



Μαρούσι, 18 Ιουλίου 2017
Αρ. πρωτ.: 2203
ΑΝΑΡΤΗΤΕΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

ΑΠΟΦΑΣΗ

(αριθμ: 41/2017)

Θέμα:

Κλήση σε ακρόαση της εταιρείας με την επωνυμία «.....» (εφεξής «.....») 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. 294/2013 απόφαση της Α.Δ.Α.Ε. Πολιτική Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών της εταιρείας, όπως αυτές αναφέρονται στην από 10 Φεβρουαρίου 2015 Έκθεση Διενέργειας τακτικού Ελέγχου στην εν λόγω εταιρεία.

Την Τετάρτη, 1^η Φεβρουαρίου 2017, η Ολομέλεια της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών, παρισταμένων του Αντιπροέδρου κ. Μιχαήλ Σακκά, των τακτικών μελών κ.κ. Μιχαήλ Γεωργιακόδη, Γεωργίου Μπακάλη, Αικατερίνης Παπανικολάου και Παναγιώτη Ριζομυλιώτη, καθώς και του αναπληρωματικού μέλους κ. Δημόσθενη Βουγιούκα, ο οποίος παρέστη προς αναπλήρωση του τακτικού μέλους κ. Ιωάννη Ασκοξυλάκη, ο οποίος δεν προσήλθε λόγω κωλύματος, αν και είχε νομίμως και εμπροθέσμως προσκληθεί και απόντος και του Προέδρου κ. Χρήστου Ζαμπίρα, ο οποίος δεν παρέστη επίσης 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. 294/2013 απόφαση της Α.Δ.Α.Ε. Πολιτική Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών της εταιρείας, όπως αυτές αναφέρονται στην από 10 Φεβρουαρίου 2015 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 10 Φεβρουαρίου 2015 Έκθεση Διενέργειας τακτικού Ελέγχου αναφορικά με την εφαρμογή της Πολιτικής διασφάλισης του απορρήτου των επικοινωνιών στην εταιρεία «.....», όπως αυτή τροποποιήθηκε και εγκρίθηκε από την Ολομέλεια της Αρχής κατά τη συνεδρίαση της 23^{ης} Ιουλίου 2015, παρατηρήθηκαν αποκλίσεις από την Πολιτική Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών της ως άνω εταιρείας, όπως αυτή είχε εγκριθεί με την υπ' αριθμ. 294/2013 Απόφαση της Α.Δ.Α.Ε.. Τα αποτελέσματα του τακτικού ελέγχου έχουν ως εξής :

«Γ. ΕΞΕΤΑΣΗ 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 7.10.2013 Έκθεση Ελέγχου Συμμόρφωσης Πολιτικής

Η Ο.Ε. έλεγξε την επικαιροποιημένη πολιτική ασφάλειας για τη διασφάλιση του απορρήτου των επικοινωνιών που παρέλαβε από την εταιρεία και διαπίστωσε ότι έχουν ενσωματωθεί οι παρατηρήσεις της από 7.10.2013 Έκθεσης Ελέγχου Συμμόρφωσης Πολιτικής η οποία κοινοποιήθηκε στην εταιρεία συνημμένη στην υπ' αριθμ. 294/2013 Απόφαση της ΑΔΑΕ.

2. Πολιτική Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών

Παράγραφος 3

Η εταιρεία παρέδωσε τη διαδικασία: «Διαχείριση Εξαιρέσεων από την Πολιτική Ασφάλειας» ως διαδικασία καταγραφής και τεκμηρίωσης των αδυναμιών της παραγράφου 3.2.3 της Απόφασης 165/2011. Αναφορικά με τις εξαιρέσεις, η εταιρεία παρέδωσε δύο έντυπα καταγραφής εξαιρέσεων από τις πολιτικές ασφάλειας για τη διασφάλιση του απορρήτου των επικοινωνιών, ένα για τα συστήματα του δικτύου και ένα για τα συστήματα της πληροφορικής. Επίσης, η εταιρεία απέστειλε, με την υπ' αριθμ. πρωτ. ΑΔΑΕ ΑΠΡ 2345/15.7.2014 επιστολή, μια επιπλέον εξαίρεση η οποία αφορά σε μια παράγραφο της Πολιτικής Φυσικής Ασφάλειας.

Στα ως άνω έγγραφα περιλαμβάνονται οι εξαιρέσεις από επιμέρους πολιτικές και για κάθε μια από αυτές αναφέρονται τα συστήματα που επηρεάζονται, η αιτιολόγηση, οι εναλλακτικοί μηχανισμοί ελέγχου και οι



προϋποθέσεις άρσης της εξαίρεσης, σύμφωνα με τα οριζόμενα στην παράγραφο 3 και τη σχετική διαδικασία.

Ωστόσο, από την εξέταση των παραπάνω εγγράφων διαπιστώθηκαν τα ακόλουθα:

- Στην εξαίρεση με τίτλο: «Εξαίρεση των ψηφιακών κέντρων (.....) από απαιτήσεις της Πολιτικής Ασφάλειας για τη διασφάλιση του απορρήτου»:
 - Η εταιρεία αναφέρει αφενός ότι η πρόσβαση πραγματοποιείται αποκλειστικά μέσω των αντίστοιχων συστημάτων και αφετέρου ότι η τοπική πρόσβαση στα κέντρα είναι πλήρως ελεγχόμενη.
 - Η εταιρεία αναφέρει αφενός ότι η κρυπτογράφηση κατά την αποθήκευση και μεταφορά των CDRs δεν είναι εφικτή και αφετέρου ότι εξαιτίας του τρόπου λειτουργίας των συστημάτων η κρυπτογράφηση δεν θα προσφέρει σημαντικά κέρδη στη διασφάλιση του απορρήτου των επικοινωνιών, οπότε το ρίσκο είναι πολύ μικρό και αποδεκτό.

Κατά συνέπεια, δημιουργείται ασάφεια ως προς τη διατύπωση της αιτιολόγησης για την πρόσβαση στα ψηφιακά κέντρα και την κρυπτογράφηση κατά την αποθήκευση και μεταφορά των CDRs.

- Δεν υπάρχει επαρκής τεκμηρίωση των αιτιολογήσεων.
- Δεν αναφέρεται για όλες τις εξαιρέσεις στην ενότητα «προϋποθέσεις άρσης της εξαίρεσης» σαφές χρονοδιάγραμμα ενεργειών αναφορικά με την άρση ή τη διερεύνηση για την άρση της εξαίρεσης.

Παρατήρηση 1: Η εταιρεία, αναφορικά με την εξαίρεση με τίτλο: «Εξαίρεση των ψηφιακών κέντρων (.....) από απαιτήσεις της Πολιτικής Ασφάλειας για τη διασφάλιση του απορρήτου», οφείλει να διατυπώσει με μεγαλύτερη σαφήνεια τη σχετική αιτιολόγηση.

Παρατήρηση 2: Η εταιρεία οφείλει να συμπληρώσει τις αιτιολογήσεις παραθέτοντας επαρκή τεκμηρίωση αυτών.

Παρατήρηση 3: Η εταιρεία οφείλει να ορίσει στη διαδικασία, και να εφαρμόσει, ότι στις προϋποθέσεις άρσης της εξαίρεσης θα πρέπει να καταγράφεται και το χρονοδιάγραμμα ενεργειών της άρσης ή της διερεύνησης για την άρση.

Παράγραφος 5.1.5 και 5.1.8

Η εταιρεία παρέδωσε το έγγραφο με τίτλο «Ειδικό Σχέδιο Αρχείων Καταγραφής Συστημάτων». Στο έγγραφο αυτό αναφέρονται τα ΠΕΣ τα οποία έχουν υπαχθεί στις καταγραφές, ενώ αναφέρεται ότι τα παραγόμενα αρχεία καταγραφής μεταφέρονται στην κεντρική υποδομή Log Management, όπου έχει καταστεί τεχνικά εφικτό. Επίσης, ως συνημμένο του προηγούμενου εγγράφου, για κάθε ΠΕΣ παραδόθηκε



αρχείο (Excel) στο οποίο παρουσιάζονται τα είδη και η περιγραφή των καταγραφών ανά κατηγορία (.....), ποιες είναι ενεργοποιημένες και ποιες μεταφέρονται στην κεντρική υποδομή (.....).

Από την εξέταση του Ειδικού Σχεδίου Αρχείων Καταγραφής Συστημάτων διαπιστώθηκε ότι δεν περιλαμβάνει τα στοιχεία αναφορικά με τα μέτρα για τη διασφάλιση της ακεραιότητας, της εμπιστευτικότητας και της διαθεσιμότητας αυτών.

Απόκλιση 1: Δεν εφαρμόζεται πλήρως η παράγραφος 5.1.8 διότι δεν ορίζονται τα μέτρα για τη διασφάλιση της ακεραιότητας, της εμπιστευτικότητας και της διαθεσιμότητας των Αρχείων Καταγραφής (παράγραφος 3.2.9 του άρθρου 3 της Απόφασης 165/2011)

Από την εξέταση των αρχείων (Excel) για κάθε σύστημα διαπιστώθηκε ότι για τα συστήματα δεν έχει υλοποιηθεί η μεταφορά των αρχείων καταγραφής που παράγονται στην κεντρική υποδομή Επιπλέον, διαπιστώθηκε ότι ο χρόνος διατήρησης των περισσοτέρων αρχείων καταγραφής αυτών των συστημάτων είναι μικρότερος των δύο ετών, ενδεικτικά αναφέρονται χρόνοι διατήρησης 2, 7, 10, 30, 60, 90, 365 ημερών, ή μπορεί να μην είναι γνωστός (N/A). Σημειώνεται όμως, ότι για τα συστήματα η εταιρεία έχει καταγράψει την εξαίρεσή τους από την παράγραφο 5.1.5.

Απόκλιση 2: Δεν εφαρμόζεται για όλα τα ΠΕΣ η παράγραφος 5.1.5 αναφορικά με τη διατήρηση των αρχείων καταγραφής για δύο έτη (παράγραφος 3.2.8 του άρθρου 3 της Απόφασης 165/2011)

Παράγραφος 5.2.1

Η εταιρεία παρέδωσε ως διαδικασία αποτίμησης κινδύνου το έγγραφο: «..... - Αποτίμηση κινδύνων ασφάλειας συστημάτων». Η Ο.Ε. έλεγξε τις αναφορές αποτίμησης κινδύνων ανά σύστημα και διαπίστωσε ότι έχουν πραγματοποιηθεί οι ενέργειες, και έχουν καταγραφεί τα αποτελέσματα αυτών, που ορίζονται στην σχετική διαδικασία. Η Ο.Ε. έλεγξε το πρόγραμμα υλοποίησης προτεινόμενων μέτρων (.....), το οποίο ορίζεται στη διαδικασία, για κάθε σύστημα στο οποίο περιλαμβάνονται τα μέτρα που έχουν ληφθεί ή πρόκειται να ληφθούν σύμφωνα με τα αποτελέσματα της αποτίμησης κινδύνου.

Παράγραφος 5.2.3

Η εταιρεία παρέδωσε τον κατάλογο συστημάτων με συνοπτική περιγραφή της λειτουργίας τους. Από την εξέταση του καταλόγου και σύμφωνα με τον ορισμό των Πληροφοριακών και Επικοινωνιακών Συστημάτων (ΠΕΣ) (παράγραφος 4 της Πολιτικής Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών και άρθρο 2 της Απόφασης 165/2011) διαπιστώθηκε ότι ο κατάλογος δεν περιλαμβάνει, τουλάχιστον, τα συστήματα πρόσβασης συνδρομητών στο διαδίκτυο, τα αναχώματα ασφάλειας, τα συστήματα αποτροπής εισβολών, τα συστήματα ανίχνευσης κακόβουλου λογισμικού και τα συστήματα καταγραφής.



Απόκλιση 3: Δεν εφαρμόζεται η παράγραφος 5.2.3 αναφορικά με την πληρότητα του καταλόγου των ΠΕΣ (παράγραφος 3.3.1.1 του άρθρου 3 της Απόφασης 165/2011).

3. Πολιτική Αποδεκτής Χρήσης (Άρθρο 4 της Απόφασης 165/2011, ΦΕΚ 2715/Β/17.11.2011)

Παράγραφος 2.1.2

Η εταιρεία δήλωσε ότι οι σχετικές πολιτικές, διαδικασίες και οδηγίες, που αφορούν στην εφαρμογή της πολιτικής ασφάλειας για τη διασφάλιση του απορρήτου των επικοινωνιών, είναι αναρτημένες στο εσωτερικό δίκτυο (intranet) της εταιρείας και οι εργαζόμενοι λαμβάνουν σχετικό ενημερωτικό e-mail.

Επίσης, η εταιρεία δήλωσε ότι οι εργαζόμενοι τουδεσμεύονται, βάσει του εσωτερικού κανονισμού προσωπικού, ότι λαμβάνουν γνώση και εφαρμόζουν τα παραπάνω. Η εταιρεία παρέδωσε Παράρτημα του εσωτερικού κανονισμού (Συνημμένο 1 του Σχετικού 4). Ειδικότερα στην παράγραφο 7 του Άρθρου 6 «Καθήκοντα Εργαζομένων» του εν λόγω παραρτήματος γίνονται σχετικές αναφορές. Επιπρόσθετα, η εταιρεία επέδειξε τις συμβάσεις και τα σχετικά έγγραφα υπηρεσιακής κατάστασης τεσσάρων εργαζομένων που είναι χρήστες σε ΠΕΣ της εταιρείας (χρήστες και του συστήματος, και χρήστες και του συστήματος,), από τα οποία προκύπτει ότι η υπαλληλική σχέση διέπεται από τον Γενικό Κανονισμό Προσωπικού

Σχετικά με τους συνεργάτες, η εταιρεία δήλωσε ότι η αποδοχή της Πολιτικής Ασφάλειας για τη διασφάλιση του απορρήτου των επικοινωνιών πραγματοποιείται μέσω της σύμβασης που έχει υπογράψει ο με την εκάστοτε συνεργαζόμενη εταιρεία.

Παράγραφος 2.1.3

Η εταιρεία δήλωσε ότι είναι σε εξέλιξη το πρόγραμμα e-learning, μέσω του οποίου οι εργαζόμενοι του εκπαιδεύονται σε θέματα ασφάλειας και εφαρμογής των σχετικών πολιτικών και διαδικασιών. Με το πέρας της εκπαίδευσης, οι εργαζόμενοι υπογράφουν «Δήλωση για τη Διασφάλιση του Απορρήτου των Επικοινωνιών, την Ασφάλεια των Εταιρικών Πληροφοριών και την Προστασία των Προσωπικών Δεδομένων» (Συνημμένο 2 του Σχετικού 4).

Παράγραφος 2.2.1

Η εταιρεία παρέδωσε το έγγραφο με τίτλο «Αρχείο Συνεργατών με Δυνατότητα Πρόσβασης σε Δεδομένα Επικοινωνίας» (Συνημμένο 3 του Σχετικού 4). Το αρχείο περιέχει τους συνεργάτες με δυνατότητα λογικής πρόσβασης σε ΠΕΣ. Ορισμένοι από αυτούς έχουν περαιτέρω τη δυνατότητα απομακρυσμένης λογικής πρόσβασης. Ύστερα από αίτημα της Ο.Ε., η εταιρεία παρέδωσε επικαιροποιημένο έγγραφο με τίτλο «Αρχείο Συνεργατών με Δυνατότητα Πρόσβασης σε Δεδομένα Επικοινωνίας» (Συνημμένο 1 του Σχετικού 6), στο οποίο περιλαμβάνονται επιπλέον δύο (2) εταιρείες.

Παράγραφος 2.2.2



Η Ο.Ε. ζήτησε τις συμβάσεις που έχει υπογράψει με τις εταιρείες και Η εταιρεία παρέδωσε τμήμα της σύμβασης 60560 μεταξύ και της εταιρείας (συνημμένο 4 του Σχετικού 4), στην οποία περιλαμβάνεται το άρθρο 9 «Εμπιστευτικότητα». Επίσης, παρέδωσε τμήμα της σύμβασης 40510 μεταξύ και της εταιρείας (συνημμένο 5 του Σχετικού 4) στην οποία περιλαμβάνεται το άρθρο 9 «Εμπιστευτικότητα». Τέλος, η εταιρεία παρέδωσε έγγραφο με τίτλο «Παράρτημα Πολιτικής Ασφάλειας» (συνημμένο 6 του Σχετικού 4), για το οποίο οι εκπρόσωποι της εταιρείας δήλωσαν ότι αποτελεί το προτεινόμενο υπόδειγμα και περιλαμβάνεται στις νέες συμβάσεις.

Πλην όμως, από την εξέταση των τμημάτων των συμβάσεων με τις εταιρείες και και ειδικότερα το άρθρο 9 αυτών («Εμπιστευτικότητα»), προκύπτει ότι δεν περιλαμβάνονται οι απαιτήσεις και τα μέτρα ασφάλειας που προβλέπει η παράγραφος 2.2.2 της Πολιτικής.

Στο έγγραφο-υπόδειγμα με τίτλο «Παράρτημα Πολιτικής Ασφάλειας», περιλαμβάνονται συγκεκριμένες απαιτήσεις και μέτρα ασφάλειας. Ωστόσο, το έγγραφο αυτό δεν φαίνεται να είναι τμήμα των ως άνω δύο συμβάσεων, παρόλο που η σύμβαση με την εταιρεία είναι μεταγενέστερη της ημερομηνίας έναρξης ισχύος της Πολιτικής της εταιρείας.

Απόκλιση 4: Δεν εφαρμόζεται πλήρως η παράγραφος 2.2.2 αναφορικά με τις απαιτήσεις και τα μέτρα ασφάλειας που λαμβάνονται για τη διασφάλιση του απορρήτου των επικοινωνιών στις συμβάσεις που συνάπτει η εταιρεία με συνεργάτες της (παράγραφος 4.3.2.2 του άρθρου 4 της Απόφασης 165/2011).

Η Ο.Ε. ζήτησε πληροφορίες αναφορικά με τη χρησιμοποίηση συνεργατών – υπεργολάβων από τους συνεργάτες Πιο συγκεκριμένα, ζήτησε να πληροφορηθεί, εάν η εταιρεία χρησιμοποιεί υπεργολάβους για την εκτέλεση των εργασιών που της έχουν ανατεθεί και εάν ναι, με ποιο τρόπο καλύπτονται οι όροι της Πολιτικής Ασφάλειας της εταιρείας που σχετίζονται με τους συνεργάτες. Η εταιρεία δήλωσε (Σχετικό 5) ότι, στο πλαίσιο υλοποίησης έργων που έχουν ανατεθεί από στην, είναι δυνατόν ορισμένα έργα, που περιλαμβάνουν χωματουργικές και δικτυακές εργασίες, να ανατίθενται από την σε υπεργολάβους, οι οποίοι δεσμεύονται μέσω ιδιωτικού συμφωνητικού ως προς όλους τους όρους της Κύριας Σύμβασης Ανάθεσης Έργου (και του σχετικού τεύχους προκήρυξης) που ισχύουν μεταξύ και Η εταιρεία απέστειλε, με το σχετικό 5, απόσπασμα Σύμβασης Ανάθεσης Έργου μεταξύ, καθώς και ιδιωτικό συμφωνητικό μεταξύ και υπεργολάβου. Από την εξέταση της Σύμβασης Ανάθεσης Έργου μεταξύ και διαπιστώθηκε ότι στο Παράρτημα Α «Υποχρεώσεις που προκύπτουν από την Πολιτική Ασφάλειας Τηλεπικοινωνιακού Δικτύου και Διασφάλισης Απορρήτου» αναφέρεται ότι «Οι συμβαλλόμενοι με συνεργάτες και εργολάβοι (αναφερόμενοι κατωτέρω ως συνεργάτες) λαμβάνουν γνώση και αποδέχονται να τηρούν καθ' όλη τη διάρκεια της σύμβασης τις παρακάτω υποχρεώσεις, που δεσμεύουν τους ίδιους, απευθείας το εμπλεκόμενο προσωπικό και τους παρεπόμενους συνεργάτες τους: ...». Επίσης, από την εξέταση του ιδιωτικού συμφωνητικού μεταξύ

και υπεργολάβου διαπιστώθηκε ότι αυτό λαμβάνει υπόψη του την Κύρια σύμβαση μεταξύ και

Από την εξέταση του Παραρτήματος Β («Σύμβαση Εμπιστευτικότητας») της Σύμβασης Ανάθεσης Έργου μεταξύ και διαπιστώθηκε ότι στις παραγράφους 4 και 8 αναφέρεται, για συγκεκριμένες υποχρεώσεις, η παραπομπή στον Κανονισμό 630^α/2005, δηλαδή σε κανονισμό της ΑΔΑΕ που έχει καταργηθεί. Επιπλέον, από την εξέταση του Παραρτήματος Α («Υποχρεώσεις που προκύπτουν από την Πολιτική Ασφάλειας Τηλεπικοινωνιακού Δικτύου και Διασφάλισης Απορρήτου») διαπιστώθηκε ότι είναι διαφορετικό από το έγγραφο «Παράρτημα Πολιτικής Ασφάλειας» (συνημμένο 6 του Σχετικού 4) το οποίο σύμφωνα με δήλωση της εταιρείας περιλαμβάνεται στις νέες συμβάσεις.

Παρατήρηση 4: Η εταιρεία οφείλει να επικαιροποιήσει τα Παραρτήματα Α και Β της Σύμβασης Ανάθεσης Έργου μεταξύ και σύμφωνα με τις παραπάνω παρατηρήσεις.

Παράγραφος 2.3.1

Η εταιρεία δήλωσε ότι έχουν αναρτήσει οδηγίες ορθής χρήσης και ασφάλειας στην ιστοσελίδα της εταιρείας και διαθέτουν σχετικά φυλλάδια στα καταστήματα Επίσης, η εταιρεία παρέδωσε υπόδειγμα μηνύματος ηλεκτρονικού ταχυδρομείου προς τους συνδρομητές της, με σκοπό την υπενθύμιση αλλαγής κωδικού πρόσβασης, στο οποίο περιλαμβάνονται και οδηγίες για γενικότερα θέματα ασφάλειας (συνημμένο 7 του Σχετικού 4).

4. Πολιτική Φυσικής Ασφάλειας (Άρθρο 5 της Απόφασης 165/2011, ΦΕΚ 2715/Β/17.11.2011)

Παράγραφος 2.1.2

Η Εταιρεία παρέδωσε ως Διαδικασία Φυσικής Πρόσβασης τα έγγραφα: «..... – Διαχείριση Φυσικής Πρόσβασης σε Εγκαταστάσεις της Εταιρείας», «..... – Διαχείριση Καρτών Πρόσβασης» και «Βασική εγκύκλιος με αριθ. 70 – Γενικά Θέματα Ασφάλειας (Διαδικασία Ελέγχου Φυσικής Πρόσβασης στις Κτιριακές Εγκαταστάσεις & Υποδομές») (συνημμένο 2 του σχετικού 4). Ωστόσο, κατά τον έλεγχο δήλωσε ότι η διαδικασία και η οδηγία εργασίας είναι σε φάση τελικής ανασκόπησης και εγκρίσεων και εφαρμόζονται πιλοτικά από 24/2/2014. Η διαδικασία φυσικής πρόσβασης που προβλέπεται στην παράγραφο 2.1.2 της Πολιτικής Φυσικής Ασφάλειας και είναι σε ισχύ, περιέχεται στην Βασική Εγκύκλιο με αριθμό 70/11 της 30.6.2008.

Παράγραφος 2.1.3

Αναφορικά με τις εγκρίσεις για την παροχή εξουσιοδότησης φυσικής πρόσβασης, σύμφωνα με την παράγραφο 2.1.3 της Πολιτικής Φυσικής Ασφάλειας και τη Βασική Εγκύκλιο 70/11, η εταιρεία παρέδωσε τα ακόλουθα:



- Τα από 2.9.2013 και 8.1.2014 έντυπα έγκρισης δικαιωμάτων φυσικής πρόσβασης για τους χώρους Αίθουσα(.....,), χώρος (.....), χώρος(.....), και χώρος (συνημμένο 3 του σχετικού 7), την από 7.11.2013 έγκριση για το χώρο (.....) (συνημμένο 4 του σχετικού 8) και τα αιτήματα χορήγησης δικαιωμάτων πρόσβασης και τις αντίστοιχες εγκρίσεις για το χώρο (.....) για το διάστημα 8.11.2013 – 31.12.2013 (συνημμένο 5 του σχετικού 7).
- τα εγκεκριμένα αιτήματα αδειών εισόδου για τα έτη 2013 και 2014 (συνημμένα 2 και 3 του σχετικού 22) για την παροχή εξουσιοδότησης φυσικής πρόσβασης στο χώρο
- τα εγκεκριμένα αιτήματα αδειών εισόδου για τα έτη 2013 και 2014 (συνημμένα 4 και 5 του σχετικού 24) για την παροχή εξουσιοδότησης φυσικής πρόσβασης στην εγκατάσταση επί της οδούκαι στους χώρους και

Από την εξέταση των παραπάνω εγγράφων διαπιστώθηκε ότι:

- οι εγκρίσεις της 2.9.2013, 8.1.2014 για τους χώρους Αίθουσα(.....), χώρος(.....), χώρος (.....), και και της 7.11.2013 για το χώρο (.....) αφορούν στην έγκριση για τη διατήρηση στο σύστημα των δικαιωμάτων φυσικής πρόσβασης που έχουν χορηγηθεί και όχι την έγκριση για τη χορήγηση των δικαιωμάτων σύμφωνα με την παράγραφο 2.1.3 της Πολιτικής Φυσικής Ασφάλειας.
- δυνατότητα εισόδου στο χώρο είχαν 34 εργαζόμενοι το 2013 και 41 το 2014. Αυτό έρχεται σε αντίθεση με τη δήλωση της εταιρείας κατά τον επιτόπιο έλεγχο ότι περιορισμένος αριθμός ατόμων (2) έχουν δυνατότητα πρόσβασης στο χώρο.

Από την αντιπαραβολή των αρχείων καταγραφής φυσικής πρόσβασης στους χώρους και για το χρονικό διάστημα από 1.10.2013 έως και 31.12.2013 με τα εγκεκριμένα αιτήματα αδειών εισόδου για το έτος 2013 δεν διαπιστώθηκε πρόσβαση εργαζομένου χωρίς να υπάρχει η αντίστοιχη άδεια.

Από τη δειγματοληπτική αντιπαραβολή των αρχείων καταγραφών φυσικής πρόσβασης για την εγκατάσταση επί της οδού για την 30 και 31/12/2013 με τα εγκεκριμένα αιτήματα αδειών εισόδου για το έτος 2013 διαπιστώθηκε ότι οι κάτοχοι κάρτας:,,,,, και δεν βρέθηκαν στο έντυπο με τα εγκεκριμένα αιτήματα αδειών εισόδου.

Απόκλιση 5: Δεν εφαρμόζεται η παράγραφος 2.1.3 (παράγραφος 5.2.3, εδ. α,' του άρθρου 5 της Απόφασης 165/2011)

Παράγραφος 2.1.4



Η εταιρεία παρέδωσε το αρχείο από το σύστημα στο οποίο διατηρείται το ιστορικό χορήγησης/κατάργησης των δικαιωμάτων πρόσβασης που έχουν εν τοις πράγμασι χορηγηθεί, μέσω του αρχείου καταγραφής των ενεργειών των διαχειριστών του συστήματος (Συνημμένο 4 του Σχετικού 6).

Από την αντιπαραβολή των αρχείων καταγραφής φυσικής πρόσβασης για τους χώρους (.....),, Αίθουσα (.....), χώρος (.....), χώρος(.....), και χώρος και του αρχείου με το ιστορικό χορήγησης/κατάργησης των δικαιωμάτων πρόσβασης διαπιστώθηκε ότι υπάρχουν προσβάσεις υπαλλήλων (....., χώρος και,,, και, χώρος (.....)) οι οποίοι δεν βρέθηκαν στο αρχείο με το ιστορικό χορήγησης/κατάργησης των δικαιωμάτων πρόσβασης που έχουν εν τοις πράγμασι χορηγηθεί.

Απόκλιση 6: Δεν εφαρμόζεται συστηματικά η παράγραφος 2.1.4 (παράγραφος 5.2.3, εδ. β', του άρθρου 5 της Απόφασης 165/2011)

Παράγραφος 2.1.5

Η Ο.Ε. διαπίστωσε από τον επιτόπιο έλεγχο στις εγκαταστάσεις, επί της, στη ότι η πρόσβαση στις εγκαταστάσεις δεν καταγράφεται.

Η Ο.Ε. διαπίστωσε ότι η πρόσβαση στις εγκαταστάσεις, επί της οδού είναι ελεγχόμενη μέσω καρτανανγνώστη και καταγράφεται. Η εταιρεία παρέδωσε τα αρχεία καταγραφής φυσικής πρόσβασης, σύμφωνα με την παράγραφο 2.1.5, για την εγκατάσταση επί της οδού για το διάστημα από 1.10.2013 έως και 31.12.2013

Απόκλιση 7: Δεν εφαρμόζεται για όλες τις εγκαταστάσεις η παράγραφος 2.1.5 (παράγραφος 5.2.4 του άρθρου 5 της Απόφασης 165/2011).

Παράγραφος 2.1.7

Η εταιρεία παρέδωσε το αρχείο με τους χώρους εγκατάστασης συστημάτων και μηχανισμών ασφάλειας σε αυτούς, σύμφωνα με την παράγραφο 2.1.7 (συνημμένα 2α, 2β και 2γ του σχετικού 6).

Από την εξέταση των αρχείων αυτών διαπιστώθηκε ότι:

- στους χώρους εγκατάστασης των συστημάτων, και δεν υπάρχει εγκατεστημένο κλειστό κύκλωμα τηλεόρασης (.....) και σύστημα ανίχνευσης μη εξουσιοδοτημένης πρόσβασης (intruder detection) ή άλλος ισχυρός μηχανισμός.
- στο χώρο του (.....) αναφέρεται ότι δεν λειτουργεί ο καρτανανγνώστης του συστήματος access control.

Η εταιρεία, κατά τον έλεγχο των αρχείων καταγραφής φυσικής πρόσβασης σε 7 χώρους ΠΕΣ (παράγραφος 2.1.8), δήλωσε ότι ο χώρος δεν διαθέτει ηλεκτρονικό σύστημα ελέγχου φυσικής



πρόσβασης. Ωστόσο, στο αρχείο με τους χώρους εγκατάστασης συστημάτων και μηχανισμών ασφάλειας σε αυτούς καταγράφεται ότι ο χώρος διαθέτει σύστημα ελέγχου πρόσβασης με καρταναγνώστη (card reader).

Από τον έλεγχο των μηχανισμών ασφάλειας, σύμφωνα με το έντυπο «καταγραφή χώρων – μηχανισμών φυσικής ασφάλειας», (συνημμένο 2γ του σχετικού 6), στο χώρο του διαπιστώθηκε ότι ο καρταναγνώστης έχει τεθεί εκτός λειτουργίας. Οι εκπρόσωποι δήλωσαν ότι ο καρταναγνώστης δεν χρησιμοποιείται λόγω αλλαγής χρήσης του συγκεκριμένου χώρου (κατάργηση της συστέγασης του κέντρου διαχείρισης δικτύου) και του περιορισμένου αριθμού ατόμων (2) με δυνατότητα πρόσβασης στο χώρο. Η καταγραφή της πρόσβασης στο χώρο πραγματοποιείται σε έντυπο.

Από τον έλεγχο των μηχανισμών ασφάλειας, σύμφωνα με το έντυπο «καταγραφή χώρων – μηχανισμών φυσικής ασφάλειας», (συνημμένο 2γ του σχετικού 6), στο χώρο του διαπιστώθηκε ότι οι μηχανισμοί είναι σε ισχύ. Σχετικά με τους μηχανισμούς ασφάλειας των χώρων,,, που καταγράφονται στο παραπάνω έντυπο, η εταιρεία δήλωσε ότι ο έλεγχος πρόσβασης στους χώρουςπραγματοποιείται μέσω καρταναγνώστη στην είσοδο των εγκαταστάσεων, στους οποίους υπάρχουν οι παραπάνω χώροι, δεδομένου ότι οι εγκαταστάσεις αυτές είναι περιορισμένες σε μέγεθος, και ουσιαστικά στεγάζουν και το χώρο

Απόκλιση 8: Δεν εφαρμόζεται για όλους τους χώρους εγκατάστασης ΠΕΣ η παράγραφος 2.1.7 αναφορικά με την προστασία τους από ισχυρούς μηχανισμούς ασφάλειας και ελεγχόμενης πρόσβασης (παράγραφος 5.2.5 του άρθρου 5 της Απόφασης 165/2011).

Παρατήρηση 5: Η εταιρεία, σύμφωνα με τον κατάλογο συστημάτων που παρέδωσε, χρησιμοποιεί δύο συστήματα για τη μεταγωγή (switching) των κυκλωμάτων στα κέντρα (τερματικά, διαβιβαστικά, διεθνή, κτλ.), το σύστημα και το

Παράγραφος 2.1.8

Η εταιρεία παρέδωσε τα αρχεία καταγραφής φυσικής πρόσβασης, σύμφωνα με την παράγραφο 2.1.8, για τους χώρους (.....),, Αίθουσα (.....), χώρος (.....), χώρος (.....), και χώρος, για το χρονικό διάστημα από 1.10.2013 έως και 31.12.2013 (Συνημμένο 3 του Σχετικού 6). Σημειώνεται ότι η Ο.Ε. ζήτησε τα αρχεία καταγραφής φυσικής πρόσβασης και για το χώρο, για τον οποίο η εταιρεία δήλωσε ότι δεν υπάρχουν, λόγω βλάβης του συστήματος ελέγχου φυσικής πρόσβασης τη συγκεκριμένη χρονική περίοδο.

Η εταιρεία παρέδωσε τα αρχεία καταγραφής φυσικής πρόσβασης στους χώρους και για το χρονικό διάστημα από 1.10.2013 έως και 31.12.2013 (συνημμένα 1 και 2 του σχετικού 24).



Από την εξέταση των αρχείων αυτών διαπιστώθηκε ότι:

- υπάρχει μια πρόσβαση στο χώρο (.....) στην οποία δεν καταγράφεται το ονοματεπώνυμο αλλά ο αριθμός 8785524305.
- καταγράφονται συμβάντα αφόπλισης και όπλισης, χωρίς να υπάρχει ταυτόχρονα η καταγραφή της εισόδου και εξόδου στους χώρους ΠΕΣ. Η εταιρεία, αναφορικά με αυτό το γεγονός, δήλωσε ότι η διαδικασία προβλέπει μετά την αφόπλιση να ακολουθεί εκ νέου ανάγνωση της κάρτας εισόδου ώστε να επιτρέπεται η είσοδος στον χώρο. Όμως σε πολλές περιπτώσεις, επειδή είναι σε εξέλιξη αλλά δεν έχει ολοκληρωθεί ακόμα η κατάργηση της δυνατότητας ανοίγματος με συμβατικά μέσα (κλειδί), είναι δυνατόν να γίνει είσοδος χωρίς εκ νέου ανάγνωση της κάρτας εισόδου, κατά συνέπεια δεν καταγράφεται στα αρχεία καταγραφής το συμβάν της εισόδου ως ξεχωριστό συμβάν.
- ενώ καταγράφεται το ονοματεπώνυμο και η ώρα εισόδου, δεν καταγράφεται συστηματικά η ώρα εξόδου.

Απόκλιση 9: Δεν εφαρμόζεται πλήρως η παράγραφος 2.1.8 (παράγραφος 5.2.5 του άρθρου 5 της Απόφασης 165/2011).

Παράγραφος 2.1.10

Η εταιρεία δήλωσε ότι το αρχείο των μηχανισμών ασφάλειας για τα Συστήματα που τοποθετούνται εκτός των εγκαταστάσεών της (παράγραφος 2.1.10 της Πολιτικής Φυσικής Ασφάλειας) δεν διατηρείται, διότι δεν υπάρχουν Συστήματα εκτός των εγκαταστάσεών της. Ωστόσο, η εταιρεία παρέδωσε, σχετικά με τους μηχανισμούς ασφάλειας, τα ακόλουθα έγγραφα:

- Οδηγία Εργασίας (Συνημμένο 5α του Σχετικού 6)
- Ειδική Εγκύκλιο με αριθμό 730/3333 από 1.10.2009 (Συνημμένο 5β του Σχετικού 6)
- Το υπ.αριθμ. 730/526066 από 25.10.2010 της Γενικής Διεύθυνσης Περιφερειών (Συνημμένο 5γ του Σχετικού 6)
- Το υπ.αριθμ. 730/524401 από 18.2.2010 της Γενικής Διεύθυνσης Περιφερειών (Συνημμένο 5δ του Σχετικού 6)
- Οδηγό Χρήσης(έκδοση 01.30 από 11.5.2009) (Συνημμένο 5ε του Σχετικού 6)
- Περιγραφή Λειτουργίας(Συνημμένο 5στ του Σχετικού 6)

Επιπλέον, σε επόμενο έλεγχο, παρέδωσε το έγγραφο «Συνοπτική Περιγραφή Μηχανισμών/Μέτρων Ασφάλειας» (Συνημμένο 1 του Σχετικού 8).

Παρατήρηση 6:

Ειδική Εγκύκλιος 730/3333/1.10.2009: «Ασφάλεια Υλικού – Διαχείριση κλειδιών»

Η Ο.Ε. διαπίστωσε, από τον έλεγχο, ότι τηρείται το βιβλίο διαχείρισης κλειδιώντεχνικού τμήματος, σύμφωνα με την ειδική εγκύκλιο.

Οδηγία Εργασίας: «Αναγνώριση & ενημέρωση Συμβάντος»

Η εταιρεία δήλωσε ότι η παρακολούθηση των συμβάντων, στη, πραγματοποιείται από τον, εργαζόμενο του Αναφορικά με την παρακολούθηση, η Ο.Ε. ζήτησε πληροφορίες, και πιο συγκεκριμένα τι ενέργειες πραγματοποιήθηκαν ώστε να διερευνηθεί η εγγραφή «άγνωστη αιτία», σε τέσσερις συγκεκριμένες εγγραφές.....

.....

.....

Απόκλιση 10: Δεν εφαρμόζεται συστηματικά η οδηγία εργασίας: «Αναγνώριση & ενημέρωση Συμβάντος»

5. Πολιτική Λογικής Πρόσβασης (Άρθρο 6 της Απόφασης 165/2011, ΦΕΚ 2715/Β/17.11.2011)

Παράγραφος 2.1.3

Σχετικά με το αρχείο που αναφέρει αναλυτικά τους μηχανισμούς ελέγχου πρόσβασης και αυθεντικοποίησης για κάθε Σύστημα, η εταιρεία δήλωσε ότι διατηρεί ένα αρχείο excel ανά ΠΕΣ και παρέδωσε εκτύπωση αυτών (23 έγγραφα, Συνημμένο 3 του Σχετικού 8).

Παράγραφος 2.1.9

Σχετικά με το αρχείο στο οποίο καταγράφονται η συχνότητα και οι τρόποι με τους οποίους πραγματοποιείται η περιοδική αλλαγή των κωδικών πρόσβασης, η εταιρεία δήλωσε ότι η σχετική πληροφορία περιέχεται στα έγγραφα του Συνημμένου 3 του Σχετικού 8.

Από την εξέταση των εγγράφων αυτών προκύπτουν τα ακόλουθα:

- i. Για το σύστημα, αναφέρει ότι δεν αλλάζει ο κωδικός πρόσβασης σε επίπεδο εφαρμογής («no change»). Πλην όμως, το γεγονός αυτό δεν έχει καταγραφεί στα έντυπα καταγραφής εξαιρέσεων.
- ii. Για το σύστημα, δεν αναφέρεται η συχνότητα αλλαγής του κωδικού πρόσβασης σε επίπεδο λειτουργικού συστήματος.
- iii. Για το σύστημα, δεν αναφέρεται η συχνότητα αλλαγής του κωδικού πρόσβασης σε επίπεδο εφαρμογής, βάσης δεδομένων και λειτουργικού συστήματος.



- iv. Για το σύστημα, δεν αναφέρεται η συχνότητα αλλαγής του κωδικού πρόσβασης σε επίπεδο βάσης δεδομένων και λειτουργικού συστήματος. Δεν είναι κατανοητό αν η συχνότητα αλλαγής που εφαρμόζεται σε επίπεδο εφαρμογής ισχύει και για το επίπεδο βάσης δεδομένων και λειτουργικού συστήματος.
- v. Για το σύστημα, δεν αναφέρεται η συχνότητα αλλαγής του κωδικού πρόσβασης σε επίπεδο εφαρμογής, βάσης δεδομένων και λειτουργικού συστήματος.
- vi. Για το σύστημα, δεν αναφέρεται η συχνότητα αλλαγής του κωδικού πρόσβασης σε επίπεδο εφαρμογής, βάσης δεδομένων και λειτουργικού συστήματος.
- vii. Για το σύστημα, δεν αναφέρεται η συχνότητα αλλαγής του κωδικού πρόσβασης σε επίπεδο εφαρμογής, βάσης δεδομένων και λειτουργικού συστήματος.
- viii. Για το σύστημα, δεν αναφέρεται η συχνότητα αλλαγής του κωδικού πρόσβασης σε επίπεδο εφαρμογής, βάσης δεδομένων και λειτουργικού συστήματος.
- ix. Για το σύστημα, δεν αναφέρεται η συχνότητα αλλαγής του κωδικού πρόσβασης σε επίπεδο εφαρμογής, βάσης δεδομένων και λειτουργικού συστήματος. Σχετικά με το επίπεδο εφαρμογής, το έγγραφο παραπέμπει στην πολιτική του κεντρικού domain (central domain policy).
- x. Για το σύστημα, δεν αναφέρεται η συχνότητα αλλαγής του κωδικού πρόσβασης σε επίπεδο εφαρμογής, βάσης δεδομένων και λειτουργικού συστήματος. Σχετικά με το επίπεδο εφαρμογής, το έγγραφο παραπέμπει στην πολιτική του κεντρικού domain (central domain policy).
- xi. Για το σύστημα, δεν αναφέρεται η συχνότητα αλλαγής του κωδικού πρόσβασης σε επίπεδο εφαρμογής, βάσης δεδομένων και λειτουργικού συστήματος.
- xii. Για το σύστημα, δεν αναφέρεται η συχνότητα αλλαγής του κωδικού πρόσβασης σε επίπεδο βάσης δεδομένων και λειτουργικού συστήματος.
- xiii. Για το σύστημα, δεν αναφέρεται η συχνότητα αλλαγής του κωδικού πρόσβασης σε επίπεδο εφαρμογής, βάσης δεδομένων και λειτουργικού συστήματος. Επιπλέον, δεν αναφέρεται η μέθοδος πραγματοποίησης αλλαγής του κωδικού πρόσβασης για το επίπεδο βάσης δεδομένων και λειτουργικού συστήματος.

Απόκλιση 11: Δεν εφαρμόζεται πλήρως η παράγραφος 2.1.9 αναφορικά με την καταγραφή της συχνότητας και των τρόπων με τους οποίους πραγματοποιείται η περιοδική αλλαγή των κωδικών πρόσβασης (παράγραφος 6.4.2.3 του άρθρου 6 της Απόφασης 165/2011).

Παράγραφοι 2.2.1 και 2.2.2

Σχετικά με το Αρχείο με περιγραφή των κανόνων δημιουργίας ονόματος χρήστη και το Αρχείο με περιγραφή των κανόνων δημιουργίας κωδικών πρόσβασης, η εταιρεία παρέδωσε το Εγχειρίδιο (Συνημμένο 4 του Σχετικού 8) με τίτλο «Κανόνες Δημιουργίας Αναγνωριστικών Χρηστών» και το Εγχειρίδιο (Συνημμένο 5 του Σχετικού 8) με τίτλο «Κανόνες Δημιουργίας Κωδικών Πρόσβασης».

Προκειμένου να διαπιστωθεί ότι οι κανόνες αυτές εφαρμόζονται και στην πράξη, η Ο.Ε. ζήτησε και παρέλαβε για τα ΠΕΣ (Συνημμένο 6 του Σχετικού 8), (Συνημμένο 7 του Σχετικού 8), (Συνημμένο 8 του Σχετικού 8) και (Συνημμένο 9 του Σχετικού 8) εκτύπωση (printout) των κανόνων δημιουργίας και διαχείρισης κωδικών πρόσβασης, που έχουν οριστεί σε επίπεδο εφαρμογής, λειτουργικού συστήματος και βάσης δεδομένων. Από την εξέταση των παραπάνω εγγράφων προκύπτει ότι οι κανόνες δημιουργίας κωδικών πρόσβασης τηρούνται σε όλα τα συστήματα πλην μίας περίπτωσης. Στο σύστημαστο επίπεδο εφαρμογής, ορίζεται ότι το ελάχιστο μήκος κωδικού πρόσβασης είναι έξι (6) χαρακτήρες, ενώ το εγχειρίδιο αναφέρει ότι το ελάχιστο μήκος είναι οκτώ (8) χαρακτήρες. Επίσης, επισημαίνεται ότι η εκτύπωση (printout) των κανόνων δημιουργίας κωδικών πρόσβασης του συστήματος σε επίπεδο λειτουργικού συστήματος δεν αναφέρουν το ελάχιστο μήκος κωδικού πρόσβασης, και συνεπώς δεν μπορεί να πραγματοποιηθεί ο εν λόγω έλεγχος.

Απόκλιση 12: Δεν εφαρμόζεται η παράγραφος 4 του Εγχειριδίου σχετικά με το ελάχιστο μήκος των κωδικών πρόσβασης (παράγραφος 6.4.2.2 του άρθρου 6 της Απόφασης 165/2011).

Παράγραφος 2.2.5

Η εταιρεία παρέδωσε το εγχειρίδιο (Συνημμένο 10 του Σχετικού 8) με τίτλο «Όροι Χρήσης Κωδικών Πρόσβασης» με περιγραφή των όρων χρήσης των κωδικών πρόσβασης από τους εργαζόμενους και συνεργάτες.

Παράγραφος 2.2.10

Η εταιρεία παρέδωσε το εγχειρίδιο με τίτλο «Αρχείο Καταγραφής Μηχανισμών Αντιστοίχισης Ενεργειών Ομαδικού ή Προκαθορισμένου Λογαριασμού με Φυσικό Πρόσωπο» (Συνημμένο 11 του Σχετικού 8).

Παρατήρηση 7: Επειδή, από το ως άνω έγγραφο, δεν είναι απόλυτα σαφές εάν το σύνολο των μηχανισμών αυτών εφαρμόζονται σε κάθε ΠΕΣ, η εταιρεία οφείλει να εξειδικεύσει τους συγκεκριμένους μηχανισμούς που εφαρμόζονται ανά ΠΕΣ.

Παράγραφος 2.3

Σύμφωνα με τον Κατάλογο Αντιστοίχισης Διαδικασιών, η εν λόγω διαδικασία είναι η διαδικασία με κωδικό εγγράφου «Διαχείριση Δικαιωμάτων Πρόσβασης σε Πληροφοριακά Συστήματα». Σύμφωνα με την εν λόγω διαδικασία, για τη δημιουργία νέου χρήστη ή κατάργηση υφιστάμενου σε ΠΕΣ



της εταιρείας, προηγείται καταχώρηση και επεξεργασία σχετικού αιτήματος στο σύστημα ...της εταιρείας, τόσο για τους εργαζόμενους όσο και για τους εξωτερικούς συνεργάτες.

Προκειμένου να ελεγχθεί δειγματοληπτικά η εφαρμογή της ως άνω διαδικασίας, η Ο.Ε. ζήτησε και παρέλαβε για τα ΠΕΣ τον κατάλογο των λογαριασμών (accounts) που προκύπτουν από το σύστημα σε επίπεδο εφαρμογής, λειτουργικού συστήματος και βάσης δεδομένων (Συνημμένο 1 του Σχετικού 9) και τον κατάλογο των λογαριασμών που προκύπτουν από το σύστημα (Συνημμένο 12 του Σχετικού 8 και Συνημμένα 2, 3, και 4 του Σχετικού 9). Από την εξέταση των ως άνω εγγράφων προκύπτουν τα ακόλουθα:

A) Σύστημα

Η αντιπαραβολή πραγματοποιήθηκε με χρήση και του συστήματος (περιφερειών), για το οποίο η εταιρεία δηλώνει ότι αποτελεί υποσύστημα του, παρόλο που δεν το έχει δηλώσει στη λίστα των ΠΕΣ που παρέδωσε κατά τον πρώτο επιτόπιο έλεγχο.

Στο επίπεδο της εφαρμογής, δεν βρέθηκαν αιτήματα στο σύστημα ... για τους λογαριασμούς:

Στο επίπεδο της βάσης δεδομένων, η εταιρεία παρέδωσε κατάλογο με 335 accounts που έχουν οριστεί στο σύστημα, αλλά ο αντίστοιχος κατάλογος από το σύστημα περιέχει 12 accounts. Σε περαιτέρω αντιπαραβολή και με τη λίστα του επιπέδου εφαρμογής για το σύστημα, στο δειγματοληπτικό έλεγχο εξήντα (60) από τα 335 accounts, τα είκοσι τέσσερα (24) από αυτά δεν βρέθηκαν στον κατάλογο του συστήματος

Στο επίπεδο του λειτουργικού συστήματος, δεν βρέθηκαν εγκρίσεις για τα accounts:, καθώς και για τα συστημικά accounts.

B) Σύστημα

Στο επίπεδο της εφαρμογής, δεν βρέθηκαν αιτήματα στο σύστημα για τους λογαριασμούς:

Στο επίπεδο της βάσης δεδομένων, δεν βρέθηκαν εγκρίσεις για το account, καθώς και για τα συστημικά accounts.

Στο επίπεδο του λειτουργικού συστήματος, δεν βρέθηκαν εγκρίσεις για τα accounts:....., καθώς και για τα συστημικά accounts.

Γ) Σύστημα

Σε επίπεδο εφαρμογής, δεν βρέθηκαν αιτήματα στο σύστημα για τους λογαριασμούς: (αν και υπάρχει το που πιθανόν ανήκει στο ίδιο πρόσωπο),

Στο επίπεδο λειτουργικού συστήματος, δεν βρέθηκαν εγκρίσεις για τα accounts:, καθώς και για τα συστημικά accounts. Επιπρόσθετα, δεν υπάρχει ακριβής αντιστοίχιση για τα παρακάτω accounts:



(υπάρχει τοστο),..... (υπάρχει το στο), (υπάρχει το στο), (υπάρχει το στο), (υπάρχει το στο), (υπάρχει το στο).

Επιπλέον, η εταιρεία παρέδωσε με το Σχετικό 10 έντυπες αιτήσεις-εγκρίσεις προσβάσεων στο σύστημα, για τις περιπτώσεις που δεν είχε καταστεί εφικτή η αίτηση μέσω (επί παραδείγματι, account:.....).

Δ) Σύστημα

Σε επίπεδο εφαρμογής, δεν βρέθηκαν αιτήματα στο σύστημαγια τους λογαριασμούς: Επιπρόσθετα, επισημαίνεται ότι τα περισσότερα αναγνωριστικά χρήστη στο σύστημα παρουσιάζουν διαφορές σε σύγκριση με τον κατάλογο του συστήματος, παρόλο που το ονοματεπώνυμο του εργαζόμενου συμπίπτει. Επιπλέον, η εταιρεία παρέδωσε με το Σχετικό 10 έντυπες αιτήσεις-εγκρίσεις προσβάσεων στο σύστημα, για τις περιπτώσεις που δεν είχε καταστεί εφικτή η αίτηση μέσω(επί παραδείγματι, accounts:).

Στο επίπεδο λειτουργικού συστήματος, δεν βρέθηκαν εγκρίσεις για τα accounts:, καθώς και για τα συστημικά accounts.

Απόκλιση 13: Δεν εφαρμόζεται συστηματικά η διαδικασία «Διαχείριση Δικαιωμάτων Πρόσβασης σε Πληροφοριακά Συστήματα» της παραγράφου 2.3 (ειδικότερα οι 2.3.3 και 2.3.4) αναφορικά με την δημιουργία νέου χρήστη σε ΠΕΣ της εταιρείας (παράγραφος 6.3.1 του άρθρου 6 της Απόφασης 165/2011).

Παράγραφος 2.3.5

Η εταιρεία παρέδωσε τα δικαιώματα πρόσβασης των λογαριασμών που έχουν εγκριθεί, ενεργοποιηθεί και καταργηθεί στα παραπάνω ΠΕΣ, όπως προκύπτουν από το σύστημα, από 1.9.2013 (Συνημμένο 13 του Σχετικού 8). Από την εξέταση του ως άνω εγγράφου, προκύπτει ότι το αρχείο περιέχει την ενέργεια της αίτησης και έγκρισης για τη δημιουργία ή τερματισμό ενός λογαριασμού (account), τον χρόνο που πραγματοποιήθηκε η ενέργεια, και το λογαριασμό στον οποίο αναφέρεται. Δεν ακολουθεί τη δομή που περιγράφεται στην παράγραφο 2.3.5 (λογαριασμός πρόσβασης, προφίλ, χρονικό διάστημα ισχύος) και ειδικά δεν αναφέρει τα δικαιώματα ή επίπεδο πρόσβασης των λογαριασμών που έχουν εγκριθεί και ενεργοποιηθεί στα ΠΕΣ.

Απόκλιση 14: Δεν εφαρμόζεται πλήρως η παράγραφος 2.3.5 αναφορικά με το Αρχείο με το ιστορικό όλων των δικαιωμάτων ή επιπέδων πρόσβασης των λογαριασμών που έχουν εγκριθεί και ενεργοποιηθεί στα Συστήματα (παράγραφος 6.3.1.4 του άρθρου 6 της Απόφασης 165/2011).

Παράγραφος 2.3.7

Η εταιρεία παρέδωσε το έγγραφο με τίτλο «Αρχείο Μηχανισμών Πρόσβασης σε Δεδομένα Επικοινωνίας» (Συνημμένο 14 του Σχετικού 8).

Παράγραφος 2.3.8

Σχετικά με το αρχείο με την αντιστοίχιση των λογαριασμών πρόσβασης των εργαζόμενων και συνεργατών στους οποίους αυτοί έχουν αποδοθεί, η εταιρεία δήλωσε ότι η πληροφορία αυτή περιλαμβάνεται στο Συνημμένο 12 του Σχετικού 8.

Παράγραφος 2.4

Σύμφωνα με τον Κατάλογο Αντιστοίχισης Διαδικασιών, η εν λόγω διαδικασία είναι η διαδικασία με κωδικό εγγράφου «Έλεγχος Ορθής Εφαρμογής της Πολιτικής Λογικής Πρόσβασης». Σύμφωνα με την εν λόγω διαδικασία, η εταιρεία διενεργεί έξι (6) ελέγχους, οι οποίοι περιληπτικά είναι ο έλεγχος υλοποιημένων λογαριασμών πρόσβασης, ο έλεγχος δικαιωμάτων πρόσβασης, ο έλεγχος δικαιωμάτων πρόσβασης λογαριασμών (ανακάλυψη μη αιτιολογημένων προσβάσεων), έλεγχος εφαρμογής κανόνων δημιουργίας ονόματος χρήστη, έλεγχος διαδικασίας απόδοσης ονόματος χρήστη, και έλεγχος εφαρμογής κανόνων δημιουργίας κωδικών πρόσβασης. Η διαδικασία προβλέπει ότι τα αποτελέσματα του ελέγχου καταγράφονται στην αναφορά ελέγχου ορθότητας δικαιωμάτων πρόσβασης. Η εταιρεία παρέδωσε τις σχετικές αναφορές για τα συστήματα ΙΤ και τα συστήματα δικτύου, που αφορούν στο τρίτο τρίμηνο του 2013 (Συνημμένο 17 του Σχετικού 8). Από την εξέταση των παραπάνω αναφορών, προκύπτουν τα ακόλουθα:

A) Σύμφωνα με το περιεχόμενο των αναφορών, πραγματοποιήθηκε μόνο ο πρώτος έλεγχος από τους έξι που προβλέπει η διαδικασία (ο έλεγχος υλοποιημένων λογαριασμών πρόσβασης).

B) Από την αναφορά ελέγχου ορθότητας δικαιωμάτων πρόσβασης για τα συστήματα ΙΤ απουσιάζουν τα ΠΕΣ Σχετικά με αυτό, η εταιρεία δήλωσε (Σχετικό 25) ότι για το σύστημα δεν είχε πραγματοποιήσει τον σχετικό έλεγχο, ενώ για το σύστημα ο έλεγχος δεν πραγματοποιήθηκε γιατί το σύστημα χρησιμοποιείται αποκλειστικά από πελάτες. Πλην όμως, η Ο.Ε. θεωρεί ότι για το σύστημα ο έλεγχος μπορεί να πραγματοποιηθεί σε επίπεδο λειτουργικού συστήματος ή/και βάσης δεδομένων (εφόσον χρησιμοποιεί βάση δεδομένων).

Επιπρόσθετα, η εταιρεία παρέδωσε την πιο πρόσφατη Αναφορά Ελέγχου Ορθότητας Δικαιωμάτων Πρόσβασης για τα συστήματα ΙΤ του πρώτου τριμήνου του 2014 (Συνημμένο 2 του Σχετικού 25), στην οποία περιλαμβάνονται και οι χρήστες του

Απόκλιση 15: Δεν εφαρμόζεται πλήρως η παράγραφος 2.4.2 αναφορικά με τους ελέγχους που πρέπει να πραγματοποιούνται βάσει της διαδικασίας ελέγχου ορθής εφαρμογής της πολιτικής λογικής πρόσβασης (παράγραφος 6.3.2 του άρθρου 6 της Απόφασης 165/2011).



Επιπλέον, επισημαίνεται ότι στις δύο αναφορές που αφορούν στο τρίτο τρίμηνο του 2013 υπάρχουν ευρήματα, ενδεικτικά αναφέρεται ότι στα συστήματα IT βρέθηκαν 5617 λογαριασμοί χρηστών χωρίς αντίστοιχο αίτημα στο σύστημα, ενώ αντίστοιχα για τα συστήματα δικτύου, ο αριθμός αυτός είναι 362. Στην αναφορά του πρώτου τριμήνου του 2014 εξακολουθούν να υπάρχουν λογαριασμοί χρηστών χωρίς αντίστοιχο αίτημα στο σύστημα, παρόλο που ο αριθμός έχει μειωθεί σημαντικά.

Παράγραφος 2.5.1

Η εταιρεία παρέδωσε για τα ΠΕΣ, τα αρχεία καταγραφής πρόσβασης (access logs) για την περίοδο 1.9.2013 έως και 28.2.2014 με το Συνημμένο 5 του Σχετικού 9, ενώ ειδικά για το σε επίπεδο εφαρμογής απέστειλε ξανά το σχετικό αρχείο με το Συνημμένο 1 του Σχετικού 26. Από την εξέταση των ως άνω αρχείων προκύπτουν τα εξής:

A) σε ορισμένα αρχεία καταγραφής πρόσβασης δεν καταγράφεται ο χρόνος τερματισμού της πρόσβασης, ενδεικτικά: σύστημα, σύστημα σε επίπεδο βάσης δεδομένων, και σύστημα σε επίπεδο εφαρμογής και λειτουργικού συστήματος.

B) ορισμένα αρχεία καταγραφής περιέχουν ενέργειες χρηστών και όχι τα γεγονότα της εκκίνησης ή τερματισμού της πρόσβασης από τους χρήστες, ενδεικτικά για το σύστημα, και το σύστημα σε επίπεδο εφαρμογής.

Επισημαίνεται ότι η εταιρεία δήλωσε (Σχετικό 9) ότι «στο σύστημα, τα αρχεία καταγραφής πρόσβασης που αφορούν το υποσύστημα, μέσω του οποίου δίνεται πρόσβαση σε περιορισμένο αριθμό εξουσιοδοτημένων χρηστών στα mail logs, δεν είναι διαθέσιμα για το χρονικό διάστημα από 1-9-2013 έως και 15-2-2014, λόγω τεχνικού προβλήματος».

Παρατήρηση 8: Τα αρχεία καταγραφής πρόσβασης των χρηστών των ΠΕΣ σε αυτά, οφείλουν να καταγράφουν ευκρινώς, κατ' ελάχιστον, το όνομα χρήστη, που απέκτησε την πρόσβαση, και την ημερομηνία και ώρα εκκίνησης και τερματισμού της πρόσβασης, σύμφωνα με την παράγραφο 2.5.1 της πολιτικής της εταιρείας (παράγραφος 6.2.5 του άρθρου 6 της Απόφασης 165/2011).

Παράγραφος 2.5.2

Η εταιρεία παρέδωσε για τα ΠΕΣ, τις προσβάσεις σε δεδομένα επικοινωνίας και τις σχετικές αιτιολογήσεις, για την περίοδο από 1.12.2013 έως και 31.12.2013 (Συνημμένα 5 και 6 του Σχετικού 9).

Η Ο.Ε., κατά τη διάρκεια του 11^{ου} επιτόπιου ελέγχου (Σχετικό 21), έλεγξε δειγματοληπτικά δέκα (10) έγγραφα προσβάσεων σε δεδομένα επικοινωνίας στα συστήματα και διαπίστωσε ότι τα έγγραφα που αναφέρονται στο πεδίο «Justification» των έντυπων «Αιτιολογήσεις προσβάσεων σε δεδομένα επικοινωνίας για τον 12/2013 στο σύστημα» και «Αιτιολογήσεις προσβάσεων σε



δεδομένα επικοινωνίας για τον 12/2013 στο σύστημα» (Συνημμένο 6 του Σχετικού 9) διατηρούνται και αιτιολογούν τις προσβάσεις.

Σχετικά με το σύστημα, η Ο.Ε., από τον κατάλογο «Αιτιολογήσεις Προσβάσεων σε Δεδομένα Επικοινωνίας για τον 12/2013 στο Σύστημα» (Συν. 6 του Σχετικού 9), ζήτησε τα έγγραφα των αιτιολογήσεων των εγγραφών που αναγράφονται στο Συνημμένο 1 του Σχετικού 25. Η εταιρεία απέστειλε τα ζητηθέντα με το Συνημμένο 2 του Σχετικού 26. Από την εξέταση των παραπάνω στοιχείων προέκυψε ότι:

Α) Για την εγγραφή «Dec 6 14:31:34 ...», η εταιρεία δηλώνει ότι «*Η αναζήτηση έχει γίνει με βάση το message ID που έχει δοθεί από πελάτη με προφορικό αίτημα*», χωρίς να διατηρεί σχετικό έγγραφο.

Β) Για τις εγγραφές «Dec 20 10:02:40...», «Dec 20 10:03:26...», «Dec 20 10:03:36...», που αφορούν πρόσβαση στον ίδιο λογαριασμό ηλεκτρονικού ταχυδρομείου, η εταιρεία δηλώνει ότι αποτελεί «*προφορικό αίτημα συναδέλφου (επιβεβαιώθηκε με e-mail)*». Το email έχει ημερομηνία 15.10.2014, μεταγενέστερη του επιτόπιου ελέγχου, ενώ επιπλέον δεν προκύπτει η σύνδεση του ονόματος ηλεκτρονικού ταχυδρομείου με το όνομα του προσώπου, δεδομένου ότι συνήθως το όνομα ηλεκτρονικού ταχυδρομείου είναι παράγωγο του ονόματος του προσώπου.

Γ) Για την εγγραφή «Dec 15 12:38:43», η εταιρεία δηλώνει ότι «*Η αναζήτηση έγινε με προφορικό αίτημα του πελάτη*», χωρίς να διατηρεί σχετικό έγγραφο.

Πλην όμως, στις υπόλοιπες περιπτώσεις πρόσβασης, η εταιρεία προσκόμισε έγγραφα (μηνύματα ηλεκτρονικού ταχυδρομείου, εκτύπωση από το σύστημα), τα οποία αιτιολογούν την πρόσβαση.

Επιπλέον, η εταιρεία δήλωσε ότι είναι σε φάση τελικής ανασκόπησης και εγκρίσεων και από μέσα Ιανουαρίου του 2014 εφαρμόζεται πιλοτικά, η διαδικασία «*Έλεγχος Αρχείων Καταγραφής Πρόσβασης Χρηστών σε Δεδομένα Επικοινωνίας Συνδρομητών*» (Συνημμένο 15 του Σχετικού 8) και παρέδωσε τη σχετική Αναφορά Ελέγχου Προσβάσεων σε Δεδομένα Επικοινωνίας Συνδρομητών του μηνός Ιανουαρίου 2014 (Συνημμένο 16 του Σχετικού 8). Σύμφωνα με την Αναφορά, ο έλεγχος πραγματοποιήθηκε στα συστήματα

Απόκλιση 16: Δεν εφαρμόζεται πλήρως η παράγραφος 2.5.2 αναφορικά με το γεγονός ότι κάθε πρόσβαση σε δεδομένα επικοινωνίας των συνδρομητών ή χρηστών των παρεχόμενων δικτύων ή υπηρεσιών πρέπει να καταγράφεται και να αιτιολογείται (παράγραφος 6.2.6 του άρθρου 6 της Απόφασης 165/2011).

Παράγραφοι 2.6.1 και 2.6.7

Η εταιρεία παρέδωσε έγγραφο με τίτλο «*Αρχείο μηχανισμών ελέγχου πρόσβασης και αυθεντικοποίησης συνδρομητών ή χρηστών στις υπηρεσίες ή/και τα δίκτυα και μηχανισμοί*



κρυπτογράφησης» (Συνημμένο 1 του Σχετικού 10), το οποίο περιλαμβάνει πληροφορίες σχετικά (α) με τους μηχανισμούς ελέγχου πρόσβασης και αυθεντικοποίησης που χρησιμοποιούνται για την πρόσβαση των συνδρομητών ή χρηστών στις υπηρεσίες ή/και τα δίκτυα που παρέχει η εταιρεία και (β) με τους μηχανισμούς ασφαλούς αυθεντικοποίησης και κρυπτογράφησης κατά την πρόσβαση των συνδρομητών σε δεδομένα επικοινωνίας τους (ενδεικτικά εξερχόμενες κλήσεις, ηλεκτρονικό ταχυδρομείο). Το αρχείο περιέχει τις ως άνω πληροφορίες για τα συστήματα

Παρατήρηση 9: Η εταιρεία στο εν λόγω αρχείο δεν έχει συμπεριλάβει πληροφορίες σχετικά με τους μηχανισμούς ελέγχου πρόσβασης και αυθεντικοποίησης που χρησιμοποιούνται κατά την πρόσβαση των συνδρομητών τους στο Διαδίκτυο.

Παράγραφος 2.6.5

Η εταιρεία δήλωσε ότι η σχετική διαδικασία είναι η «Διαδικασία Ελέγχου Αλλαγής Κωδικού Πρόσβασης Συνδρομητών και Χρηστών Υπηρεσιών». Σχετικά με την εν λόγω διαδικασία, η εταιρεία δήλωσε ότι δεν υπάρχει διαδραστική υπηρεσία στην οποία να επιβάλλεται η αλλαγή του κωδικού πρόσβασης (παράγραφος 4.1). Για τον έλεγχο κατά την πρόσβαση στις διαδραστικές υπηρεσίες (παράγραφος 4.2), η εταιρεία παρέδωσε εκτύπωση (printout) του μηνύματος που εμφανίζεται στον χρήστη (Συνημμένο 2 του Σχετικού 10). Τέλος, σχετικά με την παράγραφο 4.3 (περιοδικός έλεγχος και ενημέρωση χρήστη στις μη διαδραστικές παρεχόμενες υπηρεσίες), οι εκπρόσωποι της εταιρείας δήλωσαν ότι ο εν λόγω έλεγχος πραγματοποιείται κάθε τρεις μήνες. Σχετικά με τα αποτελέσματα των τριών τελευταίων ελέγχων, η εταιρεία παρέδωσε τρία σχετικά μηνύματα ηλεκτρονικού ταχυδρομείου (Συνημμένο 3 του Σχετικού 10), καθώς και δείγμα του ενημερωτικού μηνύματος ηλεκτρονικού ταχυδρομείου προς τους συνδρομητές (Συνημμένο 4 του Σχετικού 10).

6. Πολιτική Απομακρυσμένης Λογικής Πρόσβασης (Άρθρο 7 της Απόφασης 165/2011, ΦΕΚ 2715/Β/17.11.2011)

Παράγραφος 2.1.2

Η εταιρεία παρέδωσε τα έγγραφα με τίτλους «ΠΕΣ στα οποία επιτρέπεται η απομακρυσμένη πρόσβαση» και «Αρχείο Συνεργατών με Δυνατότητα Πρόσβασης σε δεδομένα επικοινωνίας» (Συνημμένο 5 του Σχετικού 10).

Παράγραφος 2.1.3

Η εταιρεία δήλωσε ότι η σχετική πληροφορία προκύπτει από τα αιτήματα των εργαζόμενων μέσω του συστήματος και τα έντυπα αιτήσεων δημιουργίας λογαριασμών για εξωτερικούς συνεργάτες (.....).

Παράγραφος 2.1.7



Σχετικά με τις ενέργειες ενεργοποίησης/απενεργοποίησης των λογαριασμών πρόσβασης συνεργατών στα συστήματα απομακρυσμένης πρόσβασης, η εταιρεία δηλώνει ότι ισχύουν συνοπτικά τα εξής (πλήρης ανάλυση στο Σχετικό 11):

Α) Στο σύστημα καταγράφονται οι ενέργειες του διαχειριστή για τροποποίηση του λογαριασμού, αλλά δεν φαίνεται η ακριβής ενέργεια.

Β) Στο σύστημα, η τρέχουσα έκδοση του συστήματος δεν παρέχει τεχνική δυνατότητα καταγραφής των ενεργειών ενεργοποίησης λογαριασμών.

Γ) Στο σύστημα, έχει ενεργοποιηθεί από 24.12.2013 μηχανισμός για την καταγραφή και συλλογή των ενεργειών αυτών σε κεντρικό σύστημα αποθήκευσης αρχείων καταγραφής.

Παρατήρηση 10: η εταιρεία οφείλει να αντιμετωπίζει ως ΠΕΣ τα συστήματα απομακρυσμένης πρόσβασης, προκειμένου να εξασφαλιστεί ότι θα ισχύουν για αυτά οι απαιτήσεις της Απόφασης 165/2011.

Προκειμένου να ελεγχθεί δειγματοληπτικά η εφαρμογή της απαίτησης της παραγράφου 2.1.7, έγινε αντιπαραβολή των αιτήσεων ενεργοποίησης λογαριασμών απομακρυσμένης πρόσβασης για το σύστημα (Συνημμένο 2 του Σχετικού 11) με τις ενέργειες στο σύστημα αυτό, όπως έχουν καταγραφεί από 24.12.2013 έως 31.12.2013 (Συνημμένο 3 του Σχετικού 11), χωρίς να προκύψει κάποιο εύρημα.

Παράγραφος 2.2.1

Σύμφωνα με τον Κατάλογο Αντιστοίχισης Διαδικασιών, η εν λόγω διαδικασία είναι η διαδικασία με κωδικό εγγράφου «Διαχείριση Δικαιωμάτων Απομακρυσμένης Πρόσβασης». Η εταιρεία παρέδωσε τη διαδικασία «Ενεργοποίηση Λογαριασμού Πρόσβασης Εξωτερικού Συνεργάτη» (Συνημμένο 6 του Σχετικού 10). Σχετικά με την ενεργοποίηση των λογαριασμών πρόσβασης εξωτερικού συνεργάτη, η εταιρεία δήλωσε ότι αυτή πραγματοποιείται στους λογαριασμούς των συστημάτων απομακρυσμένης πρόσβασης (.....) και επιπλέον ότι για προσβάσεις εξωτερικών συνεργατών σε συστήματα ΠΕΣ χρησιμοποιείται μόνο η υποδομή

Παρατήρηση 11: Η εταιρεία με το Συνημμένο 5 του Σχετικού 11 δηλώνει ότι στο σύστημα, στο οποίο επιτρέπεται η απομακρυσμένη πρόσβαση από εξωτερικό συνεργάτη (.....), ο μηχανισμός απομακρυσμένης πρόσβασης είναι και όχι

Σύμφωνα με τη διαδικασία, προκειμένου ένας εργαζόμενος να αποκτήσει απομακρυσμένη πρόσβαση σε εταιρικά συστήματα, καταχωρεί σχετική αίτηση στο σύστημα ..., το οποίο προωθείται προς έγκριση και υλοποίηση. Παρομοίως, εφόσον εξωτερικός συνεργάτης επιθυμεί να αποκτήσει απομακρυσμένη πρόσβαση σε εταιρικά συστήματα, συμπληρώνει το σχετικό έντυπο «Αίτηση



Δημιουργίας Λογαριασμών για Εξωτερικούς Συνεργάτες», το οποίο προωθείται προς έγκριση και υλοποίηση.

Προκειμένου να ελεγχθεί δειγματοληπτικά η εφαρμογή της ως άνω διαδικασίας, η Ο.Ε. ζήτησε και παρέλαβε τον τρέχοντα (κατά τον χρόνο του επιτόπιου ελέγχου) κατάλογο των λογαριασμών (accounts) που έχουν οριστεί στους μηχανισμούς απομακρυσμένης πρόσβασης (.....) (Συνημμένο 4 του Σχετικού 11) και τα αιτήματα του συστήματος και τα έντυπα αιτήσεων δημιουργίας λογαριασμών για εξωτερικούς συνεργάτες, από τα οποία να προκύπτουν οι εργαζόμενοι και οι συνεργάτες που έχουν εξουσιοδοτηθεί για χρήση της απομακρυσμένης πρόσβασης από την 1.10.2013 έως την ημερομηνία του επιτόπιου ελέγχου, (Συνημμένα 5 έως και 11 του Σχετικού 11). Από την εξέταση των ως άνω εγγράφων προκύπτουν τα ακόλουθα:

A) Σύστημα

Δεν βρέθηκαν αιτήματα στο σύστημα για τους λογαριασμούς:

B) Σύστημα

Δεν βρέθηκαν αιτήματα στο σύστημα για τους λογαριασμούς:

Γ) Σύστημα

Δεν βρέθηκαν αιτήματα/εγκρίσεις για τους λογαριασμούς:

Επιπλέον επισημαίνεται ότι η εταιρεία, με το Σχετικό 11, έστειλε έντυπα αιτήσεων δημιουργίας λογαριασμών στα συστήματα και για εργαζόμενους για τους οποίους δεν είχε καταστεί εφικτή η καταχώρηση αιτήματος στο σύστημα Με το Σχετικό 25, η εταιρεία δήλωσε ότι οι χρήστες αυτοί ήταν εγκεκριμένοι με βάση την παλαιά διαδικασία, αλλά δεν είχαν προβεί εκ νέου σε αίτημα στο σύστημα

Απόκλιση 17: Δεν εφαρμόζεται πλήρως η παράγραφος 2.2.1 αναφορικά με την εφαρμογή της διαδικασίας διαχείρισης των λογαριασμών απομακρυσμένης πρόσβασης των εργαζομένων και συνεργατών, ώστε να εξασφαλίζεται η αντιστοίχιση των λογαριασμών απομακρυσμένης πρόσβασης και του Αρχείου των εργαζομένων και συνεργατών που έχουν εξουσιοδοτηθεί να χρησιμοποιούν την απομακρυσμένη πρόσβαση (παράγραφος 7.3.1 του άρθρου 7 της Απόφασης 165/2011).

Παράγραφος 2.2.2

Σχετικά με τα αποτελέσματα των τριμηνιαίων ελέγχων που διενεργεί η εταιρεία στα δικαιώματα απομακρυσμένης πρόσβασης των χρηστών, η εταιρεία παρέδωσε τα έγγραφα με τίτλους «.....» του τρίτου (Συνημμένο 7 του Σχετικού 10) και τέταρτου (Συνημμένο 8 του Σχετικού 10) τριμήνου του έτους 2013.



Από την εξέταση των ως άνω εγγράφων προκύπτουν τα ακόλουθα:

Α) Και στις δύο αναφορές υπάρχουν ευρήματα, ενδεικτικά αναφέρεται ότι στα συστήματα δικτύου (NT) βρέθηκαν 67 λογαριασμοί χρηστών το τρίτο τρίμηνο του 2013 (37 στο τέταρτο τρίμηνο) στην πλατφόρμα χωρίς αντίστοιχο αίτημα στο σύστημα Αντίστοιχα βρέθηκαν 25 λογαριασμοί χρηστών το τρίτο τρίμηνο του 2013 (21 στο τέταρτο τρίμηνο) στην πλατφόρμα χωρίς αντίστοιχο αίτημα στο σύστημα Για τα συστήματα IT βρέθηκαν 12 λογαριασμοί χρηστών το τρίτο τρίμηνο του 2013 (7 στο τέταρτο τρίμηνο) στην πλατφόρμα χωρίς αντίστοιχο αίτημα στο σύστημα (σημείωση: συμφωνία με την απόκλιση 17 της παραγράφου 2.2.1)

Β) Το 2^ο σημείο ελέγχου της παραγράφου 2.2.2, δηλαδή ο έλεγχος της υλοποίησης των απαιτούμενων μεταβολών των κωδικών και απενεργοποιήσεων των λογαριασμών απομακρυσμένης πρόσβασης των συνεργατών της παρ. 2.1.6 της Πολιτικής Απομακρυσμένης Λογικής Πρόσβασης, δεν φαίνεται να έχει πραγματοποιηθεί. Γίνεται όμως αναφορά σε δειγματοληπτικό έλεγχο (6 συνδέσεων) για τις οποίες η εταιρεία έλεγξε τις αντίστοιχες αιτήσεις (σε έντυπο) έγκρισης και ενεργοποίησης.

Απόκλιση 18: Δεν εφαρμόζεται πλήρως η παράγραφος 2.2.2 αναφορικά με τον έλεγχο της υλοποίησης των απαιτούμενων μεταβολών των κωδικών και απενεργοποιήσεων των λογαριασμών απομακρυσμένης πρόσβασης των συνεργατών της παρ. 2.1.6 της Πολιτικής Απομακρυσμένης Λογικής Πρόσβασης (παράγραφος 7.3.2.β του άρθρου 7 της Απόφασης 165/2011).

7. Πολιτική Διαχείρισης και Εγκατάστασης ΠΕΣ (Άρθρο 8 της Απόφασης 165/2011, ΦΕΚ 2715/Β/17.11.2011)

Παράγραφος 2.1.3

Αναφορικά με τις διαδικασίες Προμήθειας-Ανάπτυξης Υλικού και Λογισμικού των Συστημάτων και Δοκιμών, Αποδοχής και Ελέγχου Ορθής Λειτουργίας Υλικού και Λογισμικού των Συστημάτων, της Πολιτικής Διαχείρισης και Εγκατάστασης Συστημάτων, οι εκπρόσωποι της εταιρείας δήλωσαν ότι υλοποιούνται από τα έγγραφα,

Σχετικά με τη Διαδικασία Ελέγχου Συντήρησης – Υποστήριξης – Λειτουργίας, η Ο.Ε. επισήμανε στην εταιρεία ότι οι διαδικασίες, οι οποίες είχαν παραδοθεί στο συνημμένο 2 του σχετικού 4, ισχύουν για τα συστήματα της Διεύθυνσης Πληροφορικής. Η εταιρεία παρέδωσε τη διαδικασία «Διαχείριση Προβλημάτων Τεχνολογικής Υποδομής» (συνημμένο 10 του σχετικού 15), ως Διαδικασία Ελέγχου Συντήρησης – Υποστήριξης – Λειτουργίας των ΠΕΣ του δικτύου της Τεχνολογίας. Η διαδικασία αυτή έχει ημερομηνία έναρξης ισχύος την 15.5.2014.

Παράγραφος 2.1.4



Η εταιρεία δήλωσε ότι για τα συστήματα ΙΤ, η καταγραφή οποιασδήποτε αλλαγής υλικού ή λογισμικού διατηρείται στο σύστημα, ενώ για τα συστήματα ΝΤ, διατηρείται ανά σύστημα.

Για τα συστήματα του δικτύου (ΝΤ), η εταιρεία δήλωσε ότι δεν έχει πραγματοποιηθεί καμία αλλαγή υλικού ή λογισμικού από 13.4.2013 έως σήμερα στα συστήματα, ενώ έχουν πραγματοποιηθεί στα συστήματα Επίσης, αλλαγές μικρού μεγέθους (π.χ. εγκατάσταση διορθωτικού λογισμικού) έχουν γίνει στα συστήματα

Η εταιρεία παρέδωσε αρχείο αλλαγών που πραγματοποιήθηκαν στο σύστημακαι αφορά στην προληπτική εγκατάσταση διορθωτικού λογισμικού (Patches) (συνημμένο 1 του σχετικού 14) και στο σύστημα που αφορά επίλυση προβλημάτων (συνημμένο 2 του σχετικού 13). Η Ο.Ε. εξέτασε τα παραπάνω αρχεία και διαπίστωσε ότι διατηρούνται σύμφωνα με την παράγραφο 2.1.4.

Η εταιρεία παρέδωσε αρχεία αλλαγών των συστημάτων πληροφορικής (ΙΤ) (συνημμένο 7 του σχετικού 13), πλην τωνγια τα οποία δήλωσε ότι δεν έχει πραγματοποιηθεί καμία αλλαγή. Η Ο.Ε. εξέτασε τα παραπάνω αρχεία και διαπίστωσε ότι διατηρούνται σύμφωνα με την παράγραφο 2.1.4. Επίσης, διαπίστωσε ότι το αρχείο αλλαγών υλικού ή λογισμικού για τα συστήματα δεν έχει προκύψει από το σύστημα Η εταιρεία επιβεβαίωσε τη διαπίστωση (σχετικό 25) και υποστήριξε ότι δεν γινόταν χρήση του σε αυτά τα συστήματα λόγω μικρού πλήθους αλλαγών. Ωστόσο, αυτή η δήλωση της εταιρείας έρχεται σε αντίθεση με προηγούμενη δήλωσή της στην οποία ανέφερε ότι για τα συστήματα ΙΤ, η καταγραφή οποιασδήποτε αλλαγής υλικού ή λογισμικού διατηρείται στο σύστημα

Παρατήρηση 12: Η εταιρεία οφείλει να ακολουθεί τη σχετική διαδικασία (.....) και να καταγράφει όλες τις αλλαγές στο σύστημα

Παράγραφος 2.4.2

Η εταιρεία, αναφορικά με τις ενέργειες για την υλοποίηση των αλλαγών στο σύστημα, που περιέχονται στο αρχείο (συνημμένο 7 του σχετικού 13),

- δήλωσε ότι σε επίπεδο λειτουργικού συστήματος δεν έχει καταστεί τεχνικά εφικτή η ενεργοποίηση μηχανισμού καταγραφής ενεργειών, λόγω επίπτωσης στην απόδοση του συστήματος ενώ έχει ξεκινήσει έργο, ώστε, σε συνεργασία με τους αρμόδιους προμηθευτές, να παραμετροποιηθεί κατάλληλα ο εγγενής μηχανισμός καταγραφής του συστήματος και να περιοριστούν οι επιπτώσεις στη λειτουργία του. Αναφορικά με τον παρόντα χρόνο, εκ παραδρομής δεν συμπεριελήφθη το σύστημα στην αντίστοιχη εξαίρεση.



- Παρέδωσε την καταγραφή ενεργειών στη Βάση Δεδομένων, για την αλλαγή με TaskID: 73518 του αρχείου αλλαγών καθώς και τις ρυθμίσεις που αφορούν την ενεργοποίηση του auditing (Task ID : 73553) (συνημμένο 11 του σχετικού 15)

Από την εξέταση των παραπάνω στοιχείων διαπιστώθηκε ότι η εταιρεία παρέδωσε τις ενέργειες για 2 από τις 6 αλλαγές του συστήματος

Απόκλιση 19: Δεν εφαρμόζεται η παράγραφος πλήρως 2.4.2 σχετικά με την καταγραφή των ενεργειών στα ΠΕΣ (παράγραφος 8.3.3.2 του άρθρου 8 της Απόφασης 165/2011)

Διαδικασία (Διεργασία) «Ανάλυση, Ανάπτυξη & Υλοποίηση Νέου Συστήματος / Πλατφόρμας Τεχνολογικής Υποδομής»

Η εταιρεία δήλωσε, κατόπιν ερώτησης της Ο.Ε. εάν έχει πραγματοποιηθεί ή βρίσκεται σε εξέλιξη προμήθεια ή ανάπτυξη υλικού ή λογισμικού από τις 13.04.2013 (έναρξη ισχύος πολιτικής ασφάλειας) έως την ημερομηνία του ελέγχου, ότι είχε ξεκινήσει προ της 13.4.2013 και είναι σε εξέλιξη η ανάπτυξη λογισμικού για την υπηρεσία ηλεκτρονικού ταχυδρομείου (σύστημα MAIL). Η εταιρεία, αναφορικά με την τεκμηρίωση που προκύπτει από τις ενέργειες της διαδικασίας, παρέδωσε:

- την κατηγοριοποίηση του έργου (συνημμένο 9 του σχετικού 13) και
- τις απαιτήσεις ασφάλειας που έχουν οριστεί για το σύστημα και το επίπεδο συμμόρφωσης με αυτές (συνημμένο 10 του σχετικού 13).

Από την εξέταση των παραπάνω στοιχείων διαπιστώθηκε ότι έχει πραγματοποιηθεί κατηγοριοποίηση βάσει του PSA σύμφωνα με την ενότητα 6.1. Επίσης, έχουν οριστεί οι απαιτήσεις ασφάλειας σύμφωνα με την παράγραφο 6.2 καθώς και η συμμόρφωση με αυτές σύμφωνα με την 6.8.

Διαδικασία (Διεργασία) «Υλοποίηση Νέων Εταιρικών Πληροφοριακών Συστημάτων»

Η Ο.Ε. διαπίστωσε ότι έχουν συνταχθεί οι δώδεκα διαδικασίες επιπέδου 4 (.....) που αναφέρονται στην εν λόγω διαδικασία και οι οποίες σύμφωνα με δήλωση της εταιρείας είναι υπό έγκριση.

Διαδικασία (Διεργασία) «Υλοποίηση Αναβάθμισης / Διόρθωσης Λογισμικού Τεχνολογικής Υποδομής»

Η εταιρεία, αναφορικά με την τεκμηρίωση που προκύπτει από τις ενέργειες της διαδικασίαςγια τα συστήματα, παρέδωσε:

- την κατηγοριοποίηση των αλλαγών που πραγματοποιήθηκαν, μετά την ημερομηνία εφαρμογής της διαδικασίας, στο σύστημα, για τις αλλαγές με αιτιολόγηση «1-464992» και «1-4956716», (συνημμένο 3 του σχετικού 13). Αναφορικά με την αιτιολόγηση «1-4965306 wrong announcement», η εταιρεία δήλωσε ότι η συγκεκριμένη αλλαγή πραγματοποιήθηκε κατόπιν



προβλήματος που παρουσιάστηκε στη λειτουργία του συστήματος και κατά συνέπεια δεν απαιτείται η κατηγοριοποίηση κατά PSA. Η εταιρεία παρέδωσε στην Ο.Ε. τη σχετική αλληλογραφία (Συνημμένο 3 του Σχετικού 25)

- την κατηγοριοποίηση των αλλαγών που πραγματοποιήθηκαν, μετά την ημερομηνία εφαρμογής της διαδικασίας στα (συνημμένο 4 του σχετικού 13).
- Τα “system description file” και “log management file” για το σύστημα ... (συνημμένο 5 του σχετικού 13) και το (συνημμένο 6 του σχετικού 13).

Από την εξέταση των παραπάνω στοιχείων διαπιστώθηκε ότι έχει πραγματοποιηθεί κατηγοριοποίηση βάσει του PSA σύμφωνα με την παράγραφο 6.1, πλην της αλλαγής στο με αιτιολόγηση «1-4965306 wrong announcement». Σχετικά με την αλλαγή αυτή η δήλωση της εταιρείας έρχεται σε αντίθεση με την παράγραφο 6.1 της διαδικασίας στην οποία αναφέρεται ότι η αξιολόγηση της αναγκαιότητας εισαγωγής νέας έκδοσης ή διορθωτικού λογισμικού μπορεί να είναι έκτακτη, λόγω ανάγκης εισαγωγής διορθωτικού λογισμικού ως μέσο επίλυσης στη λειτουργία του εξοπλισμού. Επίσης, διατηρούνται τα “system description file” και “log management file” σύμφωνα με την παράγραφο 6.4.

Διαδικασία (Διεργασία) «Διαχείριση Αλλαγών Εταιρικών Πληροφοριακών Συστημάτων»

Η εταιρεία, αναφορικά με την τεκμηρίωση που προκύπτει από τις ενέργειες της διαδικασίας για τις αλλαγές στο σύστημα με task ID: TAS00000004387, TAS00000004392, TAS00000004399, TAS00000004400, TAS00000004448, παρέδωσε:

- Την κατηγοριοποίηση των έργων, στα οποία εντάσσονται οι αλλαγές που πραγματοποιήθηκαν (συνημμένο 2 του σχετικού 15)
- Την τεκμηρίωση του συστήματος (system description file και log management file) (συνημμένο 3 του σχετικού 15)
- Εκθέσεις αποδοχής της αλλαγής (συνημμένο 4 του σχετικού 15).

Από την εξέταση των παραπάνω στοιχείων διαπιστώθηκε ότι:

- Δεν προκύπτει ότι η κατηγοριοποίηση που παραδόθηκε αντιστοιχεί στις υπό εξέταση αλλαγές που πραγματοποιήθηκαν.
- Δεν προκύπτει ότι οι εκθέσεις αποδοχής που παραδόθηκαν αντιστοιχούν στις υπό εξέταση αλλαγές που πραγματοποιήθηκαν. Επιπλέον, στις εκθέσεις αποδοχής δεν υπάρχουν ημερομηνίες, καθώς και τα υπογεγραμμένα αποτελέσματα του από τα εμπλεκόμενα μέρη, σύμφωνα με την παράγραφο 6.5 της διαδικασίας.



Η εταιρεία, αναφορικά με την τεκμηρίωση που προκύπτει από τις ενέργειες της διαδικασίας για τις αλλαγές στο σύστημα με αύξοντα αριθμό 21 έως και 25 του αρχείου(συνημμένο 7 του σχετικού 13), παρέδωσε:

- Την κατηγοριοποίηση του έργου, στο πλαίσιο του οποίου πραγματοποιήθηκαν οι αλλαγές (συνημμένο 5 του σχετικού 15)
- Την τεκμηρίωση του συστήματος (system description file και log management file) (συνημμένο 7 του σχετικού 15)
- Εκθέσεις αποδοχής της αλλαγής (συνημμένο 4 του σχετικού 26).

Από την εξέταση των παραπάνω στοιχείων διαπιστώθηκε ότι:

- Δεν προκύπτει ότι η κατηγοριοποίηση που παραδόθηκε αντιστοιχεί στις υπό εξέταση αλλαγές που πραγματοποιήθηκαν.
- Δεν παραδόθηκε έκθεση αποδοχής για την αλλαγή με αριθμό 25.
- Στις υπόλοιπες εκθέσεις αποδοχής δεν υπάρχουν τα υπογεγραμμένα αποτελέσματα του ... από τα εμπλεκόμενα μέρη, σύμφωνα με την παράγραφο 6.5 της διαδικασίας.

Απόκλιση 20: Δεν εφαρμόζονται συστηματικά οι παράγραφοι 6.1 και 6.5 της Διαδικασίας «Διαχείριση Αλλαγών Εταιρικών Πληροφοριακών Συστημάτων» (παράγραφος 8.3.3 του άρθρου 8 της Απόφασης 165/2011).

Διαδικασία (Διεργασία) «Υποστήριξη Χρηστών & Διαχείριση Συμβάντων Πληροφοριακών Συστημάτων»

Η εταιρεία παρέδωσε τα συμβάντα που έχουν καταγραφεί στο από 13.4.2013 έως 13.5.2014 (συνημμένο 12 του σχετικού 15)

Η εταιρεία παρέδωσε τις έξι διαδικασίες επιπέδου 4 (.....) που αναφέρονται στην εν λόγω διαδικασία.

Διαδικασία (Διεργασία) «Υποστήριξη Λειτουργίας Πληροφοριακών Συστημάτων»

Η εταιρεία, αναφορικά με τα συμβάντα με severity 1 και 2 που έχουν καταγραφεί στο σύστημα από 13.4.2013 έως και 13.5.2014, παρέδωσε:

- τα συμβάντα από το για το διάστημα από 31.3.2014 έως 13.5.2014 (συνημμένο 14 του σχετικού 15)



- τα πρωτογενή αρχεία συμβάντων που τηρούνται στα ΠΕΣ ... για το διάστημα από 13.4.2013 έως 30.3.2014 (συνημμένο 15 του σχετικού 15), διότι δεν κατέστη τεχνικά εφικτό να εξαχθούν τα συμβάντα για αυτό το διάστημα από το

Η Ο.Ε. ζήτησε δειγματοληπτικά (συνημμένο 5 του σχετικού 25) για κάποια συμβάντα από το σύστημα την αντιστοίχιση με τα αιτήματα από το σύστημα (συνημμένο 12 του σχετικού 15), σύμφωνα με την παράγραφο 6.3 της διαδικασίας. Η εταιρεία απάντησε (σχετικό 26) αναφέροντας ότι τα αιτήματα ανοίγονται, αφού προηγηθεί αξιολόγηση των critical alarms από τον αρμόδιο μηχανικό, επομένως δεν υφίσταται πάντοτε αιτιολόγηση. Στις συγκεκριμένες περιπτώσεις δεν απαιτήθηκε η καταχώρηση σχετικού αιτήματος.

Έχοντας υπόψη, ότι τα συμβάντα που επιλέχθηκαν δειγματοληπτικά, ανήκουν στα συμβάντα που παρέδωσε η εταιρεία για το σύστημα, ως απάντηση στο αίτημα της Ο.Ε. για τα συμβάντα με severity 1 και 2 που έχουν καταγραφεί στο σύστημα, θα έπρεπε να είχαν καταχωρηθεί αιτήματα στο ..., σύμφωνα με την παράγραφο 6.3 της διαδικασίας. Επισημαίνεται όμως, ότι στο αρχείο με τα συμβάντα που παρέδωσε η εταιρεία (συνημμένο 14 του σχετικού 15) όλα τα συμβάντα χαρακτηρίζονται ως “critical” και δεν υπάρχει αποτυπωμένος χαρακτηρισμός “severity 1 ή 2”, όπως προβλέπεται στην παράγραφο 6.3 της διαδικασίας. Συνεπώς, δεν μπορεί να ελεγχθεί εάν απαιτείται η δημιουργία αιτήματος στο

Παρατήρηση 13: Δεν είναι δυνατόν να ελεγχθεί η εφαρμογή της παραγράφου 6.3 της Διαδικασίας «Υποστήριξη Λειτουργίας Πληροφοριακών Συστημάτων». Η εταιρεία οφείλει να καταγράφει τον χαρακτηρισμό “severity 1 ή 2” στα συμβάντα τουτα οποία αξιολογούνται από την εταιρεία με αυτό τον τρόπο.

Σχετικά με τα συμβάντα από τα συστήματα για το χρονικό διάστημα από 1.1.2014 έως και 31.1.2014, η εταιρεία παρέδωσε:

- τα συμβάντα που έχουν καταγραφεί στα συστήματα (συνημμένο 16 του σχετικού 15) και(συνημμένο 17 του σχετικού 15)

ενώ δήλωσε ότι τα συμβάντα για τα συστήματα περιλαμβάνονται στο συνημμένο 15 του σχετικού 15.

Διαδικασία «Διαγραφή – Απόσυρση Υλικού & Λογισμικού Συστημάτων» - Οδηγία Εργασίας «Κανόνες Διαγραφής Δεδομένων»

Η εταιρεία παρέδωσε για τις Διευθύνσεις που υπάγονται στη Γενική Διεύθυνση Τεχνολογίας & Λειτουργιών το αρχείο απόσυρσης (συνημμένο 21 του σχετικού 15) και τα αρχεία ενεργειών διαγραφής δεδομένων (συνημμένο 22 του σχετικού 15), και για τις Διευθύνσεις που υπάγονται στη

Γενική Διεύθυνση Τεχνολογιών Πληροφορικής το αρχείο απόσυρσης (συνημμένο 23 του σχετικού 15) και τα αρχεία ενεργειών διαγραφής δεδομένων (συνημμένο 24 του σχετικού 15).

Από την εξέταση των παραπάνω αρχείων διαπιστώθηκε ότι τηρούνται τα αρχεία σύμφωνα με την παράγραφο 6.2 της διαδικασίας και την 4.1 της οδηγίας εργασίας, πλην της περίπτωσης των αρχείων των Διευθύνσεων που υπάρχουν στη Γενική Διεύθυνση Τεχνολογιών Πληροφορικής στα οποία δεν αποτυπώνεται το ΠΕΣ με το οποίο σχετίζονται τα συγκεκριμένα υλικά.

Παρατήρηση 14: Η εταιρεία οφείλει να έχει καταγεγραμμένο το σύστημα στο οποίο υπάρχουν τα δεδομένα σύμφωνα με την παράγραφο 4.1 της Οδηγίας Εργασίας..... «Κανόνες Διαγραφής Δεδομένων».

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

Παράγραφος 2.1.1

Η εταιρεία παρέδωσε ως Διαδικασία Διαχείρισης Περιστατικών Ασφάλειας τη Διαδικασία «Διαχείριση Περιστατικών Ασφάλειας».

Παράγραφος 2.1.6

Σχετικά με την ετοιμότητα ενεργοποίησης της Διαδικασίας Διαχείρισης Περιστατικών Ασφάλειας, η εταιρεία δήλωσε ότι έχουν πραγματοποιηθεί μία φορά (Δεκέμβριος 2013) σχετικές ασκήσεις ετοιμότητας. Επιπλέον δήλωσε, ότι δεδομένου ότι η διαδικασία έχει ενεργοποιηθεί και εφαρμοστεί αρκετές φορές λόγω ύπαρξης πραγματικών περιστατικών ασφάλειας, η ετοιμότητα ενεργοποίησης της διαδικασίας επιβεβαιώνεται στην πράξη.

Διαδικασία «Διαχείριση Περιστατικών Ασφάλειας»

Η εταιρεία, αναφορικά με τον φάκελο καταγραφής περιστατικών ασφάλειας, παρέδωσε λίστα με τα περιστατικά ασφάλειας από την έναρξη ισχύος της πολιτικής και τις σχετικές εκθέσεις αναφοράς περιστατικών ασφάλειας (συνημμένο 1 του σχετικού 16).

Από την εξέταση της λίστας των περιστατικών και των σχετικών εκθέσεων διαπιστώθηκαν τα εξής:

- Δεν έχει καταγραφεί στις εκθέσεις αναφοράς περιστατικών ασφάλειας οποιαδήποτε αναφορά σχετικά με τα συλλεχθέντα στοιχεία για τη διερεύνηση του περιστατικών και γενικότερα εάν έχει πραγματοποιηθεί περαιτέρω διερεύνηση των περιστατικών.
- Δεν είναι σαφές, εάν οι εκθέσεις του φακέλου αποτελούν τις εκθέσεις άμεσης αναφοράς ή τις τελικές εκθέσεις. Ωστόσο, τουλάχιστον για τις περιπτώσεις τις οποίες, σύμφωνα με την ως άνω διαπίστωση, θα έπρεπε να είχε πραγματοποιηθεί περαιτέρω διερεύνηση, η έκθεση που

περιλαμβάνονται στο φάκελο είναι η έκθεση άμεσης αναφοράς και λείπει η τελική έκθεση με τα αποτελέσματα από την ολοκλήρωση της διερεύνησης του περιστατικού.

- Δεν έχουν καταγραφεί στις εκθέσεις αναφοράς περιστατικών ασφάλειας τα διορθωτικά μέτρα και το σχετικό χρονοδιάγραμμα.
- Δεν περιλαμβάνεται στη λίστα με τα περιστατικά ασφάλειας το με αριθ. πρωτ. ΑΔΑΕ ΑΠΡ 4431/18.11.2013 (893907/15.11.2013) περιστατικό ασφάλειας

Απόκλιση 21: Δεν εφαρμόζεται πλήρως η παράγραφος 6.6 της Διαδικασίας «Διαχείριση Περιστατικών Ασφάλειας» και της παραγράφου 2.1.2, αναφορικά με τα ελάχιστα στοιχεία που πρέπει να καταγράφονται στην Έκθεση Άμεσης Αναφοράς Περιστατικού Ασφάλειας (παράγραφος 9.2.2 του άρθρου 9 της Απόφασης 165/2011).

Απόκλιση 22: Δεν εφαρμόζεται πλήρως η παράγραφος 6.8 της Διαδικασίας «Διαχείριση Περιστατικών Ασφάλειας» και της παραγράφου 2.1.3, αναφορικά με τη σύνταξη και αποστολή στην ΑΔΑΕ της Τελικής Έκθεσης Αναφοράς Περιστατικού Ασφάλειας (παράγραφος 9.2.3 του άρθρου 9 της Απόφασης 165/2011).

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

Παράγραφος 2.1.1 και 2.2.1

Η εταιρεία απέστειλε τα αρχεία που καλύπτουν τις απαιτήσεις των παραγράφων 2.1.1 και 2.2.1 για τα ΠΕΣ με τίτλο «Αρχείο Λογικού Διαχωρισμού – Μηχανισμών & Συστημάτων Δικτύου» (Συνημμένο 19 του Σχετικού 15) και για τα ΠΕΣ ... με τίτλο «Αρχείο Λογικού Διαχωρισμού Δικτύων – Μηχανισμοί & Συστήματα Ασφάλειας Δικτύου» (Συνημμένο 20 του Σχετικού 15) αντίστοιχα.

Αναφορικά με το «Αρχείο Λογικού Διαχωρισμού – Μηχανισμών & Συστημάτων Δικτύου» για τα ΠΕΣ ..., η εταιρεία, κατά τον 9^ο επιτόπιο έλεγχο (Σχετικό 18) έδωσε πληροφορίες αναφορικά με την αρχιτεκτονική που έχει υλοποιηθεί, τις διασυνδέσεις των ΠΕΣ με εσωτερικά δίκτυα και με το Internet, και τα συστήματα ασφάλειας δικτύου που χρησιμοποιούνται. Ειδικότερα, σχετικά με την τεχνική διαμόρφωση των συστημάτων ασφάλειας δικτύου, η εταιρεία παρουσίασε στην Ο.Ε., μέσω του αντίστοιχου λογισμικού διαχείρισής τους, την τρέχουσα διαμόρφωση ορισμένων συστημάτων (.....).

Περαιτέρω, η εταιρεία, κατόπιν αιτήματος της Ο.Ε, παρέδωσε με το Συνημμένο 1 του Σχετικού 19 τα εξής στοιχεία:

1. τις λίστες ACL του δρομολογητή ASR 1006 που εφαρμόζονται στα εσωτερικά ΠΕΣ IT, για το εύρος διευθύνσεων IP 10.101.1.X, 10.101.16.X και 10.101.0.X, σύμφωνα με την σελίδα 6 του «Αρχείου Λογικού Διαχωρισμού – Μηχανισμών & Συστημάτων Δικτύου».



2. τα policies/ACL που εφαρμόζονται στο firewall Palo Alto PA-5020 για τα ΠΕΣ στα οποία υπάρχει Internet πρόσβαση, σύμφωνα με την σελίδα 8 του «Αρχείου Λογικού Διαχωρισμού – Μηχανισμών & Συστημάτων Δικτύου».

3. τους συναγερμούς με υψηλή κρισιμότητα που έχουν ενεργοποιηθεί στο firewall Palo Alto PA-5020 για τα ΠΕΣ στα οποία υπάρχει Internet πρόσβαση.

4. τα σημεία εκτός Αθηνών από τα οποία υπάρχει πρόσβαση σε ΠΕΣ ΙΤ της εταιρείας.

Σχετικά με τα ως άνω υπό σημείο 3 στοιχεία, η εταιρεία δήλωσε (Σχετικό 19) ότι σε καθημερινή βάση το σύστημα στέλνει αυτόματα ένα μήνυμα ηλεκτρονικού ταχυδρομείου με συγκεντρωτικές πληροφορίες σχετικά με τα συμβάντα, στα αρμόδια στελέχη της υποδιεύθυνσης Σταθερής και Κινητής. Η Ο.Ε. ζήτησε δειγματοληπτικά μια σχετική αναφορά του Μαΐου 2014 και παρέλαβε τα έγγραφα με τίτλο «Flooding Top Attackers» με ημερομηνία 13.05.2014 και «Top Threats» με ημερομηνία 14.5.2014 (Συνημμένο 2 του Σχετικού 19). Σε ερώτηση της Ο.Ε. σχετικά με το εάν έχει ενεργοποιηθεί η Πολιτική Διαχείρισης Περιστατικών Ασφάλειας, ύστερα από επεξεργασία των συμβάντων στο firewall αυτό, η εταιρεία δήλωσε ότι δεν υπήρχε λόγος να ενεργοποιηθεί η διαδικασία, γιατί οι απειλές αντιμετωπίστηκαν αυτόματα και άμεσα από το σύστημα.

Περαιτέρω, σε συνέχεια των ως άνω στοιχείων υπό σημεία 1 και 2, η Ο.Ε. ζήτησε :

1. από τις λίστες ACL του δρομολογητή ASR 1006 που εφαρμόζονται στα εσωτερικά ΠΕΣ ..., τον σκοπό που εξυπηρετούν και αιτιολόγηση για τη δημιουργία τους, για τις εγγραφές:
 - permit icmp host 10.101.0.112 host 62.103.157.62 (αρχείο e10-in.txt)
 - permit tcp host 10.101.1.97 eq 1521 host 212.205.85.241 (αρχείο e301-in.txt)
 - permit tcp host 10.101.1.97 eq 1521 host 212.205.85.242 (αρχείο e301-in.txt)
 - permit ip 10.100.30.0 0.0.0.255 10.101.16.96 0.0.0.31 time-range mediation-eksoterikoι (αρχείο mediation-out.txt)
2. από τα policies/ACL που εφαρμόζονται στο firewall Palo Alto PA-5020 για τα ΠΕΣ στα οποία υπάρχει Internet πρόσβαση, τον σκοπό που εξυπηρετεί και αιτιολόγηση για τη δημιουργία του, για την εγγραφή με όνομα (Name) «remotedesktop».

Η εταιρεία παρέδωσε τα υπό σημείο 1 ζητούμενα στοιχεία (Συνημμένο 7 του Σχετικού 25). Από την εξέταση του εγγράφου αυτού, προκύπτει ότι :

Α) Για τις εγγραφές «permit tcp host 10.101.1.97 eq 1521 host 212.205.85.241» και «permit tcp host 10.101.1.97 eq 1521 host 212.205.85.242», το έγγραφο αναφέρει ότι «το παραπάνω το χρειαζόμαστε



να είναι *active* μέχρι την Τρίτη 28/2, όπου έχει προγραμματιστεί το *live*. Μετά δεν το χρειαζόμαστε άλλο». Σημειώνεται ότι το email αναφέρεται στο έτος 2012.

Β) Για την εγγραφή «permit ip 10.100.30.0 0.0.0.255 10.101.16.96 0.0.0.31 time-range mediation-eksoterikoι», η εταιρεία δεν απέστειλε αιτιολόγηση.

Σχετικά με το σημείο 2, η εταιρεία δήλωσε (Σχετικό 25) ότι ο κανόνας αυτός έχει δημιουργηθεί βάσει της πολιτικής για να επιτρέπει τη χρήση του remote desktop των διαχειριστών προς τα συστήματα Internet.

Παρατήρηση 15: Η εταιρεία οφείλει να αιτιολογεί και να κρατά τεκμηρίωση των κανόνων που εφαρμόζονται στους μηχανισμούς και στα συστήματα ασφάλειας, σύμφωνα με την παράγραφο 2.1.3 της Πολιτικής Ασφάλειας Δικτύου και των σχετικών κανόνων και διαδικασιών της Πολιτικής Διαχείρισης και Εγκατάστασης Συστημάτων, στην οποία παραπέμπει.

Η Ο.Ε. κατά τον 10^ο επιτόπιο έλεγχο (Σχετικό 19), επεσήμανε στην εταιρεία ότι το αρχείο «Αρχείο Λογικού Διαχωρισμού Δικτύων – Μηχανισμοί & Συστήματα Ασφάλειας Δικτύου ...» δεν περιέχει το σύνολο των πληροφοριών που προβλέπεται στις παραγράφους 2.1.1 και 2.2.1 της Πολιτικής Ασφάλειας Δικτύου της εταιρείας, διότι είναι σε πολύ υψηλό επίπεδο ανάλυσης, δεν αναφέρει όλα τα συστήματα ανά κατηγορία ΠΕΣ, δεν καταγράφεται η ζώνη ασφάλειας στην οποία έχουν τοποθετηθεί τα συστήματα, δεν απεικονίζεται αναλυτικά ο λογικός διαχωρισμός και η κατάτμηση των δικτύων και δεν περιλαμβάνονται όλοι οι μηχανισμοί ασφάλειας που χρησιμοποιούνται. Η εταιρεία δήλωσε ότι θεωρεί ότι με το συγκεκριμένο αρχείο που παρέδωσε καλύπτει τις απαιτήσεις της πολιτικής ασφάλειας, αλλά παρόλα αυτά έστειλε εκ νέου το αρχείο, βάσει των επισημάνσεων που έγιναν, με το Συνημμένο 1 του Σχετικού 20. Η εταιρεία έδωσε διευκρινίσεις αναφορικά με την αρχιτεκτονική που έχει υλοποιηθεί και ειδικότερα σχετικά με το δίκτυο διαχείρισης ...και τα συστήματα ασφάλειας αυτού. Ειδικά για το σύστηματου δικτύου, που περιγράφεται στο ως άνω αρχείο, η εταιρεία δήλωσε ότι αντικαταστάθηκε πρόσφατα από

Παρατήρηση 16: Τα αρχεία των παραγράφων 2.1.1 και 2.2.1 τόσο για τα συστήματα ... όσο και για τα συστήματα ... πρέπει να περιέχουν την προβλεπόμενη πληροφορία (ή να κάνουν τις κατάλληλες παραπομπές σε αυτήν) αναλυτικά ανά ΠΕΣ. Επί παραδείγματι, με το Συνημμένο 4 του Σχετικού 16, η εταιρεία παρέδωσε την αναφορά εσωτερικού ελέγχου για το ΠΕΣ Στην ενότητα 1 του ως άνω εγγράφου, γίνεται πλήρης ανάλυση του ΠΕΣ ... στους εξυπηρετητές και στις βάσεις δεδομένων από τα οποία απαρτίζεται, καθώς και στις διεπαφές (interfaces) με άλλα ΠΕΣ. Τα αρχεία των παραγράφων 2.1.1 και 2.2.1 της Πολιτικής Ασφάλειας Δικτύου πρέπει να περιέχουν την προβλεπόμενη πληροφορία σε αυτό το επίπεδο ανάλυσης.

Παράγραφος 2.2.5



Σχετικά με το Αρχείο που περιέχει ανάλυση των μέτρων προστασίας και ασφάλειας για τα συστήματα που δεν τοποθετούνται σε αποστρατικοποιημένες ή έμπιστες ζώνες, η εταιρεία δήλωσε (Σχετικό 15) ότι τα ΠΕΣ της εταιρείας είναι τοποθετημένα σε αποστρατικοποιημένες ή έμπιστες ζώνες και συνεπώς δεν τηρείται το Αρχείο αυτής της παραγράφου.

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

Παράγραφος 2.2.1 και 2.2.2

Σχετικά με τα στοιχεία προετοιμασίας του ελέγχου, που καταγράφονται σε σχετικό Αρχείο, η εταιρεία παρέδωσε το έγγραφο με τίτλο «Πλάνο Ελέγχων –» για το έτος 2014 (Συνημμένο 2 του Σχετικού 16) και τα αρχεία προετοιμασίας ελέγχου για τα συστήματα(Συνημμένο 3 του Σχετικού 16). Στα συστήματα αυτά, με βάση το Πλάνο Ελέγχων, ήταν προγραμματισμένο να πραγματοποιηθεί ο έλεγχος κατά τα δύο πρώτα τρίμηνα του έτους 2014. Από την εξέταση των ως άνω αρχείων, προκύπτει ότι αυτά περιλαμβάνουν τα αναγραφόμενα στην παράγραφο 2.2.1 της Πολιτικής Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών της εταιρείας.

Παράγραφος 2.3.1

Σχετικά με τα στάδια διεξαγωγής κάθε ελέγχου, τα σχετικά ευρήματα και τις προτεινόμενες βελτιώσεις ή τροποποιήσεις, που καταγράφονται σε ειδικό Αρχείο, η εταιρεία παρέδωσε το τελικό σχέδιο αναφοράς ελέγχου ασφάλειας για τα συστήματα (Συνημμένο 4 του Σχετικού 16). Στα συστήματα αυτά, με βάση το Πλάνο Ελέγχων, ήταν προγραμματισμένο να πραγματοποιηθεί ο έλεγχος κατά το πρώτο τρίμηνο του έτους 2014. Αναφορικά με το χρονοδιάγραμμα υλοποίησης των διορθωτικών ενεργειών που περιλαμβάνονται στις αναφορές ελέγχου, η εταιρεία δήλωσε (Σχετικό 16) ότι είναι σε στάδιο οριστικοποίησης σε συνεργασία με τα αντίστοιχα τμήματα.

Σε συνέχεια του ελέγχου της Πολιτικής Ελέγχου Εφαρμογής της Πολιτικής Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών, η Ο.Ε. κατά τον 13^ο επιτόπιο έλεγχο, ζήτησε το χρονοδιάγραμμα υλοποίησης των διορθωτικών ενεργειών που περιλαμβάνονται στις αναφορές ελέγχου, για τις οποίες η εταιρεία είχε δηλώσει ότι είναι σε στάδιο οριστικοποίησης σε συνεργασία με τα αντίστοιχα τμήματα. Η εταιρεία παρέδωσε τα σχετικά αρχεία (Συνημμένο 6 του Σχετικού 25). Από την εξέταση των αρχείων αυτών για τα συστήματα, προκύπτει ότι αυτά όντως περιλαμβάνουν το σχετικό χρονοδιάγραμμα καθώς και ένδειξη της κατάστασης των διορθωτικών ενεργειών.

11. Πολιτική Αντιμετώπισης Κακόβουλου Λογισμικού (Άρθρο 12 της Απόφασης 165/2011, ΦΕΚ 2715/Β/17.11.2011)



Παράγραφος 2.1.3

Η εταιρεία ενημέρωσε την Ο.Ε. (σχετικό 17) σχετικά με τον έλεγχο ακεραιότητας του λογισμικού των συστημάτων. Ειδικότερα:

- Στα συστήματαπραγματοποιείται έλεγχος ακεραιότητας μέσω του λογισμικού OSSEC, από 1.2.2014, και δεν έχουν υπάρξει ευρήματα εγκατάστασης μη εξουσιοδοτημένου λογισμικού.
- Τα υπόλοιπα ΠΕΣ της Πληροφορικής (IT) προγραμματίζεται να ενταχθούν στο μηχανισμό ελέγχου ακεραιότητας μέσω του συστήματος μέχρι 31.12.2014.
- Στα συστήματα πραγματοποιείται έλεγχος ακεραιότητας του λογισμικού μέσω, από 4.4.2014 και 5.4.2014 αντίστοιχα, και δεν έχουν υπάρξει ευρήματα εγκατάστασης μη εξουσιοδοτημένου λογισμικού.
- Στα συστήματα προγραμματίζεται η εγκατάσταση του μέχρι το τέλος του 2014.
- Το σύστημαέχει ενταχθεί σε πλατφόρμα, που χρησιμοποιείται αποκλειστικά για τα συστήματα, από το Μάρτιο του 2014, κατόπιν αναβάθμισης του λογισμικού και λήψης σχετικού πιστοποιητικού (συνημμένο 1 του σχετικού 17) για το λογισμικό της εταιρείας.
- Στο σύστημα πραγματοποιήθηκε, στο πλαίσιο του λογισμικού το Νοέμβριο του 2013 και προγραμματίζεται έλεγχος από τον προμηθευτή πριν το τέλος του Q3/14, με ταυτόχρονη ένταξή του στο ..., εφόσον δοθεί η συγκατάθεση του κατασκευαστή.
- Για τα υπόλοιπα ΠΕΣ της Τεχνολογίας (NT) είναι σε εξέλιξη η λήψη προτάσεων από τους προμηθευτές για την παροχή πιστοποίησης ως προς την ακεραιότητα του λογισμικού, προκειμένου να αξιολογηθούν οικονομοτεχνικά. Επισημαίνεται ότι για την παροχή της διασφάλισης τη ακεραιότητας από τους προμηθευτές απαιτούνται ιδιαίτερος υψηλά και δυσανάλογα κόστη. Παράλληλα εξετάζεται εναλλακτικά η χρήση του

Από τις παραπάνω δηλώσεις της εταιρείας διαπιστώθηκε ότι, ενώ σε κάποια από τα συστήματα της Πληροφορικής (IT) έχει πραγματοποιηθεί έλεγχος ακεραιότητας του λογισμικού και έχει προγραμματιστεί ο έλεγχος των υπολοίπων μέχρι το τέλος του 2014, όπως δηλώνεται και στις εξαιρέσεις, στα συστήματα της Τεχνολογίας (NT), πλην τωνδεν έχουν πραγματοποιηθεί έλεγχοι ούτε υπάρχει σαφές χρονοδιάγραμμα για την πραγματοποίησή τους.

Απόκλιση 23: Δεν εφαρμόζεται η παράγραφος 2.1.3 για όλα τα ΠΕΣ (παράγραφος 12.2.3 του άρθρου 12 της Απόφασης 165/2011)

Παράγραφος 2.1.5



Η εταιρεία παρέδωσε αναφορικά με το αρχείο της εν λόγω παραγράφου την Οδηγία Εργασίας «Εφαρμογή Πολιτικής Αντιμετώπισης Κακόβουλου Λογισμικού». Από την εξέταση του εν λόγω εγγράφου προέκυψε ότι δεν καταγράφονται οι λεπτομέρειες εφαρμογής των απαιτήσεων της πολιτικής. Για παράδειγμα, δεν αναφέρονται οι μηχανισμοί για τον έλεγχο ακεραιότητας του λογισμικού των ΠΕΣ, μηχανισμοί προστασίας από κακόβουλο λογισμικό, μηχανισμοί για τον περιορισμό εξάπλωσης του κακόβουλου λογισμικού, κτλ.

Παρατήρηση 17: Η εταιρεία οφείλει να συμπληρώσει την Οδηγία Εργασίας με τις λεπτομέρειες εφαρμογής της Πολιτικής Αντιμετώπισης Κακόβουλου Λογισμικού.

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

Παράγραφος 2.1.9

Σχετικά με το Αρχείο στο οποίο καταγράφονται οι λεπτομέρειες εφαρμογής των απαιτήσεων που ορίζονται στην Πολιτική Χρήση Κρυπτογραφίας, η εταιρεία παρέδωσε το εγχειρίδιο(Συνημμένο 6 του Σχετικού 16) με τίτλο «Αρχείο Εφαρμογής Πολιτικής Χρήσης Κρυπτογραφίας». Από την εξέταση του ως άνω εγγράφου, προκύπτει ότι αυτό δεν περιέχει τις λεπτομέρειες εφαρμογής των απαιτήσεων της Πολιτικής, αλλά επαναλαμβάνει το περιεχόμενο της πολιτικής. Ενδεικτικά, δεν αναφέρονται τα συστήματα κρυπτογράφησης για την επαρκή προστασία των δεδομένων επικοινωνίας κατά την αποθήκευση και μεταφορά τους μέσω δικτύων (παρ.4, σημείο 1), οι χρησιμοποιούμενοι αλγόριθμοι κρυπτογράφησης και τα σχετικά μήκη κλειδιών (παρ.4, σημείο 4), τα τεχνικά ή διαδικαστικά μέσα με τα οποία εξασφαλίζεται η αυθεντικότητα των πιστοποιητικών (παρ.4, σημείο 6), οι διαδικασίες για τη δημιουργία, πιστοποίηση, διανομή και ανάκληση κρυπτογραφικών κλειδιών (παρ.4, σημείο 7).

Παρατήρηση 18: Η εταιρεία οφείλει να συμπληρώσει το εγχειρίδιο με τις λεπτομέρειες εφαρμογής της Πολιτικής Χρήσης Κρυπτογραφίας.

Α. 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 εφήρμοξε πλήρως την εγκριθείσα, με την Απόφαση 294/2013, 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 Πρακτικό της από 23 Ιουλίου 2015 συνεδρίασης και η σχετική Απόφαση υπ' αριθμ. 209/2015 περί έγκρισης της διενέργειας του εν λόγω ελέγχου, μετά της συνημμένης έκθεσης, παρεδόθη στην εταιρεία «.....», όπως προκύπτει από την υπ' αριθμ. πρωτ. ΑΔΑΕ 2241/14-10-2015 Απόδειξη παράδοσης – παραλαβής, σε συνδυασμό με το υπ' αριθμ. πρωτ. ΑΔΑΕ 2293/05-10-2016 έγγραφο της Α.Δ.Α.Ε. προς την εταιρεία «.....», το οποίο παραδόθηκε στην εταιρεία, όπως προκύπτει από την υπ' αριθμ. πρωτ. ΑΔΑΕ 2308/06-10-2016 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 την Παράγραφο 5.1.5 και 5.1.8 της Πολιτικής Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών

Η εταιρεία παρέδωσε το έγγραφο με τίτλο «Ειδικό Σχέδιο Αρχείων Καταγραφής Συστημάτων». Στο έγγραφο αυτό αναφέρονται τα ΠΕΣ τα οποία έχουν υπαχθεί στις καταγραφές, ενώ αναφέρεται ότι τα παραγόμενα αρχεία καταγραφής μεταφέρονται στην κεντρική υποδομή Log Management, όπου έχει καταστεί τεχνικά εφικτό. Επίσης, ως συνημμένο του προηγούμενου εγγράφου, για κάθε ΠΕΣ παραδόθηκε αρχείο (Excel) στο οποίο παρουσιάζονται τα είδη και η περιγραφή των καταγραφών ανά κατηγορία (.....), ποιες είναι ενεργοποιημένες και ποιες μεταφέρονται στην κεντρική υποδομή (...).

Απόκλιση 1 : Από την εξέταση του Ειδικού Σχεδίου Αρχείων Καταγραφής Συστημάτων διαπιστώθηκε ότι αυτό δεν περιλαμβάνει τα στοιχεία αναφορικά με τα μέτρα για τη διασφάλιση της ακεραιότητας, της εμπιστευτικότητας και της διαθεσιμότητας αυτών, όπως απαιτείται, σύμφωνα με την παράγραφο 3.2.9 του άρθρου 3 της Απόφασης 165/2011 και κατά συνέπεια, δεν εφαρμόζεται πλήρως η παράγραφος 5.1.8 της Πολιτικής Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών της εταιρείας.

Από την εξέταση των αρχείων (Excel) για κάθε σύστημα διαπιστώθηκε ότι για τα συστήματα δεν έχει υλοποιηθεί η μεταφορά των αρχείων καταγραφής που παράγονται στην



κεντρική υποδομή Επιπλέον, διαπιστώθηκε ότι ο χρόνος διατήρησης των περισσότερων αρχείων καταγραφής αυτών των συστημάτων είναι μικρότερος των δύο ετών, ενδεικτικά αναφέρονται χρόνοι διατήρησης 2, 7, 10, 30, 60, 90, 365 ημερών, ή μπορεί να μην είναι γνωστός (N/A). Σημειώνεται όμως, ότι για τα συστήματα η εταιρεία έχει καταγράψει την εξαίρεσή τους από την παράγραφο 5.1.5.

Απόκλιση 2: Επομένως, δεν εφαρμόζεται για τα ΠΕΣ που εξετάστηκαν η παράγραφος 5.1.5 αναφορικά με τη διατήρηση των αρχείων καταγραφής για δύο έτη, όπως προβλέπεται στην παράγραφο 3.2.8 του άρθρου 3 της Απόφασης 165/2011.

β) Ως προς την παράγραφο 5.2.3 της Πολιτικής Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών

Η εταιρεία παρέδωσε τον κατάλογο συστημάτων με συνοπτική περιγραφή της λειτουργίας τους. Από την εξέταση του καταλόγου και σύμφωνα με τον ορισμό των Πληροφοριακών και Επικοινωνιακών Συστημάτων (ΠΕΣ) (παράγραφος 4 της Πολιτικής Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών και άρθρο 2 της Απόφασης 165/2011) διαπιστώθηκε ότι ο κατάλογος δεν περιλαμβάνει, τουλάχιστον, τα συστήματα πρόσβασης συνδρομητών στο διαδίκτυο, τα αναχώματα ασφάλειας, τα συστήματα αποτροπής εισβολών, τα συστήματα ανίχνευσης κακόβουλου λογισμικού και τα συστήματα καταγραφής.

Απόκλιση 3: Ενόψει της έλλειψης συγκεκριμένων συστημάτων από το κατάλογο των ΠΕΣ της εταιρείας, προκύπτει ότι δεν εφαρμόζεται η παράγραφος 5.2.3 αναφορικά με την πληρότητα του καταλόγου των ΠΕΣ, όπως προβλέπεται στην παράγραφο 3.3.1.1 του άρθρου 3 της Απόφασης 165/2011.

γ) Ως προς την παράγραφο 2.2.2 της Πολιτικής Αποδεκτής Χρήσης

Από την εξέταση των τμημάτων των συμβάσεων με τις εταιρείες και ειδικότερα από το άρθρο 9 αυτών («Εμπιστευτικότητα»), όπως αναφέρεται αναλυτικά ανωτέρω, προκύπτει ότι δεν περιλαμβάνονται οι απαιτήσεις και τα μέτρα ασφάλειας που προβλέπει η παράγραφος 2.2.2 της Πολιτικής.



Στο έγγραφο-υπόδειγμα με τίτλο «Παράρτημα Πολιτικής Ασφάλειας», περιλαμβάνονται συγκεκριμένες απαιτήσεις και μέτρα ασφάλειας. Ωστόσο, το έγγραφο αυτό δεν φαίνεται να είναι τμήμα των ως άνω δύο συμβάσεων, παρόλο που η σύμβαση με την εταιρεία είναι μεταγενέστερη της ημερομηνίας έναρξης ισχύος της Πολιτικής της εταιρείας.

Απόκλιση 4: Επομένως, δεν εφαρμόζεται πλήρως η παράγραφος 2.2.2 αναφορικά με τις απαιτήσεις και τα μέτρα ασφάλειας που λαμβάνονται για τη διασφάλιση του απορρήτου των επικοινωνιών στις συμβάσεις που συνάπτει η εταιρεία με συνεργάτες της, όπως προβλέπεται στην παράγραφο 4.3.2.2 του άρθρου 4 της Απόφασης 165/2011.

δ) Ως προς την παράγραφο 2.1.3 της Πολιτικής Φυσικής Ασφάλειας

Αναφορικά με τις εγκρίσεις για την παροχή εξουσιοδότησης φυσικής πρόσβασης, σύμφωνα με την παράγραφο 2.1.3 της Πολιτικής Φυσικής Ασφάλειας και τη Βασική Εγκύκλιο 70/11, από τα έγγραφα που προσκόμισε η εταιρεία, όπως της ζητήθηκαν και όπως αναλυτικά εκτίθενται ανωτέρω διαπιστώθηκε ότι:

- οι εγκρίσεις της αφορούν στην έγκριση για τη διατήρηση στο σύστημα των δικαιωμάτων φυσικής πρόσβασης που έχουν χορηγηθεί και όχι στην έγκριση για τη χορήγηση των δικαιωμάτων, σύμφωνα με την παράγραφο 2.1.3 της Πολιτικής Φυσικής Ασφάλειας.
- δυνατότητα εισόδου στο χώρο είχαν 34 εργαζόμενοι το 2013 και 41 το 2014. Αυτό έρχεται σε αντίθεση με τη δήλωση της εταιρείας κατά τον επιτόπιο έλεγχο ότι περιορισμένος αριθμός ατόμων (2) έχει δυνατότητα πρόσβασης στο χώρο.

Από την αντιπαραβολή των αρχείων καταγραφής φυσικής πρόσβασης στους χώρους για το χρονικό διάστημα από 1.10.2013 έως και 31.12.2013 με τα εγκεκριμένα αιτήματα αδειών εισόδου για το έτος 2013 δε διαπιστώθηκε πρόσβαση εργαζομένου χωρίς να υπάρχει η αντίστοιχη άδεια.

Από τη δειγματοληπτική αντιπαραβολή των αρχείων καταγραφών φυσικής πρόσβασης για την εγκατάσταση για την 30 και 31/12/2013 με τα εγκεκριμένα αιτήματα αδειών εισόδου για το έτος 2013 διαπιστώθηκε ότι οι κάτοχοι κάρτας:δε βρέθηκαν στο έντυπο με τα εγκεκριμένα αιτήματα αδειών εισόδου.



Απόκλιση 5: Από τα ανωτέρω προκύπτει ότι δεν εφαρμόζεται η παράγραφος 2.1.3, όπως προβλέπεται στην παράγραφο 5.2.3, εδ. α,' του άρθρου 5 της Απόφασης 165/2011.

ε) Ως προς την παράγραφο 2.1.4 της Πολιτικής Φυσικής Ασφάλειας

Η εταιρεία παρέδωσε το αρχείο από το σύστημαστο οποίο διατηρείται το ιστορικό χορήγησης/κατάργησης των δικαιωμάτων πρόσβασης που έχουν εν τοις πράγμασι χορηγηθεί, μέσω του αρχείου καταγραφής των ενεργειών των διαχειριστών του συστήματος.

Από την αντιπαραβολή των αρχείων καταγραφής φυσικής πρόσβασης για τους χώρους ότι υπάρχουν προσβάσεις υπαλλήλων οι οποίοι δε βρέθηκαν στο αρχείο με το ιστορικό χορήγησης/κατάργησης των δικαιωμάτων πρόσβασης που έχουν εν τοις πράγμασι χορηγηθεί.

Απόκλιση 6: Από τα ανωτέρω προκύπτει ότι δεν εφαρμόζεται συστηματικά η παράγραφος 2.1.4 της εν λόγω Πολιτικής της εταιρείας, όπως προβλέπεται στην παράγραφο 5.2.3, εδ. β', του άρθρου 5 της Απόφασης 165/2011.

στ) Ως προς την παράγραφο 2.1.5 της Πολιτικής Φυσικής Ασφάλειας

Η Ο.Ε. διαπίστωσε από τον επιτόπιο έλεγχο στις εγκαταστάσεις ότι η πρόσβαση στις εγκαταστάσεις δεν καταγράφεται.

Η Ο.Ε. διαπίστωσε ότι η πρόσβαση στις εγκαταστάσεις είναι ελεγχόμενη μέσω καρταναγνώστη και καταγράφεται. Η εταιρεία παρέδωσε τα αρχεία καταγραφής φυσικής πρόσβασης, σύμφωνα με την παράγραφο 2.1.5, για την εγκατάσταση για το διάστημα από 1.10.2013 έως και 31.12.2013

Απόκλιση 7: Από τα ανωτέρω προκύπτει ότι δεν εφαρμόζεται για όλες τις εγκαταστάσεις του η παράγραφος 2.1.5 της εν λόγω Πολιτικής της εταιρείας, όπως προβλέπεται στην παράγραφο 5.2.4 του άρθρου 5 της Απόφασης 165/2011.

ζ) Ως προς την παράγραφο 2.1.7 της Πολιτικής Φυσικής Ασφάλειας



Η εταιρεία παρέδωσε το αρχείο με τους χώρους εγκατάστασης συστημάτων και μηχανισμών ασφάλειας σε αυτούς, σύμφωνα με την παράγραφο 2.1.7. Από την εξέταση των αρχείων αυτών διαπιστώθηκε ότι:

- στους χώρους εγκατάστασης των συστημάτων δεν υπάρχει εγκατεστημένο κλειστό κύκλωμα τηλεόρασης (CCTV) και σύστημα ανίχνευσης μη εξουσιοδοτημένης πρόσβασης (intruder detection) ή άλλος ισχυρός μηχανισμός.
- στο χώρο του αναφέρεται ότι δε λειτουργεί ο καρταναγνώστης του συστήματος access control.

Η εταιρεία, κατά τον έλεγχο των αρχείων καταγραφής φυσικής πρόσβασης σε 7 χώρους ΠΕΣ (παράγραφος 2.1.8), δήλωσε ότι ο χώρος δεν διαθέτει ηλεκτρονικό σύστημα ελέγχου φυσικής πρόσβασης. Ωστόσο, στο αρχείο με τους χώρους εγκατάστασης συστημάτων και μηχανισμών ασφάλειας σε αυτούς καταγράφεται ότι ο χώρος διαθέτει σύστημα ελέγχου πρόσβασης με καρταναγνώστη (card reader).

Από τον έλεγχο των μηχανισμών ασφάλειας, σύμφωνα με το έντυπο «καταγραφή χώρων – μηχανισμών φυσικής ασφάλειας», στο χώρο του διαπιστώθηκε ότι ο καρταναγνώστης έχει τεθεί εκτός λειτουργίας. Οι εκπρόσωποι δήλωσαν ότι ο καρταναγνώστης δε χρησιμοποιείται λόγω αλλαγής χρήσης του συγκεκριμένου χώρου (κατάργηση της συστέγασης του κέντρου διαχείρισης δικτύου) και του περιορισμένου αριθμού ατόμων (2) με δυνατότητα πρόσβασης στο χώρο. Η καταγραφή της πρόσβασης στο χώρο πραγματοποιείται σε έντυπο.

Από τον έλεγχο των μηχανισμών ασφάλειας, σύμφωνα με το έντυπο «καταγραφή χώρων – μηχανισμών φυσικής ασφάλειας», στο χώρο του διαπιστώθηκε ότι οι μηχανισμοί είναι σε ισχύ. Σχετικά με τους μηχανισμούς ασφάλειας των χώρων που καταγράφονται στο παραπάνω έντυπο, η εταιρεία δήλωσε ότι ο έλεγχος πρόσβασης στους χώρους πραγματοποιείται μέσω καρταναγνώστη στην είσοδο των εγκαταστάσεων, στους οποίους υπάρχουν οι παραπάνω χώροι, δεδομένου ότι οι εγκαταστάσεις αυτές είναι περιορισμένες σε μέγεθος και ουσιαστικά στεγάζουν τον καταναλωτή και το χώρο

Απόκλιση 8: Από τα ανωτέρω προκύπτει ότι δεν εφαρμόζεται για όλους τους χώρους εγκατάστασης ΠΕΣ η παράγραφος 2.1.7 αναφορικά με την προστασία τους μέσω ισχυρών



μηχανισμών ασφάλειας και ελεγχόμενης πρόσβασης, όπως προβλέπεται στην παράγραφο 5.2.5 του άρθρου 5 της Απόφασης 165/2011.

η) Ως προς την παράγραφο 2.1.8 της Πολιτικής Φυσικής Ασφάλειας

Από την εξέταση των αρχείων καταγραφής φυσικής πρόσβασης, σύμφωνα με την παράγραφο 2.1.8, όπως αναλυτικά αναφέρονται ανωτέρω, διαπιστώθηκε ότι:

- υπάρχει μια πρόσβαση στο χώρο στην οποία δεν καταγράφεται το ονοματεπώνυμο αλλά ο αριθμός 8785524305.
- καταγράφονται συμβάντα απόπλισης και όπλισης, χωρίς να υπάρχει ταυτόχρονα η καταγραφή της εισόδου και εξόδου στους χώρους ΠΕΣ. Η εταιρεία, αναφορικά με αυτό το γεγονός, δήλωσε ότι η διαδικασία προβλέπει μετά την απόπλιση να ακολουθεί εκ νέου ανάγνωση της κάρτας εισόδου ώστε να επιτρέπεται η είσοδος στον χώρο. Όμως σε πολλές περιπτώσεις, επειδή είναι σε εξέλιξη αλλά δεν έχει ολοκληρωθεί ακόμα η κατάργηση της δυνατότητας ανοίγματος με συμβατικά μέσα (κλειδί), είναι δυνατόν να γίνει είσοδος χωρίς εκ νέου ανάγνωση της κάρτας εισόδου, κατά συνέπεια δεν καταγράφεται στα αρχεία καταγραφής το συμβάν της εισόδου ως ξεχωριστό συμβάν.
- ενώ καταγράφεται το ονοματεπώνυμο και η ώρα εισόδου, δεν καταγράφεται συστηματικά η ώρα εξόδου.

Απόκλιση 9: Από τα ανωτέρω προκύπτει ότι δεν εφαρμόζεται πλήρως η παράγραφος 2.1.8 της εν λόγω Πολιτικής της εταιρείας, όπως προβλέπεται στην παράγραφο 5.2.5 του άρθρου 5 της Απόφασης 165/2011.

θ) Ως προς την παράγραφο 2.1.10 της Πολιτικής Φυσικής Ασφάλειας

Η εταιρεία δήλωσε ότι η παρακολούθηση των συμβάντων του πραγματοποιείται από Αναφορικά με την παρακολούθηση, η Ο.Ε. ζήτησε πληροφορίες, και πιο συγκεκριμένα τι ενέργειες πραγματοποιήθηκαν ώστε να διερευνηθεί η εγγραφή «άγνωστη αιτία», Η εταιρεία δήλωσε ότι για τους συναγερμούς αυτούς πραγματοποιήθηκε άμεσα τεχνικός έλεγχος από το προσωπικό του, κατά τον οποίο δεν διαπιστώθηκε περιστατικό ασφάλειας. Οι συναγερμοί οφείλονται σε λάθος αλληλουχία ενεργειών των τεχνικών στο



πλαίσιο προγραμματισμένων εργασιών. Ωστόσο, εάν είχε πραγματοποιηθεί αυτή η διερεύνηση από το τεχνικό τμήμα σε συνεργασία με τον επόπτη, θα έπρεπε να είχε γίνει σαφής σχολιασμός, σύμφωνα με την παράγραφο 4.2 της οδηγίας εργασίας.

Αναφορικά με την παρακολούθηση των συμβάντων, η εταιρεία δήλωσε ότι αυτή πραγματοποιείται από Η Ο.Ε. ζήτησε πληροφορίες σχετικά με τη μη αιτιολόγηση (σχολιασμός) δύο συγκεκριμένων εγγραφών (events) Η εταιρεία δήλωσε κατά τον έλεγχο ότι, ως προς την δεύτερη εγγραφή, λόγω απουσίας του προσωπικού που παρακολουθεί την 6.12.2013, δεν έγινε σχολιασμός της. Επιπλέον, δήλωσε ότι οι συναγερμοί αυτοί προκλήθηκαν από λάθος αλληλουχία ενεργειών του τεχνικού που επισκέφτηκε για προγραμματισμένες εργασίες. Ωστόσο, σύμφωνα με την παράγραφο 4.2 της οδηγίας εργασίας θα έπρεπε να είχαν σχολιαστεί οι συναγερμοί εντός 24ώρου.

Ως προς το περιστατικό ασφάλειας της 6.6.2013 σύμφωνα με το αρ. πρωτ. ΑΔΑΕ έγγραφο ΑΠΡ4431/18.11.2013, η εταιρεία παρέδωσε τα αρχεία καταγραφής των συμβάντων για το χρονικό διάστημα από 1.5.2013 έως 6.6.2013 για Από την εξέταση των καταγραφών διαπιστώθηκε ότι υπάρχουν την 5.6.2013, 0:26 και την 6.6.2013, 0:43 στις οποίες δεν υπάρχει κανένας σχολιασμός (αιτιολόγηση). ,.....

Απόκλιση 10: Από τα ανωτέρω προκύπτει ότι δεν εφαρμόζεται συστηματικά η οδηγία εργασίας: «Αναγνώριση & ενημέρωση Συμβάντος,» την οποία η εταιρεία παρέδωσε στην Ο.Ε. ως μέρος των μηχανισμών ασφάλειας

ι) Ως προς την παράγραφο 2.1.9 της Πολιτικής Λογικής Πρόσβασης

Από την εξέταση των εγγράφων που αφορούν στο αρχείο στο οποίο καταγράφονται η συχνότητα και οι τρόποι με τους οποίους πραγματοποιείται η περιοδική αλλαγή των κωδικών πρόσβασης στα πληροφοριακά και επικοινωνιακά συστήματα (ΠΕΣ) της εταιρείας, προκύπτουν τα ακόλουθα:

- i. Για το σύστημα, αναφέρει ότι δεν αλλάζει ο κωδικός πρόσβασης σε επίπεδο εφαρμογής («no change»). Πλην όμως, το γεγονός αυτό δεν έχει καταγραφεί στα έντυπα καταγραφής εξαιρέσεων.
- ii. Για το σύστημα, δεν αναφέρεται η συχνότητα αλλαγής του κωδικού πρόσβασης σε επίπεδο λειτουργικού συστήματος.



- iii. Για το σύστημα, δεν αναφέρεται η συχνότητα αλλαγής του κωδικού πρόσβασης σε επίπεδο εφαρμογής, βάσης δεδομένων και λειτουργικού συστήματος.
- iv. Για το σύστημα, δεν αναφέρεται η συχνότητα αλλαγής του κωδικού πρόσβασης σε επίπεδο βάσης δεδομένων και λειτουργικού συστήματος. Δεν είναι κατανοητό αν η συχνότητα αλλαγής που εφαρμόζεται σε επίπεδο εφαρμογής ισχύει και για το επίπεδο βάσης δεδομένων και λειτουργικού συστήματος.
- v. Για το σύστημα, δεν αναφέρεται η συχνότητα αλλαγής του κωδικού πρόσβασης σε επίπεδο εφαρμογής, βάσης δεδομένων και λειτουργικού συστήματος.
- vi. Για το σύστημα, δεν αναφέρεται η συχνότητα αλλαγής του κωδικού πρόσβασης σε επίπεδο εφαρμογής, βάσης δεδομένων και λειτουργικού συστήματος.
- vii. Για το σύστημα δεν αναφέρεται η συχνότητα αλλαγής του κωδικού πρόσβασης σε επίπεδο εφαρμογής, βάσης δεδομένων και λειτουργικού συστήματος.
- viii. Για το σύστημα δεν αναφέρεται η συχνότητα αλλαγής του κωδικού πρόσβασης σε επίπεδο εφαρμογής, βάσης δεδομένων και λειτουργικού συστήματος.
- ix. Για το σύστημα δεν αναφέρεται η συχνότητα αλλαγής του κωδικού πρόσβασης σε επίπεδο εφαρμογής, βάσης δεδομένων και λειτουργικού συστήματος. Σχετικά με το επίπεδο εφαρμογής, το έγγραφο παραπέμπει στην πολιτική του κεντρικού domain (central domain policy).
- x. Για το σύστημα, δεν αναφέρεται η συχνότητα αλλαγής του κωδικού πρόσβασης σε επίπεδο εφαρμογής, βάσης δεδομένων και λειτουργικού συστήματος. Σχετικά με το επίπεδο εφαρμογής, το έγγραφο παραπέμπει στην πολιτική του κεντρικού domain (central domain policy).
- xi. Για το σύστημα, δεν αναφέρεται η συχνότητα αλλαγής του κωδικού πρόσβασης σε επίπεδο εφαρμογής, βάσης δεδομένων και λειτουργικού συστήματος.
- xii. Για το σύστημα δεν αναφέρεται η συχνότητα αλλαγής του κωδικού πρόσβασης σε επίπεδο βάσης δεδομένων και λειτουργικού συστήματος.
- xiii. Για το σύστημα, δεν αναφέρεται η συχνότητα αλλαγής του κωδικού πρόσβασης σε επίπεδο εφαρμογής, βάσης δεδομένων και λειτουργικού συστήματος. Επιπλέον, δεν



αναφέρεται η μέθοδος πραγματοποίησης αλλαγής του κωδικού πρόσβασης για το επίπεδο βάσης δεδομένων και λειτουργικού συστήματος.

Απόκλιση 11: Από τα ανωτέρω προκύπτει ότι δεν εφαρμόζεται πλήρως η παράγραφος 2.1.9 αναφορικά με την καταγραφή της συχνότητας και των τρόπων με τους οποίους πραγματοποιείται η περιοδική αλλαγή των κωδικών πρόσβασης, όπως προβλέπεται στην παράγραφο 6.4.2.3 του άρθρου 6 της Απόφασης 165/2011.

ια) Ως προς τις παραγράφους 2.2.1 και 2.2.2 της Πολιτικής Λογικής Πρόσβασης

Σχετικά με το Αρχείο με περιγραφή των κανόνων δημιουργίας ονόματος χρήστη και το Αρχείο με περιγραφή των κανόνων δημιουργίας κωδικών πρόσβασης, η εταιρεία παρέδωσε το Εγχειρίδιο με τίτλο «Κανόνες Δημιουργίας Αναγνωριστικών Χρηστών» και το Εγχειρίδιο με τίτλο «Κανόνες Δημιουργίας Κωδικών Πρόσβασης».

Προκειμένου να διαπιστωθεί ότι οι κανόνες αυτές εφαρμόζονται και στην πράξη, η Ο.Ε. ζήτησε και παρέλαβε για τα ΠΕΣ εκτύπωση (printout) των κανόνων δημιουργίας και διαχείρισης κωδικών πρόσβασης, που έχουν οριστεί σε επίπεδο εφαρμογής, λειτουργικού συστήματος και βάσης δεδομένων. Από την εξέταση των παραπάνω εγγράφων προκύπτει ότι οι κανόνες δημιουργίας κωδικών πρόσβασης τηρούνται σε όλα τα συστήματα πλην μίας περίπτωσης. Στο σύστημα στο επίπεδο εφαρμογής, ορίζεται ότι το ελάχιστο μήκος κωδικού πρόσβασης είναι έξι (6) χαρακτήρες, ενώ το εγχειρίδιο αναφέρει ότι το ελάχιστο μήκος είναι οκτώ (8) χαρακτήρες. Επίσης, επισημαίνεται ότι η εκτύπωση (printout) των κανόνων δημιουργίας κωδικών πρόσβασης του συστήματος σε επίπεδο λειτουργικού συστήματος δεν αναφέρουν το ελάχιστο μήκος κωδικού πρόσβασης, και συνεπώς δεν μπορεί να πραγματοποιηθεί ο εν λόγω έλεγχος.

Απόκλιση 12: Από τα ανωτέρω προκύπτει ότι δεν εφαρμόζεται η παράγραφος 4 του Εγχειριδίου σχετικά με το ελάχιστο μήκος των κωδικών πρόσβασης, όπως προβλέπεται στην παράγραφο 6.4.2.2 του άρθρου 6 της Απόφασης 165/2011.

ιβ) Ως προς την παράγραφο 2.3 της Πολιτικής Λογικής Πρόσβασης



Σύμφωνα με τη διαδικασία με κωδικό εγγράφου «Διαχείριση Δικαιωμάτων Πρόσβασης σε Πληροφοριακά Συστήματα», για τη δημιουργία νέου χρήστη ή κατάργηση υφιστάμενου σε ΠΕΣ της εταιρείας, προηγείται καταχώριση και επεξεργασία σχετικού αιτήματος στο σύστημα της εταιρείας, τόσο για τους εργαζόμενους όσο και για τους εξωτερικούς συνεργάτες.

Από την εξέταση των εγγράφων που ζήτησε και παράλαβε η Ο.Ε. για τον έλεγχο της εφαρμογής της εν λόγω διαδικασίας, όπως αναλυτικά αναφέρονται ανωτέρω, προκύπτουν τα ακόλουθα:

Α) Σύστημα

Η αντιπαραβολή πραγματοποιήθηκε με χρήση και του συστήματος (περιφερειών), για το οποίο η εταιρεία δηλώνει ότι αποτελεί υποσύστημα, παρόλο που δεν το έχει δηλώσει στη λίστα των ΠΕΣ που παρέδωσε κατά τον πρώτο επιτόπιο έλεγχο.

Στο επίπεδο της εφαρμογής, δε βρέθηκαν αιτήματα στο σύστημα για τους λογαριασμούς:

Στο επίπεδο της βάσης δεδομένων, η εταιρεία παρέδωσε κατάλογο με 335 accounts που έχουν οριστεί στο σύστημα, αλλά ο αντίστοιχος κατάλογος από το περιέχει 12 accounts. Σε περαιτέρω αντιπαραβολή και με τη λίστα του επιπέδου εφαρμογής για το σύστημα, στο δειγματοληπτικό έλεγχο εξήντα (60) από τα 335 accounts, τα είκοσι τέσσερα (24) από αυτά δε βρέθηκαν στον κατάλογο του συστήματος

Στο επίπεδο του λειτουργικού συστήματος, δε βρέθηκαν εγκρίσεις για τα accounts:, καθώς και για τα συστημικά accounts.

Β) Σύστημα

Στο επίπεδο της εφαρμογής, δε βρέθηκαν αιτήματα στο σύστημα για τους λογαριασμούς:

Στο επίπεδο της βάσης δεδομένων, δε βρέθηκαν εγκρίσεις για το account, καθώς και για τα συστημικά accounts.

Στο επίπεδο του λειτουργικού συστήματος, δε βρέθηκαν εγκρίσεις για τα accounts: καθώς και για τα συστημικά accounts.

Γ) Σύστημα



Σε επίπεδο εφαρμογής, δε βρέθηκαν αιτήματα στο σύστημα για τους λογαριασμούς: spysta (αν και υπάρχει το που πιθανόν ανήκει στο ίδιο πρόσωπο),

Στο επίπεδο λειτουργικού συστήματος, δε βρέθηκαν εγκρίσεις για τα accounts: καθώς και για τα συστημικά accounts. Επιπρόσθετα, δεν υπάρχει ακριβής αντιστοίχιση για τα παρακάτω accounts:

Επιπλέον, η εταιρεία παρέδωσε έντυπες αιτήσεις-εγκρίσεις προσβάσεων στο σύστημα, για τις περιπτώσεις που δεν είχε καταστεί εφικτή η αίτηση μέσω (επί παραδείγματι, account:).

Δ) Σύστημα

Σε επίπεδο εφαρμογής, δε βρέθηκαν αιτήματα στο σύστημα για τους λογαριασμούς: Επιπρόσθετα, επισημαίνεται ότι τα περισσότερα αναγνωριστικά χρήστη στο σύστημα παρουσιάζουν διαφορές σε σύγκριση με τον κατάλογο του συστήματος, παρόλο που το ονοματεπώνυμο του εργαζόμενου συμπίπτει. Επιπλέον, η εταιρεία παρέδωσε έντυπες αιτήσεις-εγκρίσεις προσβάσεων στο σύστημα, για τις περιπτώσεις που δεν είχε καταστεί εφικτή η αίτηση μέσω(επί παραδείγματι, accounts:).

Στο επίπεδο λειτουργικού συστήματος, δε βρέθηκαν εγκρίσεις για τα accounts:, καθώς και για τα συστημικά accounts.

Απόκλιση 13: Από τα ανωτέρω προκύπτει ότι δεν εφαρμόζεται συστηματικά η διαδικασία «Διαχείριση Δικαιωμάτων Πρόσβασης σε Πληροφοριακά Συστήματα» της παραγράφου 2.3 (ειδικότερα οι 2.3.3 και 2.3.4) αναφορικά με τη δημιουργία νέου χρήστη σε ΠΕΣ της εταιρείας, όπως προβλέπεται στην παράγραφο 6.3.1 του άρθρου 6 της Απόφασης 165/2011.

ιγ) Ως προς την παράγραφο 2.3.5 της Πολιτικής Λογικής Πρόσβασης

Η εταιρεία παρέδωσε τα δικαιώματα πρόσβασης των λογαριασμών που έχουν εγκριθεί, ενεργοποιηθεί και καταργηθεί στα ΠΕΣ που αναφέρονται αναλυτικά ανωτέρω, όπως προκύπτουν από το σύστημα, από 1.9.2013. Από την εξέταση του ως άνω εγγράφου, προκύπτει ότι το αρχείο περιέχει την ενέργεια της αίτησης και έγκρισης για τη δημιουργία ή τερματισμό ενός λογαριασμού (account), το χρόνο που πραγματοποιήθηκε η ενέργεια, και το



λογαριασμό στον οποίο αναφέρεται. Πλην όμως, δεν ακολουθεί τη δομή που περιγράφεται στην παράγραφο 2.3.5 (λογαριασμός πρόσβασης, προφίλ, χρονικό διάστημα ισχύος) και ειδικότερα, δεν αναφέρει τα δικαιώματα ή επίπεδο πρόσβασης των λογαριασμών που έχουν εγκριθεί και ενεργοποιηθεί στα ΠΕΣ.

Απόκλιση 14: Από τα ανωτέρω προκύπτει ότι δεν εφαρμόζεται πλήρως η παράγραφος 2.3.5 αναφορικά με το Αρχείο με το ιστορικό όλων των δικαιωμάτων ή επιπέδων πρόσβασης των λογαριασμών που έχουν εγκριθεί και ενεργοποιηθεί στα Συστήματα, όπως προβλέπεται στην παράγραφο 6.3.1.4 του άρθρου 6 της Απόφασης 165/2011.

ιδ) Ως προς την παράγραφο 2.4 της Πολιτικής Λογικής Πρόσβασης

Σύμφωνα με τη διαδικασία με κωδικό εγγράφου «Έλεγχος Ορθής Εφαρμογής της Πολιτικής Λογικής Πρόσβασης», η εταιρεία διενεργεί έξι (6) ελέγχους, οι οποίοι περιληπτικά είναι ο έλεγχος υλοποιημένων λογαριασμών πρόσβασης, ο έλεγχος δικαιωμάτων πρόσβασης, ο έλεγχος δικαιωμάτων πρόσβασης λογαριασμών (ανακάλυψη μη αιτιολογημένων προσβάσεων), ο έλεγχος εφαρμογής κανόνων δημιουργίας ονόματος χρήστη, ο έλεγχος διαδικασίας απόδοσης ονόματος χρήστη και ο έλεγχος εφαρμογής κανόνων δημιουργίας κωδικών πρόσβασης. Η διαδικασία προβλέπει ότι τα αποτελέσματα του ελέγχου καταγράφονται στην αναφορά ελέγχου ορθότητας δικαιωμάτων πρόσβασης. Η εταιρεία παρέδωσε τις σχετικές αναφορές για τα συστήματα και τα συστήματα δικτύου, που αφορούν στο τρίτο τρίμηνο του 2013. Από την εξέταση των παραπάνω αναφορών, προκύπτουν τα ακόλουθα:

A) Σύμφωνα με το περιεχόμενο των αναφορών, πραγματοποιήθηκε μόνο ο πρώτος έλεγχος από τους έξι που προβλέπει η διαδικασία (ο έλεγχος υλοποιημένων λογαριασμών πρόσβασης).

B) Από την αναφορά ελέγχου ορθότητας δικαιωμάτων πρόσβασης για τα συστήματα IT απουσιάζουν τα ΠΕΣ Σχετικά με αυτό, η εταιρεία δήλωσε ότι για το σύστημα FMS δεν είχε πραγματοποιήσει το σχετικό έλεγχο, ενώ για το σύστημα ο έλεγχος δεν πραγματοποιήθηκε, γιατί το σύστημα χρησιμοποιείται αποκλειστικά από πελάτες. Πλην όμως, η Ο.Ε. θεωρεί ότι για το σύστημα ο έλεγχος μπορεί να πραγματοποιηθεί σε



επίπεδο λειτουργικού συστήματος ή/και βάσης δεδομένων (εφόσον χρησιμοποιεί βάση δεδομένων).

Επιπρόσθετα, η εταιρεία παρέδωσε την πιο πρόσφατη Αναφορά Ελέγχου Ορθότητας Δικαιωμάτων Πρόσβασης για τα συστήματα ΙΤ του πρώτου τριμήνου του 2014, στην οποία περιλαμβάνονται και οι χρήστες του

Απόκλιση 15: Από τα ανωτέρω προκύπτει ότι δεν εφαρμόζεται πλήρως η παράγραφος 2.4.2 αναφορικά με τους ελέγχους που πρέπει να πραγματοποιούνται βάσει της διαδικασίας ελέγχου ορθής εφαρμογής της πολιτικής λογικής πρόσβασης, όπως προβλέπεται στην παράγραφο 6.3.2 του άρθρου 6 της Απόφασης 165/2011.

ιε) Ως προς την παράγραφο 2.5.2 της Πολιτικής Λογικής Πρόσβασης

Από την εξέταση των στοιχείων που ζήτησε και παρέλαβε η Ο.Ε. αναφορικά με την καταγραφή της πρόσβασης και της αιτιολόγησης σε δεδομένα επικοινωνίας συνδρομητών, όπως αναλυτικά εκτίθενται ανωτέρω, προέκυψε ότι:

Α) Για την εγγραφή «Dec 6 14:31:34 ...», η εταιρεία δηλώνει ότι «*Η αναζήτηση έχει γίνει με βάση το message ID που έχει δοθεί από πελάτη με προφορικό αίτημα*», χωρίς να διατηρεί σχετικό έγγραφο.

Β) Για τις εγγραφές «Dec 20 10:02:40...», «Dec 20 10:03:26...», «Dec 20 10:03:36...», που αφορούν πρόσβαση στον ίδιο λογαριασμό ηλεκτρονικού ταχυδρομείου, η εταιρεία δηλώνει ότι αποτελεί «*προφορικό αίτημα συναδέλφου (επιβεβαιώθηκε με e-mail)*». Το email έχει ημερομηνία 15.10.2014, μεταγενέστερη του επιτόπιου ελέγχου, ενώ επιπλέον δεν προκύπτει η σύνδεση του ονόματος ηλεκτρονικού ταχυδρομείου με το όνομα του προσώπου, δεδομένου ότι συνήθως το όνομα ηλεκτρονικού ταχυδρομείου είναι παράγωγο του ονόματος του προσώπου.

Γ) Για την εγγραφή «Dec 15 12:38:43», η εταιρεία δηλώνει ότι «*Η αναζήτηση έγινε με προφορικό αίτημα του πελάτη*», χωρίς να διατηρεί σχετικό έγγραφο.

Πλην όμως, στις υπόλοιπες περιπτώσεις πρόσβασης, η εταιρεία προσκόμισε έγγραφα (μηνύματα ηλεκτρονικού ταχυδρομείου, εκτύπωση από το σύστημα,), τα οποία αιτιολογούν την πρόσβαση.



Επιπλέον, η εταιρεία δήλωσε ότι είναι σε φάση τελικής ανασκόπησης και εγκρίσεων και ότι από μέσα Ιανουαρίου του 2014 εφαρμόζεται πιλοτικά η διαδικασία «Έλεγχος Αρχείων Καταγραφής Πρόσβασης Χρηστών σε Δεδομένα Επικοινωνίας Συνδρομητών» και παρέδωσε τη σχετική Αναφορά Ελέγχου Προσβάσεων σε Δεδομένα Επικοινωνίας Συνδρομητών του μηνός Ιανουαρίου 2014. Σύμφωνα με την Αναφορά, ο έλεγχος πραγματοποιήθηκε στα συστήματα

Απόκλιση 16: Από τα ανωτέρω προκύπτει ότι δεν εφαρμόζεται πλήρως η παράγραφος 2.5.2 αναφορικά με το γεγονός ότι κάθε πρόσβαση σε δεδομένα επικοινωνίας των συνδρομητών ή χρηστών των παρεχόμενων δικτύων ή υπηρεσιών πρέπει να καταγράφεται και να αιτιολογείται, όπως προβλέπεται στην παράγραφο 6.2.6 του άρθρου 6 της Απόφασης 165/2011.

ιστ) Ως προς την παράγραφο 2.2.1 της Πολιτικής Απομακρυσμένης Λογικής Πρόσβασης

Σύμφωνα με τη διαδικασία «Ενεργοποίηση Λογαριασμού Πρόσβασης Εξωτερικού Συνεργάτη», προκειμένου ένας εργαζόμενος να αποκτήσει απομακρυσμένη πρόσβαση σε εταιρικά συστήματα, καταχωρεί σχετική αίτηση στο σύστημα, το οποίο προωθείται προς έγκριση και υλοποίηση. Παρομοίως, εφόσον εξωτερικός συνεργάτης επιθυμεί να αποκτήσει απομακρυσμένη πρόσβαση σε εταιρικά συστήματα, συμπληρώνει το σχετικό έντυπο «Αίτηση Δημιουργίας Λογαριασμών για Εξωτερικούς Συνεργάτες», το οποίο προωθείται προς έγκριση και υλοποίηση.

Από την εξέταση των εγγράφων που ζήτησε και παρέλαβε η Ο.Ε., προκειμένου να ελεγχθεί δειγματοληπτικά η εφαρμογή της ως άνω διαδικασίας, όπως αυτά αναλυτικά εκτίθενται ανωτέρω, προκύπτουν τα ακόλουθα:

A) Σύστημα

Δε βρέθηκαν αιτήματα στο σύστημα για τους λογαριασμούς:

B) Σύστημα

Δε βρέθηκαν αιτήματα στο σύστημα για τους λογαριασμούς:

Γ) Σύστημα

Δε βρέθηκαν αιτήματα/εγκρίσεις για τους λογαριασμούς:



Επιπλέον επισημαίνεται ότι η εταιρεία έστειλε έντυπα αιτήσεων δημιουργίας λογαριασμών στα συστήματα για εργαζόμενους για τους οποίους δεν είχε καταστεί εφικτή η καταχώριση αιτήματος στο σύστημα Για το θέμα αυτό, η εταιρεία δήλωσε ότι οι χρήστες αυτοί ήταν εγκεκριμένοι με βάση την παλαιά διαδικασία, αλλά δεν είχαν προβεί εκ νέου σε αίτημα στο σύστημα

Απόκλιση 17: Από τα ανωτέρω προκύπτει ότι δεν εφαρμόζεται πλήρως η παράγραφος 2.2.1 αναφορικά με την εφαρμογή της διαδικασίας διαχείρισης των λογαριασμών απομακρυσμένης πρόσβασης των εργαζομένων και συνεργατών, ώστε να εξασφαλίζεται η αντιστοίχιση των λογαριασμών απομακρυσμένης πρόσβασης και του Αρχείου των εργαζομένων και συνεργατών που έχουν εξουσιοδοτηθεί να χρησιμοποιούν την απομακρυσμένη πρόσβαση, όπως προβλέπεται στην παράγραφο 7.3.1 του άρθρου 7 της Απόφασης 165/2011.

ιζ) Ως προς την παράγραφο 2.2.2 της Πολιτικής Απομακρυσμένης Λογικής Πρόσβασης

Σχετικά με τα αποτελέσματα των τριμηνιαίων ελέγχων που διενεργεί η εταιρεία στα δικαιώματα απομακρυσμένης πρόσβασης των χρηστών, η εταιρεία παρέδωσε τα έγγραφα με τίτλους «..... του τρίτου και τέταρτου τριμήνου του έτους 2013.

Από την εξέταση των ως άνω εγγράφων προκύπτουν τα ακόλουθα:

A) Και στις δύο αναφορές υπάρχουν ευρήματα, ενδεικτικά αναφέρεται ότι στα συστήματα δικτύου (..) βρέθηκαν 67 λογαριασμοί χρηστών το τρίτο τρίμηνο του 2013 (37 στο τέταρτο τρίμηνο) στην πλατφόρμα χωρίς αντίστοιχο αίτημα στο Αντίστοιχα βρέθηκαν 25 λογαριασμοί χρηστών το τρίτο τρίμηνο του 2013 (21 στο τέταρτο τρίμηνο) στην πλατφόρμα χωρίς αντίστοιχο αίτημα στο Για τα συστήματα ΙΤ βρέθηκαν 12 λογαριασμοί χρηστών το τρίτο τρίμηνο του 2013 (7 στο τέταρτο τρίμηνο) στην πλατφόρμα χωρίς αντίστοιχο αίτημα στο σύστημα Επισημαίνεται ότι τα συγκεκριμένα αποτελέσματα του ελέγχου εκ μέρους της εταιρείας επιβεβαιώνουν τα αποτελέσματα του ελέγχου της Α.Δ.Α.Ε., όπως αυτά έχουν αποτυπωθεί ανωτέρω στην Απόκλιση 17.

B) Το 2^ο σημείο ελέγχου της παραγράφου 2.2.2, δηλαδή ο έλεγχος της υλοποίησης των απαιτούμενων μεταβολών των κωδικών και απενεργοποιήσεων των λογαριασμών απομακρυσμένης πρόσβασης των συνεργατών της παρ. 2.1.6 της Πολιτικής



Απομακρυσμένης Λογικής Πρόσβασης, δε φαίνεται να έχει πραγματοποιηθεί. Γίνεται όμως αναφορά σε δειγματοληπτικό έλεγχο (6 συνδέσεων) για τις οποίες η εταιρεία έλεγξε τις αντίστοιχες αιτήσεις (σε έντυπο) έγκρισης και ενεργοποίησης.

Απόκλιση 18: Από τα ανωτέρω προκύπτει ότι δεν εφαρμόζεται πλήρως η παράγραφος 2.2.2 αναφορικά με τον έλεγχο της υλοποίησης των απαιτούμενων μεταβολών των κωδικών και απενεργοποιήσεων των λογαριασμών απομακρυσμένης πρόσβασης των συνεργατών της παρ. 2.1.6 της Πολιτικής Απομακρυσμένης Λογικής Πρόσβασης, όπως προβλέπεται στην παράγραφο 7.3.2.β του άρθρου 7 της Απόφασης 165/2011.

ιη) Ως προς την παράγραφο 2.4.2 της Πολιτικής Διαχείρισης και Εγκατάστασης ΠΕΣ

Η εταιρεία, αναφορικά με τις ενέργειες για την υλοποίηση των αλλαγών στο σύστημα, που περιέχονται στο αρχείο,

- δήλωσε ότι σε επίπεδο λειτουργικού συστήματος δεν έχει καταστεί τεχνικά εφικτή η ενεργοποίηση μηχανισμού καταγραφής ενεργειών, λόγω επίπτωσης στην απόδοση του συστήματος ενώ έχει ξεκινήσει έργο, ώστε, σε συνεργασία με τους αρμόδιους προμηθευτές, να παραμετροποιηθεί κατάλληλα ο εγγενής μηχανισμός καταγραφής του συστήματος και να περιοριστούν οι επιπτώσεις στη λειτουργία του. Αναφορικά με τον παρόντα χρόνο, εκ παραδρομής δε συμπεριελήφθη το σύστημα στην αντίστοιχη εξαίρεση.
- Παρέδωσε την καταγραφή ενεργειών στη Βάση Δεδομένων, για την αλλαγή με TaskID: 73518 του αρχείου αλλαγών καθώς και τις ρυθμίσεις που αφορούν την ενεργοποίηση του auditing (Task ID : 73553)

Από την εξέταση των παραπάνω στοιχείων διαπιστώθηκε ότι η εταιρεία παρέδωσε τις ενέργειες για 2 από τις 6 αλλαγές του συστήματος

Απόκλιση 19: Από τα ανωτέρω προκύπτει ότι δεν εφαρμόζεται πλήρως η παράγραφος 2.4.2 σχετικά με την καταγραφή των ενεργειών στα ΠΕΣ, όπως προβλέπεται στην παράγραφο 8.3.3.2 του άρθρου 8 της Απόφασης 165/2011.



ιθ) Ως προς την εφαρμογή της διαδικασίας με κωδικό «Διαχείριση Αλλαγών Εταιρικών Πληροφοριακών Συστημάτων»

Από την εξέταση των στοιχείων που παραδόθηκαν στην Ο.Ε. αναφορικά με την τεκμηρίωση που προκύπτει από τις ενέργειες της διαδικασίας για τις αλλαγές στο σύστημα με task ID: TAS000000004387, TAS000000004392, TAS000000004399, TAS000000004400, TAS000000004448, όπως αναλυτικά εκτίθενται ανωτέρω, διαπιστώθηκε ότι:

- Δεν προκύπτει ότι η κατηγοριοποίηση που παραδόθηκε αντιστοιχεί στις υπό εξέταση αλλαγές που πραγματοποιήθηκαν.
- Δεν προκύπτει ότι οι εκθέσεις αποδοχής που παραδόθηκαν αντιστοιχούν στις υπό εξέταση αλλαγές που πραγματοποιήθηκαν. Επιπλέον, στις εκθέσεις αποδοχής δεν υπάρχουν ημερομηνίες, καθώς και τα υπογεγραμμένα αποτελέσματα του από τα εμπλεκόμενα μέρη, σύμφωνα με την παράγραφο 6.5 της διαδικασίας.

Από την εξέταση των στοιχείων που παραδόθηκαν στην Ο.Ε. αναφορικά με την τεκμηρίωση που προκύπτει από τις ενέργειες της διαδικασίας για τις αλλαγές στο σύστημα με αύξοντα αριθμό 21 έως και 25 του αρχείου, όπως αναλυτικά εκτίθενται ανωτέρω, διαπιστώθηκε ότι:

- Δεν προκύπτει ότι η κατηγοριοποίηση που παραδόθηκε αντιστοιχεί στις υπό εξέταση αλλαγές που πραγματοποιήθηκαν.
- Δεν παραδόθηκε έκθεση αποδοχής για την αλλαγή με αριθμό 25.
- Στις υπόλοιπες εκθέσεις αποδοχής δεν υπάρχουν τα υπογεγραμμένα αποτελέσματα του από τα εμπλεκόμενα μέρη, σύμφωνα με την παράγραφο 6.5 της διαδικασίας.

Απόκλιση 20: Από τα ανωτέρω προκύπτει ότι δεν εφαρμόζονται συστηματικά οι παράγραφοι 6.1 και 6.5 της Διαδικασίας «Διαχείριση Αλλαγών Εταιρικών Πληροφοριακών Συστημάτων», όπως προβλέπεται στην παράγραφο 8.3.3 του άρθρου 8 της Απόφασης 165/2011.

ιυ) Ως προς την εφαρμογή της διαδικασίας «Διαχείριση Περιστατικών Ασφάλειας» της Πολιτικής Διαχείρισης Περιστατικών Ασφάλειας



Η εταιρεία, αναφορικά με τον φάκελο καταγραφής περιστατικών ασφάλειας, παρέδωσε λίστα με τα περιστατικά ασφάλειας από την έναρξη ισχύος της πολιτικής και τις σχετικές εκθέσεις αναφοράς περιστατικών ασφάλειας.

Από την εξέταση της λίστας των περιστατικών και των σχετικών εκθέσεων διαπιστώθηκαν τα εξής:

- Δεν έχει καταγραφεί στις εκθέσεις αναφοράς περιστατικών ασφάλειας οποιαδήποτε αναφορά σχετικά με τα συλλεχθέντα στοιχεία για τη διερεύνηση του περιστατικών και γενικότερα εάν έχει πραγματοποιηθεί περαιτέρω διερεύνηση των περιστατικών.
- Δεν είναι σαφές, εάν οι εκθέσεις του φακέλου αποτελούν τις εκθέσεις άμεσης αναφοράς ή τις τελικές εκθέσεις. Ωστόσο, τουλάχιστον για τις περιπτώσεις τις οποίες, σύμφωνα με την ως άνω διαπίστωση, θα έπρεπε να είχε πραγματοποιηθεί περαιτέρω διερεύνηση, η έκθεση που περιλαμβάνονται στο φάκελο είναι η έκθεση άμεσης αναφοράς και λείπει η τελική έκθεση με τα αποτελέσματα από την ολοκλήρωση της διερεύνησης του περιστατικού.
- Δεν έχουν καταγραφεί στις εκθέσεις αναφοράς περιστατικών ασφάλειας τα διορθωτικά μέτρα και το σχετικό χρονοδιάγραμμα.
- Δεν περιλαμβάνεται στη λίστα με τα περιστατικά ασφάλειας το με αριθ. πρωτ. ΑΔΑΕ ΑΠΡ 4431/18.11.2013 (893907/15.11.2013)

Απόκλιση 21: Από τα ανωτέρω προκύπτει ότι δεν εφαρμόζεται πλήρως η παράγραφος 6.6 της Διαδικασίας «Διαχείριση Περιστατικών Ασφάλειας» και η παράγραφος 2.1.2 της Πολιτικής Διαχείρισης Περιστατικών Ασφαλείας της εταιρείας, αναφορικά με τα ελάχιστα στοιχεία που πρέπει να καταγράφονται στην Έκθεση Άμεσης Αναφοράς Περιστατικού Ασφάλειας, όπως προβλέπεται στην παράγραφο 9.2.2 του άρθρου 9 της Απόφασης 165/2011.

Απόκλιση 22: Από τα ανωτέρω προκύπτει ότι δεν εφαρμόζεται πλήρως η παράγραφος 6.8 της Διαδικασίας «Διαχείριση Περιστατικών Ασφάλειας» και η παράγραφος 2.1.3 της Πολιτικής Διαχείρισης Περιστατικών Ασφαλείας της εταιρείας, αναφορικά με τη σύνταξη και αποστολή στην ΑΔΑΕ της Τελικής Έκθεσης Αναφοράς Περιστατικού Ασφάλειας, όπως προβλέπεται στην παράγραφο 9.2.3 του άρθρου 9 της Απόφασης 165/2011.



ικ) Ως προς την παράγραφο 2.1.3 της Πολιτικής Αντιμετώπισης Κακόβουλου Λογισμικού

Η εταιρεία ενημέρωσε την Ο.Ε. σχετικά με τον έλεγχο ακεραιότητας του λογισμικού των συστημάτων. Ειδικότερα:

- Στα συστήματα πραγματοποιείται έλεγχος ακεραιότητας μέσω του λογισμικού, από 1.2.2014, και δεν έχουν υπάρξει ευρήματα εγκατάστασης μη εξουσιοδοτημένου λογισμικού.
- Τα υπόλοιπα ΠΕΣ της Πληροφορικής (IT) προγραμματίζεται να ενταχθούν στο μηχανισμό ελέγχου ακεραιότητας μέσω του συστήματος μέχρι 31.12.2014.
- Στα συστήματα πραγματοποιείται έλεγχος ακεραιότητας του λογισμικού μέσω, από 4.4.2014 και 5.4.2014 αντίστοιχα, και δεν έχουν υπάρξει ευρήματα εγκατάστασης μη εξουσιοδοτημένου λογισμικού.
- Στα συστήματα προγραμματίζεται η εγκατάσταση τουμέχρι το τέλος του 2014.
- Το σύστημα έχει ενταχθεί σε πλατφόρμα, που χρησιμοποιείται αποκλειστικά για τα συστήματα, από το Μάρτιο του 2014, κατόπιν αναβάθμισης του λογισμικού και λήψης σχετικού πιστοποιητικού (συνημμένο 1 του σχετικού 17) για το λογισμικό της εταιρείας.
- Στο σύστημα πραγματοποιήθηκε, στο πλαίσιο του λογισμικού το Νοέμβριο του 2013 και προγραμματίζεται έλεγχος από τον προμηθευτή πριν το τέλος του Q3/14, με ταυτόχρονη ένταξή του στο, εφόσον δοθεί η συγκατάθεση του κατασκευαστή.
- Για τα υπόλοιπα ΠΕΣ της Τεχνολογίας (.....) είναι σε εξέλιξη η λήψη προτάσεων από τους προμηθευτές για την παροχή πιστοποίησης ως προς την ακεραιότητα του λογισμικού, προκειμένου να αξιολογηθούν οικονομοτεχνικά. Επισημαίνεται ότι για την παροχή της διασφάλισης τη ακεραιότητας από τους προμηθευτές απαιτούνται ιδιαίτερος υψηλά και δυσανάλογα κόστη. Παράλληλα εξετάζεται εναλλακτικά η χρήση του

Από τις παραπάνω δηλώσεις της εταιρείας διαπιστώθηκε ότι, ενώ σε κάποια από τα συστήματα της Πληροφορικής (.....) έχει πραγματοποιηθεί έλεγχος ακεραιότητας του λογισμικού και έχει προγραμματιστεί ο έλεγχος των υπολοίπων μέχρι το τέλος του 2014, όπως δηλώνεται και στις εξαιρέσεις, στα συστήματα της Τεχνολογίας (....), πλην των



δεν έχουν πραγματοποιηθεί έλεγχοι ούτε υπάρχει σαφές χρονοδιάγραμμα για την πραγματοποίησή τους.

Απόκλιση 23: Δεν εφαρμόζεται η παράγραφος 2.1.3 για όλα τα ΠΕΣ, όπως προβλέπεται στην παράγραφο 12.2.3 του άρθρου 12 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. Τις υπ' αριθμ. 3319/2010 και 1361/2013 αποφάσεις του Συμβουλίου της Επικρατείας,
16. Την υπ' αριθμ. πρωτ. ΑΔΑΕ ΕΜΠ 146/18-07-2013 Πολιτική Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών της εταιρείας «.....», όπως εγκρίθηκε με την υπ' αριθμ. 294/2013 Απόφαση της Α.Δ.Α.Ε.,
17. Την υπ' αριθμ. 3/2014 Απόφαση της Α.Δ.Α.Ε. σχετικά με τη σύσταση ομάδας ελέγχου για τη διενέργεια τακτικού ελέγχου στην εταιρεία «.....»,
18. το Πρακτικό Διενέργειας Επιτόπιου Ελέγχου στις εγκαταστάσεις, με αριθμ. πρωτ. ΑΔΑΕ ΕΜΠ36/7.02.2014,
19. το Πρακτικό Διενέργειας Επιτόπιου Ελέγχου στις εγκαταστάσεις, με αριθμ. πρωτ. ΑΔΑΕ ΕΜΠ49/21.02.2014,
20. το Πρακτικό Διενέργειας Επιτόπιου Ελέγχου στις εγκαταστάσεις, με αριθμ. πρωτ. ΑΔΑΕ ΕΜΠ69/5.03.2014,
21. το Πρακτικό Διενέργειας Επιτόπιου Ελέγχου στις εγκαταστάσεις, με αριθμ. πρωτ. ΑΔΑΕ ΕΜΠ78/24.03.2014,
22. το Πρακτικό Διενέργειας Επιτόπιου Ελέγχου στις εγκαταστάσεις, με αριθμ. πρωτ. ΑΔΑΕ ΕΜΠ94/10.04.2014,
23. το Πρακτικό Διενέργειας Επιτόπιου Ελέγχου στις εγκαταστάσεις, με αριθμ. πρωτ. ΑΔΑΕ ΕΜΠ104/16.04.2014,



24. το Πρακτικό Διενέργειας Επιτόπιου Ελέγχου στις εγκαταστάσεις, με αριθμ. πρωτ. ΑΔΑΕ ΕΜΠ135/15.05.2014,
25. το Πρακτικό Διενέργειας Επιτόπιου Ελέγχου στις εγκαταστάσεις, με αριθμ. πρωτ. ΑΔΑΕ ΕΜΠ143/30.05.2014,
26. το Πρακτικό Διενέργειας Επιτόπιου Ελέγχου στις εγκαταστάσεις, με αριθμ. πρωτ. ΑΔΑΕ ΕΜΠ151/18.06.2014,
27. το Πρακτικό Διενέργειας Επιτόπιου Ελέγχου στις εγκαταστάσεις, με αριθμ. πρωτ. ΑΔΑΕ ΕΜΠ153/23.06.2014,
28. το Πρακτικό Διενέργειας Επιτόπιου Ελέγχου στις εγκαταστάσεις, με αριθμ. πρωτ. ΑΔΑΕ ΕΜΠ190/10.09.2014,
29. το Πρακτικό Διενέργειας Επιτόπιου Ελέγχου στις εγκαταστάσεις, με αριθμ. πρωτ. ΑΔΑΕ ΕΜΠ192/15.09.2014,
30. το Πρακτικό Διενέργειας Επιτόπιου Ελέγχου στις εγκαταστάσεις, με αριθμ. πρωτ. ΑΔΑΕ ΕΜΠ207/13.10.2014,
31. την υπ. αριθμ. πρωτ. ΑΔΑΕ ΑΠΡ919/14.3.2014 επιστολή, με θέμα «Παροχή πληροφοριών σε συνέχεια του υπ. αρ. πρωτ. ΑΔΑΕ 2489/22.11.2013 εγγράφου»,
32. την υπ. αριθμ. πρωτ. ΑΔΑΕ 739/14.3.2014 επιστολή, με θέμα «Παροχή στοιχείων σε συνέχεια του από 04/03/2014 Τακτικού Ελέγχου»,
33. την υπ. αριθμ. πρωτ. ΑΔΑΕ 861/27.3.2014 επιστολή, με θέμα «Παροχή στοιχείων σε συνέχεια του από 18/03/2014 Τακτικού Ελέγχου»,
34. την υπ. αριθμ. πρωτ. ΑΔΑΕ ΑΠΡ1290/14.04.2014 επιστολή, με θέμα «Παροχή στοιχείων σε συνέχεια του από 8/4/2014 Τακτικού Ελέγχου»,
35. την υπ. αριθμ. πρωτ. ΑΔΑΕ ΑΠΡ1389/24.04.2014 επιστολή, με θέμα «Παροχή στοιχείων σε συνέχεια του από 15/4/2014 Τακτικού Ελέγχου»,
36. την υπ. αριθμ. πρωτ. ΑΔΑΕ ΑΠΡ1752/23.05.2014 επιστολή, με θέμα «Παροχή στοιχείων σε συνέχεια του από 13/5/2014 Τακτικού Ελέγχου»,
37. την υπ. αριθμ. πρωτ. ΑΔΑΕ ΑΠΡ1874/3.06.2014 επιστολή, με θέμα «Παροχή στοιχείων σε συνέχεια του από 27/5/2014 Τακτικού Ελέγχου»,
38. την υπ. αριθμ. πρωτ. ΑΔΑΕ ΑΠΡ2254/7.07.2014 επιστολή, με θέμα «Παροχή στοιχείων σε συνέχεια του από 20/6/2014 Τακτικού Ελέγχου»,



39. την υπ' αριθμ. πρωτ. ΑΔΑΕ ΑΠΡ 2345/15.7.2014 επιστολή, με θέμα «Κοινοποίηση εντύπου καταγραφής εξαίρεσης από την Πολιτική Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών»,
40. την υπ. αριθμ. πρωτ. ΑΔΑΕ ΑΠΡ3195/22.09.2014 επιστολή, με θέμα «Παροχή στοιχείων σε συνέχεια διενέργειας Τακτικού Ελέγχου»,
41. την υπ. αριθμ. πρωτ. ΑΔΑΕ ΑΠΡ3196/22.09.2014 επιστολή, με θέμα «Παροχή στοιχείων σε συνέχεια διενέργειας Τακτικού Ελέγχου»,
42. την υπ. αριθμ. πρωτ. ΑΔΑΕ ΑΠΡ3594/20.10.2014 επιστολή, με θέμα «Παροχή στοιχείων σε συνέχεια του από 9/10/2014 Τακτικού Ελέγχου»,
43. την από 10.2.2015 «Έκθεση Διενέργειας Τακτικού Ελέγχου στην εταιρεία» με τα σχετικά αυτής,
44. Την υπ' αριθμ. 65/2015 Εισήγηση προς την Ολομέλεια της Α.Δ.Α.Ε.,
45. Το πρακτικό της από 23-07-2015 συνεδρίασης της Ολομέλειας της Α.Δ.Α.Ε.,
46. Την υπ' αριθμ. 209/2015 Απόφαση της Α.Δ.Α.Ε. περί έγκρισης της ως άνω από 10-02-2015 Έκθεσης διενέργειας τακτικού ελέγχου στην εταιρεία «.....», η οποία παραδόθηκε στην εταιρεία «.....», όπως προκύπτει από την υπ' αριθμ. πρωτ. ΑΔΑΕ 2241/14-10-2015 Απόδειξη παράδοσης – παραλαβής,
47. Το υπ' αριθμ. πρωτ. ΑΔΑΕ 2293/05-10-2016 έγγραφο της Α.Δ.Α.Ε. προς την εταιρεία «.....» μετά των συνημμένων αυτού, το οποίο παραδόθηκε στην εταιρεία, όπως προκύπτει από την υπ' αριθμ. πρωτ. ΑΔΑΕ 2308/06-10-2016 Απόδειξη παράδοσης – παραλαβής,
48. Την υπ' αριθμ. 32/2017 εισήγηση προς την Ολομέλεια της Α.Δ.Α.Ε.,
49. Το πρακτικό της από 1 Φεβρουαρίου 2017 συνεδρίασης της Ολομέλειας της Α.Δ.Α.Ε.,
50. 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 **6^η Σεπτεμβρίου 2017, 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 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. 294/2013 απόφαση της Α.Δ.Α.Ε. Πολιτική Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών της εταιρείας, όπως αυτές αναφέρονται στην από 10 Φεβρουαρίου 2015 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 αναπληρωματικό μέλος της Α.Δ.Α.Ε., κ. Γεώργιος Μισαηλίδης.

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

Κρίθηκε και αποφασίστηκε την 1^η Φεβρουαρίου 2017.

Ο Πρόεδρος

Χρήστος Ζαμπίρας