ΒΟΥΛΗ ΤΩΝ ΕΛΛΗΝΩΝ
ΔΙΕΥΘΥΝΣΗ ΚΟΙΝΟΒΟΥΛΕΥΤΙΚΟΥ ΕΛΕΓΧΟΥ

Αριθμ. Πρωτ. ΕΡΩΤΗΣΕΩΝ: 1564
Αριθμ. Πρωτ. Αίτησ. Κατ. Εγγράφων: 277
Ημερομ. Κατάθεσης: 18/11/2026

ΒΟΥΛΗ ΤΩΝ ΕΛΛΗΝΩΝ

ΕΡΩΤΗΣΗ & ΑΙΤΗΣΗ ΚΑΤΑΘΕΣΗΣ ΕΓΓΡΑΦΩΝ

ΠΡΟΣ: **1. Τον κ. Υπουργό Ψηφιακής Διακυβέρνησης**
2. Τον κ. Υπουργό Εθνικής Άμυνας
3. Τον κ. Υπουργό Προστασίας του Πολίτη
4. Τον κ. Υπουργό Εθνικής Οικονομίας & Οικονομικών
5. Τον κ. Υπουργό Υγείας
6. Τον κ. Υπουργό Υποδομών & Μεταφορών
7. Τον κ. Υπουργό Περιβάλλοντος & Ενέργειας
8. Τον κ. Υπουργό Ανάπτυξης
9. Τον κ. Υπουργό Εσωτερικών

ΘΕΜΑ: «Θωράκιση των κρίσιμων υποδομών της χώρας απέναντι στις υβριδικές απειλές και τις παγκόσμιες ψηφιακές καταρρεύσεις – Ψηφιακή κυριαρχία, επιχειρησιακή συνέχεια και συντονισμός φυσικής και ψηφιακής προστασίας (CER/ NIS2)»

Οι διαδοχικές, εκτεταμένες διακοπές λειτουργίας παγκόσμιων ψηφιακών υπηρεσιών και υποδομών νέφους (Cloud) ανέδειξαν με τον πλέον εμφατικό τρόπο την ευαλωτότητα των σύγχρονων κρατών και την εξάρτησή τους από περιορισμένο αριθμό ιδιωτικών παρόχων τεχνολογίας. Η πρόσφατη διακοπή υπηρεσιών της Microsoft τον Νοέμβριο του 2026, η δυσλειτουργία του Google Cloud τον Οκτώβριο του ίδιου έτους, η οποία επηρέασε μεταξύ άλλων υπηρεσίες της Revolut, αλλά και το εκτεταμένο περιστατικό της CrowdStrike τον Ιούλιο του 2024, κατέδειξαν ότι μια τεχνική αστοχία, μια ελαττωματική ενημέρωση λογισμικού ή ένα πρόβλημα σε υποδομή τρίτου παρόχου μπορεί να προκαλέσει αλυσιδωτές επιπτώσεις σε κρίσιμες υπηρεσίες, επιχειρήσεις και δημόσιους οργανισμούς. Η υπερσυγκέντρωση κρίσιμων λειτουργιών σε περιορισμένο αριθμό παρόχων δημιουργεί, συνεπώς, έναν σοβαρό συστημικό κίνδυνο, ανεξάρτητα από το εάν η διακοπή οφείλεται σε κυβερνοεπίθεση ή σε τεχνική αστοχία.

Ταυτόχρονα, οι σύγχρονες υβριδικές απειλές συνδυάζουν ολοένα περισσότερο την ψηφιακή με τη φυσική διάσταση. Η Εθνική Αρχή Κυβερνοασφάλειας, με προειδοποίησή της στις 14 Οκτωβρίου 2026, γνωστοποίησε τον εντοπισμό περισσότερων από 300 εκτεθειμένων συστημάτων βιομηχανικού ελέγχου στην Ελλάδα, κυρίως ελεγκτών εμπορικής ψύξης. Τα συστήματα αυτά ήταν προσβάσιμα από το δημόσιο διαδίκτυο, με την Αρχή να συστήνει την άμεση αποσύνδεσή τους από αυτό, την αλλαγή των προεπιλεγμένων κωδικών, την εγκατάσταση ενημερώσεων ασφαλείας και τη χρήση ασφαλών μηχανισμών απομακρυσμένης πρόσβασης. Η συγκεκριμένη προειδοποίηση αναδεικνύει ότι η προστασία των κρίσιμων υποδομών δεν μπορεί να περιορίζεται στα κεντρικά πληροφοριακά συστήματα, αλλά πρέπει να επεκτείνεται και στις επιμέρους διασυνδεδεμένες εγκαταστάσεις που υποστηρίζουν βασικές λειτουργίες της οικονομίας και της κοινωνίας.

Η σημασία αυτών των κινδύνων επιβεβαιώνεται και από τις κυβερνοεπιθέσεις σε συστήματα ψύξης επιχειρήσεων τροφίμων στη Γαλλία, οι οποίες αποτέλεσαν αφορμή για την προειδοποίηση της Εθνικής Αρχής Κυβερνοασφάλειας. Παράλληλα, οι αναφορές για προβλήματα σε συστήματα ψύξης και ελληνικών επιχειρήσεων ανέδειξαν την ανάγκη πρόληψης και αποτελεσματικής αντιμετώπισης τέτοιων περιστατικών.

Επιπλέον, οι καταγεγραμμένες ζημιές και οι ενδείξεις εσκεμμένων παρεμβάσεων σε υποθαλάσσιες τηλεπικοινωνιακές και ενεργειακές καλωδιακές υποδομές στην Ευρώπη έχουν αναδείξει τη στρατηγική σημασία της προστασίας τους. Η Ευρωπαϊκή Ένωση έχει ήδη προχωρήσει σε σχέδιο δράσης και ειδικά μέτρα για την ενίσχυση της ασφάλειας και της ανθεκτικότητας των υποθαλάσσιων καλωδίων, αναγνωρίζοντας ότι η διακοπή λειτουργίας τους μπορεί να επηρεάσει κρίσιμες υπηρεσίες και τη διασυνδεσιμότητα των κρατών.

Στην Ελλάδα, ενώ αναπτύσσονται σημαντικές εθνικές ψηφιακές και υπολογιστικές υποδομές, όπως το Κυβερνητικό Νέφος (G-Cloud), οι υποδομές της ΕΔΥΤΕ και ο εθνικός υπερυπολογιστής «Δαίδαλος» στο Λαύριο, παραμένει κρίσιμο το ερώτημα κατά πόσο αυτές εντάσσονται σε έναν συνεκτικό σχεδιασμό ψηφιακής κυριαρχίας και επιχειρησιακής ανθεκτικότητας του Δημοσίου.

Ειδικότερα, απαιτείται σαφής εικόνα του βαθμού εξάρτησης των κρίσιμων κρατικών λειτουργιών από εξωτερικούς εμπορικούς παρόχους, της φιλοξενίας των κρατικών δεδομένων και των εναλλακτικών δυνατοτήτων λειτουργίας σε περίπτωση παρατεταμένης διακοπής των υπηρεσιών αυτών.

Παράλληλα, η εφαρμογή του Ν. 5236/2025, με τον οποίο ενσωματώθηκε η ευρωπαϊκή Οδηγία CER για την ανθεκτικότητα των κρίσιμων οντοτήτων, και του Ν. 5160/2024, με τον οποίο ενσωματώθηκε η Οδηγία NIS2 για την κυβερνοασφάλεια, απαιτεί ουσιαστικό συντονισμό των αρμόδιων υπουργείων και υπηρεσιών. Η φυσική ανθεκτικότητα των κρίσιμων οντοτήτων και η ασφάλεια των δικτύων και πληροφοριακών συστημάτων αποτελούν αλληλοσυμπληρούμενες διαστάσεις της εθνικής ασφάλειας. Η αποτελεσματική αντιμετώπιση υβριδικών περιστατικών προϋποθέτει, επομένως, κοινό σχεδιασμό, σαφή κατανομή αρμοδιοτήτων και δοκιμασμένα σχέδια επιχειρησιακής συνέχειας.

Ιδιαίτερη σημασία έχει και η πρόοδος εφαρμογής του Ν. 5236/2025, καθώς ο προσδιορισμός των κρίσιμων οντοτήτων από τη Γενική Γραμματεία Προστασίας Κρίσιμων Οντοτήτων προβλεπόταν να ολοκληρωθεί έως τις 17 Ιουλίου 2026. Η πορεία υλοποίησης των σχετικών προβλέψεων και η εκπόνηση των απαιτούμενων σχεδίων ανθεκτικότητας αποτελούν κρίσιμα στοιχεία για την αξιολόγηση της πραγματικής ετοιμότητας της χώρας.

Επειδή η ψηφιοποίηση κρίσιμων κρατικών λειτουργιών, όπως η δημόσια διοίκηση, η φορολογική διοίκηση, η υγεία, η δικαιοσύνη και οι ηλεκτρονικές συναλλαγές, δημιουργεί αυξημένες απαιτήσεις προστασίας και επιχειρησιακής συνέχειας,

Επειδή οι διαδοχικές παγκόσμιες διακοπές ψηφιακών υπηρεσιών αναδεικνύουν τους κινδύνους της υπερβολικής εξάρτησης από περιορισμένο αριθμό ιδιωτικών παρόχων και καθιστούν αναγκαία τη διασφάλιση εναλλακτικών λύσεων,

Επειδή η προειδοποίηση της Εθνικής Αρχής Κυβερνοασφάλειας για τα περισσότερα από 300 εκτεθειμένα βιομηχανικά συστήματα ελέγχου στην Ελλάδα καταδεικνύει την ανάγκη προστασίας και των περιφερειακών υποδομών που υποστηρίζουν κρίσιμες λειτουργίες,

Επειδή η αποτελεσματική εφαρμογή των Ν. 5236/2025 (CER) και Ν. 5160/2024 (NIS2) προϋποθέτει συντονισμό της φυσικής και ψηφιακής προστασίας των κρίσιμων οντοτήτων,

Επειδή οι εθνικές υποδομές G-Cloud, ΕΔΥΤΕ και ο υπερυπολογιστής «Δαίδαλος» οφείλουν να εντάσσονται σε έναν συνολικό σχεδιασμό ψηφιακής κυριαρχίας, τεχνολογικής αυτονομίας και ενίσχυσης των εθνικών υπολογιστικών δυνατοτήτων,

Επειδή η προστασία των υποθαλάσσιων καλωδίων, των τηλεπικοινωνιακών και σιδηροδρομικών κόμβων, των δικτύων ενέργειας και των λοιπών κρίσιμων υποδομών αποτελεί ζήτημα εθνικής ασφάλειας,

Ερωτώνται οι κ.κ. Υπουργοί:

1. Ποιος είναι ο βαθμός εξάρτησης των κρίσιμων πληροφοριακών συστημάτων του ελληνικού Δημοσίου στους τομείς της υγείας, της φορολογικής διοίκησης, της δικαιοσύνης, της δημόσιας διοίκησης και της αυτοδιοίκησης από ξένους εμπορικούς παρόχους υπηρεσιών νέφους (Cloud); Ποιο ποσοστό των κρίσιμων κρατικών δεδομένων φιλοξενείται σε κρατικές υποδομές, όπως το G-Cloud, και ποιο σε υποδομές τρίτων παρόχων; Πώς διασφαλίζονται η κυριότητα, η πρόσβαση και η επιχειρησιακή διαθεσιμότητα των δεδομένων σε περίπτωση διακοπής των υπηρεσιών ενός παρόχου;

2. Πώς εντάσσονται οι εθνικές υποδομές G-Cloud, ΕΔΥΤΕ και ο υπερυπολογιστής «Δαίδαλος» σε μια συνεκτική στρατηγική ψηφιακής κυριαρχίας και τεχνολογικής αυτονομίας; Ποιος είναι ο προβλεπόμενος ρόλος τους στην κάλυψη των υπολογιστικών και ψηφιακών αναγκών του ελληνικού Δημοσίου και ποια μέτρα λαμβάνονται για τη μείωση της εξάρτησης από εξωτερικούς εμπορικούς παρόχους;

3. Πώς διασφαλίζεται ο συντονισμός των αρμόδιων υπουργείων και υπηρεσιών για την εφαρμογή των Ν. 5236/2025 (CER) και Ν. 5160/2024 (NIS2); Υπάρχουν συγκεκριμένα πρωτόκολλα συνεργασίας και κοινές διαδικασίες αντιμετώπισης περιστατικών που συνδυάζουν κυβερνοεπιθέσεις, φυσικές δολιοφθορές και διακοπή λειτουργίας κρίσιμων υποδομών; Ποιος φορέας έχει την ευθύνη του συνολικού επιχειρησιακού συντονισμού σε τέτοιες περιπτώσεις;

4. Υπάρχουν επικαιροποιημένα και δοκιμασμένα Σχέδια Επιχειρησιακής Συνέχειας (και εναλλακτικοί μηχανισμοί λειτουργίας, συμπεριλαμβανομένων αναλογικών διαδικασιών, για τα δημόσια νοσοκομεία, τα συστήματα της ΗΔΙΚΑ, την ηλεκτρονική συνταγογράφηση και τους φακέλους ασθενών, την εναέρια κυκλοφορία της ΥΠΑ, τον σιδηρόδρομο, τα δίκτυα ενέργειας ΑΔΜΗΕ και ΔΕΔΔΗΕ, τις δημοτικές επιχειρήσεις ύδρευσης (ΔΕΥΑ) και τα συστήματα πληρωμών (POS, IRIS και διατραπεζικές συναλλαγές), σε περίπτωση γενικευμένης ή πολυήμερης διακοπής ψηφιακών υπηρεσιών; Έχουν πραγματοποιηθεί δοκιμές ετοιμότητας και προσομοιώσεις τέτοιων περιστατικών και ποια ήταν τα αποτελέσματά τους;

5. Ποια είναι η πορεία συμμόρφωσης μετά την επίσημη προειδοποίηση της Εθνικής Αρχής Κυβερνοασφάλειας στις 14 Οκτωβρίου 2026 για τα περισσότερα από 300 εκτεθειμένα βιομηχανικά συστήματα ελέγχου στην Ελλάδα; Πόσα από αυτά έχουν αποσυνδεθεί από το δημόσιο διαδίκτυο ή έχουν λάβει τα απαιτούμενα μέτρα προστασίας; Πόσοι από τους διαχειριστές τους έχουν ενημερωθεί απευθείας από την Αρχή; Πόσα από τα συστήματα αυτά συνδέονται με οντότητες που υπάγονται στο πεδίο εφαρμογής του Ν. 5160/2024 (NIS2), πόσοι σχετικοί έλεγχοι έχουν διενεργηθεί και ποιες κυρώσεις έχουν επιβληθεί όπου συντρέχουν οι νόμιμες προϋποθέσεις; Ποια μέτρα λαμβάνονται για την ασφαλή εγκατάσταση, συντήρηση και απομακρυσμένη πρόσβαση στα συστήματα IoT/OT από εξωτερικούς τεχνικούς και προμηθευτές;

6. Ποια μέτρα λαμβάνονται για τη φυσική και ψηφιακή προστασία των υποθαλάσσιων τηλεπικοινωνιακών και ενεργειακών καλωδίων που συνδέουν τη χώρα με το εξωτερικό, καθώς και των τηλεπικοινωνιακών και σιδηροδρομικών κόμβων; Ποια είναι η πρόοδος συμμόρφωσης των υπόχρεων φορέων με τον Ν. 5160/2024 (NIS2) στους τομείς των κρίσιμων υποδομών και πώς συντονίζονται οι αρμόδιες υπηρεσίες για την πρόληψη και αντιμετώπιση περιστατικών φυσικής ή ψηφιακής δολιοφθοράς;

7. Σε ποιο στάδιο βρίσκεται η εφαρμογή του Ν. 5236/2025 για την ανθεκτικότητα των κρίσιμων οντοτήτων; Έχει ολοκληρωθεί ο προσδιορισμός των κρίσιμων οντοτήτων από τη Γενική Γραμματεία Προστασίας Κρίσιμων Οντοτήτων εντός της προθεσμίας της 17ης Ιουλίου 2026; Πόσες οντότητες έχουν προσδιοριστεί ανά τομέα και ποια είναι η πρόοδος εκπόνησης των απαιτούμενων εκτιμήσεων κινδύνου και σχεδίων ανθεκτικότητας;

Επιπλέον, ζητείται να κατατεθούν στη Βουλή τα κάτωθι έγγραφα:

1. Το ισχύον Εθνικό Πλαίσιο και η Εθνική Στρατηγική Κυβερνοασφάλειας 2026–2030, καθώς και τυχόν επικαιροποιημένες οδηγίες της Εθνικής Αρχής Κυβερνοασφάλειας προς τους φορείς του Δημοσίου και τους ΟΤΑ για την αντιμετώπιση διακοπών λειτουργίας παρόχων υπηρεσιών νέφους.

2. Συγκεντρωτικά στοιχεία για τα κρίσιμα πληροφοριακά συστήματα του Δημοσίου που φιλοξενούνται στο Κυβερνητικό Νέφος (G-Cloud) και στις λοιπές κρατικές υποδομές, έναντι εκείνων που φιλοξενούνται σε υποδομές τρίτων ή εμπορικών παρόχων, καθώς και οι σχετικές συμβάσεις ή τα μνημόνια συνεργασίας με τους παρόχους, κατά το μέρος που αφορούν τη φιλοξενία και την τοποθεσία των δεδομένων, την κυριότητα και την πρόσβαση σε αυτά, καθώς και τις ρήτρες επιχειρησιακής συνέχειας και διαθεσιμότητας (SLA).

3. Τα συγκεντρωτικά στοιχεία για την πορεία συμμόρφωσης των περισσότερων από 300 εκτεθειμένων βιομηχανικών συστημάτων ελέγχου που εντόπισε η Εθνική Αρχή Κυβερνοασφάλειας με την προειδοποίηση της 14ης/10 2026, συμπεριλαμβανομένου του αριθμού των συστημάτων που αποσυνδέθηκαν ή έλαβαν τα απαιτούμενα μέτρα προστασίας, των διαχειριστών που ενημερώθηκαν απευθείας, καθώς και των ελέγχων και των διοικητικών κυρώσεων που έχουν πραγματοποιηθεί ή επιβληθεί σε φορείς που υπάγονται στο πεδίο εφαρμογής του Ν. 5160/2024 (NIS2).

4. Τις εγκυκλίους, τις τεχνικές οδηγίες και τους σχετικούς καταλόγους ελέγχου που έχουν εκδοθεί προς τους φορείς του Δημοσίου, τα νοσοκομεία, το ΕΚΕΑ, τους ΟΤΑ, τις ΔΕΥΑ και τους φορείς ενέργειας, μεταφορών και εφοδιαστικής αλυσίδας για την ασφάλεια των συσκευών IoT και των συστημάτων βιομηχανικού ελέγχου (OT), καθώς και για την ασφαλή εγκατάσταση και συντήρησή τους.

5. Τις εκθέσεις απολογισμού των τελευταίων ασκήσεων κυβερνοασφάλειας και αντιμετώπισης υβριδικών απειλών, συμπεριλαμβανομένης τυχόν άσκησης «ΠΑΝΟΠΤΗΣ» ή αντίστοιχων δοκιμών ετοιμότητας υπό τον συντονισμό της Εθνικής Αρχής Κυβερνοασφάλειας και των αρμόδιων υπηρεσιών ασφαλείας.

6. Το χρονοδιάγραμμα πλήρους λειτουργίας του υπερυπολογιστή «Δαίδαλος», το πλαίσιο διασύνδεσής του με τις υποδομές της ΕΔΥΤΕ και τα στοιχεία σχετικά με την προβλεπόμενη αξιοποίησή του για την κάλυψη υπολογιστικών αναγκών του ελληνικού Δημοσίου.

7. Τα διαθέσιμα στοιχεία για την πορεία εφαρμογής του Ν. 5236/2025, συμπεριλαμβανομένου του αριθμού των κρίσιμων οντοτήτων που έχουν προσδιοριστεί ανά τομέα, των σχετικών εκτιμήσεων κινδύνου, της προόδου εκπόνησης των σχεδίων ανθεκτικότητας και των χρονοδιαγραμμάτων ολοκλήρωσής τους.

8. Τα διαθέσιμα Σχέδια Επιχειρησιακής Συνέχειας των ανωτέρω κρίσιμων δημόσιων υποδομών, καθώς και τις εκθέσεις ή τα πορίσματα των δοκιμών και ασκήσεων που έχουν πραγματοποιηθεί για την αντιμετώπιση παρατεταμένων διακοπών ψηφιακών υπηρεσιών και υποδομών νέφους.

Σε περίπτωση που τμήματα των ανωτέρω εγγράφων περιλαμβάνουν πληροφορίες διαβαθμισμένου χαρακτήρα ή στοιχεία που δεν μπορούν να δημοσιοποιηθούν για λόγους εθνικής ασφάλειας, ζητούνται οι αντίστοιχες αποχαρακτηρισμένες επιτελικές συνόψεις και τα βασικά συμπεράσματα.

Η ερωτώσα βουλευτής

Παναγιού (Γιώτα) Πούλου

Βουλευτής Βοιωτίας