

Αριθμ. Πρωτ. ΕΡΩΤΗΣΕΩΝ: 184
Αριθμ. Πρωτ. Αίτησ. Κατ. Εγγράφων: 36
Ημερομ. Κατάθεσης: 8/10/2026



**ΒΟΥΛΗ ΤΩΝ ΕΛΛΗΝΩΝ
ΚΟΙΝΟΒΟΥΛΕΥΤΙΚΗ ΟΜΑΔΑ
ΠΑΣΟΚ-ΚΙΝΗΜΑ ΑΛΛΑΓΗΣ**

Αθήνα 8/10/2026

ΕΡΩΤΗΣΗ & ΑΚΕ

Προς:

Τον Υπουργό Εθνικής Οικονομίας και Οικονομικών
Τον Υπουργό Ψηφιακής Διακυβέρνησης
Τον Υπουργό Προστασίας του Πολίτη

Θέμα:

«Σοβαρή κυβερνοεπίθεση στο Νομικό Συμβούλιο του Κράτους – Ερωτήματα για την έκταση της παραβίασης, την επιχειρησιακή συνέχεια, την προστασία των δεδομένων και τη διαχείριση του περιστατικού»

Σοβαρά ερωτήματα για την ασφάλεια των πληροφοριακών συστημάτων του Νομικού Συμβουλίου του Κράτους (ΝΣΚ), τη διαχείριση της πρόσφατης κυβερνοεπίθεσης και την προστασία κρίσιμων δεδομένων του Ελληνικού Δημοσίου προκαλούν δημοσιεύματα της εφημερίδας «Το Βήμα» της 1ης Σεπτεμβρίου 2026.

Σύμφωνα με τα δημοσιεύματα, στις αρχές Αυγούστου το ΝΣΚ δέχθηκε σοβαρή κυβερνοεπίθεση τύπου ransomware. Οι δράστες φέρονται να απέκτησαν πρόσβαση στα πληροφοριακά του συστήματα, να αφαίρεσαν ή να κρυπτογράφησαν δεδομένα και να απαίτησαν την καταβολή λύτρων.

Οι δημοσιογραφικές πληροφορίες που έχουν δημοσιοποιηθεί εγείρουν, μεταξύ άλλων, ερωτήματα ως προς την έκταση της πρόσβασης των δραστών και την ενδεχόμενη εξαγωγή δεδομένων, τη δυνατότητα των λειτουργών του ΝΣΚ να έχουν πρόσβαση στα αναγκαία υπηρεσιακά δεδομένα, την ύπαρξη και λειτουργικότητα των αντιγράφων ασφαλείας και των υποδομών ανάκτησης από καταστροφή, καθώς και ως προς το εάν υπήρξε επικοινωνία ή διαπραγμάτευση με τους δράστες και εάν καταβλήθηκε οποιοδήποτε ποσό ως λύτρα.

Οι πληροφορίες αυτές πρέπει να **επιβεβαιωθούν ή να διαψευστούν επισήμως**. Εφόσον επιβεβαιωθεί ότι υπήρξαν σοβαρές ελλείψεις στους μηχανισμούς ασφάλειας, επιχειρησιακής συνέχειας ή ανάκτησης δεδομένων, ανακύπτει μείζον ζήτημα ως προς την ανθεκτικότητα ενός πληροφοριακού συστήματος κρίσιμου για τη λειτουργία του Ελληνικού Δημοσίου. Στο αρχικό σχέδιο οι σχετικές πληροφορίες εμφανίζονταν επίσης ως δημοσιογραφικές αναφορές και όχι ως ήδη αποδεδειγμένα περιστατικά.

Το πληροφοριακό σύστημα του ΝΣΚ δεν αποτελεί ένα απλό σύστημα ηλεκτρονικού πρωτοκόλλου. Περιλαμβάνει τη διαχείριση δικαστικών υποθέσεων του Δημοσίου, δικογράφων, δικασίμων και προθεσμιών, γνωμοδοτήσεων, νομικού αρχείου και νομολογίας, καθώς και την ηλεκτρονική διακίνηση εγγράφων μεταξύ του ΝΣΚ,

υπουργείων και άλλων δημόσιων υπηρεσιών. Ενδεχόμενη μη εξουσιοδοτημένη πρόσβαση, αφαίρεση, αλλοίωση ή διαρροή τέτοιων δεδομένων μπορεί συνεπώς να έχει σημαντικές θεσμικές, δικονομικές και οικονομικές συνέπειες.

Παράλληλα, βρίσκεται σε εξέλιξη έργο αναβάθμισης του πληροφοριακού συστήματος του ΝΣΚ. Απαιτείται επομένως να αποσαφηνιστούν το ακριβές συμβατικό αντικείμενο, το χρονοδιάγραμμα υλοποίησης και η κατάσταση των σχετικών παραδοτέων και, κυρίως, να προσδιοριστεί ποιος φορέας και ποιος ανάδοχος είχαν κατά τον χρόνο εκδήλωσης του περιστατικού τις επιμέρους συμβατικές και επιχειρησιακές ευθύνες για τη λειτουργία, συντήρηση, κυβερνοπροστασία, δημιουργία αντιγράφων ασφαλείας και ανάκτηση του πληροφοριακού συστήματος που επηρεάστηκε.

Περαιτέρω, η απουσία επίσημης δημόσιας ενημέρωσης επί σειρά εβδομάδων γεννά εύλογα ερωτήματα. Η προσωρινή μη δημοσιοποίηση τεχνικών λεπτομερειών μπορεί ασφαλώς να δικαιολογείται για λόγους κυβερνοασφάλειας ή προστασίας μιας εν εξελίξει ποινικής έρευνας. Δεν αναιρεί όμως την ανάγκη θεσμικής ενημέρωσης και λογοδοσίας ούτε τις υποχρεώσεις αναφοράς που προβλέπει το ισχύον θεσμικό πλαίσιο.

Υπενθυμίζεται ότι το άρθρο 16 του ν. 5160/2024, με τον οποίο ενσωματώθηκε το άρθρο 23 της Οδηγίας (ΕΕ) 2022/2555 (NIS2), προβλέπει συγκεκριμένο πλαίσιο αναφοράς σημαντικών περιστατικών κυβερνοασφάλειας, με έγκαιρη προειδοποίηση εντός 24 ωρών, κοινοποίηση περιστατικού εντός 72 ωρών και τελική έκθεση εντός της προβλεπόμενης προθεσμίας. Παράλληλα, σε περίπτωση παραβίασης δεδομένων προσωπικού χαρακτήρα εφαρμόζονται οι σχετικές υποχρεώσεις που απορρέουν από τον Γενικό Κανονισμό Προστασίας Δεδομένων.

Κατόπιν αυτών, ερωτώνται οι αρμόδιοι Υπουργοί:

1. Ποια ακριβώς ημερομηνία εκδηλώθηκε και πότε εντοπίστηκε η κυβερνοεπίθεση στο ΝΣΚ; Ποια ήταν, στο μέτρο που η δημοσιοποίησή της δεν δημιουργεί νέο κίνδυνο ασφάλειας ή δεν επηρεάζει την ποινική έρευνα, η αρχική πύλη εισόδου των δραστών και για πόσο χρονικό διάστημα είχαν πρόσβαση στα πληροφοριακά συστήματα;
2. Αφαιρέθηκαν, αντιγράφηκαν ή εξήχθησαν δεδομένα από τα πληροφοριακά συστήματα του ΝΣΚ; Εφόσον ναι, ποιος ήταν ο συνολικός όγκος και ποιες κατηγορίες δεδομένων αφαιρέθηκαν, αντιγράφηκαν, κρυπτογραφήθηκαν, αλλοιώθηκαν ή καταστράφηκαν;
3. Επηρεάστηκαν δικόγραφα, γνωμοδοτήσεις, δικαστικές προθεσμίες, στοιχεία εκκρεμών υποθέσεων, εμπιστευτικά έγγραφα, προσωπικά δεδομένα ή πληροφορίες που αφορούν τη νομική στρατηγική και τις οικονομικές διεκδικήσεις του Ελληνικού Δημοσίου;
4. Υπήρξε διακοπή ή περιορισμός της πρόσβασης των λειτουργών του ΝΣΚ σε δικόγραφα και λοιπά υπηρεσιακά δεδομένα και, εφόσον ναι, για πόσο χρονικό διάστημα; Πόσες υποθέσεις, δικάσιμοι και δικαστικές ή διοικητικές προθεσμίες επηρεάστηκαν;
5. Χάθηκε, παρήλθε ή κινδύνευσε να παρέλθει οποιαδήποτε προθεσμία για την άσκηση ένδικου μέσου ή άλλης διαδικαστικής ενέργειας; Προέκυψε ή ενδέχεται να προκύψει οικονομική, δικονομική ή άλλη ζημία για το Ελληνικό Δημόσιο;

6. Διέθετε το ΝΣΚ, κατά τον χρόνο της επίθεσης, λειτουργικά, επικαιροποιημένα και επαρκώς απομονωμένα από το βασικό δίκτυο αντίγραφα ασφαλείας; Πότε είχε πραγματοποιηθεί η τελευταία δοκιμή επιτυχούς επαναφοράς δεδομένων από τα αντίγραφα αυτά και χρησιμοποιήθηκαν τελικά για την αποκατάσταση των συστημάτων;
7. Λειτουργούσε κατά τον χρόνο της επίθεσης δευτερογενές πληροφοριακό σύστημα ή άλλη υποδομή ανάκτησης από καταστροφή; Εάν όχι, για ποιους λόγους και ποια εναλλακτικά μέτρα επιχειρησιακής συνέχειας και αποκατάστασης ίσχυαν;
8. Ποιο είναι το ακριβές αντικείμενο, η συμβατική αξία, η πηγή χρηματοδότησης, το αρχικό χρονοδιάγραμμα και η σημερινή κατάσταση υλοποίησης του έργου αναβάθμισης του πληροφοριακού συστήματος του ΝΣΚ;
9. Προβλέπει η σχετική σύμβαση τη δημιουργία δευτερογενούς συστήματος, μηχανισμών εφεδρικών αντιγράφων ή/και υποδομής ανάκτησης από καταστροφή; Ποια από τα σχετικά παραδοτέα έπρεπε, σύμφωνα με το ισχύον κατά τον χρόνο της επίθεσης συμβατικό χρονοδιάγραμμα, να έχουν ήδη παραδοθεί και ποια είχαν πράγματι παραληφθεί;
10. Ποια είναι σήμερα η συμβατική ημερομηνία ολοκλήρωσης του έργου; Έχουν δοθεί παρατάσεις, έχουν τροποποιηθεί το χρονοδιάγραμμα, οι όροι ή το οικονομικό αντικείμενο της σύμβασης και έχουν ενεργοποιηθεί ή εξεταστεί συμβατικές ρήτρες για τυχόν καθυστερήσεις;
11. Ποιος φορέας και ποιος ανάδοχος είχαν, κατά τον χρόνο εκδήλωσης της κυβερνοεπίθεσης, τη συμβατική και επιχειρησιακή ευθύνη για τη λειτουργία, συντήρηση, κυβερνοπροστασία, δημιουργία και τήρηση αντιγράφων ασφαλείας και ανάκτηση του πληροφοριακού συστήματος που επηρεάστηκε; Έχει ελεγχθεί εάν τηρήθηκαν οι σχετικές συμβατικές υποχρεώσεις;
12. Ζήτησαν οι δράστες λύτρα και ποιο ήταν το ύψος του αιτήματος; Υπήρξε άμεση ή έμμεση επικοινωνία ή διαπραγμάτευση εκπροσώπων του Δημοσίου, του ΝΣΚ ή τρίτου μέρους με τους δράστες;
13. Καταβλήθηκε, άμεσα ή έμμεσα, οποιοδήποτε ποσό ή άλλο αντάλλαγμα στους δράστες από δημόσιο φορέα, ανάδοχο, ασφαλιστική εταιρεία ή τρίτο μέρος; Εφόσον ναι, ποιος αποφάσισε την καταβολή, από ποια πηγή χρηματοδοτήθηκε και με ποια διαδικασία;
14. Εφόσον δεν καταβλήθηκαν λύτρα, με ποιον τρόπο ανακτήθηκαν ή αποκαταστάθηκαν τα δεδομένα και οι υπηρεσίες; Έχει ελεγχθεί και πιστοποιηθεί η πληρότητα, ακεραιότητα και ασφάλεια των δεδομένων που αποκαταστάθηκαν και από ποιον φορέα;
15. Πότε πραγματοποιήθηκαν οι προβλεπόμενες από το άρθρο 16 του ν. 5160/2024 αναφορές προς τις αρμόδιες αρχές κυβερνοασφάλειας και τηρήθηκαν οι προβλεπόμενες προθεσμίες; Πότε και με ποια διαδικασία ενημερώθηκαν, κατά λόγο αρμοδιότητας, οι αρμόδιες διωκτικές και εισαγγελικές αρχές και, εφόσον συνέτρεχε σχετική υποχρέωση, η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα;
16. Διαπιστώθηκε παραβίαση δεδομένων προσωπικού χαρακτήρα; Εφόσον ναι, ποιες κατηγορίες δεδομένων και προσώπων επηρεάστηκαν και τηρήθηκαν οι

προβλεπόμενες υποχρεώσεις γνωστοποίησης και, όπου απαιτείται, ενημέρωσης των υποκειμένων των δεδομένων;

17. Υπήρξε απόφαση, εισήγηση ή οδηγία σχετικά με τη δημόσια γνωστοποίηση ή την προσωρινή μη γνωστοποίηση του περιστατικού; Εφόσον ναι, από ποιο όργανο, τότε και με ποια αιτιολογία;
18. Υπάρχει ενιαίο και εγκεκριμένο πρωτόκολλο για τη δημόσια ενημέρωση σε περίπτωση σοβαρής κυβερνοεπίθεσης σε δημόσιο φορέα; Ποια είναι τα κριτήρια βάσει των οποίων αποφασίζεται η έκταση και ο χρόνος της δημόσιας ενημέρωσης;
19. Πότε πραγματοποιήθηκαν ο τελευταίος έλεγχος κυβερνοασφάλειας, η τελευταία δοκιμή διείσδυσης και η τελευταία άσκηση επιχειρησιακής συνέχειας ή ανάκτησης από καταστροφή στο ΝΣΚ πριν από το περιστατικό; Ποια κενά είχαν εντοπιστεί και ποια από αυτά παρέμεναν σε εκκρεμότητα κατά τον χρόνο της επίθεσης;
20. Έχει διαταχθεί ανεξάρτητος τεχνικός, διοικητικός ή άλλος αρμόδιος έλεγχος για τη διερεύνηση του περιστατικού και τυχόν ευθυνών σχετικά με την επάρκεια των μηχανισμών ασφάλειας και εφεδρείας, την πορεία υλοποίησης των σχετικών έργων και συμβάσεων και τη συνολική διαχείριση της επίθεσης;
21. Ποια μέτρα έχουν ληφθεί για τον περιορισμό του κινδύνου περαιτέρω αξιοποίησης δεδομένων που ενδεχομένως αφαιρέθηκαν, ιδίως για εκβιασμό, απάτες, παρεμβάσεις σε δικαστικές υποθέσεις ή νέες επιθέσεις σε διασυνδεδεμένους δημόσιους φορείς;
22. Προτίθεται η κυβέρνηση, μετά την ολοκλήρωση της διερεύνησης του περιστατικού και εφόσον δεν τίθεται σε κίνδυνο η ασφάλεια των πληροφοριακών συστημάτων, η προστασία διαβαθμισμένων ή άλλων προστατευόμενων πληροφοριών ή η εξέλιξη τυχόν ποινικής έρευνας, να δημοσιοποιήσει επίσημη έκθεση για τα αίτια, την έκταση και τις επιπτώσεις της κυβερνοεπίθεσης, το κόστος αποκατάστασης, τα μέτρα που ελήφθησαν και τις τυχόν ευθύνες που θα έχουν διαπιστωθεί;
23. Έχει διενεργηθεί ή προγραμματίζεται, με αφορμή το συγκεκριμένο περιστατικό, οριζόντιος έλεγχος στους λοιπούς φορείς του Δημοσίου που εμπίπτουν στο πεδίο εφαρμογής του ν. 5160/2024, ιδίως ως προς την ύπαρξη λειτουργικών, επικαιροποιημένων, απομονωμένων και δοκιμασμένων αντιγράφων ασφαλείας, σχεδίων ανάκτησης από καταστροφή και σχεδίων επιχειρησιακής συνέχειας; Πόσοι από τους φορείς αυτούς διαθέτουν σήμερα εγκεκριμένα και δοκιμασμένα σχέδια επιχειρησιακής συνέχειας και ανάκτησης από καταστροφή και σε πόσους έχουν εντοπιστεί ελλείψεις που απαιτούν διορθωτικές ενέργειες;

Αίτηση Κατάθεσης Εγγράφων

Παρακαλούνται οι αρμόδιοι Υπουργοί να καταθέσουν στη Βουλή, **με την εξαίρεση των τεχνικών, επιχειρησιακών, διαβαθμισμένων ή άλλων πληροφοριών των οποίων η δημοσιοποίηση θα μπορούσε να δημιουργήσει κίνδυνο για την ασφάλεια των συστημάτων, να διευκολύνει μελλοντικές επιθέσεις ή να επηρεάσει εν εξελίξει έρευνα:**

1. Τη σύμβαση για την αναβάθμιση του πληροφοριακού συστήματος του ΝΣΚ, μαζί με τα παραρτήματα, το αρχικό και ισχύον χρονοδιάγραμμα, τις τροποποιήσεις και τις παρατάσεις της.
2. Τα πρωτόκολλα παραλαβής των επιμέρους παραδοτέων και τις εκθέσεις προόδου του έργου.
3. Τις εκθέσεις ελέγχου κυβερνοασφάλειας, δοκιμών διείσδυσης, επιχειρησιακής συνέχειας και ανάκτησης από καταστροφή που είχαν συνταχθεί πριν από την επίθεση, σε κατάλληλα διαβαθμισμένη ή απομειωμένη από ευαίσθητες τεχνικές πληροφορίες μορφή.
4. Τις προβλεπόμενες από το άρθρο 16 του ν. 5160/2024 αναφορές προς τις αρμόδιες αρχές, σε μορφή από την οποία θα έχουν αφαιρεθεί τεχνικές ή άλλες πληροφορίες που ενδέχεται να θέσουν σε κίνδυνο την ασφάλεια των συστημάτων ή την εξέλιξη της έρευνας.
5. Την έκθεση αποτίμησης των δεδομένων και υπηρεσιών που επηρεάστηκαν, εφόσον έχει συνταχθεί, καθώς και το σχέδιο αποκατάστασης και ασφαλούς επαναλειτουργίας των πληροφοριακών συστημάτων.
6. Τυχόν απόφαση, εισήγηση ή άλλο υπηρεσιακό έγγραφο σχετικά με τη δημόσια γνωστοποίηση ή την προσωρινή μη γνωστοποίηση του περιστατικού.
7. Κάθε σύμβαση, συμφωνία συντήρησης ή άλλη πράξη που ίσχυε κατά τον χρόνο εκδήλωσης του περιστατικού και αφορούσε τη λειτουργία, τεχνική υποστήριξη, κυβερνοασφάλεια, δημιουργία και τήρηση αντιγράφων ασφαλείας ή αποκατάσταση του πληροφοριακού συστήματος του ΝΣΚ, καθώς και τα αντίστοιχα πρωτόκολλα παραλαβής, με εξαίρεση τις πληροφορίες των οποίων η δημοσιοποίηση θα μπορούσε να δημιουργήσει κίνδυνο ασφαλείας.
8. Εφόσον έχει ήδη διενεργηθεί οριζόντιος έλεγχος σε φορείς του Δημοσίου μετά το συγκεκριμένο περιστατικό, τα συγκεντρωτικά αποτελέσματά του ως προς την ύπαρξη και δοκιμή αντιγράφων ασφαλείας, σχεδίων επιχειρησιακής συνέχειας και σχεδίων ανάκτησης από καταστροφή, χωρίς στοιχεία που θα μπορούσαν να αποκαλύψουν συγκεκριμένες τεχνικές ευπάθειες φορέων ή πληροφοριακών συστημάτων.

Οι ερωτώντες Βουλευτές

Κουκουλόπουλος Παρασκευάς (Πάρις)

Πάνας Απόστολος

Μουλκιώτης Γεώργιος