ΒΟΥΛΗ ΤΩΝ ΕΛΛΗΝΩΝ
ΔΙΕΥΘΥΝΣΗ ΚΟΙΝΟΒΟΥΛΕΥΤΙΚΟΥ ΕΛΕΓΧΟΥ

Αριθμ. Πρωτ. ΕΡΩΤΗΣΕΩΝ: 4436
Ημερομ. Κατάθεσης: 19/4/2024

ΒΟΥΛΗ ΤΩΝ ΕΛΛΗΝΩΝ

ΚΟΙΝΟΒΟΥΛΕΥΤΙΚΗ ΟΜΑΔΑ
ΠΑΣΟΚ - ΚΙΝΗΜΑ ΑΛΛΑΓΗΣ

Αθήνα, 19 Απριλίου 2024

ΕΡΩΤΗΣΗ

Προς τον Υπουργό :
Ψηφιακής Διακυβέρνησης κο. Δημήτριο Παπαστεργίου

ΘΕΜΑ: « Κυβερνοασφάλεια και Διαρροές Προσωπικών Δεδομένων»

Κύριε Υπουργέ,

Πρόσφατα δημοσιεύματα αναφέρουν ότι τα κενά ασφαλείας στα ΕΛΤΑ ήταν γνωστά ένα χρόνο πριν, και πιο αναλυτικά πως «η απειλή ήταν γνωστή, αλλά δεν αντιμετωπίστηκε». Στο άρθρο της Καθημερινής φανερώνεται συγκεκριμένα πως «Τον Απρίλιο του 2021, μια έρευνα στα υπολογιστικά συστήματα των ΕΛΤΑ είχε προειδοποιήσει για τον υψηλό κίνδυνο υποκλοπής δεδομένων. Διαπίστωνε μάλιστα σημαντικά κενά ασφαλείας, χρήση απαρχαιωμένων εφαρμογών, ελλείψεις στην εκπαίδευση προσωπικού και έκρινε ότι υπήρχε μεγάλο ρίσκο επίθεσης τύπου ransomware, με την οποία οι χάκερ θέτουν σε ψηφιακή ομηρία αρχεία και ζητούν λύτρα για την αποδέσμευσή τους. Το χτύπημα ήταν ζήτημα χρόνου.» Η κυβερνοεπίθεση στα Ελληνικά Ταχυδρομεία το 2022 «κόστισε» 3,9 εκατ. ευρώ.

Για αυτή την υπόθεση τον περασμένο Φεβρουάριο η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα επέβαλε πρόστιμο 2,9 εκατ. ευρώ στον οργανισμό.

Παράλληλα η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα διαπιστώνει την παραβίαση πολλαπλών διατάξεων του Γενικού Κανονισμού Προστασίας Δεδομένων, αλλά και την έλλειψη συνεργασίας του Υπουργείου και επιβάλει πρόστιμο 175.000 ευρώ στο Υπουργείο Μετανάστευσης για τα προγράμματα Κένταυρος και Υπερίων (ΑΠΔΠΧ 13/2024).

Επίσης σχεδόν 3 εκατ. ευρώ διεκδικούν δεκάδες απόδημοι για τη διαρροή των email τους ,ενώ αναμένονται εξελίξεις από την Αρχή Προστασίας Δεδομένων Προσωπικού

Χαρακτήρα «κατόπιν της δικής της έρευνας» και σχετικά «με την άρνηση του υπουργείου Εσωτερικών να ικανοποιήσει το δικαίωμα πρόσβασης των αποδήμων με χορήγηση αντιγράφων.

Επιπλέον αυτών, θυμίζουμε αντίστοιχες περιπτώσεις Κυβερνοεπιθέσεων:

- στο Δήμο Θεσσαλονίκης το καλοκαίρι του 2021 όπου οι χάκερ ζητούσαν λύτρα
- στο Εθνικό Σύστημα Διαχείρισης Φυσικού Αερίου το 2022,
- στα Ελληνικά Αμυντικά Συστήματα (ΕΑΣ) το 2021,
- στο Υπουργείο Περιβάλλοντος το 2021,
- το 2020 στην Cosmote με μεγάλης κλίμακας διαρροή δεδομένων και στην οποία πρόσφατα επιβλήθηκε πρόστιμο 6.000.000 € και 3.250.000 € στον ΟΤΕ για διαρροή προσωπικών δεδομένων από την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα,
- στο Μέγαρο Μαξίμου, Ε.Υ.Π, ΕΛ.ΑΣ το 2020

καθώς και

- στο Υφυπουργείο Αθλητισμού το 2019

Σημειώνουμε ότι το ΠΑΣΟΚ, με ερώτηση από τον Μάρτιο του 2022 (με Α.Π 427/28.03.22) προς τον τότε Υπουργό Ψηφιακής Διακυβέρνησης κ. Πιερρακάκη, είχε αναδείξει το σημαντικό αυτό θέμα και την επίθεση στα ΕΛΤΑ χωρίς όμως να λαμβάνει απάντηση. Η στάση αυτή της Νέας Δημοκρατίας και του τότε Υπουργού μας θορυβεί μέχρι και σήμερα, διότι μας κάνει να αναρωτιόμαστε εάν το θέμα θεωρήθηκε ασήμαντο, όπως και η διαρροή έως 5 εκατ. προσώπων στο Dark Web καθώς και τα 2.9 εκατομμύρια πρόστιμο της αρχής.

Γίνεται λοιπόν κατανοητό ότι τα στοιχεία των πολιτών διακινούνται ανεξέλεγκτα είτε μεταξύ των στελεχών της Νέας Δημοκρατίας, είτε ως προϊόν κυβερνοεπιθέσεων. Υπάρχουν αμέτρητες παρόμοιες υποθέσεις που είδαν το φως της δημοσιότητας, άλλες τόσες που δεν το είδαν και φυσικά άγνωστο το πόσες θα ακολουθήσουν.

Με βάση τα παραπάνω ερωτάται ο κος Υπουργός:

- Ποιες είναι οι βασικές πολιτικές και στρατηγικές που έχει υιοθετήσει η κυβέρνηση για την αντιμετώπιση των κυβερνοεπιθέσεων και της διαρροής προσωπικών δεδομένων;
- Πώς οργανώνεται η κυβέρνηση για την αντιμετώπιση αυτών των ζητημάτων; Υπάρχει κάποιος κεντρικός φορέας συντονισμού; Λειτουργεί;

- Ποιος είναι ο π/υ που διατίθενται για την υλοποίηση των μέτρων προστασίας;
- Η κυβέρνηση έχει αξιολογήσει την αποτελεσματικότητα των υφιστάμενων μέτρων; Υπάρχει κάποια συγκεντρωτική αναφορά;
- Στα νέα έργα τι σχεδιασμός γίνεται για αποφυγή παρόμοιων περιστατικών στο μέλλον;
- Ποιές τεχνολογίες και λύσεις ασφαλείας χρησιμοποιούνται από τους κυβερνητικούς φορείς για την προστασία των συστημάτων και των δεδομένων τους;
- Πώς διασφαλίζεται η εκπαίδευση και η ευαισθητοποίηση των υπαλλήλων σε θέματα κυβερνοασφάλειας;
- Πώς διαχειρίζεται η κυβέρνηση τα περιστατικά κυβερνοεπιθέσεων και διαρροής δεδομένων; Υπάρχουν οδηγίες; Ο κάθε φορέας ενεργεί αυτόνομα; Έχουν οι φορείς σχεδία εναλλακτικής λειτουργίας (plan-b);
- Υπάρχει σύστημα έγκαιρης προειδοποίησης κυβερνοεπιθέσεων;
- Ποιες διαδικασίες υπάρχουν για την ενημέρωση των πολιτών σε περίπτωση διαρροής δεδομένων;
- Πώς διασφαλίζεται η συμμόρφωση των κυβερνητικών φορέων με τους κανονισμούς προστασίας δεδομένων;
- Ποιές είναι οι συνεργασίες που έχει η κυβέρνηση με τον ιδιωτικό τομέα και την ακαδημαϊκή κοινότητα για την αντιμετώπιση των κυβερνοαπειλών;
- Πώς προετοιμάζεται η κυβέρνηση για μελλοντικές κυβερνοεπιθέσεις, λαμβάνοντας υπόψη την εξέλιξη των απειλών;
- Ποιές είναι οι ευθύνες των παρόχων υπηρεσιών για την προστασία των δεδομένων των πολιτών;
- Υπάρχει πρόβλεψη για την πρόσληψη ειδικού επιστημονικού προσωπικού στον τομέα των νέων τεχνολογιών πληροφορίας και επικοινωνιών με εξειδίκευση στην κυβερνοασφάλεια στους φορείς;

Οι ερωτώντες βουλευτές

Αχμέτ Ιλχάν

Λιακούλη Ευαγγελία

Σταρακά Χριστίνα

Πάνας Απόστολος

Μάντζος Δημήτριος

Αποστολάκη Ελένη – Μαρία (Μιλένα)

Βατσινά Ελένη

Γερουλάνος Παύλος

Γιαννακοπούλου Κωνσταντίνα (Νάντια)

Γρηγοράκου Παναγιώτα (Νάγια)

Καζάνη Αικατερίνη

Κουκουλόπουλος Παρασκευάς (Πάρις)

Κωνσταντινόπουλος Οδυσσέας

Μιχαηλίδης Σταύρος

Μουλκιώτης Γεώργιος

Μπιάγκης Δημήτριος

Νικητιάδης Γεώργιος

Νικολαΐδης Αναστάσιος

Παπανδρέου Γεώργιος

Παρασκευαΐδης Παναγιώτης

Παραστατίδης Στέφανος

Παρασύρης Φραγκίσκος

Πουλάς Ανδρέας

Σπυριδάκη Αικατερίνη

Τσίμαρης Ιωάννης

Χνάρης Εμμανουήλ

Χρηστίδης Παύλος

Χριστοδουλάκης Εμμανουήλ