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

4) ΓΓΔΕ «υπό τον έλεγχο ξένων»: Ανάμεσα στα λεγόμενα του πρώην Υπουργού, αναφέρεται με σαφήνεια ότι η Γενική Γραμματεία Δημοσίων Εσόδων, η οποία είναι υπεύθυνη για την επίβλεψη και λειτουργία του κύριου όγκου του λογισμικού των φορολογικών εφαρμογών του TAXIS (η ΓΓΠΣ είναι αρμόδια κυρίως για τις υλικές υποδομές – data centers), σήμερα βρίσκεται υπό τον έλεγχο ξένων φορέων. Στο σημείο αυτό θα πρέπει να επισημανθούν τα εξής:

- Βάσει του καταστατικού λειτουργίας της και του σχετικού νόμου ιδρύσεώς της (Ν.4093/2013), η ΓΓΔΕ αποτελεί πλέον ανεξάρτητη Αρχή. Συνεπώς, η λειτουργία της διέπεται από τις σχετικές προβλέψεις του υφιστάμενου θεσμικού πλαισίου και έχει κάποια σχετική ανεξαρτησία, καθώς δεν υπόκειται σε άμεσο διοικητικό έλεγχο από τις προϊστάμενες αρχές ως προς την εσωτερική της λειτουργία, πέρα φυσικά από κάποιες βασικές διοικητικές πράξεις που σχετίζονται π.χ. με τον διορισμό του/της γ.γ. ως επικεφαλής (πράξη Υπουργικού Συμβουλίου).
- Το λογισμικό που βρίσκεται υπό την εποπτεία της ΓΓΔΕ είναι από τη φύση του «κρίσιμο» (safety-critical), λόγω της υποδομής με την οποία διασυνδέεται και λόγω του όγκου των δεδομένων προσωπικού χαρακτήρα στον οποίο έχει πρόσβαση. Οποιαδήποτε παραβίαση ή μη εξουσιοδοτημένη χρήση μπορεί να οδηγήσει εν δυνάμει σε μαζική διαρροή ευαίσθητων δεδομένων με εξαιρετικά υψηλό κόστος σε ατομικό και εθνικό επίπεδο.
- Υπάρχει τεράστια διαφορά μεταξύ ενός ανεξάρτητου φορέα που είναι (βάσει νόμου) εκτός του άμεσου δημόσιου ελέγχου και ενός φορέα που βρίσκεται «υπό τον έλεγχο ξένων», ειδικά όταν πρόκειται για τόσο κρίσιμες εθνικές υποδομές.
- Επομένως, η συγκεριμένη αιτίαση του πρώην Υπουργού θα πρέπει να διερευνηθεί άμεσα και σε βάθος, ώστε να διαπιστωθεί αν πράγματι υπάρχει οποιαδήποτε αμφιβολία σχετικά με την ανεξαρτησία της ΓΓΔΕ, σε διοικητικό και λειτουργικό επίπεδο. Μάλιστα, η διερεύνηση αυτή θα πρέπει να περιλαμβάνει και πολύ συγκεκριμένους ελέγχους σε τεχνικό επίπεδο, όπως για παράδειγμα αν/πώς τηρούνται η αντίστοιχη Πολιτική Ασφάλειας (Security Policy), οι νομικά υποχρεωτικές απαιτήσεις των ΑΠΔΠΧ και ΑΔΑΕ σχετικά με την προστασία των δεδομένων προσωπικών δεδομένων και του απορρήτου των επικοινωνιών αντίστοιχα, καθώς και λεπτομερής έλεγχος

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

των ατόμων που είναι νομικά και ουσιαστικά υπεύθυνοι για τη σωστή τήρηση των παραπάνω.

Αξίζει να σημειωθεί ότι ήδη για τα (1) και (2) ο γ.γ. της ΓΓΠΣ κ. Χατζηθεοδώρου έχει προβεί σε επίσημη ανακοίνωση, διαψεύδοντας την πραγματοποίηση οποιωνδήποτε παρόμοιων ενεργειών και επιβεβαιώνοντας την επάρκεια των πρωτοκόλλων ασφαλείας του οργανισμού, ενώ για το (4) η γ.γ. της ΓΓΔΕ κα. Σαββαΐδου έχει δώσει εντολή ένορκης διοικητικής εξέτασης για τη διακρίβωση αν και κατά πόσο τέτοιες ενέργειες έχουν πραγματοποιηθεί και ποια πρόσωπα εμπλέκονται. Επίσης η Εισαγγελεία του Αρείου Πάγου έχει ήδη ξεκινήσει διαδικασίες διερεύνησης πιθανών ποινικών ευθυνών του πρώην Υπουργού και όποιων άλλων εμπλέκονται στην υπόθεση, σε σχέση με το αν οι ενέργειες που περιγράφουν όντως στοιχειοθετούν ποινικά αδικήματα.

Θα πρέπει επίσης να επισημανθούν **δύο σχετικές υποθέσεις**, για τις οποίες η ΕΠΕ έχει πραγματοποιήσει εγκαίρως παρεμβάσεις.

Η πρώτη υπόθεση αφορά στην **τελεσίδικη καταδίκη της ΓΓΠΣ από την ΑΠΔΠΧ**[2], με το ανώτατο προβλεπόμενο χρηματικό πρόστιμο και με απόρριψη του αιτήματος έφεσης (αλλά χωρίς κατηγορίες εναντίον συγκεκριμένων προσώπων), για τη μαζική διαρροή φορολογικών στοιχείων τουλάχιστον 9 εκατ. πολιτών από το σύστημα του TAXIS τουλάχιστον μέχρι και το 2012. Μάλιστα, σύμφωνα με την επίσημη απόφαση της ΑΠΔΠΧ, η διαρροή αφορά παραβιάσεις που φθάνουν ως και 12 χρόνια πριν (2000), ενώ μέχρι και τον Ιούλιο του 2013 διαπιστώνει πως η ΓΓΠΣ εξακολουθούσε να μη διαθέτει τις απαραίτητες και βάσει νόμου υποχρεωτικές διαδικασίες για την ασφάλεια των συστημάτων της, συμπεριλαμβανομένης και μιας ολοκληρωμένης και πρακτικά εφαρμοσμένης Πολιτικής Ασφάλειας (Security Policy). Είναι χαρακτηριστικό ότι στην αιτιολογική έκθεση αναφέρεται πως η έλλειψη αυτών των μηχανισμών κατέστησε ουσιαστικά αδύνατο τον εντοπισμό συγκεκριμένων ατόμων που προέβησαν στις παράνομες αυτές ενέργειες. Χαρακτηριστικά, αναφέραται ότι στα συστήματα της ΓΓΠΣ δεν υπήρχε κανένας έλεγχος, ούτε καταγραφή της πρόσβασης στις εκτυπώσεις, στην απομακρυσμένη σύνδεση (μέσω εξωτερικού δικτύου), στη χρήση φορητών αποθηκευτικών μέσων (USB sticks, disks), κ.ο.κ. Βάσει της απόφασης, η ΓΓΠΣ ήταν υποχρεωμένη να συμμορφωθεί και να εκπονήσει λεπτομερές χρονοδιάγραμμα υλοποίησης όλων των απαραίτητων ενεργειών, με τακτικούς τριμηνιαίους ελέγχους για την τήρησή του. Για την υπόθεση αυτή η ΕΠΕ είχε καταθέσει επίσημη καταγγελία στην

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

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

ΑΠΔΠΧ[3].

Η δεύτερη υπόθεση αφορά σε δημόσια παρέμβαση της ΕΠΕ[4] σχετικά με το **ζήτημα της ύπαρξης και εφαρμογής Πολιτικής Ασφάλειας (Security Policy) σε δημόσιες υπηρεσίες και οργανισμούς**. Η παρέμβαση είχε πραγματοποιηθεί το Οκτώβριο του 2011 και αποτέλεσε αφορμή για σχετική ερώτηση στη Βουλή[5] στα πλαίσια κοινοβουλευτικού ελέγχου, ενώ το θέμα αναδείχθηκε και από τα ΜΜΕ εκείνη την περίοδο. Το βασικό ερώτημα προς τις αρμόδιες αρχές ήταν κατά πόσο τα άτομα που συμμετείχαν στην τότε διαπραγμάτευση, των ελληνικών υπηρεσιών αλλά και των ξένων φορέων (η αρχική «τρόικα» και οι συνεργάτες τους), μπορούσαν τεχνικά να περιοριστούν και να ελεγχθούν σε ότι αφορά την πρόσβαση σε ευαίσθητα και απόρρητα δεδομένα εθνικής σημασίας, όπως για παράδειγμα η αποτίμηση της αξίας εθνικής περιουσίας ή τα ενεργειακά αποθέματα της χώρας. Από τις επίσημες απαντήσεις των συναρμόδιων υπουργείων η πιο ενδιαφέρουσα ήταν αυτή του υπουργείου Εσωτερικών[6] (τότε Υπουργός: κ. Αν. Γιαννίτσης), όπου μεταξύ άλλων αναφερόταν επί λέξει:

«...Δεν διαθέτει ολοκληρωμένη πολιτική ασφάλειας με συγκεριμένες διαδικασίες που να ελέγχονται περιοδικά, έτσι ώστε να διασφαλίζεται η ασφάλεια των δεδομένων και των ευαίσθητων χώρων...»

Η παραπάνω απάντηση αποτελεί ιστορικά ίσως την πρώτη επίσημη παραδοχή της παντελούς απουσίας εθνικής στρατηγικής και συγκεκριμένων πολιτικών σε σχέση με τη διασφάλιση της ασφάλειας κρίσιμων πολιτικών (μη στρατιωτικών) υποδομών της χώρας - την ίδια στιγμή που πρόσφατες μελέτες[7] καταδεικνύουν ότι οι παγκόσμιες δαπάνες για την ασφάλεια των πληροφοριακών συστημάτων φθάνουν τα $77 δις με τάση αύξησης +8% ετησίως. Δυστυχώς η ΕΠΕ δεν είναι καθόλου περήφανη για αυτή της την «επιτυχία», καθώς μόλις ένα χρόνο μετά επιβεβαιώθηκε πλήρως με τον πιο τραγικό τρόπο, με την υπόθεση της μαζικής διαρροής δεδομένων από το TAXIS και την καταδίκη της ΓΓΠΣ.

3 ΑΠΔΠΧ αίτηση: Γ/ΕΙΣ/1597, 4-3-2013 (αρ. υπόθεσης: 057744_0101_04_13)

4 ΕΠΕ (13-10-2011): http://is.gd/zBbBD7

5 Αρ. πρωτ.: 372/21-10-2011

6 Υπουργείο Εσωτερικών: αρ. πρωτ. 3442/15-11-2011

7 Gartner / ESET, «Market Share: All Software Markets, Worldwide, 2014» - http://is.gd/gZ7us5

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

Με αφορμή τη σημερινή υπόθεση ψηφιακών παραβιάσεων, κτλ, **η ΕΠΕ ζητά επιτακτικά**:

(α) από τους συναρμόδιους φορείς του Δημοσίου να επιδείξουν την πρέπουσα προσοχή και επαγγελματισμό στη διασφάλιση των κρίσιμων πληροφοριακών υποδομών της χώρας,

(β) από τις αρμόδιες δημόσιες αρχές να προβούν στην πλήρη διερεύνηση της υπόθεσης και τη διαλεύκανση όλων των λεπτομερειών,

(γ) από τις επίσημες κρατικές αρχές την έγκαιρη και σωστή ενημέρωση του κοινού, επισημαίνοντας τις πραγματικές διαστάσεις της υπόθεσης με ψυχραιμία και αντικειμενικότητα,

(δ) από τα ΜΜΕ να επιδείξουν την απαραίτητη σοβαρότητα και τη δημοσιογραφική εγκυρότητα, αποφεύγοντας τα αυθαίρετα συμπεράσματα και το σχολιασμό χωρίς προηγουμένως να υπάρχει επαρκής διερεύνηση/τεκμηρίωση.

Η ΕΠΕ συνεχίζει να παρακολουθεί την εξέλιξη της συγκεκριμένης υπόθεσης και παραμένει όπως πάντα στη διάθεση κάθε φορέα για την συμβολή της με την επιστημονική κατάρτιση και την τεχνογνωσία που μπορεί να προσφέρει.

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

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