ΒΟΥΛΗ ΤΩΝ ΕΛΛΗΝΩΝ
ΔΙΕΥΘΥΝΣΗ ΚΟΙΝΟΒΟΥΛΕΥΤΙΚΟΥ ΕΛΕΓΧΟΥ

Αριθμ. Πρωτ. ΕΡΩΤΗΣΕΩΝ: 899
Αριθμ. Πρωτ. Αίτησ. Κατ. Εγγράφων: 161
Ημερομ. Κατάθεσης: 30/10/2026

Αθήνα, 30 Οκτωβρίου 2026

ΕΡΩΤΗΣΗ και ΑΙΤΗΣΗ ΚΑΤΑΘΕΣΗΣ ΕΓΓΡΑΦΩΝ

Προς: Τον Υπουργό Ψηφιακής Διακυβέρνησης κ. Δημήτρη Παπαστεργίου
Τον Υπουργό Εσωτερικών κ. Θεόδωρο Λιβάνιο
Τον Υπουργό Προστασίας του Πολίτη κ. Μιχάλη Χρυσοχοΐδη

Θέμα: «Κυβερνοεπιθέσεις σε διεθνείς ψηφιακές υποδομές και στο ιταλικό Κοινοβούλιο – Πόσο προστατευμένα είναι τα πληροφοριακά συστήματα του Ελληνικού Δημοσίου και τα προσωπικά δεδομένα των πολιτών;»

Οι πρόσφατες διεθνείς κυβερνοεπιθέσεις αναδεικνύουν σοβαρούς κινδύνους για την ασφάλεια πληροφοριακών συστημάτων, την προστασία προσωπικών δεδομένων και τη λειτουργία κρίσιμων ψηφιακών υποδομών.

Στις 29 Οκτωβρίου 2026, το ανταλλακτήριο κρυπτονομισμάτων Binance ανακοίνωσε σοβαρό περιστατικό ασφαλείας, με εκτιμώμενο οικονομικό αντίκτυπο περίπου 6,3 δισεκατομμυρίων δολαρίων. Σύμφωνα με τα αρχικά στοιχεία της έρευνας, ένας από τους πιθανούς τρόπους παραβίασης ήταν η απόκτηση πρόσβασης στον φορητό υπολογιστή μηχανικού της εταιρείας, γεγονός που επέτρεψε την εκτέλεση μη εξουσιοδοτημένων συναλλαγών. Μεταγενέστερες πληροφορίες έκαναν λόγο για περισσότερα σημεία παραβίασης.

Εταιρείες εξειδικευμένες στην ανάλυση κυβερνοεπιθέσεων και συναλλαγών κρυπτονομισμάτων εκτιμούν ότι πίσω από την επίθεση ενδέχεται να βρίσκονται ομάδες που συνδέονται με τη Βόρεια Κορέα, χωρίς να έχει ολοκληρωθεί η διερεύνηση.

Λίγες ημέρες νωρίτερα, στις 27 Οκτωβρίου 2026, δημοσιοποιήθηκε κυβερνοεπίθεση στα πληροφοριακά συστήματα της ιταλικής Βουλής, η οποία αφορούσε λογαριασμούς ηλεκτρονικής αλληλογραφίας βουλευτών, μεταξύ αυτών και της πρωθυπουργού Τζόρτζια Μελόνι. Οι ιταλικές αρχές κινητοποιήθηκαν για τη διερεύνηση και αντιμετώπιση του περιστατικού, ενώ από το γραφείο της πρωθυπουργού διευκρινίστηκε ότι ο συγκεκριμένος λογαριασμός δεν χρησιμοποιούνταν για κυβερνητικές επικοινωνίες.

Τα περιστατικά αυτά καταδεικνύουν την ανάγκη ουσιαστικής προστασίας των συστημάτων από τα οποία εξαρτώνται κρίσιμες λειτουργίες, ιδιαίτερα όταν εργαζόμενοι ή εξωτερικοί συνεργάτες διαθέτουν αυξημένα δικαιώματα πρόσβασης.

Στην Ελλάδα, η συνεχής επέκταση των ψηφιακών υπηρεσιών του Δημοσίου, η διαλειτουργικότητα των κρατικών μητρώων και η χρήση συστημάτων ηλεκτρονικής ταυτοποίησης δημιουργούν αυξημένες απαιτήσεις ασφάλειας. Τα πληροφοριακά συστήματα του κράτους επεξεργάζονται

φορολογικά, ασφαλιστικά, υγειονομικά, οικογενειακά και άλλα προσωπικά δεδομένα εκατομμυρίων πολιτών.

Ιδιαίτερη σημασία έχουν οι μηχανισμοί πρόσβασης και ανταλλαγής πληροφοριών μεταξύ υπηρεσιών, η προστασία των διαπιστευτηρίων των διαχειριστών, η καταγραφή των ενεργειών τους και η δυνατότητα άμεσης απομόνωσης ενός παραβιασμένου λογαριασμού ή συστήματος.

Η ασφάλεια αποκτά πρόσθετη βαρύτητα σε υπηρεσίες όπως το gov.gr, το Gov.gr Wallet, τα πληροφοριακά συστήματα του Προσωπικού Αριθμού και τα μητρώα που χρησιμοποιούνται για την παροχή δημόσιων υπηρεσιών, καθώς ενδεχόμενη μη εξουσιοδοτημένη πρόσβαση θα μπορούσε να επηρεάσει σημαντικό αριθμό πολιτών.

Η προστασία των κρατικών δεδομένων έχει ήδη απασχολήσει τη Βουλή με αφορμή τη διαρροή προσωπικών στοιχείων αποδήμων εκλογέων, τις καταγγελίες για ανεξέλεγκτη διακίνηση δεδομένων εκπαιδευτικών και την εμπορική συγκέντρωση πληροφοριών κρατικών αξιωματούχων από ιδιωτικές πλατφόρμες.

Παράλληλα, το νέο κρατικό σύστημα πιστοληπτικής βαθμολόγησης αναδεικνύει την ανάγκη αυστηρής προστασίας των οικονομικών δεδομένων που αξιοποιούνται για την αξιολόγηση πολιτών και επιχειρήσεων, καθώς και αποτελεσματικού ελέγχου της πρόσβασης σε αυτά.

Με τον ν. 5160/2024 ενσωματώθηκε στην ελληνική νομοθεσία η ευρωπαϊκή Οδηγία NIS2, με την οποία ενισχύθηκαν οι υποχρεώσεις κυβερνοασφάλειας δημόσιων και ιδιωτικών φορέων που υπάγονται στο πεδίο εφαρμογής της. Η Εθνική Αρχή Κυβερνοασφάλειας διαθέτει αρμοδιότητες εποπτείας, ελέγχου, συντονισμού και αντιμετώπισης σημαντικών περιστατικών.

Κατά το 2026 εκδόθηκαν πρόσθετες οδηγίες για την εφαρμογή των απαιτούμενων μέτρων από υπηρεσίες του Δημοσίου και τη διαχείριση ευπαθειών κρίσιμων πληροφοριακών συστημάτων.

Η ύπαρξη νομοθετικών προβλέψεων και διοικητικών οδηγιών καθιστά αναγκαία την παρουσίαση συγκεκριμένων στοιχείων για την εφαρμογή τους, τους ελέγχους που έχουν πραγματοποιηθεί και τα αποτελέσματα που έχουν καταγραφεί.

Με βάση τα ανωτέρω, ερωτάσθε:

1. Πόσα σημαντικά περιστατικά κυβερνοασφάλειας έχουν αναφερθεί στην Εθνική Αρχή Κυβερνοασφάλειας από το 2024 έως σήμερα και πόσα αφορούσαν φορείς της Κεντρικής Διοίκησης, της Τοπικής Αυτοδιοίκησης και παρόχους ψηφιακών υπηρεσιών του Δημοσίου; Σε πόσες περιπτώσεις διαπιστώθηκε μη εξουσιοδοτημένη πρόσβαση, διαρροή δεδομένων ή διακοπή λειτουργίας κρίσιμων υπηρεσιών και ποια ήταν η γενική έκβαση των σχετικών ελέγχων;

2. Ποια συγκεκριμένα μέτρα εφαρμόζονται για την προστασία των διαχειριστικών λογαριασμών και των συσκευών εργαζομένων και εξωτερικών συνεργατών που διαθέτουν αυξημένα δικαιώματα

πρόσβασης σε κρατικά πληροφοριακά συστήματα; Εφαρμόζονται υποχρεωτικά ισχυρή πολυπαραγοντική ταυτοποίηση, διαχωρισμός αρμοδιοτήτων, καταγραφή προνομιακών προσβάσεων και διαδικασίες άμεσης ανάκλησης δικαιωμάτων; Πόσοι σχετικοί έλεγχοι έχουν πραγματοποιηθεί από το 2024 έως σήμερα;

3. Ποιες ανεξάρτητες αξιολογήσεις κυβερνοασφάλειας έχουν πραγματοποιηθεί στα κρίσιμα πληροφοριακά συστήματα που υποστηρίζουν τις υπηρεσίες gov.gr, Gov.gr Wallet, Προσωπικού Αριθμού και τη διαλειτουργικότητα κρατικών μητρώων; Πότε πραγματοποιήθηκαν οι τελευταίοι έλεγχοι και ποια ποσοστά των διαπιστωμένων ευπαθειών έχουν αντιμετωπιστεί; Υπάρχουν τεκμηριωμένα σχέδια απομόνωσης παραβιασμένων συστημάτων ώστε να περιορίζεται η πιθανότητα επέκτασης μιας επίθεσης σε άλλες δημόσιες υπηρεσίες;

4. Ποιοι μηχανισμοί εποπτείας εφαρμόζονται στις ιδιωτικές εταιρείες και στους εξωτερικούς αναδόχους που αναπτύσσουν, συντηρούν ή υποστηρίζουν κρίσιμες κρατικές ψηφιακές υποδομές; Πώς ελέγχονται οι απομακρυσμένες συνδέσεις, τα δικαιώματα πρόσβασης του προσωπικού τους και η συμμόρφωσή τους με τις απαιτήσεις ασφαλείας; Πόσοι έλεγχοι εξωτερικών παρόχων έχουν ολοκληρωθεί από το 2024 και ποιες διορθωτικές ενέργειες ζητήθηκαν;

5. Ποια είναι η πρόοδος εφαρμογής του ν. 5160/2024 και της Οδηγίας NIS2 στους δημόσιους φορείς που υπάγονται στις σχετικές υποχρεώσεις; Πόσοι φορείς έχουν ολοκληρώσει τις προβλεπόμενες αξιολογήσεις κινδύνου, πόσοι έχουν ελεγχθεί από την Εθνική Αρχή Κυβερνοασφάλειας και σε πόσους έχουν διαπιστωθεί ελλείψεις; Με ποιο χρονοδιάγραμμα προβλέπεται η αντιμετώπισή τους;

6. Ποιες ειδικές εγγυήσεις προστατεύουν τα πληροφοριακά συστήματα των εκλογικών διαδικασιών από μη εξουσιοδοτημένη πρόσβαση, εξαγωγή προσωπικών δεδομένων και πιθανές κυβερνοεπιθέσεις; Έχουν ολοκληρωθεί οι προβλεπόμενοι έλεγχοι πρόσβασης, ασφαλείας και διαχείρισης περιστατικών στο Εθνικό Εκλογικό Δίκτυο; Ποια μέτρα εφαρμόστηκαν μετά τις διαπιστωμένες παραβιάσεις προσωπικών δεδομένων αποδήμων εκλογέων;

7. Υπάρχει επικαιροποιημένο εθνικό σχέδιο αντιμετώπισης συντονισμένης κυβερνοεπίθεσης μεγάλης κλίμακας, η οποία θα επηρεάζει ταυτόχρονα πολλαπλές δημόσιες ψηφιακές υπηρεσίες; Πότε πραγματοποιήθηκε η τελευταία διακλαδική άσκηση ετοιμότητας, ποιοι φορείς συμμετείχαν και ποιες διορθωτικές παρεμβάσεις προέκυψαν; Έχουν προβλεφθεί διαδικασίες συνέχισης βασικών υπηρεσιών προς τους πολίτες σε περίπτωση εκτεταμένης διακοπής;

Και αιτούμεθα την κατάθεση των παρακάτω εγγράφων:

1. Συγκεντρωτικό, ανωνυμοποιημένο πίνακα σημαντικών περιστατικών κυβερνοασφάλειας που έχουν αναφερθεί κατά την περίοδο 2024–2026, με κατηγοριοποίηση ανά έτος, γενική κατηγορία φορέα, τύπο περιστατικού και αποτέλεσμα διαχείρισης, χωρίς στοιχεία που θα μπορούσαν να διευκολύνουν μελλοντικές επιθέσεις.

2. Τις διαθέσιμες μη διαβαθμισμένες συγκεντρωτικές εκθέσεις της Εθνικής Αρχής Κυβερνοασφάλειας για την εφαρμογή των απαιτήσεων NIS2 στους δημόσιους φορείς, τον αριθμό των ελέγχων και τον βαθμό υλοποίησης των απαιτούμενων μέτρων.

3. Τις ισχύουσες γενικές οδηγίες και τα μη διαβαθμισμένα πρότυπα ασφαλείας για τη διαχείριση προνομιακών λογαριασμών, την πρόσβαση εξωτερικών αναδόχων, την καταγραφή προσβάσεων και την αντιμετώπιση περιστατικών σε κρίσιμα πληροφοριακά συστήματα του Δημοσίου.

4. Τις διαθέσιμες μη διαβαθμισμένες συγκεντρωτικές εκθέσεις ασκήσεων κυβερνοασφάλειας μεγάλης κλίμακας που πραγματοποιήθηκαν από το 2024 έως σήμερα, με τις γενικές διαπιστώσεις και την πρόοδο υλοποίησης των διορθωτικών μέτρων.

Η Βουλευτής

Ασπασία Ιωάννη Κουρουπάκη
ΒΟΥΛΕΥΤΗΣ Β1' ΒΟΡΕΙΟΥ ΤΟΜΕΑ ΑΘΗΝΩΝ