ΒΟΥΛΗ ΤΩΝ ΕΛΛΗΝΩΝ

ΕΛΛΗΝΙΚΗ ΛΥΣΗ

ΑΝΑΦΟΡΑ

Αθήνα, 28/05/2021

Του: Κυριάκου Βελόπουλου, Προέδρου Κόμματος, Βουλευτή Λάρισας

ΠΡΟΣ: Τον κ. Υπουργό Ψηφιακής Διακυβέρνησης, κ. Κ. Πιερρακάκη

ΘΕΜΑ: «Καταγγελία για σοβαρό πρόβλημα ασφάλειας στην διαδικτυακή πλατφόρμα "gov.gr" από κλαδικό φορέα επαγγελματιών της Πληροφορικής»

Κύριε Υπουργέ,

Παρακαλούμε για την τοποθέτησή σας επί του επισυναπτόμενου Δελτίου Τύπου, που φιλοξενήθηκε σε ιστοσελίδα του διαδικτύου ιδιοκτησίας του κλαδικού φορέα επαγγελματιών της πληροφορικής: «Ένωση Πληροφορικών Ελλάδας», όπως μας κοινοποιήθηκε, όπου οι εκπρόσωποι του εν λόγω φορέα αναλύουν τις πτυχές σοβαρού προβλήματος, που αφορά στην ασφάλεια της πολυχρησιμοποιούμενης από τους Έλληνες πολίτες διαδικτυακής πλατφόρμας "gov.gr", απευθύνοντας έκκληση στην αρμόδια πολιτική ηγεσία για επίλυσή του.

Με δεδομένα όλα τα παραπάνω, και αφού λάβετε υπόψη το συνημμένο Δελτίο Τύπου, σας παρακαλώ να το εξετάσετε και να αποφανθείτε σχετικά.

Ο Αναφέρων Βουλευτής

Κυριάκος Βελόπουλος

Επισυνάπτεται: Αντίγραφο του ως άνω Δελτίου Τύπου

(URL) Σοβαρό πρόβλημα ασφάλειας στην πλατφόρμα gov.gr- Ένωση Πληροφορικών Ελλάδας (epe.org.gr)

Σοβαρό πρόβλημα ασφάλειας στην πλατφόρμα gov.gr

18/05/2021

Θα θέλαμε να θέσουμε υπ' όψιν σας το παρακάτω σημαντικό πρόβλημα ασφάλειας κατά την επικύρωση εγγράφου που έχει παραχθεί από τις υπηρεσίες του gov.gr (https://is.gd/oDWlC9).

Συγκεκριμένα, παρατηρήσαμε πως μπορεί κανείς να βρει με απλή αναζήτηση στο Google υπερσύνδεσμο (URL) που εμφανίζει την υπεύθυνη δήλωση πολίτη, άσχετου με αυτόν που κάνει την αναζήτηση, ο οποίος έχει δημιουργήσει την δήλωσή του μέσω της πλατφόρμας: dilosi.services.gov.gr/create/q/templates.

Στις 18/5/21 η Ένωσή μας έστειλε την παρακάτω επιστολή στο Υπουργείο Ψηφιακής Διακυβέρνησης (mindigital.gr), στην ΓΓΠΣ (gsis.gr) και την ΑΠΔΠΧ (dpa.gr). Έως σήμερα (21/5) το απόγευμα δεν υπήρξε καμια -ούτε καν ανεπίσημη- απάντηση! Με άλλα λόγια το περιγραφόμενο παρακάτω πρόβλημα της πλατφόρμας dilosi.services.gov.gr παραμένει και μάλιστα δεν φαίνεται να υπάρχει πρόβλεψη διόρθωσής του στο κοντινό μέλλον. Όπως λοιπόν αναφέρουμε και στην επιστολή, είναι υποχρέωσή μας να ενημερώσουμε τους Έλληνες πολίτες για τα παρακάτω ώστε να αποφύγουν τη διαρροή προσωπικών δεδομένων τους κατά την χρήση της εν λόγω πλατφόρμας.

Προς:	Υπουργείο Ψηφιακής Διακυβέρνησης Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα Αρχή Διασφάλισης Απορρήτου Επικοινωνιών
Κοιν:	Γραφεία Τύπου πολιτικών κομμάτων ΜΜΕ

Αθήνα, 18/05/2021

Σοβαρό πρόβλημα ασφάλειας στην πλατφόρμα gov.gr

Αξιότιμοι Κύριοι,

Θα θέλαμε να θέσουμε υπ' όψιν σας το παρακάτω σημαντικό πρόβλημα ασφάλειας κατά την επικύρωση εγγράφου που έχει παραχθεί από τις υπηρεσίες του gov.gr (https://is.gd/oDWlC9). Συγκεκριμένα, παρατηρήσαμε πως μπορεί κανείς να βρει με απλή αναζήτηση στο Google υπερσύνδεσμο (URL) που εμφανίζει την υπεύθυνη δήλωση πολίτη, άσχετου με αυτόν που κάνει την αναζήτηση, ο οποίος έχει δημιουργήσει την δήλωσή του μέσω της πλατφόρμας: https://dilosi.services.gov.gr/create/q/templates. Πρακτικά, αν οποιοσδήποτε βρει από κάποια πηγή ή εντελώς τυχαία τον κωδικό hash key που χρησιμοποιείται για την επικύρωση (validation) τέτοιων εγγράφων εδώ: https://dilosi.services.gov.gr/show/q/validate, **αποκτά αυτόματα στην κατοχή του ένα PDF έγγραφο με όλα τα στοιχεία του υπογράφοντος την υπεύθυνη δήλωση**. Και όλα αυτά είναι διαθέσιμα με ένα απλό URL, χωρίς κανένα έλεγχο πρόσβασης ή αυθεντικοποίηση (login) του χρήστη. Μπορεί μάλιστα να κατεβάσει το έγγραφο τοπικά με την ψηφιακή υπογραφή του Υπουργείου, δηλαδή έτοιμο προς οποιαδήποτε νόμιμη χρήση.

Για του λόγου το αληθές επισυνάπτουμε screenshot (Παράρτημα Α). Έχουν αποκρυφτεί τα ευαίσθητα στοιχεία, έχουμε όμως το URL στη διάθεση οποιουδήποτε για επαλήθευση, καθώς και σχετικές αναφορές παρόμοιων περιστατικών από συναδέλφους μας.

Καταλαβαίνετε φυσικά πως πρόκειται για σοβαρή καταστρατήγηση του πλαισίου της προστασίας των προσωπικών δεδομένων βάσει του GDPR, καθώς και της κείμενης νομοθεσίας σχετικά με την Πολιτική Ασφάλειας που υποχρεωτικά πρέπει να εφαρμόζει κάθε παρόμοια υπηρεσία στο διαδίκτυο. Η προστασία και μόνο με ένα hash key, χωρίς έλεγχο πρόσβασης, χωρίς αυθεντικοποίηση (login) του χρήστη και χωρίς διαδικασία ρητής άδειας μεταβίβασης μεταξύ κατόχου-παραλήπτη, βρίσκεται σαφέστατα εκτός των ελάχιστων υποχρεωτικών προδιαγραφών, όπως ορίζονται σαφέστατα από τη σχετική νομοθεσία.

Το παραπάνω σοβαρότατο κενό ασφάλειας είναι κάτι που από τεχνικής πλευράς θα μπορούσε να διορθωθεί εύκολα και κυρίως πολύ γρήγορα. Εντελώς ενδεικτικά, θα μπορούσε η επικύρωση να γίνεται **μόνο μέσα σε session** με απαίτηση login από συγκεκριμένο εξουσιοδοτημένο πρόσωπο, το οποίο θα ήταν και ο μόνος που θα είχε το hash key. Θα μπορούσε επίσης να απαιτείται κάποιο επιπλέον συνθηματικό (γενικότερα security token) που θα γνώριζε μόνο ο πολίτης που έχει δημιουργήσει το έγγραφο.
Ακόμα σωστότερο και αποτελεσματικό θα ήταν στην πλατφόρμα να υπάρχει οργανωμένο προσωπικό αρχείο με ψηφιακά έγγραφα το πολίτη στα οποία θα μπορεί να δίνει επιλεκτικά πρόσβαση σε συγκεκριμένα τρίτα πρόσωπα ή φορείς μετά από σχετική (αυτόματη) αίτησή τους στην πλατφόρμα, έτσι ώστε να διατηρείται η αρχή της διμερούς και μόνο ανταλλαγής εγγράφων, όπως άλλωστε γίνεται και με αντίστοιχα φυσικά έγγραφα που βεβαίως δεν αναρτώνται πουθενά δημόσια για χρήση από οποιονδήποτε το επιθυμεί ή απλά γνωρίζει την ύπαρξή τους.

Σε κάθε περίπτωση, το ζήτημα είναι πολύ κρίσιμο και **πρέπει να επιλυθεί άμεσα**. Η Ένωσή μας παραμένει στη διάθεσή σας για οποιαδήποτε επιστημονική βοήθεια ή άλλου είδους συνδρομή. Τέλος, οφείλουμε να ενημερώσουμε πως βάσει του πλαισίου GDPR (άρθρο 33), καθώς και του Κώδικα Δεοντολογίας των Πληροφορικών (https://tinyurl.com/cf4rzvxb) σχετικά με το Δημόσιο Συμφέρον και την Υποχρέωση Γνωστοποίησης, είμαστε υποχρεωμένοι να δημοσιοποιήσουμε το εν λόγω κενό ασφαλείας σε 72 ώρες από τη στιγμή αποστολής της παρούσας επιστολής προς εσάς.

Με εκτίμηση,

Το ΔΣ της Ένωσης Πληροφορικών Ελλάδας (ΕΠΕ)

Η Πρόεδρος	**Ο Αντιπρόεδρος**	**Ο Γεν. Γραμματέας**	**Ο Ειδ. Γραμματέας**
Χαρά Ξανθάκη	**Χρ. Σταυρουλάκης**	**Χάρης Γεωργίου**	**Φώτης Αλεξάκος**
proedros@epe.org.gr	antiproedros@epe.org.gr	gen_grammateas@epe.org.gr	eid_grammateas@epe.org.gr

Ένωση Πληροφορικών Ελλάδας, Τ.Θ. 13801, Τ.Κ. 10310, Αθήνα
E-mail: info@epe.org.gr – Τηλέφωνο: 210 5699408