ΒΟΥΛΗ ΤΩΝ ΕΛΛΗΝΩΝ

155
20/10/16

ΘΕΟΔΩΡΟΣ ΚΑΡΑΟΓΛΟΥ
Βουλευτής Β΄ Θεσ/νίκης – ΝΕΑ ΔΗΜΟΚΡΑΤΙΑ

Αρ. Πρωτ.:

Αθήνα, 18 Οκτωβρίου 2016

Προς Υπουργό
-Οικονομικών

ΑΝΑΦΟΡΑ

Σας υποβάλλω συνημμένα υπόμνημα της Ένωσης Πληροφορικών Ελλάδας αναφορικά με την νέα αναβολή της αναβάθμισης ασφαλείας στις διαδικτυακές υπηρεσίες του TAXIS.
Παρακαλώ για τις δικές σας ενέργειες.

-Ο-
ΒΟΥΛΕΥΤΗΣ

ΘΕΟΔΩΡΟΣ Γ. ΚΑΡΑΟΓΛΟΥ

Μητροπόλεως 1, 105 57 Αθήνα, Τηλ: 2103709321-2
Μοναστηρίου 13, 546 27 Θεσσαλονίκη, Τηλ:2310525545, Φαξ:2310525547
Κιν: 6944770782, info@karaoglou.gr

ΕΠΕ 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

Διοικητικό Συμβούλιο:
Κυριακός Δημήτρης (Πρόεδρος)
Γιάννης Κιομουρτζής (Αντιπρόεδρος)
Χάρης Γεωργίου (Γεν. Γραμμ.)
Φώτης Αλεξάκος (Ειδ. Γραμμ.)
Λένα Καπετανάκη (Ταμίας)

ΔΕΛΤΙΟ ΤΥΠΟΥ

Νέα αναβολή της αναβάθμισης ασφάλειας στις διαδικτυακές υπηρεσίες του TAXIS

Αθήνα, 9-10-2016

Με μεγάλη μας έκπληξη ενημερωθήκαμε, μετά από σχετική ανακοίνωση της Γενικής Γραμματείας Πληροφοριακών Συστημάτων (ΓΓΠΣ)[1], ότι μετατίθεται η ημερομηνία της προγραμματισμένης αναβάθμισης των υπολογιστικών συστημάτων της ΓΓΠΣ για το Δεκέμβριο. Η έκπληξή μας μεγάλωσε όταν διαβάσαμε στην ανακοίνωση της ΓΓΠΣ πως η μεταφορά της ημερομηνίας αναβάθμισης οφείλεται σε αιτήματα φορέων και ενώσεων επαγγελματιών φοροτεχνικών, με πρώτη και πιο έντονη αντίδραση πιθανότατα αυτή της Ένωσης Ελλήνων Χρηστών Internet (ΕΕΧΙ)[2].

Με την παρούσα επιστολή επιθυμούμε να γνωστοποιήσουμε στη ΓΓΠΣ, καθώς και στο αρμόδιο εποπτεύον Υπουργείο, ότι όσοι εισηγήθηκαν την αναβολή της αναβάθμισης **φαίνεται να μην έχουν στοιχειώδεις τεχνικές γνώσεις** σχετικά με θέματα ασφάλειας πληροφοριακών συστημάτων και συγκεκριμένα των σχετικών πρωτοκόλλων ασφαλούς σύνδεσης μέσω Internet.

Στα πιθανά προβλήματα της εν λόγω αναβάθμισης αναφέρονται κυρίως προβλήματα συμβατότητας με όλους σχεδόν τους περιηγητές ιστού (web browsers) και διαφόρων

1 http://www.gsis.gr/gsis/export/sites/default/gsis_site/News/documents_news/METAFORA-HMEROMHNIAS-ANAVATHMISHS.pdf

2 https://goo.gl/eWjidq

λειτουργικών συστημάτων Η/Υ. Οι αναφορές αυτές δεν έχουν καμία σχέση με την πραγματικότητα.

Συγκεκριμένα, αναφέρεται (χωρίς συγκεκριμένες εκδόσεις) ότι οι περιηγητές Firefox, Chrome, Internet Explorer, Safari, κτλ, καθώς και τα λειτουργικά συστήματα Microsoft Windows, Linux και Mac OS, δεν επιτρέπουν τη σύνδεση με τα συστήματα της ΓΓΠΣ μέσω του νέου πρωτοκόλλου TLS 1.2. Αφ' ενός το συγκεκριμένο πρωτόκολλο[3] υπάρχει εδώ και πολλά χρόνια, περιλαμβάνει πολλές βελτιώσεις και διορθώσεις σε γνωστά προβλήματα ασφάλειας προηγούμενων εκδόσεων (TLS 1.1) και υποστηρίζεται ήδη από όλους τους σύγχρονους web browsers[4], ακόμα και σε φορητές συσκευές. Αφ' ετέρου, σε Η/Υ με μη αναβαθμισμένα λειτουργικά συστήματα (π.χ. MS-Windows XP) υπάρχουν ακόμα web browsers που ενημερώνονται κανονικά και υποστηρίζονται όλα τα σύγχρονα πρωτόκολλα επικοινωνίας (π.χ. Firefox).

Πρακτικά, μια απλή και **δωρεάν** αναβάθμιση του λογισμικού περιήγησης στο διαδίκτυο αρκεί για να μπορέσει ο οποιοσδήποτε χρήστης να αξιοποιήσει το ασφαλέστερο πρωτόκολλο TLS 1.2, σε αντίθεση με όσα εσφαλμένα ισχυρίζεται η ΕΕΧΙ. Η διατήρηση παλαιότερων πρωτοκόλλων ασφαλείας με δημοσιευμένα πλέον κενά και προβλήματα αποτελεί εξαιρετικά επικίνδυνη πρακτική, ιδιαίτερα όταν συνδυάζεται με λειτουργικά συστήματα των οποίων η τεχνική υποστήριξη έχει λήξει και δεν ενημερώνονται αντίστοιχα (updates) για κενά στην ασφάλειά τους. Σε κάθε περίπτωση, η **δωρεάν** εγκατάσταση μιας εκ των τελευταίων διανομών του Linux (π.χ. Ubuntu) αναβαθμίζει αυτομάτως τόσο το λειτουργικό σύστημα, όσο και οποιουδήποτε από τους δημοφιλείς web browser που έτσι κι αλλιώς είναι διαθέσιμοι σε αυτό.

Σε οποιαδήποτε περίπτωση, η μη αναβάθμιση ούτε του λειτουργικού συστήματος, ούτε του σχετικού web browser σε Η/Υ που χρησιμοποιούνται επαγγελματικά σε φοροτεχνικά γραφεία, έχοντας εκεί αποθηκευμένα και αποστέλλοντας τα φορολογικά δεδομένα δεκάδων ή εκατοντάδων πολιτών-πελατών, ενώ είναι γνωστοί οι κίνδυνοι ασφάλειας, αποτελεί απαράδεκτη πρακτική και εκθέτει τα δεδομένα αυτά σε ξεκάθαρες ψηφιακές απειλές.

3 https://en.wikipedia.org/wiki/Transport_Layer_Security#TLS_1.2

4 https://en.wikipedia.org/wiki/Template:TLS/SSL_support_history_of_web_browsers

Σε ό,τι αφορά τη ΓΓΠΣ, η ταυτόχρονη παραδοχή και αποδοχή των συγκεκριμένων απόψεων **εκθέτει** πρωτίστως τον ίδιο το φορέα, την ηγεσία της, τους υπεύθυνους του τεχνικού τμήματος, αλλά και το ίδιο το κύρος της Πολιτείας. Η ημιμάθεια ή ακόμη και πλήρης άγνοια του αντικειμένου, ανθρώπων που δυστυχώς εκπροσωπούν και Σωματεία, καθώς και η ενδεχομένως ελλιπής στελέχωση της ΓΓΠΣ από το αναγκαίο εξειδικευμένο προσωπικό (πράγμα που ίσως εξηγεί ότι τα πρωτόκολλα ασφαλείας που ακόμα χρησιμοποιούνται είναι παρωχημένα), εκθέτουν τους πολίτες σε σοβαρούς κινδύνους. Ενδεικτικά, μπορούν να προκαλέσουν σοβαρότατα ζητήματα υποκλοπής προσωπικών δεδομένων και μάλιστα ειδικού περιεχομένου (οικονομικά, περιουσιακά, πιστοποίησης ταυτότητας).

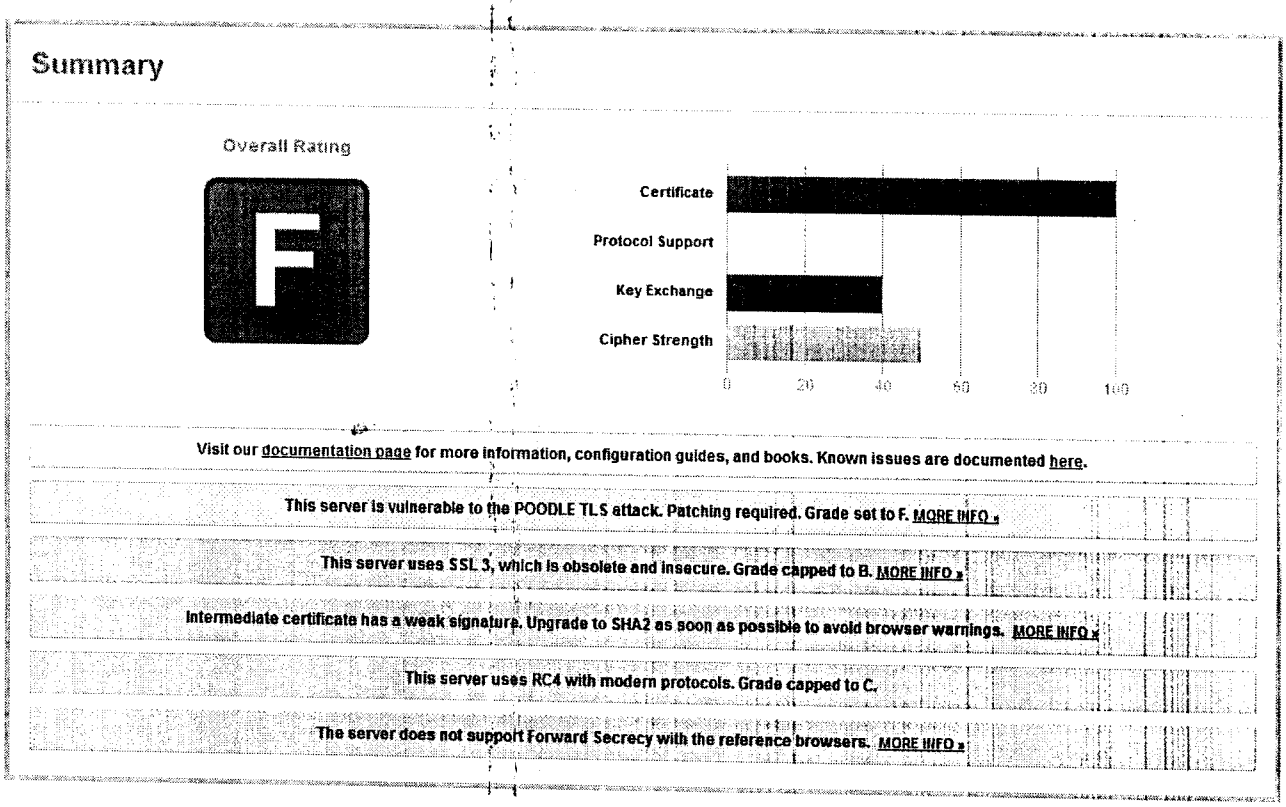
Υπενθυμίζουμε ότι μόλις το 2013 η ΓΓΠΣ καταδικάστηκε τελεσίδικα[5] από την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ) για σοβαρότατες παραλείψεις στην προστασία των προσωπικών δεδομένων των Ελλήνων φορολογουμένων και για τη μη εφαρμογή ολοκληρωμένης Πολιτικής Ασφάλειας για τον εντοπισμό, έστω, των πηγών, μεθόδων, χρόνου και υπευθύνων της πιο μαζικής διαρροής στην ιστορία του TAXIS.

Σήμερα διαπιστώνουμε με λύπη ότι η κατάσταση αυτή διαιωνίζεται, καθώς η ελληνική Πολιτεία καλεί ως εμπειρογνώμονες και εξειδικευμένους σε θέματα Πληροφορικής, ανθρώπους που δεν έχουν -ως φαίνεται- καμία σχέση με το αντικείμενο.

Προς επιβεβαίωση των παραπάνω, η Ένωση Πληροφορικών Ελλάδας (ΕΠΕ) εξέτασε την υποδομή της ΓΓΠΣ, πραγματοποιώντας συγκεκριμένες δημόσιες μετρήσεις[6], και τα αποτελέσματα απέδειξαν πολλαπλά προβλήματα ασφάλειας και τεκμηρίωσαν τις υποψίες μας. Συγκεκριμένα, από τη συνοπτική εικόνα αποτελεσμάτων (βλ. Εικόνα-1) αποδεικνύεται ξεκάθαρα ότι η ΓΓΠΣ χρησιμοποιεί πρωτόκολλα ασφαλείας, πολλά από τα οποία θεωρούνται πλέον όχι απλά ξεπερασμένα αλλά επικίνδυνα, καθώς είναι ευάλωτα σε γνωστές επιθέσεις (π.χ. POODLE TLS attack), και δε χρησιμοποιούνται από ανάλογες υπηρεσίες και υποδομές στο εξωτερικό.

5 ΑΠΔΠΧ απόφαση 98/2013: Γ/ΕΞ/5276, 9-8-2013.

6 https://www.ssllabs.com/ssltest/analyze.html?d=login.gsis.gr&hideResults=on&latest



Εικόνα-1: Συνοπτικά αποτελέσματα ελέγχου ασφάλειας (gsis.gr)

Καλούμε την Ελληνική Πολιτεία να μην εκτίθεται αποδεχόμενη εισηγήσεις όπως αυτή της ΕΕΧΙ και την προτρέπουμε να προσκαλεί επιστημονικά καταρτισμένους και εξειδικευμένους επιστήμονες Πληροφορικής, που θα ενημερώσουν σωστά και θα διευκολύνουν το έργο της με τεκμηριωμένη γνωμοδότηση.

Το Διοικητικό Συμβούλιο
της Ένωσης Πληροφορικών Ελλάδας
URL: http://www.epe.org.gr , mailto:info@epe.org.gr