***ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ***

Τη στρατηγική τους για την [κυβερνοασφάλεια](https://www.naftikachronika.gr/tag/cybersecurity/" \t "https://www.naftikachronika.gr/2020/10/31/kyvernoasfaleia-oi-nees-aspides-ton-epicheiriseon/_blank) αναθεωρούν στελέχη των επιχειρήσεων παγκοσμίως, σύμφωνα με τα αποτελέσματα ετήσιας μελέτης της PwC

Συγκεκριμένα, ποσοστό 96% των ερωτηθέντων ανέφεραν ότι σχεδιάζουν να τροποποιήσουν τη στρατηγική τους για την κυβερνοασφάλεια λόγω του COVID-19, με το 50% να δηλώνει ότι είναι πιο πιθανόν πλέον να λαμβάνουν υπόψη τους την κυβερνοασφάλεια σε κάθε επιχειρηματική απόφαση, σε σύγκριση με 25% πέρυσι.

Επιπλέον, 51% των CEO δηλώνουν ότι είναι πιο πιθανόν να έχουν συχνές αλληλεπιδράσεις με τον Υπεύθυνο Ασφάλειας Πληροφοριών (CISO).

Κατά τους τρεις πρώτους μήνες της πανδημίας, όπως ανέφεραν οι CEO, οι επιχειρήσεις τους επιτάχυναν την ψηφιοποίησή τους με εκπληκτική ταχύτητα, μεταβαίνοντας κατευθείαν στο δεύτερο ή τρίτο έτος των πενταετών πλάνων τους.

Περισσότεροι από το ένα τρίτο (35%) δηλώνουν ότι επιταχύνουν την αυτοματοποίηση για να μειώσουν τα κόστη.

Με 3,5 εκατομμύρια θέσεις εργασίας στην κυβερνοασφάλεια που αναμένεται να καλυφθούν έως το 2021, το πρόβλημα που ταλανίζει τον κλάδο της κυβερνοασφάλειας είναι η έλλειψη εξειδικευμένων εργαζομένων.

Σε ποσοστό 51% τα στελέχη ανέφεραν ότι σχεδιάζουν να προσλάβουν προσωπικό πλήρους απασχόλησης στην κυβερνοασφάλεια κατά τη διάρκεια του επόμενου έτους, με περισσότερους από 22% να δηλώνουν ότι θα αυξήσουν το προσωπικό κατά 5% ή περισσότερο.

Οι θέσεις με το μεγαλύτερο ενδιαφέρον αφορούν σε αρχιτέκτονες λύσεων cloud 43%, υπεύθυνους ασφάλειας πληροφοριών 40% και ανάλυση δεδομένων 37%.

Μια εναλλακτική λύση που έχουν αξιοποιήσει πολλές επιχειρήσεις για να καλύψουν τις κενές θέσεις, είναι οι εσωτερικές μετακινήσεις, μέσα από την αναβάθμιση δεξιοτήτων των υφιστάμενων εργαζομένων. Κάποιες εταιρείες έχουν ξεκινήσει να βασίζονται στο μοντέλο παροχής υπηρεσιών για να καλύψουν την άμεση ανάγκη για εξειδικευμένο ταλαντούχο προσωπικό.

Τα προσδοκώμενα αποτελέσματα για τα επόμενα 2-3 χρόνια είναι: αυξημένη πρόληψη έναντι των επιθέσεων, ταχύτεροι χρόνοι ανταπόκρισης, βελτιωμένη εμπιστοσύνη των επικεφαλής σχετικά με την ικανότητα διαχείρισης απειλών και βελτιωμένη εμπειρία

Αναφορικά με τις προβλέψεις για τους κινδύνους το 2021, το Ίντερνετ των Πραγμάτων (IoT) και οι πάροχοι υπηρεσιών cloud βρίσκονται στην κορυφή της λίστας των «πολύ πιθανών» απειλών (από 33%) ενώ οι κυβερνοεπιθέσεις στις υπηρεσίες cloud είναι πρώτες στη λίστα των απειλών που θα έχουν «σημαντικά αρνητικό αντίκτυπο» (αναφέρθηκαν από το 24%).

Ν. Πενθερουδακης