Μαρούσι, 8 Ιουνίου 2018
Αρ. πρωτ.: 1876
ΑΝΑΡΤΗΤΕΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

ΑΠΟΦΑΣΗ

(αριθμ: 356/2017)

Θέμα: Κλήση σε ακρόαση της εταιρείας με την επωνυμία «……...» με αντικείμενο τον έλεγχο ενδεχόμενης παραβάσεως της υπ' αριθμ. 165/2011 «Κανονισμός για τη Διασφάλιση του Απορρήτου των Ηλεκτρονικών Επικοινωνιών» (ΦΕΚ Β΄ 2715/17-11-2011) Απόφασης της Α.Δ.Α.Ε., σύμφωνα με τις αποκλίσεις που προσδιορίζονται στην εγκεκριμένη με την υπ' αριθμ. 162/2013 Απόφαση της Α.Δ.Α.Ε. Πολιτική Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών, όπως αυτές αναφέρονται στην από 10-03-2017 Έκθεση Διενέργειας Τακτικού Ελέγχου στην εταιρεία «…….», αναφορικά με την εφαρμογή της Πολιτικής Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών.

Την Τετάρτη, 22^{α} Νοεμβρίου 2017, η Ολομέλεια της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών, παρισταμένων του Προέδρου, κ. Χρήστου Ζαμπίρα, του Αντιπροέδρου κ. Μιχαήλ Σακκά, των τακτικών μελών κ.κ. Μιχαήλ Γεωργιακόδη, Γεωργίου Μπακάλη, Αικατερίνης Παπανικολάου και Παναγιώτη Ριζομυλιώτη, καθώς και του αναπληρωματικού μέλους κου Δημοσθένη Βουγιούκα, ο οποίος παρέστη 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 την επωνυμία «……...», με αντικείμενο τον έλεγχο της ενδεχόμενης παραβάσεως της υπ' αριθμ. 165/2011 Απόφασης της Α.Δ.Α.Ε. «Κανονισμός για τη Διασφάλιση του Απορρήτου των Ηλεκτρονικών Επικοινωνιών» (ΦΕΚ Β΄2715/17-11-2011) (εφεξής «Κανονισμός»), σχετικά με τις αποκλίσεις από την εγκεκριμένη με την υπ' αριθμ. 162/2013 απόφαση της Α.Δ.Α.Ε. Πολιτική Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών της εταιρείας, όπως αυτές αναφέρονται στην από 10 Μαρτίου 2017 Έκθεση Διενέργειας τακτικού Ελέγχου στην εν λόγω εταιρεία, αναφορικά με την εφαρμογή της Πολιτικής διασφάλισης του απορρήτου των επικοινωνιών. Τα μέλη της Ολομέλειας δήλωσαν ότι ενημερώθηκαν για τη μέχρι σήμερα εξέλιξη της υπόθεσης και ότι έλαβαν πλήρη γνώση αυτής.

Ειδικότερα:

Α. Με βάση την ως άνω από 10-03-2017 Έκθεση Διενέργειας Τακτικού Ελέγχου στις εγκαταστάσεις της εταιρείας «……..» αναφορικά με την εφαρμογή της Πολιτικής Ασφάλειας για τη διασφάλιση του απορρήτου των επικοινωνιών της εταιρείας και την τήρηση του Κανονισμού για τη Διασφάλιση του Απορρήτου των Ηλεκτρονικών Επικοινωνιών, όπως αυτή εγκρίθηκε από την Ολομέλεια της Α.Δ.Α.Ε. κατά τη συνεδρίαση της 5ης Απριλίου 2017, τα αποτελέσματα του εν λόγω τακτικού ελέγχου που διενεργήθηκε, όπως αυτά έχουν αποτυπωθεί στο κεφάλαιο Γ. της έκθεσης, έχουν ως εξής :

«Γ. ΕΞΕΤΑΣΗ ΣΤΟΙΧΕΙΩΝ – ΑΠΟΤΕΛΕΣΜΑΤΑ ΤΟΥ ΕΛΕΓΧΟΥ

Η Ο.Ε. εξέτασε τα έγγραφα και τα αρχεία που παρέδωσε η εταιρεία κατά τη διάρκεια των τριών (3) επιτόπιων ελέγχων (Πρακτικά Διενέργειας Επιτόπιων Ελέγχων με αρ. πρωτ. ΑΔΑΕ ΕΜΠ212/24.10.2016, ΕΜΠ249/05.12.2016 και ΕΜΠ262/12.12.2016, καθώς και τα στοιχεία που κατέθεσε η εταιρεία με τα με αριθμ. πρωτ. ΑΔΑΕ ΕΜΠ222/04.11.2016 και αριθμ. πρωτ. ΑΔΑΕ 3196/27.12.2016 έγγραφα, σε συνάρτηση με την υπ'αριθμ. πρωτ. ΑΔΑΕ ΕΜΠ145/17.05.2012 Πολιτική Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών της εταιρείας, όπως αναθεωρήθηκε με το με αριθμ.πρωτ. ΑΔΑΕ ΕΜΠ33/7.03.2013 έγγραφο και εγκρίθηκε με την υπ'αριθμ.162/2013 Απόφαση της ΑΔΑΕ.
Πιο συγκεκριμένα, προέκυψαν τα ακόλουθα:

1. Συμμόρφωση με τις παρατηρήσεις, οι οποίες αναφέρονται στην από 09.04.2013 Έκθεση Ελέγχου Συμμόρφωσης Πολιτικής, όπως εγκρίθηκε με την υπ' αριθμ. 162/2013 Απόφαση της ΑΔΑΕ.

1.1 Στο πλαίσιο του από 21.10.2016 επιτόπιου ελέγχου, η εταιρεία παρέδωσε την αναθεωρημένη έκδοση της Πολιτικής Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών της εταιρείας (συνημμένο 1 του Πρακτικού της 21ης Οκτωβρίου 2016), η οποία, σύμφωνα την εταιρεία, περιλαμβάνει την υλοποίηση των παρατηρήσεων της ΑΔΑΕ, οι οποίες αναφέρονται στην από 09.04.2013 Έκθεση Ελέγχου Συμμόρφωσης Πολιτικής, όπως εγκρίθηκε με την υπ' αριθμ. 162/2013 Απόφαση της ΑΔΑΕ.
Από τη μελέτη της ως άνω αναθεωρημένης έκδοσης της Πολιτικής Ασφάλειας της εταιρείας, η Ο.Ε. διαπίστωσε ότι η εταιρεία έχει συμμορφωθεί με το σύνολο των παρατηρήσεων της από 09.04.2013 Έκθεσης Ελέγχου Συμμόρφωσης Πολιτικής.

2. Γενικές Παρατηρήσεις ως προς την εφαρμογή της Πολιτικής Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών της εταιρείας (Κεφάλαιο 1 – Εισαγωγή της Πολιτικής Ασφάλειας της εταιρείας, σελ. 9-11 - Άρθρο 3 της Απόφασης 165/2011, ΦΕΚ 2715/Β/17.11.2011)

2.1 Στο πλαίσιο του από 21.10.2016 επιτόπιου ελέγχου, η εταιρεία παρέδωσε στη ΑΔΑΕ έγγραφο (συνημμένο 2 του Πρακτικού της 21ης Οκτωβρίου 2016) που περιλαμβάνει, σύμφωνα με την εταιρεία, την αποτίμηση κινδύνων της εταιρείας.

Παρατήρηση 1: Διαπιστώνεται ότι το έγγραφο που παρέδωσε η εταιρεία στην ΑΔΑΕ, περιλαμβάνει έναν κατάλογο κινδύνων ανά σύστημα της εταιρείας, καθώς και το υπολογισμένο επίπεδο ρίσκου με βάση την αντίστοιχη πιθανότητα εμφάνισης της εκάστοτε απειλής και της επίπτωσής της στην εταιρεία. Πλην όμως, δεν είναι ξεκάθαρο εάν η ως άνω βαθμολόγηση έχει πραγματοποιηθεί με κριτήριο τη διασφάλιση του απορρήτου της επικοινωνίας. Για παράδειγμα, η απειλή με τίτλο «*Μη εξουσιοδοτημένη πρόσβαση στον ηλεκτρονικό φάκελο με τις συμβάσεις του προσωπικού*» έχει βαθμολογηθεί με τον μέγιστο βαθμό ρίσκου 4. Πλην όμως, ο κίνδυνος *«Billing Server - Μη εξουσιοδοτημένη πρόσβαση»* έχει βαθμολογηθεί με τον βαθμό ρίσκου 3, και ο κίνδυνος *«Αντιγραφή κάρτας πρόσβασης από μη εξουσιοδοτημένο προσωπικό»* έχει βαθμολογηθεί με τον ελάχιστο βαθμό ρίσκου 1. Είναι προφανές, δε, ότι και οι δύο τελευταίες απειλές, αν εκδηλωθούν, μπορούν να έχουν σοβαρή επίπτωση στο απόρρητο των επικοινωνιών.

Επομένως, η εταιρεία οφείλει να αξιολογήσει εκ νέου την αποτίμηση κινδύνων με γνώμονα τη διασφάλιση του απορρήτου των επικοινωνιών. Επίσης, οφείλει να καταγράψει τους κινδύνους και τις απειλές για τα οποία σχεδιάζει να εφαρμόσει τις διορθωτικές της ενέργειες.

2.2 Στο πλαίσιο του από 21.10.2016 επιτόπιου ελέγχου, η Ο.Ε. ζήτησε από την εταιρεία να της παραδώσει το «Ειδικό Σχέδιο Αρχείων Καταγραφής».

Σε συνέχεια του επιτόπιου ελέγχου, η εταιρεία απέστειλε το υπ΄αριθμ. πρωτ. ΑΔΑΕ ΕΜΠ222/04.11.2016 έγγραφο, στο οποίο περιλαμβάνεται το «Ειδικό Σχέδιο Αρχείων Καταγραφής» της εταιρείας. Διαπιστώνεται ότι το εν λόγω έγγραφο περιλαμβάνει την αρχιτεκτονική και τις επιμέρους μεθόδους δημιουργίας, συλλογής, αποθήκευσης και διαχείρισης των αρχείων καταγραφής, καθώς και περιγραφή του περιεχομένου αυτών.

Απόκλιση 1: Πλην όμως, το «Ειδικό Σχέδιο Αρχείων Καταγραφής» της εταιρείας δε περιλαμβάνει τα μέτρα για τη διασφάλιση της ακεραιότητας, της εμπιστευτικότητας και της διαθεσιμότητάς των αρχείων καταγραφής, το οποίο προβλέπεται στην Ενότητα «Εισαγωγή» της πολιτικής ασφάλειας της εταιρείας, σελίδα 10 αυτής (παρ. 3.2.9. της Απόφασης 165/2011).

2.3 Στο πλαίσιο του από 21.10.2016 επιτόπιου ελέγχου, η Ο.Ε. ζήτησε από την εταιρεία να την ενημερώσει αναφορικά με τις αδυναμίες συμμόρφωσής της με τις απαιτήσεις του Κανονισμού, όπως αυτές προβλέπονται στην παρ. 9.18 της Πολιτικής Ασφάλειας της εταιρείας (παρ. 3.2.3, Άρθρου 3 της Απόφασης 165/2011). Σε συνέχεια του επιτόπιου ελέγχου, η εταιρεία απέστειλε το υπ΄αριθμ. πρωτ. ΑΔΑΕ ΕΜΠ222/04.11.2016 έγγραφο που περιλαμβάνει, σύμφωνα με την εταιρεία, την καταγραφή των αδυναμιών συμμόρφωσης (Σχετικό 1 αυτού υπό τον τίτλο «ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ-ΕΞΑΙΡΕΣΕΙΣ»).

Διαπιστώνεται ότι το έγγραφο που παρέδωσε η εταιρεία στην ΑΔΑΕ, περιέχει τέσσερις (4) αδυναμίες συμμόρφωσης με τις απαιτήσεις του Κανονισμού. Πιο αναλυτικά αναφέρεται ότι: 1) δεν έχουν πραγματοποιηθεί έλεγχοι ακεραιότητας λογισμικού στα ΠΕΣ της εταιρείας, 2) δεν υπάρχει καταγραφή των ενεργειών στις βάσεις δεδομένων, 3) η εφαρμογή με την οποία γίνεται η διαχείριση των καρτών φυσικής πρόσβασης των υπαλλήλων της εταιρείας στις εγκαταστάσεις της εταιρείας διαθέτει έναν

προκαθορισμένο, κοινό χρήστη admin, αλλά στη συνέχεια του ελέγχου της ΑΔΑΕ δημιουργήθηκαν δύο νέα προσωπικά accounts και 4) υπάρχουν προβλήματα στη λήψη αρχείων καταγραφής των firewalls της εταιρείας από το …μετά το Φεβρουάριο του 2016.

2.4. Στο έγγραφο με τίτλο «ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ-ΕΞΑΙΡΕΣΕΙΣ» του υπ΄αριθμ. πρωτ. ΑΔΑΕ ΕΜΠ222/04.11.2016 εγγράφου της ….. (4η, ως άνω διατυπωμένη, αδυναμία συμμόρφωσης) αναφέρεται ότι *«…το …. δεν έχει λάβει logs από τα firewalls…»* από τον Φεβρουάριο του 2016 και έπειτα και *«… είναι σε εξέλιξη διαδικασία διερεύνησης με τον κατασκευαστή του …., προκειμένου να αποκατασταθεί η συλλογή των logs»*.

Παρατήρηση 2: Από τις άνω δηλώσεις της εταιρείας, δεν προκύπτει ότι η εταιρεία έχει εξαντλήσει όλες τις δυνατότητες που τις δίνονται μέσω άλλων ισάξιων λύσεων αναφορικά με την λήψη και τη διατήρηση αρχείων καταγραφής. Δεδομένου ότι τα συστήματα firewall αποτελούν ιδιαίτερα ευαίσθητους κόμβους αναφορικά με την διασφάλιση του απορρήτου των επικοινωνιών, η εταιρεία οφείλει να προβεί άμεσα σε λύση που να ικανοποιεί την απαίτηση της ΑΔΑΕ για λήψη και διατήρηση ασφαλών αρχείων καταγραφής των προσβάσεων και των ενεργειών των διαχειριστών για χρονικό διάστημα τουλάχιστον δύο ετών και να ενημερώσει άμεσα την ΑΔΑΕ.

3. Υλοποίηση της Πολιτικής Αποδεκτής Χρήσης (Πολιτική Αποδεκτής Χρήσης, σελ. 12-15 της Πολιτικής Ασφάλειας της εταιρείας - Άρθρο 4 της Απόφασης 165/2011, ΦΕΚ 2715/Β/17.11.2011)

3.1 Στο πλαίσιο του από 21.10.2016 επιτόπιου ελέγχου, η Ο.Ε. έθεσε ερώτημα στην εταιρεία αναφορικά με τον τρόπο με τον οποίο εξασφαλίζει την ενημέρωση-εκπαίδευση των χρηστών ως προς την Πολιτική Ασφάλειας, όπως προβλέπεται στις παρ. 4.2.1 και 4.2.2, Άρθρο 4 της Απόφασης 165/2011 (παρ. 2.1.1, 2.2.1, 2.2.2 Πολιτική Αποδεκτής Χρήσης της …..). Η εταιρεία δήλωσε ότι πραγματοποιείται ενημέρωση των χρηστών, τόσο κατά την πρόσληψή τους, όσο και κατά τη διάρκεια της εργασίας τους, όποτε αυτό κρίνεται απαραίτητο. Οι εργαζόμενοι έχουν επίσης τη δυνατότητα πρόσβασης στην Πολιτική Ασφάλειας της εταιρείας, μέσω ηλεκτρονικού portal. Οι εκπαιδεύσεις των εργαζομένων καταγράφονται ηλεκτρονικά. Η εταιρεία παρέδωσε έγγραφο με τίτλο «Συμφωνία τήρησης εχεμύθειας και συμμόρφωσης με την εταιρική πολιτική ασφάλειας», το οποίο υπογράφεται κατά την πρόσληψη των εργαζομένων της εταιρείας (συνημμένο 5Α , 5Β, 5Γ του Πρακτικού της 21ης Οκτωβρίου 2016). Από τα συγκεκριμένα έγγραφα που προσκόμισε η εταιρεία προκύπτει ότι, για τους εν λόγω τρεις υπαλλήλους της, οι οποίοι είναι υπάλληλοι τηλεφωνικής εξυπηρέτησης, έχουν υπογραφεί, συνημμένα στην εν λόγω «Συμφωνία τήρησης εχεμύθειας και συμμόρφωσης με την εταιρική πολιτική ασφάλειας» τα τμήματα της Πολιτικής Ασφάλειας της εταιρείας που αναφέρονται στη Διαδικασία της εταιρείας με τίτλο «Διαδικασία Ενημέρωσης και Εκπαίδευσης Υπαλλήλων» (παρ. 2.2.1 Πολιτική Αποδεκτής Χρήσης της ……).

3.2 Στο πλαίσιο του από 21.10.2016 επιτόπιου ελέγχου, η Ο.Ε. ζήτησε από την εταιρεία να της παραδώσει το αρχείο συνεργατών της παραγράφου 4.3.1 του Άρθρου 4 της Απόφασης 165/2011 (παρ. 2.1.1, 2.3.3 Πολιτική Αποδεκτής Χρήσης της ….) και η εταιρεία παρέδωσε το συνημμένο 6 του Πρακτικού της 21ης Οκτωβρίου 2016, στο οποίο περιλαμβάνονται οι 4 συνεργάτες της εταιρείας με δυνατότητα πρόσβασης σε ΠΕΣ.

3.3. Στο πλαίσιο του από 21.10.2016 επιτόπιου ελέγχου, η Ο.Ε. ζήτησε από την εταιρεία να την ενημερώσει αναφορικά με το αν περιλαμβάνονται στις συμβάσεις με τους συνεργάτες της τα προβλεπόμενα στην παρ. 4.3.2, Άρθρο 4 της Απόφασης 165/2011 (παρ. 2.1.3, 2.3.2 Πολιτική Αποδεκτής Χρήσης της ……) και η εταιρεία παρέδωσε το συνημμένο 7 του Πρακτικού της 21ης Οκτωβρίου 2016, το οποίο αποτελεί σχετικό παράρτημα σύμβασης με τους 4 συνεργάτες (συνημμένο 7Α , 7Β, 7Γ, 7Δ του Πρακτικού της 21ης Οκτωβρίου 2016), οι οποίοι έχουν δυνατότητα απομακρυσμένης πρόσβασης σε ΠΕΣ. Από τη μελέτη του παραρτήματος, η Ο.Ε. διαπίστωσε ότι έχουν συμπεριληφθεί στις συμβάσεις με τους εν λόγω συνεργάτες της εταιρείας τα προβλεπόμενα στη Διαδικασία της εταιρείας με τίτλο «Διαδικασία Ενημέρωσης και Εκπαίδευσης Συνεργατών» (παρ. 2.2.2 Πολιτική Αποδεκτής Χρήσης της MEDIATEL).

4. Υλοποίηση της Πολιτικής Φυσικής Ασφάλειας (Πολιτική Φυσικής Ασφάλειας, σελ. 16-19 της Πολιτικής Ασφάλειας της εταιρείας, Άρθρο 5 της Απόφασης 165/2011, ΦΕΚ 2715/Β/17.11.2011)

4.1. Στο πλαίσιο του από 21.10.2016 επιτόπιου ελέγχου, η Ο.Ε. πραγματοποίησε έλεγχο του computer room και ζήτησε από την εταιρεία να της παραδώσει αντίγραφο του αρχείου καταγραφής των συνεργατών στο χώρο των ΠΕΣ. Η εταιρεία παρέδωσε το συνημμένο 8 του Πρακτικού της 21ης Οκτωβρίου 2016. Το εν λόγω έγγραφο περιλαμβάνει καταγραφή των συνεργατών που πραγματοποίησαν πρόσβαση σε χώρο ΠΕΣ το διάστημα από 30.10.2013 έως 06.10.2016. Τα στοιχεία που καταγράφονται για έκαστη πρόσβαση είναι αυτά που προβλέπονται στην παρ. 3.3.3. της Πολιτικής Φυσικής Ασφάλειας της εταιρείας (παρ. 5.2.4. Απόφασης 165/2011).

4.2. Στο πλαίσιο του από 21.10.2016 επιτόπιου ελέγχου, η Ο.Ε. ζήτησε τις αιτήσεις για είσοδο συνεργατών στο χώρο των ΠΕΣ, σύμφωνα με την παρ. 3.2.3 της Πολιτικής Φυσικής Ασφάλειας της …….. (παρ. 5.2.3. Απόφασης 165/2011), για τους συνεργάτες από τις εταιρείες «…» και «……..», οι οποίοι πραγματοποίησαν πρόσβαση σε χώρο ΠΕΣ στις 11.2.2016 και 6.10.2016 αντίστοιχα, όπως προκύπτει από το συνημμένο 8 του Πρακτικού της 21ης Οκτωβρίου 2016. Η εταιρεία παρέδωσε τα συνημμένα 9Α και 9Β του Πρακτικού της 21ης Οκτωβρίου 2016, από τα οποία προκύπτει ότι οι συγκεκριμένες αιτήσεις πρόσβασης είχαν εγκριθεί από τον αρμόδιο υπάλληλο της εταιρείας στις 10.02.2016 και 06.10.2016 αντίστοιχα.

4.3. Στο πλαίσιο του από 21.10.2016 επιτόπιου ελέγχου, οι εκπρόσωποι της εταιρείας επέδειξαν στα μέλη της Ο.Ε. την ηλεκτρονική εφαρμογή (…) καταγραφής πρόσβασης εισόδου στις εγκαταστάσεις της ……... Η εταιρεία δήλωσε ότι στο εν λόγω σύστημα καταγράφονται οι είσοδοι των εργαζομένων στις

εγκαταστάσεις της εταιρείας και όχι οι έξοδοι. Η Ο.Ε. ζήτησε από την εταιρεία να της παραδώσει το αρχείο από την ηλεκτρονική εφαρμογή με τις προσβάσεις στο computer room για το διάστημα από 01.01.2016 έως και 21.10.2016 και η εταιρεία παρέδωσε το συνημμένο 10 του Πρακτικού της 21ης Οκτωβρίου 2016-CD, το οποίο περιλαμβάνει τις εν λόγω καταγραφές.

4.4 Στο πλαίσιο του από 21.10.2016 επιτόπιου ελέγχου, η Ο.Ε. ζήτησε από την εταιρεία να της παραδώσει τα αιτήματα για ενεργοποίηση των καρτών πρόσβασης των υπαλλήλων του call center και τις εγκρίσεις αυτών, σύμφωνα με την παρ. 3.2.1 της Πολιτικής Φυσικής Ασφάλειας της …… (παρ. 5.2.2. Απόφασης 165/2011) ……., ……και ….. που εμφανίζονται σε ενδεικτική λίστα υπαλλήλων της εταιρείας (συνημμένο 11 του Πρακτικού της 21ης Οκτωβρίου 2016). Η Ο.Ε. διαπίστωσε ότι τα αιτήματα φυσικής πρόσβασης των εν λόγω υπαλλήλων έχουν πραγματοποιηθεί μέσω του ηλεκτρονικού συστήματος ……. και έχουν εγκριθεί από τους αρμόδιους υπαλλήλους της εταιρείας.

5. Υλοποίηση της Πολιτικής Λογικής Πρόσβασης (Πολιτική Λογικής Πρόσβασης, σελ. 20-28 της Πολιτικής Ασφάλειας της εταιρείας, Άρθρο 6 της Απόφασης 165/2011, ΦΕΚ 2715/Β/17.11.2011)

5.1. Στο πλαίσιο του από 21.10.2016 επιτόπιου ελέγχου, αναφορικά με την πρόσβαση στην ηλεκτρονική εφαρμογή καταγραφής πρόσβασης εισόδου στις εγκαταστάσεις της ….., η εταιρεία δήλωσε ότι υπάρχει ένας κοινός τοπικός λογαριασμός διαχειριστή (admin), ο οποίος χρησιμοποιείται από δύο άτομα. Σημειώνεται ότι, στο πλαίσιο του από 21.10.2016 επιτόπιου ελέγχου, η εταιρεία δεσμεύτηκε να εξετάσει τη δυνατότητα δημιουργίας προσωποποιημένων λογαριασμών πρόσβασης και να ενημερώσει για τα αποτελέσματα της έρευνάς της και για τον τρόπο θεραπείας της εν λόγω αδυναμίας.

Επίσης, στο πλαίσιο του από 09.12.2016 επιτόπιου ελέγχου, σε συνέχεια σχετικού αιτήματος της Ο.Ε., η εταιρεία παρέδωσε το αρχείο "ΠΑ-ΠΛΠ8.docx", το οποίο αναφέρεται στην παρ. 4.3.8 της Πολιτικής Λογικής Πρόσβασης της εταιρείας, στο οποίο καταγράφονται συστήματα με κοινούς/προκαθορισμένους λογαριασμούς πρόσβασης και εναλλακτικούς τρόπους ταυτοποίησης του φυσικού προσώπου (συνημμένο 5 του Πρακτικού της 9ης Δεκεμβρίου 2016-cd) και δεσμεύτηκε να παραδώσει συμπληρωματικό αρχείο έως την 23η Δεκεμβρίου 2016, το οποίο και έπραξε με την υπ΄αριθμ. πρωτ. ΑΔΑΕ 3196/27.12.2016 επιστολή (Σχετικό 1 αυτής με τίτλο *«Επεξηγήσεις μη ονομαστικών λογαριασμών ....συνημμένου 1 cd της 9/12/2016»*.

Επιπρόσθετα, σε συνέχεια του από 21.10.2016 επιτόπιου ελέγχου, η εταιρεία απέστειλε το υπ΄αριθμ. πρωτ. ΑΔΑΕ ΕΜΠ222/04.11.2016 έγγραφο. Στο Σχετικό 1 του εγγράφου αυτού, υπό τον τίτλο «ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ-ΕΞΑΙΡΕΣΕΙΣ», αναφορικά με την εφαρμογή διαχείρισης καρτών φυσικής πρόσβασης, η εταιρεία αναφέρει ότι η εταιρεία *«…διαθέτει ένα προκαθορισμένο χρήστη (admin) για την είσοδο σε αυτή. Προκειμένου να είναι ιχνηλατίσιμες οι ενέργειες των χειριστών της εφαρμογής, δημιουργήθηκαν δύο νέα προσωπικά (ονομαστικά) accounts»*.

Παρατήρηση 3: Σύμφωνα με το αρχείο "ΠΑ-ΠΛΠ8.docx", για την πρόσβαση στα συστήματα ….. έχει ενεργοποιηθεί ένας κοινός λογαριασμός για κάθε σύστημα (απαραίτητος για τη διενέργεια εργασιών σχετικών με την λειτουργικότητα των κόμβων) και *«δεν υπάρχει η πρόβλεψη για ενεργοποίηση άλλου λογαριασμού»*. Επίσης η εταιρεία, στο ίδιο έγγραφο, δηλώνει ότι *«δια μέσω των firewalls είναι δυνατός ο εντοπισμός του χρήστη που συνδέεται με ssh, telnet ή ftp»*.

Από την αξιολόγηση της αρχιτεκτονικής ασφάλειας και τους συγκεκριμένους κοινούς λογαριασμούς για τα εν λόγω συστήματα της εταιρείας, προκύπτει ότι παρόλο που χρησιμοποιείται ένας κοινός λογαριασμός για κάθε ένα από τα τρία αυτά συστήματα, μπορεί πράγματι να προσδιοριστεί ο πραγματικός χρήστης που αποκτά πρόσβαση μέσω του κοινού λογαριασμού πρόσβασης, δεδομένου ότι οι προσβάσεις των πραγματικών χρηστών καταγράφονται σε αρχείο στο firewall. Απαραίτητη προϋπόθεση για τον εντοπισμό τους είναι τα αρχεία καταγραφής στο firewall να παραμένουν ακέραια και να διατηρούνται για 2 έτη. Η εν λόγω διαπίστωση δύναται να αποτελέσει αντικείμενο μελλοντικού ελέγχου από την ΑΔΑΕ.

Τέλος, για την περίπτωση των backup servers, η εταιρεία δήλωσε ότι η πρόσβαση μέσω του κοινού λογαριασμού πρόσβασης καταγράφεται με syslog μέσω του …. Απαραίτητη προϋπόθεση είναι ότι τα αρχεία καταγραφής στο ……, που αφορούν τα εν λόγω συστήματα, θα πρέπει να παραμένουν ακέραια και να διατηρούνται για 2 έτη. Η εν λόγω διαπίστωση δύναται να αποτελέσει αντικείμενο μελλοντικού ελέγχου από την ΑΔΑΕ.

Για την περίπτωση τοπικής πρόσβασης χρηστών επί των εν λόγω συστημάτων με τον ίδιο κοινό λογαριασμό, ο πάροχος οφείλει να υλοποιήσει όλες εκείνες τις δεσμεύσεις που δε θα επιτρέπουν την απόκτηση φυσικής πρόσβασης στο σύστημα παρά μόνο ενός διαχειριστή ενώ απαραίτητη προϋπόθεση είναι τα αρχεία καταγραφής προσβάσεων και ενεργειών για τα εν λόγω συστήματα να διατηρούνται και αυτά για 2 έτη. Η εν λόγω διαπίστωση δύναται να αποτελέσει αντικείμενο μελλοντικού ελέγχου από την ΑΔΑΕ.

5.2 Στο πλαίσιο του από 2.12.2016 επιτόπιου ελέγχου, η εταιρεία ενημέρωσε ότι η πρόσβαση στις βάσεις μέσω της εφαρμογής …. ελέγχεται μέσω firewall (…..) και επέδειξε στην Ο.Ε. τον σχετικό κανόνα που αφορά στη δυνατότητα πρόσβασης στα διάφορα τμήματα της εταιρείας.

Η εφαρμογή …. έχει πρόσβαση στη βάση μέσω του χρήστη "sa". Ο κωδικός πρόσβασης του χρήστη "sa" είναι "hard coded", μη κρυπτογραφημένος, στον κώδικα του λογισμικού. Η Ο.Ε. θεωρεί ότι σε περίπτωση εκδήλωσης κάποιας επίθεσης, οι τεχνικές λύσεις της εταιρείας που περιγράφονται στις ανωτέρω παραγράφους αυξάνουν την πιθανότητα εμφάνισης ενός περιστατικού ασφάλειας που ενδεχομένως θα οδηγήσει σε παραβίαση του απορρήτου των επικοινωνιών. Πιο συγκεκριμένα, ενώ η πρόσβαση των χρηστών στην εφαρμογή ….. γίνεται με χρήση προσωπικών accounts, ακολούθως, η εφαρμογή …..συνδέεται με τη βάση δεδομένων μέσω ενός κωδικού πρόσβασης που είναι εισαγμένος στον κώδικα της εφαρμογής (hard coded). Συνεπώς, ο κωδικός αυτός είναι κοινός για όλους τους χρήστες και, επιπλέον,

δεν υπάρχει δυνατότητα της περιοδικής αλλαγής του. Η Ο.Ε. θεωρεί ότι η αδυναμία ασφάλειας που προκαλεί η χρήση των hard coded κωδικών πρόσβασης θα μπορούσε να μετριαστεί, εάν η hard coded πρόσβαση στη βάση δεδομένων περιοριζόταν μόνο για συγκεκριμένους χρήστες ή επιτρεπόταν μόνο από συγκεκριμένους σταθμούς εργασίας (π.χ. ορίζοντας την πρόσβαση από συγκεκριμένες IP διευθύνσεις στο Firewall), γεγονός που προβλέπεται και στην «Πολιτική ασφάλειας Δικτύου» της εταιρείας, στην οποία αναφέρεται ότι *«… επιτρέπεται μόνο η επικοινωνία των συστημάτων για τα οποία πρέπει να υπάρχει δίαυλος επικοινωνίας, και απαγορεύονται όλες οι υπόλοιπες επικοινωνίες».*

Απόκλιση 2: Πλην όμως, στην «Πολιτική Λογικής Πρόσβασης» της Πολιτικής Ασφάλειας της εταιρείας (παρ. 6.2.3., 6.4.1.δ, 6.4.2.3. της Απόφασης 165/2011) αναφέρεται ότι για τις περιπτώσεις πρόσβασης με τη χρήση της εφαρμογής και μέσω application password database *«υπάρχει μοναδικός λογαριασμός πρόσβασης για κάθε χρήστη» και «εφαρμόζεται πολιτική αλλαγής των κωδικών πρόσβασης…».*

5.3. Στο πλαίσιο του από 2.12.2016 επιτόπιου ελέγχου, η Ο.Ε. ζήτησε από την εταιρεία να της επιδείξει τους κανόνες δημιουργίας των κωδικών χρήστη και η εταιρεία παρέδωσε το αρχείο "……" (συνημμένο 1 του Πρακτικού της 2ας Δεκεμβρίου 2016-cd), από τη μελέτη του οποίου, η Ο.Ε. διαπίστωσε ότι οι κανόνες δημιουργίας των κωδικών χρήστη πληρούν τις προβλέψεις της παραγράφου 4.1. της Πολιτικής Λογικής Πρόσβασης της εταιρείας (Άρθρο 6, παρ.6.4.2.2. της Απόφασης 165/2011).

5.4. Στο πλαίσιο του από 2.12.2016 επιτόπιου ελέγχου, η Ο.Ε. ζήτησε από την εταιρεία να της παραδώσει την Αίτηση δημιουργίας λογαριασμού πρόσβασης για τον χρήστη "……." για το σύστημα …… και η εταιρεία δήλωσε ότι η εν λόγω Αίτηση δεν εμφανίζεται στο ηλεκτρονικό σύστημα ….. και δεσμεύτηκε να διερευνήσει αν διαθέτει άλλη μορφή αίτησης. Στο πλαίσιο του από 9.12.2016 επιτόπιου ελέγχου, η εταιρεία δήλωσε ότι δε βρήκε κάποια αίτησή του χρήστη "….." για δημιουργία κωδικού και ότι λόγω παλαιότητας το email δεν εντοπίσθηκε.

Περαιτέρω, στο πλαίσιο του από 2.12.2016 επιτόπιου ελέγχου η Ο.Ε. ζήτησε από την εταιρεία να της παραδώσει τις Αιτήσεις δημιουργίας λογαριασμού πρόσβασης για τους χρήστες του IT ….. και …..και η εταιρεία δήλωσε ότι οι συγκεκριμένοι χρήστες είναι παλιοί υπάλληλοι της εταιρείας και έγινε μαζικά η αρχικοποίηση της πρόσβασής τους.

Παρατήρηση 4: Στην παρ. 4.2.1 της Πολιτικής Λογικής Πρόσβασης της εταιρείας (παρ. 6.3.1.2 και 6.3.1.3 της Απόφασης 165/2011) προβλέπεται ότι *«για την περίπτωση δημιουργίας καινούργιου λογαριασμού πρόσβασης, αποστέλλεται από τον προϊστάμενο του τμήματος στο οποίο ανήκει ο εργαζόμενος, φόρμα αίτησης δημιουργίας/μεταβολής λογαριασμού πρόσβασης … προς τον υπεύθυνο λογικής πρόσβασης της εταιρείας».* Επισημαίνεται ότι η εταιρεία άμεσα και σε συνεννόηση με τους εργαζόμενούς της, για όσους δεν υπάρχουν αιτήσεις δημιουργίας/μεταβολής λογαριασμών πρόσβασης, οφείλει να δημιουργήσει αιτήσεις με αναγραφή της πραγματικής ημερομηνίας δημιουργίας/μεταβολής των λογαριασμών πρόσβασής τους και ακολούθως να τις αποδεχτεί στο σύνολο τους. Η εταιρεία οφείλει να ενημερώσει άμεσα την ΑΔΑΕ για την υλοποίηση των παραπάνω ενεργειών της.

5.5. Στο πλαίσιο του από 2.12.2016 επιτόπιου ελέγχου, η Ο.Ε. ζήτησε από την εταιρεία να της παραδώσει το αρχείο λογαριασμών πρόσβασης της παραγράφου 4.3.1 της Πολιτικής Λογικής Πρόσβασης της εταιρείας, για τους χρήστες "……" και "…." και η εταιρεία παρέδωσε τα αρχεία "…." και "……" (συνημμένα 4α, 4β του Πρακτικού της 2ας Δεκεμβρίου 2016-cd). Από τη μελέτη των αρχείων η Ο.Ε. διαπίστωσε ότι πληρούνται οι προβλέψεις της παραγράφου 4.3.1.

5.6. Στο πλαίσιο του από 2.12.2016 επιτόπιου ελέγχου, η Ο.Ε. διαπίστωσε ότι από τους χρήστες που έχουν πρόσβαση μέσω του συστήματος ….. (συνολικά 38, συνημμένο 2 του Πρακτικού της 2ας Δεκεμβρίου 2016), για 12 χρήστες (αρχείο "……..", συνημμένο 5 του Πρακτικού της 2ας Δεκεμβρίου 2016-cd), υπάρχουν Αιτήσεις δημιουργίας/μεταβολής κωδικών πρόσβασης στο …….. Αναφορικά με την αιτιολόγηση των λογαριασμών που εμφανίζονται στο αρχείο "……." (συνημμένο 2α του από 02.12.2016 Πρακτικού ελέγχου) και που δεν ανήκουν σε φυσικά πρόσωπα, η εταιρεία παρέδωσε το συνημμένο 1 του Πρακτικού της 9ης Δεκεμβρίου 2016 - cd και παρείχε προφορικά στην Ο.Ε. επεξηγήσεις ανά λογαριασμό. Η Ο.Ε. ζήτησε από την εταιρεία να της παραδώσει εγγράφως τις εν λόγω επεξηγήσεις και η εταιρεία δεσμεύτηκε να αποστείλει τα στοιχεία σε προθεσμία που θα τάξει η Ο.Ε. Από τη μελέτη του απεσταλμένου αρχείου με τίτλο «Επεξηγήσεις λογαριασμών ……» συνημμένο 1 cd της 9/12/2016, η Ο.Ε. διαπίστωσε ότι οι επεξηγήσεις της εταιρείας είναι επαρκείς.

5.7. Στο πλαίσιο του από 9.12.2016 επιτόπιου ελέγχου, η Ο.Ε. ζήτησε από τον εκπρόσωπο της εταιρείας να πραγματοποιήσει πρόσβαση στο ……. και επιβεβαίωσε την καταγραφή των ενεργειών του από την εφαρμογή.

Επίσης, η Ο.Ε. επιβεβαίωσε την καταγραφή της σύνδεσης του …… στον …… από το …… και παρατήρησε ότι η πρόσβαση του …. καταγράφεται ως πρόσβαση από το χρήστη "sa" και επίσης καταγράφεται η source ip.

5.8. Στο πλαίσιο του από 2.12.2016 επιτόπιου ελέγχου, η Ο.Ε. ζήτησε από την εταιρεία να της παραδώσει τη λίστα με τα συστήματα ΠΕΣ στα οποία έχουν δυνατότητα πρόσβασης οι χρήστες του ΙΤ …..και ….. (παρ. 4.3.1. της Πολιτικής Λογικής Πρόσβασης της εταιρείας) και η εταιρεία παρέδωσε τα αρχεία …… (συνημμένα 6 και 7 του Πρακτικού της 2ας Δεκεμβρίου 2016 – cd).). Από τη μελέτη των αρχείων η Ο.Ε. διαπίστωσε ότι πληρούνται οι προβλέψεις της παραγράφου 4.3.1 που αφορούν στο επίπεδο της πρόσβασης και στα στοιχεία ΠΕΣ στα οποία έχουν δυνατότητα πρόσβασης οι εν λόγω χρήστες.

5.9. Στο πλαίσιο του από 9.12.2016 επιτόπιου ελέγχου, η εταιρεία, σε συνέχεια σχετικού αιτήματος της Ο.Ε., δημιούργησε έναν δοκιμαστικό χρήστη/συνεργάτη (adae_test) στο ….. μέσω του …….. Η Ο.Ε. διαπίστωσε ότι ο χρήστης ενημερώνεται μέσω email για την ενεργοποίηση της πρόσβασής του στη νέα υπηρεσία και ότι πρέπει να αλλάξει τον αρχικό κωδικό πρόσβασης. Η εταιρεία παρέδωσε το εν λόγω email (συνημμένο 3 του Πρακτικού της 9ης Δεκεμβρίου 2016-cd), στο οποίο περιλαμβάνονται και οδηγίες προς το συγκεκριμένο χρήστη για την πρόσβασή του και την υποχρέωση δημιουργίας του νέου κωδικού. Η εταιρεία δήλωσε επίσης, ότι η συχνότητα αλλαγής των κωδικών πρόσβασης είναι 3 μήνες και ότι ο

χρήστης ενημερώνεται με αυτοματοποιημένο τρόπο για τη λήξη του κωδικού του. Η εταιρεία παρέδωσε εγγραφές από τη βάση για το χρήστη adae_test (συνημμένο 4α, 4β του Πρακτικού της 9ης Δεκεμβρίου 2016-cd), στις οποίες φαίνονται, μεταξύ άλλων, πληροφορίες για τη δημιουργία του κωδικού, ο κωδικός χρήστη κρυπτογραφημένος και η συχνότητα αλλαγής αυτού.

Η ως άνω περιγραφόμενη διαχείριση του νέου χρήστη της εφαρμογής ……. είναι σύμφωνη με τα προβλεπόμενα στην παρ. 4.2.1.1 της Πολιτικής Λογικής Πρόσβασης της εταιρείας (παρ. 6.5.2. Άρθρο 6, Απόφαση 165/2011).

5.12. Στο πλαίσιο του από 9.12.2016 επιτόπιου ελέγχου, η Ο.Ε. έθεσε ερώτημα στην εταιρεία αναφορικά με τον έλεγχο της Πολιτικής Λογικής Πρόσβασης (παρ. 4.2.3 της Πολιτικής Λογικής Πρόσβασης της εταιρείας) και ζήτησε από την εταιρεία να της παραδώσει αποτελέσματα πρόσφατων ελέγχων.

Η εταιρεία παρέδωσε έγγραφο με τίτλο *«ΠΑ-ΠΕΠΑΔΑΕ4-Πολιτική_Λογικής Πρόσβασης_072016»* ως Σχετικό 1 της με υπ΄αριθμ. πρωτ. ΑΔΑΕ 3196/27.12.2016 επιστολής, στο οποίο αναφέρεται ότι πραγματοποιήθηκε έλεγχος των αρχείων καταγραφής του συστήματος …..(σύστημα καταγραφής των ηχογραφημένων συνομιλιών) για το χρονικό διάστημα από 01.06.2016 έως 30.06.2016 και δειγματοληπτικός έλεγχος των αιτήσεων ενεργοποίησης πρόσβασης στο εν λόγω σύστημα για 3 υπαλλήλους της εταιρείας.

Απόκλιση 3: Πλην όμως, ο εν λόγω έλεγχος αφορά σε ένα μόνο σύστημα της εταιρείας και συνεπώς δεν καλύπτει επαρκές δείγμα των ΠΕΣ της εταιρείας. Επιπρόσθετα, στην Πολιτική Λογικής Πρόσβασης της εταιρείας (παρ. 4.2.3.) αναφέρεται ότι ο έλεγχος πραγματοποιείται σε εξαμηνιαία βάση, γεγονός που δεν έχει εφαρμοστεί για το έτος 2016 για το σύστημα ……, για το οποίο παραδόθηκε ο ανωτέρω έλεγχος.

6. Υλοποίηση της Πολιτικής Απομακρυσμένης Λογικής Πρόσβασης (Πολιτική Απομακρυσμένης Λογικής Πρόσβασης, σελ. 29-32 της Πολιτικής Ασφάλειας της εταιρείας , Άρθρο 7 της Απόφασης 165/2011, ΦΕΚ 2715/Β/17.11.2011)

6.1. Αναφορικά με την απομακρυσμένη πρόσβαση, η Ο.Ε. ζήτησε από την εταιρεία, στο πλαίσιο του από 2.12.2016 επιτόπιου ελέγχου, τα αρχεία των παραγράφων 5.3.1 και 5.3.2 της Πολιτικής Απομακρυσμένης Λογικής Πρόσβασης. Η εταιρεία παρέδωσε το αρχείο της παραγράφου 5.3.1. (αρχείο …., συνημμένο 9 του Πρακτικού της 2ας Δεκεμβρίου 2016-cd).

6.2. Στο πλαίσιο του από 9.12.2016 επιτόπιου ελέγχου, η εταιρεία δεσμεύτηκε να παραδώσει αρχεία αναφορικά με τον έλεγχο της Πολιτικής Απομακρυσμένης Λογικής Πρόσβασης (παρ. 5.2.3.της Πολιτικής Απομακρυσμένης Λογικής Πρόσβασης της εταιρείας) έως την 23η Δεκεμβρίου 2016.

Η εταιρεία παρέδωσε έγγραφο με τίτλο *«pol.pdf»* ως Σχετικό 2 της με υπ΄αριθμ. πρωτ. ΑΔΑΕ 3196/27.12.2016 επιστολής, στο οποίο περιγράφονται έλεγχοι της απομακρυσμένης λογικής πρόσβασης των συνεργατών σε ΠΕΣ κατά τις ημερομηνίες 03.03.2016, 01.04.2016, 06.06.2016, 12.08.2016, 26.10.2016 και 01.12.2016.

Απόκλιση 4: Πλην όμως, στην Πολιτική Απομακρυσμένης Λογικής Πρόσβασης της εταιρείας, παρ. 5.2.4, αναφέρεται ότι ο έλεγχος της απομακρυσμένης λογικής πρόσβασης των συνεργατών σε ΠΕΣ *«…πραγματοποιείται μία φορά το μήνα»*.

Επιπλέον, στην παρ. 5.2.3 της Πολιτικής Απομακρυσμένης Λογικής Πρόσβασης της εταιρείας προβλέπεται ότι ανά 3 μήνες πραγματοποιείται έλεγχος των λογαριασμών απομακρυσμένης λογικής πρόσβασης των υπαλλήλων της εταιρείας, αλλά η εταιρεία δεν έχει παραδώσει στην Ο.Ε. αντίστοιχες αναφορές.

7. Υλοποίηση της Πολιτικής Διαχείρισης και Εγκατάστασης ΠΕΣ (Πολιτική Διαχείρισης και Εγκατάστασης ΠΕΣ, σελ. 33-36 της Πολιτικής Ασφάλειας της εταιρείας, Άρθρο 8 της Απόφασης 165/2011, ΦΕΚ 2715/Β/17.11.2011)

7.1. Στο πλαίσιο του από 21.10.2016 επιτόπιου ελέγχου και σε συνέχεια σχετικού αιτήματος της Ο.Ε., η εταιρεία παρέδωσε τις Εκθέσεις που αφορούν στην εγκατάσταση και στον έλεγχο, ενδεικτικά του database server του ΠΕΣ ……., το οποίο αποτελεί το billing και reporting σύστημα της εταιρείας (συνημμένο 12 του Πρακτικού της 21ης Οκτωβρίου 2016), καθώς και λίστα με μερικές από τις αλλαγές σε λογισμικό (συνημμένο 13 του Πρακτικού της 21ης Οκτωβρίου 2016) σε ΠΕΣ της εταιρείας. Η εταιρεία δήλωσε ότι η λίστα που παρέδωσε αποτυπώνει τις βασικές αλλαγές (π.χ. αλλαγές OS), ενώ η εταιρεία δε διατηρεί ιστορικότητα για τις πιο λεπτομερείς αλλαγές όπως τις αναβαθμίσεις εφαρμογών και λειτουργικών συστημάτων.

Απόκλιση 5: Η εταιρεία οφείλει να διατηρεί αρχείο στο οποίο να καταγράφεται οποιαδήποτε αλλαγή υλικού ή λογισμικού ΠΕΣ με κάθε λεπτομέρεια και κατ' ελάχιστον η ημερομηνία, ο τρόπος αλλαγής, η αιτιολόγηση της αλλαγής, ο εργαζόμενος ή συνεργάτης που πραγματοποίησε τις αλλαγές, σύμφωνα με την παράγραφο 6.1 της Πολιτικής Διαχείρισης και Εγκατάστασης ΠΕΣ της εταιρείας (παρ. 8.2.3, Απόφασης 165/2011).

7.2. Στο πλαίσιο του από 9.12.2016 επιτόπιου ελέγχου, η Ο.Ε. έθεσε ερώτημα στην εταιρεία αναφορικά με την καταγραφή της ενημέρωσης του λογισμικού του firewall (……..) από τον προμηθευτή (παρ. 8.2.2 της Απόφασης 165/2011, Ενότητα 6, παρ. 6.3.1. της Πολιτικής Ασφάλειας της εταιρείας). Η εταιρεία δήλωσε ότι καταγράφονται οι προσβάσεις του εξωτερικού συνεργάτη μέσω vpn, καθώς και μία γενική αιτιολόγηση των ενεργειών που πραγματοποίησε.

Επίσης, παρέδωσε ενδεικτικά email του προμηθευτή για προγραμματισμό αναβάθμισης (συνημμένο 7α του Πρακτικού της 9ης Δεκεμβρίου 2016 – cd), καθώς και την Αίτηση Πρόσβασης στο χώρο Φιλοξενίας ΠΕΣ του συνεργάτη (συνημμένο 7β του Πρακτικού της 9ης Δεκεμβρίου 2016 – cd), για την πραγματοποίηση της αναβάθμισης.

7.3. Στο πλαίσιο του από 9.12.2016 επιτόπιου ελέγχου, η εταιρεία δήλωσε ότι στους sql servers καταγράφεται μόνο η σύνδεση (πρόσβαση), αλλά όχι οι ενέργειες. Σημειώνεται ότι η εταιρεία έχει

παραδώσει στην ΑΔΑΕ, με το υπ΄αριθμ. πρωτ. ΑΔΑΕ ΕΜΠ222/04.11.2016 έγγραφο (σχετικό 1 αυτού υπό τον τίτλο «ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ-ΕΞΑΙΡΕΣΕΙΣ»), σχετική αδυναμία συμμόρφωσης στην οποία αναφέρεται ότι *«… δεν έχει υλοποιηθεί η καταγραφή ενεργειών που κάνουν οι χρήστες των βάσεων δεδομένων SQL server της εταιρείας κατά τη σύνδεσή τους…»*. Για την ως άνω αδυναμία συμμόρφωσης δεν παρέχεται από την εταιρεία επαρκής τεκμηρίωση, όπως προβλέπεται στην Ενότητα «Εισαγωγή» της Πολιτικής Ασφάλειας της εταιρείας, σελίδα 9 αυτής (παρ. 3.2.3. της Απόφασης 165/2011). Επιπρόσθετα, η εταιρεία δεν επικαλείται συγκεκριμένο χρονοδιάγραμμα για τη θεραπεία της. Κατά συνέπεια, η ως άνω αδυναμία συμμόρφωσης δεν δύναται να γίνει αποδεκτή από την Ο.Ε.

Απόκλιση 6: Στην Ενότητα «Πολιτική Διαχείρισης και Εγκατάστασης ΠΕΣ» της Πολιτικής Ασφάλειας της εταιρείας, σελίδα 34 αυτής (παρ. 8.3.2.2 της Απόφασης 165/2011), προβλέπεται ότι *«Ενέργειες στο λειτουργικό σύστημα και τις εφαρμογές των ΠΕΣ, καθώς και τα συμβάντα συστήματος ΠΕΣ καταγράφονται και διατηρούνται σε αρχείο»*.

Η εταιρεία οφείλει να υποστηρίξει τεχνικές λύσεις, με τις οποίες να παρακάμπτει τα τεχνικά προβλήματα και να καταγράφει το σύνολο των ενεργειών κατά την πρόσβαση των χρηστών παρόχου σε δεδομένα επικοινωνίας. Να σημειωθεί ότι για το ενδεχόμενο όπου η άμεση εφαρμογή της ως άνω απαίτησης δημιουργήσει προβλήματα λειτουργίας όπως για παράδειγμα την υπερφόρτωση της βάσης δεδομένων, αυτό πρέπει να δικαιολογηθεί επαρκώς και σε περίπτωση επαλήθευσης του να εξασφαλιστεί η υλοποίηση της απαίτησης με τη χρήση άλλων ισάξιων λύσεων και μηχανισμών ασφάλειας όπου θα τεκμηριώνονται για την ορθότητα τους ως προς την καταγραφή των προσβάσεων και ενεργειών των διαχειριστών. Η εταιρεία οφείλει να ενημερώσει άμεσα την ΑΔΑΕ για την υλοποίηση των παραπάνω ενεργειών της.

8. Υλοποίηση της Πολιτικής Ασφάλειας Δικτύου (Πολιτική Ασφάλειας Δικτύου, σελ. 40-43 της Πολιτικής Ασφάλειας της εταιρείας, Άρθρο 10 της Απόφασης 165/2011, ΦΕΚ 2715/Β/17.11.2011)

8.1. Στο πλαίσιο του από 21.10.2016 επιτόπιου ελέγχου, η εταιρεία παρέδωσε στην ΑΔΑΕ το διάγραμμα του εσωτερικού δικτύου της κατατετμημένο σε ζώνες (συνημμένο 3 του Πρακτικού της 21ης Οκτωβρίου 2016), με επαρκή πληροφορία, το οποίο προβλέπεται στην παρ. 8.2.3. της Πολιτικής Ασφάλειας της εταιρείας (παρ. 10.1 του Άρθρου 10 της Απόφασης 165/2011).

9. Υλοποίηση της Πολιτικής Διαχείρισης Περιστατικών Ασφάλειας (Πολιτική Διαχείρισης Περιστατικών Ασφάλειας, σελ. 37-39 της Πολιτικής Ασφάλειας της εταιρείας, Άρθρο 9 της Απόφασης 165/2011, ΦΕΚ 2715/Β/17.11.2011)

9.1. Στο πλαίσιο του από 21.10.2016 επιτόπιου ελέγχου, η εταιρεία δήλωσε ότι έως την ημερομηνία του ελέγχου, δεν έχουν παρουσιαστεί περιστατικά ασφάλειας που να αφορούν σε παραβίαση του απορρήτου των επικοινωνιών.

10. Υλοποίηση της Πολιτικής Ελέγχου Εφαρμογής της Πολιτικής Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών (Πολιτική Ελέγχου Εφαρμογής της Πολιτικής Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών, σελ. 44-46 της Πολιτικής Ασφάλειας της εταιρείας, Άρθρο 11 της Απόφασης 165/2011, ΦΕΚ 2715/Β/17.11.2011)

10.1. Στο πλαίσιο του από 9.12.2016 επιτόπιου ελέγχου, η εταιρεία δήλωσε ότι ο έλεγχος εφαρμογής της πολιτικής ασφάλειας πραγματοποιείται από εξωτερική εταιρεία σε ετήσια βάση και ότι θα παραδώσει προγραμματισμό και αποτελέσματα ελέγχων για το έτος 2015 έως την 23η Δεκεμβρίου 2016. Με την υπ΄αριθμ. πρωτ. ΑΔΑΕ 3196/27.12.2016 επιστολή, η εταιρεία παρέδωσε αρχείο ετήσιου ελέγχου (Σχετικό 3 της επιστολής με τίτλο *«Αναφορά Επιθεώρησης»*). Από τη μελέτη του ως άνω εγγράφου, η Ο.Ε. διαπίστωσε τα ακόλουθα:

- Δεν είναι ξεκάθαρη η ημερομηνία σύνταξης του εν λόγω εγγράφου, δεδομένου ότι αναφέρονται 2 διαφορετικές ημερομηνίες (8/3/2016 και 15/2/2015)
- Δεν περιλαμβάνονται τα συστήματα (ΠΕΣ) που ελέγχθηκαν ως προς την ορθή τήρηση των επιμέρους πολιτικών και διαδικασιών, καθώς και η συλλογή των απαιτούμενων πληροφοριών και δεδομένων που οδήγησαν στα αναφερόμενα αποτελέσματα
- Δεν περιλαμβάνονται αποτελέσματα ελέγχων για την εύρεση τεχνικών ευπαθειών στα ΠΕΣ (penetration tests)
- Δεν περιλαμβάνεται χρονοδιάγραμμα διεξαγωγής του ελέγχου

Απόκλιση 7: Πλην όμως, στην ενότητα 9 της Πολιτικής Ασφάλειας της εταιρείας (Άρθρο 11 της Απόφασης 165/2011), προβλέπεται ότι *«… προγραμματίζεται έλεγχος εφαρμογής της Πολιτικής Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών, καταγράφεται σε αρχείο, καλύπτει όλο το εύρος της Πολιτικής και πραγματοποιείται κατ΄ελάχιστον ανά 2 έτη…»*. Ο έλεγχος περιλαμβάνει τα στοιχεία που αναφέρονται στην παρ. 9.1. της Πολιτικής Ασφάλειας της εταιρείας, όπως άλλωστε προβλέπεται και στην παρ. 11.3 της υπ' αριθμ. 165/2011 Απόφασης της ΑΔΑΕ.

11. Υλοποίηση της Πολιτικής Αντιμετώπισης Κακόβουλου Λογισμικού (Πολιτική Αντιμετώπισης Κακόβουλου Λογισμικού, σελ. 47-49 της Πολιτικής Ασφάλειας της εταιρείας, Άρθρο 12 της Απόφασης 165/2011, ΦΕΚ 2715/Β/17.11.2011)

11.1. Στο πλαίσιο του από 9.12.2016 επιτόπιου ελέγχου, η εταιρεία δήλωσε ότι τα αντιικά ενημερώνονται με αυτοματοποιημένη διαδικασία, γεγονός το οποίο είναι σύμφωνο με την παρ. 10.1. της Πολιτικής Αντιμετώπισης Κακόβουλου Λογισμικού της εταιρείας.

11.2. Ως προς τον έλεγχο ακεραιότητας λογισμικού (παρ. 10.1.), στο πλαίσιο του από 9.12.2016 επιτόπιου ελέγχου, η εταιρεία δήλωσε ότι επί του παρόντος δεν πραγματοποιείται, αλλά η εταιρεία βρίσκεται σε

αναζήτηση σχετικού λογισμικού για τα πληροφοριακά συστήματα. Σημειώνεται ότι η εταιρεία έχει παραδώσει στην ΑΔΑΕ, με το υπ΄αριθμ. πρωτ. ΑΔΑΕ ΕΜΠ222/04.11.2016 έγγραφο, σχετική αδυναμία συμμόρφωσης (υπ΄αριθμόν 1 αδυναμία συμμόρφωσης με τίτλο «Εφαρμογή παρακολούθησης ακεραιότητας αρχείων»), στην οποία αναφέρεται ότι δεν έχουν πραγματοποιηθεί έλεγχοι ακεραιότητας λογισμικού στα ΠΕΣ της εταιρείας. Επισημαίνεται ότι για την ως άνω αδυναμία συμμόρφωσης δεν παρέχεται από την εταιρεία επαρκής τεκμηρίωση, όπως προβλέπεται στην Ενότητα «Εισαγωγή» της Πολιτικής Ασφάλειας της εταιρείας, σελίδα 9 αυτής (παρ. 3.2.3. της Απόφασης 165/2011).

Παρατήρηση 5: Η διασφάλιση της ακεραιότητας λογισμικού των ΠΕΣ της εταιρείας, λαμβάνοντας υπόψη το βαθμό δυσκολίας υλοποίησής της ανά σύστημα (για παράδειγμα η κάλυψη των απαιτήσεων για την διασφάλιση της ακεραιότητας του λογισμικού σε δικτυακά συστήματα ή συστήματα με κλειστό λογισμικό σε σύγκριση με συστήματα που φέρουν ανοικτό λογισμικό), οφείλει σταδιακά να υλοποιηθεί. Η εταιρεία οφείλει να τεκμηριώσει και να αποτυπώσει όλα τα στάδια που απαιτούνται για τη σταδιακή ενσωμάτωση της απαίτησης για επιτυχή διασφάλιση της ακεραιότητας λογισμικού στα ΠΕΣ. Η εταιρεία οφείλει να ενημερώσει άμεσα την ΑΔΑΕ για την σταδιακή υλοποίηση των παραπάνω ενεργειών της.

12. Υλοποίηση της Πολιτικής Χρήσης Κρυπτογραφίας (Πολιτική Χρήσης Κρυπτογραφίας, σελ. 50 της Πολιτικής Ασφάλειας της εταιρείας, Άρθρο 13 της Απόφασης 165/2011, ΦΕΚ 2715/Β/17.11.2011)

12.1. Στο πλαίσιο του από 2.12.2016 επιτόπιου ελέγχου, πραγματοποιήθηκε πρόσβαση στη βάση …….. και η εταιρεία επέδειξε τους χρήστες του ….. και παρέδωσε τα αρχεία …., Taxis-users 1/2/3 of 3 (συνημμένα 2α, 2β, 2γ, 2δ του Πρακτικού της 2^{ας} Δεκεμβρίου 2016-cd). Διαπιστώθηκε ότι οι κωδικοί διατηρούνται κρυπτογραφημένοι.

12.2. Στο πλαίσιο του από 9.12.2016 επιτόπιου ελέγχου, η εταιρεία δήλωσε ότι κρυπτογραφούνται οι κωδικοί πρόσβασης στα ΠΕΣ με …… και ότι, επίσης, τα αντίγραφα των cdrs που προέρχονται από το switch καταλήγουν σε τρίτο δικτυακό χώρο αποθήκευσης (…….) και κρυπτογραφούνται με …….

13. Άλλες Παρατηρήσεις

13.1. Κατά τη διάρκεια του από 21.10.2016 επιτόπιου ελέγχου, σε σχετική ερώτηση της Ο.Ε., η εταιρεία δήλωσε ότι τα δεδομένα επικοινωνίας που διατηρούνται στα συστήματά της είναι οι τηλεφωνικοί αριθμοί αυτών που χρησιμοποιούν τις υπηρεσίες πολυμεσικής πληροφόρησης, οι τηλεφωνικοί αριθμοί που αφορούν εισερχόμενα sms (premium sms) και εξερχόμενα bulk sms, και το περιεχόμενο των sms.

Στο πλαίσιο του από 02.12.2016 επιτόπιου ελέγχου, η Ο.Ε. ζήτησε από την εταιρεία να την ενημερώσει αναφορικά με το χρόνο διατήρησης των δεδομένων κλήσεων και sms (περιεχόμενο και εξωτερικά δεδομένα επικοινωνίας) στα συστήματα της και η εταιρεία δήλωσε ότι διατηρούνται 2 με 3 έτη.

Αναφορικά με τη διαγραφή των δεδομένων, η εταιρεία δήλωσε ότι δε γίνεται αυτοματοποιημένα, αλλά εκτελούνται scripts χειροκίνητα.

Η Ο.Ε. επεσήμανε στην εταιρεία τις ισχύουσες διατάξεις της κείμενης νομοθεσίας (ν.3471/2006, 3917/2011) αναφορικά με τις υποχρεώσεις των παρόχων για το χρόνο διατήρησης και την καταστροφή δεδομένων επικοινωνίας.

Στο πλαίσιο του από 09.12.2016 επιτόπιου ελέγχου, η Ο.Ε. επανέλαβε στην εταιρεία ότι τα δεδομένα πρέπει να διαγράφονται μετά το πέρας των 12 μηνών, σύμφωνα με την κείμενη νομοθεσία (ν.3471/2006, 3917/2011) και η εταιρεία δεσμεύτηκε ότι θα παραδώσει στην ΑΔΑΕ αποδείξεις καταστροφής των δεδομένων που διατηρούνται στα συστήματά της πέραν των 12 μηνών έως την 28η Φεβρουαρίου 2017. Η εταιρεία απέστειλε το υπ΄αριθμ. πρωτ. ΑΔΑΕ 610/28.02.2017 έγγραφο, στο οποίο αναφέρει ότι *«... υλοποιήθηκαν αυτόματες διεργασίες στα συστήματα sql server της εταιρείας μας, στα οποία τηρούνται δεδομένα επικοινωνίας, οι οποίες εφαρμόζουν τις ακόλουθες πολιτικές τήρησης δεδομένων επικοινωνίας:*

1. *Σε όσους πίνακες SQL server περιέχουν κεντρικά δεδομένα επικοινωνίας (cdrs, sms logs, κλπ), βάσει των οποίων υλοποιούνται αριθμητικές αναφορές κίνησης, γίνεται «ανωνυμοποίηση» των δεδομένων επικοινωνίας με ηλικία άνω των 12 μηνών ώστε να μπορεί να λειτουργεί απρόσκοπτα η εκτέλεση των αναφορών σε δεδομένα επικοινωνίας...».*

2. *«Σε όσους πίνακες SQL server περιέχουν κεντρικά δεδομένα επικοινωνίας με σκοπό την εξυπηρέτηση συγκεκριμένου τύπου υπηρεσίας... γίνεται διαγραφή των εγγραφών με ηλικία άνω των 12 μηνών. Επίσης, γίνεται διαγραφή των αντίστοιχων αρχείων ηχογραφήσεων, όπου υπάρχουν, των στοιχείων των συμμετεχόντων σε διαγωνισμούς. Οι διεργασίες αυτές εκτελούνται αυτόματα, σε εβδομαδιαία βάση.»*

Δ. ΣΥΜΠΕΡΑΣΜΑΤΑ

Από τα στοιχεία του φακέλου που εξετάστηκαν κατά τη διενέργεια του τακτικού ελέγχου στην εταιρεία …….και ειδικότερα:

α. από τη μελέτη της υπ΄αριθμ. πρωτ. ΑΔΑΕ ΕΜΠ145/17.05.2012 Πολιτικής Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών της εταιρείας, όπως αυτή αναθεωρήθηκε με το με αριθμ.πρωτ. ΑΔΑΕ ΑΔΑΕ ΕΜΠ33/7.03.2013 έγγραφο, και εγκρίθηκε με την υπ'αριθμ.162/2013 Απόφαση της ΑΔΑΕ, η οποία παρελήφθη από την εταιρεία την 04.07.2013, σύμφωνα με το υπ' αριθμ. πρωτ. ΑΔΑΕ 1552/04.07.2013 Πρωτόκολλο Παράδοσης-Παραλαβής.

β. από τον δειγματοληπτικό έλεγχο εφαρμογής της Πολιτικής Ασφάλειας, ο οποίος πραγματοποιήθηκε βάσει της υπ' αριθμ. 59/2016 Απόφασης της Ολομέλειας της ΑΔΑΕ,

γ. από τα Πρακτικά των επιτόπιων ελέγχων και τα συνημμένα αυτών,

δ. από την εξέταση των παραληφθέντων στοιχείων, όπως αναφέρονται στην παρούσα Έκθεση, και όπως προκύπτουν από τα σχετικά έγγραφα, τα οποία είναι στη διάθεση της Ολομέλειας της ΑΔΑΕ,

διαπιστώθηκε ότι η εταιρεία «…...», κατά το χρόνο διεξαγωγής του παρόντος τακτικού ελέγχου, δεν εφήρμοζε πλήρως την εγκριθείσα με την υπ'αριθμ. 162/2013 Απόφαση της ΑΔΑΕ Πολιτική Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών, ως προς τα σημεία, και με τις παρατηρήσεις, που αναφέρονται αναλυτικά στην ενότητα Γ της παρούσας έκθεσης.».

Κατόπιν της έγκρισης της από 10 Μαρτίου 2017 έκθεσης διενέργειας τακτικού ελέγχου στις εγκαταστάσεις της εταιρείας «…...» σύμφωνα με την υπ' αριθμ. 134/2017 Απόφαση της Ολομέλειας της Αρχής, η εταιρεία «……..» έλαβε γνώση της εν λόγω Απόφασης, μετά της συνημμένης έκθεσης ελέγχου, όπως προκύπτει από την υπ' αριθμ. πρωτ. ΑΔΑΕ 2510/06-09-2017 Απόδειξη παράδοσης – παραλαβής.

Β. Ενόψει των ανωτέρω και με βάση τα αποτελέσματα του διενεργηθέντος τακτικού ελέγχου στις εγκαταστάσεις της εταιρείας «…….», όπως αυτά αναλυτικά παρατίθενται ανωτέρω, αποδίδονται οι ακόλουθες ενδεχόμενες παραβάσεις της κείμενης νομοθεσίας σε σχέση με το απόρρητο των επικοινωνιών εκ μέρους της εταιρείας «……..»:

α) Ως προς την υποχρέωση τήρησης Ειδικού Σχεδίου Αρχείων Καταγραφής

Κατόπιν αιτήματος της Α.Δ.Α.Ε. να της παραδοθεί το «Ειδικό Σχέδιο Αρχείων Καταγραφής», όπως αυτό προβλέπεται στην παράγραφο 3.2.9 της υπ' αριθμ. 165/2011 Απόφασης της Α.Δ.Α.Ε., η εταιρεία «…...» απέστειλε το υπ΄ αριθμ. πρωτ. ΑΔΑΕ ΕΜΠ222/04.11.2016 έγγραφο, στο οποίο περιλαμβάνεται το «Ειδικό Σχέδιο Αρχείων Καταγραφής» της εταιρείας. Διαπιστώνεται ότι το εν λόγω έγγραφο περιλαμβάνει την αρχιτεκτονική και τις επιμέρους μεθόδους δημιουργίας, συλλογής, αποθήκευσης και διαχείρισης των αρχείων καταγραφής, καθώς και περιγραφή του περιεχομένου αυτών.

Απόκλιση 1: Πλην όμως, το «Ειδικό Σχέδιο Αρχείων Καταγραφής» της εταιρείας δε περιλαμβάνει τα μέτρα για τη διασφάλιση της ακεραιότητας, της εμπιστευτικότητας και της διαθεσιμότητάς των αρχείων καταγραφής, το οποίο προβλέπεται στην Ενότητα «Εισαγωγή» της πολιτικής ασφάλειας της εταιρείας (σελίδα 10 αυτής), όπως ορίζεται στην παρ. 3.2.9. της υπ' αριθμ. 165/2011 Απόφασης της Αρχής.

β) Ως προς την υλοποίηση της Πολιτικής Λογικής Πρόσβασης

Στο πλαίσιο του επιτόπιου ελέγχου, η εταιρεία «…...» ενημέρωσε ότι η πρόσβαση στις βάσεις μέσω της εφαρμογής ……. ελέγχεται μέσω firewall (….) και επέδειξε στην Ο.Ε. τον σχετικό κανόνα που αφορά στη δυνατότητα πρόσβασης στα διάφορα τμήματα της εταιρείας.

Η εφαρμογή …. έχει πρόσβαση στη βάση μέσω του χρήστη "sa". Ο κωδικός πρόσβασης του χρήστη "sa" είναι "hard coded", μη κρυπτογραφημένος, στον κώδικα του λογισμικού. Ειδικότερα, ενώ η πρόσβαση των χρηστών στην εφαρμογή …… γίνεται με χρήση προσωπικών accounts, ακολούθως, η εφαρμογή ……συνδέεται με τη βάση δεδομένων μέσω ενός κωδικού πρόσβασης που είναι εισαγμένος στον κώδικα της εφαρμογής (hard coded). Συνεπώς, ο κωδικός αυτός είναι κοινός για όλους τους χρήστες και, επιπλέον, δεν υπάρχει δυνατότητα της περιοδικής αλλαγής του. Η Ο.Ε. θεωρεί ότι η αδυναμία ασφάλειας που προκαλεί η χρήση των hard coded κωδικών πρόσβασης θα μπορούσε να μετριαστεί, εάν η hard coded πρόσβαση στη βάση δεδομένων περιοριζόταν μόνο για συγκεκριμένους χρήστες ή επιτρεπόταν μόνο από συγκεκριμένους σταθμούς εργασίας (π.χ. ορίζοντας την πρόσβαση από συγκεκριμένες IP διευθύνσεις στο Firewall), γεγονός που προβλέπεται και στην «Πολιτική ασφάλειας Δικτύου» της εταιρείας, στην οποία αναφέρεται ότι *«… επιτρέπεται μόνο η επικοινωνία των συστημάτων για τα οποία πρέπει να υπάρχει δίαυλος επικοινωνίας, και απαγορεύονται όλες οι υπόλοιπες επικοινωνίες».*

Απόκλιση 2: Πλην όμως, στην «Πολιτική Λογικής Πρόσβασης» της Πολιτικής Ασφάλειας της εταιρείας (σελ. 21 αυτής) αναφέρεται ότι για τις περιπτώσεις πρόσβασης με τη χρήση της εφαρμογής και μέσω application password database *«υπάρχει μοναδικός λογαριασμός πρόσβασης για κάθε χρήστη» και «εφαρμόζεται πολιτική αλλαγής των κωδικών πρόσβασης…»,* όπως άλλωστε προβλέπεται στις παρ. 6.2.3., 6.4.1.δ, 6.4.2.3. της υπ' αριθμ. 165/2011 Απόφασης της Α.Δ.Α.Ε..

γ) Ως προς την παράγραφο 4.2.3 της Πολιτικής Λογικής Πρόσβασης της εταιρείας

Στο πλαίσιο του επιτόπιου ελέγχου, ζητήθηκε από την εταιρεία «…….» να της παραδοθούν πρόσφατα αποτελέσματα ελέγχου της Πολιτικής Λογικής Πρόσβασης (παρ. 4.2.3 της Πολιτικής Λογικής Πρόσβασης της εταιρείας).

Η εταιρεία παρέδωσε έγγραφο με τίτλο *«ΠΑ-ΠΕΠΑΔΑΕ4-Πολιτική_Λογικής Πρόσβασης_072016»*, στο οποίο αναφέρεται ότι πραγματοποιήθηκε έλεγχος των αρχείων καταγραφής του συστήματος ……(σύστημα καταγραφής των ηχογραφημένων συνομιλιών) για το χρονικό διάστημα από 01.06.2016 έως 30.06.2016 και δειγματοληπτικός έλεγχος των αιτήσεων ενεργοποίησης πρόσβασης στο εν λόγω σύστημα για 3 υπαλλήλους της εταιρείας.

Απόκλιση 3: Πλην όμως, ο εν λόγω έλεγχος αφορά σε ένα μόνο σύστημα της εταιρείας και συνεπώς δεν καλύπτει επαρκές δείγμα των ΠΕΣ της εταιρείας. Επιπρόσθετα, στην Πολιτική Λογικής Πρόσβασης της εταιρείας (παρ. 4.2.3.) αναφέρεται ότι ο έλεγχος πραγματοποιείται σε

εξαμηνιαία βάση, γεγονός που δεν έχει εφαρμοστεί για το έτος 2016 για το σύστημα …, για το οποίο παραδόθηκε ο ανωτέρω έλεγχος. Προκύπτει συνεπώς ότι η εταιρεία «…….» δεν εφαρμόζει πλήρως τις απαιτήσεις της παρ. 6.3.2 της υπ' αριθμ. 165/2011 Απόφασης της Α.Δ.Α.Ε..

δ) Ως προς την υλοποίηση της Πολιτικής Απομακρυσμένης Λογικής Πρόσβασης

Στο πλαίσιο του επιτόπιου ελέγχου, η εταιρεία «…….» δεσμεύτηκε να παραδώσει αρχεία αναφορικά με τον έλεγχο της Πολιτικής Απομακρυσμένης Λογικής Πρόσβασης (παρ. 5.2.3.της Πολιτικής Απομακρυσμένης Λογικής Πρόσβασης της εταιρείας) έως την 23η Δεκεμβρίου 2016.
Στο σχετικό έγγραφο που παρέδωσε η εταιρεία, συνημμένο στην υπ΄αριθμ. πρωτ. ΑΔΑΕ 3196/27.12.2016 επιστολή της, περιγράφονται έλεγχοι της απομακρυσμένης λογικής πρόσβασης των συνεργατών σε ΠΕΣ κατά τις ημερομηνίες 03.03.2016, 01.04.2016, 06.06.2016, 12.08.2016, 26.10.2016 και 01.12.2016.
Απόκλιση 4: Πλην όμως, στην Πολιτική Απομακρυσμένης Λογικής Πρόσβασης της εταιρείας (παρ. 5.2.4 αυτής), αναφέρεται ότι ο έλεγχος της απομακρυσμένης λογικής πρόσβασης των συνεργατών σε ΠΕΣ *«…πραγματοποιείται μία φορά το μήνα»*.
Επιπλέον, στην παρ. 5.2.3 της Πολιτικής Απομακρυσμένης Λογικής Πρόσβασης της εταιρείας προβλέπεται ότι ανά 3 μήνες πραγματοποιείται έλεγχος των λογαριασμών απομακρυσμένης λογικής πρόσβασης των υπαλλήλων της εταιρείας, αλλά η εταιρεία δεν έχει παραδώσει στην Ο.Ε. αντίστοιχες αναφορές. Προκύπτει συνεπώς πλημμελής τήρηση εκ μέρους της εταιρείας «……..» της Πολιτικής Απομακρυσμένης Λογικής Πρόσβασης αυτής και συνακόλουθα των απαιτήσεων του άρθρου 7 της υπ' αριθμ. 165/2011 Απόφασης της Α.Δ.Α.Ε..

ε) Ως προς την εφαρμογή της απαίτησης της παρ. 8.2.3 της υπ' αριθμ. 165/2011 Απόφασης της Α.Δ.Α.Ε.

Στο πλαίσιο του επιτόπιου ελέγχου και σε συνέχεια σχετικού αιτήματος της Α.Δ.Α.Ε., η εταιρεία «…….» παρέδωσε τις Εκθέσεις που αφορούν στην εγκατάσταση και στον έλεγχο, ενδεικτικά του database server του ΠΕΣ ……., το οποίο αποτελεί το billing και reporting σύστημα της εταιρείας, καθώς και λίστα με μερικές από τις αλλαγές σε λογισμικό σε ΠΕΣ της εταιρείας. Η εταιρεία δήλωσε ότι η λίστα που παρέδωσε αποτυπώνει τις βασικές αλλαγές (π.χ. αλλαγές OS),

ενώ η εταιρεία δε διατηρεί ιστορικότητα για τις πιο λεπτομερείς αλλαγές όπως τις αναβαθμίσεις εφαρμογών και λειτουργικών συστημάτων.

Απόκλιση 5: Από τα ανωτέρω προκύπτει μη πλήρης εφαρμογή των οριζόμενων στην παράγραφο 6.1 της Πολιτικής Διαχείρισης και Εγκατάστασης ΠΕΣ της εταιρείας, κατά παράβαση συνακόλουθα της παρ. 8.2.3 της υπ' αριθμ. 165/2011 Απόφασης της Α.Δ.Α.Ε..

στ) Ως προς την εφαρμογή της απαίτησης της παρ. 8.3.3.2 της υπ' αριθμ. 165/2011 Απόφασης της Α.Δ.Α.Ε.

Στο πλαίσιο του επιτόπιου ελέγχου, η εταιρεία «.....» δήλωσε ότι στους sql servers καταγράφεται μόνο η σύνδεση (πρόσβαση), αλλά όχι οι ενέργειες. Σημειώνεται ότι η εταιρεία παρέδωσε στην ΑΔΑΕ, με το υπ΄αριθμ. πρωτ. ΑΔΑΕ ΕΜΠ222/04.11.2016 έγγραφο (σχετικό 1 αυτού υπό τον τίτλο «ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ-ΕΞΑΙΡΕΣΕΙΣ»), σχετική αδυναμία συμμόρφωσης στην οποία αναφέρεται ότι *«... δεν έχει υλοποιηθεί η καταγραφή ενεργειών που κάνουν οι χρήστες των βάσεων δεδομένων SQL server της εταιρείας κατά τη σύνδεσή τους...»*. Για την ως άνω αδυναμία συμμόρφωσης δεν παρέχεται από την εταιρεία επαρκής τεκμηρίωση, όπως προβλέπεται στην Ενότητα «Εισαγωγή» της Πολιτικής Ασφάλειας της εταιρείας, σελίδα 9 αυτής (παρ. 3.2.3. της Απόφασης 165/2011). Επιπρόσθετα, η εταιρεία δεν επικαλείται συγκεκριμένο χρονοδιάγραμμα για τη θεραπεία της. Κατά συνέπεια, η ως άνω αδυναμία συμμόρφωσης δεν δύναται να γίνει αποδεκτή από την Ο.Ε.

Απόκλιση 6: Στην Ενότητα «Πολιτική Διαχείρισης και Εγκατάστασης ΠΕΣ» της Πολιτικής Ασφάλειας της εταιρείας, σελίδα 34 αυτής, προβλέπεται ότι *«Ενέργειες στο λειτουργικό σύστημα και τις εφαρμογές των ΠΕΣ, καθώς και τα συμβάντα συστήματος ΠΕΣ καταγράφονται και διατηρούνται σε αρχείο»*. Ενόψει της μη καταγραφής των ενεργειών των χρηστών στους sql servers της εταιρείας, προκύπτει μη εφαρμογή της ανωτέρω πρόβλεψης της Πολιτικής Ασφάλειας της εταιρείας και συνακόλουθα παραβίαση της απαίτησης της παρ. 8.3.3.2 της υπ' αριθμ. 165/2011 Απόφασης της Α.Δ.Α.Ε.. Η δε υποβολή της συγκεκριμένης αδυναμίας συμμόρφωσης ως εξαίρεση, δυνάμει της παρ. 3.2.3 της υπ' αριθμ. 165/2011 Απόφασης της Αρχής, αφενός υπεβλήθη το πρώτον ενόψει του τακτικού ελέγχου και όχι στο χρόνο υποβολής της Πολιτικής Ασφάλειας προς έγκριση στην Α.Δ.Α.Ε., αφετέρου, δεν παρέχει επαρκή τεκμηρίωση, όπως προαναφέρθηκε.

ζ) Ως προς την παρ. 9.1 της Πολιτικής Ασφάλειας της εταιρείας (Πολιτική Ελέγχου Εφαρμογής της Πολιτικής Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών)

Στο πλαίσιο του επιτόπιου ελέγχου, η εταιρεία «…….» δήλωσε ότι ο έλεγχος εφαρμογής της πολιτικής ασφάλειας πραγματοποιείται από εξωτερική εταιρεία σε ετήσια βάση και ότι θα παραδώσει προγραμματισμό και αποτελέσματα ελέγχων για το έτος 2015 έως την 23η Δεκεμβρίου 2016. Με την υπ΄αριθμ. πρωτ. ΑΔΑΕ 3196/27.12.2016 επιστολή, η εταιρεία παρέδωσε αρχείο ετήσιου ελέγχου. Από τη μελέτη του ως άνω εγγράφου, η Ο.Ε. διαπίστωσε τα ακόλουθα:

- Δεν είναι ξεκάθαρη η ημερομηνία σύνταξης του εν λόγω εγγράφου, δεδομένου ότι αναφέρονται 2 διαφορετικές ημερομηνίες (8/3/2016 και 15/2/2015)
- Δεν περιλαμβάνονται τα συστήματα (ΠΕΣ) που ελέγχθηκαν ως προς την ορθή τήρηση των επιμέρους πολιτικών και διαδικασιών, καθώς και η συλλογή των απαιτούμενων πληροφοριών και δεδομένων που οδήγησαν στα αναφερόμενα αποτελέσματα
- Δεν περιλαμβάνονται αποτελέσματα ελέγχων για την εύρεση τεχνικών ευπαθειών στα ΠΕΣ (penetration tests)
- Δεν περιλαμβάνεται χρονοδιάγραμμα διεξαγωγής του ελέγχου

Απόκλιση 7: Πλην όμως, στην ενότητα 9 της Πολιτικής Ασφάλειας της εταιρείας (Άρθρο 11 της Απόφασης 165/2011), προβλέπεται ότι *«… προγραμματίζεται έλεγχος εφαρμογής της Πολιτικής Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών, καταγράφεται σε αρχείο, καλύπτει όλο το εύρος της Πολιτικής και πραγματοποιείται κατ΄ελάχιστον ανά 2 έτη…».* Προκύπτει συνεπώς πλημμελής τήρηση των οριζόμενων στην παρ. 9.1. της Πολιτικής Ασφάλειας της εταιρείας, όπως άλλωστε προβλέπεται και στην παρ. 11.3 της υπ' αριθμ. 165/2011 Απόφασης της Α.Δ.Α.Ε..

Γ. Κατόπιν των παραπάνω, 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. Το 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. Το 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. Την υπ' αριθμ. πρωτ. ΑΔΑΕ ΕΜΠ 145/17-05-2012 Πολιτική Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών της εταιρείας «……..», όπως αυτή αναθεωρήθηκε με το υπ' αριθμ. πρωτ. ΑΔΑΕ ΕΜΠ 33/07-03-2013 έγγραφο και τελικώς εγκρίθηκε με την υπ' αριθμ. 162/2013 Απόφαση της Α.Δ.Α.Ε.,

16. Την υπ' αριθμ. 59/2016 Απόφαση της Α.Δ.Α.Ε. σχετικά με τη διενέργεια τακτικού ελέγχου στην εταιρεία «…...»,

17. Την υπ' αριθμ. 291/2016 Απόφαση του Προέδρου της Α.Δ.Α.Ε. σχετικά με τη σύσταση της Ομάδας Ελέγχου για τη διενέργεια τακτικού ελέγχου στην εταιρεία «…...»,

18. το Πρακτικό Διενέργειας Επιτόπιου Ελέγχου στις εγκαταστάσεις της εταιρείας «…….», με αριθμ. πρωτ. ΑΔΑΕ ΕΜΠ 212/24-10-2016,

19. το Πρακτικό Διενέργειας Επιτόπιου Ελέγχου στις εγκαταστάσεις της εταιρείας «…….», με αριθμ. πρωτ. ΑΔΑΕ ΕΜΠ 249/05-12-2016,

20. το Πρακτικό Διενέργειας Επιτόπιου Ελέγχου στις εγκαταστάσεις της εταιρείας «...», με αριθμ. πρωτ. ΑΔΑΕ ΕΜΠ 262/12-12-2016,

21. Την υπ' αριθμ. πρωτ. ΑΔΑΕ ΕΜΠ 222/04-11-2016 επιστολή της εταιρείας «…..» προς την Α.Δ.Α.Ε.,

22. Την υπ' αριθμ. πρωτ. ΑΔΑΕ 3196/27-12-2016 επιστολή της εταιρείας «…» προς την Α.Δ.Α.Ε.,

23. Την υπ' αριθμ. πρωτ. ΑΔΑΕ 610/28-02-2017 επιστολή της εταιρείας «….» προς την Α.Δ.Α.Ε.,

24. την από 10.03.2017 «Έκθεση Διενέργειας Τακτικού Ελέγχου στις εγκαταστάσεις της εταιρείας …...» με τα συνημμένα αυτής,

25. Την υπ' αριθμ. 149/2017 Εισήγηση προς την Ολομέλεια της Α.Δ.Α.Ε.,

26. Το πρακτικό της από 5 Απριλίου 2017 συνεδρίασης της Ολομέλειας της Α.Δ.Α.Ε.,

27. Την υπ' αριθμ. 134/2017 Απόφαση της Α.Δ.Α.Ε. περί έγκρισης της ως άνω από 10-03-2017 Έκθεσης διενέργειας τακτικού ελέγχου στην εταιρεία «……..», η οποία παραδόθηκε στην εταιρεία «……», μετά της οικείας έκθεσης ελέγχου, όπως προκύπτει από την υπ' αριθμ. πρωτ. ΑΔΑΕ 2510/06-09-2017 Απόδειξη παράδοσης – παραλαβής,

28. Την υπ' αριθμ. 414/2017 εισήγηση προς την Ολομέλεια της Α.Δ.Α.Ε.,

29. Το υπ' αριθμ. 92 πρακτικό της από 22 Νοεμβρίου 2017 συνεδρίασης της Ολομέλειας της Α.Δ.Α.Ε.,

30. Την ανάγκη διασφάλισης του απορρήτου των επικοινωνιών,

Η ΑΡΧΗ ΔΙΑΣΦΑΛΙΣΗΣ ΤΟΥ ΑΠΟΡΡΗΤΟΥ ΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ (ΑΔΑΕ)
ΑΠΟΦΑΣΙΖΕΙ

την κλήση σε Ακρόαση της εταιρείας με την επωνυμία «…..», ενώπιον της Ολομέλειας της Α.Δ.Α.Ε., την **4η Ιουλίου 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 και Β της παρούσας.

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

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

Κρίθηκε και αποφασίστηκε την 22α Νοεμβρίου 2017.

Ο Πρόεδρος

Χρήστος Ζαμπίρας