ΒΟΥΛΗ ΤΩΝ ΕΛΛΗΝΩΝ
ΔΙΕΥΘΥΝΣΗ ΚΟΙΝΟΒΟΥΛΕΥΤΙΚΟΥ ΕΛΕΓΧΟΥ

Αριθμ. Πρωτ. ΕΡΩΤΗΣΕΩΝ: 4505
Ημερομ. Κατάθεσης: 7/4/2022

ΒΟΥΛΗ ΤΩΝ ΕΛΛΗΝΩΝ

ΙΛΧΑΝ ΑΧΜΕΤ – ΒΟΥΛΕΥΤΗΣ ΡΟΔΟΠΗΣ

Κίνημα Αλλαγής

ΕΡΩΤΗΣΗ

Αθήνα, 7/04/2022

Προς τον Υπουργό Ψηφιακής Διακυβέρνησης κ. Κυριάκο Πιερρακάκη

Θέμα: «Κυβερνοασφάλεια - Χωρίς Πιστοποιητικά Ασφαλείας SSL κρίσιμες ιστοσελίδες Υπουργείων, Φορέων και Οργανισμών»

Η κυβερνοεπίθεση που δέχθηκαν τα Ελληνικά Ταχυδρομεία (ΕΛΤΑ) στις 20/03/2022 αποδεδειγμένα προκάλεσε πολλαπλά προβλήματα στις χρηματοοικονομικές υπηρεσίες και την αποστολή αλληλογραφίας, υπηρεσίες οι οποίες άρχισαν να επανέρχονται από την Πέμπτη 24 Μαρτίου. Εξαιτίας μάλιστα της εν λόγω κυβερνοεπίθεσης, σύμφωνα με τη διοίκηση των ΕΛΤΑ, ενδέχεται να έχει καθυστερήσει η καταβολή συντάξεων σε 15 περιοχές της χώρας.

Η συγκεκριμένη επίθεση έθεσε εκτός λειτουργίας συστήματα και λειτουργίες κρίσιμες για το κοινωνικό σύνολο και την αγορά, ενώ είναι ασαφές ακόμα εάν το συγκεκριμένο περιστατικό έχει οδηγήσει και στη διαρροή δεδομένων επικοινωνίας των πολιτών γεγονός που θα παραβίαζε το συνταγματικό δικαίωμά τους στην προστασία του απόρρητο των επικοινωνιών.

Το δυστύχημα είναι πως δεν είναι η πρώτη φορά που η χώρα μας γίνεται εύκολος στόχος κυβερνοεπιθέσεων. Το καλοκαίρι του 2021 χάκαραν τους servers του Δήμου Θεσσαλονίκης για να ζητήσουν λύτρα, το 2020 επίθεση δέχεται η Cosmote με μεγάλης κλίμακας διαρροή δεδομένων, με την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα να της επιβάλλει για την εν λόγω διαρροή πρόστιμο 6.000.000 ευρώ. Στο στόχαστρο των χάκερ το 2019 βρέθηκε το Μέγαρο Μαξίμου, το υπουργείο Εσωτερικών, η ΕΥΠ και η Ελληνική Αστυνομία, στο πλαίσιο μιας διεθνούς εκστρατείας κυβερνοκατασκοπείας με την κωδική ονομασία «Θαλάσσια Χελώνα» (Sea Turtle), ενώ και το Υφυπουργείο Αθλητισμού το ίδιο έτος δέχτηκε επίθεση από τον ιό «Sudikobi», για τον οποίο παγκοσμίως δεν υπάρχει κλειδί

αποκρυπτογράφησης. Παράλληλα παραμένει ανοιχτή η υπόθεση συνεργασίας της κυβέρνησης με τη cisco και την προβληματική κατοχύρωση των δεδομένων εκατοντάδων χιλιάδων μελών της εκπαιδευτικής κοινότητας, μαθητών και καθηγητών, για την οποία η αρμόδια ανεξάρτητη Αρχή (ΑΠΔΠΧ) εντόπισε σωρεία παραλήψεων σε σχέση με το Γενικό Κανονισμό Προστασίας Προσωπικών Δεδομένων από το Υπουργείο Παιδείας.

Με βάση τα παραπάνω, αλλά και άλλες περιπτώσεις που πιθανά δεν έχουν δει το φως της δημοσιότητας δεν αποτελεί έκπληξη η έκθεση "Outseer Fraud and Payments Report Q4 2021", σύμφωνα με την οποία οι κυβερνοεγκληματίες κατευθύνουν το 7% των απειλών phishing σε ελληνικές επιχειρήσεις και οργανισμούς, με αποτέλεσμα η Ελλάδα να βρίσκεται στην 5η θέση παγκοσμίως μεταξύ των χωρών με τις περισσότερες ψηφιακές επιθέσεις «ηλεκτρονικού ψαρέματος» (phising).

Αυτό που προκαλεί έκπληξη είναι πως κρίσιμες ιστοσελίδες Υπουργείων, φορέων και οργανισμών δεν διαθέτουν, ακόμη και σήμερα Ηλεκτρονικό Πιστοποιητικό Ασφαλείας SSL, που είναι απαραίτητο για μια ασφαλή σύνδεση μεταξύ της εκάστοτε ιστοσελίδας και του web browser (Google Chrome, Microsoft Edge, Mozilla, Firefox κ.α.) του χρήστη. Τα πιστοποιητικά ασφαλείας SSL εξυπηρετούν αφενός την ασφαλή μεταφορά δεδομένων μεταξύ web server και ενός browser και αφετέρου την πιστοποίηση – ταυτοποίηση της ιστοσελίδας ώστε ο χρήστης να γνωρίζει πως συναλλάσσεται σε ένα ασφαλές περιβάλλον. Είναι χαρακτηριστική η απουσία του εν λόγω πιστοποιητικού τόσο από την ιστοσελίδα του Υπουργείου Αγροτικής Ανάπτυξης, όσο και από την ιστοσελίδα των διαβατηρίων (!) http://www.passport.gov.gr, στην οποία σαφώς οι πολίτες εκθέτουν προσωπικά στοιχεία.

Δεδομένου ότι σύμφωνα με την Check Point Research (CPR), το 2021 και με στοιχεία του περασμένου Οκτωβρίου, στην Ελλάδα παρατηρήθηκε μέσος όρος 485 εβδομαδιαίων επιθέσεων ανά οργανισμό – μια αύξηση της τάξης του 21% σε σχέση με το 2020.

Δεδομένου ότι μία απλή περιήγηση σε ιστοσελίδες αρκετών ελληνικών Υπουργείων, φορέων και οργανισμών, αποδεικνύει πως συνεχίζουν να μην διαθέτουν ασφαλή σύνδεση, δηλαδή Ηλεκτρονικό Πιστοποιητικό Ασφαλείας SSL.

Δεδομένου ότι το Υπουργείο Ψηφιακής Διακυβέρνησης, συνεχίζει να διαχειρίζεται τα σοβαρά θέματα της κυβερνοασφάλειας, διακινώντας επιστολές και εγκύκλιούς όπως γίνεται σε ένα γραφειοκρατικό δημόσιο αντί να οργανώνει συγκεκριμένες ενέργειες, δράσεις και ομάδες ανθρώπων στο πεδίο.

Δεδομένου ότι οι κυβερνοεπιθέσεις θέτουν σε σοβαρό κίνδυνο ευαίσθητα προσωπικά δεδομένα των πολιτών (πχ υγείας) που όλο και περισσότερο διακινούνται ψηφιακά.

Ερωτάται ο αρμόδιος κ. Υπουργός:

1. Ποιος είναι ο σχεδιασμός για τον εντοπισμό αλλά και την αντιμετώπιση περιστατικών κυβερνοασφάλειας σε φορείς της κεντρικής κυβέρνησης, στους δήμους αλλά και επιχειρήσεις κοινής ωφέλειας που έχουν σημαντικά μεγάλο αριθμό πελατών, τη στιγμή που όλο και περισσότερα προσωπικά δεδομένα, διακινούνται ψηφιακά, τα οποία βασίζονται σε πληροφοριακά συστήματα περασμένων δεκαετιών;

2. Για ποιο λόγο υπάρχουν μέχρι σήμερα ιστοσελίδες Υπουργείων και φορέων που σε πολλές περιπτώσεις ζητούν προσωπικά στοιχεία από τους πολίτες χωρίς Ηλεκτρονικά Πιστοποιητικά Ασφαλείας SSL;
3. Υπάρχει στην Ελλάδα επίσημος μηχανισμός παρακολούθησης και αναφορών περιστατικών κυβερνοασφάλειας;
4. Γιατί το Υπουργείο Ψηφιακής Διακυβέρνησης δεν έχει μέχρι σήμερα γνωστοποιήσει - εκπονήσει το στρατηγικό πλάνο κυβερνοασφάλειας για το δημόσιο και τον ιδιωτικό τομέα;

Ο ερωτών Βουλευτής

Ιλχάν Αχμέτ