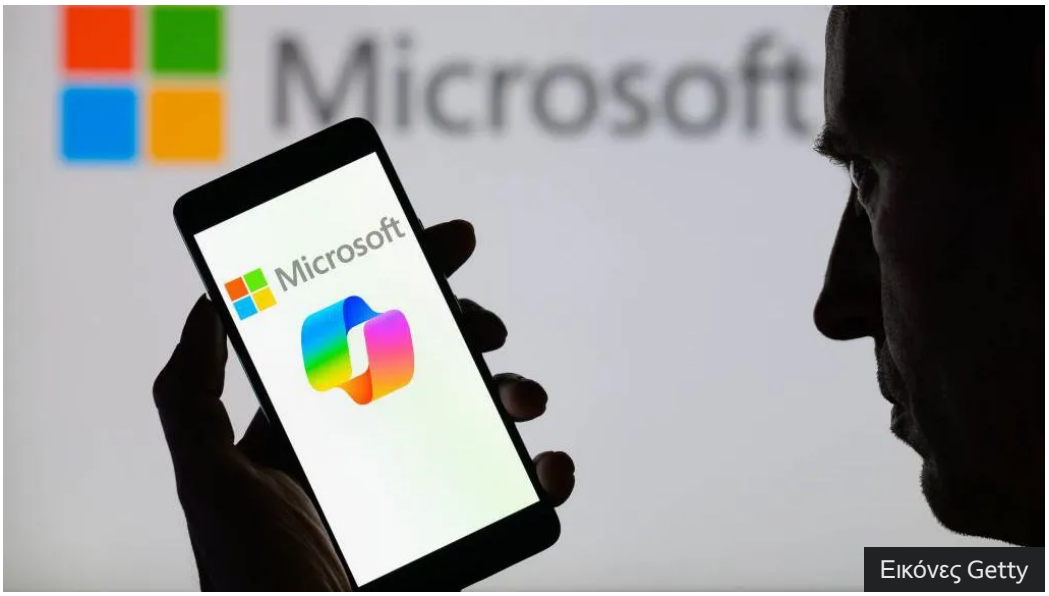
Σφάλμα της Microsoft δείχνει εμπιστευτικά email να εκτίθενται στο εργαλείο τεχνητής νοημοσύνης Copilot

πριν από 2 ημέρες

Μερίδιο Εκτός

Λιβ ΜακΜάχον

Τεχνολογικός ρεπόρτερ



Εικόνες Getty

Η Microsoft παραδέχτηκε ένα σφάλμα που προκάλεσε κατά λάθος την πρόσβαση και τη σύνοψη εμπιστευτικών email ορισμένων χρηστών από τον βοηθό εργασίας της τεχνητής νοημοσύνης.

Ο τεχνολογικός γίγαντας έχει προωθήσει το Microsoft 365 Copilot Chat ως έναν ασφαλή τρόπο για τους χώρους εργασίας και το προσωπικό τους να χρησιμοποιούν το δημιουργικό chatbot τεχνητής νοημοσύνης.

Ωστόσο, ανέφερε ότι ένα πρόσφατο πρόβλημα προκάλεσε την εμφάνιση πληροφοριών σε ορισμένους εταιρικούς χρήστες από μηνύματα που ήταν αποθηκευμένα στα πρόχειρά τους και στους φακέλους απεσταλμένων email - συμπεριλαμβανομένων εκείνων που είχαν επισημανθεί ως εμπιστευτικά.

Η Microsoft αναφέρει ότι κυκλοφόρησε μια ενημέρωση για την επίλυση του προβλήματος και ότι «δεν παρείχε σε κανέναν πρόσβαση σε πληροφορίες που δεν είχε ήδη εξουσιοδότηση να δει».

Ωστόσο, ορισμένοι ειδικοί προειδοποίησαν ότι η ταχύτητα με την οποία οι εταιρείες ανταγωνίζονται για την προσθήκη νέων χαρακτηριστικών τεχνητής νοημοσύνης σήμαινε ότι τέτοιου είδους λάθη ήταν αναπόφευκτα.

Το Copilot Chat μπορεί να χρησιμοποιηθεί σε προγράμματα της Microsoft, όπως το Outlook και το Teams, για email και λειτουργίες συνομιλίας, για να λαμβάνετε απαντήσεις σε ερωτήσεις ή να συνοψίζετε μηνύματα.

«Εντοπίσαμε και αντιμετωπίσαμε ένα πρόβλημα όπου το Microsoft 365 Copilot Chat μπορούσε να επιστρέψει περιεχόμενο από email με ετικέτα εμπιστευτικού χαρακτήρα, τα οποία είχε συντάξει ένας χρήστης και ήταν αποθηκευμένα στα Πρόχειρα και τα Απεσταλμένα στοιχεία στην επιφάνεια εργασίας του Outlook», δήλωσε εκπρόσωπος της Microsoft στο BBC News.

«Ενώ οι πολιτικές ελέγχου πρόσβασης και προστασίας δεδομένων παρέμειναν άθικτες, αυτή η συμπεριφορά δεν ανταποκρινόταν στην προβλεπόμενη εμπειρία Copilot, η οποία έχει σχεδιαστεί για να αποκλείει το προστατευμένο περιεχόμενο από την πρόσβαση στο Copilot», πρόσθεσαν.

"Έχει αναπτυχθεί μια ενημέρωση διαμόρφωσης παγκοσμίως για εταιρικούς πελάτες."

Το λάθος αναφέρθηκε για πρώτη φορά από το τεχνολογικό ειδησεογραφικό πρακτορείο **Bleeping Computer** , το οποίο ανέφερε ότι είδε μια ειδοποίηση υπηρεσίας που επιβεβαίωνε το πρόβλημα.

Επικαλέστηκε μια ειδοποίηση της Microsoft που ανέφερε ότι «τα μηνύματα email των χρηστών με ετικέτα εμπιστευτικότητας υποβάλλονται σε εσφαλμένη επεξεργασία από τη συνομιλία του Microsoft 365 Copilot».

Η ειδοποίηση πρόσθετε ότι μια καρτέλα εργασίας στο Copilot Chat είχε συνοψίσει τα μηνύματα email που ήταν αποθηκευμένα στα πρόχειρα και τους φακέλους απεσταλμένων ενός χρήστη, ακόμη και όταν είχαν μια ετικέτα ευαισθησίας και μια πολιτική πρόληψης απώλειας δεδομένων που είχε ρυθμιστεί για να αποτρέπει την μη εξουσιοδοτημένη κοινή χρήση δεδομένων.

Οι αναφορές υποδεικνύουν ότι η Microsoft αντιλήφθηκε για πρώτη φορά το σφάλμα τον Ιανουάριο.

Η ειδοποίησή της σχετικά με το σφάλμα κοινοποιήθηκε επίσης σε έναν πίνακα ελέγχου υποστήριξης για τους εργαζόμενους του NHS στην Αγγλία - όπου η βασική αιτία αποδίδεται σε ένα "πρόβλημα κώδικα".

Ένα τμήμα της **ειδοποίησης στον ιστότοπο υποστήριξης IT του NHS** υπονοεί ότι έχει επηρεαστεί.

Ωστόσο, δήλωσε στο BBC News ότι το περιεχόμενο οποιουδήποτε προσχεδίου ή απεσταλμένων email που υποβάλλονται σε επεξεργασία από το Copilot Chat θα παραμείνει στους δημιουργούς τους και τα στοιχεία των ασθενών δεν έχουν αποκαλυφθεί.

«Θα υπάρξει διαρροή δεδομένων»

Τα εργαλεία τεχνητής νοημοσύνης για επιχειρήσεις, όπως το Microsoft 365 Copilot Chat - που διατίθενται σε οργανισμούς με συνδρομή στο Microsoft 365 - συχνά διαθέτουν αυστηρότερους ελέγχους και προστασίες ασφαλείας για την αποτροπή της κοινοποίησης ευαίσθητων εταιρικών πληροφοριών.

Ωστόσο, για ορισμένους ειδικούς, το ζήτημα εξακολουθεί να υπογραμμίζει τους κινδύνους υιοθέτησης εργαλείων γενετικής τεχνητής νοημοσύνης σε ορισμένα εργασιακά περιβάλλοντα.

Ο Nader Henein, αναλυτής προστασίας δεδομένων και διακυβέρνησης τεχνητής νοημοσύνης στην Gartner, δήλωσε ότι «αυτό το είδος σύγχυσης είναι αναπόφευκτο», δεδομένης της συχνότητας κυκλοφορίας «νέων και καινοτόμων δυνατοτήτων τεχνητής νοημοσύνης».

Είπε στο BBC News ότι οι οργανισμοί που χρησιμοποιούν αυτά τα προϊόντα τεχνητής νοημοσύνης συχνά δεν διαθέτουν τα εργαλεία που χρειάζονται για να προστατευτούν και να διαχειριστούν κάθε νέα λειτουργία.

«Υπό κανονικές συνθήκες, οι οργανισμοί απλώς θα απενεργοποίησαν τη λειτουργία και θα περίμεναν μέχρι να αναλάβουν δράση οι υπεύθυνοι διακυβέρνησης», δήλωσε ο Henein.

«Δυστυχώς, η πίεση που προκαλείται από τον χείμαρρο της αβάσιμης διαφημιστικής εκστρατείας για την τεχνητή νοημοσύνη το καθιστά σχεδόν αδύνατο», πρόσθεσε.

Ο ειδικός στην κυβερνοασφάλεια, καθηγητής Άλαν Γούντγουορντ του Πανεπιστημίου του Σάρεϊ, δήλωσε ότι αυτό καταδεικνύει τη σημασία του να καταστούν τέτοια εργαλεία ιδιωτικά από προεπιλογή και μόνο με επιλογή.

«Αναπόφευκτα θα υπάρχουν σφάλματα σε αυτά τα εργαλεία, κυρίως καθώς προχωρούν με ιλιγγιώδη ταχύτητα, επομένως, παρόλο που η διαρροή δεδομένων μπορεί να μην είναι σκόπιμη, θα συμβεί», δήλωσε στο BBC News.

Οι μετοχές της Amazon υποχωρούν καθώς εντάσσονται στο ξέσπασμα δαπανών για την τεχνητή νοημοσύνη των μεγάλων τεχνολογιών
Ο παραγωγός του Xbox λέει στο προσωπικό να χρησιμοποιεί την Τεχνητή Νοημοσύνη για να μετριάσει τον πόνο της απώλειας εργασίας
Η Microsoft κυκλοφορεί εργαλείο τεχνητής νοημοσύνης για λήψη στιγμιότυπων οθόνης με την ονομασία «εφιάλτης απορρήτου»