Εκπαίδευση στην κυβερνοασφάλεια στην εποχή της τεχνητής νοημοσύνης

Δημήτρης Τακετζής
Security Operations Center / Directorate of Cyber Defence / Hellenic National Defence General Staff
Dimitrios T. | LinkedIn

Είναι Ιούνιος του 2004 και έχω οριστεί ως εκπαιδευτής στο Κέντρο Εκπαίδευσης Νεοσυλλέκτων στη Νιγρίτα Σερρών. Η κλασική μέθοδος για τη Βασική Στρατιωτική Εκπαίδευση των κληρωτών μας περιλαμβάνει θεωρητική εκπαίδευση σε εξωτερικό χώρο με τη βοήθεια του πίνακα, του τρίποδα και του αναλογίου για την θεωρητική εκπαίδευση, λίγο πριν ο εκπαιδευτής προχωρήσει στην πρακτική εξάσκηση. Από τις αρχές της δεκαετίας του 2000 είχαμε ήδη εισέλθει στην εποχή της ευρείας χρήσης των ηλεκτρονικών υπολογιστών. Έτσι και εγώ γνώριζα ότι δεν θα αργούσε η στιγμή που όπου ο εκπαιδευόμενος θα απολάμβανε περισσότερο την εκπαίδευση με τη βοήθεια της τεχνολογίας και θα την θεωρούσε πιο διασκεδαστική παρά ως μία αναγκαιότητα στο πλαίσιο του αυστηρού προγράμματος της στρατιωτικής του θητείας.

Βέβαια η εκπαίδευση στα αντικείμενα του Πεζικού για να είναι πραγματικά επωφελής για τον εκπαιδευόμενο, πρέπει να είναι κατά βάση πρακτική, στο πεδίο των ασκήσεων. Από την άλλη, η εκπαίδευση στην κυβερνοασφάλεια μπορεί να διεξαχθεί σχεδόν αποκλειστικά μέσω του ηλεκτρονικού υπολογιστή, γι' αυτό και η πρόοδος της την τελευταία 20ετία είναι γεωμετρική, και ειδικότερα την τελευταία 10ετία με την ευρεία χρήση των υπηρεσιών υπολογιστικού νέφους (cloud services). Πλέον αυτός που επιθυμεί να γίνει ικανός αμυνόμενος ή επιτιθέμενος στον κυβερνοχώρο έχει να διαλέξει από μία ευρεία γκάμα εταιρειών και υπηρεσιών από τις πιο απλές (cyber security awareness) μέχρι τις πιο εξειδικευμένες (red teaming, blue teaming, κτλ.).

Η τεχνητή νοημοσύνη (ΤΝ) είναι το επόμενο μεγάλο άλμα της τεχνολογίας στην εκπαίδευση της κυβερνοασφάλειας. Ασφαλώς η ευρεία χρήση της ΤΝ στην πληροφορική δεν είναι κάτι καινούργιο, όμως από τον Νοέμβριο του 2022 που το ChatGPT έγινε δημόσια διαθέσιμο, όλος ο πλανήτης κατάλαβε την τεράστια αξία και την δυναμική αυτής της τεχνολογίας.

Σήμερα, η ΤΝ αναμένεται να «απογειώσει» την εκπαίδευση στην κυβερνοασφάλεια. Οι παραδοσιακές μέθοδοι εκπαίδευσης με την κλασσική διάλεξη μέσω του Powerpoint και τα στατικά μαθήματα έρχονται να δώσουν τη θέση τους σε ψηφιακούς εκπαιδευτές που θα διδάσκουν το μάθημα έχοντας αντλήσει τις πιο πρόσφατες πληροφορίες την ίδια μέρα που θα γίνεται η εκπαίδευση. Με αυτό τον τρόπο πετυχαίνουμε πιο εύκολα την πολυπόθητη συμμετοχή (engagement) του εκπαιδευόμενου, δηλαδή την εσωτερική παρότρυνση του να ολοκληρώσει επιτυχώς το μάθημα και να αποκομίσει την πολύτιμη γνώση και εμπειρία που του προσφέρει το μάθημα. Όροι όπως upskilling και reskilling, δηλαδή η επέκταση των υφιστάμενων δεξιοτήτων στην κυβερνοασφάλεια, ώστε να αντιμετωπιστούν οι προηγμένες απειλές γίνονται ευρέως γνωστές και οι εταιρείες σπεύδουν να τις υιοθετήσουν για να μην μείνουν πίσω από τον ανταγωνισμό.

Οι εκπαιδευτικές πλατφόρμες χρησιμοποιούν πλέον ΤΝ για να προσαρμόζουν το περιεχόμενο βάσει των ικανοτήτων του εκπαιδευόμενου, να αξιολογούν σε πραγματικό χρόνο την πρόοδό του και να δημιουργούν εξατομικευμένα μονοπάτια μάθησης. Έτσι για παράδειγμα, η εταιρεία που θέλει να προσλάβει ένα νέο εργαζόμενο μπορεί να δημιουργήσει ένα κουίζ με βάση την συγκεκριμένη θέση εργασίας (job description) για την οποία τον προορίζει. Αυτό φυσικά προϋποθέτει την συγκατάθεση του εκπαιδευομένου για την συλλογή των δεδομένων που θα αφορούν αυτή την διαδικασία, αφού η ΤΝ θα παράξει τόσο καλά αποτελέσματα όσο καλή πληροφορία θα λάβει ως είσοδο (input).

Στον τομέα της εκπαίδευσης των εργαζόμενων σε έναν οργανισμό σχετικά με την κυβερνοασφάλεια, η ΤΝ μπορεί επίσης να προσφέρει πολύτιμες υπηρεσίες. Η κοινωνική μηχανική (Social Engineering) αποτελεί την μεγαλύτερη απειλή για τα περιουσιακά στοιχεία (assets) ενός οργανισμού. Με την βοήθεια της ΤΝ σήμερα προσομοιώνουμε σενάρια απειλών από τον πραγματικό κόσμο, όπως επιθέσεις ψαρέματος (phishing) και λυτρισμικού (ransomware), ενώ σε ακόμα πιο εξειδικευμένες περιπτώσεις μπορούμε να ενσωματώσουμε και το τοπίο απειλών (cyber threat landscape), δηλαδή να παρέχουμε στο μοντέλο ΤΝ πληροφορίες για τις απειλές που αντιμετωπίζει ο οργανισμός μας, με σκοπό να μας δημιουργήσει μια προσομοίωση όσο γίνεται πιο κοντά στον πραγματικό κόσμο.

Φανταστείτε λοιπόν ότι οι Ένοπλες Δυνάμεις της Ελλάδας έχουν πάρει την αποστολή να αναπτυχθούν σε μία ξένη χώρα στο πλαίσιο μιας ειρηνευτικής αποστολής. Εγώ ως επικεφαλής της εκπαίδευσης στην κυβερνοασφάλεια, θα πρέπει αρχικά να διερευνήσω διεξοδικά το περιβάλλον που θα αντιμετωπίσει η Μονάδα μου εκεί. Δίκτυα υπολογιστών, επικοινωνίες, Μέσα Κοινωνικής Δικτύωσης, ακόμα και την πολιτική κατάσταση. Αφού έχω αποκτήσει μια γενική εικόνα, μπορώ πλέον να δημιουργήσω μια εξατομικευμένη εκπαίδευση για το προσωπικό μου. Θα αναπαράξω με τη βοήθεια της ΤΝ τα δικτυακά συστήματα για τους τεχνικούς μου σε περιβάλλον υπολογιστικού νέφους, θα προσομοιώσω τα συστήματα επικοινωνιών για να ανιχνεύσω τυχόν απειλές και θα δημιουργήσω σενάρια απειλών στα Μέσα Κοινωνικής Δικτύωσης για την ομάδα της Στρατηγικής Επικοινωνίας (Strategic Communications - StratCom). Έτσι θα εκθέσω τους συναδέλφους μου σε μια διαδραστική εμπειρία χωρίς να υπάρχει κίνδυνος για τα πραγματικά συστήματα και όλα αυτά έχοντας ουσιαστικά εξασφαλίσει τον μέγιστο βαθμό συμμετοχής και ενδιαφέροντος αφού όλοι γνωρίζουν ότι εκπαιδεύονται όπως θα πολεμήσουν (train as you fight)1.

Βέβαια κάθε ισχυρό όπλο όπως η ΤΝ σήμερα ενέχει και διάφορους κινδύνους. Η ΤΝ δημιουργεί πλήθος ηθικών ζητημάτων όπως για παράδειγμα το γεγονός ότι αυτή πολλές φορές λειτουργεί ως «μαύρο κουτί» (black box), δηλαδή, δεν γνωρίζουμε με ποιο τρόπο έχει πάρει μία συγκεκριμένη απόφαση. Αυτό μπορεί να έχει αρνητικές επιπτώσεις όπως για παράδειγμα στην περίπτωση της διαδικασίας πρόσληψης ενός εργαζομένου, όπου αυτός μπορεί να απορριφθεί αυτόματα από το σύστημα χωρίς όμως να έχει κάνει κάποιο σοβαρό λάθος.

Επίσης, επειδή όπως αναφέραμε παραπάνω, το μοντέλο απαιτεί μεγάλο όγκο δεδομένων και μάλιστα ποιοτικών για να παράξει ικανοποιητικά αποτελέσματα, αν για κάποιο λόγο τα δεδομένα αυτά υποκλαπούν τότε ο οργανισμός ή η εταιρεία θα βρεθεί σε μεγάλο κίνδυνο.

Τέλος, δεν μπορούμε να παραλείψουμε την χρήση της ΤΝ επ' ωφελεία των κακόβουλων, όπου τεχνικές όπως deepfakes μπορούν να παρασύρουν ακόμα και τους πιο εκπαιδευμένους στην αντιμετώπιση της κοινωνικής μηχανικής.

Επίλογος

Η ΤΝ ήδη έχει αρχίσει να δημιουργεί το αποτύπωμα της στην εκπαίδευση πάνω στην κυβερνοασφάλεια, ανοίγοντας νέους ορίζοντες και δημιουργώντας καθημερινά νέες προοπτικές σε αυτούς που την υιοθετούν. Πτυχές όπως Προσωποποιημένα Μαθησιακά Ταξίδια (Personalized Learning Journeys), Βιωματική Μάθηση (Experiential Learning), Παιχνιδοποιημένες ασκήσεις (Gamification) και Εκπαίδευση Άμεσης Χρήσης (Just-in-Time Training) είναι μερικές μόνο από τις δυνατότητες που θα μας δώσει η ΤΝ στο άμεσο μέλλον!