



**ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΥΠΟΥΡΓΕΙΟ ΕΡΓΑΣΙΑΣ ΚΑΙ
ΚΟΙΝΩΝΙΚΩΝ ΥΠΟΘΕΣΕΩΝ
ΥΠΗΡΕΣΙΑ ΣΥΝΤΟΝΙΣΜΟΥ
ΓΡΑΦΕΙΟ ΝΟΜΙΚΩΝ ΚΑΙ
ΚΟΙΝΟΒΟΥΛΕΥΤΙΚΩΝ ΘΕΜΑΤΩΝ**

Ταχ. Δ/νση: Σταδίου 29
Ταχ. Κώδικας: 101 10 - Αθήνα
Πληροφορίες: Π.Παναγιωτακοπούλου
Τηλέφωνο: 2131516475
e-mail: ypertns@ypakp.gr

Αθήνα
Αριθ. Εσωτ. Πρωτ.: 1022Ε

ΠΡΟΣ: Τη Βουλή των Ελλήνων
Δ/νση Κοιν/κού Ελέγχου
Τμήμα Ερωτήσεων
Αθήνα

ΚΟΙΝ. : Πολιτική Γραμματεία Υφυπουργού
Κοινωνικής Ασφάλισης

ΘΕΜΑ: «Σοβαρά κενά ασφαλείας στα πληροφοριακά συστήματα e-ΕΦΚΑ και του Υπουργείου Ψηφιακής Διακυβέρνησης τα καθιστούν ευάλωτα σε κυβερνοεπιθέσεις».

ΣΧΕΤ.: Η με αρ. πρωτ. 6464/11-5-2021 Ερώτηση που διαβιβάστηκε από το Υπουργείο Ψηφιακής Διακυβέρνησης.

Σε απάντηση της σχετικής Ερώτησης που κατατέθηκε στη Βουλή από τους Βουλευτές κ. κ. Κάτση Μάριο και Γκαρά Αναστασία (Νατάσα), αναφορικά με το παραπάνω θέμα και σύμφωνα με όσα μας γνωστοποίησε η Διοίκηση του e- ΕΦΚΑ, σας πληροφορούμε τα εξής:

Όσον αφορά στο δημοσίευμα το οποίο αναρτήθηκε στο διαδικτυακό τόπο iguru.gr σχετικά με πιθανό κενό ασφαλείας στην ιστοσελίδα του e-ΕΦΚΑ στις 06.04.2021 ενημερώθηκαν άμεσα και συγκεκριμένα την ίδια ημέρα οι εμπλεκόμενες μονάδες καθώς και ο ανάδοχος υποστήριξης παραγωγικής λειτουργίας της ιστοσελίδας του e-ΕΦΚΑ. Στις 07.04.2021 η Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων - ΕΘΝΙΚΟ CERT ενημέρωσε σχετικά και τη Δ/νση Ηλεκτρονικής Διακυβέρνησης και Εξυπηρέτησης του Πολίτη του Υπουργείου μας.

Στο πλαίσιο της διερεύνησης της εγκυρότητας του δημοσιεύματος εντατικοποιήθηκε η συνεργασία και επικοινωνία των εμπλεκόμενων μερών. Πιο συγκεκριμένα πραγματοποιήθηκαν οι ακόλουθες άμεσες ενέργειες:

- Ενημερώθηκε σχετικά η Διοίκηση του e-ΕΦΚΑ και ο Υπεύθυνος Προστασίας Δεδομένων.
- Αναζητήθηκε ανεπιτυχώς πρότερη ενημέρωση για το κενό ασφαλείας, η οποία αναφέρεται στο δημοσίευμα. Επισημαίνεται ότι οι υπηρεσίες του e-ΕΦΚΑ ανταποκρίνονται πάντα και άμεσα σε οποιαδήποτε υπόνοια περιστατικού ή κενού ασφαλείας το οποίο εντοπίζεται.
- Πραγματοποιήθηκε τηλεδιάσκεψη όλων των εμπλεκόμενων υπηρεσιών του φορέα και της αναδόχου εταιρείας υποστήριξης παραγωγικής λειτουργίας των πληροφοριακών συστημάτων του e-ΕΦΚΑ στις 07.04.2021.
- Συλλέχθηκαν και αναλύθηκαν τα διαθέσιμα αρχεία καταγραφής από διάφορες πηγές. Επισημαίνεται ότι ο συνολικός όγκος των αρχείων καταγραφής που αφορά στο συγκεκριμένο περιστατικό υπερβαίνει τα 20GB.
- Εξακριβώθηκε προσπάθεια κυβερνοεπίθεσης στην προς κατάργηση ηλεκτρονική υπηρεσία "Επιβεβαίωση εγκυρότητας βεβαιώσεων ασφαλιστικής ενημερότητας πριν την 10/01/2012» και όχι στον επίσημο ιστότοπο του e-ΕΦΚΑ. Διευκρινίζεται ότι η εν λόγω

υπηρεσία λειτουργούσε στις παλιές υποδομές του τ.ΙΚΑ-ΕΤΑΜ, οι οποίες ήταν σε διαδικασία μετάπτωσης. Από 09/04/2021 όλες οι εναπομείναντες ηλεκτρονικές υπηρεσίες, οι οποίες λειτουργούσαν στις παλιές υποδομές του τ. ΙΚΑ-ΕΤΑΜ, έχουν μεταπέσει στις νέες υποδομές του ιστότοπου του e-ΕΦΚΑ αφού ελήφθησαν πρόσθετα μέτρα ασφάλειας.

- Πραγματοποιήθηκε αποκλεισμός της πρόσβασης της συγκεκριμένης υπηρεσίας από το διαδίκτυο, σύμφωνα με τις οδηγίες και την έγκριση της Διοίκησης του Φορέα, στις 07.04.2021.
- Δημιουργήθηκαν κανόνες αποκλειστικής πρόσβασης σε συγκεκριμένη ομάδα χρηστών – διαχειριστών του e-ΕΦΚΑ προς την συγκεκριμένη υπηρεσία από το εσωτερικό δίκτυο του e-ΕΦΚΑ.

Από τη διερεύνηση του συγκεκριμένου περιστατικού:

- Εντοπίστηκαν στοιχεία για τα εργαλεία, τα σενάρια και τις ip διευθύνσεις του επιτιθέμενου.
- Εξακριβώθηκε ότι δεν υπάρχει διασύνδεση από την εν λόγω ηλεκτρονική υπηρεσία προς λοιπές Βάσεις Δεδομένων ή/και ηλεκτρονικές υπηρεσίες του e-ΕΦΚΑ.
- Προέκυψε ότι πραγματοποιήθηκε από τον επιτιθέμενο προσπάθεια εκτέλεσης πλήθους εντολών για τις οποίες δεν μπορεί να τεκμηριωθεί η επιτυχία ή/και ολοκλήρωση από τα διαθέσιμα αρχεία καταγραφής και συνεπώς δεν δύναται να τεκμηριωθεί/ στοιχειοθετηθεί διαρροή προσωπικών δεδομένων.

Διευκρινίζεται ότι η ηλεκτρονική υπηρεσία, στην οποία έγινε προσπάθεια κυβερνοεπίθεσης δε χρησιμοποιούσε μηχανισμό αυθεντικοποίησης μέσω κωδικών TAXIS. Εντούτοις ο e-ΕΦΚΑ αξιοποιεί τον εν λόγω μηχανισμό στις περισσότερες ηλεκτρονικές υπηρεσίες που παρέχει για λόγους ασφάλειας, ομοιογένειας και βελτίωσης της εμπειρίας των χρηστών. Επισημαίνεται ότι ο e-ΕΦΚΑ δεν αποθηκεύει στις βάσεις δεδομένων κωδικούς taxisnet πολιτών και η χρήση του εν λόγω μηχανισμού αυθεντικοποίησης γίνεται μέσω ασφαλών πρωτοκόλλων επικοινωνίας των πληροφοριακών συστημάτων του e-ΕΦΚΑ με αυτά της Γενικής Γραμματείας Πληροφοριακών Συστημάτων Δημόσιας Διοίκησης.

Επισημαίνεται τέλος ότι ο e-ΕΦΚΑ μεριμνά για την ασφάλεια των πληροφοριακών συστημάτων και δεδομένων που διαχειρίζεται. Στο εν λόγω πλαίσιο διενεργεί τακτικούς και εξειδικευμένους ελέγχους ασφάλειας σε συνεργασία με εξειδικευμένη εταιρεία, η οποία έχει επιλεγεί με αυστηρά κριτήρια επιλογής κατόπιν διαγωνιστικής διαδικασίας.

Ο ΥΦΥΠΟΥΡΓΟΣ

Π.ΤΣΑΚΛΟΓΛΟΥ