

Πώς η τεχνητή νοημοσύνη (A.I.) επηρεάζει την ασφάλεια στο διαδίκτυο;

Με τον όρο τεχνητή νοημοσύνη (ΤΝ) εννοούμε την ικανότητα μιας μηχανής να αναπαράγει τις γνωστικές λειτουργίες ενός ανθρώπου, όπως είναι η μάθηση, ο σχεδιασμός και η δημιουργικότητα.



Οι άνθρωποι προσπάθησαν να αντιμετωπίσουν τους κινδύνους που ενέχει η ταχέως εξελισσόμενη τεχνολογία. Τα συστήματα τεχνητής νοημοσύνης θα μπορούσαν να επισπεύσουν τη διάγνωση ασθενειών, να βοηθήσουν στην αντιμετώπιση της κλιματικής αλλαγής και να εξορθολογήσουν τις διαδικασίες παραγωγής. Παράλληλα, όμως, παρουσιάζουν σημαντικούς κινδύνους από την άποψη της απώλειας θέσεων εργασίας, της παραπληροφόρησης και της εθνικής ασφάλειας.

Ορισμένες εφαρμογές της είναι τα συστήματα ρομποτικής, αυτόματης οδήγησης (smart cars) ακόμη και συστήματα διάγνωσης. Παρόλο που η τεχνητή νοημοσύνη έχει επιφέρει σημαντικές αλλαγές στην σύγχρονη ζωή των ατόμων, αυτοματοποιώντας πολλές διαδικασίες παρουσιάζει και διάφορα θέματα ασφάλειας. Η τεχνητή νοημοσύνη χρησιμοποιείται καθημερινά και εξακολουθεί να συμβάλλει στην διευκόλυνση των ατόμων, στην μείωση των λαθών και στην αυτοματοποίηση των διαδικασιών, όμως οι κίνδυνοι που ελλοχεύει είναι αρκετοί. Ωστόσο, θα συνεχίσει να εξελίσσεται καθώς και οι τρόποι αντιμετώπισης των πιθανών κινδύνων που πρόκειται να προκύψουν.

Ορισμένα παραδείγματα εφαρμογών της τεχνητής νοημοσύνης είναι τα παρακάτω:

1. Διαδικτυακές αγορές και διαφήμιση:

Η τεχνητή νοημοσύνη χρησιμοποιείται ευρέως για την παροχή εξατομικευμένων συστάσεων ή/και διαφημίσεων, για παράδειγμα βάσει προηγούμενων αναζητήσεων και αγορών ή άλλων συμπεριφορών. Η τεχνητή νοημοσύνη παίζει, επίσης, εξαιρετικά σημαντικό ρόλο στο ηλεκτρονικό εμπόριο, καθώς χρησιμοποιείται για τη βελτιστοποίηση προϊόντων, τον προγραμματισμό των αποθεμάτων, τον εφοδιαστικό τομέα, κ.λπ.



2. Διαδικτυακή αναζήτηση: Οι μηχανές αναζήτησης παρέχουν πιο ακριβή αποτελέσματα βάσει της τεράστιας ποσότητας δεδομένων που εισάγουν οι χρήστες στο διαδίκτυο.

3. Προσωπικοί ψηφιακοί βοηθοί: Τα έξυπνα τηλέφωνα (smartphones) χρησιμοποιούν την τεχνητή νοημοσύνη για την παροχή βελτιστοποιημένων και εξατομικευμένων ρυθμίσεων στους χρήστες τους. Ο εικονικός βοηθός λειτουργεί ως προσωπικός γραμματέας του χρήστη: απαντά σε ερωτήσεις, παρέχει συστάσεις, υπενθυμίζει συναντήσεις. Είναι επίσης ένας ηλεκτρονικός συνομιλητής που προσαρμόζεται στα ατομικά χαρακτηριστικά ενός συγκεκριμένου ατόμου, λαμβάνοντας υπόψη το περιβάλλον του χρήστη, το εύρος των ενδιαφερόντων του και τις συνήθειες του.

4. Αυτόματες μεταφράσεις: Τα λογισμικά αυτόματης μετάφρασης και υποτιτλισμού, που βασίζονται είτε σε γραπτό είτε σε προφορικό λόγο, χρησιμοποιούν τη τεχνητή νοημοσύνη για την παροχή και βελτίωση μεταφράσεων.

5. Έξυπνα σπίτια, πόλεις και υποδομές: Οι έξυπνοι θερμοστάτες αναλύουν τη συμπεριφορά μας προκειμένου να αποθηκεύσουν ενέργεια, ενώ οι έξυπνες πόλεις βασίζονται σε ευφυή συστήματα ρύθμισης της κυκλοφορίας, για να βελτιώσουν τη συνδεσιμότητα και να μειώσουν την κυκλοφοριακή συμφόρηση.

6. Αυτοκίνητα: Παρότι τα αυτόνομα οχήματα δεν αποτελούν ακόμα μέρος της καθημερινότητάς μας, τα αυτοκίνητα απαρτίζονται ήδη από ευφυή συστήματα ασφαλείας που κάνουν χρήση τεχνητής νοημοσύνης. Η ΕΕ, για παράδειγμα, συμμετείχε στη χρηματοδότηση των αυτόματων αισθητήρων VI-DAS που εντοπίζουν ενδεχόμενες καταστάσεις κινδύνου και ατυχήματα.

7. Κυβερνοασφάλεια: Τα συστήματα τεχνητής νοημοσύνης μπορούν να συμβάλουν στην αναγνώριση και αντιμετώπιση επιθέσεων και απειλών στον κυβερνοχώρο βάσει της συνεχόμενης εισροής δεδομένων.

Η τεχνητή νοημοσύνη (Α.Ι.) επηρεάζει την ασφάλεια στο διαδίκτυο σε πολλούς τομείς. Σε πρόσφατη έκθεση της βρετανικής κυβέρνησης επισημαίνεται ότι τα συστήματα προηγμένης τεχνητής νοημοσύνης «μπορεί να βοηθήσουν τους κακόβουλους φορείς να εκτελούν επιθέσεις στον κυβερνοχώρο, να διεξάγουν εκστρατείες παραπληροφόρησης και να σχεδιάζουν βιολογικά ή χημικά όπλα». Άρα, γίνεται κατανοητό ότι η τεχνητή νοημοσύνη αν και μπορεί να προσφέρει προηγμένες λύσεις για την αντιμετώπιση κινδύνων, ταυτόχρονα δημιουργεί νέες προκλήσεις. Εδώ είναι μερικοί τρόποι που η Α.Ι. επηρεάζει την κυβερνοασφάλεια:

1. Εντοπισμός και Αντιμετώπιση Κινδύνων:

Εντοπισμός Απειλών: Τα συστήματα Α.Ι. μπορούν να αναλύουν μεγάλα σύνολα δεδομένων, για να εντοπίσουν ανωμαλίες ή ανεπιθύμητες δραστηριότητες στο διαδίκτυο.

Αυτοματοποιημένη Αντιμετώπιση: Ορισμένα συστήματα Α.Ι. μπορούν να λαμβάνουν αυτόματα μέτρα για τον περιορισμό κακόβουλων ενεργειών.

2 Κιβώτια Ασφαλείας και Επίθεση Α.Ι.:

Επιθέσεις με Χρήση Α.Ι.: Οι επιτιθέμενοι μπορεί να χρησιμοποιήσουν την Α.Ι. για τη δημιουργία πιο εξελιγμένων και δύσκολα ανιχνεύσιμων επιθέσεων.

Ανάπτυξη Κιβωτίων Ασφαλείας: Εταιρίες ασφαλείας χρησιμοποιούν την Α.Ι. για την ανάπτυξη προηγμένων κιβωτίων ασφαλείας που προστατεύουν από τις συνεχώς εξελισσόμενες απειλές.

3 Προστασία της Ιδιωτικότητας:

Ανώνυμη Ανάλυση Δεδομένων: Η Α.Ι. μπορεί να χρησιμοποιηθεί για την ανώνυμη ανάλυση δεδομένων χωρίς να αποκαλύπτει προσωπικές πληροφορίες.

4 Κοινωνική Παρακολούθηση:

Επίβλεψη και Ανάλυση: Συστήματα Α.Ι. μπορούν να χρησιμοποιηθούν για την επίβλεψη και ανάλυση δραστηριοτήτων στα κοινωνικά δίκτυα για τον εντοπισμό πιθανών απειλών.



Παρόλο που η Α.Ι. προσφέρει πλεονεκτήματα στον τομέα της κυβερνοασφάλειας, είναι σημαντικό να λαμβάνονται υπόψη η ηθική και οι πτυχές της ιδιωτικότητας για να διασφαλιστεί η υπεύθυνη χρήση της τεχνολογίας.

Πηγές:

- <https://www.kathimerini.gr/economy/562705201/techniti-noimosyni-kai-asfaleia/>, ανακτήθηκε 9/3/2024.
- https://saferinternet4kids.gr/hot-topics/ai_tn/, ανακτήθηκε 28/2/2024.
- <https://bitdefender.gr/blog/texniti-nohmosyni-kai-kyvernoasfaleia/>, ανακτήθηκε 9/3/2024
- <https://saferinternet4kids.gr/nea/artificialintelligence/>, ανακτήθηκε 28/2/2024.