ΕΝΩΣΗ ΠΛΗΡΟΦΟΡΙΚΩΝ ΕΛΛΑΔΑΣ

Ένωση Πληροφορικών Ελλάδας
Κοδριγκτώνος 33, 5ος όροφος
ΤΚ 10434, Αθήνα
http://www.epe.org.gr
e-mail: info@epe.org.gr

Πληροφορίες:
Κυριακός Δημήτρης (Πρόεδρος ΔΣ) τηλ. 6942819819
Μουμουτζής Νεκτάριος (Αντιπρόεδρος ΔΣ) τηλ. 6942819819
Κωνσταντινίδου Κυριακή (Γενικός Γραμματέας ΔΣ) τηλ. 6976893915
Χατζημίσιος Περικλής (Ειδικός Γραμματέας ΔΣ) τηλ. 6945859601
Δημόπουλος Θεόδωρος (Ταμίας ΔΣ) τηλ. 6974893274

ΠΡΟΣ: κ. Κωνσταντίνο Αρβανιτόπουλο, Υπουργό Παιδείας και Θρησκευμάτων

ΚΟΙΝ: κ. Κυριάκο Μητσοτάκη, Υπ. Διοικ. Μεταρρύθμισης και Ηλεκτρονικής Διακυβέρνησης
κ. Αθανάσιο Κυριαζή, Γενικό Γραμματέα Υπουργείου Παιδείας και Θρησκευμάτων
Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα
Βουλευτές
Τμήματα Πληροφορικής ΑΕΙ
Μέσα Ενημέρωσης

ΘΕΜΑ: Προβλήματα ασφάλειας στη διαδικτυακή πλατφόρμα απογραφής υπαλλήλων ΑΕΙ

Αθήνα, 19 Οκτωβρίου 2013

Κύριε Υπουργέ,

Το Υπουργείο Παιδείας και Θρησκευμάτων έχει θέσει σε λειτουργία διαδικτυακή πλατφόρμα (http://odysseas.it.minedu.gov.gr/), με σκοπό την συλλογή στοιχείων απογραφής των διοικητικών υπαλλήλων διαφόρων κλάδων και ειδικοτήτων των οκτώ μεγαλύτερων Πανεπιστημίων της χώρας (Εθνικό Καποδιστριακό Πανεπιστήμιο Αθήνας, Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης, Εθνικό Μετσόβιο Πολυτεχνείο, Πανεπιστήμιο Θεσσαλίας, Πανεπιστήμιο Ιωαννίνων, Πανεπιστήμιο Κρήτης, Πανεπιστήμιο Πάτρας, Οικονομικό Πανεπιστήμιο Αθήνας), με σκοπό την μοριοδότηση και την ένταξη σε διαθεσιμότητα 1349 εξ αυτών των υπαλλήλων.

Πέραν των ουσιωδών ζητημάτων που περιγράψαμε σε προηγούμενη παρέμβασή μας (βλ. http://www.epe.org.gr/showarticle.jsp?articleid=553), η οποία ανέδειξε την καταστροφική πρακτική του ΥΠΑΙΘ για τα Ελληνικά Πανεπιστήμια, η συγκεκριμένη διαδικτυακή εφαρμογή παρουσιάζει σοβαρότατα προβλήματα και κινδύνους ασφάλειας, καθώς παρουσιάζει τεχνικά, διοικητικά και νομικά κενά. Συγκεκριμένα:

1. Δεν διασφαλίζεται η ταυτοποίηση των χρηστών, τα υποβαλλόμενα στοιχεία και το εν γένει περιεχόμενο της βάσης δεδομένων.

   Σε ότι αφορά τον χρήστη της διαδικτυακής εφαρμογής, η ταυτοποίηση γίνεται συνδυαστικά μέσω της εισαγωγής του ΑΦΜ και του ΑΜΚΑ του διοικητικού υπαλλήλου. Όμως, και οι δύο αυτοί αριθμοί μητρώου είναι δημόσια διαθέσιμοι, τόσο εντός των Πανεπιστημίων, όσο και σε διάφορες άλλες δημόσιες ή ιδιωτικές υπηρεσίες. Το ΑΦΜ και το ΑΜΚΑ κάθε διοικητικού υπαλλήλου είναι γνωστά σε ανεξέλεγκτα μεγάλο πλήθος ανθρώπων και φορέων.

   Επιπροσθέτως, οι αριθμοί αυτοί έχουν ευρεία και ενδεχομένως καθημερινή χρήση, ενώ ταυτόχρονα εμφανίζονται ακόμη και σε ένα απλό ενημερωτικό έγγραφο ασφαλιστικού ταμείου ή τράπεζας ή

άλλου φορέα. Επομένως, σε καμία περίπτωση δεν επαρκούν για την αξιόπιστη και ασφαλή ταυτοποίηση του χρήστη. Επιπλέον, δημιουργούν μείζον ζήτημα για τον πραγματικό χρήστη της διαδικτυακής εφαρμογής, καθώς οποιοσδήποτε τρίτος (πέραν του ίδιου του ενδιαφερόμενου διοικητικού υπαλλήλου) μπορεί να εισάγει στο σύστημα δεδομένα αντί αυτού. Τέλος, το ίδιο το πληροφοριακό σύστημα συνολικά καθίσταται αναξιόπιστο ως προς τα δεδομένα που καταγράφει, καθώς κανείς δεν μπορεί εν γένει να διασφαλίσει την ταυτοποίηση των χρηστών και την εγκυρότητα των υποβαλλόμενων στοιχείων και της βάσης δεδομένων.

2. Δεν υπάρχει πιστοποιητικό ασφάλειας του φορέα εξυπηρέτησης της διαδικτυακής υπηρεσίας.
   Σε ότι αφορά το φορέα εξυπηρέτησης της διαδικτυακής υπηρεσίας, δεν υπάρχει εγκατεστημένο πιστοποιητικό ασφάλειας, έτσι ώστε να είναι δυνατός ο έλεγχος και η πιστοποίηση του φορέα εξυπηρέτησης. Συνεπώς, οποιοδήποτε πρόβλημα ασφάλειας στον εξυπηρετητή (π.χ. DNS redirection) μπορεί να οδηγήσει σε σοβαρότατη διαρροή προσωπικών δεδομένων (phishing), καθώς οι χρήστες δεν είναι δυνατό να γνωρίζουν αν τα στοιχεία τους υποβάλλονται όντως στην αρμόδια υπηρεσία ή σε κάποιον τρίτο ο οποίος τα υποκλέπτει.
3. Δεν υπάρχει κρυπτογράφηση δεδομένων.
   Σε ότι αφορά τη μετάδοση των δεδομένων, δεν προβλέπεται τυπική κρυπτογράφηση (SSL/TLS) έτσι ώστε η υποβολή των στοιχείων να προστατεύεται από περιπτώσεις διαρροής κατά τη μεταφορά και διαμεσολάβηση άλλων κόμβων στο διαδίκτυο. Σημειώνεται ότι πολλοί ενδιάμεσοι κόμβοι υποδομής (π.χ. ISP) λειτουργούν με πρόσθετες υπηρεσίες προσωρινής αποθήκευσης δεδομένων, όπως για παράδειγμα HTTP proxy ή caching. Αυτό σημαίνει ότι πολλές από αυτές τις (χωρίς κρυπτογράφηση) πληροφορίες, παραμένουν αποθηκευμένες σε αυτούς τους κόμβους για πολλές ημέρες ή και εβδομάδες, καθιστώντας τις εξαιρετικά ευάλωτες σε ότι αφορά την ανάκτησή τους από τρίτους.
4. Δεν υπάρχει δήλωση περί προστασίας των προσωπικών δεδομένων.
   Στη συγκεκριμένη σελίδα δεν αναφέρεται πουθενά δήλωση για την τήρηση των προβλέψεων του νόμου περί προστασίας των προσωπικών δεδομένων, σχετικά με τον τρόπο επεξεργασίας, το χρόνο και τον τόπο αποθήκευσης, καθώς και τον υπεύθυνο διαχείρισης, όπως προβλέπεται από τους σχετικούς νόμους και τις διατάξεις της Αρχής Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.
5. Τα δεδομένα της συγκεκριμένης υπηρεσίας είναι άνευ οποιασδήποτε νομικής υπόστασης.
   Η καταχώρηση και επεξεργασία δεδομένων σε παρόμοιες υπηρεσίες γενικά ακολουθεί ένα από τα εξής μοντέλα: (α) άμεση πρόσβαση στη βάση δεδομένων (online) με άμεσο έλεγχο/καταχώρηση, (β) ετεροχρονισμένη υποβολή, έλεγχο και καταχώρηση στη βάση δεδομένων (offline), (γ) κάποιο ενδιάμεσο μοντέλο, τυπικά με άμεση πρόσβαση για ανάγνωση-μόνο και ετεροχρονισμένο έλεγχο/καταχώρηση τυχόν αλλαγών. Αν στο συγκεκριμένο σύστημα εφαρμόζεται το (α), τότε ο εξαιρετικά αδύναμος μηχανισμός ταυτοποίησης κατά την είσοδο (login) καθιστά ολόκληρη τη βάση δεδομένων ανοικτή σε καταστροφικές αλλαγές από τρίτους, μη εξουσιοδοτημένους χρήστες. Αν στο

Κοδριγκτώνος 33, (5ος όροφος), ΤΚ 10434, Αθήνα, http://www.epe.org.gr, e-mail: info@epe.org.gr

σύστημα εφαρμόζεται είτε το (β) είτε το (γ), αυτό σημαίνει ότι για την οριστική καταχώρηση των στοιχείων στη βάση δεδομένων πρέπει αναγκαστικά να προηγηθεί έλεγχος και επικύρωση από αρμόδιους υπαλλήλους - κάτι που δεν προβλέπεται ούτε στην περιγραφή της συγκεκριμένης υπηρεσίας (βλ. 4), ούτε και στην αντίστοιχη "Πρόσκληση Απογραφής" που αναφέρεται (150628/15-10-2013). Ως εκ τούτου, η συγκεκριμένη υπηρεσία είναι άνευ οποιασδήποτε νομικής υπόστασης σε ότι αφορά τη διασφάλιση της εγκυρότητας του τρόπου επεξεργασίας των δεδομένων που υποβάλλονται, κάτι που επιβεβαιώνεται και από την ίδια την πρόσκληση (βλ. παρ. Β, περί πρόσθετης κατάθεσης εγγράφως).

6. Τα δεδομένα της συγκεκριμένης υπηρεσίας είναι άκυρα και παράνομα.

   Εφόσον ο συγκεκριμένος μηχανισμός που έχει υλοποιηθεί στην εν λόγω πλατφόρμα, σε καμία περίπτωση δεν διασφαλίζει την αξιόπιστη ταυτοποίηση του χρήστη, είναι φανερό πως δεν μπορεί να χρησιμοποιηθεί σύμφωνα με τους σκοπούς που αναφέρει και δεν επέχει θέση υπεύθυνης δήλωσης από τον υπάλληλο. Επιπλέον, οποιοσδήποτε υπάλληλος έχει ήδη καταγραφεί στο σύστημα μπορεί κάλλιστα να ισχυριστεί ότι η εισαγωγή των στοιχείων του έγινε από κάποιον τρίτο χωρίς την έγκριση του ίδιου (άρα είναι άκυρη και παράνομη). Συνεπώς δεν ισχύει η πρόβλεψη της παρ. Δ στην πρόσκληση απογραφής περί ισχύος ως υπεύθυνης δήλωσης του ν.1599/1986.

Κατόπιν των ανωτέρω, ως Ένωση Πληροφορικών Ελλάδος:

1. Καλούμε την αρμόδια υπηρεσία του Υπουργείου Παιδείας και Θρησκευμάτων να απενεργοποιήσει άμεσα τη συγκεκριμένη πλατφόρμα, καθώς επίσης και να ενημερώσει άμεσα όσους χρήστες φέρονται να την έχουν χρησιμοποιήσει ήδη σχετικά με τους κινδύνους ασφάλειας ως προς τα δεδομένα που έχουν καταχωρηθεί, καθώς δεν υπάρχει ταυτοποίηση των χρηστών.
2. Καλούμε την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα να προχωρήσει σε πλήρη εξωτερικό έλεγχο (external audit) σχετικά με πιθανή παραβίαση του συστήματος με πιθανή διαρροή ή αλλοίωση προσωπικών δεδομένων.
3. Ενημερώνουμε τους διοικητικούς υπαλλήλους τους οποίους αφορά η συγκεκριμένη απογραφή, ότι το συγκεκριμένο σύστημα ενέχει σοβαρότατους κινδύνους για την ασφάλεια των προσωπικών τους δεδομένων.
4. Ενημερώνουμε τους διοικητικούς υπαλλήλους ότι ενδέχεται να έχουν υποβληθεί στοιχεία στη συγκεκριμένη διαδικτυακή πλατφόρμα εν αγνοία τους, με τη χρήση του ΑΦΜ και του ΑΜΚΑ τους.

Εκ μέρους του Διοικητικού Συμβουλίου
της Ένωσης Πληροφορικών Ελλάδας

Ο Πρόεδρος
Δημήτρης Κυριακός
κιν. 6942819819

Η Γενική Γραμματέας
Κυριακή Κωνσταντινίδου
κιν. 6976893915

Κοδριγκτώνος 33, (5ος όροφος), ΤΚ 10434, Αθήνα, http://www.epe.org.gr, e-mail: info@epe.org.gr