Αθήνα, 17/12/2024
Α. Π.: 42062 ΕΞ 2024
Απάντηση στο έγγραφο: 37646 ΕΞ 2024

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΕΘΝΙΚΗ ΑΡΧΗ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ
ΓΕΝΙΚΗ ΔΙΕΥΘΥΝΣΗ ΕΠΙΤΕΛΙΚΟΥ ΣΧΕΔΙΑΣΜΟΥ
ΓΕΝΙΚΗ ΔΙΕΥΘΥΝΣΗ ΕΠΙΧΕΙΡΗΣΙΑΚΟΥ ΣΧΕΔΙΑΣΜΟΥ
Δ/νση: Χανδρή 1 & Θεσσαλονίκης
Τ.Κ.: 18346, Μοσχάτο Αττικής
Πληροφορίες: Ι. Βοζώρης
Τηλ.: 210 4802040
E-mail: i.vozoris@mindigital.gr

Προς: 1. Υπηρεσία Συντονισμού
2.Γραφείο Νομικών και Κοινοβουλευτικών Θεμάτων

Κοιν: Γραφείο Υπουργού

Θέμα: Απάντηση σε Ερώτηση στο πλαίσιο κοινοβουλευτικού ελέγχου

Σχετ.: **α.** Το υπ' αρ. πρωτ. 37646 ΕΞ 2024/11.11.2024 έγγραφο της Υπηρεσίας Συντονισμού

β. Η υπ' αρ. πρωτ. 1109/08.11.2024 Ερώτηση τεσσάρων βουλευτών της Κοινοβουλευτικής Ομάδας της Νέας Αριστεράς με θέμα: «Αναγκαία ενημέρωση των φοιτητών και λήψη μέτρων προστασίας τους από την κυβερνοεπίθεση στο Ελληνικό Ανοικτό Πανεπιστήμιο»

Σε απάντηση του α' σχετικού, με το οποίο διαβιβάστηκε στην Υπηρεσία μας το ως άνω β' σχετικό, και στο πλαίσιο των αρμοδιοτήτων μας, σας ενημερώνουμε για τα εξής:

Η Εθνική Αρχή Κυβερνοασφάλειας (ν.5086/2024, Α΄23) είναι αρμόδια για την οργάνωση, τον συντονισμό, την εφαρμογή και τον έλεγχο ενός ολοκληρωμένου πλαισίου (στρατηγικών, μέτρων και δράσεων) για την επίτευξη υψηλού επιπέδου κυβερνοασφάλειας στη χώρα, στα πεδία της πρόληψης, της προστασίας, της αποτροπής, του εντοπισμού, της αντιμετώπισης, της αποκατάστασης και της ανάκαμψης από κυβερνοεπιθέσεις. Ορίζεται δε, ως αρμόδια για τη χάραξη της ενιαίας πολιτικής κυβερνοασφάλειας στο πλαίσιο της ελληνικής και ενωσιακής νομοθεσίας για την κυβερνοασφάλεια και τις κρίσιμες υποδομές του δημόσιου και ιδιωτικού τομέα, όπως αυτές εκάστοτε ορίζονται νομοθετικά. Η Αρχή αναβαθμίστηκε με τον ανωτέρω νόμο, ώστε να ενισχυθεί ο ρόλος και οι αρμοδιότητες της στο σύνολο των βασικών πυλώνων της δημόσιας πολιτικής κυβερνοασφάλειας, ήτοι:

- Διακυβέρνηση και στρατηγικός σχεδιασμός κυβερνοασφάλειας
- Νομοθετικός και ρυθμιστικός πυλώνας, καθώς και κανονιστική συμμόρφωση, μέσω ελεγκτικών μηχανισμών, προκειμένου να διασφαλίζεται η κανονιστική συμμόρφωση των οντοτήτων κρίσιμων υποδομών

- Επιχειρησιακός σχεδιασμός για την αντιμετώπιση περιστατικών μεγάλης κλίμακας και κρίσεων στον κυβερνοχώρο

- Τεχνικές λειτουργίες και δυνατότητες, με στόχο τον εντοπισμό και την παρακολούθηση απειλών και την αντιμετώπιση περιστατικών κυβερνοασφάλειας (μεταξύ των οποίων συγκαταλέγονται λειτουργίες CSIRT, SOC, cybersecurity lab).

Επιπλέον η Εθνική Αρχή Κυβερνοασφάλειας βρίσκεται σε συνεργασία με τις συναρμόδιες για την κυβερνοασφάλεια αρχές σε εθνικό, ενωσιακό και διεθνές επίπεδο για την επίτευξη των εθνικών στόχων για τη διασφάλιση υψηλού επιπέδου ασφαλείας, καθώς και για την προάσπιση των ατομικών δικαιωμάτων στον κυβερνοχώρο. Περαιτέρω, η Αρχή συνεργάζεται με το σύνολο των συναρμόδιων φορέων, και ιδίως τις υπηρεσίες του Υπουργείου Εθνικής Άμυνας, του Υπουργείου Προστασίας του Πολίτη και την Εθνική Υπηρεσία Πληροφοριών (Ε.Υ.Π.), στο πλαίσιο της αποστολής και των αρμοδιοτήτων τους.

Η Εθνική Αρχή Κυβερνοασφάλειας, αν και καταρχήν δεν είχε τυπικώς αρμοδιότητα, ωστόσο κατόπιν σχετικού αιτήματος από το ΕΑΠ, το οποίο προέβη σε εθελούσια κοινοποίηση του περιστατικού σύμφωνα με τις διατάξεις του α. 14 του ν. 4577/2018 (Α’ 199) ανέλαβε να συνδράμει στη διαχείριση του περιστατικού, συνδυάζοντας άμεση επιχειρησιακή ανταπόκριση, τεχνική ανάλυση, και ενίσχυση των προληπτικών μέτρων ασφάλειας.

Σε συνέχεια της ενημέρωσης που έλαβε η Εθνική Αρχή Κυβερνοασφάλειας από το ΕΑΠ σχετικά με το εν εξελίξει περιστατικό, η Ομάδας Απόκρισης Συμβάντων στον Κυβερνοχώρο (CSIRT) της ΕΑΚ κινητοποιήθηκε άμεσα (περ. ιβ’ της παρ. 2 του άρθρου 4 ν. 5086/2024).

Συγκεκριμένα, οι ενέργειες στις οποίες προέβη η CSIRT της ΕΑΚ για τη διαχείριση του περιστατικού είναι οι εξής:

- Επιτόπια Παρέμβαση: Η Ομάδα Απόκρισης Συμβάντων στον Κυβερνοχώρο (CSIRT) της ΕΑΚ μετέβη στην έδρα του ΕΑΠ στην Πάτρα, την επόμενη κιόλας ημέρα από την κοινοποίηση του περιστατικού, για επιτόπια έρευνα και συλλογή στοιχείων.
- Συγκρότηση Ομάδας Διαχείρισης: Συστάθηκε Ομάδα Διαχείρισης Περιστατικού, αποτελούμενη από προσωπικό του ΕΑΠ, την CSIRT της ΕΑΚ, και την ομάδα αντιμετώπισης περιστατικών κυβερνοασφάλειας (Incident Response Team) εξωτερικού συνεργάτη του ΕΑΠ.
- Κατευθύνσεις και Αναφορές: Δόθηκαν οδηγίες στις Πρυτανικές Αρχές για τις υποχρεώσεις αναφοράς του περιστατικού στην ΑΠΔΠΧ, κατά τα οριζόμενα στον ΓΚΠΔ, καθώς και τη Δίωξη Ηλεκτρονικού Εγκλήματος της ΕΛ.ΑΣ..
- Συμβουλές και Σχέδιο Αποκατάστασης: Προτάθηκαν μέτρα και πολιτικές απόκρισης, ενώ παραδόθηκε σχετικό report από την Incident Response Team με συγκεκριμένες ενέργειες. Η CSIRT της ΕΑΚ παρείχε οδηγίες για την κατάρτιση πλάνου αποκατάστασης.
- Μελλοντική Πρόληψη: Προτάθηκαν μέτρα για την αποφυγή παρόμοιων περιστατικών.
- Συνεχής Συντονισμός: Πραγματοποιήθηκε τηλεδιάσκεψη για περαιτέρω συντονισμό, ενώ συνεχίστηκε η συνεργασία με την Ομάδα Διαχείρισης και τους εξωτερικούς συνεργάτες του ΕΑΠ.
- Επικοινωνιακή Διαχείριση: Σε συνεργασία με την ΕΑΚ, οργανώθηκε η ενημέρωση του κοινού για το περιστατικό.

- Συνεχής Υποστήριξη: Η ΕΑΚ διατηρεί στενή επικοινωνία με το ΕΑΠ προκειμένου να παραμένει ενήμερη και να παρέχει καθοδήγηση και υποστήριξη, εφόσον απαιτείται, για την αντιμετώπιση των επιπτώσεων του συγκεκριμένου περιστατικού.

Συνοψίζοντας, σε συνεργασία με το ΕΑΠ, η ΕΑΚ έδρασε άμεσα για τη διαχείριση του περιστατικού, παρέχοντας τεχνική υποστήριξη, επιχειρησιακές οδηγίες και κατευθύνσεις για την αποκατάσταση και την πρόληψη μελλοντικών επιθέσεων στον κυβερνοχώρο. Παράλληλα, ενημερώθηκαν οι αρμόδιες αρχές και εφαρμόστηκαν μέτρα για τη διαφύλαξη της ασφάλειας των δεδομένων. Η ΕΑΚ παραμένει σε συνεχή επικοινωνία με το ΕΑΠ, διασφαλίζοντας τη λήψη όλων των απαραίτητων ενεργειών για την αποτροπή εκδήλωσης παρόμοιων περιστατικών στο μέλλον.

Το συγκεκριμένο περιστατικό υπογραμμίζει τη σημασία της συνεχούς αναβάθμισης της κυβερνοασφάλειας στα ελληνικά πανεπιστήμια, που ως φορείς δεν ανήκουν μεν στις οντότητες που υπάγονται υποχρεωτικά στο πεδίο εφαρμογής της Οδηγίας (ΕΕ) 2022/2555 (Οδηγία NIS2), εντούτοις ο ρόλος τους είναι πολλαπλώς σημαντικός σε εθνικό επίπεδο και, άλλωστε, διαχειρίζονται πληθώρα δεδομένων προσωπικού χαρακτήρα. Συνεπώς, οφείλουν να συμμορφώνονται με τις σχετικές υποχρεώσεις που απορρέουν από την εθνική και ευρωπαϊκή νομοθεσία που διέπει τη λειτουργία τους. Στο πλαίσιο αυτό, είναι σημαντική η τήρηση και ενίσχυση των εφαρμοζόμενων πολιτικών ασφάλειας και η υιοθέτηση κατάλληλων οργανωτικών και τεχνικών μέτρων κυβερνοασφάλειας για την αποτροπή μελλοντικών επιθέσεων στα πληροφοριακά τους συστήματα, εξασφαλίζοντας την επιχειρησιακή τους συνέχεια και την προστασία των προσωπικών δεδομένων που διαχειρίζονται.

Θέτουμε υπόψη σας τα παραπάνω και παραμένουμε στη διάθεσή σας για κάθε σχετικό θέμα.

Ο Διοικητής

Μιχαήλ Μπλέτσας

Εσωτερική διανομή:

1. Γραφείο Διοικητή Εθνικής Αρχής Κυβερνοασφάλειας
2. Γραφείο Υποδιοικήτριας Εθνικής Αρχής Κυβερνοασφάλειας
3. Γενική Διεύθυνση Επιτελικού Σχεδιασμού
4. Γενική Διεύθυνση Επιχειρησιακού Σχεδιασμού