ΒΟΥΛΗ ΤΩΝ ΕΛΛΗΝΩΝ
ΔΙΕΥΘΥΝΣΗ ΚΟΙΝΟΒΟΥΛΕΥΤΙΚΟΥ ΕΛΕΓΧΟΥ

Αριθμ. Πρωτ. ΕΡΩΤΗΣΕΩΝ: 5220
Αριθμ. Πρωτ. Αίτησ. Κατ. Εγγράφων: 511
Ημερομ. Κατάθεσης: 12/5/2026

ΒΟΥΛΗ ΤΩΝ ΕΛΛΗΝΩΝ

ΑΠΟΣΤΟΛΟΣ ΠΑΝΑΣ
Βουλευτής Χαλκιδικής
ΠΑΣΟΚ-ΚΙΝΗΜΑ ΑΛΛΑΓΗΣ

11/05/2026

ΕΡΩΤΗΣΗ ΚΑΙ ΑΙΤΗΣΗ ΚΑΤΑΘΕΣΗΣ ΕΓΓΡΑΦΩΝ (Α.Κ.Ε.)

Προς: τον Υπουργό Ψηφιακής Διακυβέρνησης

Θέμα: Σοβαρή ευπάθεια ασφαλείας στο Gov.gr Wallet, καθυστέρηση αποκατάστασης και ζητήματα διαφάνειας και λογοδοσίας

Σύμφωνα με πρόσφατα δημοσιογραφικά ευρήματα, εντοπίστηκε σοβαρή ευπάθεια ασφαλείας στην εφαρμογή **Gov.gr Wallet**, η οποία αφορά την έκδοση για συσκευές Android και φέρεται να παρέμενε ενεργή για σημαντικό χρονικό διάστημα, από τον Σεπτέμβριο 2025 έως και τις 22 Απριλίου 2026.

Η εν λόγω ευπάθεια φέρεται να επέτρεπε, υπό προϋποθέσεις, μη εξουσιοδοτημένη πρόσβαση στο περιεχόμενο της εφαρμογής χωρίς την κανονική διαδικασία ταυτοποίησης χρήστη. Το ζήτημα εντοπίστηκε από ανεξάρτητο ερευνητή και γνωστοποιήθηκε στην Εθνική Αρχή Κυβερνοασφάλειας στις 30 Μαρτίου 2026, η οποία – σύμφωνα με τα ίδια δημοσιεύματα – το αξιολόγησε ως ευπάθεια με δυνητικά σημαντικές επιπτώσεις.

Παρά ταύτα, η αποκατάσταση του προβλήματος φέρεται να ολοκληρώθηκε περίπου τρεις εβδομάδες αργότερα. Το χρονικό αυτό διάστημα, σε συνδυασμό με την απουσία επίσημης ενημέρωσης των πολιτών και τη μη δημοσιοποίηση σχετικών τεχνικών ή διοικητικών στοιχείων, δημιουργεί εύλογα ερωτήματα ως προς:

- την επάρκεια των μηχανισμών εσωτερικού ελέγχου,
- την ταχύτητα αντίδρασης των αρμόδιων φορέων,
- και τη συμμόρφωση με τις υποχρεώσεις διαφάνειας και λογοδοσίας.

Το **Gov.gr Wallet** αποτελεί κρίσιμη εφαρμογή του ψηφιακού κράτους, καθώς φιλοξενεί ψηφιακά έγγραφα υψηλής ευαισθησίας, όπως στοιχεία ταυτότητας, άδειες οδήγησης και λοιπά προσωπικά δεδομένα πολιτών. Ως εκ τούτου, η ασφάλεια, η διαρκής αξιολόγηση κινδύνου και η θεσμική διαχείριση περιστατικών κυβερνοασφάλειας αποκτούν ιδιαίτερη σημασία.

Παράλληλα, το ισχύον ευρωπαϊκό και εθνικό πλαίσιο (ιδίως ο Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR) και η ενσωμάτωση της οδηγίας NIS2 στο εθνικό δίκαιο) επιβάλλει συγκεκριμένες υποχρεώσεις ως προς την αξιολόγηση περιστατικών, τη γνωστοποίηση προς τις αρμόδιες αρχές και, υπό προϋποθέσεις, την ενημέρωση των υποκειμένων των δεδομένων.

Με βάση τα ανωτέρω, προκύπτει ανάγκη πλήρους και θεσμικά τεκμηριωμένης ενημέρωσης της Βουλής.

Ερωτάται ο κ. Υπουργός:

1. **Ποιο είναι το ακριβές χρονοδιάγραμμα εντοπισμού, γνωστοποίησης, αξιολόγησης και αποκατάστασης της συγκεκριμένης ευπάθειας;**
2. **Ποια ήταν η φύση και η τεχνική σοβαρότητα της ευπάθειας, σύμφωνα με την αξιολόγηση των αρμόδιων υπηρεσιών και της Εθνική Αρχή Κυβερνοασφάλειας;**
3. **Προέκυψαν ενδείξεις ή ευρήματα μη εξουσιοδοτημένης πρόσβασης ή εκμετάλλευσης της ευπάθειας κατά το διάστημα που αυτή παρέμεινε ενεργή;**
4. **Για ποιους λόγους μεσολάβησε χρονικό διάστημα περίπου τριών εβδομάδων από τη γνωστοποίηση έως την αποκατάσταση της ευπάθειας;**
5. **Πραγματοποιήθηκε αξιολόγηση περιστατικού παραβίασης δεδομένων προσωπικού χαρακτήρα κατά τα οριζόμενα στον Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR); Αν ναι, ποια ήταν τα συμπεράσματά της και ποια η αιτιολόγηση ως προς τυχόν μη γνωστοποίηση;**
6. **Ενημερώθηκε η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα και, εφόσον όχι, για ποιους λόγους κρίθηκε ότι δεν απαιτείται;**
7. **Υφίσταται θεσμοθετημένο πρόγραμμα τακτικών ελέγχων ασφαλείας (penetration testing) για το Gov.gr Wallet και, εάν ναι, πότε πραγματοποιήθηκαν οι τελευταίοι σχετικοί έλεγχοι;**
8. **Υφίσταται πρόγραμμα υπεύθυνης γνωστοποίησης ευπαθειών (responsible disclosure) ή/και bug bounty για τις κρατικές εφαρμογές και ειδικότερα για το Gov.gr Wallet;**
9. **Ποιος ήταν ο αριθμός ενεργών χρηστών της εφαρμογής κατά το επίμαχο χρονικό διάστημα;**
10. **Προτίθεται το Υπουργείο να προχωρήσει σε θεσμικές παρεμβάσεις για την ενίσχυση της λογοδοσίας και της ανεξάρτητης εποπτείας σε ζητήματα κυβερνοασφάλειας του Δημοσίου;**

Αίτηση Κατάθεσης Εγγράφων (Α.Κ.Ε.)

Παρακαλείται ο κ. Υπουργός να καταθέσει στη Βουλή τα ακόλουθα:

1. **Το πλήρες χρονολόγιο ενεργειών (incident report) από τον εντοπισμό έως την αποκατάσταση της ευπάθειας.**
2. **Την αναφορά γνωστοποίησης της ευπάθειας προς την Εθνική Αρχή Κυβερνοασφάλειας.**
3. **Την εσωτερική αξιολόγηση κινδύνου και σοβαρότητας του περιστατικού.**
4. **Τα σχετικά τεχνικά πορίσματα και καταγραφές (logs), σε βαθμό που δεν θίγεται η ασφάλεια των συστημάτων.**
5. **Τυχόν επικοινωνία ή γνωστοποίηση προς την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.**
6. **Τις συμβάσεις, εκθέσεις και παραδοτέα ελέγχων ασφαλείας (penetration tests, audits) για το Gov.gr Wallet από το 2024 έως σήμερα.**

7. **Το ισχύον πλαίσιο ή κανονισμό για υπεύθυνη γνωστοποίηση ευπαθειών (vulnerability disclosure policy).**

Ο ερωτών Βουλευτής

Πάνας Απόστολος