκαμψης της ασφάλειας του συστήματος (π.χ. εργαλεία διαχείρισης

δεδομένων, εργαλεία διαχείρισης registry, εργαλεία διαχείρισης δίσκου, εργαλεία restore λειτουργικού κλπ.), πρέπει να ελέγχεται αυστηρά και η χρήση τους να περιορίζεται σε συγκεκριμένα άτομα και για ειδικές συνθήκες. Πρόκειται για εφαρμογές του λειτουργικού συστήματος οι οποίες πρέπει να περιορίζονται μόνο σε διαχειριστές και μόνο έπειτα από σχετική έγκριση.

Διαχείριση των κωδικών

Όλοι οι κωδικοί που χρησιμοποιούνται για οποιαδήποτε πρόσβαση αποτελούνται από τουλάχιστον 8 χαρακτήρες οι οποίοι πρέπει υποχρεωτικά να είναι συνδυασμός γραμμάτων, αριθμών και συμβόλων. Οι κωδικοί είναι προσωπικοί δεν πρέπει να γνωστοποιούνται ή να κοινοποιούνται σε καμία περίπτωση.

Ο Προϊστάμενος της Διεύθυνσης Πληροφορικής του Οργανισμού ενημερώνει τον χρήστη ότι ο κωδικός είναι αυστηρά προσωπικός. Για τη διασφάλιση του αυστηρά προσωπικού κωδικού ο IT φροντίζει να είναι ενεργοποιημένη η επιλογή για αλλαγή κωδικού πριν από την πρώτη είσοδο. Ο κάθε χρήστης φέρει την ευθύνη για την διαφύλαξη των προσωπικών του κωδικών ασφαλείας. Σε περίπτωση απώλειας κάποιου κωδικού ή/και σε περίπτωση υποψίας υποκλοπής κωδικού, ο χρήστης ενημερώνει άμεσα τον Προϊστάμενο Διεύθυνσης Πληροφορικής ή τον αρμόδιο του σχετικού πληροφοριακού συστήματος ο οποίος αρχικοποιεί τη διαδικασία επιλογής κωδικού, ώστε να μπορεί ο χρήστης να ορίσει νέο κωδικό

Ο Προϊστάμενος Διεύθυνσης Πληροφορικής πρέπει να ενημερώνει τους χρήστες για τις οδηγίες που θα πρέπει να ακολουθούν έτσι ώστε να αποτρέψουν την υποκλοπή των κωδικών τους. Οι οδηγίες αυτές είναι :

- Να μη χρησιμοποιούν εύκολα προβλέψιμους κωδικούς (π.χ. ονοματεπώνυμα, ημερομηνία γεννήσεως κ.λπ.)
- Να διαμορφώνουν τους κωδικούς ώστε να περιέχουν συνδυασμό από γράμματα, σύμβολα και αριθμούς.
- Να απομνημονεύουν τους κωδικούς και να μην τους καταγράφουν σε μέρη που μπορεί να υποκλαπούν (ατζέντες, σημειωματάρια κ.λπ.)
- Να αλλάζουν κατ’ ελάχιστον κάθε 6 μήνες 180 ημέρες.
- Να μην επαναχρησιμοποιούν τον κωδικό που έχουν χρησιμοποιήσει τις 3 τελευταίες φορές.

- Στην οθόνη σύνδεσης πρέπει να περιλαμβάνεται μια τυπική ανακοίνωση για να ενημερώνει τους χρήστες, ότι ο πόρος αυτός είναι μόνο για εταιρική χρήση.
- Πρέπει να εμφανίζονται μόνο περιορισμένα βοηθητικά μηνύματα σχετικά με τη διαδικασία, έτσι ώστε να μην παρέχει πληροφορίες και να βοηθά τους μη εξουσιοδοτημένους χρήστες.

Παρακολούθηση και καταγραφή ενεργειών του ελέγχου πρόσβασης

Η καταγραφή των ενεργειών για τυχόν συμβάντα ασφαλείας και παραβίασης δεδομένων πρέπει να ενεργοποιηθεί για όλα τα συστήματα του Οργανισμού.

ΠΑΡΑΡΤΗΜΑ Α. ΕΝΤΥΠΟ ΔΙΑΧΕΙΡΙΣΗΣ ΠΡΟΣΒΑΣΕΩΝ

Α/Α	ΟΝΟΜΑΤΕΠΩΝΥΜΟ	ΤΜΗΜΑ / ΘΕΣΗ	ΤΗΛΕΦΩΝΟ	ΧΩΡΟΣ

Ο Υπεύθυνος Α.Σ.Π.Ε. **Διοίκηση**

(Όνομα – Υπογραφή) **(Όνομα – Υπογραφή)**

ΠΑΡΑΡΤΗΜΑ Β. ΑΤΟΜΙΚΗ ΚΑΡΤΕΛΑ ΠΡΟΣΒΑΣΕΩΝ

ΟΝΟΜΑΤΕΠΩΝΥΜΟ	ΤΜΗΜΑ / ΘΕΣΗ	ΗΜΕΡΟΜΗΝΙΑ ΕΝΑΡΞΗΣ ΕΡΓΑΣΙΩΝ ΣΤΗ ΘΕΣΗ ΑΥΤΗ	ΗΜΕΡΟΜΗΝΙΑ ΛΗΞΗΣ ΕΡΓΑΣΙΩΝ ΣΤΗ ΘΕΣΗ ΑΥΤΗ

ΜΕΤΑΒΑΛΛΕΙ ΤΗΝ ΠΡΟΗΓΟΥΜΕΝΗ ΚΑΡΤΕΛΑ No	

Α/Α	ΕΙΔΟΣ / ΠΕΡΙΓΡΑΦΗ (ΚΛΕΙΔΙΑ, ΚΩΔΙΚΟΣ ΣΥΝΑΓΕΡΜΟΥ, ΚΙΝΗΤΟ, LAPTOP κ.α.)	ΠΑΡΑΛΑΒΗ (ΗΜΕΡΟΜΗΝΙΑ & ΥΠΟΓΡΑΦΗ ΕΡΓΑΖΟΜΕΝΟΥ)	ΠΑΡΑΔΟΣΗ (ΗΜΕΡΟΜΗΝΙΑ & ΥΠΟΓΡΑΦΗ ΑΡΜΟΔΙΟΥ)

Κωδικός Διαδικασίας	1.0	**Έκδοση**	1.0	**Σχετικά Πρότυπα**	*Ν. 4961/2022, ISO/IEC 27001:2013, Γενικός Κανονισμός, Προστασίας Δεδομένων, ENISA (Consumerization of IT), Οδηγίες της ΑΠΔΠΧ*
Σχετικές Απαιτήσεις	*Συμμόρφωση του Δήμου Περάματος με τον Ν. 4961/2022*				

ΠΡΟΣΒΑΣΕΙΣ	
ΧΩΡΟΙ	
ΣΥΣΤΗΜΑΤΑ / ΕΦΑΡΜΟΓΕΣ	

Ο Υπεύθυνος Α.Σ.Π.Ε. **Διοίκηση**

(Όνομα – Υπογραφή) **(Όνομα – Υπογραφή)**

6.4 Πολιτική Αντιγράφων Ασφαλείας

Εισαγωγή

Κάθε χρήστης των Πληροφοριακών Συστημάτων (Π.Σ.) του Δήμου Περάματος (εφεξής «Οργανισμός» ή Φορέας) θα πρέπει να συνεισφέρει στην ασφάλεια πληροφοριών και των υποδομών με την ορθή χρήση των πόρων τους και να τηρεί θεμελιώδεις κανόνες ορθής χρήσης και δεοντολογίας.

Σκοπός

Ο στόχος της συγκεκριμένης πολιτικής είναι να καθορίσει τον τρόπο με τον οποίο πρέπει να λαμβάνονται τα αντίγραφα ασφαλείας των πληροφοριακών συστημάτων του Οργανισμού, συμπεριλαμβανομένων:

- της πληροφορίας που αποθηκεύεται
- της συχνότητας των αντιγράφων ασφαλείας
- του απαιτούμενου χρόνου για την επαναφορά των αντιγράφων ασφαλείας
- της περιόδου τήρησης/διαγραφής των αντιγράφων ασφαλείας
- των τύπων αντιγράφων ασφαλείας
- του συγχρονισμού των αντιγράφων ασφαλείας
- της τοποθεσίας που αποθηκεύονται τα αντίγραφα ασφαλείας
- του τρόπου με τον οποίο χρησιμοποιούνται οι δίσκοι αντιγράφων ασφαλείας.

Έχοντας ως στόχο την αντιμετώπιση των δυσμενέστερων σεναρίων, η δημιουργία και εφαρμογή της Πολιτικής Αντιγράφων Ασφαλείας (εφεξής: Πολιτική) αποτελεί μία από τις προϋποθέσεις συμμόρφωσης με την κείμενη νομοθεσία περί ασφάλειας πληροφοριών και προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΔΠΧ) συγκεκριμένα:

- *τις διατάξεις του Ν. 4961/2022 (ΦΕΚ Α' 146/27.07.2022)*[11]
- *τις διατάξεις του Κανονισμού (ΕΕ) 2016/679 (GDPR/ΓΚΠΔ)* [12],
- *τις διατάξεις του Ν. 4624/2019 (ΦΕΚ Α' 137/29.08.2019)* [13]

Πεδίο εφαρμογής

Η συγκεκριμένη πολιτική πρέπει να εφαρμόζεται σε όλα τα συστήματα, διαδικασίες και χρήστες του Οργανισμού, συμπεριλαμβανομένων Διευθυντών, Προϊσταμένων, υπαλλήλων, προμηθευτών και λοιπών τρίτων που έχουν πρόσβαση στα ΠΣ του Οργανισμού.

Πολιτική

Αντίγραφα ασφάλειας (backup files) πρέπει να λαμβάνονται από όλες τις πληροφορίες που βρίσκονται αποθηκευμένες στα ΠΣ του Οργανισμού, ιδιαίτερα για αυτές που χαρακτηρίζονται ως κρίσιμες πληροφορίες από πλευράς εμπιστευτικότητας, ακεραιότητας ή/και διαθεσιμότητας.

Αντίγραφα ασφαλείας πρέπει να λαμβάνονται και για τα αρχεία διαμόρφωσης των κρίσιμων συστημάτων.

Αντίγραφα ασφαλείας πρέπει να τηρούνται τόσο στο Computer Room του Οργανισμού ή σε άλλο προστατευμένο χώρο.

Επιπλέον αντίγραφα ασφάλειας πρέπει να τηρούνται σε απομακρυσμένο γεωγραφικά σημείο σε περίπτωση που τα κύρια αντίγραφα ασφαλείας καταστούν μη διαθέσιμα.

---

[11] Νόμος υπ' αριθμ. 4961/2022 Τεύχος Α' 146/27.07.2022: Αναδυόμενες τεχνολογίες πληροφορικής και επικοινωνιών, ενίσχυση της ψηφιακής διακυβέρνησης και άλλες διατάξεις.

[12] Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων).

[13] Νόμος υπ' αριθμ. 4624 Τεύχος Α' 137/29.08.2019, Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 και άλλες διατάξεις.

Ο χρόνος τήρησης των διαφόρων αντιγράφων ασφαλείας καθορίζεται ανάλογα με τις ανάγκες κάθε πόρου, από τον Ιδιοκτήτη του Πληροφοριακού Πόρου, με την έγκριση του Υπευθύνου Ασφάλειας.

Πρέπει να προβλεφθεί και να αναπτυχθεί κεντρικός μηχανισμός για την αυτοματοποιημένη λήψη όλων των απαραίτητων αντιγράφων ασφαλείας από τα κεντρικά συστήματα, τις πληροφοριακές και δικτυακές υποδομές (συστήματα διαχείρισης δικτύου, συστήματα ασφάλειας κλπ.), τους file servers και τις βάσεις δεδομένων.

Τα αντίγραφα ασφάλειας πρέπει να αντιγράφονται πριν χρησιμοποιηθούν για ανάκτηση πληροφοριών. Αυτή η πολιτική στοχεύει να προστατεύσει τα αντίγραφα ασφαλείας από ενδεχόμενη ζημιά κατά τη διάρκεια ανάκτησης των πληροφοριών που περιέχουν.

Πρέπει να τηρείται και να ενημερώνεται διαρκώς το αρχείο καταγραφής των διαθέσιμων αντιγράφων ασφαλείας και των μέσων αποθήκευσης αντιγράφων ασφαλείας (και να αντιγράφονται σε απομακρυσμένη τοποθεσία σε περίπτωση απώλειας των αρχικών δεδομένων).

Τα αντίγραφα ασφάλειας πρέπει να τηρούνται για πέντε (5) χρόνια (ή διαφορετικά αν καθορίζεται από τη νομοθεσία).

Ο Υπεύθυνος της διαδικασίας λήψης αντιγράφων ασφαλείας πρέπει να ελέγχει κάθε πρωί την κατάσταση των αντιγράφων ασφαλείας και να αναφέρει τυχόν αστοχίες στον Υπεύθυνο Ασφάλειας.

Μέθοδος λήψης αντιγράφων ασφαλείας και χρονοπρογραμματισμός

Το προτεινόμενο μοντέλο αποθήκευσης δεδομένων εντός του Οργανισμού προϋποθέτει:

- τη λήψη ενός πλήρους (full) μηνιαίου αντιγράφου ασφαλείας (grandfather) το οποίο αποθηκεύεται εντός της κτιριακής εγκατάστασης του Οργανισμού, σε ασφαλές χρηματοκιβώτιο και σε χώρο εκτός Computer Room. Η λήψη του μηνιαίου backup μπορεί να γίνεται την τελευταία Παρασκευή του μήνα.

Επίσης, τον τελευταίο μήνα του έτους θα πραγματοποιείται και η λήψη του ετήσιου backup.

- τη λήψη ενός πλήρους (full) εβδομαδιαίου αντιγράφου (father) το οποίο αποθηκεύεται εντός της κτιριακής εγκατάστασης του Οργανισμού, σε ασφαλές χρηματοκιβώτιο και σε διαφορετικό χώρο από το Computer Room. Η λήψη του εβδομαδιαίου backup μπορεί να γίνεται κάθε Παρασκευή, εκτός από την τελευταία Παρασκευή του μήνα οπότε θα γίνεται το μηνιαίο Backup.
- τη λήψη ημερησίων αυξητικών (incremental) αντιγράφων (son) τα οποία και αποθηκεύονται εντός του Οργανισμού. Σημειώνεται ότι τις Παρασκευές δεν θα λαμβάνεται το ημερήσιο backup, αλλά στη θέση του θα γίνεται η λήψη του εβδομαδιαίου ή του μηνιαίου backup.

Πίνακας 3 – Χρόνος λήψης αντιγράφων ασφαλείας

ΕΒΔΟΜΑΔΑ ΤΟΥ ΜΗΝΑ	ΔΕΥΤΕΡΑ	ΤΡΙΤΗ	ΤΕΤΑΡΤΗ	ΠΕΜΠΤΗ	ΠΑΡΑΣΚΕΥΗ	ΣΑΒΒΑΤΟ	ΚΥΡΙΑΚΗ
1η	ΗΜΕΡΗΣΙΟ	ΗΜΕΡΗΣΙΟ	ΗΜΕΡΗΣΙΟ	ΗΜΕΡΗΣΙΟ	ΕΒΔΟΜΑΔΙΑΙΟ	ΗΜΕΡΗΣΙΟ	ΗΜΕΡΗΣΙΟ
2η	ΗΜΕΡΗΣΙΟ	ΗΜΕΡΗΣΙΟ	ΗΜΕΡΗΣΙΟ	ΗΜΕΡΗΣΙΟ	ΕΒΔΟΜΑΔΙΑΙΟ	ΗΜΕΡΗΣΙΟ	ΗΜΕΡΗΣΙΟ
3η	ΗΜΕΡΗΣΙΟ	ΗΜΕΡΗΣΙΟ	ΗΜΕΡΗΣΙΟ	ΗΜΕΡΗΣΙΟ	ΕΒΔΟΜΑΔΙΑΙΟ	ΗΜΕΡΗΣΙΟ	ΗΜΕΡΗΣΙΟ
4η	ΗΜΕΡΗΣΙΟ	ΗΜΕΡΗΣΙΟ	ΗΜΕΡΗΣΙΟ	ΗΜΕΡΗΣΙΟ	ΜΗΝΙΑΙΟ	ΗΜΕΡΗΣΙΟ	ΗΜΕΡΗΣΙΟ

Επιπλέον οδηγίες:

- Να γίνεται λήψη αντιγράφων ασφαλείας των βάσεων δεδομένων σύμφωνα με το παραπάνω σχέδιο.
- Να γίνεται η λήψη των αντιγράφων ασφαλείας του Συστήματος Αρχείων (file system) σύμφωνα με το παραπάνω πλάνο με την εξαίρεση ότι δεν θα

λαμβάνονται ημερήσια αντίγραφα ασφαλείας.

- Να γίνεται λήψη αντιγράφων ασφαλείας των λειτουργικών συστημάτων των ΠΣ του Οργανισμού (OS backup) πριν την εγκατάσταση νέων ενημερώσεων και μετά από κάθε ενημέρωσή τους (update).

Περίοδος διατήρησης αντιγράφων ασφαλείας

Η προτεινόμενη περίοδος διατήρησης των αντιγράφων ασφαλείας αποτυπώνεται στον παρακάτω πίνακα:

Πίνακας 4 – Περίοδος διατήρησης αντιγράφων ασφαλείας

ΠΕΡΙΟΔΙΚΟΤΗΤΑ ΑΝΤΙΓΡΑΦΟΥ ΑΣΦΑΛΕΙΑΣ	ΤΥΠΟΣ ΑΝΤΙΓΡΑΦΟΥ ΑΣΦΑΛΕΙΑΣ	ΠΕΡΙΟΔΟΣ ΔΙΑΤΗΡΗΣΗΣ
Καθημερινά	Incremental	2 εβδομάδες
Εβδομαδιαία	Full	3 μήνες
Μηνιαία	Full	12 μήνες
Ετήσια	Full	5 έτη

Αποθήκευση δεδομένων εκτός του Οργανισμού

Η φύλαξη των ηλεκτρονικών αντιγράφων ασφαλείας, πρέπει να γίνεται και εκτός του κεντρικού κτιρίου του Οργανισμού, σε περίπτωση που η καταστροφή δεν αφήνει περιθώρια ανάκτησης της σημαντικής πληροφορίας από κάποιον χώρο του Οργανισμού (π.χ. ολική καταστροφή του κεντρικού κτιρίου).

Συγκεκριμένα, όλα τα αντίγραφα των ΠΣ του Οργανισμού (δεδομένα, αρχεία παραμετροποίησης, πηγαίος κώδικας κλπ.) πρέπει να αποθηκεύονται σε ειδικό χώρο φύλαξης αντιγράφων ασφαλείας εκτός του Οργανισμού. Προτείνεται να αποφασιστεί έπειτα από σχετική Απόφαση της Διοίκησης του Οργανισμού.

Οι έλεγχοι φυσικής πρόσβασης που εφαρμόζονται σε τοποθεσίες αποθήκευσης αντιγράφων ασφαλείας εκτός του Οργανισμού πρέπει να πληρούν ή να υπερβαίνουν τους ελέγχους φυσικής πρόσβασης των συστημάτων της κύριας υποδομής του Οργανισμού. Επιπλέον, τα μέσα αποθήκευσης αντιγράφων ασφαλείας πρέπει να προστατεύονται σύμφωνα με το επίπεδο διαβάθμισης των πληροφοριών των ΠΣ του Οργανισμού.

Αποτυχία δημιουργίας αντιγράφων ασφαλείας

Πρέπει να πραγματοποιούνται έλεγχοι για να εντοπιστούν τυχόν αποτυχίες στη διαδικασία δημιουργίας αντιγράφων ασφαλείας και να ενημερωθεί κατάλληλα το σχετικό προσωπικό. Επιπλέον, πρέπει να καταγραφούν όλες οι σχετικές πληροφορίες, σχετικά με το πιθανό σφάλμα και την ημερομηνία.

Σε περίπτωση ανεπιτυχούς δημιουργίας αντιγράφων ασφαλείας, ο Υπεύθυνος της διαδικασίας λήψης αντιγράφων ασφαλείας πρέπει να:

- Σημειώσει τυχόν μηνύματα/πληροφορίες που εμφανίζονται στην οθόνη του εξυπηρετητή.
- Ελέγξει τη ρύθμιση αντιγράφων ασφαλείας, τα μέσα αποθήκευσης αντιγράφων ασφαλείας και το υλικό.
- Επικοινωνήσει με τον κατάλληλο προμηθευτή για να αναφέρει την αποτυχία, εάν υπάρχει αποτυχία υλικού.
- Καταγράψει την αποτυχία σε αρχείο καταγραφής αντιγράφων ασφαλείας και τα τυχόν διορθωτικά μέτρα που λήφθηκαν.
- Εκτελέσει εάν είναι απαραίτητο μια χειροκίνητη δημιουργία αντιγράφων ασφαλείας, εάν η δημιουργία αντιγράφων ασφαλείας αποτυγχάνει επανειλημμένα. Επειδή η συγκεκριμένη διαδικασία απαιτεί χρόνο πρέπει να εκτελείται, όταν όλοι οι χρήστες έχουν αποσυνδεθεί.
- Να καταγράψει όλες τις πληροφορίες στην κατάλληλη Φόρμα Αναφοράς Περιστατικών/ Αδυναμιών Ασφάλειας και να ενημερώσει τον Υπεύθυνο Ασφάλειας (σύμφωνα με τη Διαδικασία Διαχείρισης Περιστατικών)

Δοκιμή επαναφοράς αντιγράφων ασφαλείας

Τα αντίγραφα ασφαλείας πρέπει να δοκιμάζονται ανά τακτά χρονικά διαστήματα (τουλάχιστον μια (1) φορά τον χρόνο), ώστε να διασφαλίζεται η ακεραιότητα και η πληρότητα των περιεχομένων τους.

Μερική δοκιμή τους (π.χ. ανάκαμψη των δεδομένων για ένα συγκεκριμένο υποσύστημα των ΠΣ του Οργανισμού) πρέπει να πραγματοποιείται τουλάχιστον μία φορά κάθε έξι (6) μήνες.

Έπειτα από κάθε δοκιμή των αντιγράφων ασφαλείας πρέπει να διασφαλίζονται τα εξής:

- Η ολική επαναφορά των συστημάτων των ΠΣ του Οργανισμού είναι εφικτή.
- Η διαδικασία επαναφοράς καλύπτει τους στόχους επαναφοράς (Recovery Time Objectives, RTO).
- Τα δεδομένα μπορούν να εγκατασταθούν με επιτυχία σε εναλλακτικά συστήματα (άλλο υλικό ή/και άλλο λογισμικό).
- Το προσωπικό το οποίο συμμετέχει στις διαδικασίες λήψης αντιγράφων

ασφαλείας, δοκιμών και επαναφοράς, έχει πλήρη επίγνωση όλων των βημάτων που απαιτούνται στις διαδικασίες αυτές.

- Τα αποτελέσματα των δοκιμών πρέπει να καταγράφονται και να αξιολογούνται. Πρέπει να χρησιμοποιούνται οι παρακάτω φόρμες για την δοκιμή και αξιολόγηση των δοκιμών αντιγράφων ασφαλείας:
  - Αρχείο Δοκιμών Ανάκτησης Αντιγράφων Ασφαλείας
  - Φόρμα Αξιολόγησης Δοκιμών Ανάκτησης Αντιγράφων Ασφαλείας

Επαναφορά

- Οι διαδικασίες επαναφοράς πρέπει να ελέγχονται τακτικά και να δοκιμάζονται, ώστε να διασφαλιστεί, ότι τα αντίγραφα ασφαλείας θα είναι αποτελεσματικά και συμβατά με τους στόχους επαναφοράς (Recovery Time Objectives – RTO), δηλαδή, ότι η αποκατάσταση των συστημάτων μπορεί να ολοκληρωθεί στο απαιτούμενο χρονικό διάστημα. Αυτές οι δοκιμές πρέπει να πραγματοποιούνται σε ένα πρόσφατο αντίγραφο ασφαλείας.
- Τα δεδομένα πρέπει να αποκατασταθούν μόνο στην αρχική τους τοποθεσία ή σε άλλη προκαθορισμένη εξουσιοδοτημένη τοποθεσία. Αυτός ο κανόνας μπορεί να παρακαμφθεί σε εξαιρετικές περιπτώσεις (π.χ. κατά τη διάρκεια ενός σημαντικού συμβάντος), μετά από έγκριση του Κατόχου του Συστήματος του Οργανισμού.

Τα δεδομένα που λαμβάνονται ως αντίγραφα ασφαλείας και περιλαμβάνονται στο παρόν έγγραφο, πρέπει να διατηρούνται τουλάχιστον για τις ακόλουθες χρονικές περιόδους. Ο Οργανισμός είναι υποχρεωμένος να παρακολουθεί την ισχύουσα νομοθεσία και να προσαρμόζει κατάλληλα την εν λόγω πολιτική.

Αν απαιτείται εξαίρεση για οποιαδήποτε από αυτές τις περιόδους, ο ενδιαφερόμενος πρέπει να επικοινωνεί με τον Υπεύθυνο Ασφάλειας. Τυχόν εξαιρέσεις πρέπει να τεκμηριώνονται και να εγκρίνονται από τον Υπεύθυνο Ασφάλειας.

Την ίδια πολιτική πρέπει να ακολουθούν και τα αρχεία καταγραφής (log files) των συστημάτων.

6.5 Πολιτική Διαχείρισης Περιστατικών και Επιχειρησιακής Συνέχειας

Εισαγωγή

Η προστασία των δεδομένων και ιδιαίτερα των Δεδομένων Προσωπικού Χαρακτήρα (εφεξής: ΔΠΧ) σε έναν Οργανισμό αναδεικνύεται σε μια σημαντική, οργανωμένη και επιμελή καθημερινή δραστηριότητα. Τα ΔΠΧ αποτελούν ίσως το πλέον σημαντικό κεφάλαιο για κάθε Οργανισμό και θα πρέπει να συλλέγονται, επεξεργάζονται, διακινούνται, φυλάσσονται, προστατεύονται με την εφαρμογή των κατάλληλων πρακτικών, διαδικασιών, πολιτικών και εργαλείων. Έχοντας ως στόχο την αντιμετώπιση των δυσμενέστερων σεναρίων, η δημιουργία και εφαρμογή ενός Πλάνου Αντιμετώπισης Περιστατικών Παραβίασης ΔΠΧ (εφεξής: Πλάνο) αποτελεί μία από τις προϋποθέσεις συμμόρφωσης με την κείμενη νομοθεσία περί προστασίας ΔΠΧ, συγκεκριμένα:

- *τις διατάξεις του Κανονισμού (ΕΕ) 2016/679 (GDPR/ΓΚΠΔ)* [14],
- *τις διατάξεις του Ν. 4624/2019 (ΦΕΚ Α' 137/29.08.2019)* [15].

Βασικός στόχος της παρούσας Πολιτικής είναι να διαχειριστεί η επιχείρηση αποτελεσματικά, τα περιστατικά που σχετίζονται με την παραβίαση ιδιωτικότητας ή ασφάλειας, να περιορίσει τη ζημιά, να αυξήσει την εμπιστοσύνη των υποκειμένων των δεδομένων προς τον Οργανισμό (υπεύθυνο επεξεργασίας[16]), να συνδράμει στην ταχύτερη και αποτελεσματικότερη αντιμετώπιση του περιστατικού (και των πιθανών δυσχερών αποτελεσμάτων του), να ικανοποιήσει τις νομικές υποχρεώσεις, να μειώσει το κόστος του περιστατικού στα οικονομικά αποτελέσματα Οργανισμού και στη φήμη

[14] Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων).

[15] Ν. υπ' αριθμ. 4624 Τεύχος Α' 137/29.08.2019, Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 και άλλες διατάξεις.

[16] Υπεύθυνος Επεξεργασίας είναι το φυσικό ή νομικό πρόσωπο, η δημόσια αρχή, η υπηρεσία ή άλλος φορέας που, μόνα ή από κοινού με άλλα, καθορίζουν τους σκοπούς και τον τρόπο της επεξεργασίας δεδομένων προσωπικού χαρακτήρα· όταν οι σκοποί και ο τρόπος της επεξεργασίας αυτής καθορίζονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους, ο υπεύθυνος επεξεργασίας ή τα ειδικά κριτήρια για τον διορισμό του μπορούν να προβλέπονται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους, αρ. 4, στοιχ. 7, ΓΚΠΔ.

του και να περιορίσει (ή δυνατόν αποτρέψει) διοικητικές ή/και ποινικές κυρώσεις, που απορρέουν από την ισχύουσα νομοθεσία.

Πεδίο εφαρμογής

Η Πολιτική αφορά όλα τα συστήματα πληροφορικής, τα δίκτυα και τα δεδομένα του Δήμου Περάματος (εφεξής «Φορέας» ή «Οργανισμός») καθώς και τους χρήστες και τις συσκευές τους μέσα στον Οργανισμό. Η Πολιτική του Οργανισμού θα αναθεωρείται κάθε 12 μήνες και όλα τα έγγραφα θα ενημερώνονται όποτε είναι απαραίτητο. Σε περίπτωση που συμβεί περιστατικό, κατά την διαδικασία ελέγχου και αναθεώρησης, αλλά πριν από την αναθεώρηση του εγγράφου, θα συγκλεισθεί συνάντηση για να διορθωθεί το έγγραφο το συντομότερο δυνατό.

Ασφάλεια ΔΠΧ

Παραδοσιακά, ο όρος ασφάλεια πληροφορίας/δεδομένων (information/data security) χρησιμοποιείται για να περιγράψει τη μεθοδολογία, καθώς και τις μεθόδους και τεχνικές που ακολουθούνται προκειμένου να επιτευχθούν οι εξής στόχοι:

- **Εμπιστευτικότητα** (confidentiality): Οι πληροφορίες/δεδομένα δεν πρέπει να αποκαλύπτονται σε μη εξουσιοδοτημένα άτομα.
- **Ακεραιότητα** (integrity): Οι πληροφορίες/δεδομένα πρέπει να είναι ακριβή, ακέραια και γνήσια – όχι εσφαλμένα, αλλοιωμένα ή μη ενημερωμένα.
- **Διαθεσιμότητα** (availability): Οι πληροφορίες/δεδομένα πρέπει να είναι στη διάθεση των χρηστών όποτε απαιτείται η χρήση τους.

Στους 3 ανωτέρω βασικούς στόχους της ασφάλειας, ο ΓΚΠΔ προσθέτει και την αξιοπιστία των συστημάτων (resilience). Στη σημερινή εποχή, κατά την οποία κρίσιμες λειτουργίες της κοινωνίας βασίζονται σε πληροφοριακά συστήματα, ένας φορέας οφείλει να εξασφαλίζει ότι τα συστήματα και οι εφαρμογές του θα συνεχίζουν να λειτουργούν υπό δυσμενείς συνθήκες, όπως μετά από ένα φυσικό ή τεχνικό περιστατικό, και ότι θα είναι σε θέση να τα επαναφέρει σε λειτουργία.
Τέλος, τμήμα των αυξημένων νέων υποχρεώσεων των υπευθύνων επεξεργασίας (εν προκειμένω ο Οργανισμός) σχετικά με την ασφάλεια της επεξεργασίας αποτελεί η εισαγωγή της υποχρέωσης κατάλληλης διαχείρισης των περιστατικών παραβίασης, που προϋποθέτει την ύπαρξη διαδικασιών αναγνώρισης, καταγραφής, αμελλητί γνωστοποίησης στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ) και ανακοίνωσης στα επηρεαζόμενα φυσικά πρόσωπα των εν λόγω περιστατικών.

Υποχρεώσεις Υπευθύνου επεξεργασίας

Όπως ορίζεται στην κείμενη νομοθεσία προστασίας ΔΠΧ, ο υπεύθυνος επεξεργασίας, οφείλει να λαμβάνει τα κατάλληλα τεχνικά και οργανωτικά μέτρα[17] για την επεξεργασία[18] των ΔΠΧ, ενώ, παράλληλα, θα πρέπει να πληροί (ο υπεύθυνος επεξεργασίας) τις αρχές της επεξεργασίας[19], καθώς ο Οργανισμός (ως υπεύθυνος επεξεργασίας) φέρει την ευθύνη και πρέπει να είναι σε θέση να αποδείξει τη συμμόρφωση (λογοδοσία)[20].

Ειδικότερα, τα ΔΠΧ υποβάλλονται σε επεξεργασία κατά τρόπο που εγγυάται την ενδεδειγμένη ασφάλεια, μεταξύ άλλων την προστασία τους από μη εξουσιοδοτημένη ή παράνομη επεξεργασία και τυχαία απώλεια, καταστροφή ή φθορά, με τη χρησιμοποίηση κατάλληλων τεχνικών ή οργανωτικών μέτρων («ακεραιότητα και εμπιστευτικότητα»). Ως εκ τούτου, ο Οργανισμός έχει καταρτίσει συγκεκριμένη Πολιτική για την Προστασία των Δεδομένων Προσωπικού Χαρακτήρα και τη συμμόρφωση με το GDPR, στην οποία παρουσιάζονται οι διαδικασίες που εφαρμόζει για την αντιμετώπιση περιστατικών ασφαλείας. Στο παρόν καταγράφονται οι σημαντικότερες ηλεκτρονικές απειλές που (πιθανόν) ενέχουν τα ΔΠΧ, οι φάσεις απόκρισης, περιορισμού, ανάλυσης, αναχαίτισης, εξάλειψης της επίθεσης και ανάκτησης των συστημάτων εγκαίρως. Όλες οι ενέργειες διεξάγονται σύμφωνα με ένα πλάνο ενεργειών το οποίο σκοπό έχει να εξασφαλίσει την απρόσκοπτη επικοινωνία και συνέχιση των δραστηριοτήτων του Οργανισμού.

Ορισμοί

Στο χώρο της πληροφορικής και κατ' επέκταση του διαδικτύου/κυβερνοχώρου, οι όροι «συμβάν» και «περιστατικό» χρησιμοποιούνται για την περιγραφή περιστατικών τα οποία λαμβάνουν χώρα ή επηρεάζουν ένα δίκτυο υπολογιστών.

Συμβάν: Ένα συμβάν αποτελεί οποιαδήποτε ενέργεια σε συστήματα πληροφορικής η οποία είτε ηθελημένα (π.χ. στα πλαίσια δοκιμών, ενημερώσεων, ελέγχων) είτε όχι ,μπορεί να θέσει σε κίνδυνο την ορθή λειτουργία ή να έχει ως συνέπεια την μερική ή την πλήρη κατάρρευση των συστημάτων πληροφορικής, των δικτύων, των βάσεων

[17] Αρ. 24, αιτ. 78, ΓΚΠΔ.

[18] Επεξεργασία είναι κάθε πράξη ή σειρά πράξεων που πραγματοποιείται με ή χωρίς τη χρήση αυτοματοποιημένων μέσων, σε δεδομένα προσωπικού χαρακτήρα ή σε σύνολα δεδομένων προσωπικού χαρακτήρα, όπως η συλλογή, η καταχώριση, η οργάνωση, η διάρθρωση, η αποθήκευση, η προσαρμογή ή η μεταβολή, η ανάκτηση, η αναζήτηση πληροφοριών, η χρήση, η κοινολόγηση με διαβίβαση, η διάδοση ή κάθε άλλη μορφή διάθεσης, η συσχέτιση ή ο συνδυασμός, ο περιορισμός, η διαγραφή ή η καταστροφή, αρ. 4, στοιχ. 2, ΓΚΠΔ.

[19] Αρ. 5, §1, ΓΚΠΔ.

[20] Αρ. 5, §2, ΓΚΠΔ.

δεδομένων και εν γένει την λειτουργία ενός Οργανισμού. Ο αριθμός των συμβάντων που συμβαίνουν κάθε μέρα εξαρτάται από το μέγεθος, δηλαδή το οικονομικό μέγεθος και τον αριθμό των εργαζομένων και συνεργατών και την επιχειρηματική δραστηριότητα του Οργανισμού. Κάθε οργανισμός μπορεί να αντιμετωπίσει εκατοντάδες γεγονότα που προκαλούνται από διάφορους λόγους, όπως κυβερνοεπιθέσεις, ενέργειες εργαζομένων, κακόβουλο λογισμικό το οποίο είναι είτε συνημμένο σε μήνυμα ηλεκτρονικού ταχυδρομείου, είτε διεισδύει από μολυσμένη συσκευή, κακή χρήση του χρήστη κ.λπ.

Περιστατικό: Κάθε περιστατικό αποτελεί γεγονός ενώ κάθε γεγονός δεν χαρακτηρίζεται απαραίτητα ως περιστατικό. Δηλαδή, συμβαίνει ένα περιστατικό όταν ένα συμβάν προκαλεί απώλεια δεδομένων, ιδιωτικότητα και συμβιβασμό συστήματος. Ως εκ τούτου, περιστατικό νοείται οποιαδήποτε ενέργεια συνίσταται σε παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, άνευ άδειας κοινολόγηση ή πρόσβαση δεδομένων ανεξάρτητα αν είναι δεδομένα προσωπικού χαρακτήρα ή όχι που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία και κατά συνέπεια παραβιάζει το απόρρητο, την ακεραιότητα ή τη διαθεσιμότητα των δεδομένων προσβάλλοντας ή θέτοντας σε κίνδυνο την ιδιωτική ζωή των υποκειμένων και περιουσιακών στοιχείων του Οργανισμού σύμφωνα και με τις πολιτικές ασφάλειας. Για παράδειγμα, η ύπαρξη και ο καθυστερημένος εντοπισμός στον καθορισμό οποιασδήποτε ευπάθειας στο δίκτυο υπολογιστών ή στο λογισμικό των συστημάτων του Οργανισμού είναι ένα συμβάν. Όταν όμως εντοπιστεί και διαπιστωθεί (από την ομάδα διαχείρισης και αντιμετώπισης περιστατικών) ότι από αυτό το κενό ή την ευπάθεια έχει προκύψει παραβίαση των υπολογιστικών συστημάτων και άρα και της ασφάλειας των δεδομένων, τότε αυτό χαρακτηρίζεται ως περιστατικό. Μερικά από τις πιο συνηθισμένες ενδείξεις περιστατικού ασφαλείας είναι οι εξής:

i. Άγνωστες συνδέσεις ή δραστηριότητα του συστήματος, ειδικά από ανενεργούς λογαριασμούς χρηστών.
ii. Η υπερβολική χρήση της απομακρυσμένης πρόσβασης στο επιχειρησιακό σύστημα υπολογιστών
iii. Η ύπαρξη νέου ασύρματου δικτύου ορατού στο περιβάλλον του συστήματος υπολογιστών
iv. Μη φυσιολογική δραστηριότητα η οποία σχετίζεται με κακόβουλο λογισμικό στο σύστημα, ύποπτα αρχεία, μη εκτελέσιμο αρχείο ή προγράμματα στο δίκτυο και τα υπολογιστικά συστήματα.

v. Επιθέσεις: άρνησης εξυπηρέτησης (DoS attack & DDoS),Man-in-the-middle (MitM) attack, Phishing and spear phishing attacks, Brute force attacks, SQL injection attacks, Malware attacks, Ransomware attacks, Zero-day exploit, Cross-Site Scripting (XSS) attacks

Η Ομάδα Διαχείρισης Περιστατικών παρακολουθεί και ελέγχει τον Οργανισμό για την ύπαρξη περιστατικών αξιοποιώντας τεχνολογικά εργαλεία παρακολούθησης, αλλά και πληροφορίες ή αναφορές από οποιονδήποτε υπάλληλο ή και συνεργάτες ή τρίτους. Μόλις γνωστοποιηθεί ή ύπαρξη περιστατικού, η ομάδα γνωστοποιεί στον υπεύθυνο ασφαλείας ΙΤ, στον Υπεύθυνο Προστασίας Δεδομένων, στην ομάδα υποστήριξης του Υπεύθυνου Προστασίας Δεδομένων, και στους άμεσα ενδιαφερόμενους. Το περιστατικό θα ταξινομηθεί, ανάλογα με το βαθμό της απειλής για την υποδομή του συστήματος και την βάση δεδομένων με τους όρου, Υψηλό, Μέτριο, Χαμηλό.

Ανάλογα με τη σοβαρότητα και τον τύπο του συμβάντος και του περιστατικού θα τεθεί σε εφαρμογή και το αντίστοιχο σχέδιο διαχείρισης συμβάντος ή περιστατικού. Συγκεκριμένα θα ακολουθηθούν τα εξής βήματα: (ο κύκλος ζωής του περιστατικού) προπαρασκευαστικές ενέργειες, ανίχνευση, περιορισμός/καραντίνα, εκρίζωσης, αποκατάσταση. Εν τω μεταξύ, ο Οργανισμός θα ενεργήσει προκειμένου τα συστήματα πληροφορικής, οι υπηρεσίες και διαδικασίες του Οργανισμού, να έχουν όσο τον δυνατόν λιγότερες απώλειες, παρέχοντας, παράλληλα, και την απαραίτητη τεκμηρίωση για τις ενέργειες που θα διασφαλίσουν την επιχειρησιακή συνέχεια του Οργανισμού.

Εκτός από τις ενέργειες που αναφέρονται ανωτέρω, ο Οργανισμός θα προβεί στην απαραίτητη τεκμηρίωση και θα παρέχει επαναλαμβανόμενες εκπαιδευτικές δράσεις ασφάλειας και διαχείρισης περιστατικών και συμβάντων στους υπαλλήλους και συνεργάτες του.

Κατηγοριοποίηση περιστατικών παραβίασης

Ως περιστατικό ασφάλειας πληροφοριών ορίζεται ένα ή μια σειρά από ανεπιθύμητα ή απρόβλεπτα συμβάντα ασφάλειας πληροφοριών τα οποία μπορούν να δημιουργήσουν πρόβλημα στην επιχειρησιακή λειτουργία ενός οργανισμού και να απειλήσουν την ασφάλεια των ΔΠΧ, δηλαδή την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των ΔΠΧ, που ο οργανισμός επεξεργάζεται. Τα περιστατικά παραβίασης ασφάλειας πληροφοριών κατηγοριοποιούνται ανάλογα με τις απειλές σε:

- Φυσικές καταστροφές (σεισμός, έντονα καιρικά φαινόμενα, πλημμύρα, κ.α.).

- Φυσική ζημιά, σκόπιμη ή κατά λάθος (πυρκαγιά, πλημμύρα, βραχυκύκλωμα, διάβρωση, καταστροφή – κλοπή – απώλεια ή αλλοίωση εξοπλισμού, καταστροφή – κλοπή, απώλεια μέσων, παραβίαση πολυμέσων κ.α.).
- Τεχνική αστοχία (αστοχία υλικού, δυσλειτουργία λογισμικού, κορεσμός της χωρητικότητας του συστήματος κ.α.).
- Τεχνική επίθεση (σάρωση δικτύου, εκμετάλλευση ευπάθειας, εκμετάλλευση backdoor, προσπάθειες σύνδεσης, παρεμβολές, DoS κ.α.).
- Παραβίαση κανόνων με η χωρίς ανθρώπινη παρέμβαση ή συμμετοχή (μη εξουσιοδοτημένη χρήση πόρων, παραβίαση πνευματικών δικαιωμάτων κ.α.).
- Παραβίαση της ασφαλείας των λειτουργιών του συστήματος (κατάχρηση δικαιωμάτων, πλαστογράφηση δικαιωμάτων, άρνηση δράσεων, εσφαλμένες ενέργειες, παραβίαση διαθεσιμότητας κ.α.).
- Παραβίαση της ασφαλείας των πληροφοριών του συστήματος (παρακολούθηση, κατασκοπεία, υποκλοπή, αποκάλυψη, social engineering, phishing, κλοπή, απώλεια, παραβίαση ή σφάλμα δεδομένων, ανίχνευση θέσης κ.α.).
- Περιστατικά επιβλαβούς περιεχόμενου (παράνομο περιεχόμενο, περιεχόμενο για πρόκληση πανικού, κακόβουλο περιεχόμενο, προσβλητικό περιεχόμενο κ.α.).

Κατηγοριοποίηση των περιστατικών παραβίασης:

- Πολύ σοβαρά

  Είναι τα περιστατικά εκείνα που εκδηλώνονται σε ιδιαίτερα σημαντικά συστήματα πληροφοριών, καθώς έχουν ως αποτέλεσμα δυσμενέστατη επιχειρηματική ζημία, ή ενέχουν υψηλό κοινωνικό αντίκτυπο.
- Σοβαρά

  Είναι τα περιστατικά εκείνα που εκδηλώνονται σε ιδιαίτερα σημαντικά συστήματα πληροφοριών ή σε σημαντικά συστήματα πληροφοριών, και προκαλούν σοβαρή επιχειρηματική ζημία, ή οδηγούν σε σημαντικές κοινωνικές επιπτώσεις.
- Λιγότερο σοβαρά

  Είναι τα περιστατικά εκείνα που εκδηλώνονται σε σημαντικά συστήματα πληροφοριών ή σε απλά/κοινά συστήματα πληροφοριών, ενώ, παράλληλα, έχουν ως αποτέλεσμα υπολογίσιμη επιχειρηματική απώλεια, ή οδηγούν σε υπολογίσιμες κοινωνικές επιπτώσεις.
- Μικρά

Είναι τα περιστατικά εκείνα που εκδηλώνονται σε απλά/κοινά πληροφοριακά συστήματα και ενδέχεται να έχουν ως αποτέλεσμα μικρές επιχειρηματικές απώλειες ή/και καμία, ενδέχεται να οδηγούν σε ήπιες κοινωνικές επιπτώσεις ή/και μηδενικές κοινωνικές επιπτώσεις. Γενικά, τα αποτελέσματα από τέτοιες ή έχουν καθόλου συνέπειες και δεν απαιτείται καμία ενέργεια.

Ταξινόμηση των περιστατικών παραβίασης ασφάλειας πληροφοριών

Μία προσέγγιση ταξινόμησης των παραβιάσεων ασφάλειας πληροφοριών είναι η παρακάτω, λαμβάνοντας υπόψη τους ακόλουθους παράγοντες:

- Την Σημασία των πληροφοριακών συστημάτων
  Η σημασία των πληροφοριακών συστημάτων που επηρεάζονται από περιστατικά παραβίασης, καθορίζεται από τη σημασία των δραστηριοτήτων του Οργανισμού, όπως αυτές υποστηρίζονται από τα σχετικά συστήματα.
- Την επιχειρησιακή απώλεια
  Η απώλεια της επιχειρησιακής δραστηριότητας που προκαλείται από περιστατικά ασφάλειας πληροφοριών καθορίζεται λαμβάνοντας υπόψη τη σοβαρότητα των επιπτώσεων της διακοπής των εργασιών του Οργανισμού λόγω της βλάβης του υλικού, του λογισμικού, των λειτουργιών και των δεδομένων των συστημάτων του Οργανισμού. Η σοβαρότητα των επιπτώσεων μπορεί να εξαρτηθεί από το κόστος για την ανάκαμψη του Οργανισμού και την επαναφορά της στην κανονική λειτουργία, καθώς και από άλλες αρνητικές επιπτώσεις των παραβιάσεων της ασφάλειας, συμπεριλαμβανομένης της απώλειας κερδών ή/και ευκαιριών. Αυτή η προσέγγιση κατατάσσει την επιχειρηματική ζημία σε τέσσερα ευρεία επίπεδα: Ιδιαίτερα σοβαρές επιχειρησιακές απώλειες, σοβαρές επιχειρησιακές απώλειες, σημαντικές επιχειρησιακές απώλειες και μικρές επιχειρηματικές απώλειες.

  - **Ιδιαίτερα σοβαρή επιχειρησιακή απώλεια**, θα συνεπαγόταν μεγάλη παράλυση του Οργανισμού σε βαθμό που θα έχανε την επιχειρηματική του ικανότητα ή/και πολύ σοβαρή ζημία στην εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των ΔΠΧ, που διατηρεί και επεξεργάζεται. Παράλληλα, θα σήμαινε τεράστιο κόστος για την επαναφορά του Οργανισμού στην κανονική λειτουργία και την εξάλειψη των επιπτώσεων.

- **Η σοβαρή επιχειρησιακή ζημία,** θα σήμαινε διακοπή επιχειρηματικών δραστηριοτήτων για μεγάλο χρονικό διάστημα ή τοπική παράλυση του Οργανισμού, σε βαθμό που θα επηρέαζε σοβαρά την επιχειρηματική του ικανότητα ή/και θα έβλαπτε σοβαρά την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των ΔΠΧ, που διατηρεί και επεξεργάζεται. Επιπλέον, θα σήμαινε υψηλό κόστος για την επαναφορά του Οργανισμού σε κανονική λειτουργία και την εξάλειψη των επιπτώσεων.
- **Σημαντική επιχειρησιακή ζημία,** σημαίνει διακοπή των επιχειρηματικών δραστηριοτήτων κατά τρόπο που να επηρεάζει σημαντικά τον Οργανισμού, ενώ, παράλληλα, προκαλεί σημαντική ζημιά στην εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των ΔΠΧ, που διατηρεί και επεξεργάζεται. Επιπροσθέτως, θα σήμαινε σημαντικό κόστος για την επαναφορά του Οργανισμού σε κανονική λειτουργία και την εξάλειψη των επιπτώσεων.
- **Η μειωμένη επιχειρησιακή ζημία,** θα σήμαινε διακοπή των επιχειρηματικών δραστηριοτήτων για μικρό χρονικό διάστημα, σε βαθμό που επηρεάζει τον Οργανισμό ενέχοντας μικρό (ή/και πιθανόν ελάχιστο) αντίκτυπο στην εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των ΔΠΧ, διατηρεί και επεξεργάζεται. Παράλληλα, θα σήμαινε μικρό κόστος για την επαναφορά της επιχείρησης σε κανονική λειτουργία και την εξάλειψη (πιθανών) δυσμενών αποτελεσμάτων.

- Τις κοινωνικές επιπτώσεις

Πολλά κοινωνικά φαινόμενα συνδέονται με τις παραβιάσεις ασφάλειας πληροφοριών, όπως το ηλεκτρονικό έγκλημα, η παραβίαση των δικαιωμάτων πνευματικής ιδιοκτησίας, η παρακολούθηση, η εμπορία ΔΠΧ κ.α. Ο αντίκτυπος στην κοινωνία από τις παραβιάσεις ασφάλειας πληροφοριών καθορίζεται λαμβάνοντας υπόψη την κλίμακα και το βαθμό των επιπτώσεων στην εργασιακή ζωή των ανθρώπων, στην προσωπική και κοινωνική ζωή, στο επίπεδο των θεσμών και της κοινωνίας, στην εθνική ασφάλεια, την κοινωνική τάξη, την οικονομική ανάπτυξη κ.α. Η προσέγγιση αυτή κατατάσσει τον κοινωνικό αντίκτυπο σε τέσσερα επίπεδα: ιδιαίτερα σημαντικό κοινωνικό αντίκτυπο, σημαντικό κοινωνικό αντίκτυπο, υπολογίσιμο κοινωνικό αντίκτυπο και μικρό κοινωνικό αντίκτυπο.

Πριν την εκδήλωση συμβάντος

Κατάρτιση σχεδίου αντιμετώπισης παραβίασης ΔΠΧ

Ομάδα Διαχείρισης Περιστατικών

Η δημιουργία Ομάδας Διαχείρισης Περιστατικών (εφεξής: Ομάδα) είναι το πρωταρχικό βήμα για την αντιμετώπιση περιστατικών ασφαλείας. Η βασική αρχή λειτουργίας της Ομάδας αυτής είναι η καταγραφή, η ανάλυση, η αξιολόγηση διαδικασιών και λειτουργιών, η πληροφόρηση και η ενημέρωση μεταξύ των μελών, ο σχεδιασμός, η βελτίωση με βάση την εμπειρία που αποκτάται.

Η Ομάδα πρέπει να είναι αντιπροσωπευτική το σύνολο των επιμέρους τμημάτων του Οργανισμού, που, μεταξύ άλλων, θα πρέπει να περιλαμβάνει μέλη από:

- Τον επικεφαλής της Ομάδας (μέλος της Διοίκησης)
- Τον Υπεύθυνο Προστασίας Δεδομένων (ΥΠΔ/DPO) του Οργανισμού.
- Την Πληροφορική (IT).
- Την Νομική υπηρεσία (ή εξωτερικό συνεργάτη πάροχο νομικών υπηρεσιών).
- Το τμήμα Ανθρώπινου Δυναμικού.

Τα κριτήρια επιλογής των μελών της Ομάδας, είναι η ευρεία γνώση των δραστηριοτήτων του Οργανισμού, η γνώση του αντικειμένου, η υπευθυνότητα, η ομαδικότητα και συνεργασία, η διαθεσιμότητα όταν παραστεί ανάγκη. Η Ομάδα οπλίζεται και λειτουργεί αποτελεσματικά όταν έχει τη στήριξη αλλά και την ευχέρεια να παίρνει αποφάσεις κατά τη λειτουργία της, από τη Διοίκηση του Οργανισμού.

Η ομάδα πρέπει να συνεδριάζει σε τακτικά χρονικά διαστήματα και να εκπονεί ασκήσεις προσομοίωσης διάφορων σεναρίων ώστε τα μέλη της να είναι σε ετοιμότητα για την αντιμετώπιση περιστατικών.

Είναι πολύ σημαντικό να γνωρίζουν τα μέλη της ομάδας τι είδους πληροφορίες διατηρεί ο Οργανισμός, ποιοι τις διαχειρίζονται, που είναι αποθηκευμένες και ποιές είναι οι ευθύνες της λόγω των κατηγοριών των ΔΠΧ που επεξεργάζεται.

Πιο συγκεκριμένα θα πρέπει να γνωρίζουν:

- Τι είδος πληροφορίες διατηρεί ο Οργανισμός για το ανθρώπινο δυναμικό του, τους επισκέπτες του, τους συνεργάτες του, τους προμηθευτές του.
- Τις τοποθεσίες διατήρησης και αποθήκευσης των πληροφοριών (ΔΠΧ).

- Τα συστήματα που χρησιμοποιούνται για την διαχείριση των πληροφοριών (ΔΠΧ), τις πολιτικές ασφάλειας πληροφοριών εφαρμόζονται για αυτά και αν είναι ενημερωμένες[21].
- Ποια μέλη της Ομάδας είναι υπεύθυνα για τα συστήματα αυτά.
- Αν υπάρχουν συνεργασίες με τρίτους (Processors) οι οποίοι διαχειρίζονται δεδομένα και εμπιστευτικές πληροφορίες του Οργανισμού

Ρόλοι και Ευθύνες

Επικεφαλής ομάδας

Το μέλος του Διοικητικού Συμβουλίου θα εξασφαλίσει ότι όλα τα μέλη της ομάδας επικοινωνούν αποτελεσματικά, συνεργάζονται και συντονίζονται με στόχο την γρήγορη και πλήρη ανάκαμψη.

Υπεύθυνος Ερευνών

Ο προϊστάμενος του τμήματος τεχνικής υποστήριξης (IT) θα συλλέξει, θα αναλύσει όλα τα αποδεικτικά στοιχεία, θα καθορίσει την αιτία, θα κατευθύνει τους υπόλοιπους αναλυτές ασφαλείας και θα εφαρμόσει ένα πλάνο για την ταχεία ανάκαμψη των συστημάτων και των υπηρεσιών.

Συντονιστής Επικοινωνίας

Ο προϊστάμενος του τομέα Ανθρώπινου Δυναμικού θα αναλάβει την επικοινωνία με όλους τους εμπλεκόμενους υπαλλήλους ή τρίτους εντός ή εκτός του Οργανισμού (π.χ. αρχές, υποκείμενα, συνεργάτες κ.λπ.).

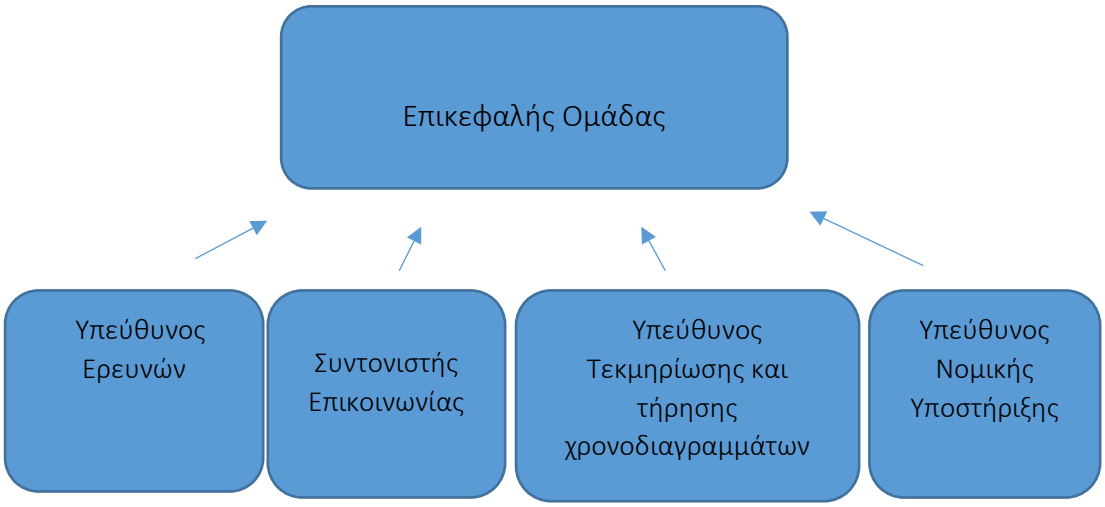
Υπεύθυνος Τεκμηρίωσης και τήρησης χρονοδιαγραμμάτων

Ο Υπεύθυνος Προστασίας Δεδομένων θα βεβαιωθεί ότι όλες οι δραστηριότητες της Ομάδας είναι τεκμηριωμένες ή θα τεκμηριωθούν στο τέλος των ενεργειών, συμπεριλαμβανομένων των ενεργειών κατά την διερεύνηση, ανακάλυψη και αποκατάστασης και θα φροντίσει για την θέση σε εφαρμογή ενός αξιόπιστου χρονοδιαγράμματος για κάθε στάδιο του περιστατικού.

Διαχείρισης Εργαζομένων/Νομική Υποστήριξη

Η Νομική Υπηρεσία του Οργανισμού θα βοηθήσει στην νομική υποστήριξη και καθοδήγηση της Διεύθυνσης ανθρωπίνων πόρων.

[21] Η δημιουργία ενός Πλάνου αντιμετώπισης περιστατικού παραβίασης συγκεντρώνει όλες τις διαδικασίες που θα επιτρέψουν στον Οργανισμό να παραμείνει ενεργός μετά από περιστατικά παραβίασης ΔΠΧ. Πρακτικά, είναι η συλλογή όλων των διαδικασιών που σχετίζονται με την αναγνώριση, τον προσδιορισμό, την έρευνα, την αντιμετώπιση, την ανταπόκριση σε περιπτώσεις περιστατικών παραβίασης, με γνώμονα τον περιορισμό των επιπτώσεων και τη γρήγορη ανάκαμψη.



Σχήμα 1 Ρόλοι και ευθύνες

Εξασφάλιση εξωτερικής Υποστήριξης

Δεν είναι ακραίο να παρομοιάσουμε ένα περιστατικό παραβίασης σαν μια κατάσταση φυσικής καταστροφής (πυρκαγιά, σεισμός, πλημμύρα), που η αντιμετώπισή της χρειάζεται πολλές δεξιότητες, γνώση, ετοιμότητα και διαθεσιμότητα. Ανάλογα με την έκταση και σοβαρότητα της παραβίασης ο Οργανισμός μπορεί να μην είναι σε θέση να λειτουργήσει στο σύνολό του ή σε σημαντικές δραστηριότητές του.

Βασικό στοιχείο του Πλάνου είναι η εξασφάλιση των απαιτούμενων πόρων στις κατάσταση κρίσης. Υπάρχουν περιπτώσεις που οι εσωτερικοί πόροι δεν επαρκούν. Η έγκαιρη εξασφάλιση εξωτερικής βοήθειας καθίσταται σημαντικός παράγοντας αποτελεσματικής αντιμετώπισης της κρίσης.

Γι’ αυτό η έγκαιρη προετοιμασία και η συμφωνία για συνεργασία με εξωτερικούς συνεργάτες, εξασφαλίζει διαθεσιμότητα πόρων στη διάρκεια μιας κρίσης και σε αποδεκτό κόστος. Συνήθως προτείνεται η εξασφάλιση συνεργασίας στους κάτωθι τομείς:

- Υπηρεσίες Νομικής Υποστήριξης
- Υπηρεσίες Πληροφορικής

- Υπηρεσίες Διαδικτυακής Εγκληματολογίας οι οποίες είναι απαραίτητες για τον εντοπισμό της πηγής της παραβίασης
- Υπηρεσίες Επικοινωνίας/Ενημέρωσης & Δημοσίων Σχέσεων
- Ασφαλιστική Κάλυψη κινδύνων παραβίασης (Cyber Insurance)

Εκπαίδευση εργαζομένων

Η συνεχής ενημέρωση και εκπαίδευση του προσωπικού εξασφαλίζει την απαιτούμενη προσοχή, εγρήγορση και αντιμετώπιση περιστατικών παραβίασης ΔΠΧ. Η έλλειψη κατάρτισης μπορεί να οδηγήσει σε αθώα λάθη που μπορεί να έχουν σημαντικές επιπτώσεις αργότερα. Συνίσταται η δημιουργία δύο εκπαιδευτικών προγραμμάτων. Ένα γενικό πρόγραμμα για όλο το προσωπικό και ένα για το προσωπικό που συμμετέχει στην αντιμετώπιση περιστατικών παραβίασης, ώστε να λάβουν γνώση για τη προστασία των ΔΠΧ και τη αντιμετώπιση περιστατικών ασφαλείας. Όσον αφορά το προσωπικό αντιμετώπισης περιστατικών το εκπαιδευτικό πρόγραμμα θα περιλαμβάνει εξειδικευμένες μεθοδολογίες, τεχνικές, εργαλεία, ανάλυση περιπτώσεων κ.λπ. Το γενικό εκπαιδευτικό πρόγραμμα στοχεύει πρωτίστως στη δημιουργία κουλτούρας ΔΠΧ. Θα πρέπει να δίνεται έμφαση σε αληθινά παραδείγματα από την αγορά, το περιεχόμενο να είναι απλό και κατανοητό, να γίνεται τακτικά και να έχει επίπεδα γνώσης. Το ενημερωμένο και σε ετοιμότητα προσωπικό είναι το καλύτερο μέσο προστασίας, το καλύτερο «εργαλείο» ασφάλειας των ΔΠΧ. Η δημιουργία και η συνεχής ενίσχυση κουλτούρας προστασίας ΔΠΧ έχει αποτρέψει κινδύνους παραβίασης σε μεγάλο αριθμό οργανισμών.

Προετοιμασία για την αντιμετώπιση περιστατικού

Το στάδιο αυτό αποτελεί την κινητήρια δύναμη του Πλάνου για την προστασία του Οργανισμού. Ειδικότερα, η προετοιμασία στο πλαίσιο διαχείρισης ενός περιστατικού, βοηθά τον Οργανισμό να αντιμετωπίσει όσο το δυνατόν πιο αποτελεσματικά ένα περιστατικό ασφαλείας την ώρα που θα συμβεί και θα βρίσκεται σε εξέλιξη καθώς και να εμποδίσει, όσο είναι δυνατό την πιθανότητα επέλευσης ενός περιστατικού με τον έλεγχο και την εγκατάσταση ενημερωμένων συστημάτων ασφαλείας πληροφορικής και δικτύου. Σε αυτή τη φάση δημιουργούνται, τίθενται σε εφαρμογή και δοκιμάζονται πολιτικές, διαδικασίες, στρατηγικές επικοινωνίας και συντονισμού, εργαλεία και πόροι για την αντιμετώπιση και διαχείριση κάποιου περιστατικού, όπως πληροφορίες επικοινωνίας με αρμόδια άτομα, έλεγχος συσκευών επικοινωνίας π.χ. smartphones, λογισμικό κρυπτογράφησης, ψηφιακά εργαλεία ελέγχου και έρευνας, φορητοί

υπολογιστές, αχρησιμοποίητες ή αδρανοποιημένες συσκευές αφαιρούμενες ή μη κ.λπ. Πιο συγκεκριμένα, θα πρέπει να υλοποιούνται:

- η ανάπτυξη πολιτικών και διαδικασιών που πρέπει να ακολουθηθούν σε περίπτωση περιστατικού κυβερνοασφάλειας, περιλαμβάνοντας τον προσδιορισμό της ακριβούς σύνθεσης της Ομάδας,
- η ανάπτυξη σεναρίων αντιμετώπισης περιστατικών και τακτική διεξαγωγή σχετικών ασκήσεων για την αξιολόγηση του Πλάνου και
- η εξασφάλιση ότι οι εργαζόμενοι είναι κατάλληλα εκπαιδευμένοι σχετικά με τους ρόλους και τις ευθύνες τους όσον αφορά την αντιμετώπιση περιστατικών ασφάλειας.

Περιγραφή

Σε αυτό το στάδιο ο Οργανισμός πρέπει να προετοιμαστεί για να είναι σε θέση να χειριστεί το οποιοδήποτε περιστατικό, εγκαίρως και να συνεχίσει τις επόμενες φάσεις του σχεδίου Πλάνου. Το στάδιο της προετοιμασίας είναι για την διαχείριση ενός περιστατικού, το πιο σημαντικό μέρος ενός Πλάνου, καθώς το πιο πιθανό είναι ότι από την στιγμή που θα εντοπιστεί μία απειλή ή εκδηλωθεί μία επίθεση, η εξάπλωσή της θα είναι ταχύτατη. Συνήθως μόλις εντοπιστεί ένα περιστατικό σε επίπεδο λογισμικού π.χ. κακόβουλος κώδικας/ransomware στο σύστημα, θα είναι πολύ αργά για ενέργειες όπως η αποθήκευση αρχείων, ή η κρυπτογράφηση. Ως εκ τούτου, η Ομάδα και γενικότερα ο Οργανισμός πρέπει να έχει έτοιμο ένα πλάνο ενεργειών, μία στρατηγική που να βοηθήσει όλους τους εμπλεκόμενους να διαχειριστούν με τον ιδανικότερο τρόπο ένα περιστατικό. Παράλληλα, θα πρέπει κατά το στάδιο της προεργασίας να έχουν ήδη ληφθεί κατάλληλα μέτρα και ενέργειες που θα εμποδίσουν εξαρχής την επίθεση, κάτι στο οποίο θα συνδράμει η ομάδα υποστήριξης Υπεύθυνου Προστασίας Δεδομένων.

Επομένως η Ομάδα θα πρέπει να έχει:

1. Φορητό υπολογιστή με εργαλεία λογισμικού με τα οποία θα μπορεί να ερευνήσει υπολογιστικά συστήματα, να διαχειριστεί κακόβουλο λογισμικό, να αναλύσει δίσκους κλπ..
2. Λίστα καταγραφής των υπολογιστικών πόρων και συστημάτων του Οργανισμού, π.χ. θύρες επικοινωνίας και πρόσβασης σε χώρους και συστήματα, εγχειρίδια τεκμηρίωσης και εγχειρίδια χρήσης για εφαρμογές, λειτουργικά συστήματα και προγράμματα προστασίας από ιούς, κατάλογος κρίσιμων στοιχείων, όπως διακομιστές βάσεων δεδομένων, ελεγκτές τομέα, αρχεία καταγραφής των δυνατοτήτων κατακερματισμού, διαγράμματα δικτύου, και φορητό υπολογιστή που περιέχει αρχεία καταγραφής προηγούμενων περιστατικών και ενέργειες διαχείρισης συνοδευόμενες από τεχνικές μελέτες και αναλύσεις.
3. Ολοκληρωμένη αναφορά περί της τρωτότητας του δικτύου του Οργανισμού, ώστε να είναι γνωστές οι πιο πιθανές θύρες εισόδου της επίθεσης και να είναι οι πρώτες που θα περάσουν από τον έλεγχο της Ομάδας.

Σε αυτό το στάδιο ο στόχος της Ομάδας είναι να δημιουργήσει ένα καλό σχέδιο για την διασφάλιση της συνέχειας του Οργανισμού. Απαιτείται ο σχεδιασμός πολιτικών, διαδικασιών, διαχείριση της υποχρέωσης ενημέρωσης και επικοινωνίας, προκειμένου να γίνει με το καλύτερο δυνατό τρόπο η διαχείριση μίας επίθεσης ή ενός περιστατικού. Διαδικασίες για την ανίχνευση απειλών ή επιθέσεων και διενέργεια δοκιμών και αξιολογήσεων της εταιρείας για την ικανότητα διαχείρισης απειλών. Η Ομάδα ελέγχει και επικαιροποιεί εργαλεία και διαθέσιμους πόρους.

Το Πλάνο πρέπει να είναι καλά τεκμηριωμένο, εξηγώντας πλήρως τους ρόλους και τις ευθύνες όλων. Στη συνέχεια, το σχέδιο πρέπει να δοκιμαστεί προκειμένου να διασφαλιστεί ότι οι συμμετέχοντες θα αντιδράσουν όπως προβλέπεται στα πλαίσια της εκπαίδευσής τους. Βασικό στοιχείο αυτής της διαδικασίας είναι η αποτελεσματική εκπαίδευση για την αντιμετώπιση παραβίασης και τεκμηρίωσης για την καταγραφή των ενεργειών που γίνονται για μεταγενέστερη αναθεώρηση.

Κατά τη διάρκεια του εκδήλωσης του συμβάντος

Αναγνώριση/Ανίχνευση του συμβάντος

Στόχος του σχεδίου αναγνώρισης είναι η ανίχνευση της παραβίασης και η δυνατότητα γρήγορης και εστιασμένης αντίδρασης. Οι παραβιάσεις εντοπίζονται

χρησιμοποιώντας διάφορους μηχανισμούς threat intelligence, συστήματα ανίχνευσης εισβολών και τείχη προστασίας.

Μέσα ανίχνευσης

1) Η ανίχνευση ενός περιστατικού παραβίασης μπορεί να επιτευχθεί με τη χρήση ενός ενημερωμένου προγράμματος εντοπισμού ιών, όταν το κακόβουλο λογισμικό είναι γνωστό.
2) Επίσης ένα σύστημα ανίχνευσης συμβάντων, π.χ. τεχνολογία SIEM, μπορεί να ανακαλύψει ένα κακόβουλο λογισμικό στο σύστημα αναλύοντας μη φυσιολογικές δραστηριότητες όπως υπερβολική κατανάλωση CPU, μεγάλη κατανάλωση μνήμης στο σύστημα, κ.λπ.
3) Συχνές σαρώσεις ασφαλείας και αντίστοιχα ενδελεχής έλεγχος των αποτελεσμάτων.

Ενέργειες κατά την αναγνώριση

Κατά τη διάρκεια εξέλιξης του περιστατικού:

1) Οι εμπλεκόμενοι Η/Υ ή servers πρέπει να απομονωθούν από το υπόλοιπο δίκτυο (πχ. Αποσυνδέοντας το καλώδιο ethernet, ή απομονώνοντάς τους μέσω firewall).
2) οι εργαζόμενοι ενημερώνουν άμεσα την Ομάδα για την ύπαρξη του περιστατικού.

Σε κάθε περίπτωση, στο στάδιο αναγνώρισης, πρέπει να καταγράφονται κατ' ελάχιστον, οι κάτωθι πληροφορίες:

- Πότε συνέβη το περιστατικό.
- Πως ανακαλύφθηκε και από ποιόν.
- Διαδικασίες, τμήματα του οργανισμού ή συστήματα που το περιστατικό επηρέασε.
- Ποιο είναι το εύρος του περιστατικού.
- Σε ποιο βαθμό το περιστατικό επηρεάζει την λειτουργία του οργανισμού.
- Ποια είναι η «πηγή» του περιστατικού.

Ανακοίνωση στο υποκείμενο των δεδομένων[22]

Σε ορισμένες περιπτώσεις, ο υπεύθυνος επεξεργασίας υποχρεούται να ανακοινώσει μια παραβίαση στα επηρεαζόμενα φυσικά πρόσωπα. *«Όταν η παραβίαση δεδομένων*

[22] Κατευθυντήριες γραμμές Ομάδας Εργασίας Άρθρου 29 σχετικά με τη γνωστοποίηση παραβιάσεων δεδομένων προσωπικού χαρακτήρα δυνάμει του κανονισμού 2016/679, WP 250 rev.01 Ομάδας για την προστασία των

προσωπικού χαρακτήρα ενδέχεται να θέσει σε υψηλό κίνδυνο τα δικαιώματα και τις ελευθερίες φυσικών προσώπων, ο υπεύθυνος της επεξεργασίας ανακοινώνει αμελλητί την παραβίαση των δεδομένων προσωπικού χαρακτήρα στο υποκείμενο των δεδομένων»[23].

Ο ΓΚΠΔ αναφέρει ότι η ανακοίνωση μιας παραβίασης στα πρόσωπα θα πρέπει να γίνεται «αμελλητί», δηλαδή το συντομότερο δυνατόν. Ο κύριος στόχος της ανακοίνωσης στα πρόσωπα είναι η παροχή συγκεκριμένων πληροφοριών σχετικά με τις ενέργειες στις οποίες θα πρέπει να προβούν τα ίδια για να προστατευτούν[24].

Απαιτούμενες πληροφορίες ενημέρωσης

«Στην ανακοίνωση στο υποκείμενο των δεδομένων η οποία αναφέρεται στην παράγραφο 1 του παρόντος άρθρου περιγράφεται με σαφήνεια η φύση της παραβίασης των δεδομένων προσωπικού χαρακτήρα και περιέχονται τουλάχιστον οι πληροφορίες και τα μέτρα που αναφέρονται στο άρθρο 33 παράγραφος 3 στοιχεία β), γ) και δ)»[25].

Σύμφωνα με την ως άνω διάταξη, ο υπεύθυνος επεξεργασίας, θα πρέπει κατ' ελάχιστο να παρέχει τις ακόλουθες πληροφορίες:

- σύντομη περιγραφή της φύσεως της παραβίασης,
- το όνομα και τα στοιχεία επικοινωνίας του ΥΠΔ ή άλλου σημείου επικοινωνίας
- περιγραφή των ενδεχόμενων συνεπειών της παραβίασης και
- περιγραφή των ληφθέντων ή των προτεινόμενων προς λήψη μέτρων από τον υπεύθυνο επεξεργασίας για την αντιμετώπιση της παραβίασης, καθώς και, όπου ενδείκνυται, μέτρων για την άμβλυνση ενδεχόμενων δυσμενών συνεπειών της[26].

Ο υπεύθυνος επεξεργασίας (Οργανισμός) θα πρέπει επίσης, κατά περίπτωση, να παρέχει ειδικές συμβουλές στα πρόσωπα για την προστασία τους από ενδεχόμενες δυσμενείς συνέπειες της παραβίασης, π.χ. επαναφορά κωδικού πρόσβασης σε περίπτωση που έχουν τεθεί σε κίνδυνο τα διαπιστευτήρια πρόσβασής τους. Ο υπεύθυνος επεξεργασίας (Οργανισμός) μπορεί και πάλι να επιλέξει να παράσχει πληροφορίες επιπλέον εκείνων που απαιτούνται σε αυτή την περίπτωση.

προσώπων έναντι της επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα**,** https://www.dpa.gr/sites/default/files/2020-05/wp250rev01_el.pdf.

[23] Αρ. 34, §1, ΓΚΠΔ.

[24] Αιτ. σκ. 86, ΓΚΠΔ.

[25] Αρ. 34, §1, ΓΚΠΔ.

[26] Ως παράδειγμα μέτρων που έχουν ληφθεί για την αντιμετώπιση της παραβίασης και την άμβλυνση ενδεχόμενων δυσμενών συνεπειών της, ο υπεύθυνος επεξεργασίας θα μπορούσε να αναφέρει ότι, αφού γνωστοποίησε την παραβίαση στην αρμόδια εποπτική αρχή, έλαβε συμβουλές σχετικά με τη διαχείριση της παραβίασης και τον μετριασμό των επιπτώσεών της.

Ενέργειες για την επικοινωνία με τα πρόσωπα

1) Κατά την ανακοίνωση μιας παραβίασης στα υποκείμενα των δεδομένων θα πρέπει να χρησιμοποιούνται ειδικά μηνύματα[27], τα οποία **δεν** θα πρέπει να αποστέλλονται μαζί με άλλες πληροφορίες, όπως τακτικές ενημερώσεις, ενημερωτικά δελτία ή τυποποιημένα μηνύματα.
2) Ο υπεύθυνος επεξεργασίας (Οργανισμός) μπορεί επίσης να πρέπει να εξασφαλίζουν ότι η ανακοίνωση είναι προσβάσιμη σε κατάλληλους εναλλακτικούς μορφοτύπους και στις σχετικές γλώσσες, ώστε να διασφαλίζεται ότι τα πρόσωπα μπορούν να κατανοήσουν τις πληροφορίες που τους παρέχονται.
3) Όταν δεν είναι δυνατόν για τον υπεύθυνο επεξεργασίας (Οργανισμός) να ανακοινώσει μια παραβίαση σε ένα πρόσωπο λόγω του ότι δεν υπάρχουν επαρκή δεδομένα αποθηκευμένα για να επικοινωνήσει με το πρόσωπο, σε αυτήν συγκεκριμένη περίσταση ο υπεύθυνος επεξεργασίας θα πρέπει να ενημερώνει το πρόσωπο μόλις είναι ευλόγως εφικτό να το πράξει (π.χ., όταν ένα πρόσωπο ασκεί το δικαίωμά του, σύμφωνα με το άρθρο 15, για πρόσβαση στα ΔΠΧ και παρέχει στον υπεύθυνο επεξεργασίας τις απαραίτητες πρόσθετες πληροφορίες για να επικοινωνήσει μαζί του).
4) Σε περίπτωση εκδήλωσης περιστατικού ενημερώνεται τάχιστα ο ΥΠΔ του Οργανισμού, για να παρασχεθεί καθοδήγηση και να γίνουν οι δέουσες ενέργειες για την ανακοίνωση του περιστατικού στα επηρεαζόμενα φυσικά πρόσωπα (βλ. Συμμετοχή ΥΠΔ στη διαδικασία)

Προϋποθέσεις σύμφωνα με τις οποίες δεν απαιτείται ανακοίνωση

Στο ΓΚΠΔ αναφέρονται τρεις προϋποθέσεις οι οποίες, εάν πληρούνται, δεν απαιτείται ανακοίνωση στα πρόσωπα σε περίπτωση παραβίασης[28]. Αυτές είναι οι εξής:

- Ο υπεύθυνος επεξεργασίας (Οργανισμός) εφάρμοσε κατάλληλα τεχνικά και οργανωτικά μέτρα προστασίας για την προστασία των ΔΠΧ πριν από την παραβίαση, κυρίως μέτρα που καθιστούν μη κατανοητά τα ΔΠΧ σε όσους δεν διαθέτουν άδεια πρόσβασης σε αυτά. Τα μέτρα αυτά θα μπορούσαν, για παράδειγμα, να περιλαμβάνουν την προστασία των ΔΠΧ με κρυπτογράφηση προηγμένης τεχνολογίας ή δειγματοποίηση.

[27] Παραδείγματα διαφανών μεθόδων ανακοίνωσης περιλαμβάνουν την απευθείας αποστολή μηνυμάτων (π.χ., μήνυμα ηλεκτρονικού ταχυδρομείου, μήνυμα SMS, άμεσο μήνυμα), τα πλαίσια γνωστοποίησης σε περίοπτη θέση σε ιστοτόπους, τις ανακοινώσεις μέσω ταχυδρομείου και τις διαφημίσεις σε έντυπα μέσα ενημέρωσης σε περίοπτη θέση. Μια ανακοίνωση που περιορίζεται αποκλειστικά σε ένα δελτίο Τύπου ή σε ένα εταιρικό ιστολόγιο δεν θα αποτελούσε αποτελεσματικό μέσο ανακοίνωσης μιας παραβίασης σε ένα πρόσωπο. Η ΟΕ29 συνιστά οι υπεύθυνοι επεξεργασίας να επιλέγουν το μέσο που μεγιστοποιεί τις πιθανότητες δέουσας ανακοίνωσης των πληροφοριών σε όλα τα επηρεαζόμενα πρόσωπα. Ανάλογα με τις περιστάσεις, αυτό μπορεί να σημαίνει ότι ο υπεύθυνος επεξεργασίας χρησιμοποιεί διάφορους τρόπους ανακοίνωσης αντί ενός μόνο διαύλου επικοινωνίας.

[28] Αρ. 34, §3, ΓΚΠΔ.

- Αμέσως έπειτα από μια παραβίαση, ο υπεύθυνος επεξεργασίας (Οργανισμός) έλαβε μέτρα που διασφαλίζουν ότι δεν είναι πλέον πιθανό να προκύψει υψηλός κίνδυνος για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. Για παράδειγμα, αναλόγως με τις περιστάσεις της περίπτωσης, ο υπεύθυνος επεξεργασίας μπορεί να έχει εξακριβώσει την ταυτότητα και να έχει λάβει δράση αμέσως έναντι του προσώπου (που έπραξε την παραβίαση) που έχει αποκτήσει πρόσβαση σε δεδομένα προσωπικού χαρακτήρα προτού αυτό μπορέσει να τα χρησιμοποιήσει με οποιονδήποτε τρόπο.

- Όταν η επικοινωνία με τα φυσικά πρόσωπα συνεπάγεται δυσανάλογες προσπάθειες, ίσως εάν τα στοιχεία επικοινωνίας έχουν χαθεί ως αποτέλεσμα της παραβίασης ή δεν είναι εξαρχής γνωστά. Για παράδειγμα, η αποθήκη μιας στατιστικής υπηρεσίας έχει πλημμυρίσει και τα έγγραφα που περιέχουν ΔΠΧ ήταν αποθηκευμένα μόνο σε έντυπη μορφή. Ο υπεύθυνος επεξεργασίας (Οργανισμός) πρέπει να κάνει μια δημόσια ανακοίνωση ή να λάβει παρεμφερή μέτρα με τα οποία τα φυσικά πρόσωπα θα ενημερωθούν με εξίσου αποτελεσματικό τρόπο[29].

Γνωστοποίηση στην εποπτική Αρχή

Πέραν της ανακοίνωσης του περιστατικού παραβίασης στα επηρεαζόμενα φυσικά πρόσωπα (υποκείμενα των δεδομένων), όπως ήδη αναφέρθηκε, ο υπεύθυνος επεξεργασίας (Οργανισμός) *«γνωστοποιεί αμελλητί και, αν είναι δυνατό, εντός 72 ωρών από τη στιγμή που αποκτά γνώση του γεγονότος την παραβίαση των δεδομένων προσωπικού χαρακτήρα στην εποπτική αρχή που είναι αρμόδια, εκτός εάν η παραβίαση δεδομένων προσωπικού χαρακτήρα δεν ενδέχεται να προκαλέσει κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, όταν η γνωστοποίηση στην εποπτική αρχή δεν πραγματοποιείται εντός 72 ωρών συνοδεύεται από τους λόγους της καθυστέρησης»*[30]. Στο τέλος του (παρόντος) εγγράφου (βλ. Παράρτημα Β) παρατίθεται κατάλογος, που περιλαμβάνει ενδεικτικά περιπτώσεις ανακοίνωσης περιστατικών παραβίασης στα επηρεαζόμενα φυσικά πρόσωπα και γνωστοποίησης στην εποπτική Αρχή (Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα – ΑΠΔΠΧ)[31].

---

[29] Μια ανακοίνωση που περιορίζεται αποκλειστικά σε ένα δελτίο Τύπου ή σε ένα εταιρικό ιστολόγιο δεν θα αποτελούσε αποτελεσματικό μέσο ανακοίνωσης μιας παραβίασης σε ένα πρόσωπο.

[30] Αρ. 33, §1, ΓΚΠΔ.

[31] Περισσότερες περιπτώσεις περιλαμβάνονται στο κείμενο: Κατευθυντήριες γραμμές Ομάδας Εργασίας Άρθρου 29 σχετικά με τη γνωστοποίηση παραβιάσεων δεδομένων προσωπικού χαρακτήρα δυνάμει του κανονισμού 2016/679, WP 250 rev.01 Ομάδας για την προστασία των προσώπων έναντι της επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα**,** https://www.dpa.gr/sites/default/files/2020-05/wp250rev01_el.pdf.

Ενέργειες για την γνωστοποίηση στην ΑΠΔΠΧ

1) Ο Οργανισμός (ως υπεύθυνος επεξεργασίας) φέρει την υποχρέωση χειρισμού κάθε περιστατικού παραβίασης ΔΠΧ, στα πλαίσια ασφάλειας της επεξεργασίας. Σε περίπτωση που από το περιστατικό ενδέχεται να προκληθεί κίνδυνος στα δικαιώματα και τις ελευθερίες των προσώπων τα οποία αυτό αφορά, ο Οργανισμός οφείλει να το γνωστοποιήσει στην ΑΠΔΠΧ.
2) Η εν λόγω γνωστοποίηση πρέπει να γίνεται αμελλητί και, αν είναι δυνατό, εντός 72 ωρών από τη στιγμή που ο Οργανισμός ενημερωθεί για το περιστατικό.
3) Η γνωστοποίηση πρέπει να περιέχει συγκεκριμένες πληροφορίες (π.χ. φύση/έκταση του περιστατικού, κατηγορίες προσώπων που επλήγησαν, αιτία και συνέπειες αυτού, ενέργειες που έγιναν προς αντιμετώπισή του, κ.ά.). Ακόμα και αν οι πληροφορίες αυτές δεν είναι όλες διαθέσιμες κατά την υποβολή της γνωστοποίησης, αυτή θα πρέπει να υποβληθεί ως αρχική και να ακολουθήσει στη συνέχεια, χωρίς αδικαιολόγητη καθυστέρηση, επικαιροποίησή της (με υποβολή συμπληρωματικής γνωστοποίησης).
4) Σε περίπτωση εκδήλωσης περιστατικού ενημερώνεται τάχιστα ο ΥΠΔ του Οργανισμού, για να παρασχεθεί καθοδήγηση και να γίνουν οι δέουσες ενέργειες για την γνωστοποίηση του περιστατικού στην ΑΠΔΠΧ (βλ. Συμμετοχή ΥΠΔ στη διαδικασία).
5) Πληροφορίες για την γνωστοποίηση περιστατικού παραβίασης στην ΑΠΔΠΧ, παρέχονται στον ακόλουθο σύνδεσμο: https://www.dpa.gr/el/foreis/asfaleia_dedomenwn/gnwstopoiisi_paraviasis/upovoli_gnwstopoihshs_paraviashs.

Επισημάνσεις

Περαιτέρω, όταν η παραβίαση ενδέχεται να θέσει σε υψηλό κίνδυνο τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων τα οποία αφορά το περιστατικό, τότε ο υπεύθυνος επεξεργασίας οφείλει να ανακοινώνει αμελλητί την παραβίαση και στα πρόσωπα αυτά. Αυτή η ανακοίνωση είναι ανεξάρτητη της προαναφερθείσας γνωστοποίησης στην ΑΠΔΠΧ (η οποία γνωστοποίηση στην ΑΠΔΠΧ υποβάλλεται ακόμα και αν ο σχετικός κίνδυνος δεν κρίνεται ως υψηλός).

Σημειώνεται ότι η Αρχή δύναται σε κάθε περίπτωση να δώσει εντολή στον υπεύθυνο επεξεργασίας να ενημερώσει τα φυσικά πρόσωπα για το περιστατικό[32].

Σε περίπτωση παραβίασης, ο Οργανισμός. γνωστοποιεί την παραβίαση αμελλητί και, αν είναι δυνατό, εντός 72 ωρών από τη στιγμή που αποκτά γνώση του γεγονότος. Αυτό

[32] Αρ. 58, §2, στοιχ. ε' ΓΚΠΔ.

σημαίνει ότι ο υπεύθυνος επεξεργασίας θα πρέπει να θεωρείται ότι αποκτά «γνώση» όταν έχει εύλογο βαθμό βεβαιότητας ότι έχει προκύψει περιστατικό ασφάλειας το οποίο έχει ως αποτέλεσμα να τεθούν σε κίνδυνο τα ΔΠΧ[33].

Μη γνωστοποίηση στην εποπτική Αρχή ΑΠΔΠΧ

Ο ΓΚΠΔ προβλέπει ότι είναι δυνατή η μη γνωστοποίηση μίας παραβίασης εάν η παραβίαση δεν ενδέχεται να θέσει σε κίνδυνο τα δικαιώματα και τις ελευθερίες των προσώπων και ο υπεύθυνος επεξεργασίας εφάρμοσε κατάλληλα τεχνικά και οργανωτικά μέτρα προστασίας, και τα μέτρα αυτά εφαρμόστηκαν στα επηρεαζόμενα από την παραβίαση ΔΠΧ και στη συνέχεια έλαβε μέτρα που διασφαλίζουν ότι δεν είναι πλέον πιθανό να προκύψει υψηλός κίνδυνος για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων. Λαμβάνονται υπόψη οι τελευταίες εξελίξεις, το κόστος εφαρμογής και η φύση, το πεδίο εφαρμογής, το πλαίσιο και οι σκοποί της επεξεργασίας, καθώς και οι κίνδυνοι διαφορετικής πιθανότητας επέλευσης και σοβαρότητας για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. Επίσης, ο ΓΚΠΔ απαιτεί να εφαρμόζονται όλα τα κατάλληλα μέτρα τεχνολογικής προστασίας και οργανωτικά μέτρα για τον άμεσο εντοπισμό κάθε παραβίασης δεδομένων προσωπικού χαρακτήρα και την άμεση ενημέρωση της εποπτικής αρχής και του υποκειμένου των δεδομένων.

Περιορισμός του συμβάντος

Το ενδεδειγμένο βήμα μετά το στάδιο της αναγνώρισης, είναι ο περιορισμός της βλάβης και η αποφυγή περαιτέρω διείσδυσης που μπορεί να προκαλέσει πρόσθετη ζημιά στον οργανισμό, έχοντας έτοιμες βραχυπρόθεσμες και μακροπρόθεσμες στρατηγικές περιορισμού, οι οποίες μπορεί να περιλαμβάνουν: την αποσύνδεση των επηρεαζόμενων συστημάτων από το δίκτυο ή την χρήση εφεδρικών συστημάτων για την επαναφορά των επιχειρησιακών λειτουργιών. Πρέπει να είναι κατανοητό ότι ο οργανισμός πιθανότατα θα παραμείνει σε κατάσταση έκτακτης ανάγκης μέχρι να περιέλθει η επίθεση και εξαλειφθούν το σύνολο των επιπτώσεων. Είναι επίσης, η κατάλληλη στιγμή για την ενημέρωση και την αναβάθμιση των συστημάτων, τον έλεγχο των πρωτοκόλλων απομακρυσμένης πρόσβασης, καθώς και της αλλαγής των διαπιστευτηρίων πρόσβασης χρηστών και διαχειριστών. Κατά το στάδιο του περιορισμού, πρέπει να είμαστε σε θέση να απαντήσουμε στις ακόλουθες ερωτήσεις:

[33] Κατευθυντήριες γραμμές Ομάδας Εργασίας Άρθρου 29 σχετικά με τη γνωστοποίηση παραβιάσεων δεδομένων προσωπικού χαρακτήρα δυνάμει του κανονισμού 2016/679, WP 250 rev.01 Ομάδας για την προστασία των προσώπων έναντι της επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα, https://www.dpa.gr/sites/default/files/2020-05/wp250rev01_el.pdf.

- Ποιες δράσεις λήφθησαν για να περιοριστεί η παραβίαση βραχυπρόθεσμα;
- Ποιες δράσεις λήφθησαν για να περιοριστεί η παραβίαση μακροπρόθεσμα;
- Έχει απομακρυνθεί πιθανό κακόβουλο λογισμικό από τα συστήματα;
- Τι είδους αντίγραφα ασφαλείας υπάρχουν;
- Αν έχουν επανεξετάσει όλα τα διαπιστευτήρια πρόσβασης για λόγους νομιμότητας και αλλαγής.
- Αν έχουν επιλεγεί κατάλληλα διαπιστευτήρια.
- Αν έχουν εφαρμοστεί όλες τις πρόσφατες ενημερώσεις και αναβαθμίσεις των συστημάτων.

Ενέργειες για τον περιορισμό

1) Αποσυνδέστε τον μολυσμένο Η/Υ από το δίκτυο αποσυνδέοντας το καλώδιο δικτύου.
2) Ακυρώστε την όποια διεργασία ή διαδικασία βρίσκεται σε εξέλιξη και διαγράψτε τα κακόβουλα λογισμικά και τα μολυσμένα αρχεία.
3) Προβείτε σε σάρωση όσο το δυνατόν περισσότερων Η/Υ με λογισμικό το οποίο έχει ενημερωθεί για τα στοιχεία του κακόβουλου λογισμικού με το οποίο έγινε η επίθεση προκειμένου να βεβαιωθείτε ποιοι είναι μολυσμένοι και να τους απομονώσετε από το δίκτυο.
4) Απενεργοποιήστε ή διαγράψτε το κοινόχρηστο στοιχείο ή αρχεία σε διακομιστές αρχείων. Η πρόσβαση στο διακομιστή αρχείων πρέπει να τερματιστεί.
5) Εάν το κακόβουλο λογισμικό διείσδυσε μέσω ηλεκτρονικού ταχυδρομείου, πρέπει να καθαριστεί από ολόκληρο το «κουτί» του ηλεκτρονικού ταχυδρομείου όλων των χρηστών στους οποίους διανεμήθηκες ή κοινοποιήθηκε το ηλεκτρονικό μήνυμα. Εάν διείσδυσε μετά από την επίσκεψη ενός διαδικτυακού τόπου θα πρέπει να ενημερωθεί το προσωπικό να αποφεύγει τον συγκεκριμένο διαδικτυακό τόπο, να τοποθετηθούν φραγμοί και να παρακολουθείται το σύστημα προκειμένου να εμποδιστεί η εκ νέου πρόσβαση.
6) Οι κωδικοί ασφαλείας όλων των μολυσμένων Η/Υ πρέπει να αλλάξουν.

Διαγραφή/εξάλειψη του συμβάντος

Άπαξ και το περιστατικό έχει περιοριστεί, πρέπει να εντοπιστεί και να εξαλειφθεί η βασική αιτία του περιστατικού ασφάλειας. Θα πρέπει, με άλλα λόγια να εξουδετερωθεί η απειλή και να ολοκληρωθεί η αποκατάσταση των εσωτερικών συστημάτων όσο το δυνατόν πλησιέστερα στην προηγούμενη κατάστασή τους. Αυτό σημαίνει ότι όλα τα κακόβουλα προγράμματα θα πρέπει να απομακρυνθούν με

ασφάλεια, τα συστήματα θα πρέπει να διορθωθούν και θα πρέπει να εφαρμοστούν ενημερώσεις. Επίσης, το στάδιο αυτό μπορεί να περιλαμβάνει τη δευτεροβάθμια παρακολούθηση για να εξασφαλιστεί ότι τα επηρεαζόμενα συστήματα δεν είναι πλέον ευάλωτα σε επακόλουθη επίθεση.

Ενέργειες Διαγραφής/Εξάλειψης

1) Βεβαιωθείτε ότι έχετε εντοπίσει όλα τα σημεία στα οποία είχε πρόσβαση το κακόβουλο λογισμικό ή έλαβε χώρα το περιστατικό.
2) Αναζητήσετε ένα ασφαλές αντίγραφο ασφαλείας, το οποίο πρέπει να έχει δημιουργηθεί πριν από το περιστατικό.
3) Αφαιρέστε το κακόβουλο λογισμικό από τα συστήματα και τις συσκευές.

Ανάκαμψη από το συμβάν

Αυτό είναι το στάδιο αποκατάστασης και επιστροφής των επηρεαζόμενων συστημάτων και συσκευών σε περιβάλλον παραγωγής. Κατά τη διάρκεια αυτής της φάσης, είναι σημαντικό να επανέλθουν τα συστήματά και οι επιχειρηματικές λειτουργίες χωρίς τον φόβο μιας άλλης παραβίασης.

Ενέργειες Ανάκαμψης

Το Τμήμα Υπολογιστικού Κέντρου και η Ομάδα:

1) αποκαθιστούν το σύστημα από ασφαλή αντίγραφα ασφαλείας,
2) ανακατασκευάζουν το σύστημα από την αρχή και εφαρμόζουν επιδιορθώσεις,
3) αλλάζουν κωδικούς πρόσβασης και ενημερώνουν τους κανόνες διαμόρφωσης του τείχους προστασίας και του δρομολογητή και
4) επαναφέρουν τα συστήματα αξιοποιώντας ένα ασφαλές και καθαρό αρχείο από τα διαθέσιμα αντίγραφα ασφαλείας.

Σχέδιο Ανάκαμψης

Το στάδιο Ανάκαμψης, όπως ήδη έχει αναφερθεί ανωτέρω, αποτελεί μέρος της διαχείρισης του περιστατικού ασφαλείας. Ειδικότερα, στο συγκεκριμένο στάδιο περιλαμβάνονται μέτρα ανάκαμψης και αποκατάστασης πληροφοριακών συστημάτων και τεχνολογικών υποδομών σε περιπτώσεις έκτακτης ανάγκης, όπως φυσικές καταστροφές, εξωτερικές επιθέσεις/εισβολές, κ.λπ.

Περιεχόμενο

Το σχέδιο αυτό είναι απαραίτητο για την αποτύπωση των διαδικασιών και των τεχνικών μέτρων που πρέπει να εφαρμόσει ο υπεύθυνος επεξεργασίας (ο Οργανισμός) για την προστασία των ΔΠΧ σε περίπτωση κάποιου έκτακτου περιστατικού. Οι

διαδικασίες αυτές θα πρέπει να προβλέπουν σενάρια διακοπής της επιχειρησιακής λειτουργίας του οργανισμού και τον τρόπο ανάκαμψης/συνέχισης αυτής.
Τα μέτρα που λαμβάνονται στα πλαίσια του σχεδίου ανάκαμψης θα πρέπει να στοχεύουν:

- στην ελαχιστοποίηση διακοπών της κανονικής λειτουργίας του Οργανισμού,
- στον περιορισμό της έκτασης των ζημιών και καταστροφών και αποφυγή πιθανής κλιμάκωσης αυτών,
- στη δυνατότητα ομαλής υποβάθμισης,
- στην εγκατάσταση εναλλακτικών μέσων λειτουργίας εκ των προτέρων,
- στην εκπαίδευση, εξάσκηση και εξοικείωση του ανθρώπινου δυναμικού με διαδικασίες έκτακτης ανάγκης,
- στη δυνατότητα ταχείας και ομαλής αποκατάστασης της λειτουργίας και
- στην ελαχιστοποίηση των οικονομικών επιπτώσεων.

Στο σχέδιο ανάκαμψης πρέπει να προσδιορίζονται οι πιθανοί κίνδυνοι και γενικότερα τα κριτήρια που καθορίζουν την κατάσταση ως έκτατη και επιβάλλουν την ενεργοποίησή του. Πρέπει να υπάρχουν σαφείς και γραπτές διαδικασίες που να θέτουν τον Οργανισμό σε κατάσταση έκτακτης ανάγκης. Επίσης, το σχέδιο ανάκαμψης πρέπει να ελέγχεται περιοδικά προκειμένου να διαπιστώνεται η αποτελεσματικότητα των μεθόδων ανάκαμψης. Οι έλεγχοι πρέπει να καλύπτουν όλο το εύρος, τις διαδικασίες και τα δεδομένα των συστημάτων.

Συμμετοχή ΥΠΔ στη διαδικασία

Όπως, ήδη αναφέρεται ανωτέρω (βλ. Ομάδα Διαχείρισης Περιστατικών) ο ΥΠΔ, αποτελεί μέρος της Ομάδας. Τα υποχρεωτικά καθήκοντα του ΥΠΔ, που έχουν ιδιαίτερη συνάφεια με τη γνωστοποίηση της παραβίασης, περιλαμβάνουν, μεταξύ άλλων, την παροχή συμβουλών και πληροφοριών για την προστασία των ΔΠΧ στον υπεύθυνο επεξεργασίας (Οργανισμός), την παρακολούθηση της συμμόρφωσης με τον ΓΚΠΔ και την παροχή συμβουλών όσον αφορά τις ΕΑΠΔ (Εκτίμηση Αντικτύπου Προστασίας Δεδομένων). Ο ΥΠΔ πρέπει, επίσης, να συνεργάζεται με την εποπτική αρχή (ΑΠΔΠΧ) και να λειτουργεί ως σημείο επαφής για την εποπτική αρχή και τα υποκείμενα των δεδομένων. Θα πρέπει να σημειωθεί επίσης ότι, κατά τη γνωστοποίηση της παραβίασης στην εποπτική αρχή, το άρθρο 33 παράγραφος 3 στοιχείο β) απαιτεί από τον υπεύθυνο επεξεργασίας να παρέχει το όνομα και τα στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων του ή άλλου σημείου επικοινωνίας[34].

[34] Κατευθυντήριες γραμμές Ομάδας Εργασίας Άρθρου 29 σχετικά με τη γνωστοποίηση παραβιάσεων δεδομένων προσωπικού χαρακτήρα δυνάμει του κανονισμού 2016/679, WP 250 rev.01 Ομάδας για την προστασία των προσώπων έναντι της επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα, https://www.dpa.gr/sites/default/files/2020-05/wp250rev01_el.pdf.

Όσον αφορά την τεκμηρίωση των παραβιάσεων, ο υπεύθυνος επεξεργασίας μπορεί να επιθυμεί να λάβει τη γνώμη του ΥΠΔ του όσον αφορά τη δομή, την ανάπτυξη και τη διαχείριση αυτής της τεκμηρίωσης. Ως εκ τούτου, ο ΥΠΔ μπορεί να διαδραματίζει σημαντικό ρόλο ως προς την αποτροπή μιας παραβίασης ή την προετοιμασία για την αντιμετώπιση μιας παραβίασης, παρέχοντας συμβουλές και παρακολουθώντας τη συμμόρφωση, καθώς και κατά τη διάρκεια μιας παραβίασης (δηλαδή κατά τη γνωστοποίηση στην εποπτική αρχή) και κατά τη διάρκεια οποιασδήποτε μεταγενέστερης έρευνας από την εποπτική αρχή (ΑΠΔΠΧ)[35].

Ενέργειες ενημέρωσης ΥΠΔ

1) Μόλις γίνει αντιληπτό κάτι που μπορεί να θεωρηθεί ως περιστατικό ασφαλείας, ο υπεύθυνος επεξεργασίας (ο Οργανισμός) από κοινού με την Ομάδα, οφείλει να συγκεντρώσει όσες περισσότερες πληροφορίες μπορεί για το περιστατικό, χωρίς να κάνει καμιά προσπάθεια να το σταματήσει ή να το επεξηγήσει, ώστε να επικοινωνήσει με τον ΥΠΔ του Οργανισμού.
2) Κατά τη συγκεκριμένη επικοινωνία, θα πρέπει να παρασχεθούν όσο το δυνατόν περισσότερες πληροφορίες, ώστε να εκτιμηθεί η κατάσταση από τον ΥΠΔ και να δοθούν οι ανάλογες λύσεις. Στη συνέχεια του εγγράφου (βλ. Παράρτημα Α) παρατίθενται πληροφορίες, τις οποίες πρέπει να λάβει ο ΥΠΔ (οι πληροφορίες αυτές αποτελούν ελάχιστη ενημέρωση προς τον ΥΠΔ).

Μετά το συμβάν

Καταγραφή του Συμβάντος

Οι ενέργειες μετά το συμβάν έχουν ως στόχο ο Οργανισμός να μάθει από το περιστατικό και να βελτιώσει τις διαδικασίες και τα στάδια του Πλάνου προκειμένου να διαχειριστεί αποτελεσματικά τον χρόνο και να μειώσει το κόστος. Ο Οργανισμός πραγματοποιεί συνάντηση με όλα τα εμπλεκόμενα μέρη και συζητά όλες τις πτυχές του συμβάντος ή του περιστατικού και τον αντίκτυπό τους στον Οργανισμό. Στη συνάντηση, απαντώνται οι παρακάτω ερωτήσεις:

- Τι τύπος συμβάντος ή περιστατικού ήταν και πότε πραγματικά επήλθε ή/και έγινε γνωστό;
- Πόσο αποτελεσματικά ενήργησε η Ομάδα και η Διοίκηση;
- Το συμβάν και το περιστατικό μαζί με τις σχετικές ενέργειες τεκμηριώνονται;
- Ποια μέτρα και δράσεις έχουν ληφθεί;
- Ποια διαφορετικά βήματα ή στρατηγικές θα μπορούσαν να ακολουθηθούν σε παρόμοιο ή ίδιο περιστατικό στο μέλλον;

[35] Ομοίως με υπ. 11.

- Πόσο γρήγορη και αποτελεσματική ήταν η επικοινωνία και η πληροφόρηση της Ομάδας;

Ενέργειες καταγραφής

Κατά τη διάρκεια αυτού του σταδίου, η Ομάδα και οι συνεργάτες της:

1) συναντώνται για να καθορίσουν τον τρόπο βελτίωσης των μελλοντικών προσπαθειών αντιμετώπισης περιστατικών αξιολογώντας:
   - οι τρέχουσες πολιτικές και διαδικασίες,
   - αποφάσεις που έλαβε η Ομάδα κατά τη διάρκεια του συμβάντος και
   - οι παράγοντες που λειτούργησαν με επιτυχία στο σχέδιο αντιμετώπισης, καθώς και εντοπίστηκαν κενά,
2) καταρτίζουν έκθεση που θα χρησιμοποιηθεί για μελλοντική χρήση, και πρέπει αν περιλαμβάνει κατ' ελάχιστον:
   - απαραίτητες αλλαγές στην πολιτική ασφάλειας και τις σχετικές διαδικασίες,
   - αναγκαίες αλλαγές στην εκπαίδευση των εργαζομένων,
   - καταγραφή των αδυναμιών που έγιναν αντικείμενο εκμετάλλευσης κατά την διάρκεια του περιστατικού ασφάλειας και
   - μέτρα αποτροπής παρόμοιας παραβίασης.

Αρχείο καταγραφής

«Ο υπεύθυνος επεξεργασίας (Οργανισμός) *τεκμηριώνει κάθε παραβίαση δεδομένων προσωπικού χαρακτήρα, που συνίστανται στα πραγματικά περιστατικά που αφορούν την παραβίαση δεδομένων προσωπικού χαρακτήρα, τις συνέπειες και τα ληφθέντα διορθωτικά μέτρα. Η εν λόγω τεκμηρίωση επιτρέπει στην εποπτική αρχή να επαληθεύει τη συμμόρφωση προς το παρόν άρθρο»*[36].

Αυτό συνδέεται με την αρχή της λογοδοσίας του ΓΚΠΔ. Ο σκοπός της καταγραφής μη γνωστοποιήσεων αλλά και γνωστοποιήσεων παραβιάσεων συνδέεται επίσης με τις υποχρεώσεις του υπευθύνου επεξεργασίας. Η εποπτική αρχή μπορεί να ζητήσει να δει αυτά τα αρχεία.

Ο υπεύθυνος επεξεργασίας (Οργανισμός) μπορεί να επιλέξει να καταγράφει τις παραβιάσεις στο αρχείο των δραστηριοτήτων επεξεργασίας που τηρεί σύμφωνα με τον ΓΚΠΔ[37]. Δεν απαιτείται η τήρηση ξεχωριστού μητρώου, υπό την προϋπόθεση ότι οι πληροφορίες που αφορούν την παραβίαση είναι σαφώς αναγνωρίσιμες και μπορούν να εξαχθούν κατόπιν αιτήματος.

[36] Αρ. 33, §5, ΓΚΠΔ.
[37] Αρ. 30, ΓΚΠΔ.

Πληροφορίες για την τεκμηρίωση της καταγραφής

Παρότι εναπόκειται στον υπεύθυνο επεξεργασίας (Οργανισμός) να καθορίζει τη μέθοδο και τη δομή που θα χρησιμοποιεί κατά την τεκμηρίωση μιας παραβίασης, υπάρχουν ορισμένα βασικά στοιχεία που θα πρέπει να περιλαμβάνονται σε κάθε περίπτωση όσον αφορά τις πληροφορίες που πρέπει να καταγράφονται. Συγκεκριμένα θα πρέπει να καταγράφονται:

- λεπτομέρειες σχετικά με την παραβίαση (αιτίες, ΔΠΧ που επηρεάζονται),
- αποτελέσματα και τις συνέπειες της παραβίασης,
- διορθωτικά μέτρα που ελήφθησαν,
- το σκεπτικό (του υπευθύνου επεξεργασίας) για τις αποφάσεις που λαμβάνει για την αντιμετώπιση μιας παραβίασης[38].

[38] Κατευθυντήριες γραμμές Ομάδας Εργασίας Άρθρου 29 σχετικά με τη γνωστοποίηση παραβιάσεων δεδομένων προσωπικού χαρακτήρα δυνάμει του κανονισμού 2016/679, WP 250 rev.01 Ομάδας για την προστασία των προσώπων έναντι της επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα**,** https://www.dpa.gr/sites/default/files/2020-05/wp250rev01_el.pdf: *«Εάν μια παραβίαση δεν γνωστοποιηθεί, θα πρέπει να καταγράφεται μια τεκμηριωμένη αιτιολόγηση για αυτή την απόφαση. Αυτή η αιτιολόγηση θα πρέπει να περιλαμβάνει τους λόγους για τους οποίους ο υπεύθυνος επεξεργασίας θεωρεί ότι η παραβίαση δεν ενδέχεται να επιφέρει κίνδυνο για τα δικαιώματα και τις ελευθερίες των προσώπων».*

Κωδικός Διαδικασίας	1.0	**Έκδοση**	1.0	**Σχετικά Πρότυπα**	*Ν. 4961/2022, ISO/IEC 27001:2013, Γενικός Κανονισμός, Προστασίας Δεδομένων, ENISA (Consumerization of IT), Οδηγίες της ΑΠΔΠΧ*
Σχετικές Απαιτήσεις	*Συμμόρφωση Δήμου Περάματος με τον Ν. 4961/2022*				

Παράρτημα Α

Ημερομηνία Περιστατικού:	Γράφεται η ημερομηνία αναφοράς του περιστατικού
Στοιχεία Αναφέροντος:	Τα στοιχεία του μέλους της Ομάδα Διαχείρισης περιστατικού του Οργανισμού που αναφέρει το περιστατικό
Τι συνέβη:	Με απλά λόγια περιγράφεται τι εντόπισε το μέλος της Ομάδα Διαχείρισης περιστατικού του Οργανισμού
Πώς συνέβη:	Το στέλεχος περιγράφει τον τρόπο που έλαβε χώρα το περιστατικό
Γιατί συνέβη:	Το μέλος της Ομάδα Διαχείρισης περιστατικού του Οργανισμού δίνει μια πρώτη ερμηνεία για το περιστατικό
Τι επηρεάστηκε:	Περιγράφονται από το μέλος της Ομάδα Διαχείρισης περιστατικού του Οργανισμού οι πόροι που επηρεάστηκαν από το περιστατικό
Τρωτά σημεία:	Γράφονται από το μέλος της Ομάδα Διαχείρισης περιστατικού τα τρωτά σημεία της ασφάλειας του Οργανισμού που κατά μια πρώτη ερμηνεία αποτέλεσαν την αιτία για το περιστατικό
Συνέβη, Εντοπίστηκε, Αναφέρθηκε:	Συμπληρώνονται από το μέλος της Ομάδα Διαχείρισης περιστατικού του Οργανισμού οι σχετικές ημερομηνίες
Τελείωσε:	Επιλέγεται ΟΧΙ αν το μέλος της Ομάδα Διαχείρισης περιστατικού θεωρεί ότι το περιστατικό είναι σε εξέλιξη και ΝΑΙ αν θεωρεί ότι έχει λήξει
Συνολική διάρκεια:	Σε περίπτωση που το περιστατικό έχει λήξει, συμπληρώνεται η συνολική του διάρκεια, σε αντίθετη περίπτωση συμπληρώνεται η ώρα που η Ομάδα Διαχείρισης περιστατικού έλαβε γνώση για αυτό

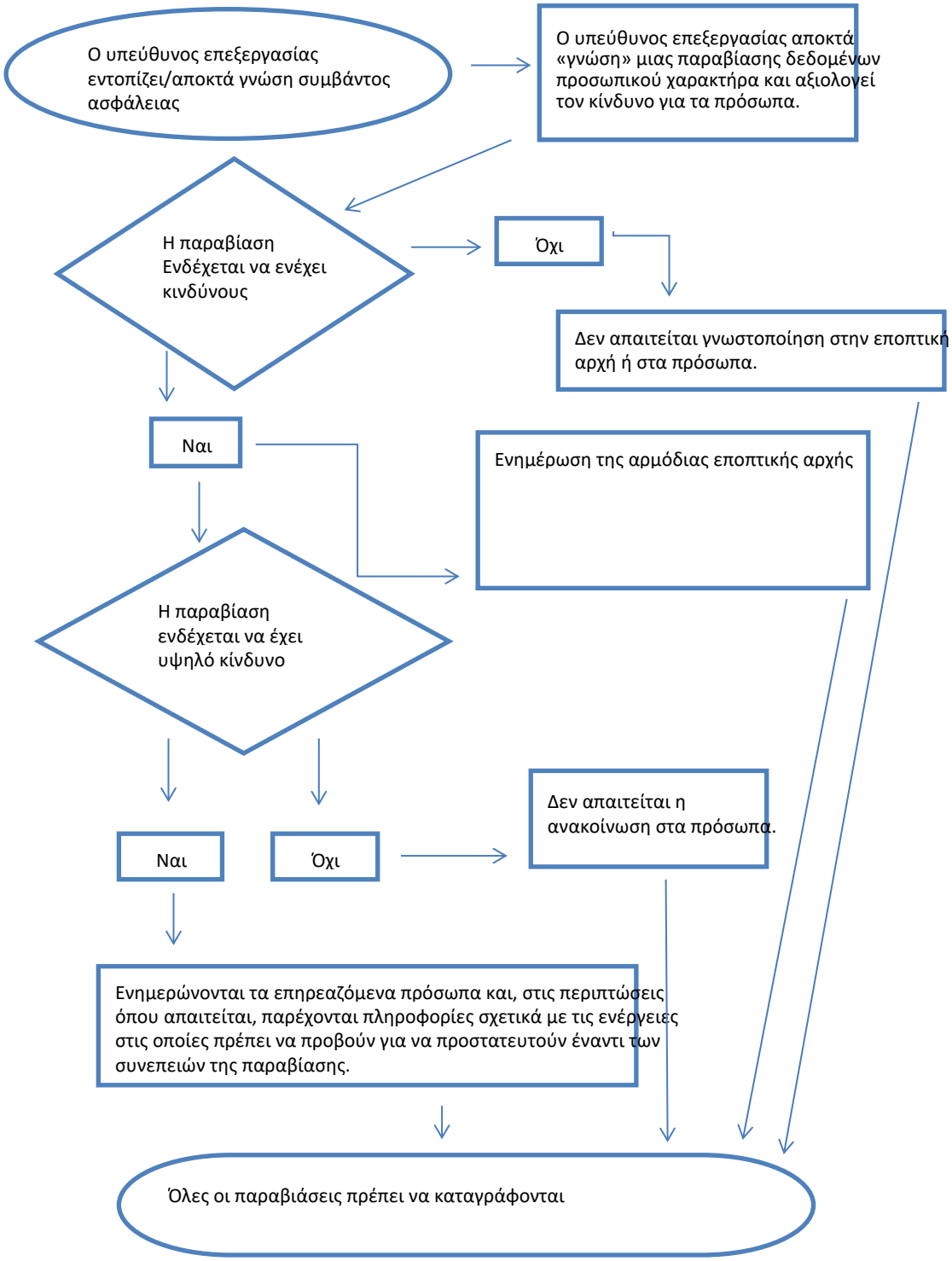
Παράρτημα Β

Παράδειγμα	Γνωστοποίηση στην εποπτική αρχή;	Ανακοίνωση στο υποκείμενο των δεδομένων;	Σημειώσεις/συστάσεις
Ένας υπεύθυνος επεξεργασίας αποθήκευσε αντίγραφο ασφαλείας αρχείου δεδομένων προσωπικού χαρακτήρα σε κρυπτογραφημένη μορφή σε κλειδί USB. Το κλειδί εκλάπη κατά τη διάρκεια διάρρηξης.	Όχι.	Όχι	Εφόσον τα δεδομένα έχουν κρυπτογραφηθεί με αλγόριθμο προηγμένης τεχνολογίας, υπάρχουν αντίγραφα ασφαλείας των δεδομένων, το μοναδικό κλειδί δεν έχει τεθεί σε κίνδυνο και είναι δυνατή η επαναφορά των δεδομένων εγκαίρως, αυτό ενδέχεται να μην συνιστά παραβίαση που πρέπει να αναφερθεί. Ωστόσο, εάν τεθεί σε κίνδυνο σε μεταγενέστερο στάδιο, απαιτείται γνωστοποίηση.
Ένας υπεύθυνος επεξεργασίας διατηρεί μια ηλεκτρονική υπηρεσία. Ως αποτέλεσμα επίθεσης στον κυβερνοχώρο σε αυτή την υπηρεσία, αποσπώνται δεδομένα προσωπικού χαρακτήρα προσώπων. Ο υπεύθυνος επεξεργασίας έχει πελάτες σε ένα μόνο κράτος μέλος.	Ναι, ενημερώνεται η εποπτική αρχή εάν είναι πιθανό να υπάρχουν συνέπειες για πρόσωπα.	Ναι, ενημερώνονται τα πρόσωπα ανάλογα με τη φύση των δεδομένων προσωπικού χαρακτήρα που επηρεάζονται και εάν η σοβαρότητα των ενδεχόμενων συνεπειών για τα πρόσωπα είναι μεγάλη.	

Ένας υπεύθυνος επεξεργασίας έχει υποστεί επίθεση από λογισμικό, η οποία είχε ως αποτέλεσμα την κρυπτογράφηση όλων των δεδομένων. Δεν υπάρχουν διαθέσιμα αντίγραφα ασφαλείας και δεν είναι δυνατή η ανάκτηση των δεδομένων. Από την έρευνα κατέστη σαφές ότι η μοναδική λειτουργία του λογισμικού ήταν η κρυπτογράφηση των δεδομένων και ότι δεν υπήρχε άλλο κακόβουλο λογισμικό στο σύστημα.	Ναι, το συμβάν αναφέρεται στην εποπτική αρχή, εάν υπάρχουν ενδεχόμενες συνέπειες για τα πρόσωπα, δεδομένου ότι πρόκειται για απώλεια της διαθεσιμότητας.	Ναι, το συμβάν αναφέρεται στα πρόσωπα, ανάλογα με τη φύση των δεδομένων προσωπικού χαρακτήρα που επηρεάζονται και τις ενδεχόμενες συνέπειες της έλλειψης διαθεσιμότητας των δεδομένων, καθώς και άλλες ενδεχόμενες συνέπειες.	Αν υπήρχε διαθέσιμο αντίγραφο ασφαλείας και ήταν δυνατή η έγκαιρη επαναφορά των δεδομένων, δεν θα απαιτούταν η αναφορά στην εποπτική αρχή ή στα πρόσωπα, καθώς δεν θα επρόκειτο για μόνιμη απώλεια της διαθεσιμότητας ή της εμπιστευτικότητας. Ωστόσο, εάν η εποπτική αρχή έλαβε γνώση του συμβάντος με άλλα μέσα, μπορεί να εξετάσει το ενδεχόμενο να διεξαγάγει έρευνα για την αξιολόγηση της συμμόρφωσης με τις απαιτήσεις του άρθρου 32 για την ευρύτερη ασφάλεια.

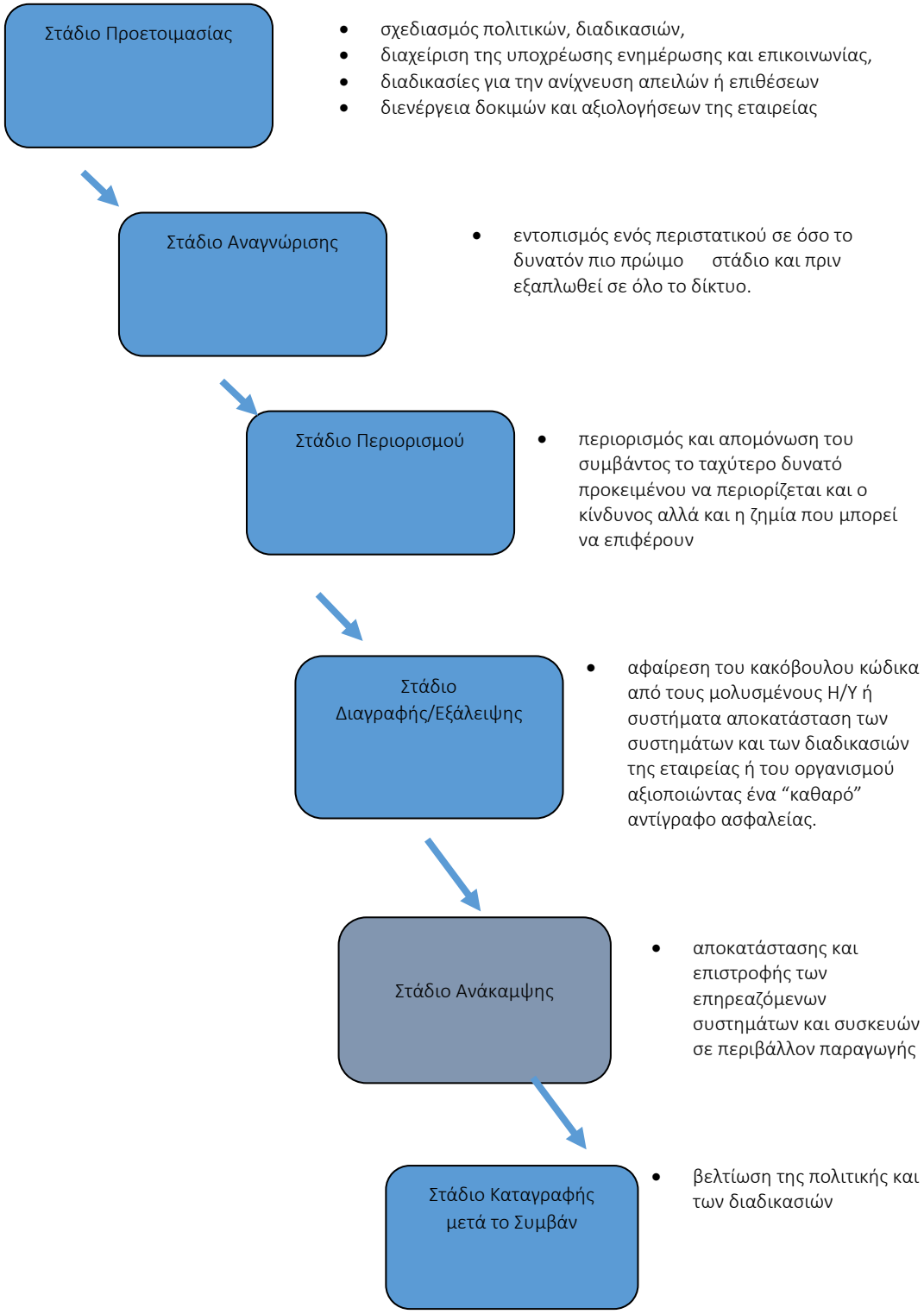
Παράρτημα Γ

Διάγραμμα ροής που απεικονίζει τις απαιτήσεις γνωστοποίησης


Ο υπεύθυνος επεξεργασίας εντοπίζει/αποκτά γνώση συμβάντος ασφάλειας
Ο υπεύθυνος επεξεργασίας αποκτά «γνώση» μιας παραβίασης δεδομένων προσωπικού χαρακτήρα και αξιολογεί τον κίνδυνο για τα πρόσωπα.
Η παραβίαση Ενδέχεται να ενέχει κινδύνους
Όχι
Δεν απαιτείται γνωστοποίηση στην εποπτική αρχή ή στα πρόσωπα.
Ναι
Ενημέρωση της αρμόδιας εποπτικής αρχής
Η παραβίαση ενδέχεται να έχει υψηλό κίνδυνο
Ναι
Όχι
Δεν απαιτείται η ανακοίνωση στα πρόσωπα.
Ενημερώνονται τα επηρεαζόμενα πρόσωπα και, στις περιπτώσεις όπου απαιτείται, παρέχονται πληροφορίες σχετικά με τις ενέργειες στις οποίες πρέπει να προβούν για να προστατευτούν έναντι των συνεπειών της παραβίασης.
Όλες οι παραβιάσεις πρέπει να καταγράφονται

Παράρτημα Δ

Διάγραμμα ενεργειών αντίδρασης σε περίπτωση συμβάντος

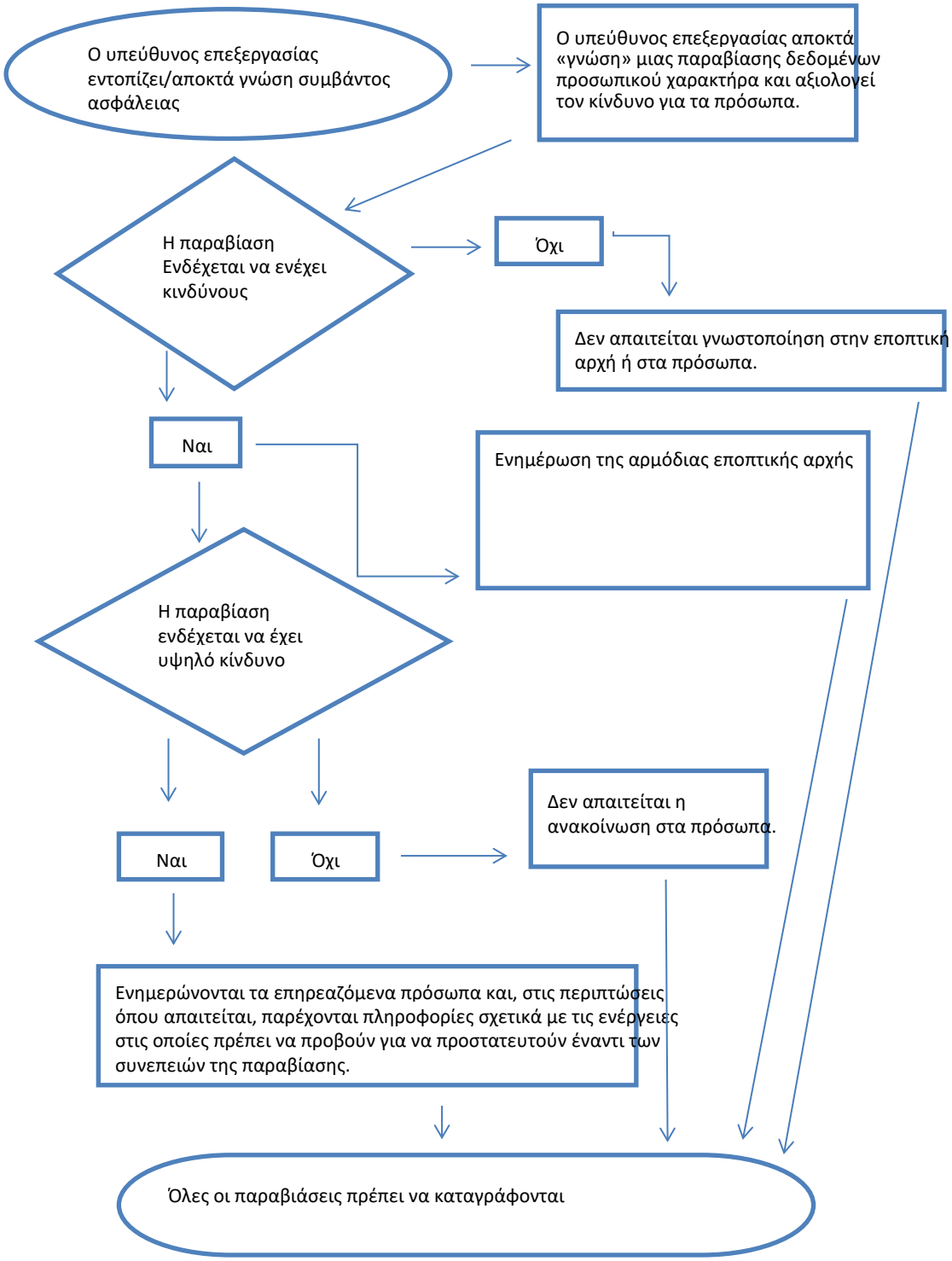


απόκρισης και διαχείρισης για μελλοντικά περιστατικά.

- αξιολόγηση της στρατηγική διαχείρισης

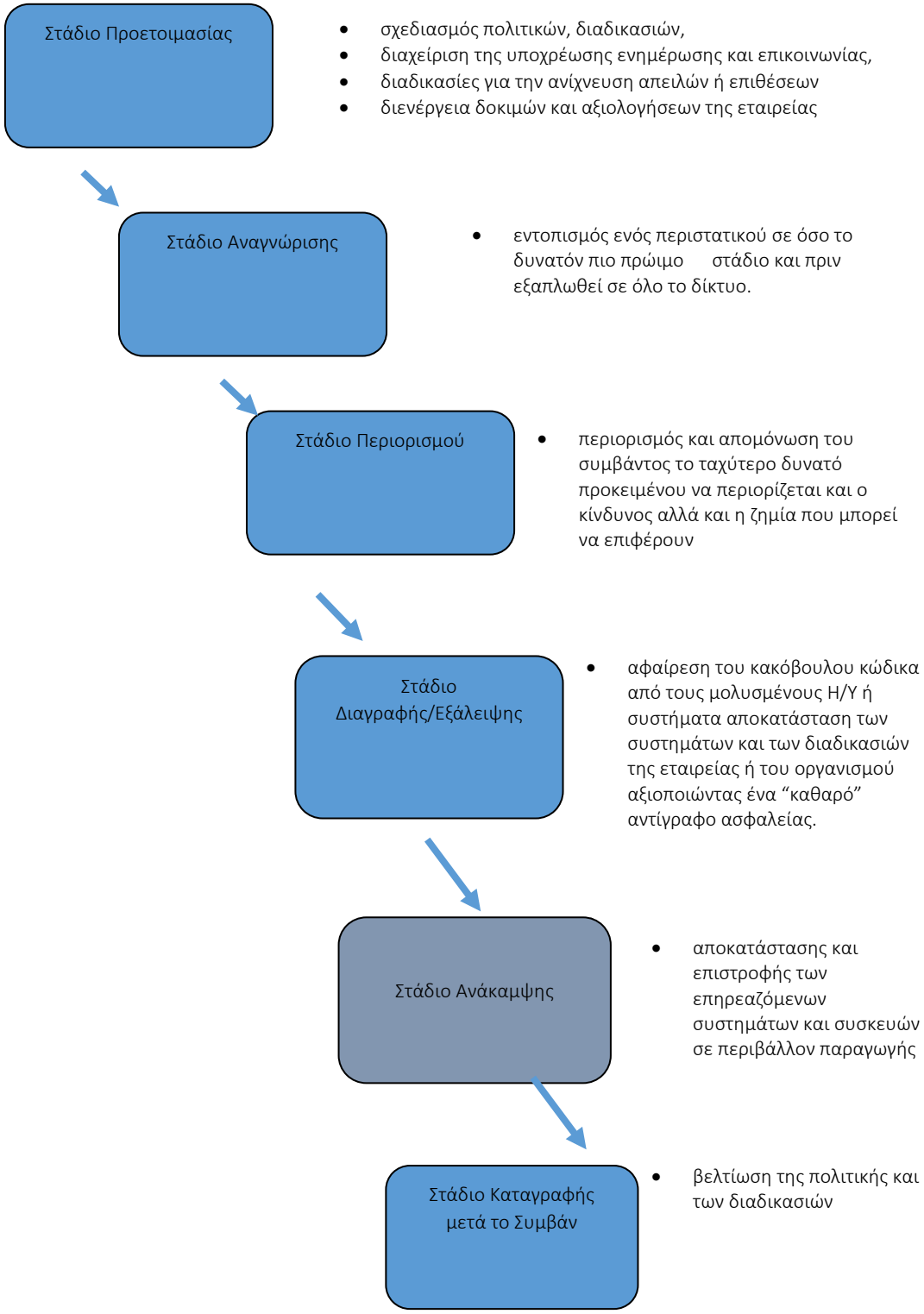
Παράρτημα Γ

Διάγραμμα ροής που απεικονίζει τις απαιτήσεις γνωστοποίησης


Ο υπεύθυνος επεξεργασίας εντοπίζει/αποκτά γνώση συμβάντος ασφάλειας
Ο υπεύθυνος επεξεργασίας αποκτά «γνώση» μιας παραβίασης δεδομένων προσωπικού χαρακτήρα και αξιολογεί τον κίνδυνο για τα πρόσωπα.
Η παραβίαση Ενδέχεται να ενέχει κινδύνους
Όχι
Δεν απαιτείται γνωστοποίηση στην εποπτική αρχή ή στα πρόσωπα.
Ναι
Ενημέρωση της αρμόδιας εποπτικής αρχής
Η παραβίαση ενδέχεται να έχει υψηλό κίνδυνο
Ναι
Όχι
Δεν απαιτείται η ανακοίνωση στα πρόσωπα.
Ενημερώνονται τα επηρεαζόμενα πρόσωπα και, στις περιπτώσεις όπου απαιτείται, παρέχονται πληροφορίες σχετικά με τις ενέργειες στις οποίες πρέπει να προβούν για να προστατευτούν έναντι των συνεπειών της παραβίασης.
Όλες οι παραβιάσεις πρέπει να καταγράφονται

Παράρτημα Δ

Διάγραμμα ενεργειών αντίδρασης σε περίπτωση συμβάντος



Κωδικός Διαδικασίας	1.0	**Έκδοση**	1.0	**Σχετικά Πρότυπα**	*Ν. 4961/2022, ISO/IEC 27001:2013, Γενικός Κανονισμός, Προστασίας Δεδομένων, ENISA (Consumerization of IT), Οδηγίες της ΑΠΔΠΧ*
Σχετικές Απαιτήσεις	*Συμμόρφωση Δήμου Περάματος με τον Ν. 4961/2022*				

απόκρισης και διαχείρισης για μελλοντικά περιστατικά.

- αξιολόγηση της στρατηγική διαχείρισης

6.6 Πολιτική Φυσικής και Περιβαλλοντικής Ασφάλειας

Εισαγωγή

Κάθε χρήστης των Πληροφοριακών Συστημάτων (Π.Σ.) του Δήμου Περάματος (εφεξής «Οργανισμός» ή Φορέας) θα πρέπει να συνεισφέρει στην ασφάλεια πληροφοριών και των υποδομών με την ορθή χρήση των πόρων τους και να τηρεί θεμελιώδεις κανόνες ορθής χρήσης και δεοντολογίας.

Σκοπός

Ο σκοπός της παρούσας Πολιτικής, είναι η διατήρηση της φυσικής ασφάλειας των εγκαταστάσεων του Οργανισμού, με σκοπό την προστασία των φυσικών και πληροφοριακών αγαθών του, από την απώλεια της εμπιστευτικότητας ή/και της ακεραιότητας ή/και της διαθεσιμότητας.

Έχοντας ως στόχο την αντιμετώπιση των δυσμενέστερων σεναρίων, η δημιουργία και εφαρμογή της παρούσας πολιτικής αποτελεί μία από τις προϋποθέσεις συμμόρφωσης με την κείμενη νομοθεσία περί ασφάλειας πληροφοριών και προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΔΠΧ) συγκεκριμένα:

- *τις διατάξεις του Ν. 4961/2022 (ΦΕΚ Α' 146/27.07.2022)*[39]
- *τις διατάξεις του Κανονισμού (ΕΕ) 2016/679 (GDPR/ΓΚΠΔ)* [40]*,*
- *τις διατάξεις του Ν. 4624/2019 (ΦΕΚ Α' 137/29.08.2019)* [41]

[39] Νόμος υπ' αριθμ. 4961/2022 Τεύχος Α' 146/27.07.2022: Αναδυόμενες τεχνολογίες πληροφορικής και επικοινωνιών, ενίσχυση της ψηφιακής διακυβέρνησης και άλλες διατάξεις.
[40] Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων).
[41] Νόμος υπ' αριθμ. 4624 Τεύχος Α' 137/29.08.2019, Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 και άλλες διατάξεις.

Τα πλεονεκτήματα από την υιοθέτηση και εφαρμογή της παρούσας Πολιτικής είναι πολλαπλά και μακροπρόθεσμα ωφέλιμα για τον Οργανισμό. Ειδικότερα, η εφαρμογή της Πολιτικής:

- Περιορίζει τη νομική έκθεση του Οργανισμού και τον προστατεύει από νομικές ενέργειες που τυχόν ασκηθούν εναντίον του, παρέχοντας στο προσωπικό εκ των προτέρων ειδοποίηση για τους κανονισμούς και τις πολιτικές που πρέπει να ακολουθούνται.
- Περιορίζει την ατομική και ιδία χρήση των πόρων και των υποδομών που παρέχονται από τον Οργανισμό.
- Συμβάλλει στη διαχείριση του κόστους μειώνοντας την ποσότητα των πόρων που χρησιμοποιούνται, όπως η αποθήκευση και το εύρος ζώνης.
- Συμβάλλει στην προστασία των πόρων και των δεδομένων των υπολογιστών ενός οργανισμού από κυβερνοεπιθέσεις και άλλες μορφές κλοπής ή διαρροής δεδομένων.
- Βοηθά στην πρόληψη παραβιάσεων συμμόρφωσης με ισχύοντες κανονισμούς και νομοθεσίες.
- Χρησιμεύει για την προστασία του Οργανισμού από τις σκόπιμες ή τυχαίες δραστηριότητες του εργατικού δυναμικού του.

Πεδίο εφαρμογής

Η συγκεκριμένη πολιτική πρέπει να εφαρμόζεται σε όλα τα συστήματα, διαδικασίες και χρήστες του Οργανισμού, συμπεριλαμβανομένων των Διευθυντών, των Προϊσταμένων, των υπαλλήλων, των προμηθευτών και λοιπών τρίτων που έχουν πρόσβαση στα ΠΣ του Οργανισμού.

Βασικές αρχές ασφαλών χώρων

Ο σχεδιασμός ασφαλών χώρων είναι μία πολύπλοκη διαδικασία που απαιτεί την πλήρη και ολοκληρωμένη αξιολόγηση κινδύνων ώστε να εντοπιστούν οι πιθανές απειλές μη εξουσιοδοτημένης πρόσβασης και ο τρόπος με τον οποίο αυτές πρέπει να αντιμετωπίζονται.

Το επίπεδο ασφάλειας που εφαρμόζεται σε κάθε χώρο πρέπει να είναι ανάλογο με τη διαβάθμιση των πληροφοριών που αποθηκεύονται ή επεξεργάζονται μέσα σε αυτό.

Περίμετρος φυσικής ασφάλειας

Το Computer Room (CR) και γενικά όλα τα συστήματα του Οργανισμού πρέπει να βρίσκονται διαχωρισμένα από τους υπόλοιπους χώρους του Οργανισμού, καθώς και από τους κοινόχρηστους χώρους ώστε να αποφεύγεται η πρόσβαση από μη εξουσιοδοτημένα πρόσωπα.

Η περίμετρος φυσικής ασφάλειας πρέπει να παρέχει πλήρη κάλυψη, χωρίς κενά ή αδυναμίες που να διευκολύνουν την είσοδο σε χώρους του Οργανισμού. Τα εξωτερικά παράθυρα πρέπει να είναι ασφαλή, κλειδωμένα και να προστατεύονται από κάγκελα, όπου αυτό χρειάζεται. Οι εξωτερικές πόρτες του CR πρέπει να είναι ασφαλείς και η πρόσβαση να επιτρέπεται μόνο σε εξουσιοδοτημένο προσωπικό.

Ειδική μέριμνα πρέπει να δοθεί για τους κανονισμούς πυρασφάλειας, καθώς και για την αποφυγή τυχόν περιβαλλοντικών απειλών (φωτιά, σεισμός, πλημμύρα κλπ.).

Χώροι υποδοχής-Έλεγχοι φυσικής εισόδου στον Οργανισμό

Η είσοδος και η έξοδος των επισκεπτών θα πρέπει να ελέγχεται με διακριτικότητα, μέσω της λειτουργίας είτε υπηρεσιών υποδοχής είτε τμημάτων γραμματείας.

Έλεγχοι πρόσβασης

Πρέπει να χρησιμοποιούνται κατάλληλοι έλεγχοι πρόσβασης σε όλα τα σημεία, όπου το επίπεδο ασφαλείας του Οργανισμού αλλάζει (πχ. είσοδος στο computer room).

Στο αρχείο Μητρώο Εξουσιοδοτημένου Προσωπικού πρέπει να καταγράφεται όλη η σχετική πληροφορία για την πρόσβαση των χρηστών στις ευαίσθητες εγκαταστάσεις του Οργανισμού. Πρέπει να γίνεται τακτική αναθεώρηση των δικαιωμάτων πρόσβασης, για να εξασφαλιστεί ότι αυτά παραμένουν επίκαιρα και αντικατοπτρίζουν τις ανάγκες του προσωπικού του Οργανισμού.

Το κτίριο όπου στεγάζονται τα πληροφοριακά συστήματα του Οργανισμού πρέπει να διαθέτει λίστα με όλους τους υπαλλήλους, ώστε να καταγράφεται η πρόσβασή τους σε ώρες μη εργάσιμες, αν αυτό απαιτηθεί.

Ασφάλεια γραφείων, δωματίων και εγκαταστάσεων

Στον χώρο του CR η πρόσβαση πρέπει να γίνεται με χρήση βιβλίου εισόδου. Μόνο συγκεκριμένοι υπάλληλοι του Οργανισμού πρέπει να έχουν πρόσβαση στο CR και να

καταγράφονται στο Αρχείο Εξουσιοδοτημένων Χρηστών έπειτα από έγκριση του Υπεύθυνου Ασφάλειας.

Κάθε κρίσιμη περιοχή πρέπει να σχεδιαστεί έτσι, ώστε ο εξοπλισμός σε περιοχές με εξυπηρετητές (πχ. CR) να μην είναι ορατός από δημόσιους χώρους. Οι οθόνες που μπορεί να εμφανίζουν ευαίσθητες πληροφορίες πρέπει να τοποθετούνται μακριά από όπου μη εξουσιοδοτημένα άτομα μπορεί να τις προσπελάσουν.

Όπου κρίνεται σκόπιμο, πρέπει να υλοποιείται πρόσθετη προστασία μέσα στις κρίσιμες περιοχές ενάντια σε απειλές όπως σκόνη, δονήσεις, ηλεκτρικές παρεμβολές και χημικές ουσίες.

Πρέπει να τηρείται πρόγραμμα συντήρησης για όλο τον κρίσιμο εξοπλισμό. Τα αντίγραφα και οι αναφορές συντήρησης πρέπει να αποθηκεύονται μαζί με τις αναφορές αστοχιών, καθώς και οι ανάλογες διορθωτικές ενέργειες.

Δεν επιτρέπεται η κατανάλωση φαγητού, ποτού και το κάπνισμα σε κρίσιμες περιοχές του Οργανισμού.

Προβλέπονται κατάλληλοι περιβαλλοντικοί έλεγχοι και ανάλογοι μηχανισμοί, όπως ο κλιματισμός. Η υγειονομική τους καταλληλόλητα πρέπει να παρακολουθείται σε συνεχή βάση.

Στο CR του Οργανισμού υπάρχει κλιματιστική μονάδα, ώστε να διασφαλίζεται η σωστή θερμοκρασία στο χώρο όπου είναι εγκατεστημένοι οι εξυπηρετητές.

Υποστηρικτικές παροχές

Έχει ληφθεί μέριμνα ώστε να εξασφαλιστούν υποστηρικτικές παροχές σε τομείς, όπως ηλεκτρική ενέργεια (UPS), τουλάχιστον για το computer room, και εξαερισμός (σύστημα αερισμού).

Χωρητικότητα κρίσιμων περιοχών

Η αξιολόγηση της χωρητικότητας κάθε κρίσιμης περιοχής πρέπει να πραγματοποιηθεί από εξειδικευμένο άτομο, κατά την εξέταση των απαιτήσεων της κρίσιμης περιοχής και του περιεχομένου της για τις υποστηρικτικές παροχές. Αυτό επιτρέπει την εκτιμώμενη χρήση, καθώς και επαρκή χώρο για ανάπτυξη.

Ασφάλεια καλωδίωσης

Τα καλώδια ρεύματος, φωνής, επικοινωνίας και δεδομένων πρέπει να προστατεύονται από φυσικές φθορές και καταστροφές.

Τα καλώδια πρέπει να φτάνουν, είτε υπόγεια, είτε μέσα από τοίχους ή ψευδοροφές. Επίσης, τα καλώδια πρέπει να τοποθετηθούν έτσι, ώστε να αποφεύγονται παρεμβολές.

Η καλωδίωση πρέπει να προστατεύεται ενάντια σε ηλεκτρομαγνητικές παρεμβολές, όπου αυτό θεωρείται αναγκαίο.

Η καλωδίωση δεν πρέπει να δρομολογείται μέσω κοινόχρηστων χώρων.

Πυροπροστασία

Μέτρα πρόληψης πυρκαγιών

Η κατασκευή των κτιρίων του Οργανισμού και ιδιαίτερα των δωματίων που περιέχουν ευαίσθητα ή κρίσιμα πληροφοριακά συστήματα, υποδομές και άλλα πληροφοριακά αγαθά πρέπει να αποτρέπει την έναρξη και την εξάπλωση πυρκαγιάς. Μερικά από τα προληπτικά μέτρα που μπορούν να εφαρμοστούν περιλαμβάνουν τη χρήση μη εύφλεκτων υλικών κατασκευής και την εγκατάσταση πυροσβεστήρων. Επιπλέον, όλες οι κρίσιμες πληροφορίες, σε ηλεκτρονική ή έντυπη μορφή, πρέπει να προστατεύονται κατά τη φύλαξή τους, κατά προτίμηση σε πυρίμαχες καμπίνες.

Όλα τα σχετικά μέτρα πρόληψης, όπως εφαρμογή της πολιτικής απαγόρευσης του καπνίσματος, αποφυγή αποθήκευσης εύφλεκτων υλικών και τακτική αφαίρεση τους, κ.λπ., υλοποιούνται.

Πιθανά εύφλεκτα υλικά πρέπει να αποθηκεύονται με ασφάλεια και σε επαρκή απόσταση από τους χώρους του Οργανισμού.

Οι πόρτες που διαχωρίζουν την πρόσβαση σε χώρους των ΠΣ πρέπει να είναι ανθεκτικές στην φωτιά.

Όλα τα απαραίτητα μέτρα πρέπει να τεθούν σε εφαρμογή, έτσι ώστε να εξασφαλιστεί πως ενδεχόμενη πυρκαγιά μπορεί να ελεγχθεί και να κατασταλεί άμεσα.

Συγκεκριμένα, πρέπει να υπάρχουν οι απαραίτητοι πυροσβεστήρες χειρός σύμφωνα με την αντίστοιχη νομοθεσία, καθώς και συναγερμός πυροπροστασίας σε όλο το κτίριο

του Οργανισμού. Οι πυροσβεστήρες πρέπει να αναγομώνονται τακτικά (μία φορά το χρόνο) και να τοποθετούνται σε ορατά και εύκολα προσβάσιμα σημεία, συνοδευόμενοι από οδηγίες λειτουργίας.

Γενικές οδηγίες

Για όλους τους εργαζόμενους, τους τρίτους και τα άλλα ενδιαφερόμενα μέρη που έχουν πρόσβαση σε ασφαλείς περιοχές του Οργανισμού, ισχύουν οι παρακάτω γενικές οδηγίες.

Πρέπει να:

- βεβαιωθείτε ότι έχετε κατανοήσει τις συγκεκριμένες οδηγίες, για όλους τους χώρους, στους οποίους σας επιτρέπεται η πρόσβαση
- παραμείνετε σε εγρήγορση, εντός της ασφαλούς περιοχής
- συνοδεύετε τους επισκέπτες σας
- βεβαιωθείτε ότι οι πόρτες και τα παράθυρα είναι ασφαλή πριν από την αναχώρηση σας, αν είστε ο τελευταίος που βγαίνει από την ασφαλή περιοχή
- ελέγξετε τους κενούς χώρους για σημάδια μη εξουσιοδοτημένης πρόσβασης Δεν πρέπει να:
- μεταφέρετε πληροφορίες που αφορούν τον Οργανισμό σε οποιονδήποτε μη εξουσιοδοτημένο, ακόμα και εάν σας ζητηθεί να το κάνετε
- επιτρέψετε σε οποιονδήποτε να σας ακολουθήσει, μέσω ενός ασφαλούς σημείου εισόδου
- κρατήσετε τις πόρτες ασφαλείας ανοιχτές για περισσότερο χρόνο από όσο χρειάζεται
- επιτρέψετε σε οποιονδήποτε να εργαστεί εντός του Οργανισμού μόνος του, εκτός εάν υπάρχει προηγούμενη συνεννόηση
- πείτε σε οποιονδήποτε τον κωδικό πρόσβασής σας
- γράψετε τον κωδικό πρόσβασής σας κάπου

- χρησιμοποιήσετε οποιαδήποτε συσκευή φωτογράφησης, βιντεοσκόπησης ή καταγραφής μέσα στον Οργανισμό, εκτός εάν υπάρχει προηγούμενη συνεννόηση
- αφήσετε διαβαθμισμένες πληροφορίες αφύλακτες σε κοινή θέα

Ο Προϊστάμενος

Σωτήρης Λαμπρινάκος
ΠΕ Πληροφορικής

Ακριβές Αντίγραφο
ΑΥΤΟΤ. ΤΜ. ΠΡΟΓΡΑΜΜΑΤΙΣΜΟΥ ΟΡΓΑΝΩΣΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ
ΛΑΜΠΡΙΝΑΚΟΣ ΣΩΤΗΡΗΣ
Δήμος Περάματος