ΧΡΙΣΤΙΑΝΟΔΗΜΟΚΡΑΤΙΚΟ ΚΟΜΜΑ ΕΛΛΑΔΟΣ

ΒΟΥΛΗ ΤΩΝ ΕΛΛΗΝΩΝ

ΑΝΕΞΑΡΤΗΤΟΙ ΕΛΛΗΝΕΣ

ΑΒ 1229

21-8-2015

ΑΝΑΦΟΡΑ

ΠΡΟΣ ΤΟΝ ΥΠΟΥΡΓΟ ΟΙΚΟΝΟΜΙΚΩΝ

Θέμα: «Ανάγκη διαλεύκανσης σχετικά με την υπόθεση ενδεχόμενων ψηφιακών παραβιάσεων και σχεδιασμού συστήματος παράλληλων πληρωμών με αξιοποίηση στοιχείων του συστήματος TAXIS»

Παρακαλείσθε για την τοποθέτησή σας επί της επιστολής-δελτίου τύπου που μου προώθησε η Ένωση Πληροφορικών Ελλάδας ΕΠΕ (info@epe.org.gr) σχετικά με αίτημα τους για την ανάγκη διευκρίνισης και διερεύνησης σε βάθος της υπόθεσης ενδεχόμενων ψηφιακών παραβιάσεων και σχεδιασμού συστήματος παράλληλων πληρωμών με αξιοποίηση στοιχείων του συστήματος TAXIS καθώς και της πρόθεσης της να συμβάλει με την επιστημονική κατάρτιση και την τεχνογνωσία που διαθέτει στη διαλεύκανση της.

Ο Αναφέρων Βουλευτής των Ανεξαρτήτων Ελλήνων

Νικόλαος Ι. Νικολόπουλος
Πρόεδρος Χριστιανοδημοκρατικού Κόμματος Ελλάδος

ΕΠΕ ΕΝΩΣΗ ΠΛΗΡΟΦΟΡΙΚΩΝ ΕΛΛΑΔΑΣ

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

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

ΔΕΛΤΙΟ ΤΥΠΟΥ

Ανακοίνωση σχετικά με ενδεχόμενες ψηφιακές παραβιάσεις και σχεδιασμού συστήματος παράλληλων πληρωμών με αξιοποίηση στοιχείων του συστήματος TAXIS, σύμφωνα με δηλώσεις του πρώην Υπουργού Οικονομικών

Αθήνα, 30-7-2015

Η Ένωση Πληροφορικών Ελλάδας (ΕΠΕ) παρακολουθεί, ως οφείλει, τα δημοσιεύματα και τις εξελίξεις των τελευταίων ημερών, σχετικά με την υπόθεση ενδεχόμενων ψηφιακών παραβιάσεων και σχεδιασμού συστήματος παράλληλων πληρωμών με αξιοποίηση στοιχείων του συστήματος TAXIS. Σύμφωνα με δημοσιεύματα που ξεκίνησαν την περασμένη Παρασκευή (24/7) και τα λεγόμενα του ίδιου του πρώην Υπουργού Οικονομικών κ. Γ. Βαρουφάκη όπως αποτυπώνονται σε ήδη δημοσιευμένο ηχητικό αρχείο, μια μικρή ομάδα έμπιστων συνεργατών του ανέλαβε να εκπονήσει μια μελέτη εφικτότητας για ένα εναλλακτικό σχέδιο αντιμετώπισης της περίπτωσης μη συμφωνίας με τους εταίρους-δανειστές στην πρόσφατη Σύνοδο Κορυφής. Το σχέδιο αυτό θα αναλάμβανε να ελαχιστοποιήσει τις επιπτώσεις στην Οικονομία αν, στην περίπτωση μη επίτευξης συμφωνίας στις διαπραγματεύσεις, αμέσως μετά οι ελληνικές τράπεζες βρίσκονταν εντελώς αποκλεισμένες από το ευρωπαϊκό τραπεζικό σύστημα (ΕΚΤ) και οι πολίτες πρακτικά χωρίς καμία πρόσβαση στις καταθέσεις τους σε ευρώ.

Το συγκεκριμένο θέμα έχει λάβει μεγάλες διαστάσεις, κυρίως πολιτικές αλλά πλέον και δικαστικές, αφού ήδη έχουν κινηθεί διαδικασίες διερεύνησης τυχόν ποινικών

ευθυνών των εμπλεκομένων προσώπων. Η ΕΠΕ εξακολουθεί να διατηρεί ουδέτερη στάση, όσο αφορά το πολιτικό και το ποινικό μέρος της υπόθεσης, και να εστιάζει αποκλειστικά και μόνο στα θέματα της αρμοδιότητάς της, δηλαδή σε επίπεδο καθαρά επιστημονικό και τεχνικό-τεχνολογικό. Δεδομένων των συνθηκών και της σοβαρότητας του θέματος, θεωρούμε ότι έχουμε την υποχρέωση, βάσει ιδρυτικής διακήρυξης και καταστατικού, αλλά κυρίως για τη σωστή πληροφόρηση των πολιτών σε τόσο κρίσιμα ζητήματα, να σχολιάσουμε το συγκεκριμένο θέμα θέτοντας ορισμένα ερωτήματα τεχνικής φύσεως που χρήζουν απάντησης με τον πιο επίσημο, σαφή και άμεσο τρόπο. Συγκεκριμένα, υπάρχουν τέσσερα σημεία που σχετίζονται άμεσα ή έμμεσα με ενδεχόμενες παραβιάσεις της πληροφοριακής υποδομής του TAXIS (ΓΓΠΣ, ΓΓΔΕ, ΚΕΠΥΟ) και που απαιτούν διευκρίνιση και διερεύνηση σε βάθος:

1) ΑΦΜ πολιτών: Σύμφωνα με τα λεγόμενα του πρώην Υπουργού, μέρος του πιθανού σχεδίου έκτακτης ανάγκης («plan B») θα ήταν η ανάπτυξη ενός παράλληλου τραπεζικού-ανταλλακτικού συστήματος εναλλακτικού «εικονικού» νομίσματος («IOU») και το οποίο θα βασιζόταν στην υπάρχουσα υποδομή του TAXIS. Συγκεκριμένα, το ΑΦΜ φυσικών και νομικών προσώπων θα μπορούσε να χρησιμοποιηθεί ως βασικό στοιχείο αναγνώρισης (πρωτεύον κλειδί – primary key) για τη δημιουργία «τραπεζικών» λογαριασμών όψεως ή αποθεματικών (reserve accounts), οι οποίοι σε τελική φάση θα συνοδεύονταν από αναγνωριστικό κωδικό (PIN) για την ασφάλεια της πρόσβασης σε αυτούς από τον εκάστοτε δικαιούχο. Στο σημείο αυτό θα πρέπει να επισημανθούν τα εξής:

- Πουθενά δεν αναφέρεται παραβίαση ή υποκλοπή ΑΦΜ ή κωδικών για την απόκτηση πρόσβασης σε αυτούς. Το ΑΦΜ κάθε φυσικού ή νομικού προσώπου αποτελεί μεν δεδομένο προσωπικού χαρακτήρα (φορολογικό στοιχείο), όμως είναι δημόσια διαθέσιμο υποχρεωτικά σε εμπορικές και φορολογικές συναλλαγές για λόγους επικύρωσης.
- Από μόνο του το ΑΦΜ δεν αποκαλύπτει περισσότερα προσωπικά δεδομένα του κατόχου, παρά μόνο αν συνδυαστεί με αντίστοιχη φορολογική Βάση Δεδομένων (ΒΔ), η οποία αποτελεί μέρος του συστήματος του TAXIS και φυσικά δεν είναι δημόσια προσβάσιμη.
- Υπάρχουν δημόσια προσβάσιμες ηλεκτρονικές υπηρεσίες του TAXIS που επιτρέπουν τον απλό έλεγχο εγκυρότητας ενός ΑΦΜ και που, υπό κάποιες συνθήκες, μπορούν να χρησιμοποιηθούν για τη μαζική καταγραφή έγκυρων

Τ.Θ. 13801, ΤΚ 10310, Αθήνα, http://www.epe.org.gr, e-mail: info@epe.org.gr

ΑΦΜ[1], χωρίς όμως κατ' ανάγκη διαρροή περισσότερων φορολογικών στοιχείων που να σχετίζονται με αυτά.

- Επομένως, στη συγκεκριμένη υπόθεση δεν φαίνεται να προκύπτει ουσιώδες νομικό ή άλλο ζήτημα «υποκλοπής» ΑΦΜ, ούτε κατάχρησης των ηλεκτρονικών υπηρεσιών επικύρωσης ΑΦΜ μέσω δικτύου με σκοπό τη σκόπιμη μη-διαθεσιμότητά τους (network attack: Distributed Denial of Service – DDoS), παρά μόνο ζήτημα διερεύνησης αν μέσω αυτών των όποιων «δοκιμαστικών» ΑΦΜ υπήρξε στην πράξη πρόσβαση από μη εξουσιοδοτημένα άτομα σε πρόσθετα φορολογικά στοιχεία φυσικών ή νομικών προσώπων.

2) Αντιγραφή κώδικα: Σύμφωνα με τα λεγόμενα του πρώην Υπουργού, στα πλαίσια της πιλοτικής σχεδίασης του πιθανού σχεδίου έκτακτης ανάγκης («plan B») θα έπρεπε να αναπτυχθεί κατάλληλο λογισμικό που να αναζητά και να επεξεργάζεται δεδομένα από τις ΒΔ του TAXIS, όπως ακριβώς συμβαίνει με το λογισμικό των φορολογικών εφαρμογών που σήμερα είναι σε χρήση. Για την ανάπτυξη, όμως, τέτοιου λογισμικού απαιτείται χρόνος λεπτομερούς προετοιμασίας, εξειδικευμένη τεχνογνωσία, απασχόληση προσωπικού για σημαντικό χρονικό διάστημα, καθώς και πλήρη πρόσβαση στις προδιαγραφές των αντίστοιχων πρωτοκόλλων επικοινωνίας, ταυτοποίησης, πιστοποίησης δικαιωμάτων και πρόσβασης στις ΒΔ, κτλ. Αντί αυτού, όπως φαίνεται αποφασίστηκε η διαχείριση να γίνει από μία πολύ μικρή ομάδα πέντε ατόμων και να χρησιμοποιηθούν ως έτοιμα πρότυπα κάποια αντίγραφα πηγαίου κώδικα (code templates) από τις εφαρμογές που ήδη λειτουργούν στο TAXIS. Στο σημείο αυτό θα πρέπει να επισημανθούν τα εξής:

- Ο πηγαίος κώδικας, οι εκτελέσιμες εφαρμογές, τα ερωτήματα ΒΔ (SQL queries), καθώς και οι ίδιες οι ΒΔ με τα δεδομένα που περιέχουν, αποτελούν τυπικά και ουσιαστικά «ιδιοκτησία» των αρμόδιων κρατικών φορέων (ΓΓΠΣ, ΓΓΔΕ, ΚΕΠΥΟ). Κατά συνέπεια, η αντιγραφή πηγαίου κώδικα θα πρέπει να θεωρηθεί τυπικά σύννομη και επιτρεπτή επεξεργασία, εφόσον φυσικά αφορά σε εξουσιοδοτημένη υπηρεσιακή χρήση.
- Παρόλα αυτά, η μεταφορά πηγαίου κώδικα εφαρμογών ή οποιωνδήποτε δεδομένων του TAXIS θα πρέπει πάντοτε να είναι σύμφωνη με τους

1 V. Prevelakis, Z. Tzermias, S. Ioannidis, "Privacy Risks from Public Data Sources", 29th International Federation for Information Processing (2014) - http://is.gd/obfa14

Τ.Θ. 13801, ΤΚ 10310, Αθήνα, http://www.epe.org.gr, e-mail: info@epe.org.gr

θεσμοθετημένους κανονισμούς και τις αντίστοιχες Πολιτικές Ασφάλειας (Security Policy) του εκάστοτε φορέα.

- Με βάση τα παραπάνω, αναδεικνύεται για άλλη μια φορά η επιτακτική ανάγκη υιοθέτησης συγκεκριμένων ανοικτών προτύπων (open standards), ειδικά σε ότι αφορά την ανάπτυξη λογισμικού και τη διάθεση πηγαίου κώδικα σε ανοικτή μορφή, σε αντίθεση με ό,τι ισχύει σήμερα. Η υιοθέτηση προτύπων ανοικτού κώδικα θα επέτρεπε αφ' ενός την ανάπτυξη λογισμικού που θα ήταν διασφαλισμένο από διαρροή ευαίσθητων στοιχείων (π.χ. κωδικών πρόσβασης) από τον πηγαίο κώδικα και αφ' ετέρου θα επέτρεπε την επισκόπησή του από οποιονδήποτε, χωρίς να υπάρχει ανάγκη παραβίασης καμίας διοικητικής διαδικασίας και κανενός μηχανισμού ασφαλείας.
- Συνεπώς, στη συγκεκριμένη υπόθεση η πρόθεση αντιγραφής πηγαίου κώδικα από ενεργές εφαρμογές του TAXIS με τον τρόπο που περιγράφεται υπάρχει κάποιο (πιθανότατα ασθενές) έρισμα για περαιτέρω διερεύνηση σε νομικό επίπεδο. Επιπλέον, σύμφωνα με τα λεγόμενα του πρώην Υπουργού η ενέργεια αυτή δεν πραγματοποιήθηκε ποτέ. Όμως, το σημαντικότερο ζήτημα είναι η περιγραφή της πρόθεσης και η αναμενόμενη ευκολία πραγματοποίησης της ενέργειας αυτής, σε σχέση με το γενικότερο θέμα της σημασίας της ασφάλειας των πληροφοριακών συστημάτων των πιο κρίσιμων κρατικών υποδομών. Η ΕΠΕ θεωρεί ότι η οποιαδήποτε επεξεργασία στοιχείων θα πρέπει να γίνεται από το αρμόδιο και ειδικά εξουσιοδοτημένο στελεχιακό δυναμικό, σύμφωνα με το θεσμικό πλαίσιο, και με ιδιαίτερη έμφαση στην ασφάλεια των πληροφοριακών συστημάτων και των σημαντικών δημόσιων υποδομών κρίσιμης σημασίας. Από την περιγραφή γίνεται φανερό ότι η αντιμετώπιση του θέματος είναι εξόχως επιφανειακή, μη επαγγελματική και τεχνικώς επικίνδυνη (πιθανή διαρροή μη πιστοποιημένου πηγαίου κώδικα εφαρμογών του TAXIS).

3) Επέκταση ομάδας εργασίας: Σύμφωνα με τα λεγόμενα του πρώην Υπουργού, υπήρξε σκέψη σχετικά με το πως η ανάπτυξη του πιλοτικού σχεδίου θα εξελισσόταν, από απλή μελέτη εφικτότητας μιας πολύ μικρής ομάδας κλίμακας πέντε ατόμων σε ρεαλιστικό επιχειρησιακό πλάνο έκτακτης ανάγκης κλίμακας 1.000 ατόμων (scale-up). Η επισήμανση έγινε κυρίως σε σχέση με τη δυσκολία διατήρησης της μυστικότητας του όλου εγχειρήματος, όμως αξίζει να σημειωθούν ορισμένα τεχνικά ζητήματα:

Τ.Θ. 13801, ΤΚ 10310, Αθήνα, http://www.epe.org.gr, e-mail: info@epe.org.gr

- Η ανάπτυξη ενός πραγματικού επιχειρησιακού πλάνου βάσει μιας απλής μελέτης εφικτότητας όπως περιγράφεται, δηλαδή για λογισμικό επιπέδου αξιοπιστίας και απόδοσης συγκρίσιμο με αυτό των εφαρμογών που λειτουργούν σήμερα στο TAXIS, απαιτούν μεγάλη προετοιμασία, σχεδίαση και χρονοπρογραμματισμό επιμέρους ομάδων εργασίας, εκτενές διάστημα δοκιμαστικής χρήσης (testing / beta versions), μετάπτωση των ΒΔ (migration) και διαρκής υποστήριξη ειδικά στις πρώτες φάσης της λειτουργίας του, αν και εφόσον ετίθεντο ποτέ σε πραγματική επιχειρησιακή λειτουργία.
- Βάσει των παραπάνω, η περιγραφή του πρώην Υπουργού φανερώνει ότι είτε (α) δεν υπήρξε ποτέ ολοκληρωμένη σχεδίαση, ίσως ούτε καν επίσημη έγκριση για αυτό, ενός πραγματικού επιχειρησιακού πλάνου έκτακτης ανάγκης, είτε (β) υπήρξε έγκριση και σχεδίαση ενός τέτοιου πλάνου, όμως σε τεχνικό επίπεδο είναι σχεδόν σίγουρο ότι δεν θα μπορούσε ποτέ να τεθεί σε επιχειρησιακή χρήση με επιτυχία και κατά συνέπεια απορρίφθηκε.
- Στη συγκεριμένη επιμέρους αναφορά δεν τίθεται ζήτημα διερεύνησης ευθυνών ή πιθανών παραβιάσεων ασφάλειας, όμως καταδεικνύεται ο κίνδυνος καταστρατήγησης των διεθνών προτύπων για τη διασφάλιση ποιότητας λογισμικού (Software Quality Assurance – SQA), η οποία σε τόσο κρίσιμα συστήματα αποτελεί πάντοτε ύψιστη απαίτηση και υποχρέωση. Πρακτικά αυτό σημαίνει ότι, ακόμα κι αν το προτεινόμενο πλάνο είχε την επίσημη κυβερνητική έγκριση ως επίσημη εναλλακτική λύση, ακόμα κι αν η σχεδίασή του είχε ολοκληρωθεί και το νέο σύστημα κατέληγε τελικά έτοιμο προς χρήση, εντούτοις λόγω των προβληματικών τεχνικών προδιαγραφών και του τρόπου ανάπτυξής του, είναι ουσιαστικά βέβαιο ότι η ενεργοποίησή του σύμφωνα με τις περιγραφές του πρώην Υπουργού θα οδηγούσε σε σοβαρά προβλήματα (αξιοπιστίας, διαθεσιμότητας, ασφάλειας, κτλ) ή ακόμα και σε πλήρη αποτυχία. Ανεξαρτήτως προθέσεων ή εμπειρίας των εμπλεκομένων ατόμων, η ανάπτυξη λογισμικού αυτής της κλίμακας και αυτής της κρισιμότητας αποτελεί πάντα ένα εξαιρετικά απαιτητικό και τεχνικώς δύσκολο εγχείρημα, το οποίο απαιτεί την εφαρμογή συγκεκριμένων διαδικασιών, διεθνών προτύπων και αναλυτικού χρονοπρογραμματισμού, στα πλαίσια του επιστημονικού τομέα της Τεχνολογίας / Μηχανικής Λογισμικού (Software Engineering).

Τ.Θ. 13801, ΤΚ 10310, Αθήνα, http://www.epe.org.gr, e-mail: info@epe.org.gr