Μαρούσι, 3 Απριλίου 2017
Αρ. πρωτ.:1029
ΑΝΑΡΤΗΤΕΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

ΑΠΟΦΑΣΗ

(αριθμ: 108/2017)

Θέμα: Κλήση 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), σχετικά με τις αποκλίσεις από την εγκεκριμένη με την υπ' αριθμ. 235/2013 απόφαση της Α.Δ.Α.Ε. Πολιτική Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών της εταιρείας, όπως αυτές αναφέρονται στην από 15 Φεβρουαρίου 2016 Έκθεση Διενέργειας τακτικού Ελέγχου στην εν λόγω εταιρεία.

Την Τετάρτη, 15η Μαρτίου 2017, η Ολομέλεια της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών, παρισταμένων του Προέδρου της Αρχής κ. Χρήστου Ζαμπίρα, του Αντιπροέδρου κ. Μιχαήλ Σακκά, καθώς και των τακτικών μελών κ.κ. Μιχαήλ Γεωργιακόδη, Γεωργίου Μπακάλη, Παναγιώτη Ριζομυλιώτη και Αικατερίνης Παπανικολάου και απόντος του τακτικού μέλους κου Ιωάννη Ασκοξυλάκη, ο οποίος δεν παρέστη λόγω κωλύματος, αν και είχε νομίμως και εμπροθέσμως προσκληθεί, προς αναπλήρωση του οποίου παρέστη το αναπληρωματικό μέλος αυτού, κος Δημοσθένης Βουγιούκας, 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. 235/2013 απόφαση της Α.Δ.Α.Ε. Πολιτική Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών της εταιρείας, όπως αυτές αναφέρονται στην από 15 Φεβρουαρίου 2016 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.

Α. Σύμφωνα με την από 15 Φεβρουαρίου 2016 Έκθεση Διενέργειας τακτικού Ελέγχου αναφορικά με την εφαρμογή της Πολιτικής διασφάλισης του απορρήτου των επικοινωνιών στην εταιρεία «……» παρατηρήθηκαν αποκλίσεις από την Πολιτική Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών της ως άνω εταιρείας, όπως αυτή εγκρίθηκε με την υπ' αριθμ. 235/2013 Απόφαση της Α.Δ.Α.Ε.. Τα αποτελέσματα του τακτικού ελέγχου έχουν ως εξής :

«Γ. ΕΞΕΤΑΣΗ ΤΩΝ ΣΤΟΙΧΕΙΩΝ – ΑΠΟΤΕΛΕΣΜΑΤΑ ΤΟΥ ΕΛΕΓΧΟΥ

Η Ο.Ε. κατά τους επιτόπιους ελέγχους αλλά και από την εξέταση των στοιχείων που παρέλαβε έλεγξε δειγματοληπτικά την εφαρμογή της εγκριθείσας Πολιτικής Ασφάλειας για τη Διασφάλιση του Απορρήτου των επικοινωνιών. Ειδικότερα, έλεγξε συγκεκριμένα σημεία των επιμέρους πολιτικών και διαδικασιών όπως αναλύεται παρακάτω:

1. **Συμμόρφωση με τις παρατηρήσεις που περιλαμβάνονται στην από 25.07.2013 Έκθεση Ελέγχου Συμμόρφωσης Πολιτικής (συνημμένη στην υπ' αριθμ. 235/2013 Απόφαση της ΑΔΑΕ με αρ. πρωτ. ΑΔΑΕ 1810/04.09.2013).**

   - Η πρώτη παρατήρηση αφορούσε στη μη διατήρηση των αρχείων των παραγράφων 6.5.1. και 6.5.4 του άρθρου 6 της Απόφασης 165/2011. Από την εξέταση της Πολιτικής Ασφάλειας της εταιρείας (Έκδοση 3η, συνημμένο στην επιστολή 1960/21.09.2015), η Ο.Ε. διαπίστωσε ότι η εταιρεία έχει καλύψει τις παραπάνω απαιτήσεις στην ενότητα 4.5 της Πολιτικής Τοπικής και Απομακρυσμένης Λογικής Πρόσβασης.

   - Η δεύτερη παρατήρηση αφορούσε στη μη καταγραφή και τήρηση αρχείου με τα αποτελέσματα δοκιμών που περιγράφεται στην παράγραφο 8.3.2.1 του άρθρου 8 της Απόφασης 165/2011. Από την εξέταση της Πολιτικής Ασφάλειας της εταιρείας (Έκδοση 3η, συνημμένο στην επιστολή 1960/21.09.2015), η Ο.Ε. διαπίστωσε ότι η εταιρεία έχει καλύψει την παραπάνω απαίτηση στην ενότητα 5.2 της Πολιτικής Διαχείρισης και Εγκατάστασης ΠΕΣ.

   - Η τρίτη παρατήρηση αφορούσε στις απαιτήσεις των παραγράφων 8.3.3.1, 8.3.3.2 και 8.3.4.2 του άρθρου 8 της Απόφασης 165/2011. Από την εξέταση της Πολιτικής Ασφάλειας της εταιρείας (Έκδοση 3η, συνημμένο στην επιστολή 1960/21.09.2015), η Ο.Ε. διαπίστωσε ότι η εταιρεία έχει καλύψει τις απαιτήσεις των παραγράφων 8.3.3.1 και 8.3.3.2 στην ενότητα 5.3 και της παραγράφου 8.3.4.2 στην ενότητα 5.4 της Πολιτικής Διαχείρισης και Εγκατάστασης ΠΕΣ.

   - Η τέταρτη παρατήρηση αφορούσε ότι στις απαιτήσεις της παραγράφου 12.2.3 του άρθρου 12 της Απόφασης 165/2011. Από την εξέταση της Πολιτικής Ασφάλειας της εταιρείας (Έκδοση 3η, συνημμένο στην επιστολή 1960/21.09.2015), η Ο.Ε. διαπίστωσε ότι η εταιρεία έχει καλύψει την παραπάνω απαίτηση στην ενότητα 9.1 της Πολιτικής Προστασίας από Κακόβουλο Λογισμικό.

2. **Γενική Παρατήρηση**

Η εταιρεία στην Πολιτική Ασφάλειας για τη διασφάλιση του Απορρήτου των Επικοινωνιών και στις Διαδικασίες παραπέμπει σε άλλα έγγραφα (Διαδικασίες, Οδηγίες) για τα οποία αναφέρει ότι περιέχουν διάφορα στοιχεία (μέτρα ασφάλειας, μεθοδολογίες, κτλ) υλοποίησης της Πολιτικής ή συμμόρφωσης με τις απαιτήσεις της Απόφασης 165/2011. Ωστόσο, σε αρκετά από αυτά τα έγγραφα είτε δεν αναφέρονται τα απαραίτητα στοιχεία είτε είναι ελλιπή. Πιο συγκεκριμένα, τα παραπάνω διαπιστώθηκαν στις ακόλουθες περιπτώσεις:

α. Στο κεφάλαιο της Τοπικής και Απομακρυσμένης Λογικής Πρόσβασης γίνεται συχνά παραπομπή στο έγγραφο «Πολιτική Ελέγχου Πρόσβασης/ Access Control Policy (ACP)» αναφορικά με την υλοποίηση συγκεκριμένων απαιτήσεων. Από την εξέταση του εν λόγω εγγράφου διαπιστώθηκε ότι δεν περιλαμβάνει καμία αναφορά σχετικά με την υλοποίηση των παραπάνω απαιτήσεων.

β. Στο κεφάλαιο Διαχείριση και Εγκατάσταση ΠΕΣ γίνεται παραπομπή στο έγγραφο «Διαδικασία Διαχείρισης και Εγκατάστασης ΠΕΣ (ΔΑΠ-2)». Από την εξέταση της διαδικασίας διαπιστώθηκε ότι παραπέμπει με τη σειρά της στο έγγραφο «Οδηγία Λειτουργίες Τμήματος Πληροφορικής (Ο-3)» στο οποίο δεν υπάρχουν όλες οι πληροφορίες που αναφέρονται στη διαδικασία.

γ. Στο κεφάλαιο της Ασφάλειας Δικτύου γίνεται παραπομπή στο έγγραφο «Οδηγία Λειτουργίες Τμήματος Πληροφορικής (Ο-3)» στο οποίο δεν καλύπτονται οι αναφορές της παραγράφου 7.1 του εν λόγω κεφαλαίου της Πολιτικής Ασφάλειας.

δ. Στο κεφάλαιο Έλεγχος Εφαρμογής Πολιτικής Ασφάλειας γίνεται συχνά παραπομπή στο έγγραφο «Διαδικασία Ελέγχων και Εσωτερικών Επιθεωρήσεων (ΔΑΠ-5)». Από την εξέταση του εγγράφου διαπιστώθηκε ότι δεν καλύπτεται η μεθοδολογία προγραμματισμού ελέγχων (παράγραφος 8.1 της Πολιτικής) και η μεθοδολογία σχεδιασμού, υλοποίησης και τεκμηρίωσης ελέγχων και εσωτερικών επιθεωρήσεων (παράγραφος 8.2 της Πολιτικής).

ε. Στο κεφάλαιο Προστασία από Κακόβουλο Λογισμικό γίνεται παραπομπή στο έγγραφο «Οδηγία Λειτουργίες Τμήματος Πληροφορικής (Ο-3)». Στο σημείο Α.10.3.1 της Οδηγίας στο οποίο περιλαμβάνονται οι έλεγχοι για κακόβουλο λογισμικό και στο σημείο Α.10.3.2 στο οποίο αναφέρονται οι έλεγχοι για μεταφερόμενο κώδικα δεν καταγράφονται οι λεπτομέρειες εφαρμογής των απαιτήσεων της παραγράφου 9.1 του εν λόγω κεφαλαίου.

Η εταιρεία οφείλει να συμπληρώσει τα έγγραφα (Διαδικασίες, Οδηγίες) ώστε να περιλαμβάνουν την υλοποίηση των απαιτήσεων της Πολιτικής Ασφάλειας.

3. Γενικές Απαιτήσεις Ασφάλειας

1.2 Διαδικασία Ελέγχου Εξαιρέσεων

Η εταιρεία αναφέρει στη Διαδικασία Ελέγχου (παράγραφο 1.2) ότι στη Διαδικασία Ελέγχων και Εσωτερικών Επιθεωρήσεων (ΔΑΠ-5) (περιλαμβάνεται στο συνημμένο 2 του σχετικού 3) περιλαμβάνεται η μεθοδολογία για την αναγνώριση, καταγραφή και διαχείριση των περιπτώσεων εξαιρέσεων που μπορεί να προκύψουν σε μελλοντική έκδοση της Π.Α.

Απόκλιση 1: Η εταιρεία στη Διαδικασία Ελέγχων και Εσωτερικών Επιθεωρήσεων (ΔΑΠ-5) δεν περιλαμβάνει τη μεθοδολογία για την αναγνώριση, καταγραφή και διαχείριση των περιπτώσεων εξαιρέσεων που μπορεί να προκύψουν σε μελλοντική έκδοση της Π.Α., όπως αναφέρει στην παράγραφο 1.2 με τίτλο Διαδικασία Ελέγχου Εξαιρέσεων (παράγραφος 3.2.3 του άρθρου 3 της Απόφασης 165/2011).

Αναφορικά με τις εξαιρέσεις, η εταιρεία δήλωσε, στην υπ' αριθμ. πρωτ. ΑΔΑΕ 2621/16.11.2015 επιστολή, τις εξαιρέσεις από την Πολιτική Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών. Στις εξαιρέσεις που δηλώνει η εταιρεία καταγράφεται η αιτιολόγηση για την αδυναμία συμμόρφωσης, ωστόσο διαπιστώθηκαν τα ακόλουθα:

- Για την εξαίρεση αναφορικά με το κοινό account για πρόσβαση στο WebAdmin από την εταιρεία call center για τηλεφωνική υποστήριξη των χρηστών των υπηρεσιών της:
  - Σχετικά με τους κοινούς ή προκαθορισμένους λογαριασμούς υπάρχει η πρόβλεψη στην παράγραφο 6.2.3 της Απόφασης 165/2011 ότι στην περίπτωση που δεν είναι η εφικτή η αποφυγή τέτοιων λογαριασμών τότε θα πρέπει να δικαιολογείται και να εξασφαλίζεται η αντιστοίχιση του συγκεκριμένου φυσικού προσώπου που αποκτά πρόσβαση σε ένα ΠΕΣ με τις ενέργειες που τελούνται σε αυτό. Η εταιρεία αιτιολογεί μεν την ύπαρξη του συγκεκριμένου κοινού λογαριασμού για πρόσβαση στο WebAdmin από την εξωτερική εταιρεία call center για τηλεφωνική υποστήριξη των χρηστών των υπηρεσιών της εταιρείας, δεν αναφέρει όμως κανέναν μηχανισμό για αντιστοίχιση του φυσικού προσώπου που αποκτά πρόσβαση μέσω αυτού του λογαριασμού.
- Για την εξαίρεση αναφορικά με τη μόνιμη απομακρυσμένη πρόσβαση στα ΠΕΣ:
  - Η εταιρεία δήλωσε ότι δεν μπορεί να εφαρμόσει το μοντέλο αίτησης/έγκρισης για απομακρυσμένη πρόσβαση στα συστήματα της όπως αναφέρεται στην παράγραφο 7.2 της Απόφασης 165/2011 αφού η πρόσβαση στα εν λόγω συστήματα από τους τεχνικούς της εταιρείας επιβάλλεται να είναι συχνή και συνεχής για λόγους monitoring και επίλυσης προβλημάτων σε πραγματικό χρόνο όπως απαιτείται επιχειρησιακά. Επίσης, η εταιρεία στο πλαίσιο του από 08.10.2015 επιτόπιου ελέγχου δήλωσε ότι στις εγκαταστάσεις της εταιρείας δεν φιλοξενούνται ΠΕΣ, αλλά βρίσκονται όλα στην ……..και για επιχειρησιακούς λόγους πρέπει να υπάρχει μόνιμη πρόσβαση, επομένως η απαίτηση σχετικά με τη διάρκεια

ισχύος των λογαριασμών για την απομακρυσμένη πρόσβαση (παράγραφος 4.6) δεν μπορεί να εφαρμοστεί.

Η αιτιολόγηση της εταιρείας για την αδυναμία εφαρμογής των απαιτήσεων των παραγράφων 7.2.6 και 7.2.7 της Απόφασης 165/2011, για τους εργαζόμενους της εταιρείας, θεωρείται επαρκής.

1.5 Διαδικασία Διαχείρισης Πολιτικής Ασφάλειας

Η εταιρεία παρέδωσε το έγγραφο «Διαδικασία Διαχείρισης Εγγράφων και Αρχείων (Δ-2)» (περιλαμβάνεται στο συνημμένο 2 του σχετικού 3). Από την εξέταση της Διαδικασίας (Δ-2) διαπιστώθηκε ότι δεν περιλαμβάνονται σε αυτήν η αρχιτεκτονική, οι μέθοδοι δημιουργίας, συλλογής, αποθήκευσης και διαχείρισης των αρχείων καταγραφής, το περιεχόμενό τους και τα μέτρα διασφάλισης της ακεραιότητας, της εμπιστευτικότητας και της διαθεσιμότητάς τους, σύμφωνα με την παράγραφο 1.5 της Πολιτικής Ασφάλειας της εταιρείας.

Απόκλιση 1: Δεν εφαρμόζεται η παράγραφος 1.5 αναφορικά με το περιεχόμενο της Διαδικασίας Διαχείρισης Εγγράφων και Αρχείων (Δ-2) διότι δεν περιλαμβάνονται τα στοιχεία που αφορούν το ειδικό σχέδιο αρχείων καταγραφής (παράγραφος 3.2.9 του άρθρου 3 της Απόφασης 165/2011).

1.6 Διαδικασία Αποτίμησης Πληροφοριακού Κινδύνου

Η εταιρεία παρέδωσε τη Διαδικασία Αποτίμησης Πληροφοριακού Κινδύνου (ΔΑΠ-1) (περιλαμβάνεται στο συνημμένο 2 του σχετικού 3) στην οποία περιγράφεται η μεθοδολογία αποτίμησης του πληροφοριακού κινδύνου και αναφέρονται τα αρχεία τα οποία τηρούνται.

Η Ο.Ε. έλεγξε τις Αναφορές Αποτίμησης Πληροφοριακού Κινδύνου (Έντυπα Ε-16) και διαπίστωσε ότι έχουν πραγματοποιηθεί οι ενέργειες, και έχουν καταγραφεί τα αποτελέσματα αυτών, που ορίζονται στην σχετική διαδικασία. Ωστόσο, δεν είναι σαφή στα εν λόγω έντυπα Ε-16 ποια είναι η αντιστοίχιση των Πόρων με τα ΠΕΣ της εταιρείας, εάν έχει πραγματοποιηθεί η Αποτίμηση Κινδύνου για το σύνολο των ΠΕΣ, καθώς και το μέτρο – δείκτης κάθε πιθανού κινδύνου επί των ΠΕΣ.

Παρατήρηση 1: Η εταιρεία οφείλει να αποτυπώνει με μεγαλύτερη σαφήνεια στις Αναφορές Αποτίμησης Πληροφοριακού Κινδύνου (Έντυπα Ε-16) τα ΠΕΣ για τα οποία έχει πραγματοποιήσει Αποτίμηση Κινδύνου καθώς και το μέτρο – δείκτης κάθε πιθανού κινδύνου επί αυτών.

4. Αποδεκτή Χρήση (Άρθρο 4 της Απόφασης 165/2011, ΦΕΚ 2715/Β/17.11.2011)

2.2 Πολιτική Αποδεκτής Χρήσης για τους συνεργάτες

Η εταιρεία παρέδωσε τα παρακάτω έγγραφα αναφορικά με τους συνεργάτες:

1. Σύμβαση που έχει συνάψει με την εταιρεία …….. (συνημμένο 2 του σχετικού 4). Η εταιρεία δήλωσε ότι δεν έχει απευθείας σύμβαση με τη ……., στην οποία φιλοξενούνται τα ΠΕΣ, αλλά με την εταιρεία …….
2. Τους Όρους (Terms and Conditions) και το Service Level Agreement (SLA, συνημμένο 7 του σχετικού 4) με την εταιρεία ……. (Data Center στην ……..).
3. Σύμβαση που έχει συνάψει με την εταιρεία …… (call center) για την εξυπηρέτηση των πελατών της (συνημμένο 4 του σχετικού 5).
4. Σύμβαση που έχει συνάψει με την εταιρεία ……. (συνημμένο 6 του σχετικού 4).

Από την εξέταση των παραπάνω εγγράφων διαπιστώθηκε ότι δεν περιλαμβάνονται σε αυτά οι όροι σχετικά με τους συνεργάτες που ορίζονται στην παράγραφο 2.2 της Πολιτικής Αποδεκτής χρήσης.

Απόκλιση 2: Δεν εφαρμόζεται η παράγραφος 2.2 αναφορικά με το ελάχιστο περιεχόμενο των συμβάσεων με τους συνεργάτες (παράγραφος 4.3.2 του Άρθρου 4 της Απόφασης 165/2011)

5. Φυσική Ασφάλεια και Πρόσβαση (Άρθρο 5 της Απόφασης 165/2011, ΦΕΚ 2715/Β/17.11.2011)

3.1 Φυσική Ασφάλεια και Πρόσβαση σε ΠΕΣ

Η εταιρεία παρέδωσε ως Διαδικασία Φυσικής Πρόσβασης το έγγραφο «Πολιτική Ελέγχου Πρόσβασης / Access Control Policy – ACP» (περιλαμβάνεται στο συνημμένο 2 του σχετικού 3).

3.2 Ασφαλείς Χώροι Εγκαταστάσεων

Η εταιρεία παρέδωσε αρχείο καταγραφής προσβάσεων των επισκεπτών στους χώρους της εταιρείας (περιλαμβάνεται στο συνημμένο 2 του σχετικού 3). Από την εξέταση των καταγραφών διαπιστώθηκε ότι καταγράφονται η ημερομηνία, η ώρα, το όνομα του επισκέπτη, ο σκοπός της επίσκεψης και ο υπεύθυνος έγκρισης.

Πολιτική Ελέγχου Πρόσβασης – ACP

Η εταιρεία παρέδωσε:

- τον κατάλογο με τα πρόσωπα που έχουν εξουσιοδοτηθεί για πρόσβαση στο χώρο του Data Center στην …… (συνημμένο 1 του σχετικού 4).
- το αρχείο καταγραφής των προσβάσεων στο χώρο της …….. (συνημμένο 1 του σχετικού 5).

Από τον έλεγχο των παραπάνω αρχείων διαπιστώθηκε ότι οι καταγεγραμμένες προσβάσεις στο χώρο στη …… πραγματοποιήθηκαν από πρόσωπο που έχει εξουσιοδοτηθεί.

6. Τοπική και Απομακρυσμένη Λογική Πρόσβαση (Άρθρα 6 και 7 της Απόφασης 165/2011, ΦΕΚ 2715/Β/17.11.2011)

4.2 Λογαριασμοί Πρόσβασης Χρηστών ΠΕΣ

Η εταιρεία παρέδωσε το αρχείο στο οποίο καταγράφονται τα πρόσωπα, οι λογαριασμοί που τους αντιστοιχούν, οι ομάδες χρηστών και τα δικαιώματα πρόσβασης των λογαριασμών στα ΠΕΣ (συνημμένο 3 του σχετικού 4). Η Ο.Ε. διαπίστωσε, κατά τον επιτόπιο έλεγχο, ότι όλοι οι χρήστες που αναφέρονται στο παραπάνω αρχείο έχουν σε κάθε σύστημα διαχειριστικές δυνατότητες, αφού η εταιρεία δήλωσε ότι, λόγω των αδειών που έχει αγοράσει από την εταιρεία ……για τη χρήση των terminal services, της επιτρέπεται μόνο να δημιουργεί χρήστες που έχουν το προφίλ του διαχειριστή. Μετά από σχετικό ερώτημα της Ο.Ε., η εταιρεία δήλωσε ότι θα χρειαζόταν επιπλέον άδεια από την εταιρεία ……, ώστε οι χρήστες να συνδέονται μέσω terminal services με απλά και ξεχωριστά δικαιώματα χρήστη. Επίσης, η εταιρεία, στην υπ' αριθμ. πρωτ. ΑΔΑΕ 2621/16.11.2015 επιστολή, συμπεριέλαβε την περίπτωση αυτή ως εξαίρεση δηλώνοντας επιπλέον ότι για να έχει remote access ο χρήστης χωρίς δικαιώματα admin απαιτείται αγορά άδειας της οποίας το κόστος δεν δικαιολογεί ο μειωμένος κίνδυνος που διατρέχεται.

Από την εξέταση του σχετικού αρχείου διαπιστώθηκε, επιπλέον, ότι δεν είναι σαφή τα δικαιώματα πρόσβασης για κάθε λογαριασμό.

Παρατήρηση 2: Η εταιρεία οφείλει να αποδίδει στον κάθε εργαζόμενο εκείνα τα δικαιώματα πρόσβασης που του είναι απαραίτητα σύμφωνα με την εργασία του.

Παρατήρηση 3: Η εταιρεία οφείλει να καταγράψει με σαφήνεια τα δικαιώματα πρόσβασης των λογαριασμών των χρηστών σε κάθε ΠΕΣ σύμφωνα με την παράγραφο 4.2 της Πολιτικής Ασφάλειας της εταιρείας (παράγραφος 6.2.4 του άρθρου 6 της Απόφασης 165/2011).

Αναφορικά με το αρχείο καταγραφής προσβάσεων στα ΠΕΣ, η εταιρεία δήλωσε ότι έχει ενεργοποιήσει μόνο σε επίπεδο Windows τη διατήρηση των login/logout των χρηστών. Η εταιρεία δήλωσε ότι ο χρόνος διατήρησης των εν λόγω εγγραφών εξαρτάται από το rotation που κάνει ο event logger και η Ο.Ε. διαπίστωσε ότι τα εν λόγω log files διατηρούνται από 10.03.2015. Επίσης, η εταιρεία δήλωσε ότι με χρήση του …….. καταγράφει τις προσβάσεις καθώς και τις ενέργειες σε επίπεδο Windows και παρέδωσε screenshots από την εν λόγω εφαρμογή (συνημμένο 5 του από 20.10.2015 Πρακτικού Διενέργειας Επιτόπιου Ελέγχου). Η εταιρεία δήλωσε ότι οι προσβάσεις καθώς και οι ενέργειες των χρηστών και πελατών που εισέρχονται στην πλατφόρμα WebAdmin καταγράφονται και διατηρούνται για 2 χρόνια.

Απόκλιση 3: Δεν εφαρμόζεται η παράγραφος 1.5 των Γενικών Απαιτήσεων αναφορικά με το χρόνο διατήρησης για 2 έτη των αρχείων καταγραφής προσβάσεων των χρηστών σε επίπεδο Windows σε όλα τα ΠΕΣ (παράγραφος 3.2.8 του άρθρου 3 της Απόφασης 165/2011).

Αναφορικά με τις προσβάσεις σε δεδομένα επικοινωνίας των συνδρομητών η εταιρεία δήλωσε ότι τα συστήματα που διατηρούν δεδομένα επικοινωνίας είναι οι βάσεις, ……., ……., …….. και ……..

και διατηρεί μόνο τα Login/logout σε επίπεδο Windows, χωρίς τις αντίστοιχες αιτιολογήσεις. Στη συνέχεια, στο πλαίσιο του από 20.10.2015 επιτόπιου ελέγχου, η εταιρεία δήλωσε ότι οι προσβάσεις των χρηστών της εταιρείας στο σύνολο των βάσεων δεδομένων καταγράφονται με χρήση του λογισμικού ……., το οποίο διατηρεί τις εν λόγω ενέργειες για 2 χρόνια.

Απόκλιση 4: Η εταιρεία δεν εφαρμόζει την παράγραφο 4.2 της Πολιτικής Ασφάλειας αναφορικά με την αιτιολόγηση των προσβάσεων στα δεδομένα επικοινωνίας (παράγραφος 6.2.6 του άρθρου 6 της Απόφασης 165/2011).

Αναφορικά με την πρόσβαση των πελατών στο WebAdmin μέσω https, η εταιρεία δήλωσε ότι οι πελάτες της εισέρχονται στη συγκεκριμένη εφαρμογή, την οποία έχει αναπτύξει η εταιρεία, και βλέπουν στατιστικά στοιχεία. Αναφορικά με το MSIDN οι πελάτες βλέπουν μόνο τα 3 τελευταία ψηφία του αριθμού. Η εταιρεία παρέδωσε τη λίστα με τους λογαριασμούς των πελατών και τα δικαιώματα πρόσβασης αυτών (συνημμένο 3 του από 20.10.2015 Πρακτικού Διενέργειας Επιτόπιου Ελέγχου). Αναφορικά με την εν λόγω λίστα, οι λογαριασμοί με κόκκινο έχουν πρόσβαση στο πλήρες MSIDN.

Από την εξέταση του καταλόγου των χρηστών που έχουν πρόσβαση στο Webadmin (συνημμένο 3 του σχετικού χ) διαπιστώθηκε ότι οι λογαριασμοί χρηστών της ……..: «…..», «…..», «……», «……», «……..» και «….» δεν περιλαμβάνονται στο αρχείο στο οποίο καταγράφονται τα πρόσωπα, οι λογαριασμοί που τους αντιστοιχούν, οι ομάδες χρηστών και τα δικαιώματα πρόσβασης των λογαριασμών στα ΠΕΣ (συνημμένο 3 του σχετικού 4)

Η εταιρεία παρέδωσε κατάλογο των ενεργών λογαριασμών για τα υποσυστήματα ……..,…….. και …… που ανήκουν στο ΠΕΣ …….. και για το υποσύστημα …… που ανήκει στο ΠΕΣ …….(συνημμένο 4 του σχετικού 4). Από την εξέταση αυτού του αρχείου διαπιστώθηκε ότι ο χρήστης με όνομα χρήστη «……..» ενώ έχει πρόσβαση στο σύστημα ……., ως ενεργός λογαριασμός, δεν έχει εξουσιοδοτηθεί να έχει πρόσβαση στο ……, όπως φαίνεται στο αρχείο στο οποίο καταγράφονται τα πρόσωπα, οι λογαριασμοί που τους αντιστοιχούν, οι ομάδες χρηστών και τα δικαιώματα πρόσβασης των λογαριασμών στα ΠΕΣ (συνημμένο 3 του σχετικού 4).

Παρατήρηση 4: Η εταιρεία οφείλει να συμπληρώνει με ακρίβεια και να ενημερώνει αμελλητί το αρχείο στο οποίο καταγράφονται τα πρόσωπα, οι λογαριασμοί που τους αντιστοιχούν, οι ομάδες χρηστών και τα δικαιώματα πρόσβασης των λογαριασμών στα ΠΕΣ.

4.3 Διαχείριση Χρηστών ΠΕΣ και Λογαριασμών

Σχετικά με τις εγκρίσεις για την εισαγωγή και διαγραφή χρηστών, καθώς και για τη μεταβολή των δικαιωμάτων και επιπέδων πρόσβασης, η εταιρεία δήλωσε ότι δεν υπάρχει το αντίστοιχο αρχείο, δεδομένου ότι από το χρόνο ισχύος της Πολιτικής της, δεν υπήρξε σχετική ενέργεια. Για το λόγο αυτό,

η εταιρεία παρέδωσε την ανασκόπηση λογαριασμών λογικής πρόσβασης των χρηστών με ημερομηνία 12.10.2015 (συνημμένο 2 του σχετικού 5).

Όσον αφορά στη δημιουργία των κωδικών ασφάλειας, η εταιρεία δήλωσε ότι έχουν υλοποιηθεί να επιβάλλονται αυτοματοποιημένα σε κάθε ΠΕΣ μέσω Domain Controller ο οποίος επιβάλλει τους κανόνες δημιουργίας και αλλαγής των κωδικών ασφαλείας και παρέδωσε εκτύπωση οθόνης με τους κανόνες (συνημμένο 5 του σχετικού 4). Από την εξέταση του αρχείου διαπιστώθηκε ότι τηρούνται οι κανόνες δημιουργίας των κωδικών ασφάλειας.

4.6 Απαιτήσεις για την Απομακρυσμένη Λογική Πρόσβαση

Η εταιρεία δήλωσε το αρχείο με τα ΠΕΣ στα οποία επιτρέπεται η απομακρυσμένη πρόσβαση και τους τρόπους με τους οποίους υλοποιείται είναι το ίδιο αρχείο που παρέδωσε ως συνημμένο 3 του σχετικού 4. Για το ίδιο αρχείο, η εταιρεία δήλωσε ότι αποτελεί και το αρχείο με τους εργαζομένους που έχουν εξουσιοδοτηθεί σε απομακρυσμένη λογική πρόσβαση. Στο εν λόγω αρχείο αποτυπώνεται ότι για όλα τα ΠΕΣ υπάρχει απομακρυσμένη πρόσβαση μέσω ……., ενώ δεν είναι σαφές ποιοι από τους λογαριασμούς χρηστών που αναφέρονται ανήκουν σε συνεργάτες της εταιρείας.

Παρατήρηση 5: Η εταιρεία οφείλει να αποτυπώνει με σαφήνεια τους λογαριασμούς χρηστών που ανήκουν σε εργαζόμενους και συνεργάτες της εταιρείας.

Η εταιρεία κατά τον από 08.10.2015 επιτόπιο έλεγχο δήλωσε ότι ο χρήστης ……. αποτελεί εξωτερικό συνεργάτη με μόνιμη απομακρυσμένη πρόσβαση. Επίσης, όπως φαίνεται και στο συνημμένο 3 του σχετικού 4 ο χρήστης …… έχει πρόσβαση στο ΠΕΣ ……. μέσω terminal services και κατά συνέπεια έχει δικαιώματα διαχειριστή.

Απόκλιση 5: Δεν εφαρμόζονται οι απαιτήσεις της παραγράφου 4.6 της Πολιτικής Ασφάλειας της εταιρείας αναφορικά με τη συγκεκριμένη χρονική διάρκεια ισχύος του λογαριασμού πρόσβασης και την υποβολή σχετικού αιτήματος και την έγκρισή του από αρμόδιο πρόσωπο (παράγραφοι 7.2.6 και 7.2.7 του άρθρου 7 της Απόφασης 165/2011).

7. Διαχείριση και Εγκατάσταση ΠΕΣ (Άρθρο 8 της Απόφασης 165/2011, ΦΕΚ 2715/Β/17.11.2011)

Η εταιρεία παρέδωσε το αρχείο Ε-19 στο οποίο διατηρούνται όλες οι μεταβολές σε υλικό και λογισμικό των ΠΕΣ. Η εταιρεία παρέδωσε τη Διαδικασία Διαχείρισης και Εγκατάστασης ΠΕΣ (ΔΑΠ-2-01).

Σε ερώτημα της Ο.Ε. εάν έχει υπάρξει προμήθεια ή ανάπτυξη υλικού ή λογισμικού, η εταιρεία δήλωσε ότι έχει παραδώσει το σύνολο των προμηθειών στον αρχικό φάκελο, οι οποίες καταγράφονται στα έντυπα Ε-18. Η εταιρεία δήλωσε ότι στα εν λόγω έγγραφα διατηρείται το σύνολο της πληροφορίας που αφορά στην παράγραφο 5.1 της Πολιτικής Διαχείρισης και Εγκατάστασης ΠΕΣ, αναφορικά με τις απαιτήσεις ασφάλειας και τις προδιαγραφές των προς προμήθεια ΠΕΣ.

Τα έντυπα Ε-18 δεν περιλαμβάνουν τις απαιτήσεις της παραγράφου 5.1 με τίτλο «Διαδικασία Προμήθειας – Ανάπτυξης Υλικού και Λογισμικού» της εταιρείας αναφορικά σε προδιαγραφές ή ρυθμίσεις που πρέπει να έχει το υπό προμήθεια/ανάπτυξη ΠΕΣ προκειμένου να διασφαλίζεται το απόρρητο των επικοινωνιών. Στα έντυπα αυτά επίσης δεν καταγράφονται οι ελάχιστες απαιτήσεις αναφορικά με τα χαρακτηριστικά διαμόρφωσης και διαχείρισης του υπό προμήθεια/ανάπτυξη ΠΕΣ και οι ελάχιστες απαιτήσεις διαμόρφωσης της μεθόδου καταγραφής της πρόσβασης και των ενεργειών στο εν λόγω ΠΕΣ

Απόκλιση 6: Δεν εφαρμόζονται οι απαιτήσεις της παραγράφου 5.1 με τίτλο «Διαδικασία Προμήθειας – Ανάπτυξης Υλικού και Λογισμικού» αναφορικά με το περιεχόμενο των εντύπων Ε-18 (παράγραφος 8.3.1.2 του άρθρου 8 της Απόφασης 165/2011).

Αναφορικά με τις απαιτήσεις της παραγράφου 5.2 της Πολιτικής Διαχείρισης και Εγκατάστασης ΠΕΣ για τις δοκιμές στα συστήματα, η εταιρεία δήλωσε ότι δεν διατηρεί επιπλέον πληροφορίες, πέραν των αναφερόμενων στα έντυπα Ε-19. Στα έντυπα Ε-19 σύμφωνα με την παράγραφο 3.2 της Διαδικασίας Διαχείρισης ΠΕΣ της εταιρείας καταγράφονται τα αποτελέσματα των δοκιμών στο πρώτο πεδίο του Εντύπου.

Παρατήρηση 6. Η εταιρεία οφείλει να καταγράφει αναλυτικά στα έντυπα Ε-19 τις δοκιμές υλοποίησης ή διαμόρφωσης των απαιτήσεων που έχουν καθοριστεί για κάθε καινούργιο ΠΕΣ καθώς και τα αποτελέσματα αυτών.

Στην Οδηγία Λειτουργίες Διεύθυνσης Πληροφορικής (Ο-3) αναφέρεται στο Α.10.10.1 η καταγραφή των ελέγχων και συγκεκριμένα οι ενέργειες των χρηστών, exceptions και errors. Η εταιρεία δήλωσε ότι με χρήση του …… καταγράφονται τα σχετικά events μέσω σχετικών sensors και αποστέλλονται με e-mail στον Υπεύθυνο Ασφάλειας της εταιρείας. Η εταιρεία παρέδωσε για το σύστημα …….. τους sensors που έχουν οριστεί (συνημμένο 6 του από 20.10.2015 Πρακτικού Διενέργειας Επιτόπιου Ελέγχου).

Στην Οδηγία Ο-3 αναφέρεται ο έλεγχος δικτύου (Α.10.6.1) και συγκεκριμένα η καθημερινή παρακολούθηση της χρήσης των πόρων του δικτύου. Η εταιρεία δήλωσε ότι αυτό πραγματοποιείται με χρήση των εργαλείων …….. και ……..

Η εταιρεία δήλωσε ότι δεν έχει προβεί σε διαγραφή ή απόσυρση υλικού και λογισμικού σύμφωνα με την παράγραφο 5.4 της Πολιτικής Διαχείρισης και Εγκατάστασης ΠΕΣ.

8. Διαχείριση Περιστατικών Ασφάλειας (Άρθρο 9 της Απόφασης 165/2011, ΦΕΚ 2715/Β/17.11.2011)

Παράγραφος 6.1

Η εταιρεία παρέδωσε τη Διαδικασία Διαχείρισης Περιστατικών Ασφάλειας (ΔΑΠ-3). Στη διαδικασία περιγράφονται οι ενέργειες και η τήρηση των σχετικών αρχείων που προβλέπονται στην ενότητα 6 «Διαχείριση Περιστατικών Ασφάλειας».

Η εταιρεία δήλωσε ότι δεν έχει υπάρξει κάποιο περιστατικό ασφάλειας ώστε να ενεργοποιηθεί η διαδικασία.

9. Ασφάλεια Δικτύου (Άρθρο 10 της Απόφασης 165/2011, ΦΕΚ 2715/Β/17.11.2011)

7.2 Μηχανισμοί και Συστήματα Ασφάλειας Δικτύων

Η εταιρεία παρέδωσε την αρχιτεκτονική του δικτύου της σύμφωνα με την παράγραφο 7.2 της Πολιτικής Ασφάλειας Δικτύου (συνημμένο με τίτλο ……. της υπ'αριθμ. πρωτ. ΑΔΑΕ 1960/21-09-2015 επιστολής της).

10. Έλεγχος Εφαρμογής Πολιτικής Ασφάλειας (Άρθρο 11 της Απόφασης 165/2011, ΦΕΚ 2715/Β/17.11.2011)

Αναφορικά με τον Έλεγχο Εφαρμογής Πολιτικής Ασφάλειας, η εταιρεία παρέδωσε τα έγγραφα που αναφέρονται στη Διαδικασία Ελέγχων και Εσωτερικών Επιθεωρήσεων (ΔΑΠ-5-01) και συγκεκριμένα την Αναφορά Επιθεώρησης (Ε-27) και το Έντυπο Ενέργειες-Προγράμματα (Ε-13). Η Ο.Ε. ζήτησε αναλυτικό κατάλογο των Αντικειμένων Επιθεώρησης, όπως αναφέρονται στις φόρμες Ε-27, και η εταιρεία με την υπ' αριθμ. πρωτ. ΑΔΑΕ 2621/16.11.2015 επιστολή δήλωσε ότι «*δεν υπάρχει κατάλογος διότι ο έλεγχος περιλάμβανε το σύνολο της τεκμηρίωσης του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ΣΔΑΠ) της εταιρείας η οποία εμπεριέχει και την Πολιτική Ασφάλειας Πληροφοριών…. Για αυτό το λόγο προχωράμε σε επανασχεδιασμό των ελέγχων ώστε ο επερχόμενος να είναι πιο ουσιαστικό και παραγωγικός*.»

Απόκλιση 7: Τα έντυπα Ε-27 δεν πληρούν τις απαιτήσεις των παραγράφων 8.2.1 και 8.2.3 της Πολιτικής (παράγραφοι 11.3 και 11.4 και 11.5 του άρθρου 11 της Απόφασης 165/2011).

Αναφορικά με τον προγραμματισμό των ελέγχων, η εταιρεία δήλωσε ότι δεν διατηρεί αρχεία προγραμματισμού των ελέγχων.

Απόκλιση 8: Δεν εφαρμόζεται η παράγραφος 8.1 της Πολιτικής Ασφάλειας σχετικά με τον προγραμματισμό των ετήσιων ελέγχων και επιθεωρήσεων (παράγραφος 11.2.1 του άρθρου 11 της Απόφασης 165/2011).

11. Προστασία από Κακόβουλο Λογισμικό (Άρθρο 12 της Απόφασης 165/2011, ΦΕΚ 2715/Β/17.11.2011)

9.1 Μέτρα Ασφάλειας έναντι Κακόβουλου Λογισμικού

Η Πολιτική Κακόβουλου Λογισμικού της εταιρείας παραπέμπει στην Οδηγία Λειτουργίες Τμήματος Πληροφορικής (Ο-3) αναφορικά με τα μέτρα που αποσκοπούν στην αποτροπή, ανίχνευση, αντιμετώπιση και περιορισμό του κακόβουλου κώδικα.

Αναφορικά με τον έλεγχο που διεξάγει η εταιρεία για ύπαρξη λογισμικού πέραν εκείνου που έχει προμηθευτεί η εταιρεία, σύμφωνα με την παράγραφο 9.1 της εν λόγω Πολιτικής, η εταιρεία στην υπ' αριθμ. πρωτ. ΑΔΑΕ 2621/16.11.2015 επιστολή της περιγράφει τα μέτρα που λαμβάνει για τα διάφορα συστήματά της ώστε να διασφαλίσει την ακεραιότητα αυτών από κακόβουλο λογισμικό.

12. Χρήση Κρυπτογραφίας (Άρθρο 13 της Απόφασης 165/2011, ΦΕΚ 2715/Β/17.11.2011)

10.1 Προδιαγραφές Κρυπτογράφησης Δεδομένων

Η εταιρεία παρέδωσε την Οδηγία Λειτουργίας Τμήματος Πληροφορικής (Ο-3) στην οποία, σύμφωνα με την Πολιτική Ασφάλειας, περιγράφονται τα συστήματα κρυπτογράφησης και ο αλγόριθμοι που επιλέγονται. Πλην όμως, από την εξέταση της συγκεκριμένης οδηγίας διαπιστώθηκε ότι δεν γίνεται καμία αναφορά σε συστήματα ή αλγόριθμους κρυπτογράφησης.

Απόκλιση 9: Δεν εφαρμόζεται η παράγραφος 10.1 αναφορικά με το περιεχόμενο της Οδηγίας Λειτουργίας Τμήματος Πληροφορικής (Ο-3) (παράγραφος 13.2.9 του άρθρου 13 της Απόφασης 165/2011).

Η εταιρεία δήλωσε ότι διατηρεί backup server (incremental backups) στη …….. για την αποθήκευση των δεδομένων επικοινωνίας, ο οποίος τα προωθεί και σε Data Center στην ….. της εταιρείας ……. Τα εν λόγω αντίγραφα ασφαλείας δεν είναι κρυπτογραφημένα στους παραπάνω servers. Η εταιρεία στη συνέχεια στην υπ'αριθμ. πρωτ. ΑΔΑΕ 2621/16.11.2015 επιστολή της δήλωσε ότι τα backups είναι πλέον κρυπτογραφημένα και στα δυο data centers, …….. και ……. Η υλοποίηση της κρυπτογράφησης (……) παρέχεται από το backup software ……..που χρησιμοποιεί η εταιρεία και επισυνάπτει και σχετική απόδειξη της υλοποίησης.

Δ. ΣΥΜΠΕΡΑΣΜΑΤΑ

Από τον δειγματοληπτικό έλεγχο εφαρμογής της Πολιτικής Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών της εταιρείας ……. κατά τους επιτόπιους ελέγχους και με την εξέταση των παρεληφθέντων στοιχείων διαπιστώθηκε ότι, η εταιρεία ……. κατά το χρόνο διεξαγωγής του τακτικού ελέγχου δεν εφήρμοζε πλήρως την εγκριθείσα, με την Απόφαση 235/2013, Πολιτική Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών, ως προς τα σημεία που αναφέρονται αναλυτικά στην ενότητα Γ.»

Β. Η εν λόγω Έκθεση διενέργειας τακτικού ελέγχου στην εταιρεία «…….» εγκρίθηκε από την Ολομέλεια της Α.Δ.Α.Ε. σύμφωνα με το υπ' αριθμ. 18 Πρακτικό της από 29 Ιουνίου 2016 συνεδρίασης και η σχετική Απόφαση υπ' αριθμ. 209/2016 περί έγκρισης της διενέργειας του εν λόγω ελέγχου, μετά της συνημμένης έκθεσης, παρεδόθη στην εταιρεία «……..», όπως προκύπτει από την υπ' αριθμ. πρωτ. ΑΔΑΕ 2513/25-10-2016 Απόδειξη παράδοσης – παραλαβής.

Γ. 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 τη Διαδικασία Ελέγχου Εξαιρέσεων

Η εταιρεία αναφέρει στη Διαδικασία Ελέγχου (παράγραφο 1.2) ότι στη Διαδικασία Ελέγχων και Εσωτερικών Επιθεωρήσεων (ΔΑΠ-5) περιλαμβάνεται η μεθοδολογία για την αναγνώριση, καταγραφή και διαχείριση των περιπτώσεων εξαιρέσεων που μπορεί να προκύψουν σε μελλοντική έκδοση της Π.Α.

Απόκλιση: Η εταιρεία στη Διαδικασία Ελέγχων και Εσωτερικών Επιθεωρήσεων (ΔΑΠ-5) δεν περιλαμβάνει τη μεθοδολογία για την αναγνώριση, καταγραφή και διαχείριση των περιπτώσεων εξαιρέσεων που μπορεί να προκύψουν σε μελλοντική έκδοση της Π.Α., όπως αναφέρει στην παράγραφο 1.2 με τίτλο Διαδικασία Ελέγχου Εξαιρέσεων και όπως προβλέπεται στην παράγραφο 3.2.3 του άρθρου 3 της Απόφασης 165/2011.

β) Ως προς την παράγραφο 1.5 της Πολιτικής Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών

1.5 Διαδικασία Διαχείρισης Πολιτικής Ασφάλειας

Η εταιρεία παρέδωσε το έγγραφο «Διαδικασία Διαχείρισης Εγγράφων και Αρχείων (Δ-2)». Από την εξέταση της Διαδικασίας (Δ-2) διαπιστώθηκε ότι δεν περιλαμβάνονται σε αυτήν η αρχιτεκτονική, οι μέθοδοι δημιουργίας, συλλογής, αποθήκευσης και διαχείρισης των αρχείων καταγραφής, το περιεχόμενό τους και τα μέτρα διασφάλισης της ακεραιότητας, της

εμπιστευτικότητας και της διαθεσιμότητάς τους, σύμφωνα με την παράγραφο 1.5 της Πολιτικής Ασφάλειας της εταιρείας.

Απόκλιση 1: Δεν εφαρμόζεται η παράγραφος 1.5 αναφορικά με το περιεχόμενο της Διαδικασίας Διαχείρισης Εγγράφων και Αρχείων (Δ-2), διότι δεν περιλαμβάνονται τα στοιχεία που αφορούν το ειδικό σχέδιο αρχείων καταγραφής, όπως προβλέπεται στην παράγραφο 3.2.9 του άρθρου 3 της Απόφασης 165/2011.

γ) Ως προς την παράγραφο 2.2. της Πολιτικής Αποδεκτής Χρήσης για τους συνεργάτες

2.2 Πολιτική Αποδεκτής Χρήσης για τους συνεργάτες

Από τις συμβάσεις με τις εταιρείες ……., …… (Data Center στην ……), …… (call center) και ……., τις οποίες παρέδωσε η εταιρεία κατά τη διάρκεια του ελέγχου, διαπιστώθηκε ότι δεν περιλαμβάνονται σε αυτές οι όροι σχετικά με τους συνεργάτες που ορίζονται στην παράγραφο 2.2 της Πολιτικής Αποδεκτής χρήσης.

Απόκλιση 2: Δεν εφαρμόζεται η παράγραφος 2.2 αναφορικά με το ελάχιστο περιεχόμενο των συμβάσεων με τους συνεργάτες, όπως προβλέπεται στην παράγραφο 4.3.2 του Άρθρου 4 της Απόφασης 165/2011.

δ) Ως προς την παράγραφο 4.2 της Τοπικής και Απομακρυσμένης Λογικής Πρόσβασης

4.2 Λογαριασμοί Πρόσβασης Χρηστών ΠΕΣ

Αναφορικά με το αρχείο καταγραφής προσβάσεων στα ΠΕΣ, η εταιρεία δήλωσε ότι έχει ενεργοποιήσει μόνο σε επίπεδο Windows τη διατήρηση των login/logout των χρηστών. Η εταιρεία δήλωσε ότι ο χρόνος διατήρησης των εν λόγω εγγραφών εξαρτάται από το rotation που κάνει ο event logger και η Ο.Ε. διαπίστωσε ότι τα εν λόγω log files διατηρούνται από 10.03.2015. Επίσης, η εταιρεία δήλωσε ότι με χρήση του …….. καταγράφει τις προσβάσεις καθώς και τις ενέργειες σε επίπεδο Windows και παρέδωσε screenshots από την εν λόγω εφαρμογή. Η εταιρεία δήλωσε ότι οι προσβάσεις, καθώς και οι ενέργειες των χρηστών και πελατών που εισέρχονται στην πλατφόρμα WebAdmin καταγράφονται και διατηρούνται για 2 χρόνια.

Απόκλιση 3: Δεν εφαρμόζεται η παράγραφος 1.5 των Γενικών Απαιτήσεων αναφορικά με το χρόνο διατήρησης για 2 έτη των αρχείων καταγραφής προσβάσεων των χρηστών σε επίπεδο Windows σε όλα τα ΠΕΣ, όπως προβλέπεται στην παράγραφο 3.2.8 του άρθρου 3 της Απόφασης 165/2011.

Αναφορικά με τις προσβάσεις σε δεδομένα επικοινωνίας των συνδρομητών η εταιρεία δήλωσε ότι τα συστήματα που διατηρούν δεδομένα επικοινωνίας είναι οι βάσεις, ……., …….., …….. και …….. και διατηρεί μόνο τα Login/logout σε επίπεδο Windows, χωρίς τις αντίστοιχες αιτιολογήσεις. Στη συνέχεια, στο πλαίσιο του από 20.10.2015 επιτόπιου ελέγχου, η εταιρεία δήλωσε ότι οι προσβάσεις των χρηστών της εταιρείας στο σύνολο των βάσεων δεδομένων καταγράφονται με χρήση του λογισμικού ……., το οποίο διατηρεί τις εν λόγω ενέργειες για 2 χρόνια.

Απόκλιση 4: Η εταιρεία δεν εφαρμόζει την παράγραφο 4.2 της Πολιτικής Ασφάλειας αναφορικά με την αιτιολόγηση των προσβάσεων στα δεδομένα επικοινωνίας, όπως προβλέπεται στην παράγραφο 6.2.6 του άρθρου 6 της Απόφασης 165/2011.

ε) Ως προς την παράγραφο 4.6 της Τοπικής και Απομακρυσμένης Λογικής Πρόσβασης

4.6 Απαιτήσεις για την Απομακρυσμένη Λογική Πρόσβαση

Η εταιρεία κατά τον από 08.10.2015 επιτόπιο έλεγχο δήλωσε ότι ο χρήστης …….. αποτελεί εξωτερικό συνεργάτη με μόνιμη απομακρυσμένη πρόσβαση. Επίσης, ο χρήστης …… έχει πρόσβαση στο ΠΕΣ …… μέσω terminal services και κατά συνέπεια έχει δικαιώματα διαχειριστή.

Απόκλιση 5: Δεν εφαρμόζονται οι απαιτήσεις της παραγράφου 4.6 της Πολιτικής Ασφάλειας της εταιρείας αναφορικά με τη συγκεκριμένη χρονική διάρκεια ισχύος του λογαριασμού πρόσβασης και την υποβολή σχετικού αιτήματος και την έγκρισή του από αρμόδιο πρόσωπο, όπως προβλέπεται στις παραγράφους 7.2.6 και 7.2.7 του άρθρου 7 της Απόφασης 165/2011.

στ) Ως προς τη Διαχείριση και Εγκατάσταση ΠΕΣ

Τα έντυπα Ε-18 της Διαδικασίας Διαχείρισης και Εγκατάστασης ΠΕΣ (ΔΑΠ-2-01) δεν περιλαμβάνουν τις απαιτήσεις της παραγράφου 5.1 με τίτλο «Διαδικασία Προμήθειας –

Ανάπτυξης Υλικού και Λογισμικού» της εταιρείας αναφορικά σε προδιαγραφές ή ρυθμίσεις που πρέπει να έχει το υπό προμήθεια/ανάπτυξη ΠΕΣ, προκειμένου να διασφαλίζεται το απόρρητο των επικοινωνιών. Στα έντυπα αυτά, επίσης, δεν καταγράφονται οι ελάχιστες απαιτήσεις αναφορικά με τα χαρακτηριστικά διαμόρφωσης και διαχείρισης του υπό προμήθεια/ανάπτυξη ΠΕΣ και οι ελάχιστες απαιτήσεις διαμόρφωσης της μεθόδου καταγραφής της πρόσβασης και των ενεργειών στο εν λόγω ΠΕΣ

Απόκλιση 6: Δεν εφαρμόζονται οι απαιτήσεις της παραγράφου 5.1 με τίτλο «Διαδικασία Προμήθειας – Ανάπτυξης Υλικού και Λογισμικού» αναφορικά με το περιεχόμενο των εντύπων Ε-18, όπως προβλέπεται στην παράγραφο 8.3.1.2 του άρθρου 8 της Απόφασης 165/2011.

ζ) Ως προς τον Έλεγχο Εφαρμογής Πολιτικής Ασφάλειας

Αναφορικά με τον Έλεγχο Εφαρμογής Πολιτικής Ασφάλειας, η εταιρεία παρέδωσε τα έγγραφα που αναφέρονται στη Διαδικασία Ελέγχων και Εσωτερικών Επιθεωρήσεων (ΔΑΠ-5-01) και συγκεκριμένα την Αναφορά Επιθεώρησης (Ε-27) και το Έντυπο Ενέργειες-Προγράμματα (Ε-13). Η Ο.Ε. ζήτησε αναλυτικό κατάλογο των Αντικειμένων Επιθεώρησης, όπως αναφέρονται στις φόρμες Ε-27, και η εταιρεία με την υπ' αριθμ. πρωτ. ΑΔΑΕ 2621/16.11.2015 επιστολή δήλωσε ότι «*δεν υπάρχει κατάλογος διότι ο έλεγχος περιλάμβανε το σύνολο της τεκμηρίωσης του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ΣΔΑΠ) της εταιρείας η οποία εμπεριέχει και την Πολιτική Ασφάλειας Πληροφοριών…. Για αυτό το λόγο προχωράμε σε επανασχεδιασμό των ελέγχων ώστε ο επερχόμενος να είναι πιο ουσιαστικό και παραγωγικός.*»

Απόκλιση 7: Τα έντυπα Ε-27 δεν πληρούν τις απαιτήσεις των παραγράφων 8.2.1 και 8.2.3 της Πολιτικής, όπως προβλέπεται στις παραγράφους 11.3 και 11.4 και 11.5 του άρθρου 11 της Απόφασης 165/2011.

Αναφορικά με τον προγραμματισμό των ελέγχων, η εταιρεία δήλωσε ότι δεν διατηρεί αρχεία προγραμματισμού των ελέγχων.

Απόκλιση 8: Δεν εφαρμόζεται η παράγραφος 8.1 της Πολιτικής Ασφάλειας σχετικά με τον προγραμματισμό των ετήσιων ελέγχων και επιθεωρήσεων, όπως προβλέπεται στην παράγραφο 11.2.1 του άρθρου 11 της Απόφασης 165/2011.

η) Ως προς την Πολιτική Χρήσης Κρυπτογραφίας

10.1 Προδιαγραφές Κρυπτογράφησης Δεδομένων

Η εταιρεία παρέδωσε την Οδηγία Λειτουργίας Τμήματος Πληροφορικής (Ο-3) στην οποία, σύμφωνα με την Πολιτική Ασφάλειας, περιγράφονται τα συστήματα κρυπτογράφησης και ο αλγόριθμοι που επιλέγονται. Πλην όμως, από την εξέταση της συγκεκριμένης οδηγίας διαπιστώθηκε ότι δεν γίνεται καμία αναφορά σε συστήματα ή αλγόριθμους κρυπτογράφησης.

Απόκλιση 9: Δεν εφαρμόζεται η παράγραφος 10.1 αναφορικά με το περιεχόμενο της Οδηγίας Λειτουργίας Τμήματος Πληροφορικής (Ο-3), όπως προβλέπεται στην παράγραφο 13.2.9 του άρθρου 13 της Απόφασης 165/2011.

Δ. Κατόπιν των παραπάνω, και έχοντας υπόψη:

1. Το άρθρο 19 του Συντάγματος,
2. Το ν.3115/2003 «Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών» (ΦΕΚ Α΄ 47/2003), όπως ισχύει,
3. Το ν. 3674/2008 «Ενίσχυση του θεσμικού πλαισίου διασφάλισης του απορρήτου της τηλεφωνικής επικοινωνίας και άλλες διατάξεις» (ΦΕΚ Α’ 136/10.07.2008), όπως ισχύει,
4. Τις διατάξεις του Κανονισμού για τη Διασφάλιση του Απορρήτου των Ηλεκτρονικών Επικοινωνιών (υπ’ αριθμ. 165/2011 Απόφαση της Α.Δ.Α.Ε., ΦΕΚ Β΄2715/17.11.2011),
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 76/30-04-2013 Πολιτική Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών της εταιρείας «……», όπως αυτή συμπληρώθηκε με το υπ' αριθμ. πρωτ. ΑΔΑΕ ΕΜΠ 119/03-07-2013 έγγραφο και όπως τελικώς αυτή εγκρίθηκε με την υπ' αριθμ. 235/2013 Απόφαση της Α.Δ.Α.Ε.,
16. Την υπ' αριθμ. 149/2015 Απόφαση της Α.Δ.Α.Ε. σχετικά με τη διενέργεια τακτικού ελέγχου στην εταιρεία «…….»,
17. Την υπ' αριθμ. 261/2015 Απόφαση του Αντιπροέδρου 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 1963/21.09.2015,
19. το Πρακτικό Διενέργειας Επιτόπιου Ελέγχου στις εγκαταστάσεις της εταιρείας «……», με αριθμ. πρωτ. ΑΔΑΕ 2187/09.10.2015,

20. το Πρακτικό Διενέργειας Επιτόπιου Ελέγχου στις εγκαταστάσεις της εταιρείας «……», με αριθμ. πρωτ. ΑΔΑΕ 2360/23.10.2015,
21. την υπ' αριθμ. πρωτ. ΑΔΑΕ 1960/21.09.2015 επιστολή της εταιρείας «……..», με θέμα «Διενέργεια τακτικού ελέγχου – Πρόσθετες πληροφορίες»,
22. την υπ' αριθμ. πρωτ. ΑΔΑΕ 2621/16.11.2015 επιστολή της εταιρείας «……..», με θέμα «Διενέργεια τακτικού ελέγχου»,
23. την από 15.02.2016 «Έκθεση Διενέργειας Τακτικού Ελέγχου στις εγκαταστάσεις της ……» με τα σχετικά αυτής,
24. Την υπ' αριθμ. 142/2016 Εισήγηση προς την Ολομέλεια της Α.Δ.Α.Ε.,
25. Το υπ' αριθμ. 18 πρακτικό της από 29 Ιουνίου 2016 συνεδρίασης της Ολομέλειας της Α.Δ.Α.Ε.,
26. Την υπ' αριθμ. 209/2016 Απόφαση της Α.Δ.Α.Ε. περί έγκρισης της ως άνω από 15-02-2016 Έκθεσης διενέργειας τακτικού ελέγχου στην εταιρεία «…….», η οποία παραδόθηκε στην εταιρεία «……..», όπως προκύπτει από την υπ' αριθμ. πρωτ. ΑΔΑΕ 2513/25-10-2016 Απόδειξη παράδοσης – παραλαβής,
27. Την υπ' αριθμ. 113/2017 εισήγηση προς την Ολομέλεια της Α.Δ.Α.Ε.,
28. Το πρακτικό της από 15 Μαρτίου 2017 συνεδρίασης της Ολομέλειας της Α.Δ.Α.Ε.,
29. 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 **10η Μαΐου 2017, ημέρα Τετάρτη και ώρα 13.30 μ.μ.**, στην έδρα της Α.Δ.Α.Ε., Ιερού Λόχου 3, Μαρούσι, με αντικείμενο τον έλεγχο της ενδεχόμενης παράβασης 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), σύμφωνα με τις αποκλίσεις που προσδιορίζονται στην εγκεκριμένη με την υπ' αριθμ. 235/2013 απόφαση της Α.Δ.Α.Ε. Πολιτική Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών της εταιρείας, όπως αυτές αναφέρονται στην από 15 Φεβρουαρίου 2016 Έκθεση Διενέργειας τακτικού Ελέγχου στην εν λόγω εταιρεία, αναφορικά με την εφαρμογή της Πολιτικής διασφάλισης του απορρήτου των επικοινωνιών και όπως αυτές αναλυτικά εκτίθενται ανωτέρω στο σημείο Γ της παρούσας.

Εισηγητής για την εν λόγω υπόθεση ορίζεται το τακτικό μέλος της Α.Δ.Α.Ε., κ. Μιχαήλ Γεωργιακόδης.

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

Κρίθηκε και αποφασίστηκε την 15 Μαρτίου 2017.

Ο Πρόεδρος

Χρήστος Ζαμπίρας