ΣΥΡΙΖΑ
ΠΡΟΟΔΕΥΤΙΚΗ ΣΥΜΜΑΧΙΑ

Αθήνα, 11 Μαΐου 2021

ΕΡΩΤΗΣΗ

Προς τον Υπουργό Ψηφιακής Διακυβέρνησης

ΘΕΜΑ: «Σοβαρά κενά ασφαλείας στα πληροφοριακά συστήματα e-ΕΦΚΑ και Υπουργείου Ψηφιακής Διακυβέρνησης τα καθιστούν ευάλωτα σε κυβερνοεπιθέσεις»

Πρόσφατα δημοσιεύματα σε γνωστές ιστοσελίδες με θέματα πληροφορικής (βλ. π.χ. https://iguru.gr/2021/04/06/keno-asfaleias-stin-istoselida-tou-efka), αποκάλυψαν ότι σε δοκιμές διείσδυσης (penetration testings) που έγιναν από ιδιώτες επαγγελματίες ειδικούς Κυβερνοασφάλειας (cybersecurity experts) κατά των ιστοσελίδων και πληροφοριακών συστημάτων του e-ΕΦΚΑ και του Υπουργείου Ψηφιακής Διακυβέρνησης, εντοπίστηκαν σοβαρά κενά ασφαλείας που μπορούσαν εύκολα να θέσουν σε κίνδυνο υποκλοπής, ευαίσθητα προσωπικά δεδομένα των πολιτών και κρατικές πληροφορίες. Αυτού του είδους οι δοκιμές αποτελούν δοκιμαστικές εισβολές σε πληροφοριακά συστήματα για την αξιολόγηση της ασφάλειάς τους, κατά τις οποίες γίνεται προσομοίωση πιθανής επίθεσης κακόβουλου εισβολέα (hacker) που έχει σκοπό την εκμετάλλευση κενών ασφαλείας στις βάσεις δεδομένων δημόσιων και ιδιωτικών οργανισμών.

Οι συγκεκριμένες δοκιμές αποκάλυψαν ότι ένας κακόβουλος εισβολέας θα μπορούσε να αποκτήσει πρόσβαση στους κωδικούς χρήστη και ασφαλείας (user names και passwords) των ασφαλισμένων του e-ΕΦΚΑ, κυρίως λόγω της παλαιότητας των τεχνικών κρυπτογράφησής τους, γεγονός που κατά τεκμήριο ενδέχεται να του δώσει πρόσβαση και δυνατότητα επεξεργασίας στοιχείων του κάθε ασφαλισμένου, όπως οφειλές κ.ά. Σε συνέντευξή του στο διαδικτυακό κανάλι της ιστοσελίδας insomnia.gr (βλ. σχετ. https://www.youtube.com/watch?v=Xc-7HIeorp8&t=514s) που δημοσιεύθηκε στις 13/4/2021, ο ένας εκ των ειδικών κυβερνοασφάλειας εκτιμά πως υπάρχουν πάνω από δέκα (10) σοβαρά κενά ασφαλείας στον e-ΕΦΚΑ, ενώ αντίστοιχα κενά εντόπισε και στα συστήματα του Υπουργείου Ψηφιακής Διακυβέρνησης. Μάλιστα, ισχυρίζεται ότι ενημέρωσε άμεσα με ηλεκτρονικό ταχυδρομείο τους υπεύθυνους των υπηρεσιών για τα κενά ασφαλείας που ανακάλυψε, προτείνοντας ταυτόχρονα τρόπους αντιμετώπισης και διόρθωσης των συστημάτων, χωρίς όμως να λάβει κάποια απάντηση. Επιπλέον, δηλώνει πως θεωρεί

ιδιαιτέρως ευάλωτα όλα τα συστήματα του δημοσίου τομέα, ενδεχομένως και αυτό του taxisnet, στο οποίο εκτός από φορολογικά στοιχεία των πολιτών, τηρούνται και οι αντίστοιχοι κωδικοί με τους οποίους οι πολίτες πλέον έχουν πρόσβαση σε πλήθος ψηφιακών υπηρεσιών μέσω κυρίως του gov.gr.

Τα ζητήματα Κυβερνοασφάλειας έχουν καταστεί υψηλής σημασίας και εκ των ων ουκ άνευ για τον ψηφιακό μετασχηματισμό του Κράτους και της οικονομίας, ιδίως έπειτα από την ισχυρές ρυθμίσεις για τα προσωπικά δεδομένα που εισήγαγε ο ευρωπαϊκός Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR). Η χώρα μας το 2018 έκανε σημαντικά βήματα ώστε να αποκτήσει ένα συνεκτικό θεσμικό πλαίσιο και να αναβαθμίσει τις υπηρεσίες που σχετίζονται με την Κυβερνοασφάλεια. Ενσωμάτωσε με τον ν.4577/2018 στο εθνικό δίκαιο την ευρωπαϊκή Οδηγία 2016/1148/ΕΕ σχετικά με μέτρα για υψηλό κοινό ευρωπαϊκό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών (NIS), αναθεώρησε την Εθνική Στρατηγική Κυβερνοασφάλειας (Υ.Α. έγκρισης με ΑΔΑ: Ψ4Ρ7465ΧΘ0-Ζ6Ω) και υπέγραψε στις 13/11/2018 συμφωνία έδρας για την αναβάθμιση του ευρωπαϊκού Οργανισμού Ασφάλειας Δικτύων και Πληροφοριών - Ευρωπαϊκού Οργανισμού Κυβερνοασφάλειας (ENISA) που εδρεύει στην Ελλάδα, ως σημείου αναφοράς και αριστείας της Κυβερνοασφάλειας στην Ευρώπη (κυρώθηκε στη συνέχεια με τον ν.4627/2019). Η κατ΄ εφαρμογή του ν.4577/2018 εκδοθείσα Υ.Α. 1027 (ΦΕΚ 3739Β'/2019) εξειδίκευσε τις βασικές απαιτήσεις ασφαλείας συστημάτων δικτύου και πληροφοριών, τις διαδικασίες παροχής πληροφοριών και κοινοποίησης συμβάντων στις αρμόδιες Αρχές, καθώς και τους Φορείς Εκμετάλλευσης Βασικών Υπηρεσιών (κρίσιμες υποδομές και υπηρεσίες των οποίων, εάν η ομαλή δραστηριότητα διαταραχθεί, αναμένεται να υπάρξουν σημαντικές επιπτώσεις στην εύρυθμη λειτουργία του κρατικού μηχανισμού και στη ζωή των πολιτών).

Σύμφωνα με τον ν.4577/2018, ως αρμόδια Εθνική Αρχή Κυβερνοασφάλειας, έχει οριστεί η νυν υπηρεσιακή δομή της Γενικής Διεύθυνσης Κυβερνοασφάλειας του Υπουργείου Ψηφιακής Διακυβέρνησης. Ωστόσο, μια Αρχή με τόσο υψηλή σημασία, στελεχώνεται με ευθύνη της κυβέρνησης, κατά παρέκκλιση των διατάξεων των άρθρων 85 και 86 του Κώδικα Κατάστασης Δημοσίων Πολιτικών Διοικητικών Υπαλλήλων και Υπαλλήλων Ν.Π.Δ.Δ. (που κυρώθηκε με το άρθρο πρώτο του ν. 3528/2007, όπως ισχύει). Συγκεκριμένα, σύμφωνα με τα άρ.50 του ν.4635/2019 και άρ.57 του ΠΔ 40/2020, ο προϊστάμενος της δομής αυτής επιλέγεται και τοποθετείται με απόφαση του Υπουργού, ύστερα από εισήγηση τριμελούς επιτροπής που αποτελείται από δύο Γενικούς Γραμματείς και έναν Υπηρεσιακό Γραμματέα, δηλαδή παρακάμπτεται το σύστημα μοριοδότησης του Κώδικα, οι διαδικασίες που αυτός προβλέπει και τα Συμβούλια Επιλογής που συμμετέχουν εκπρόσωποι του ΑΣΕΠ, του Νομικού Συμβουλίου του Κράτους και του Ε.Κ.Δ.Δ.Α.

Επειδή τα κενά ασφαλείας που εντοπίστηκαν στα συστήματα του e-ΕΦΚΑ τα καθιστά ευάλωτα σε κυβερνοεπιθέσεις από τις οποίες είναι δυνατό να παραβιαστούν ευαίσθητα προσωπικά δεδομένα των ασφαλισμένων και σημαντικά δεδομένα που αφορούν την κοινωνική ασφάλιση.

Επειδή τα κενά ασφαλείας που εντοπίστηκαν στα συστήματα του Υπουργείου Ψηφιακής Διακυβέρνησης, πλήττουν συνολικά την αξιοπιστία της ασφάλειας των πληροφοριακών συστημάτων του Δημοσίου, καθότι πρόκειται για το Υπουργείο στο οποίο υπάγεται η Εθνική Αρχή Κυβερνοασφάλειας.

Επειδή πιθανό κενό ασφαλείας που θα μπορούσε να δώσει πρόσβαση σε κακόβουλους στους κωδικούς taxisnet των πολιτών, θα είχε σοβαρές επιπτώσεις στη λειτουργία των ψηφιακών υπηρεσιών που παρέχονται από το Δημόσιο στους πολίτες.

Επειδή η Εθνική Αρχή Κυβερνοασφάλειας (Γενική Διεύθυνση Κυβερνοασφάλειας του Υπουργείου Ψηφιακής Διακυβέρνησης) προκειμένου να επιτελέσει το νευραλγικό ρόλο της, απαιτείται να έχει επαρκή και αξιοκρατική στελέχωση.

Ερωτάται ο αρμόδιος Υπουργός:

1. **Είναι σε γνώση του τα αποτελέσματα των δοκιμών διείσδυσης (penetration tests) που είδαν το φως της δημοσιότητας, σύμφωνα με τα οποία τα πληροφοριακά συστήματα του e-ΕΦΚΑ και του Υπουργείου Ψηφιακής Διακυβέρνησης παρουσίαζαν σοβαρά κενά ασφαλείας και ήταν εκτεθειμένα ακόμα και σε πιθανές υποκλοπές ευαίσθητων προσωπικών δεδομένων των ασφαλισμένων; Αν ναι, ποια ακριβώς δεδομένα ήταν εκτεθειμένα;**
2. **Ενημερώθηκαν οι αρμόδιες υπηρεσίες για τα αποτελέσματα αυτά και τα κενά ασφαλείας που εντοπίστηκαν; Σε ποιες ενέργειες προέβησαν, ώστε να θωρακιστούν τα συστήματα; Ισχύει η εκτίμηση ότι υπάρχουν τουλάχιστον δέκα (10) ακόμα σοβαρά κενά ασφαλείας; Τηρούνται εν γένει οι προβλέψεις της Υ.Α. 1027 (ΦΕΚ 3739Β'/2019);**
3. **Υπήρξαν συμβάντα κυβερνοεπιθέσεων που να σχετίζονται με τα συγκεκριμένα κενά ασφαλείας; Αν ναι, προέβησαν οι αρμόδιες υπηρεσίες στις κατά τη νομοθεσία απαιτούμενες ενέργειες διαχείρισης των συμβάντων και προστασίας των προσωπικών δεδομένων;**
4. **Υπάρχει πιθανότητα να έχουν εκτεθεί σε κακόβουλες κυβερνοεπιθέσεις οι βάσεις δεδομένων που τηρούνται οι κωδικοί taxisnet των πολιτών, λόγω κενών ασφαλείας; Είναι επαρκώς θωρακισμένα τα αντίστοιχα συστήματα;**

5. **Προτίθεται να προχωρήσει σε ενέργειες εκσυγχρονισμού και αναβάθμισης των πληροφοριακών συστημάτων και ιδίως των τεχνικών κρυπτογράφησης των κωδικών χρήστη και ασφαλείας (user names και passwords) που χρησιμοποιούν οι πολίτες για την πρόσβαση σε ψηφιακές υπηρεσίες του Δημοσίου;**
6. **Πόσες οργανικές θέσεις υπαλλήλων προβλέπονται στη Γενική Διεύθυνση Κυβερνοασφάλειας, τις Διευθύνσεις και τα Τμήματα που υπάγονται σε αυτή; Πόσες από αυτές τις θέσεις είναι στελεχωμένες;**
7. **Προτίθεται να καταργήσει τις ειδικές διατάξεις του αρ.50 του ν.4635/2019 που προβλέπουν επιλογή προϊσταμένου της Γενικής Διεύθυνσης Κυβερνοασφάλειας κατά παρέκκλιση των διατάξεων των άρθρων 85 και 86 του Κώδικα Κατάστασης Δημοσίων Πολιτικών Διοικητικών Υπαλλήλων και Υπαλλήλων Ν.Π.Δ.Δ. (που κυρώθηκε με το άρθρο πρώτο του ν. 3528/2007, όπως ισχύει), προκειμένου στο εξής να επιλέγεται σύμφωνα με όσα προβλέπει ο Κώδικας;**

Οι ερωτώντες βουλευτές

Κάτσης Μάριος

Γκαρά Αναστασία (Νατάσα)