



ΔΡ. ΙΩΑΝΝΗΣ ΗΛΙΑΔΗΣ
ΠΡΟΕΔΡΟΣ ΔΣ, ISC2 HELLENIC CHAPTER

«Ενδιαφέροντες καιροί» στον χώρο της κυβερνοασφάλειας

«Είθε να ζεις σε ενδιαφέροντες καιρούς», σύμφωνα με την κινέζικη ευχή και κατάρα. Οι καιροί ήταν πάντα ενδιαφέροντες για τους επαγγελματίες της κυβερνοασφάλειας.

Από την εποχή του COVID, το ενδιαφέρον αυξήθηκε κατακόρυφα σε τρεις τομείς: γιγαντώθηκαν οι επαγγελματικές απαιτήσεις, αλλά και η ανάγκη επίγνωσης του κοινού για συναφή θέματα, πολλαπλασιάστηκαν οι διαδικασίες και τα κανονιστικά πλαίσια που οφείλουν να ακολουθούν οι επαγγελματίες του κλάδου και εκτινάχθηκε η πολυπλοκότητα των τεχνολογικών προκλήσεων. Η έλλειψη σε επαγγελματίες κυβερνοασφάλειας έφτασε τα 4 εκατ. στελέχη παγκοσμίως, σημειώνοντας αύξηση κατά 12,6% σε σχέση με το 2022 (ISC2 Cybersecurity Workforce Study 2023). Ο κλάδος είναι υποστελεχωμένος και οι επαγγελματίες καταβάλλουν υπερπροσπάθεια για να ανταπεξέλθουν στις προκλήσεις της εποχής, ενώ ταυτόχρονα 92% εξ αυτών πιστεύει ότι υπάρχει έλλειψη εξειδικευμένης τεχνογνωσίας στους τομείς ασφάλειας του Cloud και της Τεχνητής Νοημοσύνης, σύμφωνα με έρευνα της Verizon. Όσον αφορά στο ευρύ κοινό, 74% των παρεισδύσεων σε συστήματα πληροφορικής (παγκοσμίως) εκμεταλλεύτηκαν τον ανθρώπινο παράγοντα με τεχνικές Κοινωνικής Μηχανικής, με πρωταθλήτρια την τεχνική Business Email Compromise, που σημείωσε διπλασιασμό από το 2017, σύμφωνα με το Global Cybersecurity Outlook 2024, του World Economic Forum.

Σε επίπεδο διεργασιών και κανονιστικών πλαισίων που (οφείλουν να) ακολουθούν οι επαγγελματίες του κλάδου φαίνεται ότι η διασφάλιση της κυβερνοανθεκτικότητας (DORA), η διαχείριση κινδύνων και η αντιμετώπιση περιστατικών (NIS2), καθώς και η ρύθμιση της ορθής και αποδεκτής χρήσης Τεχνητής Νοημοσύνης (AI Act), αποτελούν ορισμένους από τους οδηγούς για την περαιτέρω εξέλιξη του επαγ-

γέλματος. Έπειτα από τόσα νέα κανονιστικά πλαίσια, είναι η πρώτη χρονιά που όσοι ηγούνται ομάδων κυβερνοασφάλειας συμφωνούν με τους ηγέτες των επιχειρήσεων ότι η κυβερνοανθεκτικότητα αποτελεί κρίσιμο επιχειρησιακό παράγοντα και πλέον συν-εξετάζεται ισότιμα με τους υπόλοιπους κινδύνους που διατρέχει μία επιχείρηση, σύμφωνα με το Threat Landscape 23 της ENISA. Η σημασία που αποκτά ο κλάδος υπογραμμίζεται ακόμα περισσότερο από το γεγονός ότι έχουν κάνει πλέον την εμφάνισή τους και υπουργοί Κυβερνοασφάλειας (π.χ. στην Αυστραλία)!

Σε τεχνολογικό επίπεδο, 75% των επαγγελματιών του κλάδου παγκοσμίως πιστεύουν ότι στο τοπίο των κυβερνοαπειλών εκδηλώνονται φέτος οι υψηλότερες προκλήσεις της τελευταίας πενταετίας. Η εξάπλωση του ransomware, η διάδοση των επιθέσεων στην εφοδιαστική αλυσίδα και οι νέες απειλές που εισάγει η χρήση του Cloud συνεχίζουν να απασχολούν ιδιαίτερα τον κλάδο. Όμως, την πρωτοκαθεδρία φαίνεται να παίρνει φέτος η Τεχνητή Νοημοσύνη, η οποία εκτιμάται ότι θα έχει τη μεγαλύτερη επίπτωση στην κυβερνοασφάλεια τα δυο επόμενα χρόνια και ήδη χρησιμοποιείται ευρέως στις επιθέσεις Κοινωνικής Μηχανικής. «Είθε να ζεις σε ενδιαφέροντες καιρούς», σύμφωνα με την κινέζικη ευχή και κατάρα. Οι καιροί είναι όντως ενδιαφέροντες για τους 5,4 εκατ. επαγγελματίες κυβερνοασφάλειας παγκοσμίως, που καλούνται να αντιμετωπίσουν αλληπάλληλες προκλήσεις σε επίπεδο ανθρώπινου δυναμικού, σε θέματα νέων διεργασιών και κανονιστικών πλαισίων που πρέπει να υλοποιήσουν, ταυτόχρονα με τις πρωτόγνωρες τεχνολογικές απειλές που καλούνται να διαχειριστούν.