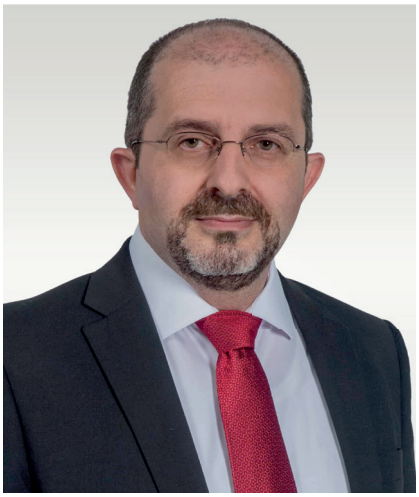


Δρ. Γιάννης Ηλιάδης

Δ/ντής Υποδομών Πληροφορικής, ΤΕΙΡΕΣΙΑΣ Α.Ε. - Πρόεδρος ΔΣ, ISC2 Hellenic Chapter, CISSP, C|CISO, CRISC

CISO: τρεις τρόποι για να μείνεις, ένας για να φύγεις

Ο ρόλος του CISO στην εποχή του ψηφιακού μετασχηματισμού, των αλλεπάλληλων αναδυόμενων κυβερνοαπειλών και της αυξημένης κανονιστικής εποπτείας είναι πολυσχιδής. Ας εξερευνήσουμε τρεις πτυχές του ρόλου που απαντώνται συχνά: ο προστάτης, ο επιχειρηματικός ενισχυτής και ο υπαίτιος.

Ο Προστάτης: Στον πυρήνα του, ο CISO παραμένει ο προστάτης των πληροφοριακών περιουσιακών στοιχείων ενός οργανισμού. Διασφαλίζει ότι ο οργανισμός είναι προετοιμασμένος να αποκρούσει τις κυβερνοεπιθέσεις, να ανακάμψει γρήγορα από τα περιστατικά και να διατηρεί συνεχώς και διαρκώς μέτρα ασφάλειας που μειώνουν τον κίνδυνο στα επιθυμητά επίπεδα.

Ο Επιχειρηματικός Ενισχυτής: Ο CISO φροντίζει ώστε τα μέτρα ασφάλειας να ευθυγραμμίζονται με τους στρατηγικούς στόχους του οργανισμού, χωρίς να εμποδίζει την καινοτομία. Ενσωματώνει την ασφάλεια πληροφοριών στη στρατηγική λήψη αποφάσεων, στην ανάπτυξη προϊόντων και σε άλλες βασικές διαδικασίες. Αυτή η προσέγγιση προάγει μια κουλτούρα ασφάλειας που υποστηρίζει την ανάπτυξη, επιτρέποντας στην εταιρεία να καινοτομεί, αποδεχόμενη τους σχετικούς επιχειρηματικούς κινδύνους, με στόχο κερδοφόρα αποτελέσματα. Η Ασφάλεια Πληροφοριών μετουσιώνεται από αμυντικός μηχανισμός σε κρίσιμο συστατικό της επιχειρηματικής στρατηγικής.

Ο Υπαίτιος: Πρόσφατες περιπτώσεις περιστατικών ασφάλειας που έγιναν γνωστές σε παγκόσμιο επίπεδο είχαν ως τελικό αποτέλεσμα να καταλογισθεί στους αρμόδιους CISO εξ ολοκλήρου η διοικητική ευθύνη ή/και να υποστούν νομικές διώξεις (π.χ. Uber, Solarwinds, Clorox). Η απειλή νομικών ενεργειών προσθέτει μια ανησυχητική διάσταση στις ευθύνες του υπεύθυνου ασφάλειας, θέτοντας το ερώτημα: ποιος είναι ο επόμενος; Πλέον, η συμπερίληψη των υπεύθυνων ασφάλειας σε συμβόλαια ασφάλισης όπως τα Directors & Officers είναι επιβεβλημένη. Η διασφάλιση σαφών καναλιών επικοινωνίας με την εκτελεστική ηγεσία και η κοινή ευθύνη για τις αποφάσεις Ασφάλειας Πληροφοριών μπορούν να βοηθήσουν στη μείωση αυτών των κινδύνων.

Σε ποιο σημείο πρέπει να εστιάσει την προσοχή του ο υπεύθυνος ασφάλειας; Στα κύρια αγαθά του οργανισμού, τα οποία καλείται να προστατεύσει (crown jewels); Στις πολιτικές και διαδικασίες που διαμορφώνει; Ίσως στα πρότυπα και στο κανονιστικό πλαίσιο με το οποίο φροντίζει τη συμμόρφωση; Το κύριο σημείο στο οποίο πρέπει να εστιάζει πάντα την προσοχή του είναι η ομάδα του, τα στελέχη στα οποία στηρίζεται για να επιτελέσει με επιτυχία το έργο του. Αν δεν συμβαίνει αυτό, η θέση του είναι -τουλάχιστον- επισφαλής.

Η ασφάλεια αντιμετωπίζει επί του παρόντος έλλειμμα ανθρώπινου δυναμικού περίπου 4 εκατομμυρίων επαγγελματιών (σύμφωνα με την τελευταία ετήσια παγκόσμια μελέτη του ISC2), με αποτέλεσμα οι ομάδες ασφαλείας να εργάζονται υπερβολικά και να διατηρούν υψηλά επίπεδα άγχους. Η υποστελέχωση οδηγεί σε εξάντληση και υψηλή εναλλαγή προσωπικού, γεγονός που με τη σειρά του επιδεινώνει τους κινδύνους ασφαλείας που αντιμετωπίζει ο οργανισμός. Για να αντιμετωπίσουν αυτήν την πρόκληση, οι υπεύθυνοι ασφάλειας επενδύουν στις ομάδες τους, αναπτύσσουν δημιουργική σκέψη σχετικά με στρατηγικές πρόσληψης και διατήρησης και προωθούν μια κουλτούρα συνεχούς βελτίωσης και εκπαίδευσης των συνάδελφων τους.

Σε ένα τοπίο γεμάτο προκλήσεις, ο ρόλος των CISO είναι αναμφισβήτητα απαιτητικός, με την πιθανότητα καταστροφικών λαθών να παραμονεύει σε κάθε στροφή. Ωστόσο, επενδύοντας με τον κατάλληλο τρόπο στις ομάδες τους, μπορούν να ευδοκιμήσουν στη θέση τους, φροντίζοντας να ισορροπήσουν τον παραδοσιακό ρόλο τους ως υπερασπιστές με την ανάγκη να προωθούν την επιχειρηματική ανάπτυξη και να παράγουν επιχειρηματική αξία.