ΕΝΩΣΗ ΠΛΗΡΟΦΟΡΙΚΩΝ ΕΛΛΑΔΑΣ

Αρ. Πρωτ: L20-0117-01V1

Προς: Κτηματολόγιο Α.Ε.

Κοιν: Υπουργείο Ψηφιακής Διακυβέρνησης
Υπουργείο Οικονομικών
Ανεξάρτητη Αρχή Δημοσίων Εσόδων
Γενική Γραμματεία Πληροφοριακών Συστημάτων
Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων
Γραφεία Τύπου πολιτικών κομμάτων
Μέσα Μαζικής Ενημέρωσης

Αθήνα, 17/1/2020

Θέμα: ΕΠΕΙΓΟΝ – Περαιτέρω διερεύνηση του περιστατικού πιθανής παραβίασης ασφάλειας (Κτηματολόγιο)

Αξιότιμοι κυρίες/κύριοι,

Αργά εχθές (16/1) ενημερωθήκαμε μέσω τρίτων, χωρίς όμως να έχουμε λάβει ακόμη επίσημη απάντηση από τον αρμόδιο φορέα, ότι η "Κτηματολόγιο Α.Ε." εξέδωσε (16/1) ανακοίνωση-απάντηση[1] στη δική μας επιστολή[2] της 15/1/2020. Στην απάντηση αναφέρεται:

Απάντηση του Ελληνικού Κτηματολογίου στην επιστολή της Ένωσης Πληροφορικών Ελλάδας

Με αφορμή επισημάνσεις της Ένωσης Πληροφορικών Ελλάδας περί «πιθανής προσπάθειας υποκλοπής προσωπικών δεδομένων», το Ελληνικό Κτηματολόγιο επιθυμεί να καταστήσει απολύτως σαφές προς τους πολίτες πώς καμία προσπάθεια υποκλοπής προσωπικών στοιχείων δεν υφίσταται.

Το μήνυμα που απεστάλη στους πολίτες, προέρχεται από την ανάδοχο ιδιωτική εταιρεία, υπεύθυνη για την διαδικασία Κτηματογράφησης στο Δήμο Αθηναίων.

Ζητήματα ασφαλείας και προστασίας των προσωπικών δεδομένων αντιμετωπίζονται με απόλυτη προτεραιότητα και δεν συντρέχει κανένας λόγος ανησυχίας για τους πολίτες.

1 https://www.ktimatologio.gr/posts/apantisi-toy-ellinikoy-ktimatologioy-stin-epistoli-tis-enosis-pliroforikon-elladas

2 https://www.epe.org.gr/index.php?id=19&tx_ttnews%5Btt_news%5D=11837&cHash=0c582b257e1399636ff7a761ee9ee0e3

Σύμφωνα με τα παραπάνω, ο επίσημος φορέας επιβεβαιώνει πως οι αναφερόμενοι στην προηγούμενη επιστολή μας ιστότοποι είναι διοικητικά και λειτουργικά ενταγμένοι στις ηλεκτρονικές υπηρεσίες προς τους πολίτες, υπό την επίβλεψη ιδιωτικού φορέα με σχέση αναδοχής έργου.

Δυστυχώς ο επίσημος φορέας δεν παρέχει καμία άλλη πληροφορία για το σοβαρότατο περιστατικό, όπως είναι η συμβατική, ηθική και νομική του υποχρέωση. Ενδεικτικά:

1. Σύμφωνα με τον **"Κανονισμό για τη Διασφάλιση του Απορρήτου των Ηλεκτρονικών Επικοινωνιών"** (ΑΔΑΕ, Αριθμ. αποφ. 165/2011, ΦΕΚ 2715/Β/17-11-2011)[3] προβλέπονται συγκεκριμένες νομικές υποχρεώσεις του υπεύθυνου οργανισμού, τυχόν αναδόχου και συγκεκριμένων προσώπων, σχετικά με την ύπαρξη και πιστή εφαρμογή Πολιτικής Ασφάλειας Δικτύου, καθώς και υποχρέωση καταγραφής και αμελλητί ενημέρωσης της ΑΔΑΕ σε περίπτωση οποιουδήποτε περιστατικού παραβίασης ή πιθανής παραβίασης ασφάλειας.
2. Σύμφωνα με τον **"Κανονισμό για την Ασφάλεια και την Ακεραιότητα Δικτύων και Υπηρεσιών Ηλεκτρονικών Επικοινωνιών"** (ΑΔΑΕ, Αριθμ. αποφ. 205/2013, ΦΕΚ 1742/Β/15-7-2013)[4] προβλέπονται συγκεκριμένες νομικές υποχρεώσεις του υπεύθυνου οργανισμού, τυχόν αναδόχου και συγκεκριμένων προσώπων, σχετικά με την αξιολόγηση παραγόντων κινδύνου, των μηχανισμών προστασίας της ασφάλειας, των επιπτώσεων σε περίπτωση παραβίασής τους, καθώς και τη διαδικασία διαχείρισης τέτοιων περιστατικών (άρθρο 17).

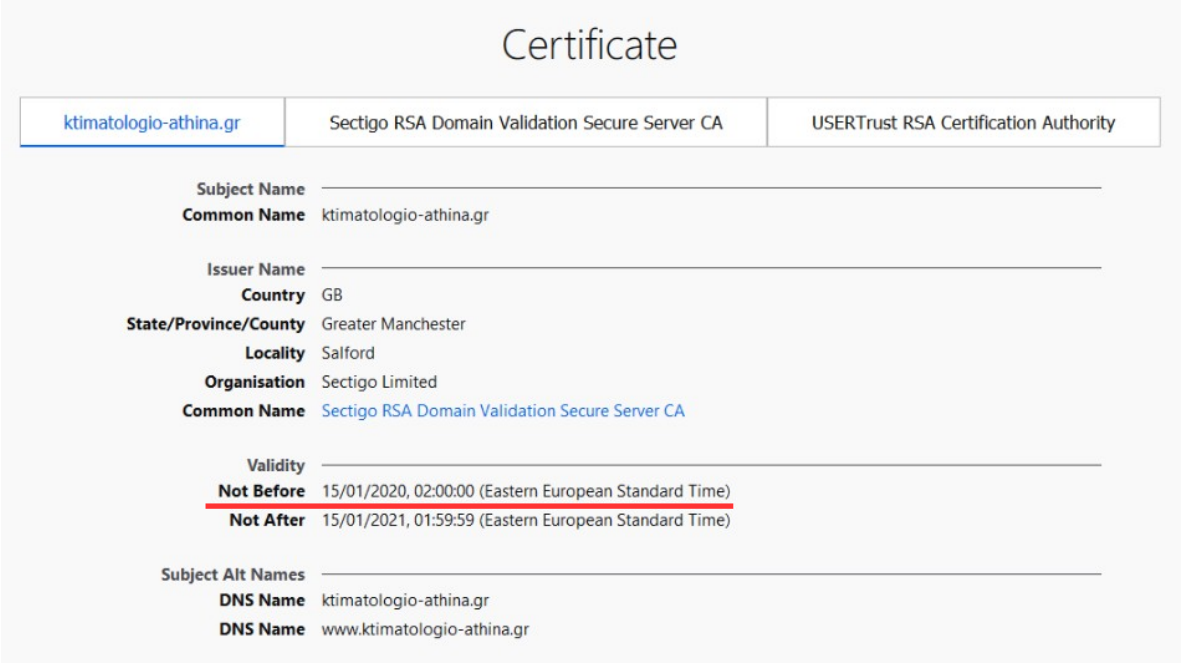
Ειδικότερα σε σχέση με την ενημέρωση σε περιπτώσεις περιστατικών παραβίασης ασφάλειας, στο (1) παραπάνω αναφέρεται χαρακτηριστικά:

> (άρθρο 9) *"ζ. Ενημέρωση για την ενδεχόμενη εμφάνιση του περιστατικού περισσότερες φορές / η. Χρόνος επίλυσης του προβλήματος / θ. Διορθωτικά μέτρα και σχετικό χρονοδιάγραμμα / ι. Ενημέρωση θιγόμενων συνδρομητών ή άλλων ατόμων που επηρεάστηκαν από το περιστατικό και γνωστοποίηση στις αρμόδιες αρχές σύμφωνα με την κείμενη νομοθεσία / ια. Ενδεχόμενες συστάσεις σε θιγόμενους συνδρομητές ή άλλα άτομα που επηρεάστηκαν από το περιστατικό, με σκοπό τον μετριασμό των αρνητικών επιπτώσεων του..."*

Σχετικά με το συγκεκριμένο περιστατικό, το οποίο περιγράφεται λεπτομερώς στην προηγούμενή μας επιστολή, συμπληρώνονται τα εξής:

3 http://www.adae.gr/fileadmin/docs/KANONISMOS_165.2011.pdf
4 http://www.adae.gr/fileadmin/docs/nomoi/kanonismoi/Kanonismos_FEK_1742_B_15_07_2013_asfaleia_akeraiotita__ADAE_205_2013.pdf

- Στον ιστότοπο “ktimatologio-athina.gr” έχει πλέον αφαιρεθεί η επιλογή πρόσβασης στη σελίδα με τη (μη ασφαλή) φόρμα τροποποίησης των προσωπικών στοιχείων χρήστη.
- Στον ίδιο ιστότοπο έχει πλέον εγκατασταθεί πιστοποιητικό ασφάλειας σύμφωνα με τα προβλεπόμενα. Το πιστοποιητικό αυτό έχει χρονοσφραγίδα δημιουργίας-ενεργοποίησης: 15/01/2020, 02:00:00 (EET), δηλαδή 15/1 στις 2πμ ώρα Ελλάδας, λίγες ώρες μετά τις πρώτες αναφορές για το εν λόγω περιστατικό στα κοινωνικά μέσα δικτύωσης και σε σύγκριση με τα δημόσια διαθέσιμα στοιχεία που συλλέξαμε στο ενδιάμεσο χρονικό διάστημα, μέχρι την κοινοποίηση της επιστολής μας το αμέσως επόμενο μεσημέρι (15/1, 3μμ).



Με βάση τα παραπάνω, καθώς τα ερωτήματα 1-3 της προηγούμενης επιστολής μας επιβεβαιώνονται πλήρως, ερωτάται και πάλι ο νόμιμος φορέας “Κτηματολόγιο Α.Ε.” για τα πιο σημαντικά και αδιευκρίνιστα ζητήματα, παρά τη σημερινή επίσημη ανακοίνωση:

1. Για ποιο λόγο δεν υπήρχαν μέχρι την 15/1/2020 2πμ στοιχεία ταυτοποίησης και πιστοποίησης του ιδιοκτήτη, δηλαδή του νόμιμου φορέα σε αυτά;
2. Για ποιο λόγο και για πόσο χρόνο στις συνδέσεις δεν παρέχονταν μέχρι την 15/1/2020 2πμ οι προβλεπόμενες από το νόμο προδιαγραφές ασφάλειας για την προστασία των επισκεπτών και ειδικότερα στην εισαγωγή-υποβολή προσωπικών και φορολογικών τους δεδομένων;

3. Επιβεβαιώνετε ότι το πιστοποιητικό ασφάλειας εγκαταστάθηκε και ενεργοποιήθηκε μετά την 15/1/2020 2πμ, ενώ πριν δεν υπήρχε έγκυρο/ενεργό;
4. Εφόσον υπήρξε διερεύνηση του περιστατικού ασφάλειας και διαπιστώθηκε πως δεν πρόκειται για επίθεση (phishing attack), έχετε προβεί σε όλες τις ενέργειες που προβλέπονται βάσει Νόμου (βλ. παραπάνω);
5. Για ποιο λόγο δεν έχουν υλοποιηθεί μέχρι τώρα οι υποχρεώσεις του άρθρου 9 (βλ. παραπάνω) περί άμεσης ενημέρωσης των θιγόμενων συνδρομητών ή άλλων ατόμων που επηρεάστηκαν από το περιστατικό, δηλαδή όλων των πολιτών;

Τέλος, ενημερώνουμε και πάλι ότι για λόγους προστασίας του δημοσίου συμφέροντος και βάσει του Κώδικα Δεοντολογίας[5] μας όπως προβλέπεται από το Καταστατικό μας, αποτελεί συμβατική υποχρέωσή μας να ενημερώσουμε τους πολίτες άμεσα και λεπτομερώς για το περιστατικό, μέχρι την πλήρη τεκμηρίωσή του και σύμφωνα με τις επόμενες ενέργειες εκ μέρους της ΑΔΑΕ.

Με εκτίμηση,

Το ΔΣ της Ένωσης Πληροφορικών Ελλάδας (ΕΠΕ)

Ο Πρόεδρος	Ο Αντιπρόεδρος	Ο Γενικός Γραμματέας	Ο Ειδικός Γραμματέας	Η Ταμίας
Δημήτρης Κυριακός	Μάριος Παπαδόπουλος	Χάρης Γεωργίου	Φώτης Αλεξάκος	Λένα Καπετανάκη
proedros@epe.org.gr	antiproedros@epe.org.gr	gen_grammateas@epe.org.gr	eid_grammateas@epe.org.gr	tamias@epe.org.gr

Ένωση Πληροφορικών Ελλάδας, Τ.Θ. 13801, Τ.Κ. 10310, Αθήνα
Email: info@epe.org.gr – Τηλέφωνο/Fax: 6981723690

5 https://www.epe.org.gr/index.php?id=19&tx_ttnews%5Btt_news%5D=11187&cHash=c63f109e0fd30c6c7aee5971d12b3f13