ΕΝΩΣΗ ΠΛΗΡΟΦΟΡΙΚΩΝ ΕΛΛΑΔΑΣ

Αρ. Πρωτ: L21-0524-01V1

Προς: "Εφημερίδα των Συντακτών" / efsyn.gr

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

Αθήνα, 24/05/2021

ΔΕΛΤΙΟ ΤΥΠΟΥ

«Διευκρινίσεις ως προς τη δημοσιοποίηση επιστολής σχετικά με σοβαρό πρόβλημα ασφάλειας στην πλατφόρμα gov.gr»

Αξιότιμοι Κύριοι,

Ευχαριστούμε για την ενημέρωση. Μέχρι και αυτή τη στιγμή δεν έχουμε λάβει καμία απολύτως απάντηση από κανέναν φορέα στους οποίους κοινοποιήθηκε η αρχική επιστολή μας στις 18/5.

Σε ό,τι αφορά το δημοσίευμα της εφημερίδας σας και τα ερωτήματα που μας θέτετε ως προς την απάντηση του υπουργείου προς εσάς, μπορούμε να σχολιάσουμε επιπρόσθετα τα εξής:

1. Από την απάντηση του υπουργείου προκύπτει πως επιβεβαιώνονται οι επισημάνσεις της ΕΠΕ ως προς τη φύση και τη σοβαρότητα του προβλήματος ασφαλείας. Πράγματι, πέρα από τον κωδικό εγγράφου (hash key), δεν υφίσταται κανένας άλλος μηχανισμός προστασίας και ελέγχου της πρόσβασης στα ηλεκτρονικά έγγραφα που εκδίδονται από την πλατφόρμα gov.gr
2. Τα νούμερα που αναφέρονται στην ανακοίνωση ως προς τις δυνατότητες επίθεσης (brute force attacks) είναι λάθος. Εφόσον πρόκειται για μόνιμα αναγνωριστικά εγγράφων, για ως και 10 εκατομμύρια πολίτες, καθένας από τους οποίους εκδίδει σε βάθος χρόνου τουλάχιστον 10 τέτοια έγγραφα στην πλατφόρμα, το σύνολο διερεύνησης είναι τουλάχιστον δύο τάξεις μεγέθους μικρότερο από το αναφερόμενο ως προς τον κωδικό ενός μόνο εγγράφου ενός συγκεκριμένου πολίτη, καθώς αρκεί μία και μόνο σωστή εύρεση hash key με οποιονδήποτε τρόπο (όχι απαραίτητα brute force attack) για να τεκμηριωθεί παραβίαση ασφάλειας στο σύστημα.
3. Ο μηχανισμός που χρησιμοποιείται εμπίπτει στην κατηγορία HMAC, δηλαδή "κωδικός αυθεντικοποίησης μηνύματος" (Message Autentication Code - MAC) με

χρήση κρυπτογραφικά ασφαλούς συνάρτησης "σύνοψης" (hash function) και ιδιωτικό κλειδί (keyed) του εκδότη. Ο μηχανισμός HMAC αποτελεί ένα είδος ψηφιακής υπογραφής με ιδιωτικό κλειδί, ο οποίος έχει σκοπό την πιστοποίηση γνησιότητας ενός ψηφιακού εγγράφου ή αρχείου, όχι την προστασία του περιεχομένου ή τον έλεγχο πρόσβασης. Ο μοναδικός τρόπος να χρησιμοποιηθεί ως τέτοιος είναι όταν: (α) έχει πολύ περιορισμένη χρονική ισχύ, δηλαδή χρησιμοποιείται ως OTAC (π.χ. κωδικός έγκρισης συναλλαγής σε e-banking), ή (β) όταν ο κάτοχος έχει τη δυνατότητα αλλαγής του συχνά και κατά βούληση (πρέπει να επιτρέπεται και να γνωρίζει το ιδιωτικό κλειδί). Στη συγκεκριμένη περίπτωση ο κωδικός εγγράφου είναι στατικός, δεν έχει χρονικό όριο ισχύος και ο κάτοχος του εγγράφου δεν έχει καμία δυνατότητα τροποποίησής του για λόγους ασφαλείας.

4. Η σύγκριση με άλλες διαδικασίες και πρωτόκολλα ελέγχου πρόσβασης όπως π.χ. login/password (token proof) στο ηλεκτρονικό ταχυδρομείο είναι επίσης λάθος. Πρόκειται για εντελώς διαφορετικά πράγματα, διαφορετικής σχεδίασης και διαφορετικής λειτουργικότητας. Το αντίστοιχο στην πλατφόρμα gov.gr θα ήταν τόσο ο χρήστης όσο και ο παραλήπτης του εκάστοτε ψηφιακού εγγράφου να πρέπει να έχουν ήδη συνδεθεί (login) με την πλατφόρμα gov.gr προτού τους δοθεί η δυνατότητα πρόσβασης και ελέγχου του κωδικού εγγράφου μέσα από την αντίστοιχη φόρμα, όπως ακριβώς προτείνουμε ως μέτρο διόρθωσης του προβλήματος ασφάλειας.
5. Με τη χρήση της μεθόδου http/https GET για την πρόσβαση στη φόρμα ελέγχου της πλατφόρμας gov.gr και την εμφάνιση του αποτελέσματος η σοβαρότητα του προβλήματος ασφάλειας πολλαπλασιάζεται, καθώς τα συγκεκριμένα URLs είναι ορατά και προσβάσιμα σε τουλάχιστον ένα ή περισσότερους ενδιάμεσους κόμβους (server logs, proxy, ...). Αυτό σημαίνει ότι, ακόμα κι αν το HMAC που εφαρμόζεται είναι κρυπτογραφικά ασφαλές, το πρωτόκολλο διασύνδεσης με το χρήστη (web browser) συγκεντρώνει και εκθέτει αυτούς τους κωδικούς εγγράφων, πιστοποιημένα έγκυρους πλέον, σε κεντρικά σημεία του δικτύου, καθώς και στην εφαρμογή του χρήστη (history) αν δεν έχουν παρθεί τα απαραίτητα μέτρα ασφάλειας σε Η/Υ πολλών χρηστών, π.χ. δημόσιες υπηρεσίες.

Ως προς το νομικό πλαίσιο, η προστασία ευαίσθητων προσωπικών δεδομένων μέσω μηχανισμών HMAC και μόνο είναι σαφέστατα εκτός του νομοθετημένου πλαισίου ελάχιστων υποχρεώσεων των παρόχων υπηρεσιών όπως η πλατφόρμα gov.gr. Ενδεικτικά αναφέρουμε τα ακόλουθα:

1. ΑΔΑΕ: "Κανονισμός για τη διασφάλιση του απορρήτου των επικοινωνιών" (2011). Οποιαδήποτε παρόμοια υπηρεσία, στο δημόσιο ή στον ιδιωτικό τομέα, έχει την υποχρέωση υποβολής και εφαρμογής συγκεκριμένης Πολιτικής Ασφάλειας, η οποία περιλαμβάνει υποχρεώσεις προστασίας και ελέγχου πρόσβασης των δεδομένων και την τήρηση της οποίας πρέπει να επιβεβαιώνει η ΑΔΑΕ με τακτικούς ελέγχους.
2. Αριθμός πράξης 01/2013: "Κοινή Πράξη της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (Α.Π.Δ.Π.Χ.) και της Αρχής Διασφάλισης του Απορρήτου

των Επικοινωνιών (Α.Δ.Α.Ε.) ως προς τις υποχρεώσεις των παροχών για την προστασία και ασφάλεια των δεδομένων σύμφωνα με τις διατάξεις του άρθρου 7 του ν. 3917/2011 (...)" / ΦΕΚ 3433 Β', 31/12/2013.

3. Κανονισμός ΕΕ/2016/679: εδάφιο 39 (υποχρέωση μηχανισμών ελέγχου πρόσβασης), εδάφιο 54 (προσωπικά δεδομένα Υγείας, βλ. πιστοποιητικό εμβολιασμού), εδάφιο 59 (δικαίωμα τροποποίησης ή διαγραφής), εδάφιο 63 (δικαίωμα ενημέρωσης παραληπτών και λόγων επεξεργασίας), εδάφιο 64 (υποχρέωση ελέγχου ταυτότητας πριν την πρόσβαση).
4. Κανονισμός ΕΕ/2016/679: άρθρο 4 - ορισμός (12) «Παραβίαση δεδομένων προσωπικού χαρακτήρα»: Η παραβίαση της ασφάλειας που οδηγεί σε τυχαία ή παράνομη καταστροφή, απώλεια, μεταβολή, άνευ άδειας κοινολόγηση ή πρόσβαση δεδομένων προσωπικού χαρακτήρα που διαβιβάστηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατ' άλλο τρόπο σε επεξεργασία.
5. Οδηγία 2009/136/ΕΚ, εδάφια 51-58 περί προστασίας της ιδιωτικότητας και τω προσωπικών δεδομένων των χρηστών σε δίκτυα και υπηρεσίες επικοινωνιών.
6. Οδηγία 2002/58/ΕΚ για την προστασία της ιδιωτικής ζωής στις ηλεκτρονικές επικοινωνίες, ειδικότερα τα άρθρα 2, 3, 4(β), 5 παρ.3 (υποχρέωση ρητής συγκατάθεσης υποκειμένου για άδεια πρόσβασης).
7. Πλατφόρμα gov.gr - "Γενικοί Όροι & Πολιτικές Χρήσης", παρ. Β9: "Ο χρήστης ορίζει τον παραλήπτη το εγγράφου είτε με καταχώρηση από υφιστάμενη λίστα κλειστού αριθμού, είτε με ελεύθερη καταχώρηση. Ο προσδιορισμός του παραλήπτη του εγγράφου είναι υποχρεωτικός για την ολοκλήρωση της έκδοσής του. Ο χρήστης φέρει την αποκλειστική ευθύνη αποστολής και επιτυχούς παράδοσης του εγγράφου (σε άυλη ηλεκτρονική ή έντυπη μορφή) στον αποδέκτη, αν δεν υφίσταται αυτοματοποιημένη διαδικασία διαρθρωμένη ως υπηρεσία της πύλης προς τούτο." (Δεν εφαρμόζεται, δεν δίνεται τέτοια δυνατότητα στην πλατφόρμα για τους κωδικούς εγγράφων).
8. Πλατφόρμα gov.gr - "Πολιτική Προστασίας Προσωπικών Δεδομένων", παρ. 5: "Τήρηση Εμπιστευτικότητας": "Το Υπουργείο δεν διαθέτει ή άλλως διαβιβάζει ή δημοσιοποιεί προσωπικά στοιχεία των επισκεπτών / χρηστών τους δικτυακού τόπου σε τρίτους, χωρίς την συγκατάθεση του επισκέπτη / χρήστη (...)" (Δεν εφαρμόζεται, η πρόσβαση στη φόρμα ελέγχου των κωδικών εγγράφων στην πλατφόρμα γίνεται χωρίς ενημέρωση ή συναίνεση των υποκειμένων).

Τέλος, ως προς την απάντηση του Υπουργείου Ψηφιακής Διακυβέρνησης που αναφέρει:

1. *"Ο μοναδικός κωδικός, όπως και τα άλλα προσωπικά στοιχεία της δήλωσης, είναι γνωστά μόνο στον ιδιοκτήτη-αποστολέα της δήλωσης και στον παραλήπτη, οι οποίοι έχουν και την ευθύνη διασφάλισής τους, ακριβώς όπως συμβαίνει και στην έντυπη δήλωση. (...)"*
2. *"Η διαδικασία αυτή διασφαλίζει τα δεδομένα του πολίτη και φυσικά δεν τα εκθέτει. (...)"*
3. *"Μη ανιχνεύσιμος αριθμός 128 bits σημαίνει ότι εάν κάποιος προσπαθήσει να μαντέψει (brute force attack) τον κωδικό ενός εγγράφου (...)"*

Σύμφωνα με όσα αναλύθηκαν παραπάνω, είναι προφανές ότι οι ισχυρισμοί (1) και (2) εκ μέρους του υπουργείου δεν ευσταθούν. Στη συγκεκριμένη υπηρεσία της πλατφόρμας gov.gr δεν υφίσταται κανένας μηχανισμός απόκρυψης δεδομένων του αρχικού εγγράφου, ελέγχου πρόσβασης σε αυτό, ούτε καν ειδοποίησης του κατόχου του, όταν κάποιος χρησιμοποιεί τον κωδικό εγγράφου για να ελέγξει την εγκυρότητά του. Επιπλέον, ο κωδικός αυτός είναι μόνιμος, χωρίς χρονικό περιορισμό, χωρίς δυνατότητα τροποποίησης από τον κάτοχο, και βρίσκεται τυπωμένος πάνω στο ίδιο το έγγραφο, άρα διαθέσιμος σε όποιον το βλέπει ή το εντοπίζει μέσω τρίτου φορέα.

Το τεχνικό μέρος της απάντησης του υπουργείου αφιερώνεται στην περιγραφή της κρυπτασφάλειας των 128-bit hash keys ως προς επιθέσεις τύπου brute force, κάτι που είναι εντελώς άσχετο με την παραπάνω αναφορά, δηλαδή την εξαιρετικά προβληματική σχεδίαση και υλοποίηση ολόκληρης της διαδικασίας στην πλατφόρμα. Άλλωστε, όπως αναλύεται παραπάνω, η περίπτωση brute force attack δεν συνδέεται με τα παραπάνω. Ακόμα και 256-bit hash key να υπήρχε στην πλατφόρμα, τα σημαντικότατα προβλήματα ασφάλειας που περιγράφουμε θα εξακολουθούσαν να ισχύουν στο ακέραιο.

Με εκτίμηση,

Το ΔΣ της Ένωσης Πληροφορικών Ελλάδας (ΕΠΕ)

Η Πρόεδρος	Ο Αντιπρόεδρος	Ο Γενικός Γραμματέας	Ο Ειδικός Γραμματέας	Ο Ταμίας
Χαρά Ξανθάκη	Χρήστος Σταυρουλάκης	Χάρης Γεωργίου	Φώτης Αλεξάκος	Γιάννης Φάκας
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: 210 5699408