ΕΝΩΣΗ ΠΛΗΡΟΦΟΡΙΚΩΝ ΕΛΛΑΔΑΣ

Ένωση Πληροφορικών Ελλάδας
Τ.Θ. 13801
ΤΚ 10310, Αθήνα
http://www.epe.org.gr
e-mail: info@epe.org.gr
Τηλέφωνο/Fax: 211 7907675

ΔΕΛΤΙΟ ΤΥΠΟΥ

Προβλήματα λειτουργίας και ασφάλειας στην Εθνική Πύλη Δημόσιας Διοίκησης Ermis

Αθήνα, 14-7-2016

Με το παρόν δελτίο Τύπου η Ένωση Πληροφορικών Ελλάδας επιθυμεί να επισημάνει ορισμένα σημαντικά θέματα/προβλήματα σχετικά με την ομαλή λειτουργία της Εθνικής Πύλης Δημόσιας Διοίκησης Ermis (http://www.ermis.gov.gr).

Συγκεκριμένα, τα πιο σημαντικά προβλήματα εντοπίζονται στα εξής σημεία:

- Το πιστοποιητικό ασφαλείας του ιστοτόπου ERMIS έχει λήξει στις **07/03/2016**. Αυτό έχει ως συνέπεια όταν προσπαθεί ο πολίτης να συνδεθεί (login) στην πύλη, το πρόγραμμα πλοήγησης να του εμφανίζει μήνυμα σφάλματος και να του **απαγορεύει την πρόσβαση**.
- Ο μόνος τρόπος για να παρακάμψεις την εν λόγω απαγόρευση είναι να χρησιμοποιηθεί **παλιά** και **παρωχημένη** έκδοση προγράμματος περιήγησης (browser). Αυτό όμως είναι **εξαιρετικά επικίνδυνο** διότι ελλοχεύει σοβαρούς κινδύνους ασφάλειας όπως μόλυνση από ιούς, διαρροή προσωπικών δεδομένων, υποκλοπή στοιχείων, κ.α. Η χρήση ενημερωμένων εκδόσεων περιηγητή (browser) είναι προαπαιτούμενο για την εύρυθμη λειτουργία του διαδικτύου σήμερα και για το λόγο αυτό οι περισσότεροι υπολογιστές έχουν ρυθμιστεί να κάνουν αυτόματη ενημέρωση των περιηγητών τους στην τελευταία έκδοση. Επομένως, είναι εξαιρετικά δύσκολο για τον μέσο πολίτη ή δημόσιο υπάλληλο να συνδεθεί στην πύλη ERMIS.

- Η έκδοση των ψηφιακών πιστοποιητικών υπογραφής και κρυπτογράφησης στις ΑΔΔΥ απαιτεί συγκεκριμένο λειτουργικό σύστημα και πρόγραμμα περιήγησης από τον τελικό χρήστη. Συγκεκριμένα απαιτείται λειτουργικό σύστημα **Microsoft Windows** και περιηγητής **Microsoft Internet Explorer**. Μπορεί η πλατφόρμα MS Windows να εξακολουθεί να είναι το πιο δημοφιλές λειτουργικό σύστημα σήμερα, αλλά υπάρχουν πολλά άλλα λειτουργικά, όπως Mac OS, διανομές Linux, καθώς και τα συστήματα κινητών συσκευών Android και iOS, τα οποία αποκτούν ολοένα και μεγαλύτερο μερίδιο της αγοράς. Σε ότι δε αφορά τον περιηγητή Internet Explorer, έχει χάσει προ πολλού την πρωτοκαθεδρία στους web browsers και το ποσοστό χρήσης του δεν ξεπερνάει πλέον το 30%. Επομένως, η αναγκαστική χρήση MS Windows με Internet Explorer καθιστά απαγορευτική την έκδοση ψηφιακών πιστοποιητικών για την πλειοψηφία των πολιτών.
- Σύμφωνα με τις υποδείξεις από ορισμένα on-line εργαλεία διαγνωστικών που ελέγχουν την εγκυρότητα και ασφάλεια ιστοτόπων που χρησιμοποιούν πιστοποιητικό ασφαλείας, η σελίδα εισόδου στην πύλη (https://login.ermis.gov.gr) αντιμετωπίζει σοβαρά προβλήματα ασφαλείας, πέραν του λήξαντος πιστοποιητικού ασφαλείας, τα οποία χρήζουν **άμεσης επίλυσης** για την αποτροπή του ενδεχομένου διαρροής προσωπικών δεδομένων με επιθέσεις τύπου man-in-the-middle attack. Ενδεικτικά αναφέρουμε ορισμένα on-line διαγνωστικά εργαλεία:

  (a) https://www.ssllabs.com/ssltest/

  (b) https://www.digicert.com/help/

  (c) https://www.sslshopper.com/ssl-checker.html

Προτάσεις επίλυσης τωρινών προβλημάτων/βελτίωσης της πύλης:

1. Θα πρέπει να εκδοθεί άμεσα νέο ψηφιακό πιστοποιητικό, το οποίο επιπρόσθετα απαιτείται να υπογραφεί με αλγόριθμο τουλάχιστον **SHA256 (256 bits)**, γιατί το υπάρχον λήξαν στις 07/03 έχει υπογραφεί με **SHA1 (160 bits)**, που θεωρείται πλέον επισφαλής[1] επιλογή.
2. Απαιτείται η άμεση **παραμετροποίηση των διακομιστών ιστού** που εξυπηρετούν την πύλη για την απενεργοποίηση μη ασφαλών και παρωχημένων πρωτοκόλλων ασφαλείας κατά την σύνδεση με το πρόγραμμα περιήγησης του τελικού χρήστη.
3. Πρέπει να υπάρξει πρόβλεψη για **συνεχή υποστήριξη** των πρόσφατων εκδόσεων των δημοφιλών προγραμμάτων περιήγησης και πλήρης εναρμόνιση

1 https://blog.qualys.com/ssllabs/2014/09/09/sha1-deprecation-what-you-need-to-know

με τις εξελίξεις όσον αφορά στα **πιστοποιητικά** και **πρωτόκολλα ασφαλείας** (TLS/SSL).

4. Πρέπει να γίνει **επανασχεδιασμός** της διαδικασίας έκδοσης των ψηφιακών πιστοποιητικών υπογραφής και κρυπτογράφησης, ώστε να προβλέπει την υποστήριξη και άλλων λειτουργικών συστημάτων πέραν των Microsoft Windows, όπως Mac OS X και τουλάχιστον 3 δημοφιλείς διανομές του λειτουργικού συστήματος Linux, καθώς και των κινητών συσκευών Android και iOS.

Η ΕΠΕ είναι όπως πάντα στη διάθεση του αρμόδιου υπουργείου για οποιαδήποτε περαιτέρω διευκρίνιση και συνεργασία, με σκοπό την επίλυση των παραπάνω ζητημάτων.

Το Διοικητικό Συμβούλιο
της Ένωσης Πληροφορικών Ελλάδας

URL: http://www.epe.org.gr , mailto:info@epe.org.gr