Σχεδιάζοντας το πλάνο της Κυβερνοασφάλειας για τις ασφαλιστικές εταιρείες

Τα θέματα κυβερνοασφάλειας που αφορούν μία ασφαλιστική εταιρεία, ποικίλουν ως προς την έκταση και στις επιπτώσεις που ενδέχεται να επιφέρουν

Τα τελευταία χρόνια, η ασφαλιστική βιομηχανία στην Κύπρο κινείται με σημαντικά ψηλούς ρυθμούς ανάπτυξης. Συγκεκριμένα, σύμφωνα με τον Σύνδεσμο Ασφαλιστικών Εταιρειών Κύπρου (ΣΑΕΚ), τα μεικτά ασφάλιστρα του κλάδου ζωής, για το έτος 2018, παρουσίασαν άνοδο 12,7% σε σύγκριση με το προηγούμενο έτος. Είναι γεγονός ότι ο ασφαλιστικός τομέας λειτουργεί ως ένας από τους βασικούς πυλώνες της Κυπριακής οικονομίας και συνεχίζει αδιάλειπτα να υποστηρίζει και να ενισχύει τη συνεχή ανάπτυξή της.

Η φύση λειτουργίας μια ασφαλιστικής εταιρείας περιλαμβάνει την διαχείριση ενός μεγάλου όγκου πληροφοριών, σε σύγκριση με μία μέση επιχείρηση. Για παράδειγμα, κάθε επιχείρηση συγκεντρώνει τα προσωπικά και ευαίσθητης φύσεως δεδομένα των υπαλλήλων της (π.χ. ιατρικά δεδομένα), αλλά σε έναν ασφαλιστικό οργανισμό, ιδιαίτερα εάν αυτός δραστηριοποιείται στον κλάδο ζωής, τα δεδομένα αυτά επεκτείνονται και στους πελάτες του. Για τον λόγο αυτό, η συχνότητα εμφάνισης των κυβερνοαπειλών και η ποικιλία αυτών, σε αυτή την περίπτωση, είναι αυξημένες σε σχέση με μία οποιαδήποτε άλλη εταιρεία που προσφέρει υπηρεσίες και προϊόντα.

Τα θέματα κυβερνοασφάλειας που αφορούν μία ασφαλιστική εταιρεία, ποικίλουν τόσο σε έκταση όσο και στις επιπτώσεις που ενδέχεται να επιφέρουν, ενώ μπορούν να ομαδοποιηθούν σε τρεις βασικές κατηγορίες:

- Διακυβέρνησης Κυβερνοασφάλειας
- Διαχείρισης δεδομένων
- Ελέγχους ποιότητας μέτρων ασφάλειας

Όπως σε κάθε πτυχή που διέπει έναν οργανισμό, έτσι και στην κυβερνοασφάλεια, πρέπει να υπάρχει ένα επαρκές πλάνο διακυβέρνησης που να ενισχύει την οργάνωση, την εφαρμογή και τη συνεχή βελτίωση του επιπέδου ασφάλειας του οργανισμού. Η απουσία του πλάνου αυτού αυξάνει σημαντικά την πιθανότητα να μη γίνει ορθή επιλογή των αναγκαίων μέτρων ασφάλειας και ως αποτέλεσμα να υπάρξει έκθεση του οργανισμού σε κίνδυνο απέναντι στις υπάρχουσες κυβερνοαπειλές. Συνεπώς, οι βέλτιστες πρακτικές ασφάλειας προτείνουν ως πρώτο βήμα την υιοθέτηση ενός πλάνου ασφάλειας και της αντίστοιχης πολιτικής. Εδώ γίνεται μία σε βάθος ανάλυση του κινδύνου η οποία περιλαμβάνει: τα αγαθά του οργανισμού (π.χ. πληροφορίες), τους κινδύνους που ελλοχεύουν και τις πιθανές επιπτώσεις ενός περιστατικού ασφάλειας στην εταιρεία. Η διαδικασία αυτή θα δώσει τις κατευθυντήριες γραμμές για να οριστεί το πλάνο και η πολιτική ασφάλειας και θα οριοθετήσει τον τρόπο λειτουργίας του οργανισμού σε θέματα που άπτονται της κυβερνοασφάλειας.

Η δεύτερη κατηγορία επικεντρώνεται στα δεδομένα του οργανισμού και στην προστασία τους από κάθε ενδεχόμενη απειλή. Το βασικό βήμα εδώ, είναι η διασφάλιση της διαθεσιμότητας, ακεραιότητας και εμπιστευτικότητας των δεδομένων και πιο συγκεκριμένα η υλοποίηση μέτρων ασφάλειας που στοχεύουν στο να διασφαλίσουν ότι τα δεδομένα αυτά θα είναι πάντα διαθέσιμα στους εξουσιοδοτημένους χρήστες, δε θα τροποποιούνται χωρίς σχετική έγκριση και δε θα γνωστοποιούνται σε χρήστες που δεν διαθέτουν τη σχετική εξουσιοδότηση. Παράλληλα, δεδομένης της εφαρμογής του Κανονισμού Προστασίας Προσωπικών Δεδομένων (GDPR) από την 25η Μαΐου 2018, ο οργανισμός θα πρέπει να συμμορφωθεί με τις σχετικές νομικές διατάξεις και να υιοθετήσει την αναγκαία σχετική κουλτούρα επαρκούς προστασίας των προσωπικών δεδομένων.

Στο τρίτο, και τελευταίο βήμα, προτείνεται η συνεχής εξέταση και βελτίωση των μέτρων προστασίας που έχουν ληφθεί. Αν θεωρηθεί πως ο οργανισμός έκανε μία σωστή αρχική εκτίμηση των κινδύνων που διατρέχει και επέλεξε σωστά τα μέτρα ασφάλειας προς εφαρμογή, αυτό δεν σημαίνει πως το πλαίσιο αυτό που εφαρμόστηκε δεν επιδέχεται αλλαγών και συνεχούς εκσυγχρονισμού. Αντιθέτως, το πλαίσιο αυτό πρέπει να ανταποκρίνεται στο συνεχώς μεταβαλλόμενο εξωτερικό και εσωτερικό περιβάλλον, δεδομένου τόσο των εξελίξεων στο εποπτικό περιβάλλον, τον ανταγωνισμό, την τεχνολογία όσο και των εσωτερικών αλλαγών στον οργανισμό. Συνεπώς, θα πρέπει να γίνεται επανεξέταση του πλαισίου αυτού, ανά τακτά χρονικά διαστήματα, έτσι ώστε να προσαρμόζεται ο οργανισμός στις τρέχουσες αλλαγές και εξελίξεις.

Για τον λόγο αυτό, οι βέλτιστες πρακτικές ασφάλειας προτείνουν την εκτέλεση ελέγχων πληροφοριακών συστημάτων (Information System audits) και τεχνικών ελέγχων ασφάλειας (Penetration testing) για να εξεταστεί αν οι διαδικασίες ασφάλειας και οι αντίστοιχοι μηχανισμοί συνάδουν με τις εξελίξεις.

Τα βασικά συστατικά ενός πλαισίου κυβερνοασφάλειας μιας σύγχρονης ασφαλιστικής εταιρείας είναι τα ίδια με μίας επιχείρησης που προσφέρει τις οποιεσδήποτε υπηρεσίες και προϊόντα. Η ιδιαιτερότητα όμως έγκειται στο είδος των δεδομένων που διαχειρίζεται μια ασφαλιστική εταιρεία. Η διαχείριση ιδιαίτερα ευαίσθητων και προσωπικών δεδομένων καθιστούν αναγκαία την εφαρμογή ενός πλήρους και αποτελεσματικού πλαισίου κυβερνοασφάλειας το οποίο να αξιολογείται και να επικαιροποιείται σε τακτά χρονικά διαστήματα. Για τον λόγο αυτό, είναι αναγκαίο η διεύθυνση της κάθε εταιρείας να αναλάβει την ευθύνη για τον σχεδιασμό, την εφαρμογή και τη συνεχή επικαιροποίηση ενός τέτοιου πλαισίου.

DR. ΝΙΚΟΣ ΤΣΑΛΗΣ

Ο Νίκος Τσάλης ανήκει στο τμήμα συμβουλευτικών υπηρεσιών (Business Consulting Services – BCS) της Logicom Solutions και είναι υπεύθυνος των υπηρεσιών ασφάλειας πληροφοριακών συστημάτων. Το τμήμα αυτό στοχεύει στην παροχή υψηλής ποιότητας συμβουλευτικών υπηρεσιών σε σχέση με την κυβερνοασφάλεια και γενικά την ψηφιακή αναβάθμιση των οργανισμών. Στο παρελθόν, ο Νίκος εργάστηκε ως εσωτερικός ελεγκτής πληροφοριακών συστημάτων σε τραπεζικό ίδρυμα στην Κύπρο και ως εξωτερικός σύμβουλος ασφάλειας στην Ομάδα Ασφάλειας Πληροφοριών και Προστασίας Κρίσιμων Υποδομών του Οικονομικού Πανεπιστημίου Αθηνών της Ελλάδος. Παράλληλα, ασχολήθηκε με την εκπαίδευση σε θέματα ασφάλειας πληροφοριακών συστημάτων σε δημόσια και ιδιωτικά τριτοβάθμια εκπαιδευτικά ιδρύματα σε Ελλάδα και Κύπρο. Κατέχει BSc στην Πληροφορική από το Οικονομικό Πανεπιστήμιο Αθηνών της Ελλάδος, MSc στον τομέα του Information Security από το Royal Holloway University of London του Hv. Βασιλείου και PhD στην Ασφάλεια Πληροφοριακών Συστημάτων από το Οικονομικό Πανεπιστήμιο Αθηνών της Ελλάδος. Επιπλέον, είναι κάτοχος επαγγελματικού τίτλου ελεγκτή πληροφοριακών συστημάτων από τον οργανισμό ISACA.

Πληροφορίες Επικοινωνίας:
Τηλέφωνο: 22 55 10 39
Ηλεκτρονική Διεύθυνση:
n.tsalis@logicom.net
Ιστοσελίδα:
www.logicomsolutions.com.cy