KORINTHIAN FOODS

INFINITE QUALITY & TASTE

ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟ-ΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ, ΠΛΗΡΟΦΟΡΙΩΝ ΚΑΙ ΔΕΔΟΜΕΝΩΝ

ΠΑΡΑΡΤΗΜΑ XVIII

ΙΣΤΟΡΙΚΟ ΕΚΔΟΣΗΣ / ΑΝΑΘΕΩΡΗΣΕΩΝ

ΕΚΔΟΣΗ	ΗΜΕΡΟΜΗΝΙΑ ΙΣΧΥΟΣ
1.0	29-04-2024

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΕΙΣΑΓΩΓΗ

Η πολιτική ασφάλειας αποτελεί το πλαίσιο στο οποίο βασίζεται η προστασία των δεδομένων και της επικοινωνίας από τους κινδύνους που υπάρχουν κατά την χρήση των πληροφοριακών συστημάτων της Εταιρείας.

ΟΡΙΣΜΟΙ ΚΑΙ ΕΡΜΗΝΕΙΑ

Πληροφοριακό σύστημα είναι ένα ολοκληρωμένο σύνολο στοιχείων με σκοπό τη συλλογή, αποθήκευση, επεξεργασία και μετάδοση δεδομένων και ψηφιακών πληροφοριών. Με τον όρο πληροφοριακά συστήματα αναφέρονται όλες οι δικτυακές εγκαταστάσεις, οι πλατφόρμες (λειτουργικά συστήματα), όλα τα συστήματα υπολογιστών (φορητοί, επιτραπέζιοι υπολογιστές, διακομιστές κ.λπ.), όλες οι εφαρμογές και τα δεδομένα που περιέχονται σε αυτά τα συστήματα είτε τοπικά είτε μέσω εγκαταστάσεων σε υπολογιστικά νέφη (cloud).

Δεδομένα: αναφέρονται ως τα γεγονότα, παρατηρήσεις, αριθμοί, στατιστικές ή γραφήματα που συλλέγονται κατά τη λειτουργία της Εταιρείας. Μπορεί να αποτελούνται από ξεχωριστά κομμάτια πληροφοριών, μορφοποιημένα και αποθηκευμένα με τρόπο που να εξυπηρετεί συγκεκριμένο σκοπό.

Διαθεσιμότητα (Availability): Η διασφάλιση ότι δεδομένα και πληροφορίες της Εταιρείας είναι διαθέσιμα για πρόσβαση ανά πάσα στιγμή από εξουσιοδοτημένους χρήστες.

Εμπιστευτικότητα (Confidentiality): Η διασφάλιση ότι δεδομένα και πληροφορίες δεν διατίθενται προς πρόσβαση σε μη εξουσιοδοτημένους χρήστες.

Ακεραιότητα (Integrity): Η διασφάλιση ότι δεδομένα και πληροφορίες δεν υπόκεινται σε τροποποιήσεις από μη εξουσιοδοτημένους χρήστες ή διαδικασίες.

Μη Αποποίηση Ευθύνης (Non-Repudiation): Η διασφάλιση ότι ένας χρήστης ή σύστημα δεν μπορεί να αποποιηθεί τη συμμετοχή του σε μία ενέργεια ή διαδικασία.

Πληροφοριακός Κίνδυνος και Ασφάλεια Πληροφορικής: Η πιθανότητα απώλειας εμπιστευτικότητας, ακεραιότητας ή διαθεσιμότητας πόρων πληροφοριών.

Chief Technology Officer (CTO): Υπεύθυνος Τεχνολογίας

Information Security Officer (ISO): Υπεύθυνος Ασφάλειας Πληροφοριών

Συμβάν Ασφάλειας: Οποιοδήποτε συμβάν συνδέεται με τη ασφάλεια των πληροφοριών είτε αφορά κίνδυνο παραβίασης φυσικής ή λογικής ασφάλειας είτε ελλιπή εφαρμογή των οριζόμενων κανόνων της Πολιτικής Ασφάλειας.

ΟΡΓΑΝΩΣΗ ΠΟΛΙΤΙΚΗΣ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ

Η Διοίκηση της Εταιρείας φέρει την συνολική ευθύνη για την ασφάλεια των πληροφοριών. Ο Chief Technology Officer(CTO) είναι υπεύθυνος για την εφαρμογή της Πολιτικής Ασφάλειας Πληροφοριών.

Ο Information Security Officer (ISO) είναι υπεύθυνος για τον εντοπισμό κινδύνων πληροφορικής και ασφάλειας, την αναφορά τους στη διοίκηση της Εταιρείας και την πρόταση μέτρων μετριασμού του κινδύνου. Επίσης, επιβλέπει την εφαρμογή της πολιτικής ασφάλειας της Εταιρείας, συμμετέχει στη διαχείριση συμβάντων ασφαλείας, εκπαιδεύει και καταγράφει την επίδοση των εργαζομένων σε θέματα πληροφοριών τροποποιώντας κατάλληλα το πρόγραμμα εκπαίδευσης τους.

Επίσης, η Εταιρεία ενσωματώνει ως κομμάτι της ετήσιας στρατηγικής του τους στόχους της ασφάλειας πληροφοριών και ιδιαιτέρως στα συστήματα πληροφορικής και στις υπηρεσίες πληροφορικής, στο προσωπικό και στις διαδικασίες που την υποστηρίζουν.

Ο ISO καταρτίζει σχέδια δράσης τα οποία περιέχουν στο σύνολο τους τα μέτρα που λαμβάνονται για την επίτευξη του στόχου της στρατηγικής πληροφοριακών συστημάτων και προβλέπει την επανεξέταση τους σε περιοδική βάση ώστε να διασφαλίζεται και η καταλληλόλητά τους και η τακτική ενημέρωση τους.

Σε ετήσια βάση είναι υπεύθυνος για την σύνταξη της σχετικής έκθεσης και υποβολή προς το διοικητικό συμβούλιο αναφορικά με δραστηριότητες, εντοπισμένους κινδύνους και την εφαρμογή μέτρων μετριασμού των κινδύνων.

ΑΠΟΔΕΚΤΗ ΧΡΗΣΗ

Η αποδεκτή χρήση δημιουργεί το πλαίσιο πάνω στο οποίο εκχωρείται στους χρήστες το δικαίωμα πρόσβασης σε πληροφοριακά συστήματα αποβλέποντας στην αποτροπή καταχρηστικής άσκησης των δικαιωμάτων τους και τον κίνδυνο παραβίασης της ασφάλειας πληροφοριών στις παρεχόμενες σε αυτούς υπηρεσίες.

Επίσης, περιλαμβάνει τα μέτρα που λαμβάνονται για την προστασία των πληροφοριών, από τους χρήστες των συστημάτων, ιδιαίτερα ως προς τους κανόνες ορθής χρήσης των δικτύων, προϊόντων ή υπηρεσιών ώστε να διασφαλίζεται η ασφάλεια των πληροφοριών. Μέρος αυτών αποτελούν οι επιτρεπόμενες και μη επιτρεπόμενες χρήσεις και δραστηριότητες των εργαζόμενων και των χρηστών ή συνδρομητών στις υπηρεσίες και τα προϊόντα της Εταιρείας.

Κύριος σκοπός είναι η προστασία των χρηστών διασφαλίζοντας ότι η παρεχόμενη σε αυτούς πρόσβαση είναι σύμφωνη με την ενότητα της Λογικής Πρόσβασης της Πολιτικής Ασφάλειας του παρόντος εντύπου. Με τον τρόπο αυτό δημιουργούνται οι συνθήκες για να διασφαλιστεί ότι η πρόσβαση τους δεν θα αποτελέσει μέσο διενέργειας παράνομων δραστηριοτήτων λαμβάνοντας υπόψη την τοπική, την ευρωπαϊκή αλλά και την διεθνή νομοθεσία.

Οι όροι και οι πολιτικές που εφαρμόζει η Εταιρεία ως μέρος αυτών και η Πολιτική Ασφάλειας Πληροφοριών, γίνονται αποδεκτά τόσο με την υπογραφή της σύμβασης εργασίας των εργαζομένων της Εταιρείας όσο με την υπογραφή συμβάσεων έργου ή παροχής υπηρεσιών από εξωτερικούς συνεργάτες.

Βάσει των παραπάνω ισχύουν τα ακόλουθα.

- Η χρήση των προϊόντων και υπηρεσιών που παρέχει η Εταιρεία συνεπάγεται την άμεση αποδοχή και συμφωνία με την παρούσα πολιτική.
- Οι εργαζόμενοι και εξωτερικοί συνεργάτες της Εταιρείας υποχρεούνται στην εφαρμογή των όρων της πολιτικής ασφάλειας πληροφοριών.
- Οι χρήστες που διαθέτουν πρόσβαση στα πληροφοριακά συστήματα της Εταιρείας απαγορεύεται να αποκαλύπτουν σε τρίτους οποιαδήποτε πληροφορία υποπίπτει στην αντίληψή τους ή την κατοχή τους, ως μέρος ή αποτέλεσμα της εργασίας τους.
- Οι εργαζόμενοι και εξωτερικοί συνεργάτες υποχρεούνται να ενημερώνουν άμεσα το αρμόδιο προσωπικό σε περίπτωση που υποπέσει στην αντίληψή τους οποιοδήποτε σχετικό περιστατικό ασφαλείας ή εντοπίσουν κενό ασφάλειας.
- Όλα τα δεδομένα που υπάρχουν ή δημιουργούνται ως αποτέλεσμα στα εταιρικά συστήματα αποτελούν ιδιοκτησία της Εταιρείας. Ως εκ τούτου, οι χρήστες είναι υπεύθυνοι για τον περιορισμό χρήσης τους ως προς τον σκοπό εργασίας τους.
- Η Εταιρεία οφείλει να παρέχει οδηγίες που αφορούν στην προσωπική χρήση των δικτυακών του πόρων.
- Η Εταιρεία δύναται να παρακολουθεί και να καταγράφει την πρόσβαση σε εξοπλισμό και σε συστήματα του για λόγους ασφάλειας αλλά και συντήρησης.
- Η Εταιρεία διατηρεί το δικαίωμα να καταγράφει και να συλλέγει πληροφορίες πρόσβασης στο δίκτυο και τα συστήματά της σε περιοδική βάση διασφαλίζοντας τη συμμόρφωση με την παρούσα πολιτική.
- Οι χρήστες οφείλουν να διατηρούν ασφαλείς τους κωδικούς πρόσβασης.
- Σε περιπτώσεις που γίνεται αντιληπτό ότι τυχόν στοιχεία πρόσβασης έχουν περιέλθει σε γνώση τρίτων, οι χρήστες θα πρέπει να προβαίνουν στην αλλαγή τους και να ενημερώνουν άμεσα τον Information Security Officer.
- Οι χρήστες οφείλουν να λαμβάνουν κάθε δυνατή προφύλαξη προκειμένου να αποτρέψουν μη εξουσιοδοτημένη πρόσβαση σε εμπιστευτικές πληροφορίες της Εταιρείας.
- Οι χρήστες θα πρέπει να ακολουθούν υπεύθυνα την πολιτική ασφάλειας των πληροφοριών της Εταιρείας.

ΔΙΑΒΑΘΜΙΣΗ ΠΛΗΡΟΦΟΡΙΩΝ

Η διαβάθμιση των πληροφοριών εφαρμόζεται με σκοπό τη διασφάλιση του απορρήτου των πληροφοριών και της ακεραιότητας τους. Η διαβάθμιση σχετίζεται με την ευαισθησία της πληροφορίας και κυρίως με τις ευαίσθητες λεπτομέρειες που περιλαμβάνουν.

Ως εκ τούτου, η Εταιρεία ακολουθεί την παρακάτω διαδικασία διαβάθμισης των πληροφοριών:

- Δημόσια πληροφορία: Οι δημόσιες πληροφορίες έχουν εγκριθεί ειδικά για δημόσια δημοσίευση από ορισμένη αρχή. Τυπικά παραδείγματα δημόσιων πληροφοριών ενδέχεται να περιλαμβάνουν φυλλάδια μάρκετινγκ ή αντίστοιχο υλικό που δημοσιεύεται σε ιστοσελίδες της Εταιρείας στο διαδίκτυο και ως εκ τούτου μπορούν να διανεμηθούν εκτός της Εταιρείας.
- Εσωτερικές Πληροφορίες: Είναι πληροφορίες προς χρήση εντός της Εταιρείας και εντός συνδεδεμένων εταιριών. Ο συγκεκριμένος τύπος πληροφοριών μπορεί να διατεθεί εντός της Εταιρείας χωρίς την άδεια από τον κάτοχο των πληροφοριών. Μη εξουσιοδοτημένη αποκάλυψη πληροφοριών αυτής της διαβάθμισης σε τρίτους ενδέχεται να καλύπτεται από νομικές ή συμβατικές διατάξεις.
- Εμπιστευτικές πληροφορίες: Αποτελούν εξαιρετικά ευαίσθητο υλικό. Είναι κατά κύριο λόγο ιδιωτικής ή άλλης ευαίσθητης φύσης και η χρήση της περιορίζεται σε εκείνους τους χρήστες που κατέχουν νόμιμη επιχειρηματική ανάγκη για πρόσβαση. Η παροχή πρόσβασης σε αυτές τις πληροφορίες πάντα καθαρίζονται μέσω του κατόχου των πληροφοριών. Η μη εξουσιοδοτημένη πρόσβαση στη συγκεκριμένη διαβάθμιση πληροφοριών σε άτομα χωρίς επιχειρηματική ανάγκη πρόσβασης ενδέχεται να παραβιάζει νόμους και κανονισμούς και ενδέχεται να προκαλέσει προβλήματα στην λειτουργία της Εταιρείας.

ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΩΝ ΤΡΙΤΩΝ

Η ασφάλεια πληροφοριών τρίτων σχετίζεται κατά κύριο λόγο με την επιλογή ενός τρίτου φορέα(third party) παροχής υπηρεσιών για σύναψη επιχειρηματικής συμφωνίας όπου η Εταιρεία θα πρέπει να αξιολογήσει τόσο ως προς τις οικονομικές αλλά λειτουργικές δυνατότητες του παρόχου των υπηρεσιών.

Κατά την σύναψη της σύμβασης συνεργασίας με το τρίτο μέρος θα πρέπει να λαμβάνονται υπόψη τα ακόλουθα:

- Ξεκάθαρη καταγραφή αναφορικά με την επιστροφή και τη διάθεση πληροφοριών και περιουσιακών στοιχείων με το πέρας της σύμβασης.

- Ρητή αναφορά ως προς τους περιορισμούς σχετικά με την αποκάλυψη πληροφοριών, την αντιγραφή και τη χρήση της συμφωνίας εμπιστευτικότητας.
- Την τήρηση των επιβαλλόμενων κανονισμών ελέγχου πρόσβασης για τα περιουσιακά στοιχεία της Εταιρείας.
- Την αποδοχή του κανονιστικού πλαισίου της Εταιρείας σχετικά με την αναφορά, την κοινοποίηση, τη διερεύνηση περιστατικών ασφάλειας πληροφοριών και παραβιάσεων των απαιτήσεων που καθορίζονται στη σύμβαση.
- Τον καθορισμό των πληροφοριών που θα είναι διαθέσιμες σε τρίτους
- Τον καθορισμό της διαβάθμισης ασφαλείας των χρησιμοποιούμενων πληροφοριών.
- Τον καθορισμό του συμφωνημένου επίπεδο εξυπηρέτησης.
- Τον ρητό προσδιορισμό ως τα πνευματικά δικαιώματα που τυχόν απορρέουν από την σύμβαση.
- Την αποδοχή των μέτρων ασφαλείας από τα δύο μέρη.
- Σαφή αναφορά ως προς τους όρους της καταγγελίας της σύμβασης.

Η Εταιρεία θα πρέπει να ορίσει τον εργαζόμενο που θα είναι ο υπεύθυνος υλοποίησης της σύμβασης. Με την λήξη της επιχειρηματικής συνεργασίας, ο εξουσιοδοτημένος υπάλληλος υποχρεούται να ενημερώσει την μονάδα Πληροφορικής για την λήξη των δικαιωμάτων τρίτων για πρόσβαση στις ευαίσθητες επιχειρηματικές πληροφορίες της Εταιρείας.

ΑΠΟΘΗΚΕΥΣΗ ΔΕΔΟΜΕΝΩΝ

Η διαθεσιμότητα των πληροφοριών καθορίζεται από τους επιχειρηματικούς ιδιοκτήτες του συστήματος. Το χρονικό διάστημα λήψης και φύλαξης των αντιγράφων ασφαλείας πρέπει να καθορίζονται από την αντίστοιχη διαβάθμιση ασφάλειας των πληροφοριών βάσει των οποίων δημιουργούνται και τους αποδεκτούς κινδύνους που έχουν καθοριστεί.

Ο υπεύθυνος των πληροφοριακών συστημάτων σχεδιάζει, εφαρμόζει και παρακολουθεί τα εφεδρικά συστήματα για πληροφορίες που υποβάλλονται σε επεξεργασία μέσω της υπηρεσίας, σύμφωνα με την εκτίμηση κινδύνου που έχει καταγραφεί.

Η διαδικασία δημιουργίας αντιγράφων ασφαλείας εταιρικών πληροφοριών τεκμηριώνεται και ενημερώνεται σε τακτά χρονικά διαστήματα. Αντίγραφα ασφαλείας λαμβάνονται για όλες τις διαμορφώσεις (configuration) των λειτουργικών συστημάτων. Σε περιπτώσεις που δεν είναι δυνατό να δημιουργηθούν

αντίγραφα ασφαλείας αυτών των διαμορφώσεων, οι σχετικές πληροφορίες αποθηκεύονται με κάποια άλλη τεκμηριωμένη μέθοδο.

Τυχόν κρίσιμα αντίγραφα ασφαλείας που απαιτούνται για την ανάκτηση κρίσιμων υπηρεσιών πληροφοριών

θα πρέπει βέλτιστα να αποθηκεύονται εκτός των εγκαταστάσεων (off premises) της Εταιρείας και να συμπεριλαμβάνονται στο σχέδιο αποκατάστασης από καταστροφή. Αν κατά τη διαδικασία δημιουργίας αντιγράφων ασφαλείας εμπλέκονται τρίτα μέρη και τα αντίγραφα ασφαλείας αποθηκεύονται σε εναλλακτική τοποθεσία της Εταιρείας, τότε το τρίτο μέρος πρέπει να είναι εξουσιοδοτημένο με κατάλληλο επίπεδο ασφαλείας για την αποθήκευση ευαίσθητων πληροφοριών ενώ θα πρέπει να τηρούνται τα αντίστοιχα μέτρα ασφάλειας στην εναλλακτική τοποθεσία.

Η μονάδα Πληροφορικής θα πρέπει να μεριμνήσει για την υποχρέωση της ύπαρξης τεχνικού περιβάλλοντος για την επικύρωση ασφαλείας των αποθηκευμένων αντιγράφων ασφαλείας. Όλα τα εφεδρικά δεδομένα θα πρέπει να ελέγχονται περιοδικά για να διασφαλίζεται η καταλληλόλητα τους σε περιπτώσεις που απαιτείται η χρήση τους.

ΑΠΟΡΡΙΨΗ Ή ΕΠΑΝΑΧΡΗΣΙΜΟΠΟΙΗΣΗ ΜΕΣΩΝ ΚΑΙ ΕΞΟΠΛΙΣΜΟΥ

Η διαχείριση της απόρριψης ψηφιακών και αναλογικών μέσων γίνεται πάντα σε συνάρτηση με την κατηγορία διαβάθμισης ασφάλειας των πληροφοριών που αποθηκεύονται στα εξεταζόμενα μέσα.

Οι εργαζόμενοι της Εταιρείας θα πρέπει να καταστρέψουν όλη την τεκμηρίωση των μέσων που πλέον δεν χρησιμοποιούνται και περιέχουν ευαίσθητες πληροφορίες χρησιμοποιώντας το αντίστοιχο ενδεδειγμένο μηχάνημα καταστροφής.

Σε περιπτώσεις που τα ψηφιακά μέσα δεν μπορούν να καταστραφούν με διαθέσιμα μηχανήματα, η μονάδα πληροφορικής ή τρίτο μέρος πρέπει να εκτελέσει την διαδικασία καταστροφής τους.

Εφόσον υφίσταται η επαναχρησιμοποίηση μέσων ή εξοπλισμού, όλες οι τυχόν ευαίσθητες πληροφορίες (και metadata) που περιέχονται στα μέσα ή τον εξοπλισμό θα πρέπει να διαγράφονται βάσει προκαθορισμένης διαδικασίας.

Αν κατά την διαδικασία απόρριψης των μέσων, εμπλέκεται τρίτο μέρος, θα πρέπει να τηρείται το αντίστοιχο αρχείο καταγραφής ως προς την εφαρμογή των διαδικασιών απόρριψης με τις ακόλουθες πληροφορίες:

- Στοιχεία του ατόμου υπεύθυνο για τις διαδικασίες διάθεσης.

- Στοιχεία και υπογραφή υπεύθυνου για την επίβλεψη της διαδικασίας διάθεσης.
- Είδος εξοπλισμού που απορρίπτεται ή δεδομένα που διαγράφηκαν.
- Μέθοδος που εφαρμόστηκε για την απόρριψη του εξοπλισμού ή την διαγραφή δεδομένων.

Τα μέσα και ο εξοπλισμός επεξεργασίας πληροφοριών που προορίζονται για απόρριψη ή διαγραφή δεδομένων θα πρέπει να αποθηκεύονται βάσει των κανονισμών ασφάλειας της Εταιρείας μέχρι την ολοκλήρωση της απόρριψης τους ή την διαγραφή των δεδομένων.

ΑΝΘΡΩΠΙΝΟ ΔΥΝΑΜΙΚΟ

Το προσωπικό της Εταιρείας θα πρέπει να εκπαιδεύεται τακτικά στην ασφάλεια των πληροφοριών ώστε να είναι σε θέση να αντιλαμβάνεται την έκταση και το πεδίο εφαρμογής της πολιτικής ασφάλειας των πληροφοριών της Εταιρείας. Με τον τρόπο θα πρέπει να είναι εξοικειωμένο με τις πολιτικές ασφάλειας πληροφοριών και θα πρέπει να ενημερώνεται τακτικά.

Η διοίκηση της Εταιρείας έχει τη συνολική ευθύνη για την ασφάλεια των πληροφοριών και είναι επίσης υπεύθυνη για τον συντονισμό της ασφάλειας των πληροφοριών. Οι εργαζόμενοι πρέπει να συμμορφώνονται με τις πολιτικές και τις οδηγίες ασφάλειας και να εκτελούν τις εργασίες τους πάντα με γνώμονα την ασφάλεια. Οι περιπτώσεις περιστατικών ασφάλειας που θα υποπέσουν στην αντίληψη των εργαζομένων, θα πρέπει άμεσα να αναφερθούν ως στο αρμόδιο προσωπικό.

Με τον τερματισμό της εργασιακής σχέσης του εργαζόμενου με την Εταιρεία ο άμεσος προϊστάμενος είναι υπεύθυνος για την ενημέρωση του αρμόδιου προσωπικού με σκοπό τον τερματισμό των προσβάσεων στα συστήματα και τις κτιριακές εγκαταστάσεις αλλά και την επιστροφή του εξοπλισμού της Εταιρείας που έκανε χρήση ο εργαζόμενος σύμφωνα με την εγκεκριμένη διαδικασία.

ΕΠΙΣΤΡΟΦΗ ΕΞΟΠΛΙΣΜΟΥ ΚΑΙ ΑΝΑΚΛΗΣΗ ΔΙΚΑΙΩΜΑΤΩΝ ΠΡΟΣΒΑΣΗΣ

Με τον τερματισμό εργασιακής σχέσης ή συμβάσεων, τα περιουσιακά στοιχεία της Εταιρείας θα πρέπει να επιστρέφονται στην Εταιρεία βάσει συγκεκριμένων διαδικασιών. Με την ενημέρωση του αρμόδιου προσωπικού από τον άμεσα εμπλεκόμενο, ενεργοποιείται η προβλεπόμενη διαδικασία σύμφωνα με την οποία πραγματοποιείται η επιστροφή τόσο του εξοπλισμού εργασίας όσο και τυχόν μέσων φυσικής πρόσβασης(κάρτα, κλειδιά κλπ.) στις εγκαταστάσεις, τα οποία αποτελούν ιδιοκτησία της Εταιρείας.

Κύριο μέρος της διαδικασίας αποτελεί η ενημέρωση του Υπεύθυνου Πληροφορικής με σκοπό τον τερματισμό των δικαιωμάτων πρόσβασης σύμφωνα με την καθορισμένη και εγκεκριμένη διαδικασία. Ο άμεσος προϊστάμενος είναι υπεύθυνος για την ενεργοποίηση της διαδικασίας τερματισμού των δικαιωμάτων πρόσβασης.

ΦΥΣΙΚΗ ΑΣΦΑΛΕΙΑ

Η Φυσική Ασφάλεια αποτελεί σημαντικό κομμάτι ελέγχου για την αποτροπή της όποιας μη εξουσιοδοτημένης φυσικής πρόσβασης στις εγκαταστάσεις της Εταιρείας.

Απαραίτητη προϋπόθεση για τον καθορισμό πλαισίου της φυσικής ασφάλειας είναι η αναγνώριση των χώρων που θα πρέπει να παραμένουν ασφαλείς και προστατευμένοι εντός των εγκαταστάσεών της Εταιρείας.

Αυτοί αφορούν κατά κύριο λόγο χώρους στους οποίους υπάρχουν εγκατεστημένα τα συστήματα πληροφορικής και επικοινωνιών (Server Room) καθώς επίσης και των συστημάτων που υποστηρίζουν την καθημερινή τους λειτουργία(χώροι συστημάτων ψύξης, τηλεπικοινωνιακών κατανεμητών, UPS κλπ.).

Ως εκ τούτου, στους συγκεκριμένους χώρους η φυσική προστασία σχετίζεται με τον περιορισμό της μη εξουσιοδοτημένης φυσικής πρόσβασης η οποία συμβάλλει στην αποτροπή διακοπής εργασιών των συστημάτων που λειτουργούν στους χώρους αυτούς.

Η Εταιρεία θα πρέπει να μεριμνήσει για την πρόσβαση των εργαζομένων στις εγκαταστάσεις των συστημάτων μέσω χρήσης ηλεκτρονικών μέσω αναγνώρισης και καταγραφής της πρόσβασης ή βάσει άλλης χειροκίνητης διαδικασίας όπου δεν είναι εφικτό με σκοπό την ελεγχόμενη είσοδο στις συγκεκριμένες εγκαταστάσεις.

Εξωτερικοί επισκέπτες επιτρέπονται μόνο στις περιοχές που προορίζονται για τους επισκέπτες ενώ τηρείται και η αντίστοιχη καταγραφή πρόσβασης τους με τα στοιχεία εισόδου. Στις περιπτώσεις που κάποιος επισκέπτης πρέπει να εισέλθει σε

φυλασσόμενες εγκαταστάσεις θα πρέπει πάντα να συνοδεύεται από το αρμόδιο προσωπικό της Εταιρείας ενώ η φυσική πρόσβαση σε συστήματα πληροφορικής επιτρέπεται μόνο σε εξουσιοδοτημένα άτομα.

Οι εγκαταστάσεις θα πρέπει να προστατεύονται με σύστημα συναγερμού που συνδέονται άμεσα με υπηρεσία παρακολούθησης συμβάντων συναγερμού ενώ πρέπει να είναι συνεχώς ενεργοποιημένο σύστημα καταγραφής εικόνας σε όσους χώρους απαιτείται.

ΛΟΓΙΚΗ ΑΣΦΑΛΕΙΑ

Η λογική πρόσβαση καθορίζει τα επίπεδα πρόσβασης θέτοντας τις αντίστοιχες απαιτήσεις για τον έλεγχο των προσβάσεων στα πληροφοριακά συστήματα της Εταιρείας. Το πλαίσιο ασφάλειας της λογικής πρόσβασης ορίζεται με βάση τα ακόλουθα:

- **Επιχειρηματικές απαιτήσεις για πρόσβαση σε πληροφοριακά συστήματα**
  Η πρόσβαση στα πληροφοριακά συστήματα βασίζεται σε απαιτήσεις επιχειρηματικής πρόσβασης,
  - ρυθμιστικές απαιτήσεις σχετικά με τη χρήση πληροφοριών,
  - τα αποτελέσματα από την ανάλυση κινδύνου ασφάλειας πληροφοριών για πληροφορίες που υποβάλλονται σε επεξεργασία, μεταφέρονται ή αποθηκεύονται στο πληροφοριακό σύστημα.

  Όλα τα δικαιώματα πρόσβασης σε συστήματα πληροφοριών της Εταιρείας πρέπει να ελέγχονται και να διατηρούνται περιοδικά από τον κάτοχο του συστήματος πληροφοριών.

- **Διαχείριση πρόσβασης χρηστών**
  Στα συστήματα πληροφορικής μπορούν να έχουν πρόσβαση μόνο εξουσιοδοτημένοι χρήστες και μόνο για χρήση εντός των αρμοδιοτήτων τους.
  - Όλα τα δικαιώματα πρόσβασης πρέπει να τεκμηριώνονται και να εγκρίνονται με βάση τις επιχειρηματικές απαιτήσεις.
  - Τα δικαιώματα και οι δραστηριότητες κάθε χρήστη προσδιορίζονται και συσχετίζονται με το όνομα χρήστη.
  - Χρησιμοποιούνται επαρκείς μέθοδοι ελέγχου ταυτότητας με το όνομα χρήστη (κωδικός πρόσβασης κλπ).
  - Οι χρήστες θα πρέπει να κατέχουν δικαιώματα πρόσβασης μόνο όπου απαιτούνται αυστηρά για την εκτέλεση των καθηκόντων τους.

- Κατά την πρόσβαση σε πληροφοριακά συστήματα, κάθε χρήστης πρέπει να ταυτοποιείται με όνομα χρήστη, ώστε να μπορεί να συσχετισθεί με τα κατάλληλα δικαιώματα πρόσβασης προκειμένου να ταυτοποιηθούν οι ενέργειες του στο πληροφοριακό σύστημα. Όπου είναι δυνατό και κρίνεται λογικό με βάση την εκτελούμενη εργασία αλλά και τη διαβάθμιση των πληροφοριών, τα δικαιώματα χρήστη πρέπει να ορίζονται σε επίπεδο λειτουργικού συστήματος και της εκάστοτε εφαρμογής.
- Ο έλεγχος πρόσβασης θα πρέπει να εφαρμόζεται μέσω κατάλληλων μηχανισμών σε όλα τα επίπεδα πρόσβασης, όπως το λειτουργικό σύστημα, το σύστημα διαχείρισης βάσεων δεδομένων και οι εφαρμογές, ώστε να διασφαλίζονται τα απαιτούμενα επίπεδα ασφάλειας σε περίπτωση αποτυχίας ενός εκ των συστημάτων ή προσπάθειας εκμετάλλευσης ευπαθειών.

- **Διαχείριση λογαριασμού χρήστη**

  Η διαχείρισης ενός λογαριασμού πρέπει να περιλαμβάνει:
  - Τη διαχείριση δικαιωμάτων πρόσβασης
  - Την τακτική ενημέρωση του αρχείου καταγραφής όλων των χρηστών και των προσβάσεων τους σε συστήματα ή δεδομένα.
  - Τον καθορισμό των αρμοδιοτήτων για τη διαχείριση λογαριασμού
  - Την κατάργηση των λογαριασμών χρηστών που πλέον δεν χρησιμοποιούνται.
  - Οι λογαριασμοί διαχειριστών πρέπει να ελέγχονται αυστηρά σε τακτικά διαστήματα και η ανάθεση τους να εγκρίνεται από τον κάτοχο του συστήματος πληροφοριών.
  - Η καταγραφή ενεργειών των συστημάτων πληροφοριών πρέπει να περιορίζεται μόνο στις απαραίτητες πληροφορίες σχετικά με το σύστημα στο οποίο έχει πρόσβαση ο χρήστης.
  - Θα πρέπει να εφαρμόζεται αυτόματη διαδικασία αποσύνδεσης των χρηστών από τα πληροφοριακά συστήματα μετά το πέρας της καθορισμένης περιόδου αδράνειας.
  - Η χρήση κοινόχρηστων λογαριασμών χρηστών απαγορεύεται.
  - Οι διακομιστές θα πρέπει να έχουν ενεργοποιημένους τους μηχανισμούς ελέγχου πρόσβασης για την αποτροπή εισβολής, την μη εξουσιοδοτημένη μεταβολή των δεδομένων καθώς και μηχανισμούς προστασίας από ιούς και κακόβουλα λογισμικά αλλά και τον μηχανισμό καταγραφής ενεργειών των χρηστών.
  - Οι χρήσεις ενός συστήματος θα πρέπει να είναι ορισμένες και καταγεγραμμένες.
  - Όλες οι προσβάσεις των χρηστών σε ευαίσθητα δεδομένα πρέπει να καταγράφονται και να τεκμηριώνεται.

- **Διαχείριση δικαιωμάτων πρόσβασης χρήστη**
  Θα πρέπει να πραγματοποιείται τακτική επανεξέταση όλων των δικαιωμάτων πρόσβασης στο δίκτυο και στα πληροφοριακά συστήματα τουλάχιστον μία φορά το εξάμηνο. Σκοπός της επανεξέτασης είναι η επιβεβαίωση όλων των λογαριασμών των χρηστών καθώς και η ισχύ των εγκεκριμένων προσβάσεων στα πληροφοριακά συστήματα.

ΑΠΟΜΑΚΡΥΣΜΕΝΗ ΕΡΓΑΣΙΑ

Στις περιπτώσεις που το προσωπικό εργάζεται εκτός των εγκαταστάσεων της Εταιρείας, θα πρέπει να διασφαλίζεται ότι το επίπεδο ασφάλειας των πληροφοριών παραμένει ίδιο με όταν εργάζεται εντός των εγκαταστάσεων. Η απομακρυσμένη πρόσβαση σε κρίσιμα συστήματα παρέχεται μόνο με βάση την αρχή ελάχιστης απαιτούμενης πληροφόρησης, χρησιμοποιώντας πάντα μέσα ελέγχου ταυτότητας πολλαπλών παραγόντων.

ΔΙΑΧΕΙΡΙΣΗ ΑΛΛΑΓΩΝ

Για τη διαχείριση αλλαγών στα συστήματα πληροφορικής και τις εφαρμογές, προκειμένου να αποφευχθεί η μη προγραμματισμένη διακοπή, η καταστροφή ή η απώλεια δεδομένων η μονάδα Πληροφορικής θα πρέπει να εφαρμόζει την ακόλουθη διαδικασία.

Κατά την λήψη αιτημάτων αλλαγών πρέπει:

- Να πραγματοποιείται ταξινόμηση πριν από την επεξεργασία. Το επίπεδο ανάλυσης, έγκρισης και δοκιμής πρέπει να είναι ευθυγραμμισμένο με το επίπεδο ταξινόμησης αλλαγών προκειμένου να αντιμετωπιστούν οι πιθανοί κίνδυνοι.
- πριν από την εφαρμογή της πλήρως δοκιμασμένης αλλαγής στο ζωντανό περιβάλλον.
- Υπάρχει η σχετική τεκμηρίωση πριν, κατά τη διάρκεια και μετά την εφαρμογή.
- Να λαμβάνονται υπόψη παράγοντες όπως η επιχειρηματική αξία, οι επιχειρηματικοί κίνδυνοι και οι κίνδυνοι ΤΠΕ

Λόγω της φύσης της Εταιρείας ενδέχεται να υπάρχουν και εξαιρέσεις στην υιοθέτηση αλλαγών που θα αποκλίνουν από την εγκεκριμένη διαδικασία και αφορούν κυρίως την υιοθέτηση αλλαγών που αφορούν την ασφάλεια δεδομένων (patching). Οι εξαιρέσεις αυτές πρέπει να τεκμηριώνονται και να εγκρίνονται επίσημα από τον Υπεύθυνο Τεχνολογίας (CTO), με αποδεικτικά στοιχεία υποστήριξης από την αρμόδια εκτελεστική διοίκηση.

Οι εξαιρέσεις πολιτικής πρέπει να περιγράφουν:

- Τη φύση της εξαίρεσης
- Μια λογική εξήγηση με τους λόγους που απαιτείται η εξαίρεση
- Τυχόν κίνδυνοι που δημιουργούνται από την εξαίρεση της αλλαγής από την εγκεκριμένη διαδικασία.
- Αποδεικτικό έγκρισης από τον επικεφαλής της μονάδας Πληροφορικής.

ΕΛΕΓΧΟΣ ΛΕΙΤΟΥΡΓΙΩΝ

Η Εταιρεία πρέπει να εφαρμόζει διαδικασίες ελέγχου και ορθής λειτουργίας σε όλα τα πληροφοριακά συστήματα της.

Μέρος αυτών διαδικασιών αποτελούν και τα ακόλουθα:

- διαδικασίες ελέγχου αλλαγών για τη διατήρηση της λειτουργίας, της ποιότητας και της ασφάλειας σε όλα τα συστήματα κατά την εισαγωγή αλλαγών.
- Κάθε σύστημα θα πρέπει να ελεγχθεί και να εγκριθεί πριν από την ανάπτυξη σε παραγωγική λειτουργία.
- Η προστασία του δικτύου, των πληροφοριών και της επικοινωνίας θα πρέπει να διατηρούνται ασφαλείς από απειλές.
- Τήρηση αρχείων καταγραφής για σημαντικές δραστηριότητες του δικτύου καθώς και των συστημάτων ώστε να είναι δυνατή η παρακολούθηση συμβάντων ασφαλείας.
- Οι εξουσιοδοτημένοι χρήστες για συστήματα δικτύου έχουν υποχρέωση για τη διασφάλιση του τύπου και της δομής των αρχείων καταγραφής, των μεθόδων συλλογής των αρχείων καταγραφής, των μεθόδων ελέγχου των αρχείων καταγραφής και των απαιτήσεων ασφαλείας που σχετίζονται με την αποθήκευση και την πρόσβαση των αρχείων καταγραφής.
- Τα ρολόγια δικτύου και διακομιστή (system clocks) πρέπει να συγχρονίζονται με τον κεντρικό διακομιστή ώρας, ώστε σε περιπτώσεις έρευνας να μπορούν να εντοπιστούν οι σχετικές καταγραφές.

ΔΟΚΙΜΕΣ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ

Κατά την διαδικασία ελέγχων της ασφάλειας των πληροφοριακών συστημάτων θα πρέπει να ακολουθούνται:

- Οι δοκιμές ελέγχων εκτελούνται πάνα κατόπιν σημαντικών αλλαγών σε υποδομές, διαδικασίες ή μετά από κρίσιμα συμβάντα ασφαλείας ή πριν από την έναρξη λειτουργίας νέων συστημάτων.
- Η αυτοματοποιημένη σάρωση ευπάθειας εκτελείται σε τακτά χρονικά διαστήματα (π.χ. τουλάχιστον μία φορά το τρίμηνο) ή όταν κρίνεται απαραίτητο.
- Οι δοκιμές παρείσφρησης (penetration tests) πραγματοποιούνται τακτικά, τουλάχιστον μια φορά ετησίως.
- Οι δοκιμές παρείσφρησης πρέπει να περιλαμβάνουν και τις υπηρεσίες εξωτερικής ανάθεσης.
- Οι δοκιμές παρείσφρησης πραγματοποιούνται από ανεξάρτητους πιστοποιημένους ελεγκτές.
- Κάθε δοκιμή θα πρέπει να ολοκληρώνεται με γραπτή έκθεση και σχέδιο δράσης για τον μετριασμό των εντοπισμένων απειλών.

ΑΞΙΟΛΟΓΗΣΗ ΤΠΕ ΚΙΝΔΥΝΟΥ

Η διαδικασία αποτίμησης κινδύνου ΤΠΕ για τα πληροφοριακά συστήματα που διαθέτει η Εταιρεία πραγματοποιείται τουλάχιστον μια φορά τον χρόνο.

Η διαδικασία περιλαμβάνει την δημιουργία και συντήρηση αρχείου πληροφοριακών συστημάτων με την περιγραφή της λειτουργίας τους, την αξιολόγηση των κινδύνων που σχετίζονται με παραβίαση του απορρήτου από εξωτερικές απειλές, την αξιολόγηση των σχετικών ευπαθειών των πληροφοριακών συστημάτων και την αξιολόγηση των πιθανών επιπτώσεων των περιστατικών παραβίασης του απορρήτου.

Τα αποτελέσματα της αξιολόγησης κινδύνου χρησιμοποιούνται κατά την αναθεώρηση της Πολιτικής Ασφάλειας Πληροφοριών αλλά για την υλοποίηση των κατάλληλων μέτρων για την εφαρμογή της.

ΕΓΚΑΤΑΣΤΑΣΗ ΕΞΟΠΛΙΣΜΟΥ

Η Εταιρεία, κατά τη διαχείριση και εγκατάσταση εξοπλισμού, λαμβάνει όλα τα απαραίτητα μέτρα προκειμένου να ελαχιστοποιείται ο κίνδυνος διαρροής πληροφοριών από τα πληροφοριακά συστήματα.

Οι αλλαγές (εισαγωγή, μεταβολή, διαγραφή) στο λογισμικό ή τα συστήματα πληροφορικής που σχετίζονται με τη διασφάλιση των πληροφοριών πραγματοποιούνται με προτεραιότητα και χωρίς καθυστέρηση.

Για οποιαδήποτε αλλαγή υλικού ή λογισμικού πραγματοποιείται στα πληροφοριακά συστήματα της Εταιρείας γίνεται καταγραφή της σχετικής διαδικασίας όπου μεταξύ άλλων καταγράφονται κατ' ελάχιστο η ημερομηνία, ο τρόπος, η αιτιολόγηση και ο εργαζόμενος που πραγματοποίησε τις αλλαγές. Σε περιπτώσεις που η αλλαγή πραγματοποιείται από εργαζόμενο εταιρίας παρόχου υποστήριξης τότε θα πρέπει μαζί με την καταγραφή να καταχωρείται και το αντίστοιχο έντυπο παροχής εργασιών με την περιγραφή των εργασιών και την ημερομηνία, ώρα και τα στοιχεία του εργαζομένου της εταιρίας παρόχου που εκτέλεσε την εργασία.

Στις περιπτώσεις που είναι εφικτό, η εγκατάσταση πραγματοποιείται πρώτα σε δοκιμαστικό περιβάλλον, πλήρως ελεγχόμενο και διαχωρισμένο από το παραγωγικό περιβάλλον από εξουσιοδοτημένο προσωπικό της Εταιρείας. Με την ολοκλήρωση εγκατάστασης ο εξοπλισμός ή το λογισμικό υποβάλλεται σε δοκιμές για να ελεγχθεί η ορθή λειτουργία του και να αξιολογηθεί η απόδοσή του βάσει προκαθορισμένων σεναρίων. Με το πέρας των δοκιμών το εξουσιοδοτημένο προσωπικό δημιουργεί την σχετική αναφορά στην οποία προτείνει την αποδοχή ή απόρριψη του εξοπλισμού ή λογισμικού βάσει των αποτελεσμάτων των δοκιμών αποδοχής του συστήματος. Ο αρμόδιος κάτοχος των πληροφοριακών συστημάτων, με βάση την αναφορά δοκιμών παρέχει την σχετική έγκριση εγκατάστασης του λογισμικού στο παραγωγικό περιβάλλον της Εταιρείας.

ΔΙΑΧΕΙΡΙΣΗ ΣΥΜΒΑΝΤΟΣ ΑΣΦΑΛΕΙΑΣ

Η Εταιρεία θα πρέπει να εφαρμόζει διαδικασία παρακολούθησης ασφάλειας που εντοπίζει εσωτερικές και εξωτερικές απειλές.
Οι εργαζόμενοι της Εταιρείας αποτελούν μέρος της διαδικασίας και είναι σε εγρήγορση να αναφέρουν γεγονότα που έχουν συμβεί ή συμβαίνουν και θα μπορούσαν να επηρεάσουν την ασφάλεια των συστημάτων και δεδομένων σύμφωνα με τη διαδικασία διαχείρισης συμβάντος ασφάλειας.

Η διαδικασία διαχείρισης συμβάντος ασφάλειας έχει σαν σκοπό να καταγραφούν οι λεπτομέρειες κάθε συμβάντος ασφάλειας, να διερευνηθούν τα αίτια και να προσδιοριστούν οι τεχνικές ή οργανωτικές αδυναμίες, να καθοριστούν οι συνέπειες και να υλοποιηθούν οι ενέργειες αποκατάστασης, να ενημερωθεί ο Υπεύθυνος Ασφάλειας Πληροφοριών(ISO) και τα αρμόδια στελέχη της Εταιρείας, οι αρμόδιες Αρχές και οι θιγόμενοι χρήστες των παρεχόμενων υπηρεσιών βάσει της κείμενης νομοθεσίας.

Ως εκ τούτου, η Εταιρεία έχει καταρτίσει και εφαρμόζει την διαδικασία Διαχείρισης Συμβάντων Ασφαλείας, η οποία ενεργοποιείται σε κάθε περίπτωση συμβάντος ασφάλειας με σκοπό την πλήρη καταγραφή του.

Συγκεκριμένα, καταγράφονται τα ακόλουθα:
- Ημερομηνία/ώρα εκδήλωσης και περιγραφή του συμβάντος.
- Πότε και πως έγινε αντιληπτό το συμβάν
- Κρισιμότητα του συμβάντος.
- Τεχνικός που ασχολήθηκε με το συμβάν.
- Που εκδηλώθηκε το συμβάν.
- Πιθανή αιτία εκδήλωσης και συνέπειες του συμβάντος.
- Πληροφορίες που συλλέχτηκαν για τη διερεύνηση του συμβάντος.
- Εκτιμώμενος χρόνος υλοποίησης διορθωτικών μέτρων επίλυσης του.
- Ενημέρωση θιγόμενων χρηστών ή συνδρομητών που επηρεάστηκαν.
- Γνωστοποίηση στις αρμόδιες αρχές βάσει κείμενης νομοθεσίας(ΤτΕ κλπ.).

ΑΣΦΑΛΕΙΑ ΛΟΓΙΚΗΣ ΥΠΟΔΟΜΗΣ

Η ασφάλεια του δικτύου αλλά και του λογισμικού αποτελεί κύριο κόμματι της πολιτικής ασφάλειας που εφαρμόζει η Εταιρεία. Για την επίτευξη ενός υψηλού επιπέδου ασφάλειας απαιτείται σωστή οργάνωση και παρακολούθηση του δικτύου του.
Συγκεκριμένα,
- Λογικός Διαχωρισμός και Κατάτμηση Δικτύων: Με τον τρόπο αυτό επιτυγχάνεται η δημιουργία ζωνών ασφάλειας ανάλογα με τα συστήματα και τη διαβάθμιση της πληροφορίας, ελέγχοντας έτσι πλήρως την πρόσβαση των χρηστών και επιτρέποντας την ευκολότερη διαχείριση της συνολικής τοπολογίας του δικτύου.
- Μηχανισμοί και Συστήματα Ασφάλειας Δικτύου: Κατάρτιση και συντήρηση αρχείου στο οποίο ορίζονται οι μηχανισμοί και τα συστήματα που χρησιμοποιούνται (εξοπλισμός και λογισμικό). Το αρχείο αυτό εκτός από τον εξοπλισμό και το λογισμικό περιέχει τον τρόπο λειτουργίας, την τεχνική διαμόρφωση, την έκδοση του λογισμικού, την ημερομηνία

τελευταίας αναβάθμισης, τις τεχνικές συντηρήσεις καθώς και τα στοιχεία σχετικά με την εγγύηση του εξοπλισμού ή λογισμικού.

- Κρυπτογράφηση: Για τη διασφάλιση της εμπιστευτικότητας και της ακεραιότητας στις συναλλαγές και τις επικοινωνίες μέσω διαδικτύου είναι απαραίτητη η εφαρμογή πρωτοκόλλων και τεχνικών κρυπτογράφησης. Για τον λόγο αυτό, η Εταιρεία εφαρμόζει τεχνικές και συστήματα κρυπτογράφησης για την αποτελεσματικότερη προστασία των μεταφερόμενων δεδομένων.
- Έλεγχος Ασφάλειας Δικτύου & Συστημάτων: Η διαδικασία ελέγχου ασφάλειας του δικτύου και των συστημάτων πραγματοποιείται σε τακτά χρονικά διαστήματα. Τον έλεγχο πραγματοποιεί ομάδα η οποία στελεχώνεται από κατάλληλα καταρτισμένο προσωπικό της Εταιρείας ενώ κατά περίπτωση μπορεί να περιλαμβάνει και εξειδικευμένο προσωπικό άλλου φορέα. Η διαδικασία ελέγχου διεξάγεται μία φορά το μήνα, καθώς και σε περιπτώσεις που προκύψουν θέματα ασφάλειας ή παραβίασης της παρούσας πολιτικής ασφάλειας.

ΔΙΑΣΦΑΛΙΣΗ ΕΠΙΧΕΙΡΗΜΑΤΙΚΗΣ ΣΥΝΕΧΕΙΑΣ

Η διασφάλιση του σχεδιασμού συνέχειας των λειτουργιών αφορά τόσο τα συστήματα πληροφορικής όσο και την προστασία των ανθρώπων, των περιουσιακών στοιχείων, των πελατών και της φήμης. Η επιχειρηματική συνέχεια πραγματοποιείται με επαρκείς πόρους με σκοπό την ασφάλεια των υποδομών, των συστημάτων και των χώρων εργασίας. Η Εταιρεία εκπονεί την ανάλογη μελέτη και συντάσσει το αντίστοιχο σχέδιο επιχειρηματικής συνέχειας (BCP).

Το σχέδιο επιχειρηματικής συνέχειας αποτελείται από τις κρίσιμες πληροφορίες που χρειάζεται μια Εταιρεία για να συνεχίσει να λειτουργεί κατά τη διάρκεια ενός μη προγραμματισμένου συμβάντος.
Το σχέδιο δηλώνει τις βασικές λειτουργίες της επιχείρησης, προσδιορίζει ποια συστήματα και διαδικασίες πρέπει να διατηρηθούν και περιγράφει λεπτομερώς τον τρόπο διατήρησής τους ενώ εξετάζει και κάθε πιθανή διακοπή της επιχείρησης.

Ένα σχέδιο επιχειρηματικής συνέχειας καλύπτει κινδύνους, συμπεριλαμβανομένων των επιθέσεων στον κυβερνοχώρο, των πανδημιών, των φυσικών καταστροφών και του ανθρώπινου λάθους.

Η σειρά των πιθανών κινδύνων καθιστά ζωτικής σημασίας για μια Εταιρεία να έχει ένα σχέδιο επιχειρηματικής συνέχειας για τη διατήρηση της υγείας και της φήμης του.

Το σχέδιο επιχειρηματικής συνέχειας συνήθως δημιουργείται από τον υπεύθυνο IT. Ωστόσο, το εκτελεστικό προσωπικό της Εταιρείας συμμετέχει ενεργά στις διαδικασίες που ορίζονται εντός του σχεδίου, παρέχοντας κρίσιμη για την Εταιρεία γνώση και εποπτεία.

Τέλος, η Εταιρεία διασφαλίζει μέσω συγκεκριμένων ελέγχων(ετήσιες δοκιμές) την αρτιότητα και ενημέρωση του σχεδίου επιχειρηματικής συνέχειας.

ΕΚΠΑΙΔΕΥΣΗ

Η Εταιρεία έχοντας ως σκοπό την διασφάλιση της ορθής εφαρμογής της πολιτικής ασφάλειας εφαρμόζει εκπαιδευτικό πρόγραμμα, συμπεριλαμβανομένων περιοδικών προγραμμάτων ευαισθητοποίησης σε θέματα ασφάλειας, για όλο το προσωπικό και τους αναδόχους έργων. Μέσω των προγραμμάτων διασφαλίζεται η κατάρτισή τους για την άσκηση των καθηκόντων και των αρμοδιοτήτων τους, σύμφωνα με τις σχετικές πολιτικές και διαδικασίες ασφάλειας για τη μείωση των φαινομένων ανθρώπινου σφάλματος, κλοπής, απάτης, κατάχρησης ή απώλειας.

Το πρόγραμμα εκπαίδευσης και ευαισθητοποίησης επικεντρώνεται κυρίως στις παρακάτω κατηγορίες
απειλών:

1. Νοημοσύνη απειλών (threat intelligence)
2. Κοινωνική μηχανική (social engineering)
3. Διαχείριση κωδικών πρόσβασης (password management)
4. Ευαισθητοποίηση σε επιθέσεις phishing (phishing awareness)
5. Ευαισθητοποίηση σε κακόβουλα λογισμικά (malware awareness)
6. Προστασία Δεδομένων (data protection)
7. Αναγνώριση και αναφορά περιστατικών ασφάλειας (Incident awareness and report)

Το εκπαιδευτικό πρόγραμμα παρέχει κατάρτιση για το σύνολο των μελών του προσωπικού τουλάχιστον σε ετήσια βάση.

ΣΥΜΜΟΡΦΩΣΗ

Για την επιτυχημένη συμμόρφωση της Εταιρείας η πολιτική ασφάλειας του θα πρέπει να ορίζεται και να τεκμηριώνεται βάσει των καθημερινών διαδικασιών που ακολουθούνται από το προσωπικό του για την ολοκλήρωση των καθημερινών εργασιών. Οι διαδικασίες αυτές θα πρέπει να ελέγχονται και να αναθεωρούνται σε τακτά χρονικά διαστήματα με σκοπό την συμμόρφωση της Εταιρείας με την νομοθεσία και τις διατάξεις που ορίζονται από την αρμόδια αρχή ελέγχου. Για τον λόγο αυτό, η Εταιρεία εκπονεί ετήσιο σχέδιο ελέγχου βάσει του οποίου υλοποιούνται εγκεκριμένα μέτρα, επιτυγχάνονται οι ετήσιοι στόχοι συμμόρφωσης, υιοθετούνται νέες ρυθμιστικές διατάξεις και νομοθεσία επιτρέποντας την διατήρηση του επιπέδου ασφάλειας των πληροφοριών εντός των προβλεπόμενων κανόνων και αρχών.