Μαρούσι, 19 Οκτωβρίου 2018
Αρ. πρωτ.: 3268
ΑΝΑΡΤΗΤΕΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

ΑΠΟΦΑΣΗ

(αριθμ: 214/2018)

Θέμα: Κλήση σε ακρόαση της εταιρείας με την επωνυμία «……..» και το διακριτικό τίτλο «….» (εφεξής «…….») με αντικείμενο τον έλεγχο ενδεχόμενης παραβάσεως της κείμενης νομοθεσίας περί προστασίας του απορρήτου των επικοινωνιών.

Την Τετάρτη, 4η Ιουλίου 2018, η Ολομέλεια της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών, παρισταμένων του Προέδρου, κ. Χρήστου Ζαμπίρα, του Αντιπροέδρου κ. Μιχαήλ Σακκά, καθώς και των τακτικών μελών κ.κ. Μιχαήλ Γεωργιακόδη, Γεωργίου Μπακάλη, Αικατερίνης Παπανικολάου και Παναγιώτη Ριζομυλιώτη, καθώς και του αναπληρωματικού μέλους κου Δημοσθένη Βουγιούκα, ο οποίος προσήλθε προς αναπλήρωση του τακτικού μέλους κου Ιωάννη Ασκοξυλάκη, ο οποίος δεν προσήλθε λόγω κωλύματος, αν και είχε νομίμως και εμπροθέσμως προσκληθεί, συνήλθε σε συνεδρίαση προκειμένου να αποφασίσει επί της ενδεχόμενης κλήσης σε ακρόαση της εταιρείας «……..», με αντικείμενο τον έλεγχο της ενδεχόμενης παραβάσεως της κείμενης νομοθεσίας περί προστασίας του απορρήτου των επικοινωνιών.

Ειδικότερα:

Α. Στην Α.Δ.Α.Ε. υποβλήθηκαν οι υπ' αριθμ. πρωτ. ΑΔΑΕ ΕΜΠ 186/25-11-2015, ΕΜΠ 187/25-11-2015 και ΕΜΠ 188/25-11-2015 αναφορές περιστατικών ασφάλειας της εταιρείας «…….», σύμφωνα με τις οποίες …….. λειτουργούσαν παράνομοι ιστότοποι, οι οποίοι προσομοίωναν ιστοτόπους διάφορων τραπεζικών ιδρυμάτων.

Για τη διερεύνηση των εν λόγω περιστατικών ασφάλειας αποφασίστηκε, με την υπ' αριθμ. 134/2016 Απόφαση της Ολομέλειας της Α.Δ.Α.Ε. και την υπ' αριθμ. 155/2016 Απόφαση του Προέδρου της Αρχής, η σύσταση ομάδας ελέγχου, η οποία διενήργησε το σχετικό έλεγχο στις εγκαταστάσεις της εταιρείας «……..». Τα αποτελέσματα του ελέγχου, όπως αυτά αποτυπώθηκαν στην από 30.06.2017 «Έκθεση Διενέργειας Εκτάκτου Ελέγχου στις εγκαταστάσεις της εταιρείας …….. κατόπιν περιστατικών ασφάλειας με αριθμ. πρωτ. ΕΜΠ187/25.11.2015, ΕΜΠ188/25.11.2015 και ΕΜΠ186/25.11.2015» και εγκρίθηκαν από την Ολομέλεια της Αρχής, κατά τη συνεδρίαση της 27ης Σεπτεμβρίου 2017, έχουν ως εξής:

«Γ. ΕΞΕΤΑΣΗ ΤΩΝ ΣΤΟΙΧΕΙΩΝ – ΑΠΟΤΕΛΕΣΜΑΤΑ ΤΟΥ ΕΛΕΓΧΟΥ

Από τον επιτόπιο έλεγχο στην εταιρεία ……. και από την εξέταση των στοιχείων που απέστειλε η εταιρεία με τα υπ΄αριθμ. πρωτ. ΑΔΑΕ 1517/07.07.2016, 2427/18.10.2016 και ΕΜΠ278/23.12.2016, 3213/28.12.2016 και 2/02.01.2017 έγγραφα, καθώς και το υπ'αριθμ. πρωτ. ΑΔΑΕ 1822/15.06.2017 έγγραφο της ΕΕΤΤ, προέκυψαν τα ακόλουθα:

1. Στο πλαίσιο του από 27.06.2016 επιτόπιου ελέγχου, η εταιρεία δήλωσε ότι παρέχει υπηρεσία email στους πελάτες της, είτε ως μεμονωμένη υπηρεσία, είτε συνδυαστικά με την υπηρεσία web hosting και ότι έχει ξεκινήσει τη διαδικασία χορήγησης Γενικής Άδειας για την υπηρεσία email από την ΕΕΤΤ από τις 25/05/2015, χωρίς όμως να της έχει χορηγηθεί από την ΕΕΤΤ μέχρι και την ημερομηνία διεξαγωγής του ελέγχου (συνημμένο 11 του Πρακτικού της 27ης Ιουνίου 2016). Σε σχετικό ερώτημα της Ο.Ε. προς την ΕΕΤΤ (υπ΄αριθμ.πρωτ. ΑΔΑΕ ΕΜΠ12/03.02.2017), η ΕΕΤΤ απάντησε ότι έως την 15.06.2017, η εταιρεία …….. *δεν είχε προχωρήσει στην υποβολή Δήλωσης Καταχώρησης υπό καθεστώς Γενικής Άδειας* (υπ΄αριθμ. πρωτ. ΑΔΑΕ 1822/15.06.2017 έγγραφο της ΕΕΤΤ).
2. Στο πλαίσιο του από 27.06.2016 επιτόπιου ελέγχου η εταιρεία δήλωσε ότι δε διαχειριζόταν το περιεχόμενο και τη λειτουργία των ιστοσελίδων των πελατών της για τα 3 υπό εξέταση περιστατικά και ενημέρωσε την Ο.Ε. ότι η ίδια πρακτική ακολουθείται για όλους τους πελάτες web hosting της εταιρείας.
3. Στο πλαίσιο του από 27.06.2016 επιτόπιου ελέγχου, η εταιρεία δήλωσε ότι διαθέτει Πολιτική Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών, σύμφωνα με το Άρθρο 1, παρ. 1.1 της Απόφασης 165/2011 της ΑΔΑΕ (ΦΕΚ Β΄2715), και παρέδωσε αυτή στην Ο.Ε. (συνημμένο 1 του Πρακτικού της 27ης Ιουνίου 2016). Η εταιρεία δήλωσε επίσης, ότι η Πολιτική Ασφάλειας ξεκίνησε να υλοποιείται περί τον Ιούλιο του 2015 (συνημμένο 2 του Πρακτικού της 27ης Ιουνίου 2016) και η τελευταία έκδοση του εν λόγω εγγράφου χρονολογείται τον Ιούνιο του 2016.
4. Η εταιρεία ….. δεν ενημέρωσε την ΑΔΑΕ για τα περιστατικά ασφάλειας που περιγράφονται στα υπ' αριθμ. πρωτ. ΑΔΑΕ ΕΜΠ 186/25.11.2015, ΑΔΑΕ ΕΜΠ 187/25.11.2015 και ΑΔΑΕ ΕΜΠ 188/25.11.2015 έγγραφα της εταιρείας …….. Πλην όμως, στην ενότητα «Διαχείριση Περιστατικών Ασφάλειας (σελ.20) της Πολιτικής ασφάλειας της εταιρείας (παρ. 9.2.3., Απόφαση 165/2011), αναφέρεται ότι *«…σε περίπτωση περιστατικού ασφάλειας που θα υποπέσει στην αντίληψή της, η εταιρεία ενημερώνει την ΑΔΑΕ, υποβάλλοντας για κάθε περιστατικό, έγγραφο με τίτλο «Έκθεση Άμεσης Αναφοράς Περιστατικού Ασφάλειας», αναφέροντας τις διαθέσιμες που*

περιγράφουν το περιστατικό πληροφορίες σύμφωνα με τα δεδομένα που είναι διαθέσιμα κατά το χρόνο πραγματοποίησης της ενημέρωσης…».

5. Ως προς την ανάλυση των περιστατικών που περιγράφονται στα υπ΄αριθμ. πρωτ. ΑΔΑΕ ΕΜΠ 187/25.11.2015 και ΑΔΑΕ ΕΜΠ 188/25.11.2015 έγγραφα της εταιρείας ……, η εταιρεία ……. δήλωσε, στο πλαίσιο του από 27.06.2016 επιτόπιου ελέγχου, ότι τα περιστατικά προέκυψαν εξαιτίας του ……. Από τη μελέτη των ως άνω συνημμένων προκύπτουν τα ακόλουθα για τη χρονική εξέλιξη των ως άνω περιστατικών ασφάλειας:

17.09.2015:

- Πραγματοποιείται ενημέρωση από τη ……. προς την …… για την επίθεση phising που περιγράφεται στο υπ΄αριθμ. πρωτ. ΑΔΑΕ ΕΜΠ 187/25.11.2015 έγγραφο (συνημμένο 4 του Πρακτικού της 27ης Ιουνίου 2016).
- Πραγματοποιείται ενημέρωση από την …….. προς την εταιρεία …… για το περιστατικό και παροχή συμβουλών ασφάλειας (συνημμένο 3 του Πρακτικού της 27ης Ιουνίου 2016).
- Γίνεται προσωρινή απενεργοποίηση του domain.

21.09.2015:

- Πραγματοποιείται ενημέρωση από την …….. προς την εταιρεία …….. για αναβάθμιση του …… (συνημμένο 3 του Πρακτικού της 27ης Ιουνίου 2016).
- Η ……. ενεργοποιεί εκ νέου το domain (συνημμένο 3 του Πρακτικού της 27ης Ιουνίου 2016).

27.09.2015:

- Πραγματοποιείται ενημέρωση από τη …… προς την …… για την επίθεση phising που περιγράφεται στο υπ΄αριθμ. πρωτ. ΑΔΑΕ ΕΜΠ 188/25.11.2015 έγγραφο (συνημμένο 4 του Πρακτικού της 27ης Ιουνίου 2016)

28.09.2015:

- Πραγματοποιείται ενημέρωση από την ……. προς την εταιρεία …….. για το δεύτερο περιστατικό (συνημμένο 3 του Πρακτικού της 27ης Ιουνίου 2016).
- Γίνεται εκ νέου απενεργοποίηση του domain

04.10.2015:

- Τα phising αρχεία διαγράφονται από το site της …….. από την ……., έπειτα από σχετικό αίτημα της πρώτης προς την δεύτερη.

- Το site ενεργοποιείται εκ νέου από ……. (συνημμένο 3 του Πρακτικού της 27ης Ιουνίου 2016).

Από τη διερεύνηση του αρχείου ……. που απέστειλε η ……. με την υπ΄αριθμ. πρωτ. ΑΔΑΕ 1517/07.07.2016 επιστολή και περιέχει το plesk action log του υπό εξέταση server που εξυπηρετούσε την περίοδο εκείνη τους ιστοτόπους, στους οποίους αναφέρονται τα περιστατικά, δεν επαληθεύεται η απενεργοποίηση των ιστοτόπων στις 17.09.2015 και 28.09.2015, όπως αναφέρεται στις επικοινωνίες της …….. με τον πελάτη (συνημμένα 3, 4 του Πρακτικού της 27ης Ιουνίου 2016).

Από τη διερεύνηση του αρχείου ……. που απέστειλε η …….. με την υπ΄αριθμ. πρωτ. ΑΔΑΕ 2/02.01.2017278 επιστολή, το οποίο περιέχει, κατά δήλωση της, τα logs του server σε επίπεδο διαχειριστή (root πρόσβαση) για την περίοδο του Σεπτεμβρίου του 2015, δεν κατέστη δυνατή η σύνδεση των ενεργειών που έχουν καταγραφεί στο εν λόγω αρχείο με τα συγκεκριμένα περιστατικά.

6. Ως προς την ανάλυση του περιστατικού ασφάλειας που περιγράφεται στο υπ' αριθμ. πρωτ. ΑΔΑΕ ΕΜΠ 186/25.11.2015 έγγραφο της εταιρείας ……., η εταιρεία …….. δήλωσε, στο πλαίσιο του από 27.06.2016 επιτόπιου ελέγχου, ότι το εν λόγω περιστατικό οφειλόταν σε κακόβουλα αρχεία που προσέβαλαν …….. και παρέδωσε τη σχετική αλληλογραφία με την εταιρεία (συνημμένο 12 του Πρακτικού της 27ης Ιουνίου 2016). Από τη μελέτη του εν λόγω εγγράφου συνημμένων προκύπτουν τα ακόλουθα για τη χρονική εξέλιξη του περιστατικού ασφάλειας:

07.09.2015:

- Πραγματοποιείται ενημέρωση από την ….. προς την εταιρεία …….. για το περιστατικό.
- Γίνεται προσωρινή απενεργοποίηση του domain.

08.09.2015:

- Γίνεται ενεργοποίηση του domain.

Από τη διερεύνηση του αρχείου ….. που απέστειλε η ……. με την υπ΄αριθμ. πρωτ. ΑΔΑΕ 1517/07.07.2016 επιστολή, και περιέχει το plesk action log του υπό εξέταση server που εξυπηρετούσε την περίοδο εκείνη τον ιστότοπο, στον οποίο αναφέρεται το περιστατικό, δεν κατέστη δυνατή η διερεύνηση του, λόγω του ότι οι εγγραφές που περιέχονται στο εν λόγω αρχείο είναι μεταγενέστερες του συμβάντος (ξεκινούν από τις 26.09.2015, δηλαδή 18 ημέρες μετά την εκ νέου ενεργοποίηση του ιστοτόπου κατόπιν αντιμετώπισης του περιστατικού, στις 08.09.2015).

Από τη διερεύνηση του αρχείου …… που απέστειλε η …… με την υπ΄αριθμ. πρωτ. ΑΔΑΕ 2/02.01.2017, το οποίο περιέχει, κατά δήλωσή της τα αρχεία καταγραφής του

server σε επίπεδο διαχειριστή (root πρόσβαση) για την περίοδο του Σεπτεμβρίου του 2015 δεν κατέστη δυνατή η επιβεβαίωση της απενεργοποίησης του συγκεκριμένου ιστοτόπου, διότι οι ενέργειες του root δεν σχετίζονται με συγκεκριμένους ιστοτόπους.

7. Η εταιρεία με την υπ΄αριθμ. πρωτ. ΑΔΑΕ 1517/07.07.2016 επιστολή της ενημέρωσε την ΑΔΑΕ ότι δε διαθέτει αρχεία κίνησης (traffic logs) του web server που εξυπηρετεί την ……εφαρμογή για την περίπτωση του περιστατικού που αναφέρεται στο υπ' αριθμ. πρωτ. ΑΔΑΕ ΕΜΠ 186/25.11.2015 έγγραφο της εταιρείας ……., λόγω της μεταφοράς του server σε άλλο data center. Επίσης, με το υπ΄αριθμ. πρωτ. ΑΔΑΕ ΕΜΠ278/23.12.2016 έγγραφο, η εταιρεία …… δήλωσε ότι δεν διαθέτει αρχεία καταγραφής εκτέλεσης των …….. και αρχεία καταγραφής λαθών (Error logs) για τα υπό εξέταση περιστατικά ασφάλειας.

   Επίσης, για το περιστατικό ασφάλειας που περιγράφεται στο υπ' αριθμ. πρωτ. ΑΔΑΕ ΕΜΠ 186/25.11.2015 έγγραφο, η εταιρεία δεν διαθέτει αρχείο καταγραφών προσβάσεων και ενεργειών (access και command logs) του διαχειριστή (administrator) της …….. (και όχι των τελικών χρηστών/πελατών που διαχειρίζονται τον λογαριασμό τους και τις υπηρεσίες που χρησιμοποιούν μέσω του …….).

   Πλην όμως, στη σελ. 5 της Πολιτικής Ασφάλειας της εταιρείας (παρ. 3.2.8. & 3.2.9 Απόφασης 165/2011) αναφέρεται ότι *«… η εταιρεία διατηρεί τα εν λόγω αρχεία για χρονικό διάστημα δύο (2) ετών…»* και στη σελ. 6 ότι *«… η εταιρεία χρησιμοποιεί κατάλληλα εργαλεία λογισμικού και φροντίζει με τακτικούς ελέγχους να εξασφαλίζει ότι οι καταγραφές που προβλέπονται στο παρόν κείμενο είναι πλήρεις και συνεχείς»*. Επίσης, στην ενότητα με τίτλο «Λογική πρόσβαση σε ΠΕΣ», σελ 13 της Πολιτικής Ασφάλειας της εταιρείας (παρ. 6.2.5 Απόφασης 165/2011) αναφέρεται ότι *«Για κάθε πρόσβαση σε ΠΕΣ, η εταιρεία τηρεί αρχείο καταγραφής των χρηστών, στο οποίο καταγράφονται το όνομα χρήστη που απέκτησε την πρόσβαση και η ημερομηνία και ώρα εκκίνησης και τερματισμού της πρόσβασης».* Τέλος, στην ενότητα με τίτλο «Διαχείριση και εγκατάσταση ΠΕΣ», σελ. 18 της Πολιτικής Ασφάλειας της εταιρείας (παρ. 8.3.3.1 Απόφασης 165/2011), αναφέρεται ότι *«Η εταιρεία ακολουθεί Διαδικασία Ελέγχου Συντήρησης-Υποστήριξης-Λειτουργίας Υλικού και Λογισμικού των ΠΕΣ παρακολουθώντας την ορθή λειτουργία των ΠΕΣ μέσω του ελέγχου των συμβάντων και των ειδοποιήσεων κάθε συστήματος ώστε να εντοπίζονται τυχόν σφάλματα ή κενά ασφάλειας».*

   Επίσης, στην ενότητα με τίτλο «Διαχείριση Περιστατικών Ασφάλειας» της Πολιτικής Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών εταιρείας, η οποία παραδόθηκε στην Ο.Ε. στο πλαίσιο του από 27.06.2016 επιτόπιου ελέγχου (συνημμένο 1 του Πρακτικού της 27ης Ιουνίου 2016), αναφέρεται ότι *«…για κάθε περιστατικό*

ασφάλειας γίνεται καταγραφή των παρακάτω στοιχείων ... συλλεχθέντα στοιχεία από το υπόχρεο πρόσωπο για τη διερεύνηση του περιστατικού (ενδεικτικά, αρχεία καταγραφής, στοιχεία παραβίασης, κ.α.)».

8. Αναφορικά με τις ενεργοποιήσεις ή μη συγκεκριμένων χαρακτηριστικών ασφάλειας του συστήματος ……, στο πλαίσιο του από 27.06.2016 επιτόπιου ελέγχου, διαπιστώθηκαν τα ακόλουθα:

   - .....

Επισημαίνεται ότι στο πλαίσιο του από 27.06.2016 επιτόπιου ελέγχου, η Ο.Ε. ζήτησε από την εταιρεία να παραδώσει οποιοδήποτε στοιχείο αποδεικνύει την ενεργοποίηση των αυτόματων ενημερώσεων (ενεργοποίηση του χαρακτηριστικού ασφάλειας ……..) κατά την περίοδο που συνέβησαν τα υπό εξέταση περιστατικά. Πλην όμως, η …… δεν απέστειλε τα εν λόγω στοιχεία, ούτε και αντίστοιχη ενημέρωση προς την ΑΔΑΕ για την ενεργοποίηση ή μη των λοιπών χαρακτηριστικών ασφάλειας του …….. που εξετάστηκαν στο πλαίσιο του από 27.06.2016 επιτόπιου ελέγχου κατά την περίοδο που συνέβησαν τα υπό εξέταση περιστατικά. Επισημαίνεται ότι στην ενότητα «Διαχείριση και εγκατάσταση ΠΕΣ» (σελ. 18) της Πολιτικής Ασφάλειας για τη Διασφάλιση του απορρήτου των Επικοινωνιών της εταιρείας ……. (παρ. 8.2.2., 8.2.3., Απόφαση 165/2011), προβλέπεται ότι « … οι αλλαγές (εισαγωγή/μεταβολή/διαγραφή στο λογισμικό/υλικό των ΠΕΣ που σχετίζονται με τη διασφάλιση του απορρήτου των επικοινωνιών, πραγματοποιούνται χωρίς καθυστέρηση» και ότι «…για οποιαδήποτε αλλαγή υλικού ή λογισμικού ΠΕΣ, το υπόχρεο πρόσωπο υποχρεούται να διατηρεί αρχείο στο οποίο καταγράφεται η ημερομηνία, ο τρόπος, η αιτιολόγηση και ο εργαζόμενος ή συνεργάτης που πραγματοποίησε τις αλλαγές. Το αρχείο ενημερώνεται και διατηρείται από συγκεκριμένη διοικητική οντότητα ή εργαζόμενο του υπόχρεου προσώπου».

Δ. ΣΥΜΠΕΡΑΣΜΑΤΑ

Από τον επιτόπιο έλεγχο που πραγματοποιήθηκε στην εταιρεία ……. με διακριτικό τίτλο ……καθώς και από τα στοιχεία που απέστειλε η εταιρεία ……., προέκυψαν τα ευρήματα που αναλυτικά περιγράφονται στην ενότητα Γ της παρούσας Έκθεσης.

Επισημαίνεται, ότι η μη διατήρηση από πλευράς …….. των αρχείων κίνησης (traffic logs) του web server που εξυπηρετεί την …….. εφαρμογή, καταγραφής προσβάσεων και ενεργειών του διαχειριστή (administrator) της ……. (και όχι των τελικών χρηστών/πελατών που διαχειρίζονται τον λογαριασμό τους και τις υπηρεσίες που χρησιμοποιούν μέσω του ……..), των αρχείων καταγραφής εκτέλεσης των …… (Action logs) και των αρχείων καταγραφής λαθών (Error logs) που αναλυτικά περιγράφονται στα σημείο 7 της ενότητας Γ, έχει ως αποτέλεσμα να μην μπορεί να εξαχθεί ασφαλές συμπέρασμα αναφορικά με την ευθύνη του παρόχου ως προς τα υπό εξέταση περιστατικά.

Επισημαίνεται ότι, στο πλαίσιο του από 30.06.2015 επιτόπιου ελέγχου στις εγκαταστάσεις της εταιρείας …….. ο οποίος πραγματοποιήθηκε σε συνέχεια της υπ΄αριθμ. 77/2015 Απόφαση Ολομέλειας ΑΔΑΕ (Πρακτικό ελέγχου υπ΄αριθμ. πρωτ. ΑΔΑΕ ΕΜΠ 71/07.07.2015 η εταιρεία …… δήλωσε ότι *«…παρέχει στους πελάτες της την υπηρεσία ……. σύμφωνα με την οποία οι πελάτες λαμβάνουν εικονικούς εξυπηρετητές από την …… με συγκεκριμένη αρχική διαμόρφωση (λειτουργικό σύστημα, …… κλπ) και οι οποίοι στη συνέχεια έχουν την πλήρη ευθύνη για τη διαχείρισή τους. Η εταιρεία, αφού αρχικά διαμορφώσει τον εικονικό εξυπηρετητή μέσα από το management vlan, τον τοποθετεί σε ξεχωριστό vlan, το οποίο είναι διαφορετικό για κάθε πελάτη. Η εταιρεία παραδίδει στους πελάτες οδηγίες για τη χρήση του εικονικού εξυπηρετητή, καθώς και επιπλέον υπηρεσίες όπως Firewall, IPS. Η εταιρεία …… δεν έχει πρόσβαση στο vlan του κάθε πελάτη και δεν έχει πρόσβαση για διαχείριση στο συγκεκριμένο εξυπηρετητή και επομένως και στα αντίστοιχα αρχεία καταγραφής αυτού. Η εταιρεία …….. μπορεί μόνο να εκτελεί ενέργειες όπως restart, stop του συγκεκριμένου Virtual Machine(VM)».*

Β. Ενόψει των ανωτέρω αποτελεσμάτων της από 30.06.2017 «Έκθεσης Διενέργειας Εκτάκτου Ελέγχου στις εγκαταστάσεις της εταιρείας …… κατόπιν περιστατικών ασφάλειας με αριθμ. πρωτ. ΕΜΠ187/25.11.2015, ΕΜΠ188/25.11.2015 και ΕΜΠ186/25.11.2015», αποδίδεται η ακόλουθη ενδεχόμενη παράβαση της κείμενης νομοθεσίας σε σχέση με το απόρρητο των επικοινωνιών εκ μέρους της εταιρείας «……»:

Παραβίαση της Πολιτικής Ασφάλειας για τη διασφάλιση του Απορρήτου των επικοινωνιών εκ μέρους της εταιρείας «……..» και συνακόλουθα της υπ' αριθμ. 165/2011 Απόφασης της Α.Δ.Α.Ε. (Κανονισμός για τη Διασφάλιση του Απορρήτου των Ηλεκτρονικών Επικοινωνιών)

α) Όπως αναφέρεται στη σελ. 8-9 της από 30.06.2017 «Έκθεσης Διενέργειας Εκτάκτου Ελέγχου στις εγκαταστάσεις της εταιρείας ……. κατόπιν περιστατικών ασφάλειας με αριθμ. πρωτ. ΕΜΠ187/25.11.2015, ΕΜΠ188/25.11.2015 και ΕΜΠ186/25.11.2015», η εταιρεία «…….» δεν ενημέρωσε την Αρχή για τα εν θέματι περιστατικά ασφαλείας. Πλην όμως, στην ενότητα «Διαχείριση Περιστατικών Ασφάλειας (σελ.20) της Πολιτικής ασφάλειας της εταιρείας αναφέρεται ότι *«…σε περίπτωση περιστατικού ασφάλειας που θα υποπέσει στην αντίληψή της, η εταιρεία ενημερώνει την ΑΔΑΕ, υποβάλλοντας για κάθε περιστατικό, έγγραφο με τίτλο «Έκθεση Άμεσης Αναφοράς Περιστατικού Ασφάλειας», αναφέροντας τις διαθέσιμες που περιγράφουν το περιστατικό πληροφορίες σύμφωνα με τα δεδομένα που είναι διαθέσιμα κατά το χρόνο πραγματοποίησης της ενημέρωσης…»*, όπως άλλωστε προβλέπεται στην παρ. 9.2.3 της υπ' αριθμ. 165/2011 Απόφασης της Αρχής.

β) Όπως αναφέρεται στη σελ. 12 της από 30.06.2017 «Έκθεσης Διενέργειας Εκτάκτου Ελέγχου στις εγκαταστάσεις της εταιρείας …….. κατόπιν περιστατικών ασφάλειας με αριθμ. πρωτ. ΕΜΠ187/25.11.2015, ΕΜΠ188/25.11.2015 και ΕΜΠ186/25.11.2015», η εταιρεία «……..» *«…δε διαθέτει αρχεία κίνησης (traffic logs) του web server που εξυπηρετεί την ……εφαρμογή για την περίπτωση του περιστατικού που αναφέρεται στο υπ' αριθμ. πρωτ. ΑΔΑΕ ΕΜΠ 186/25.11.2015 έγγραφο της εταιρείας ……. λόγω της μεταφοράς του server σε άλλο data center….»*. Πλην όμως, στη σελ. 5 της Πολιτικής Ασφάλειας της εταιρείας (παρ. 3.2.8. & 3.2.9 Απόφασης 165/2011) αναφέρεται ότι *«… η εταιρεία διατηρεί τα εν λόγω αρχεία για χρονικό διάστημα δύο (2) ετών…»* και στη σελ. 6 ότι *«… η εταιρεία χρησιμοποιεί κατάλληλα εργαλεία λογισμικού και φροντίζει με τακτικούς ελέγχους να εξασφαλίζει ότι οι καταγραφές που προβλέπονται στο παρόν κείμενο είναι πλήρεις και συνεχείς»*, όπως προβλέπεται, άλλωστε, και στις παρ. 3.2.8 και 3.2.9 της υπ' αριθμ. 165/2011 Απόφασης της Αρχής.

γ) Επίσης, όπως αναφέρεται στη σελ. 12 της από 30.06.2017 «Έκθεσης Διενέργειας Εκτάκτου Ελέγχου στις εγκαταστάσεις της εταιρείας …….. κατόπιν περιστατικών ασφάλειας με αριθμ. πρωτ. ΕΜΠ187/25.11.2015, ΕΜΠ188/25.11.2015 και ΕΜΠ186/25.11.2015», η εταιρεία «…….» *«…δεν διαθέτει αρχεία καταγραφής εκτέλεσης των …… και αρχεία καταγραφής λαθών (Error logs) για τα υπό εξέταση περιστατικά ασφάλειας….»*. Πλην όμως, στην ενότητα με τίτλο «Διαχείριση και εγκατάσταση ΠΕΣ», σελ. 18 της Πολιτικής Ασφάλειας της εταιρείας (παρ. 8.3.3.1 Απόφασης 165/2011), αναφέρεται ότι *«Η εταιρεία ακολουθεί Διαδικασία Ελέγχου Συντήρησης-Υποστήριξης-Λειτουργίας Υλικού και Λογισμικού των ΠΕΣ παρακολουθώντας την ορθή λειτουργία των ΠΕΣ μέσω του ελέγχου των συμβάντων και των ειδοποιήσεων κάθε συστήματος ώστε να εντοπίζονται τυχόν σφάλματα ή κενά ασφάλειας»,* όπως ορίζεται και στην παρ. 8.3.3.1 της υπ' αριθμ. 165/2011 Απόφασης της Αρχής, ενώ, στην ενότητα με τίτλο «Διαχείριση Περιστατικών Ασφάλειας» της Πολιτικής Ασφάλειας της εταιρείας, αναφέρεται ότι *«…για κάθε περιστατικό ασφάλειας γίνεται καταγραφή των παρακάτω στοιχείων … συλλεχθέντα στοιχεία από το υπόχρεο πρόσωπο για τη διερεύνηση του περιστατικού (ενδεικτικά, αρχεία καταγραφής, στοιχεία παραβίασης, κ.α.)»*.

δ) Περαιτέρω, όπως αναφέρεται, επίσης, στη σελ. 12 της από 30.06.2017 «Έκθεσης Διενέργειας Εκτάκτου Ελέγχου στις εγκαταστάσεις της εταιρείας …… κατόπιν περιστατικών ασφάλειας με αριθμ. πρωτ. ΕΜΠ187/25.11.2015, ΕΜΠ188/25.11.2015 και ΕΜΠ186/25.11.2015», η εταιρεία «……» *«…δεν διαθέτει αρχείο καταγραφών προσβάσεων και ενεργειών (access και command logs) του διαχειριστή (administrator) της …… (και όχι των τελικών χρηστών/πελατών που διαχειρίζονται τον λογαριασμό τους και τις υπηρεσίες που χρησιμοποιούν μέσω του ……..»*. Πλην

όμως, στην ενότητα με τίτλο «Λογική πρόσβαση σε ΠΕΣ», σελ 13 της Πολιτικής Ασφάλειας της εταιρείας αναφέρεται ότι «*για κάθε πρόσβαση σε ΠΕΣ, η εταιρεία τηρεί αρχείο καταγραφής των χρηστών, στο οποίο καταγράφονται το όνομα χρήστη που απέκτησε την πρόσβαση και η ημερομηνία και ώρα εκκίνησης και τερματισμού της πρόσβασης*», όπως προβλέπεται στην παρ. 6.2.5 της υπ' αριθμ. 165/2011 Απόφασης της Αρχής.

ε) Τέλος, όπως αναφέρεται στη σελ. 14 της από 30.06.2017 «Έκθεσης Διενέργειας Εκτάκτου Ελέγχου στις εγκαταστάσεις της εταιρείας ……. κατόπιν περιστατικών ασφάλειας με αριθμ. πρωτ. ΕΜΠ187/25.11.2015, ΕΜΠ188/25.11.2015 και ΕΜΠ186/25.11.2015», η Α.Δ.Α.Ε. ζήτησε από την εταιρεία «……» να παραδώσει οποιοδήποτε στοιχείο αποδεικνύει την ενεργοποίηση των αυτόματων ενημερώσεων (ενεργοποίηση του χαρακτηριστικού ασφάλειας "……..") κατά την περίοδο που συνέβησαν τα υπό εξέταση περιστατικά. Πλην όμως, η εταιρεία δεν απέστειλε τα εν λόγω στοιχεία, ούτε και αντίστοιχη ενημέρωση προς την Α.Δ.Α.Ε. για την ενεργοποίηση ή μη των λοιπών χαρακτηριστικών ασφάλειας του ……που εξετάστηκαν στο πλαίσιο του από 27.06.2016 επιτόπιου ελέγχου κατά την περίοδο που συνέβησαν τα υπό εξέταση περιστατικά. Πλην όμως, στην ενότητα «Διαχείριση και εγκατάσταση ΠΕΣ» (σελ. 18) της Πολιτικής Ασφάλειας για τη Διασφάλιση του απορρήτου των Επικοινωνιών της εταιρείας προβλέπεται ότι *«…οι αλλαγές (εισαγωγή/μεταβολή/διαγραφή στο λογισμικό/υλικό των ΠΕΣ που σχετίζονται με τη διασφάλιση του απορρήτου των επικοινωνιών, πραγματοποιούνται χωρίς καθυστέρηση»* και ότι *«…για οποιαδήποτε αλλαγή υλικού ή λογισμικού ΠΕΣ, το υπόχρεο πρόσωπο υποχρεούται να διατηρεί αρχείο στο οποίο καταγράφεται η ημερομηνία, ο τρόπος, η αιτιολόγηση και ο εργαζόμενος ή συνεργάτης που πραγματοποίησε τις αλλαγές. Το αρχείο ενημερώνεται και διατηρείται από συγκεκριμένη διοικητική οντότητα ή εργαζόμενο του υπόχρεου προσώπου»*, όπως, άλλωστε, ορίζεται στις παρ. 8.2.3 και 8.2.3. της υπ' αριθμ. 165/2011 Απόφασης της Αρχής.

Γ. Ενόψει των ανωτέρω και έχοντας υπόψη:

1. Το άρθρο 19 του Συντάγματος,
2. Τις διατάξεις του Ν.3115/2003 «Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών» (ΦΕΚ Α' 47) και ιδίως τα άρθρα 1 παρ. 1, 6 και 11 αυτού,
3. Τις διατάξεις του ν. 3674/2008 «Ενίσχυση του θεσμικού πλαισίου διασφάλισης του απορρήτου της τηλεφωνικής επικοινωνίας και άλλες διατάξεις» (ΦΕΚ Α' 136),
4. Τις διατάξεις της υπ' αριθμ. 165/2011 Απόφασης της Α.Δ.Α.Ε. «Κανονισμός για τη Διασφάλιση

του Απορρήτου των Ηλεκτρονικών Επικοινωνιών» (ΦΕΚ Β' 2715/2011),

5. Τις διατάξεις του Ν.3051/2002 «Συνταγματικά κατοχυρωμένες ανεξάρτητες αρχές, τροποποίηση και συμπλήρωση του συστήματος προσλήψεων στο δημόσιο τομέα και συναφείς ρυθμίσεις» (ΦΕΚ Α' 220/2002), όπως ισχύει,

6. Τις διατάξεις του Ν. 4055/2012 «Δίκαιη δίκη και εύλογη διάρκεια αυτής» (ΦΕΚ Α'51/2012), όπως ισχύει, και ιδίως τα άρθρα 61 και 110 παρ. 12 αυτού,

7. Την υπ' αριθμ. 97^{Α}/2012 Απόφαση της Α.Δ.Α.Ε. «Τροποποίηση της απόφασης της ΑΔΑΕ 44/31-10-2003 Απόφασης της ΑΔΑΕ "Κανονισμός Εσωτερικής Λειτουργίας της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (Α.Δ.Α.Ε.) (ΦΕΚ1642/Β/7.11.2003)", όπως ισχύει» (ΦΕΚ 1650/Β/11-05-2012 και 1751/Β/25-05-2012),

8. Τις διατάξεις της υπ'αριθμ. 44/31.10.2003 Απόφασης της Α.Δ.Α.Ε. «Κανονισμός Εσωτερικής Λειτουργίας της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (Α.Δ.Α.Ε.)» (ΦΕΚ Β' 1642/7.11.2003), όπως ισχύει,

9. Το άρθρο 20 παρ. 2 του Συντάγματος, περί δικαιώματος προηγούμενης ακρόασης του διοικουμένου,

10. Τη διάταξη του άρθρου 26 παρ.7 του ν.4325/2015 «Εκδημοκρατισμός της Διοίκησης – Καταπολέμηση Γραφειοκρατίας και Ηλεκτρονική Διακυβέρνηση. Αποκατάσταση Αδικιών και άλλες διατάξεις» (ΦΕΚ Α' 47/2015),

11. Τη διάταξη του άρθρου 55 παρ.10 του ν.4339/2015 (ΦΕΚ Α' 133/2015) «Αδειοδότηση παρόχων περιεχομένου επίγειας ψηφιακής τηλεοπτικής ευρυεκπομπής ελεύθερης λήψης - Ίδρυση συνδεδεμένης με την Ε.Ρ.Τ. Α.Ε. ανώνυμης εταιρίας για την ανάπτυξη δικτύου επίγειας ψηφιακής ευρυεκπομπής - Ρύθμιση θεμάτων Εθνικής Επιτροπής Τηλεπικοινωνιών και Ταχυδρομείων (Ε.Ε.Τ.Τ.) - Εθνική Επικοινωνιακή Πολιτική, Οργάνωση της Επικοινωνιακής Διπλωματίας - Σύσταση Εθνικού Κέντρου Οπτικοακουστικών Μέσων και Επικοινωνίας και Μητρώου Επιχειρήσεων Ηλεκτρονικών Μέσων Ενημέρωσης - Τροποποίηση διατάξεων του Ν. 4070/2012 (Α' 82) και άλλες διατάξεις»,

12. Τη διάταξη του άρθρου 73 του ν. 4369/2016 (ΦΕΚ Α΄ 33/2016) «Εθνικό Μητρώο Επιτελικών Στελεχών Δημόσιας Διοίκησης, βαθμολογική διάρθρωση θέσεων, συστήματα αξιολόγησης, προαγωγών και επιλογής προϊσταμένων (διαφάνεια – αξιοκρατία και αποτελεσματικότητα της Δημόσιας Διοίκησης) και άλλες διατάξεις»,

13. Την υπ' αριθμ. 16887/17-03-2016 Απόφαση του Υπουργού Δικαιοσύνης, Διαφάνειας και Ανθρωπίνων Δικαιωμάτων (ΦΕΚ Υ.Ο.Δ.Δ. 151/21-03-2016), περί συγκρότησης της Αρχής

Διασφάλισης του Απορρήτου των Επικοινωνιών,

14. Τις διατάξεις του άρθρου εικοστού τρίτου του Ν. 4411/2016 (ΦΕΚ Α΄ 142/03-08-2016),

15. Τις υπ' αριθμ. 3319/2010 και 1361/2013 αποφάσεις του Συμβουλίου της Επικρατείας,

16. Την «Έκθεση Αναφοράς Περιστατικού Ασφαλείας» με αριθμό πρωτόκολλου ΕΜΠ186/25.11.2015,

17. Την «Έκθεση Αναφοράς Περιστατικού Ασφαλείας» με αριθμό πρωτόκολλου ΕΜΠ187/25.11.2015,

18. Την «Έκθεση Αναφοράς Περιστατικού Ασφαλείας» με αριθμό πρωτόκολλου ΕΜΠ188/25.11.2015,

19. Την υπ΄αριθμ. 134/2016 Απόφαση της Ολομέλειας της Α.Δ.Α.Ε.,

20. Την υπ΄αριθμ. 155/2016 Απόφαση του Προέδρου της Α.Δ.Α.Ε.,

21. Το υπ΄ αριθμ. πρωτ. ΑΔΑΕ ΕΜΠ 124/30.06.2016 Πρακτικό διενέργειας επιτόπιου ελέγχου στις εγκαταστάσεις της εταιρείας «…….»,

22. την υπ' αριθμ. πρωτ. ΑΔΑΕ 1517/07.07.2016 επιστολή της εταιρείας «……»,

23. την υπ' αριθμ. πρωτ. ΑΔΑΕ 2427/18.10.2016 επιστολή της εταιρείας «…….»,

24. την υπ΄ αριθμ. πρωτ. ΑΔΑΕ ΕΜΠ227/14.11.2016 επιστολή της Α.Δ.Α.Ε.,

25. την υπ' αριθμ. πρωτ. ΑΔΑΕ ΕΜΠ278/23.12.2016 επιστολή της εταιρείας «……..»,

26. την υπ' αριθμ. πρωτ. ΑΔΑΕ 3213/28.12.2016 επιστολή της εταιρείας «……..»,

27. την υπ' αριθμ. πρωτ. ΑΔΑΕ 2/02.01.2017 επιστολή της εταιρείας «……..»,

28. την υπ΄ αριθμ. πρωτ. ΑΔΑΕ ΕΜΠ12/03.02.2017 επιστολή της Α.Δ.Α.Ε. προς την Ε.Ε.Τ.Τ.,

29. την υπ' αριθμ. πρωτ. ΑΔΑΕ 1822/15.06.2017 επιστολή της Ε.Ε.Τ.Τ.,

30. το αριθμ. πρωτ. ΑΔΑΕ ΕΜΠ 71/07.07.2015 Πρακτικό επιτόπιου ελέγχου στην εταιρεία ……,

31. την από 30.06.2017 «Έκθεση Διενέργειας Εκτάκτου Ελέγχου στις εγκαταστάσεις της εταιρείας …….. κατόπιν περιστατικών ασφάλειας με αριθμ. πρωτ. ΕΜΠ187/25.11.2015, ΕΜΠ188/25.11.2015 και ΕΜΠ186/25.11.2015»,

32. Την υπ' αριθμ. 340/2017 εισήγηση προς την Ολομέλεια της Α.Δ.Α.Ε.,

33. Το Πρακτικό της από 27 Σεπτεμβρίου 2017 συνεδρίασης της Ολομέλειας της Α.Δ.Α.Ε.,

34. Την υπ' αριθμ. 295/2017 Απόφαση της Α.Δ.Α.Ε. περί έγκρισης της από 30.06.2017 «Έκθεσης Διενέργειας Εκτάκτου Ελέγχου στις εγκαταστάσεις της εταιρείας …….. κατόπιν περιστατικών ασφάλειας με αριθμ. πρωτ. ΕΜΠ187/25.11.2015, ΕΜΠ188/25.11.2015 και ΕΜΠ186/25.11.2015», η οποία επιδόθηκε στην εταιρεία «……..» μετά της συνημμένης έκθεσης ελέγχου, όπως προκύπτει από την υπ' αριθμ. 3086Β/24-11-2017 έκθεση επίδοσης της δικαστικής επιμελήτριας στο Εφετείο ……,

35. Την υπ' αριθμ. πρωτ. ΑΔΑΕ 182/05-10-2017 επιστολή προς την Ε.Ε.Τ.Τ.,

36. Την υπ' αριθμ. 209/2018 εισήγηση προς την Ολομέλεια της Α.Δ.Α.Ε.,

37. Το πρακτικό της από 4 Ιουλίου 2018 συνεδρίασης της Ολομέλειας της Α.Δ.Α.Ε.,

38. Την ανάγκη διασφάλισης του απορρήτου των επικοινωνιών,

Η ΑΡΧΗ ΔΙΑΣΦΑΛΙΣΗΣ ΤΟΥ ΑΠΟΡΡΗΤΟΥ ΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ (ΑΔΑΕ)
ΑΠΟΦΑΣΙΖΕΙ

την κλήση σε Ακρόαση της εταιρείας «……..», ενώπιον της Ολομέλειας της Α.Δ.Α.Ε., την **12η Δεκεμβρίου 2018, ημέρα Τετάρτη και ώρα 13.00 μ.μ.**, στην έδρα της Α.Δ.Α.Ε., Ιερού Λόχου 3, Μαρούσι, με αντικείμενο τον έλεγχο της ενδεχόμενης παράβασης της κείμενης νομοθεσίας περί απορρήτου των επικοινωνιών, όπως αναλυτικά εκτίθεται ανωτέρω στα σημεία Α, Β και Γ της παρούσας.

Εισηγητής για την εν λόγω υπόθεση ορίζεται το αναπληρωματικό μέλος της Α.Δ.Α.Ε., κ. Γεώργιος Μισαηλίδης.

Η παρούσα απόφαση να επιδοθεί στην εταιρεία «…….» με Δικαστικό Επιμελητή.

Κρίθηκε και αποφασίστηκε την 4η Ιουλίου 2018.

Ο Πρόεδρος

Χρήστος Ζαμπίρας