ΒΟΥΛΗ ΤΩΝ ΕΛΛΗΝΩΝ
ΔΙΕΥΘΥΝΣΗ ΚΟΙΝΟΒΟΥΛΕΥΤΙΚΟΥ ΕΛΕΓΧΟΥ

Αριθμ. Πρωτ. ΕΡΩΤΗΣΕΩΝ: 4313
Ημερομ. Κατάθεσης: 29/3/2025

ΒΟΥΛΗ ΤΩΝ ΕΛΛΗΝΩΝ

Αθήνα, 29 Μαρτίου 2025

ΕΡΩΤΗΣΗ

ΠΡΟΣ: *Υπουργό Ψηφιακής Διακυβέρνησης*
Υπουργό Παιδείας, Θρησκευμάτων και Αθλητισμού
Υπουργό Προστασίας του Πολίτη

Θέμα: **«Κυβερνοεπίθεση στο Ελληνικό Ανοικτό Πανεπιστήμιο – Διαρροή 813 GB προσωπικών δεδομένων στο dark web»**

Στις 25 Οκτωβρίου 2024, τα πληροφοριακά συστήματα του Ελληνικού Ανοικτού Πανεπιστημίου (Ε.Α.Π.) δέχθηκαν κακόβουλη επίθεση τύπου ransomware, με αποτέλεσμα τη διαρροή ευαίσθητων προσωπικών δεδομένων σε αρχείο συνολικού μεγέθους 813 GB, το οποίο εντοπίζεται πλέον στο σκοτεινό διαδίκτυο (dark web). Παρά το γεγονός ότι η επίθεση σημειώθηκε πριν από περίπου πέντε μήνες, μόλις πρόσφατα ήρθε στο φως η πλήρης έκταση του περιστατικού, καθώς και η φύση των δεδομένων που εκτέθηκαν.

Σύμφωνα με την επίσημη ανακοίνωση του Ε.Α.Π., τα δεδομένα που ενδέχεται να έχουν διαρρεύσει περιλαμβάνουν μεταξύ άλλων: ονοματεπώνυμα, ΑΦΜ, ΑΜΚΑ, IBAN, ημερομηνίες γέννησης, στοιχεία επικοινωνίας, ακαδημαϊκά και οικονομικά δεδομένα, ιατρικές πληροφορίες, στοιχεία ταυτότητας, φωτογραφίες, ακόμη και υπογραφές. Ενδεικτικά, πρόκειται για πλήρες ψηφιακό προφίλ των φοιτητών, καθηγητών και διοικητικών υπαλλήλων του Ιδρύματος.

Δεδομένης της σοβαρότητας του περιστατικού και της πιθανότητας πρόκλησης ανεπανόρθωτης βλάβης στην ιδιωτικότητα και στην οικονομική ασφάλεια των πολιτών, καθώς και με γνώμονα τη συνταγματική υποχρέωση της Πολιτείας να διαφυλάσσει τα προσωπικά δεδομένα και την ψηφιακή ασφάλεια των πολιτών της..

Ερωτώνται οι αρμόδιοι Υπουργοί:

1. Πόσα φυσικά πρόσωπα έχουν επηρεαστεί από τη συγκεκριμένη διαρροή; Υπάρχει καταγραφή του αριθμού φοιτητών, καθηγητών και διοικητικού προσωπικού των οποίων τα δεδομένα εκτέθηκαν;

2. Πότε ενημερώθηκαν τα υποκείμενα των δεδομένων για τη διαρροή, όπως προβλέπεται από τον Κανονισμό (ΕΕ) 2016/679 (GDPR);

3. Ποια μέτρα ασφαλείας διέθετε το Ε.Α.Π. πριν από την επίθεση; Υπήρχε ενδελεχής αξιολόγηση κινδύνου και εφαρμογή πολιτικών κυβερνοασφάλειας;

4. Γιατί το κακόβουλο λογισμικό απέκτησε πρόσβαση και στην υποδομή των εφεδρικών αντιγράφων; Υπάρχουν ευθύνες για παραλείψεις ή κακή πρακτική;

5. Υπήρξε αξιολόγηση από την Εθνική Αρχή Κυβερνοασφάλειας για το επίπεδο ψηφιακής προστασίας του Ε.Α.Π. πριν ή μετά την επίθεση;

6. Ποιες κυρώσεις προβλέπονται για δημόσιους φορείς που αποτυγχάνουν να διασφαλίσουν προσωπικά δεδομένα σύμφωνα με την ισχύουσα νομοθεσία;

7. Ποιες συγκεκριμένες ενέργειες έχετε δρομολογήσει ώστε να μην επαναληφθούν αντίστοιχα περιστατικά σε άλλα εκπαιδευτικά ιδρύματα ή φορείς του Δημοσίου;

8. Προτίθεται η Κυβέρνηση να ενισχύσει θεσμικά και οικονομικά τη θωράκιση των δημόσιων συστημάτων απέναντι σε ψηφιακές απειλές;

Ο ερωτών Βουλευτής

Γεώργιος Μανούσος
Β2 Δυτικού Τομέα Αθηνών