FOURLIS
ΟΜΙΛΟΣ ΕΤΑΙΡΙΩΝ

Μεθοδολογία Διαχείρισης Κινδύνου Ασφάλειας Πληροφοριών του Ομίλου ΦΟΥΡΛΗΣ

Το παρόν έγγραφο παρέχει κατευθυντήριες γραμμές περί της Μεθοδολογίας Διαχείρισης Κινδύνου Ασφάλειας Πληροφοριών του Ομίλου ΦΟΥΡΛΗΣ και περιγράφει εν συντομία τη σχετική διαδικασία και τις δραστηριότητές της.

Μία συστηματική προσέγγιση στη διαχείριση κινδύνου ασφάλειας πληροφοριών είναι αναγκαία προκειμένου ο Όμιλος Εταιρειών ΦΟΥΡΛΗΣ να ταυτοποιήσει τις οργανωτικές ανάγκες αναφορικά με τις απαιτήσεις ασφάλειας πληροφοριών και να δημιουργήσει ένα αποτελεσματικό σύστημα διαχείρισης ασφάλειας πληροφοριών (ΣΔΑΠ).

Οι προσπάθειες μας για παροχή ασφάλειας αφορούν στην αντιμετώπιση κινδύνων αποτελεσματικά και έγκαιρα όπου και όποτε απαιτούνται. Η διαχείριση κινδύνου ασφάλειας πληροφοριών συνιστά αναπόσπαστο τμήμα όλων των δραστηριοτήτων διαχείρισης ασφάλειας πληροφοριών του Ομίλου μας, και εφαρμόζεται τόσο στην υλοποίηση όσο και στην διαρκή και απρόσκοπτη λειτουργία του ΣΔΑΠ. Η διαδικασία θεμελιώνει το εξωτερικό και εσωτερικό περιεχόμενο, εκτιμά τους κινδύνους και τους αντιμετωπίζει χρησιμοποιώντας ένα πρόγραμμα χειρισμού και αντιμετώπισης κινδύνων προς υλοποίηση των συστάσεων και αποφάσεων.

Η διαχείριση κινδύνων αναλύει τι μπορεί να συμβεί και ποιες μπορεί να είναι οι πιθανές συνέπειες για τον Όμιλο Εταιρειών μας, προτού αποφασίσει τί θα πρέπει να γίνει και πότε, ώστε να μειώσει τον κίνδυνο σ' ένα αποδεκτό επίπεδο. Η διαχείριση κινδύνου ασφάλειας πληροφοριών συνεισφέρει στα εξής:

- Στην αναγνώριση/ταυτοποίηση των κινδύνων.
- Στην εκτίμηση των κινδύνων όσον αφορά στις συνέπειές τους στην επιχείρηση και στην πιθανότητα εμφάνισής τους.
- Στην πιθανότητα εμφάνισης και στις συνέπειες των εν λόγω κινδύνων.
- Στη θεμελίωση σειράς προτεραιότητας για το χειρισμό και την αντιμετώπιση των κινδύνων.
- Στη θέση ενεργειών που μειώνουν τους εμφανιζόμενους κινδύνους σε προτεραιότητα
- Στην εμπλοκή ενδιαφερομένων όταν λαμβάνονται αποφάσεις διαχείρισης κινδύνων και όταν διατηρείται η ενημέρωση περί της κατάστασης διαχείρισης κινδύνων.
- Στην αποτελεσματικότητα του ελέγχου χειρισμού και αντιμετώπισης κινδύνων.
- Στον έλεγχο και στην τακτική αναθεώρηση των κινδύνων και της διαδικασίας διαχείρισης κινδύνων.
- Στη λήψη πληροφοριών με σκοπό βελτίωσης της προσέγγισης διαχείρισης κινδύνων.
- Στην εκπαίδευση του προσωπικού περί των κινδύνων και των ενεργειών που λαμβάνονται με σκοπό το μετριασμό τους.

Μία κατάλληλη προσέγγιση διαχείρισης κινδύνων έχει επιλεγεί, η οποία συνίσταται στην αξιολόγηση και χρήση από την Επιτροπή Χορηγιών σε Οργανισμούς – Διαχείρισης Επιχειρηματικών Κινδύνων βασικών κριτηρίων, όπως πχ κριτηρίων αξιολόγησης κινδύνου, κριτηρίων αντικτύπου και κριτηρίων αποδοχής κινδύνου.

Κριτήρια αξιολόγησης κινδύνων αναπτύσσονται για την αξιολόγηση του κινδύνου ασφαλείας πληροφοριών του οργανισμού μας, λαμβάνοντας υπόψη τα εξής:

- Τη στρατηγική αξία της διαδικασίας επιχειρηματικής πληροφόρησης.
- Την κρισιμότητα των πληροφοριακών πόρων που περιλαμβάνονται.
- Τη λειτουργική και επιχειρησιακή σπουδαιότητα της διαθεσιμότητας, εμπιστευτικότητας και ακεραιότητας.
- Τις προσδοκίες και τις αντιλήψεις των ενδιαφερομένων, και αρνητικές συνέπειες στην υπεραξία και στην καλή φήμη της επιχείρησης.

Επιπρόσθετα, τα κριτήρια αξιολόγησης κινδύνων μπορούν να χρησιμοποιηθούν προς καθορισμό προτεραιοτήτων αντιμετώπισης κινδύνων.

Κατά συνέπεια, κριτήρια αντικτύπου αναπτύσσονται και εξειδικεύονται υπό όρους του βαθμού της βλάβης ή εξόδων που προκαλούνται στον οργανισμό μας από ένα γεγονός ασφάλειας πληροφορίας που λαμβάνει υπόψη τα εξής:

- Το επίπεδο κατηγοριοποίησης του επηρεασμένου πληροφοριακού πόρου
- Παραβιάσεις της ασφάλειας πληροφοριών (πχ απώλεια εμπιστευτικότητας, ακεραιότητας και διαθεσιμότητας)
- Απώλεια της επιχειρηματικής και οικονομικής αξίας
- Θιγόμενες διαταρασσόμενες λειτουργίες/ επιχειρήσεις (στο εσωτερικό του Ομίλου ή τρίτων μερών)
- Διαταραχή προγραμμάτων και προθεσμιών
- Βλάβη φήμης

Τα κριτήρια αποδοχής κινδύνου είναι συνάρτηση των πολιτικών, πρακτικών του οργανισμού μας, των επιχειρησιακών στόχων, αντικειμενικών σκοπών και των ενδιαφερόντων των εμπλεκομένων. Κριτήρια αποδοχής κινδύνου διαμορφώνονται κατόπιν εξέτασης επιχειρησιακών κριτηρίων, των λειτουργιών των Εταιρειών του Ομίλου μας, της διαθέσιμης τεχνολογίας, των οικονομικών, κοινωνικών και ανθρωπιστικών παραγόντων.

Οι απειλές που αξιολογούνται και ελέγχονται βάσει της Μεθοδολογίας Αξιολόγησης Κινδύνου Ασφάλειας Πληροφοριών του Ομίλου μας είναι οι εξής:

Φυσική φθορά όπως πχ ζημία από φωτιά και νερό

Φυσικά Φαινόμενα όπως πχ μετεωρολογικά φαινόμενα και σεισμικά φαινόμενα.

Απώλεια ουσιωδών υπηρεσιών όπως πχ διακοπή λειτουργίας του συστήματος κλιματισμού ή υδροδότησης και αδυναμία/βλάβη του τηλεπικοινωνιακού εξοπλισμού

Διαρροή πληροφοριών όπως πχ εξ αποστάσεως κατασκοπεία κλοπή μέσων ή εγγράφων, κλοπή εξοπλισμού, αλλοιώσεις υλικού Η/Υ και αλλοιώσεις

Τεχνικές βλάβες όπως πχ βλάβη εξοπλισμού και δυσλειτουργία λογισμικού

Μη επιτρεπόμενες ενέργειες όπως πχ μη εξουσιοδοτημένη χρήση εξοπλισμού και αλλοίωση δεδομένων.

Διαφθορά λειτουργιών όπως σφάλμα χρήσης και καταχρηστική άσκηση δικαιωμάτων.