

ΔΡ. ΓΙΑΝΝΗΣ ΗΛΙΑΔΗΣ

ΠΡΟΕΔΡΟΣ ΔΣ, ISC2-HELLENIC CHAPTER -
ΔΙΕΥΘΥΝΤΗΣ ΥΠΟΔΟΜΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ, ΤΕΙΡΕΣΙΑΣ Α.Ε.

Τεχνητή Νοημοσύνη & κυβερνοασφάλεια στην «εποχή του Υδροχόου»

Το 1969, οι 5th Dimension τραγουδούσαν για το 'Age of Aquarius', που θα μας απελευθέρωνε το μυαλό και θα μας βοηθούσε να καταλαβαίνουμε αλλήλους. Μήπως η 'Εποχή του Υδροχόου' ήρθε με καθυστέρηση 60 ετών, μέσω της άρτι αφιχθείσας Τεχνητής Νοημοσύνης, την οποία όλοι προσπαθούν να αξιοποιήσουν πάσει θυσία; Ο αρχικός ενθουσιασμός έχει αρχίσει να ξεθωριάζει, όμως, καθώς συνειδητοποιούμε ότι πρέπει να θωρακίσουμε τον τρόπο χρήσης της, με στόχο την αύξηση της επιχειρηματικής αξίας προς τα ενδιαφερόμενα μέρη (stakeholders) και το καλό της ανθρωπότητας.

Σε οικονομικό επίπεδο, η αγορά της ΤΝ προβλέπεται να φτάσει τα 1,3 τρισεκατομμύρια δολάρια σε ετήσιο τζίρο ως το 2030. Σε τεχνικό επίπεδο, εταιρικές εφαρμογές ΤΝ επιτυγχάνουν ρυθμούς επεξεργασίας ενός εκατομμυρίου δεδομένων (data points) το δευτερόλεπτο, δημιουργώντας μεγάλα συγκριτικά πλεονεκτήματα υπέρ των εταιρειών που τις αξιοποιούν. Ενώ η ΤΝ λειτουργεί ως σπάνια ευκαιρία προς εκμετάλλευση και πρωτόγνωρος επιχειρηματικός καταλύτης, το 45% των επαγγελματιών κυβερνοασφάλειας παγκοσμίως πιστεύει ότι οι μεγαλύτερες προκλήσεις που θα κληθούν να αντιμετωπίσουν προέρχονται από αναδυόμενες τεχνολογίες, όπως η ΤΝ.

Η ενσωμάτωση της ΤΝ στην Κυβερνοασφάλεια μπορεί να γεννήσει νέες δυνατότητες και να δημιουργήσει μία αμοιβαία επωφελή σχέση. Ενδεικτικά αναφέρουμε δυνατότητες όπως τη μαζική επεξεργασία δεδομένων, με τον εντοπισμό ανωμαλιών και την ενίσχυση των Security Operations Centers με αυτοματισμούς, τη χρήση αλγορίθμων μηχανικής μάθησης για την αναγνώριση κακόβουλων μοτίβων σε λογισμικό, τη ραγδαία επιτάχυνση ελέγχου ασφαλείας πηγαίου κώδικα και την αυτοματοποίηση ελέγχων συμμόρφωσης. Όμως, ταυτόχρονα, η ΤΝ εισάγει νέες απειλές, όπως η άμεση παραγωγή παραπλανητικού περιεχομένου υψηλής ακρίβειας (deepfakes), η επίθεση με τακτικές Denial of Service σε συστήματα ΤΝ αυτόνομων οχημάτων (sponge attacks) και η χειραγώγηση της ΤΝ με στόχο λανθασμένα αποτελέσματα (prompt injection).

Επίσης, η ΤΝ εισάγει νέας γενιάς επιχειρηματικούς κινδύνους. Η ικανότητα της τεχνολογίας να εντοπίζει μοτίβα στα δεδομένα μάρκετινγκ, μπορεί να οδηγήσει σε ακούσιες συνέπειες. Στη διαφήμιση μίας Fintech, αναφερόταν "To the 12,750 people who ordered a single takeaway on Valentine's Day. You OK, hun?". Η διαφήμιση προκάλεσε αρνητική αντίδραση, υπογραμμίζοντας την ανάγκη για ανθρώπινη κρίση, με αυστηρούς κανόνες, στον εντοπισμό μοτίβων. Στην περίπτωση της Air Canada, πάλι, μία ατελής περίληψη πολιτικής αποζημίωσης που δημιουργήθηκε από ΤΝ οδήγησε σε νομικές επιπτώσεις και υψηλές αποζημιώσεις πελατών, αναδεικνύοντας τους κινδύνους υπερβολικής εξάρτησης από περιεχόμενο ΤΝ, το οποίο παράγεται χωρίς την κατάλληλη εποπτεία.

Σύμφωνα με την έρευνα "CSA State of AI & Security Survey 2024», ποσοστό 74% των οργανισμών πιστεύουν ότι, για την αποτελεσματική αντιμετώπιση των αναδυόμενων απειλών, απαιτείται η επανακατάρτιση (reskilling) των επαγγελματιών κυβερνοασφάλειας, η δημιουργία εξειδικευμένων ομάδων διακυβέρνησης και η ύπαρξη κατευθυντήριων γραμμών χρήσης.

Η ΤΝ εξελίσσεται σε εργαλείο επιχειρηματικής ανάπτυξης. Όπως με κάθε εργαλείο, η χρήση της οφείλει να υπόκειται σε μελετημένα business cases. Οι επαγγελματίες κυβερνοασφάλειας θα κληθούν ως αρωγοί σε αυτή τη διεργασία, προκειμένου οι επιχειρήσεις να δημιουργήσουν επιχειρηματική αξία και ανταγωνιστικά πλεονεκτήματα, αντί να αναλωθούν σε ζημιογόνα επιχειρηματικά πυροτεχνήματα.

Μάλλον, λοιπόν, πρέπει να ξεσκονίσουν τη δισκοθήκη με τα παλιά βινύλιά τους τους και να ανασύρουν, αν τον έχουν, τον δίσκο των 5th Dimension. Η 'Εποχή του Υδροχόου' φτάνει…