

Αριθμ. Πρωτ. ΕΡΩΤΗΣΕΩΝ: 6799
Ημερομ. Κατάθεσης: 24/6/2025



ΕΡΩΤΗΣΗ

Θεσσαλονίκη, 24/06/2025

Του: Βελόπουλου Κυριάκου, Προέδρου Κόμματος, Βουλευτή Β3' Νότιου Τομέα Αθηνών

ΠΡΟΣ: Την κ. Υπουργό Παιδείας, Θρησκευμάτων και Αθλητισμού

ΘΕΜΑ: «Ερωτήματα περί λειτουργίας συγκεκριμένων ιστότοπων Υπουργείων »

Κυρία Υπουργέ,

Στο πλαίσιο της ψηφιακής διακυβέρνησης και της προσπάθειας της Ελλάδας να εκσυγχρονίσει τις δημόσιες υπηρεσίες της, οι κυβερνητικές ιστοσελίδες αποτελούν κρίσιμες υποδομές για την επικοινωνία με τους πολίτες και τη διαχείριση ευαίσθητων δεδομένων. Πρόσφατες πληροφορίες, ωστόσο, αποκαλύπτουν ότι η πλειονότητα των ιστοσελίδων των ελληνικών υπουργείων, όπως αυτές του Υπουργείου Εθνικής Άμυνας, του Υπουργείου Εξωτερικών, του Υπουργείου Παιδείας, Θρησκευμάτων και Αθλητισμού, καθώς και πολλών άλλων, βασίζονται σε πλατφόρμες διαχείρισης περιεχομένου (CMS) όπως το WordPress και το Joomla. Η χρήση αυτών των πλατφορμών εγείρει σοβαρά ζητήματα ασφάλειας, καθώς είναι ευρέως γνωστές στους χάκερ και επιρρεπείς σε ευπάθειες λόγω ξεπερασμένων πρόσθετων, κακών ρυθμίσεων ή μη έγκαιρων ενημερώσεων. Σύμφωνα με αναφορές, το 2024, πάνω από το 40% των επιθέσεων σε ιστοσελίδες WordPress οφείλονταν σε μη ενημερωμένα plugins ή themes, ενώ παρόμοια προβλήματα παρατηρούνται και στο Joomla. Οι κίνδυνοι αυτοί είναι ιδιαίτερα ανησυχητικοί για ιστοσελίδες που διαχειρίζονται ευαίσθητα προσωπικά δεδομένα, όπως ο ιστότοπος του Προσωπικού Αριθμού ή του Υπουργείου Μετανάστευσης και Ασύλου.

Με δεδομένα όλα τα παραπάνω,

Ερωτάται η κ. Υπουργός:

1. Ποιο ήταν το συνολικό κόστος δημιουργίας και ανάπτυξης της ιστοσελίδας του υπουργείου σας;

2. Ποιο είναι το ετήσιο κόστος συντήρησης και λειτουργίας της, συμπεριλαμβανομένων των υπηρεσιών φιλοξενίας, ενημερώσεων και τεχνικής υποστήριξης;
3. Είστε ενήμεροι για τους κινδύνους που ενέχει η χρήση πλατφορμών όπως το WordPress, το Joomla σε κυβερνητικές ιστοσελίδες, ιδιαίτερα όσον αφορά την ευπάθειά τους σε κακόβουλες κυβερνοεπιθέσεις, όπως SQL injection, cross-site scripting (XSS) ή brute force επιθέσεις;
4. Ποια συγκεκριμένα μέτρα και τεχνολογίες έχουν εφαρμοστεί για την προστασία της ιστοσελίδας του υπουργείου σας από κυβερνοεπιθέσεις;
5. Έχουν διενεργηθεί τακτικοί έλεγχοι ασφαλείας (π.χ. penetration testing) για την αξιολόγηση της ανθεκτικότητας του ιστοτόπου σας; Αν ναι, πότε πραγματοποιήθηκε ο τελευταίος έλεγχος και ποια ήταν τα αποτελέσματά του;
6. Εξετάζεται η μετάβαση σε custom-made λύσεις προκειμένου να ενισχυθεί η ασφάλεια και η προσαρμοστικότητα των ιστοσελίδων σας; Εάν όχι, ποιες εναλλακτικές λύσεις προτείνονται για την ενίσχυση της προστασίας των δεδομένων των πολιτών;

Ο ερωτών Βουλευτής

ΒΕΛΟΠΟΥΛΟΣ ΚΥΡΙΑΚΟΣ