Αριθμός Απόφασης : Α4154/2024

ΤΟ

ΔΙΟΙΚΗΤΙΚΟ ΕΦΕΤΕΙΟ ΑΘΗΝΩΝ

ΤΜΗΜΑ 16ο ΤΡΙΜΕΛΕΣ

Σ υ ν ε δ ρ ί α σ ε δημόσια στο ακροατήριό του στις 16 Οκτωβρίου 2024 με δικαστές τους: Καλλιόπη Θεοδωράτου Εφέτη Διοικητικών Δικαστηρίων, ως Προεδρεύουσα δυνάμει της 28/2023 Πράξης του Τριμελούς Συμβουλίου Διεύθυνσης του Διοικητικού Εφετείου Αθηνών, Αναστάσιο Σάββα και Γεώργιο Διονύσιο Ν. Τσαπράζη (εισηγητή) Εφέτες Διοικητικών Δικαστηρίων και Γραμματέα την Κωνσταντίνα Αμερικάνη, δικαστική υπάλληλο,

για να δικάσει την προσφυγή με πράξη κατάθεσης ΠΡ 916/20.9.2022,

της ανώνυμης εταιρείας με την επωνυμία « COSMOTE –ΚΙΝΗΤΕΣ ΤΗΛΕΠΙΚΟΙΝΩΝΙΕΣ ΜΟΝΟΠΡΟΣΩΠΗ ΑΝΩΝΥΜΟΣ ΕΤΑΙΡΕΙΑ» και τον διακριτικό τίτλο «COSMOTE», που εδρεύει στο Αμαρούσιο Αττικής (Λεωφ. Κηφισίας 99) και ήδη «ΟΡΓΑΝΙΣΜΟΣ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ ΤΗΣ ΕΛΛΑΔΟΣ ΑΝΩΝΥΜΗ ΕΤΑΙΡΕΙΑ», που εδρεύει ομοίως και παραστάθηκε με την πληρεξούσια δικηγόρο της Ελένη Γερούτση, η οποία κατέθεσε την ΔΛΠ 22442/15.10.2024 δήλωση, κατ’ άρθρο 133 παρ. 2 του ΚΔΔ κατά

της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών, που εδρεύει στο Αμαρούσιο Αττικής (οδός Ιερού Λόχου 63), εκπροσωπείται από τον Πρόεδρό της και παραστάθηκε με τη δικηγόρο Αφροδίτη Κουσουνή, η οποία κατέθεσε την ΔΛΠ 22245/14.10.2024 δήλωση, κατ’ άρθρο 133 παρ. 2 του ΚΔΔ.

Μετά τη συνεδρίαση το Δικαστήριο συνήλθε σε διάσκεψη.

ΑΦΟΥ ΜΕΛΕΤΗΣΕ ΤΗ ΔΙΚΟΓΡΑΦΙΑ

ΣΚΕΦΘΗΚΕ ΚΑΤΑ ΝΟΜΟ

Επειδή, με την κρινόμενη προσφυγή, για την οποία καταβλήθηκε το νόμιμο παράβολο (βλ. το 533543678953 0320 0004 e-παράβολο τύπου 1367) και τους με αρ. καταθ. ΠΛ 163/25.9.2024 πρόσθετους λόγους (σχ. η 5184/26.9.2024 έκθεση επίδοσης του Δικαστικού Επιμελητή Π. Κουτσιβίτη), η προσφεύγουσα εταιρεία επιδιώκει παραδεκτώς την ακύρωση, άλλως την τροποποίηση της με αρ. 225/30.5.2022 απόφασης της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), με την οποία της επιβλήθηκε : α) πρόστιμο ύψους 200.000,00 ευρώ, λόγω διαρροής στοιχείων προσδιοριστικών της προσφεύγουσας και του λογαριασμού πρόσβασης (όνομα χρήστη- κωδικός) υπαλλήλου της διαχειριστή σε Πληροφοριακά και Επικοινωνιακά Συστήματα (ΠΕΣ) και β) πρόστιμο ύψους 3.000.000,00 ευρώ, λόγω πολλαπλών αποκλίσεων (6), κατά το χρόνο διαρροής των ως άνω στοιχείων, ως προς την εφαρμογή της Πολιτικής Ασφαλείας για την Διασφάλιση του Απορρήτου των Επικοινωνιών της προσφεύγουσας, που είχε εγκριθεί με τις 155/2012 και 327/2013 αποφάσεις της ΑΔΑΕ, σε συνδυασμό με τον Κανονισμό Διασφάλισης του Απορρήτου των Επικοινωνιών (βλ. κατωτέρω σκ. 16η).

Επειδή, μετά την άσκηση του υπό κρίση ενδίκου βοηθήματος, η προσφεύγουσα εταιρεία με τον διακριτικό τίτλο «COSMOTE» απορροφήθηκε λόγω συγχωνεύσεως από την ανώνυμη εταιρεία με την επωνυμία «ΟΡΓΑΝΙΣΜΟΣ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ ΕΛΛΑΔΟΣ» [σχ. η 3189349ΑΠ/2.1.2024 απόφαση της Γενικής Γραμματείας Εμπορίου /Γενική Διεύθυνση Αγοράς και Προστασίας Καταναλωτή /Διεύθυνση Εταιρειών-Τμήμα Εισηγμένων Α.Ε. (αρ. ΓΕΜΗ 3959144)], η οποία πλέον υπεισήλθε στο σύνολο των σχετικών δικαιωμάτων και υποχρεώσεων της προσφεύγουσας (βλ. άρθρο 18 ν. 4601/2019-Α΄44), νομίμως δε, συνεχίζει την παρούσα δίκη (πρβλ. ΣτΕ 1984/2018 σκ. 2η).

Επειδή, στο άρθρο 19 του Συντάγματος ορίζεται ότι : «1. Το απόρρητο των επιστολών και της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιονδήποτε άλλο τρόπο είναι απόλυτα απαραβίαστο. […] 2. Νόμος ορίζει τα σχετικά με τη συγκρότηση, τη λειτουργία και τις αρμοδιότητες ανεξάρτητης αρχής που διασφαλίζει το απόρρητο της παραγράφου 1. […]».

Επειδή, στο άρθρο 1 του ν. 3115/2003 (Α΄47) «Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών» ορίζεται ότι : «1. Συνιστάται, κατά την παράγραφο 2 του άρθρου 19 του Συντάγματος, Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (Α.Δ.Α.Ε.), με σκοπό την προστασία του απορρήτου των επιστολών και της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιονδήποτε άλλο τρόπο. Στην έννοια της προστασίας του απορρήτου των επικοινωνιών περιλαμβάνεται και ο έλεγχος της τήρησης των όρων και της διαδικασίας άρσης του απορρήτου. […] », στο άρθρο 6 ότι : «1. Η Α.Δ.Α.Ε., για την εκπλήρωση της αποστολής της, έχει τις ακόλουθες αρμοδιότητες : α) Διενεργεί, αυτεπαγγέλτως ή κατόπιν καταγγελίας, τακτικούς και έκτακτους ελέγχους, σε εγκαταστάσεις, τεχνικό εξοπλισμό, αρχεία, τράπεζες δεδομένων και έγγραφα […] ιδιωτικών επιχειρήσεων που ασχολούνται με ταχυδρομικές, τηλεπικοινωνιακές ή άλλες υπηρεσίες σχετικές με την ανταπόκριση και την επικοινωνία. Τον έλεγχο διενεργεί μέλος ή μέλη της Α.Δ.Α.Ε., συμμετέχει δε και υπάλληλός της, ειδικά προς τούτο εντεταλμένος από τον πρόεδρό της για γραμματειακή υποστήριξη της διαδικασίας του ελέγχου. […] β) Λαμβάνει πληροφορίες σχετικές με την αποστολή της, από τις υπό το στοιχείο α΄ επιχειρήσεις, […] γ) Καλεί σε ακρόαση, από τις υπηρεσίες, οργανισμούς, νομικά πρόσωπα και επιχειρήσεις που αναφέρονται στο ως άνω στοιχείο α, τις διοικήσεις, τους νόμιμους εκπροσώπους, τους υπαλλήλους και κάθε άλλο πρόσωπο, το οποίο κρίνει ότι μπορεί να συμβάλλει στην εκπλήρωση της αποστολής της. […] ιβ) Εκδίδει κανονιστικές πράξεις, δημοσιευόμενες στην Εφημερίδα της Κυβερνήσεως, δια των οποίων ρυθμίζεται κάθε διαδικασία και λεπτομέρεια σε σχέση με τις ανωτέρω αρμοδιότητές της, καθώς και με την εν γένει διασφάλιση του απορρήτου των επικοινωνιών. […]».

Επειδή, περαιτέρω στο άρθρο 4 του ν. 3471/2006 (Α΄ 133) «Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και τροποποίηση του ν.2472/1997», με τον οποίον ενσωματώθηκε στην εθνική έννομη τάξη η Οδηγία 2002/58/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου «Σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών» (L 201), ορίζεται ότι : «1.Οποιαδήποτε χρήση των υπηρεσιών ηλεκτρονικών επικοινωνιών που παρέχονται μέσω δημοσίου δικτύου επικοινωνιών και των διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών, καθώς και των συναφών δεδομένων κίνησης και θέσης, όπως ορίζονται στις διατάξεις του άρθρου 2 του παρόντος νόμου, προστατεύεται από το απόρρητο των επικοινωνιών. […]», στο άρθρο 2 ότι : «Πέραν των ορισμών που περιλαμβάνονται στο άρθρο 2 του ν. 2472/1997 (ΦΕΚ 50 Α΄), όπως ισχύει, λαμβανομένων δε υπόψη των ορισμών του ν. 3431/2006 (ΦΕΚ 13 Α΄) νοούνται, για τους σκοπούς του νόμου αυτού, ως: […] 3. "δεδομένα κίνησης": τα δεδομένα που υποβάλλονται σε επεξεργασία για τους σκοπούς της διαβίβασης μίας επικοινωνίας σε δίκτυο ηλεκτρονικών επικοινωνιών ή της χρέωσής της. Στα δεδομένα κίνησης μπορεί να περιλαμβάνονται, μεταξύ άλλων, ο αριθμός, η διεύθυνση, η ταυτότητα της σύνδεσης ή του τερματικού εξοπλισμού του συνδρομητή ή και χρήστη, οι κωδικοί πρόσβασης, τα δεδομένα θέσης, η ημερομηνία και ώρα έναρξης και λήξης και η διάρκεια της επικοινωνίας, ο όγκος των διαβιβασθέντων δεδομένων, πληροφορίες σχετικά με το πρωτόκολλο, τη μορφοποίηση, τη δρομολόγηση της επικοινωνίας καθώς και το δίκτυο από το οποίο προέρχεται ή στο οποίο καταλήγει η επικοινωνία. 4. "δεδομένα θέσης" : τα δεδομένα που υποβάλλονται σε επεξεργασία σε δίκτυο ηλεκτρονικών επικοινωνιών ή από μια υπηρεσία ηλεκτρονικών επικοινωνιών και που υποδεικνύουν τη γεωγραφική θέση του τερματικού εξοπλισμού του χρήστη μια διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών.» και στο άρθρο 12 ότι : «1.Ο φορέας παροχής διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών οφείλει να λαμβάνει τα ενδεδειγμένα τεχνικά και οργανωτικά μέτρα, προκειμένου να προστατεύεται η Ασφάλεια των υπηρεσιών του, καθώς και η Ασφάλεια του δημοσίου δικτύου ηλεκτρονικών επικοινωνιών. Τα μέτρα αυτά, εφόσον είναι αναγκαίο, λαμβάνονται από κοινού με τον φορέα παροχής του δημοσίου δικτύου ηλεκτρονικών επικοινωνιών, πρέπει δε να εγγυώνται επίπεδο ασφαλείας ανάλογο προς τον υπάρχοντα κίνδυνο, λαμβανομένων υπόψη αφ ενός των πλέον προσφάτων τεχνικών δυνατοτήτων αφ ετέρου δε του κόστους εφαρμογής τους. […] 5. Σε περίπτωση παραβίασης δεδομένων προσωπικού χαρακτήρα, ο φορέας παροχής διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών γνωστοποιεί αμελλητί την παραβίαση στην Α.Π.Δ.Π.Χ. και στην Α.Δ.Α.Ε.. Η γνωστοποίηση προς τις αρμόδιες αρχές περιλαμβάνει κατ᾽ ελάχιστον περιγραφή της φύσης της

παραβίασης δεδομένων προσωπικού χαρακτήρα και των σημείων επαφής από τα οποία μπορούν να αποκτηθούν περισσότερες πληροφορίες. Περιγράφονται επίσης οι συνέπειες της παραβίασης και τα μέτρα που προτάθηκαν ή λήφθηκαν από τον φορέα για την αντιμετώπιση της παραβίασης. […] ».

Επειδή, εξάλλου, στο άρθρο 2 του ν. 3674/2008 (Α΄ 136) «Ενίσχυση του θεσμικού πλαισίου διασφάλισης του απορρήτου της τηλεφωνικής επικοινωνίας και άλλες διατάξεις.» ορίζεται ότι : «1. Ο πάροχος ευθύνεται για την ασφάλεια των υπό την εποπτεία του χώρων, εγκαταστάσεων, συνδέσεων και των συστημάτων υλικού και λογισμικού. Προς τούτο έχει την υποχρέωση να λαμβάνει τα κατάλληλα τεχνικά και οργανωτικά μέτρα και να χρησιμοποιεί συστήματα υλικού και λογισμικού, τα οποία διασφαλίζουν το απόρρητο της επικοινωνίας και επιτρέπουν την αποκάλυψη της παραβίασης ή απόπειρας παραβίασης του απορρήτου της επικοινωνίας. 2. Ο πάροχος υποχρεούται να διασφαλίζει την τήρηση των προβλεπόμενων στην προηγούμενη παράγραφο μέτρων, να προβαίνει σε τακτικό έλεγχο των συστημάτων υλικού και λογισμικού που βρίσκονται στην εποπτεία του και να έχει πλήρη γνώση των τεχνικών δυνατοτήτων τους.», στο άρθρο 3 ότι : «1. Ο πάροχος υποχρεούται να καταρτίζει και εφαρμόζει ειδικό σχέδιο πολιτικής ασφάλειας ως προς τα μέσα, τις μεθόδους και τα μέτρα που διασφαλίζουν το απόρρητο της επικοινωνίας, σύμφωνα με τα οριζόμενα σε κανονισμούς της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ) που εκδίδονται κατά το άρθρο 6 παράγραφος 1 περίπτωση ιβ΄ του ν. 3115/2003 (ΦΕΚ 47 Α). Στο ειδικό σχέδιο πολιτικής ασφάλειας περιέχονται ιδίως: α) τα συστήματα που χρησιμοποιούνται για τη διασφάλιση του απορρήτου, β) η καταγραφή και αξιολόγηση των κινδύνων που ενδέχεται να επηρεάσουν την εύρυθμη λειτουργία του εξοπλισμού και να οδηγήσουν σε παραβίαση του απορρήτου της επικοινωνίας, και γ) τα μέτρα αποτροπής των κινδύνων που έχουν αναγνωριστεί. Το ειδικό σχέδιο πολιτικής ασφάλειας και κάθε αναθεώρηση αυτού εγκρίνεται από την ΑΔΑΕ. 2. Η εφαρμογή του ειδικού σχεδίου πολιτικής ασφάλειας ανατίθεται από τον πάροχο σε εξουσιοδοτούμενο στέλεχος, το οποίο ορίζεται ως υπεύθυνος διασφάλισης του απορρήτου. Η σχετική απόφαση του παρόχου υποβάλλεται στην ΑΔΑΕ και κοινοποιείται στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ) και στην Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ). […]. 3. Ο πάροχος, τα μέλη της διοίκησης και ο νόμιμος εκπρόσωπος αυτού, ο υπεύθυνος διασφάλισης του απορρήτου, οι εργαζόμενοι και οι συνεργάτες του παρόχου έχουν υποχρέωση εχεμύθειας για όλα τα θέματα που αφορούν το απόρρητο των επικοινωνιών.», στο άρθρο 8 ότι : «1. Σε περίπτωση παραβίασης ή ιδιαίτερου κινδύνου παραβίασης του απορρήτου της επικοινωνίας, ο υπεύθυνος διασφάλισης του απορρήτου υποχρεούται να ενημερώνει αμελλητί τον πάροχο ή τον νόμιμο εκπρόσωπο αυτού, την εισαγγελική αρχή, την ΑΔΑΕ και τους κατά περίπτωση θιγόμενους συνδρομητές. Η ενημέρωση γίνεται εγγράφως και σε περίπτωση αδυναμίας άμεσης επικοινωνίας με οποιοδήποτε άλλο πρόσφορο μέσο. […]» και στο άρθρο 11 ότι : «1. Όταν παραβιάζεται υποχρέωση που προβλέπεται στα άρθρα 2 έως 8 […] από τον πάροχο υπηρεσιών τηλεφωνίας ή τον νόμιμο εκπρόσωπο του, μέλος της διοίκησης, τον υπεύθυνο διασφάλισης του απορρήτου, εργαζόμενο ή συνεργάτη του παρόχου, επιβάλλεται για κάθε παράβαση στον πάροχο, ανάλογα με τη βαρύτητα της παράβασης, το βαθμό υπαιτιότητας και την περίπτωση υποτροπής, μία από τις παρακάτω κυρώσεις: α) σύσταση για συμμόρφωση μέσα στα χρονικά όρια της τασσόμενης προθεσμίας με προειδοποίηση επιβολής προστίμου σε περίπτωση παράλειψης συμμόρφωσης, β) πρόστιμο από είκοσι χιλιάδες (20.000) ευρώ έως πέντε εκατομμύρια (5.000.000) ευρώ, […] 2. Οι κυρώσεις της σύστασης και του προστίμου επιβάλλονται με αιτιολογημένη απόφαση της ΑΔΑΕ ύστερα από προηγούμενη κλήση του ενδιαφερομένου για παροχή εξηγήσεων. […]».

Επειδή, στον Κανονισμό για τη Διασφάλιση του Απορρήτου των Ηλεκτρονικών Επικοινωνιών [Αριθμός Απόφασης 165/2011 της Ολομέλειας της ΑΑΔΕ – Β΄ 2715/2011 (εφεξής ΚΔΑΗΕ)], που εκδόθηκε κατ’ εξουσιοδότηση του άρθρου 6 παρ.1 του ν. 3115/2003 και του άρθρου 5 του ν. 3674/2008 και ίσχυε κατά τον κρίσιμο χρόνο, προ της αντικατάστασής του με την 28/2024 απόφαση της Ολομέλειας της ΑΔΑΕ (Β΄ 551/26.1.2024), ορίζονταν στο άρθρο 1 ότι : «1.1. Στις διατάξεις του παρόντος Κανονισμού εμπίπτουν όλα τα πρόσωπα που ασχολούνται με την παροχή δικτύων ή/και υπηρεσιών ηλεκτρονικών επικοινωνιών. Τα πρόσωπα αυτά υποχρεούνται να διαθέτουν και να εφαρμόζουν Πολιτική Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών, της οποίας το περιεχόμενο είναι σύμφωνο με τις διατάξεις του παρόντος Κανονισμού.[…]», στο άρθρο 4 ότι : «4.1. Η Πολιτική Αποδεκτής Χρήσης καθορίζει τις υποχρεώσεις του υπόχρεου προσώπου αλλά και τις αρχές, τους κανόνες και τις συνέπειες για τους εργαζόμενους και συνεργάτες του, στους οποίους εκχωρείται το δικαίωμα πρόσβασης σε ΠΕΣ και δεδομένα επικοινωνίας, και αποβλέπει στην αποτροπή καταχρηστικής άσκησης των δικαιωμάτων τους και της τέλεσης πράξεων που παραβιάζουν ή συνιστούν κίνδυνο παραβίασης του απορρήτου των επικοινωνιών των συνδρομητών ή χρηστών των παρεχόμενων δικτύων ή

υπηρεσιών. 4.2.1. Οι εργαζόμενοι και συνεργάτες του υπόχρεου προσώπου οφείλουν να συμμορφώνονται με την Πολιτική Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών, συμπεριλαμβανομένων των σχετικών διαδικασιών, μέτρων ασφάλειας και οδηγιών. Για το σκοπό αυτό, το υπόχρεο πρόσωπο οφείλει να καταγράφει στην Πολιτική Αποδεκτής Χρήσης τον τρόπο με τον οποίο εξασφαλίζει ότι οι εργαζόμενοι και συνεργάτες του λαμβάνουν γνώση και έχουν αποδεχτεί την Πολιτική Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών ως προς την εργασία τους, προ της απόκτησης πρόσβασης σε ΠΕΣ και σε δεδομένα επικοινωνίας.[…]».

Επειδή, περαιτέρω, στο άρθρο 10.1 του ΚΔΑΗΕ ορίζεται ότι : «10.1. Ο σκοπός της Πολιτικής Ασφάλειας Δικτύου είναι ο λογικός διαχωρισμός των δικτύων του υπόχρεου προσώπου από εξωτερικά δίκτυα και η κατάτμηση των δικτύων του σε ζώνες ασφάλειας ή υποδίκτυα, ανάλογα με το επίπεδο ασφάλειας που απαιτείται, με στόχο την απομόνωση των ΠΕΣ σε ζώνες ασφάλειας, τον διαχωρισμό αυτών σε δικτυακό επίπεδο, και τον έλεγχο της ροής δεδομένων μεταξύ αυτών. […]» και στην παρ. 2.1.1. της Πολίτικης Ασφαλείας Δικτύου της προσφεύγουσας,που είχε εγκριθεί με τις 155/2012 και 327/2013 Αποφάσεις της ΑΔΑΕ προβλέπεται ότι : «Πρέπει να καταρτίζεται και να διατηρείται διαρκώς ενημερωμένο αρχείο στο οποίο ορίζονται οι μηχανισμοί και τα Συστήματα που χρησιμοποιούνται σε υλικό και λογισμικό για τους σκοπούς της Πολιτικής Ασφάλειας Δικτύου, καθώς και οι τρόποι λειτουργίας και τεχνικής διαμόρφωσης αυτών, οι οποίοι θα πρέπει να λαμβάνουν υπόψη τις διεθνείς ευρέως αποδεκτές πρακτικές και πρότυπα και την αποτίμηση κινδύνου που έχει πραγματοποιηθεί σύμφωνα με την παρ.5.2 της Πολιτικής ».

Επειδή, στο άρθρο 3.3.1 του ΚΔΑΗΕ ορίζονταν ότι : «3.3.1. Το υπόχρεο πρόσωπο οφείλει να διατηρεί και να εφαρμόζει διαδικασία αποτίμησης πληροφοριακού κινδύνου σχετικά με το απόρρητο της επικοινωνίας βασισμένη σε μεθοδολογία αποτίμησης κινδύνου που λαμβάνει υπόψη διεθνείς πρακτικές. Η αποτίμηση πληροφοριακού κινδύνου πραγματοποιείται κατ’ ελάχιστον κάθε δύο (2) έτη […] » και στις παρ. 5.2.4 και 5.2.5 της Διαδικασίας Αποτίμησης Κινδύνου της Πολιτικής Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών της προσφεύγουσας,,που είχε εγκριθεί με τις 155/2012 και 327/2013 Αποφάσεις της ΑΔΑΕ, ορίζεται ότι : «5.2.4. Πρέπει να διενεργείται αποτίμηση των απειλών που σχετίζονται με ενδεχόμενη παραβίαση του απορρήτου από εξωτερικές απειλές, εργαζόμενους ή συνεργάτες της εταιρείας, αποτίμηση των σχετικών ευπαθειών των Συστημάτων και αποτίμηση των πιθανών επιπτώσεων των περιστατικών παραβίασης του απορρήτου. 5.2.5. Τα αποτελέσματα της αποτίμησης κινδύνου λαμβάνονται υπόψη για τη σύνταξη και την αναθεώρηση της Πολιτικής και την υλοποίηση των κατάλληλων μέτρων για την εφαρμογή της».

Επειδή, στο άρθρο 3.2.9 του ΚΔΑΗΕ ορίζονταν ότι : «3.2.9. Αναφορικά με τα αρχεία καταγραφής των άρθρων 6.2.5 και 8.3.3.2 του παρόντος Κανονισμού, το υπόχρεο πρόσωπο υποχρεούται να εξασφαλίζει ότι οι καταγραφές που προβλέπονται στα εν λόγω άρθρα είναι πλήρεις και συνεχείς. Το υπόχρεο πρόσωπο οφείλει να διατηρεί Ειδικό Σχέδιο Αρχείων Καταγραφής, το οποίο, κατ’ ελάχιστον, περιλαμβάνει την αρχιτεκτονική και τις επιμέρους μεθόδους δημιουργίας, συλλογής, αποθήκευσης και διαχείρισης των αρχείων καταγραφής, πλήρη περιγραφή του περιεχομένου αυτών, καθώς και τα μέτρα για τη διασφάλιση της ακεραιότητας, της εμπιστευτικότητας και της διαθεσιμότητας αυτών. Το υπόχρεο πρόσωπο οφείλει να ενεργοποιεί την Πολιτική Διαχείρισης Περιστατικών Ασφάλειας, σύμφωνα με το άρθρο 9 του παρόντος Κανονισμού, σε περίπτωση διακοπής των καταγραφών που προβλέπονται στα ως άνω άρθρα και σε περίπτωση περιστατικού παραβίασης της ακεραιότητας, εμπιστευτικότητας και διαθεσιμότητας αυτών.» στο άρθρο 6.2.5 ότι : «6.2.5. Το υπόχρεο πρόσωπο οφείλει να τηρεί αρχείο καταγραφής των προσβάσεων των χρηστών των ΠΕΣ σε αυτά, στο οποίο καταγράφονται, και ελάχιστον, το όνομα χρήστη που απέκτησε την πρόσβαση, και η ημερομηνία και ώρα εκκίνησης και τερματισμού της πρόσβασης.», στο άρθρο 8.3.3.2 ότι : «8.3.3.2. Το υπόχρεο πρόσωπο υποχρεούται να καταγράφει και να διατηρεί σε αρχείο τις ενέργειες στο λειτουργικό σύστημα και στις εφαρμογές των ΠΕΣ, καθώς και τα συμβάντα συστήματος των ΠΕΣ.» και στην παρ. 5.1.7 της Πολιτικής Ασφάλειας για την Διασφάλιση του Απορρήτου των Επικοινωνιών της προσφεύγουσας ότι :« 5.1.7. Αναφορικά με τα αρχεία καταγραφής της παρ.2.5.1 της Πολιτικής Λογικής Πρόσβασης και της παρ.2.4.2 της Πολιτικής Διαχείρισης & Εγκατάστασης Συστημάτων θα πρέπει να εξασφαλίζεται ότι οι καταγραφές που προβλέπονται είναι πλήρεις και συνεχείς».

Επειδή, στο άρθρο 6.4.2.3. του ΚΔΑΗΕ ορίζονταν ότι : «6.4.2.3. Οι κωδικοί πρόσβασης θα πρέπει να αλλάζουν περιοδικά, σε συχνότητα που καθορίζεται ρητά ανά ΠΕΣ και αναφέρεται σε αρχείο που οφείλει να διατηρεί το υπόχρεο πρόσωπο. Το υπόχρεο πρόσωπο οφείλει να χρησιμοποιεί και να καταγράφει στο εν λόγω αρχείο τους τρόπους με τους οποίους

επιβάλλει την περιοδική αλλαγή των κωδικών πρόσβασης. Σε χαρακτηριστικές περιπτώσεις όπως είναι, ενδεικτικά, η αφαίρεση χρήστη ΠΕΣ ή η παραβίαση ενός λογαριασμού πρόσβασης, θα πρέπει να προβλέπεται η άμεση αλλαγή του αντίστοιχου κωδικού πρόσβασης.», στην παρ. 2.1.9 της Πολιτικής Ασφαλείας για την Διασφάλιση του Απορρήτου των Επικοινωνιών της προσφεύγουσας ότι : «2.1.9 Οι κωδικοί πρόσβασης θα πρέπει να αλλάζουν περιοδικά σε συχνότητα που καθορίζεται ρητά ανά σύστημα και αναφέρεται σε Αρχείο. Στο Αρχείο καταγράφονται οι τρόποι με τους οποίους επιβάλλεται η περιοδική αλλαγή των κωδικών πρόσβασης», στην παρ. 4.1 της Διαδικασίας «Διαχείριση & Τακτική Αλλαγή κωδικών πρόσβασης» της προσφεύγουσας ότι : « […] Σε περίπτωση που η αλλαγή του κωδικού πρόσβασης δεν είναι επιβεβλημένη, η αλλαγή του κωδικού πρόσβασης πραγματοποιείται με ευθύνη του χρήστη βάσει του Μ2.ERM.02.02.01 Εγχειριδίου Κανόνες Δημιουργίας Κωδικών Πρόσβασης», στο οποίο εγχειρίδιο προβλέπεται στην παράγραφο 4 ότι : « […] οι κωδικοί πρόσβασης των λογαριασμών που χρησιμοποιούνται από φυσικά πρόσωπα και έχουν δικαιώματα διαχειριστή ή πρόσβαση σε δεδομένα επικοινωνίας πρέπει να αλλάζουν κάθε 30 ημέρες […]».

Επειδή, στο άρθρο 6.2.1. του ΚΔΑΗΕ, όπως και στις παρ. 2.1.1. και 2.2.2. της Πολιτικής Λογικής Πρόσβασης/Πολιτική Ασφάλειας για την Διασφάλιση του Απορρήτου των Επικοινωνιών της προσφεύγουσας, ορίζονταν ότι : «6.2.1. Οι κωδικοί πρόσβασης θα πρέπει να αλλάζουν περιοδικά σε συχνότητα που καθορίζεται ρητά ανά σύστημα και αναφέρεται σε Αρχείο. Στο Αρχείο καταγράφονται οι τρόποι με τους οποίους επιβάλλεται η περιοδική αλλαγή των κωδικών πρόσβασης».

Επειδή, τέλος στο άρθρο 8.3.3.1. του ΚΔΑΗΕ ορίζονταν ότι : «8.3.3.1. Στις ελάχιστες απαιτήσεις της Διαδικασίας Ελέγχου Συντήρησης-Υποστήριξης-Λειτουργίας Υλικού και Λογισμικού των ΠΕΣ περιλαμβάνεται η παρακολούθηση της ορθής λειτουργίας των ΠΕΣ, μέσω του ελέγχου των συμβάντων και των συναγερμών κάθε συστήματος, ώστε να εντοπίζονται αμελλητί τυχόν σφάλματα ή κενά ασφάλειας», στο άρθρο 6.3.2.1. περ. γ΄ ότι : «6.3.2.1. Στη Διαδικασία Ελέγχου Ορθής Εφαρμογής της Πολιτικής Λογικής Πρόσβασης πρέπει να περιγράφονται με σαφήνεια οι περιοδικοί έλεγχοι που πραγματοποιούνται, σε συμφωνία με τις αρχές της Πολιτικής Ελέγχου Εφαρμογής της Πολιτικής Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών του άρθρου 11 του παρόντος Κανονισμού, αναφορικά με: […] (γ) Τον δειγματοληπτικό έλεγχο των αρχείων καταγραφής πρόσβασης (access logs) για την ανακάλυψη ενδεχομένων μη αιτιολογημένων προσβάσεων.», τα ανωτέρω δε προβλέπονται και στο άρθρο.4.1 της Πολιτικής Διαχείρισης και Εγκατάστασης Συστημάτων της προσφεύγουσας (Πολιτική Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών).

Επειδή, με τη διάταξη του άρθρου 19 παρ. 1 εδ. α΄ του Συντάγματος κατοχυρώνεται ως «απόλυτα απαραβίαστο», υπό την επιφύλαξη του δευτέρου εδαφίου της ίδιας παραγράφου, το δικαίωμα στην απόρρητη ελεύθερη επικοινωνία, ως ειδικότερη έκφανση των δικαιωμάτων της ελεύθερης ανάπτυξης της προσωπικότητας (άρθρο 5 παρ. 1 του Συντάγματος) και του απαραβίαστου της ιδιωτικής ζωής (άρθρο 9 παρ. 1 του Συντάγματος). Ειδικότερα, με τη διάταξη αυτή του Συντάγματος το απόρρητο της επικοινωνίας προστατεύεται έναντι πάντων (ιδιωτών ή φορέων δημόσιας εξουσίας), από κάθε είδους προσβολή και εκτείνεται στο σύνολο του επικοινωνιακού γεγονότος, καλύπτει, δηλαδή, όχι μόνο το περιεχόμενο της επικοινωνίας (φωνή, κείμενο, εικόνα, ήχο, ιστοσελίδα κλπ), αλλά και τα συναφώς παραγόμενα δεδομένα επικοινωνίας, που προσδιορίζουν τις συνθήκες επικοινωνίας και την εξατομικεύουν (όπως πληροφορίες για τον τόπο, το χρόνο, τη διάρκεια, τη μορφή και το είδος επικοινωνίας, στοιχεία προσδιοριστικά του μέσου με το οποίο διεξήχθη η επικοινωνία, στοιχεία ταυτότητας και διευθύνσεων επικοινωνούντων μερών αριθμοί τηλεφώνων καλούντος – καλούμενου κλπ [μεταδεδομένα της επικοινωνίας (βλ. ΣτΕ 1593/2016 σκ.9η με την εκεί παρατιθέμενη νομολογία του ΔΕΕ και του ΕΔΔΑ)].

Επειδή, εξάλλου στο άρθρο 5 παρ. 2 του Κώδικα Διοικητικής Δικονομίας (ν. 2717/1999, Α΄ 97, ΚΔΔ), όπως η παρ. αυτή αντικαταστάθηκε με το άρθρο 17 του ν. 4446/2016 και ισχύει από τη δημοσίευσή του στην Εφημερίδα της Κυβερνήσεως (άρθρο 129, Α΄ 240/22.12.2016), έχει δε πεδίο εφαρμογής ratione temporis στις υποθέσεις, οι οποίες συζητήθηκαν ενώπιον των διοικητικών δικαστηρίων μετά την 22.12.2016, όπως η προκείμενη, (βλ. ΣτΕ 635/2021, 951/2018 7μ.), ορίζεται ότι : «Τα δικαστήρια δεσμεύονται από τις αποφάσεις των πολιτικών δικαστηρίων, οι οποίες, σύμφωνα με τις κείμενες διατάξεις, ισχύουν έναντι όλων. Δεσμεύονται, επίσης, […] από τις αμετάκλητες αθωωτικές αποφάσεις, καθώς και από τα αμετάκλητα αποφαινόμενα να μην γίνει η κατηγορία βουλεύματα, εκτός εάν η απαλλαγή στηρίχθηκε στην έλλειψη αντικειμενικών ή υποκειμενικών στοιχείων που δεν αποτελούν προϋπόθεση της διοικητικής παράβασης». Στην

αιτιολογική έκθεση επί του σχεδίου του ν. 4446/2016, αναφέρεται σχετικά με τη θέσπιση του ανωτέρω άρθρου 17 ότι: «[...] τροποποιείται η παράγραφος 2 του άρθρου 5 του Κώδικα Διοικητικής Δικονομίας, προκειμένου η δέσμευση των διοικητικών δικαστηρίων από τις αμετάκλητες αποφάσεις των ποινικών δικαστηρίων να επεκταθεί πέραν από τις καταδικαστικές και στις αθωωτικές αποφάσεις, καθώς και στα αποφαινόμενα να μην γίνει η κατηγορία βουλεύματα που έχουν καταστεί αμετάκλητα [σχ. απόφαση ΕΔΔΑ της 13.7.2010, Σταυρόπουλος κατά Ελλάδας (βλ. ΣτΕ 803/2024 σκ. 5η)].

Επειδή, στην προκείμενη περίπτωση από τα στοιχεία της δικογραφίας προκύπτουν τα εξής: Η προσφεύγουσα με την ΑΔΑΕ ΕΜΠ 132/10.9.2020 Αναφορά Περιστατικού Ασφαλείας και το ΑΔΑΕ 2191/10.9.2020 συμπληρωματικό έγγραφό της, γνωστοποίησε στην ΑΔΑΕ ότι στις 8.9.2020 έγινε αντιληπτό μέσω συναγερμικής ειδοποίησης του συστήματος, ότι ο αποθηκευτικός χώρος ενός εξυπηρετητή (server) ξεπέρασε το όριο χωρητικότητας του και σε αυτόν κατόπιν έρευνας, διαπιστώθηκε η ύπαρξη ενός άγνωστου αρχείου, μεγέθους 30 GB περίπου (33.373.558.949 bytes) με ονομασία cd.gz, που περιείχε δεδομένα επικοινωνίας συνδρομητών, χρονικής περιόδου 1.9.-5.9.2020, καθώς και ότι διαπιστώθηκε πως στις 8.9.2020 από 10:34 πμ -11:54 πμ υπήρξε διαδικτυακή κίνηση δεδομένων ίδιου μεγέθους μεταξύ του εξυπηρετητή και εξωτερικής διαδικτυακής διεύθυνσης (IP) που ανήκει σε πάροχο διαδικτυακής φιλοξενίας υπολογιστικού νέφους (Hosting Provider- cloud) στην Λιθουανία (σχ. και το 71/ΕΜΠ155/9.9.2020 έγγραφο της προσφεύγουσας). Για τη διερεύνηση του εν λόγω περιστατικού, με την 227/2020 Απόφαση της Ολομέλειας της ΑΔΑΕ, αποφασίσθηκε η σύσταση ομάδας, προκειμένου να διενεργήσει σχετικό έλεγχο. Τα αποτελέσματα του ελέγχου αποτυπώθηκαν στην από 30.11.2021 «Έκθεση Διενέργειας Εκτάκτου Ελέγχου στην εταιρεία Cosmote ΚΙΝΗΤΕΣ ΤΗΛΕΠΙΚΟΙΝΩΝΙΕΣ Α.Ε. κατόπιν του υπ' αριθμ. πρωτ. ΑΔΑΕ ΕΜΠ 132/10.09.2020 περιστατικού ασφαλείας», εγκρίθηκαν με την 11/12.1.2022 Απόφασή της Ολομέλειας της Αρχής και γνωστοποιήθηκαν στην προσφεύγουσα με την με αρ. ΑΔΑΕ 139/17.1.2021 κλήση για ακρόαση. Συγκεκριμένα, κατά την ως άνω έκθεση ελέγχου, με βάση τα στοιχεία καταγραφής της προσφεύγουσας προέκυψε αρχικά ότι στις 8.9.2020 ο χρήστης XXXXXXXXX (υφιστάμενος λογαριασμός υπαλλήλου με δικαιώματα διαχειριστή της προσφεύγουσας) φέρονταν να συνδέθηκε στον εξυπηρετητή XXXXXXXXX μέσω του εξυπηρετητή XXXXXXXX, αλλά όταν ο τελευταίος ρωτήθηκε σχετικά, απάντησε αρνητικά. Περαιτέρω, από την ανάλυση των αρχείων καταγραφής προέκυψε ότι το αρχικό σημείο εισόδου του φερόμενου χρήστη ήταν ο χώρος φιλοξενίας ιστοσελίδων (Webhosting) της προσφεύγουσας. Εν συνεχεία, από την ανάλυση των αρχείων καταγραφής των εξυπηρετητών του webhosting διαπιστώθηκε πως στον φιλοξενούμενο ιστότοπο «oteplus.gr» είχε εγκατασταθεί λογισμικό, το οποίο χρησιμοποιείται από διαδικτυακούς πειρατές (hackers) με ημερομηνία δημιουργίας αρχείων 14.4.2020 (13:00), μέσω τεχνικής απομακρυσμένης εγκατάστασης –εκτέλεσης προγράμματος (Remote file inclusion- RFI). Λόγω ακριβώς της εγκατάστασης του ως άνω κακόβολου λογισμικού, ο επιτιθέμενος απέκτησε πρόσβαση σε εξυπηρετητή που ανήκει στην υποδομή XXXXXXXX της προσφεύγουσας και ως εκ τούτου είχε πρόσβαση σε δεδομένα πελατών της μέσω ενός εξυπηρετητή αντιγράφων ασφαλείας (Back Up server), που επικοινωνούσε με το εσωτερικό δίκτυο της προσφεύγουσας, οπότε ο ως άνω επιτιθέμενος απέκτησε διαδοχικά πρόσβαση στον εξυπηρετητή XXXXXXXXX και ακολούθως στον εξυπηρετητή XXXXXXXX και τελικά, αφού άντλησε τα δεδομένα αυτών, τα μετέφερε στο αρχείο cd.gz που ακολούθως απέστειλε στο υπολογιστικό νέφος του παρόχου που είχε την Λιθουανική IP (βλ. το σχήμα στην σελ. 18 της έκθεσης ελέγχου). Η δυνατότητα πρόσβασης στους εν λόγω εξυπηρετητές, μέσω του εξυπηρετητή αντιγράφων ασφαλείας προέκυψε, λόγω του ότι ο εξυπηρετητής αυτός ήταν ταυτόχρονα συνδεδεμένος σε περισσότερες δικτυακές ζώνες, ώστε να λαμβάνει αντίγραφα ασφαλείας από τους έτερους εξυπηρετητές που λειτουργούσαν στις ζώνες αυτές και ήταν παραμετροποιημένος κατά τρόπο, που να επιτρέπει την πρόσβαση με πρωτόκολλο SSH (Secure Shell - ασφαλές δικτυακό πρωτόκολλο επικοινωνίας μεταξύ υπολογιστών) και από την ζώνη της φιλοξενίας των ιστοσελίδων, οπότε ο εγκαταστήσας το κακόβουλο λογισμικό στην φιλοξενούμενη ιστοσελίδα, απέκτησε πρόσβαση, μέσω του λογαριασμού του ανωτέρω χρήστη στην ως άνω ιστοσελίδα, ώστε να συνδεθεί στον εξυπηρετητή των αντιγράφων ασφαλείας και εντεύθεν στους λοιπούς εξυπηρετητές (βλ. σελ. 17-18 της έκθεσης ελέγχου).

Επειδή, βάσει της ως άνω από 30.11.2021 έκθεσης ελέγχου για τα ανωτέρω συμβάντα, αποδόθηκαν στην προσφεύγουσα δυο παραβάσεις. Η πρώτη παράβαση συνίσταται στην διαρροή προσδιοριστικών στοιχείων της προσφεύγουσας ως εταιρείας και στοιχείων προσδιοριστικών του λογαριασμού πρόσβασης (όνομα χρήστη και κωδικός πρόσβασης/user name – password) υπαλλήλου της εταιρείας με δικαιώματα διαχειριστή (root) σε ΠΕΣ της προσφεύγουσας. Ειδικότερα, από όσα διαπιστώθηκαν κατά τον έλεγχο και από όσα δήλωσε η ίδια η προσφεύγουσα κατά την πρώτη αναφορά του περιστατικού, η Αρχή κατέληξε στο συμπέρασμα ότι τα δεδομένα κίνησης των συνδρομητών από τον εξυπηρετητή της

διέρρευσαν λόγω του ότι είχαν ήδη διαρρεύσει τα στοιχεία υπαλλήλου της – διαχειριστή σε ΠΕΣ από προηγούμενες επιθέσεις σε μέσα κοινωνικής δικτύωσης (LinkedIn, Facebook, κλπ.) και άλλες υπηρεσίες και ακολούθως είχαν συμπεριληφθεί σε βάσεις δεδομένων που διατηρούν διαδικτυακοί πειρατές με ονόματα χρηστών - κωδικούς πρόσβασης. Η εν λόγω τακτική της υποκλοπής κωδικών και εκ νέου χρήση τους ως μη ευχερώς εντοπίσιμη, αφού δεν δημιουργούσε ειδοποιήσεις ασφαλείας στις βάσεις δεδομένων που δέχονται την σχετική επίθεση, όπως λχ η προσπάθεια εντοπισμού κωδικού με τυχαίους χαρακτήρες, ήταν πρακτική που συνδεόταν με κυβερνοεγκληματίες. Τα στοιχεία του συγκεκριμένου υπαλλήλου της προσφεύγουσας εντοπίστηκαν κατόπιν ελέγχου σε τουλάχιστον μια τέτοια βάση. Στο πλαίσιο αυτό, ο επιτιθέμενος απέκτησε πρόσβαση με δικαιώματα διαχειριστή σε ΠΕΣ της προσφεύγουσας και στις 8.9.2020 δημιούργησε, όπως προκύπτει από τα στοιχεία που παρέδωσε η προσφεύγουσα στην ΑΔΑΕ, το αρχείο με τίτλο cd.gz μεγέθους περίπου 30GB, το οποίο, όπως προεκτέθηκε, μεταφέρθηκε και αποθηκεύτηκε την ίδια ημέρα σε υπολογιστικό νέφος λιθουανικού παρόχου. Το δε αρχείο cd.gz, σύμφωνα με όσα ανέφερε η προσφεύγουσα, περιείχε προσωπικά δεδομένα και δεδομένα κίνησης συνδρομητών κινητής τηλεφωνίας (εξαιρούμενων των κλήσεων VoLTE -VoWiFi) για το χρονικό διάστημα 1.9.2020 – 5.9.2020 ήτοι : α) τα δεδομένα κίνησης και τις συντεταγμένες σταθμών βάσης για 4.792.869 μοναδικούς συνδρομητές της προσφεύγουσας, β) τον διεθνή αριθμό σύνδεσης κινητής τηλεφωνίας/ αναγνώρισης καλούντος [Mobile Station International Subscriber Directory Number / Caller identification (MSISDN/CLI)] 6.939.656 χρηστών άλλων εγχώριων παρόχων σταθερής - κινητής τηλεφωνίας που κάλεσαν ή κλήθηκαν από συνδρομητές της προσφεύγουσας και γ) την διεθνή ταυτότητα εξοπλισμού κινητής τηλεφωνίας [International Mobile Equipment Identity (IMEI)], την διεθνή ταυτότητα συνδρομητή κινητής τηλεφωνίας [International Mobile Subsciber Identity (IMSI)] το MSISDN και συντεταγμένες σταθμών βάσης για 281.403 συνδρομητές περιαγωγής που πραγματοποίησαν κλήσεις μέσω του δικτύου κινητής τηλεφωνίας της προσφεύγουσας.

Επειδή, εκτός των προαναφερθέντων, οι ελέγχοντες υπάλληλοι διαπίστωσαν ότι η προσφεύγουσα υπέπεσε και σε δεύτερη παράβαση η οποία συνίσταται στην μη τήρηση των πολιτικών ασφαλείας για την διασφάλιση του απορρήτου των επικοινωνιών εκ μέρους της προσφεύγουσας και διαιρείται σε 6 επί μέρους παραβιάσεις – αποκλίσεις από τις πολιτικές ασφαλείας, όπως περιγράφονται στον ΚΔΑΗΕ και στις αντίστοιχες Πολιτικές Ασφάλειας της προσφεύγουσας για το απόρρητο των επικοινωνιών. Ειδικότερα, ως προς την τήρηση της πολιτικής ασφάλειας για τη διασφάλιση του απορρήτου των επικοινωνιών της προσφεύγουσας διαπιστώθηκε ότι κατά τον χρόνο που έλαβε χώρα η υποκλοπή των προαναφερθέντων στοιχείων, δεν υπήρχε μηχανισμός προστασίας που να εφαρμόζεται στον εξυπηρετητή αντιγράφων ασφαλείας, με αποτέλεσμα να υπάρχει δικτυακή πρόσβαση από την αποστρατικοποιημένη ζώνη (DMZ), στην οποία ήταν εγκατεστημένος ο εξυπηρετητής για την φιλοξενία ιστοσελίδων προς τις εσωτερικές ζώνες, μέσω του ως άνω εξυπηρετητή αντιγράφων ασφαλείας, κατά παράβαση όσων προβλέπονται στο άρθρο 10 παρ.1 του ΚΔΑΗΕ και στις παραγράφους 1 και 2.1.1 της Πολιτικής Ασφάλειας Δικτύου της προσφεύγουσας. Εξάλλου,όπως ανέφερε και η προσφεύγουσα κατά την γνωστοποίηση του περιστατικού,ο επιτιθέμενος από την αποστρατικοποιημένη ζώνη απέκτησε πρόσβαση στο εσωτερικό της δίκτυο, μέσω ενός εφεδρικού εξυπηρετητή, ο οποίος συνδέονταν με αυτό, στον εφεδρικό όμως εξυπηρετητή δεν υπήρχε η απαραίτητη λίστα ελέγχου πρόσβασης (access list), παρότι ήταν ταυτόχρονα συνδεδεμένος σε πολλές εσωτερικές δικτυακές ζώνες, εκτός της ζώνης φιλοξενίας ιστοσελίδων, ώστε να λαμβάνει αντίγραφα ασφαλείας από τους εξυπηρετητές στις ζώνες αυτές. Η παραμετροποίηση του εξυπηρετητή αντιγράφων ασφαλείας επέτρεπε την πρόσβαση με πρωτόκολλο SSH και από την ζώνη φιλοξενίας ιστοσελίδων, οπότε ο επιτιθέμενος ήταν σε θέση να χρησιμοποιεί τον παραβιασμένο λογαριασμό χρήστη για να συνδέεται στον εξυπηρετητή αυτόν και από εκεί στις εσωτερικές δικτυακές ζώνες. Και τούτο διότι η παραμετροποίηση του εφεδρικού εξυπηρετητή επέτρεπε την επικοινωνία του δικτύου φιλοξενίας ιστοσελίδων με το εσωτερικό δίκτυο (1η απόκλιση - Πολιτική Ασφάλειας Δικτύου). Περαιτέρω, κατά τον έλεγχο διαπιστώθηκε ότι κατά παράβαση του άρθρου 3 παρ. 3.3 του ΚΔΑΗΕ και των παρ. 5.2.4 και 5.2.5 της εγκριθείσας πολιτικής ασφαλείας της προσφεύγουσας, δεν είχε διενεργηθεί αξιολόγηση τρωτότητας (vulnerability assessment) στους εφεδρικούς εξυπηρετητές (2η απόκλιση- Πολιτική Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών). Πέραν των ανωτέρω, διαπιστώθηκε παράβαση του άρθρου 3 παρ. 3.2.9 του ΚΔΑΗΕ, σε συνδυασμό με την παράγραφο 5.1.7 της Πολιτικής Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών της προσφεύγουσας,καθώς η τελευταία δεν παρέδωσε κατά τον έλεγχο αρχεία καταγραφής του επίμαχου εξυπηρετητή XXXXXXXXX για τις ημερομηνίες 7 -8.7.2020, δηλώνοντας στο από 30.9.2020 πρακτικό ελέγχου ότι τα αρχεία καταγραφής μεταξύ 6.7.2020 και ώρα 13.00 και 9.7.2020 και ώρα 15:00 δεν έχουν διατηρηθεί, λόγω τεχνικού προβλήματος στο syslog εξυπηρετητή (εξυπηρετητής με αποθηκευμένα αρχεία καταγραφής εισόδων χρηστών σε έτερα μηχανήματα), ζήτημα μη

σχετιζόμενου με το περιστατικό, ενώ στο από 4.2.2021 πρακτικό ελέγχου αναφορικά με τις ημερομηνίες 6 -7.7.2020 η προσφεύγουσα δήλωσε ότι, ναι μεν υπήρχε δυνατότητα εγγραφής, αλλά με τέτοιο τρόπο που οδηγούσε σε διατήρηση των αρχείων μόνο για (3) ημέρες, με αποτέλεσμα να μην έχουν διατηρηθεί τα αρχεία των εν λόγω ημερομηνιών (3η απόκλιση - Πολιτική Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών). Κατά τον έλεγχο διαπιστώθηκε επίσης παράβαση του άρθρου 6 παρ. 6.4.2.3 του ΚΔΑΗΕ σε συνδυασμό με την παράγραφο 2.1.9 της Πολιτικής Λογικής Πρόσβασης της προσφεύγουσας και του άρθρου 4.1 «Διαχείριση & Τακτική Αλλαγή κωδικών πρόσβασης» και τούτο διότι κατά την εξέταση των αρχείων καταγραφής προσβάσεων και ενεργειών προέκυψε ότι έχει μεσολαβήσει διάστημα τουλάχιστον ενός έτους (από 19.7.2019 έως και 2.7.2020), στο οποίο δεν έχει πραγματοποιηθεί καμία αλλαγή κωδικού πρόσβασης στον εξυπηρετητή XXXXXXXXX του λογαριασμού του υπαλλήλου, δια του οποίου διενεργήθηκε η επίθεση. Συγκεκριμένα από την εξέταση του αρχείου διαμόρφωσης «XXXXXXXXX-login» για τον εν λόγω εξυπηρετητή, προέκυψε ότι, κατά τον χρόνο που έλαβε χώρα το κρίσιμο περιστατικό, δεν ήταν καθορισμένη η περιοδική αλλαγή του κωδικού πρόσβασης με τον ορισμό μέγιστου αριθμού ημερών για την αλλαγή του (PASS_MAX_DAYS 99999). Τούτο επιβεβαιώθηκε και από το αρχείο, στο οποίο έχει αποτυπωθεί η συχνότητα αλλαγής κωδικού πρόσβασης για κάθε εξυπηρετητή των ΠΕΣ συστημάτων που αναφέρονται στην Τελική Έκθεση Αναφοράς της προσφεύγουσας προς την ΑΔΑΕ και ο τρόπος επιβολής του, στο οποίο δεν υπήρχε καθορισμένη συχνότητα, ούτε και αλλαγή του κωδικού πρόσβασης από το σύστημα στους χρήστες. Εξάλλου, από την εξέταση του αρχείου με τους ελέγχους που διενήργησε η προσφεύγουσα κατά την διαδικασία αποτίμησης κινδύνων (άρθρο 2.2.6 της Πολιτικής Λογικής Πρόσβασης) για το σύστημα XXXXXXXXX, προέκυψε ότι η μη συμμόρφωση με την απαίτηση για περιοδική αλλαγή των κωδικών πρόσβασης (Password expiration must be enforced) είχε διαγνωστεί ήδη από τις αρχές του 2018 (ημερομηνία έκδοσης αρχείου 1.2018), αλλά ως χρόνος αναμενόμενης συμμόρφωσης είχε οριστεί το πρώτο τρίμηνο του 2021, ήτοι 3 και πλέον έτη από την αρχική διαπίστωση της μη συμμόρφωσης, και χωρίς μάλιστα να έχουν προταθεί κατάλληλα μέτρα για τη μείωση του προκαλούμενου κινδύνου. (4η απόκλιση-Πολιτική λογικής πρόσβασης). Εκτός των ανωτέρω αποκλίσεων, στο πλαίσιο του σχετικού ελέγχου διαπιστώθηκε ειδικά για τον εξυπηρετητή XXXXXXXXX παράβαση των διατάξεων του άρθρου 6 παρ. 6.4.2.3 του ΚΔΑΗΕ, του άρθρου 2.1.9 της Πολιτικής Λογικής Πρόσβασης της εταιρείας (Πολιτική Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών της εταιρείας,) και της παρ. 4.1 της Διαδικασίας «Διαχείριση και Τακτική Αλλαγή κωδικών πρόσβασης», όπως και του Εγχειριδίου Μ2.ERM.02.02.01 «Κανόνες Δημιουργίας Κωδικών Πρόσβασης.», της προσφεύγουσας, καθώς δεν υπήρχε καθορισμένη περιοδική αλλαγή του κωδικού πρόσβασης με τον ορισμό μέγιστου αριθμού ημερών για την αλλαγή του. Επίσης, στον εν λόγω εξυπηρετητή διαπιστώθηκε και έτερη παραβίαση ως προς την λειτουργία αυτού, ήτοι αντίθεση με τα οριζόμενα στο άρθρο 6 παρ. 6.2.1. του ΚΔΑΗΕ και στις παραγράφους 2.1.1. και 2.2.2. της Πολιτικής Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών της προσφεύγουσας, καθώς στο αρχείο διαμόρφωσης της υπηρεσίας sudo του XXXXXXXXX για την παροχή αυξημένων δικαιωμάτων (τύπου root) σε έναν ή περισσότερους χρήστες, εντοπίσθηκαν ενεργές οι εξής εντολές: «User_Alias SYSTEMS_STANDBY = XXXXXXXXX, XXXXXXXXX, XXXXXXXXX, XXXXXXXXX, XXXXXXXXX, XXXXXXXXX, XXXXXXXXX Cmnd_Alias SU_ROOT=/bin/su – SYSTEMS_STANDBY ALL=(root) NOPASSWD: SU_ROOT XXXXXXXXX server», που αντιστοιχούσαν σε επτά (7) λογαριασμούς χρηστών (μεταξύ των οποίων και ο λογαριασμός «XXXXXXXXX» που χρησιμοποίησε ο επιτιθέμενος), οι οποίοι είχαν τη δυνατότητα, αφού συνδεθούν στο σύστημα XXXXXXXXX, εκτελώντας την εντολή sudo, να συνδεθούν ως χρήστες «root», χωρίς τη χρήση κωδικού πρόσβασης για τη σύνδεση με αυτό τον λογαριασμό. Βάσει των πιο πάνω εντολών του αρχείου διαμόρφωσης της υπηρεσίας sudo και των εκτελεσμένων συστημικών εντολών, διαπιστώθηκε κατά τον έλεγχο ότι ο λογαριασμός «XXXXXXXXX», τον οποίο χρησιμοποίησε ο επιτιθέμενος, με τη χρήση του κωδικού πρόσβασής του, συνδεόταν στο σύστημα και ακολούθως, εκτελώντας την εντολή sudo και χωρίς τη χρήση του κωδικού πρόσβασης του λογαριασμού root, αποκτούσε πλήρη δικαιώματα βάσει του λογαριασμού root και εκτελούσε εντολές, γεγονός που συνιστούσε παράβαση της πολιτικής λογικής πρόσβασης. Τέλος, πέραν των ανωτέρω αποκλίσεων διαπιστώθηκε και αντίθεση στα άρθρα 8 παρ. 8.3.3.1. και 6 παρ. 6.3.2.1.γ του ΚΔΑΗΕ και στην παράγραφο 2.4.1 της Πολιτικής Διαχείρισης και Εγκατάστασης Συστημάτων της εταιρείας. Και τούτο διότι κατά τον χρόνο που έλαβε χώρα το επίμαχο συμβάν, καταγράφηκαν στη βάση δεδομένων της εταιρείας (hadoop) εντολές αναζήτησης των δεδομένων επικοινωνίας των χρηστών και συνδρομητών που δεν ήταν ούτε προγραμματισμένες, ούτε εντάσσονταν στις συνήθεις εργασίες, με τις οποίες είναι επιφορτισμένος ένας διαχειριστής λειτουργικών συστημάτων, όπως προέκυψε από ανάλυση - ανάσυρση αιτημάτων (queries στη βάση δεδομένων). Επομένως, παρά την μη κανονική υποβολή αιτημάτων, μετά από έλεγχο συμβάντων και συναγερμών, από τα όργανα της προσφεύγουσας, δεν ανέκυπτε κενό ασφάλειας, γεγονός που συνιστούσε παράβαση της Πολιτικής Διαχείρισης και Εγκατάστασης Λογισμικού. (6η απόκλιση)

Επειδή, κατόπιν των ανωτέρω διαπιστώσεων, η ΑΔΑΕ με την 11/2022 απόφασή της εκτίμησε ότι οι προαναφερθείσες ελλείψεις συνιστούν παράβαση της κείμενης νομοθεσίας περί απορρήτου των επικοινωνιών και κάλεσε σε ακρόαση την προσφεύγουσα (σχ. η ΑΔΑΕ 139/17.1.2022 κλήση), η οποία υπέβαλε σχετικώς το ΑΔΑΕ ΕΜΠ 75/21.02.2022 υπόμνημά της. Με αυτό, η προσφεύγουσα δεν αμφισβήτησε τα πραγματικά περιστατικά, όπως αναφέρθηκαν στην έκθεση ελέγχου, διευκρίνισε όμως ότι στο αρχείο με όνομα cd.gz, το οποίο εξήχθη από σύστημα της δεν περιλαμβάνονταν περιεχόμενο κλήσεων (συνομιλίες) ή μηνυμάτων, ονοματεπώνυμα ή διευθύνσεις, κωδικοί πρόσβασης ή δεδομένα πιστωτικών καρτών ή τραπεζικών λογαριασμών. Περαιτέρω, προέβαλε ότι το επίμαχο περιστατικό αναγόταν στις εγγενείς αδυναμίες του ελέγχου ταυτότητας μονού παράγοντα με κωδικό πρόσβασης (password-based single factor authentication) σε όλα τα συστήματα ελέγχου ταυτότητας αυτού του τύπου και δεν σχετιζόταν με ανεπαρκή παραμετροποίηση των πολιτικών κωδικών πρόσβασης. Κατά την άποψη δηλαδή της προσφεύγουσας, οι αδυναμίες δεν θα μπορούσαν να αντιμετωπιστούν με τις ρυθμίσεις πολυπλοκότητας κωδικών ή διάρκειας κωδικών (password complexity/expiration), που ήταν παραμετροποιημένες στους εξυπηρετητές. Για την αντιμετώπιση των αδυναμιών αυτών, η προσφεύγουσα ανέφερε ότι είχε ήδη προμηθευτεί το σύστημα Διαχείρισης Προνομιακών Προσβάσεων (PAM – Privileged Access Management) XXXXXXXX, το οποίο ήταν σε παραγωγική λειτουργία από τον Ιούλιο του 2020, ενώ η διασύνδεση των εξυπηρετητών με το σύστημα PAM ήταν προγραμματισμένη να ολοκληρωθεί τον Οκτώβριο του 2020. Περαιτέρω η προσφεύγουσα προέβαλε ότι το περιστατικό οφειλόταν και στη δικτυακή παραμετροποίηση του εξυπηρετητή αντιγράφων ασφαλείας, ο οποίος ήταν ταυτόχρονα συνδεδεμένος με το δίκτυο φιλοξενίας ιστοσελίδων και το εσωτερικό δίκτυο. Παράλληλα η προσφεύγουσα τόνισε την άμεση αντίδρασή της κατόπιν του περιστατικού και τις κατά νόμο ενέργειές της για τη γνωστοποίησή του στις αρμόδιες αρχές και τα θιγόμενα πρόσωπα, την ενημέρωση του αρμόδιου Εισαγγελέα, και την κατάθεση μηνυτήριας αναφοράς κατ' αγνώστων. Ακολούθως, η προσφεύγουσα ανέφερε τις διορθωτικές ενέργειες στις οποίες προέβη για να διακοπεί η περαιτέρω πρόσβαση του επιτιθέμενου στα συστήματα, αλλά και για να αποτραπούν παρόμοια περιστατικά στο μέλλον, ιδίως με την υλοποίηση του συστήματος Διαχείρισης Προνομιακών Προσβάσεων XXXXXXXXX και του ελέγχου ταυτότητας δύο παραγόντων (2FA– two-factor authentication), την υλοποίηση νέας ανεξάρτητης υποδομής αντιγράφων ασφαλείας για τη φιλοξενία ιστοσελίδων και την παραμετροποίηση των εξυπηρετητών, ώστε να μην είναι δυνατή η σύνδεση σε αυτούς με πρωτόκολλο SSH από τους ιστοχώρους που φιλοξενούν, την υλοποίηση μηχανισμών βασισμένων σε Τεχνητή Νοημοσύνη/ Μηχανική εκμάθηση [TN/ME Artificial Intelligence /Machine learning (AI/ML)] για τον εντοπισμό ύποπτων ερωτημάτων σε βάσεις δεδομένων (σύστημα XXXXXXXX), την ενεργοποίηση διαδικασίας προληπτικής αλλαγής σε όλα τα ιδιωτικά κλειδιά (private keys) και τους κωδικούς πρόσβασης υπηρεσιακών λογαριασμών (service accounts) και την ολοκλήρωση πλήρους επανεγκατάστασης λογισμικού (από ασφαλή αντίγραφα) σε εξυπηρετητές, στους οποίους κρίθηκε απαραίτητο για προληπτικούς λόγους. Συναφώς, η προσφεύγουσα ανέφερε ότι οι κωδικοί πρόσβασης του υπαλλήλου της διέρρευσαν από μέσο κοινωνικής δικτύωσης και περιλαμβάνονταν σε λίστα διαδικτυακών πειρατών στον παγκόσμιο ιστό και επομένως πρόκειται για τυχαίο περιστατικό που δεν θα μπορούσε να αποτρέψει, καθώς δεν εμπίπτει στην σφαίρα επιρροής της, αλλά συνιστά εγκληματική ενέργεια τρίτου προσώπου, για το οποίο η ίδια δεν υπέχει ευθύνη. Επιπροσθέτως, η προσφεύγουσα υποστήριξε ότι η ελεγχόμενη παρατυπία δεν ήταν ευρείας κλίμακας διότι : α) δεν υπήρχε απολύτως καμία ένδειξη ότι τα δεδομένα που μεταφέρθηκαν στο νέφος είχαν ήδη χρησιμοποιηθεί ή δημοσιευθεί οπουδήποτε και β) δεν υπήρχε κανένα στοιχείο ή επιβεβαίωση ότι ο επιτιθέμενος κατάφερε να ανοίξει επιτυχώς το αρχείο που μετέφερε, καθώς ακόμη και μια μικρή έστω αλλοίωση (corruption) σε συμπιεσμένο αρχείο δεδομένων, μπορεί να καταστήσει το αρχείο ως συνολικά μη αναγνώσιμο. Επί των επιμέρους αποδιδόμενων αποκλίσεων από την Πολιτική της, η προσφεύγουσα με το ίδιο υπόμνημα υποστήριξε ειδικότερα ότι (α) : [Απόκλιση 1], η εν λόγω έλλειψη αντιμετωπίστηκε άμεσα με διόρθωση της σχετικής παραμετροποίησης και καλύφθηκε οριστικά μέσω της υλοποίησης νέας ανεξάρτητης υποδομής αντιγράφων ασφαλείας για την φιλοξενία ιστοσελίδων, (β) [Απόκλιση 2] διαμορφώθηκε η από Ιανουαρίου 2021 Μελέτη Εκτίμησης Αντίκτυπου την οποία προσκόμισε σε ψηφιακό δίσκο (CD) στην ΑΔΑΕ, (γ) [Απόκλιση 3] κατά την διάρκεια των επιτόπιων ελέγχων (σχ. τα από 30.10.2020, και 4.2.2021 πρακτικά επιτόπιου ελέγχου), προέκυψε ότι η έλλειψη αρχείων καταγραφής του εξυπηρετητή XXXXXXXXX κατά τις ημερομηνίες 6 και 7.7.2020 οφειλόταν σε προϋπάρχον του περιστατικού τεχνικό πρόβλημα στο syslog εξυπηρετητή, που είχε ήδη διορθωθεί από 9.7.2020, ενώ υπήρχε κατάλογος των αρχείων καταγραφής, τα οποία όμως δεν μεταφέρονταν σωστά στο syslog εξυπηρετητή, λόγω του προαναφερόμενου τεχνικού προβλήματος, με αποτέλεσμα να πραγματοποιείται επανεγγραφή αυτών (overwrite) και τελικά να διατηρούνται για χρονικό διάστημα τριών (3) ημερών και παρότι η προσφεύγουσα είχε λάβει όλα τα απαραίτητα μέτρα, τεχνικά και

διαδικαστικά, για τη συνεχή συλλογή και αποθήκευση των αρχείων καταγραφής με ασφαλή τρόπο, δεν υπήρχε κανένα απολύτως σύστημα που να ήταν σε απόλυτα βαθμό θωρακισμένο έναντι τεχνικών αστοχιών και προβλημάτων, και ότι η εν λόγω αποδιδόμενη απόκλιση αποτελούσε προσωρινό τεχνικό πρόβλημα και δεν οφειλόταν σε υπαιτιότητα της, ώστε να συνιστά παραβίαση του άρθρου 3 παρ. 3.2.9 του Κανονισμού, (δ) [Απόκλιση 4] κατά την ημερομηνία εκδήλωσης του περιστατικού, η επιχείρηση συμμορφωνόταν πλήρως με την απαίτηση του Κανονισμού περί περιοδικής αλλαγής των κωδικών πρόσβασης, ορίζοντας στο σχετικό Εγχειρίδιο Μ2.ERM.02.02.01 πως, σε περίπτωση που η αλλαγή του κωδικού δεν είναι επιβεβλημένη από το ίδιο το σύστημα, αυτή πραγματοποιείται με ευθύνη του χρήστη, ενώ για να θωρακίσει ακόμη περισσότερο τους κωδικούς πρόσβασης, ήδη από το 2019 είχε ξεκινήσει διαδικασία προμήθειας και εφαρμογής του συστήματος PAM, η οποία ολοκληρώθηκε το 2020. Στο πλαίσιο αυτό, σύμφωνα με την προσφεύγουσα, διασυνδέθηκαν όλοι οι εξυπηρετητές της Δ/νσης Πληροφορικής με το PAM, αφαιρέθηκαν από τους εξυπηρετητές οι προσωποποιημένοι λογαριασμοί πρόσβασης των διαχειριστών της υποδομής, διακόπηκε η απευθείας δικτυακή πρόσβαση από τα δίκτυα των διαχειριστών προς τους εξυπηρετητές και υλοποιήθηκαν μηχανισμοί βασισμένοι σε μηχανισμούς TN/ME (AI/ML) για τον εντοπισμό ύποπτων ενεργειών από λογαριασμούς διαχειριστών, (ε) [Απόκλιση 5] για τη χρήση του λογαριασμού χρήστη root από οποιονδήποτε από τους εξουσιοδοτημένους χρήστες/φυσικά πρόσωπα, θα έπρεπε υποχρεωτικά να έχει γίνει πρώτα σύνδεση στο σύστημα με προσωποποιημένο λογαριασμό χρήστη και τον αντίστοιχο κωδικό εισόδου και, κατά συνέπεια, δεν ήταν εφικτή η εκτέλεση εντολών από τον συστημικό χρήστη root, χωρίς προηγουμένως να έχει εισαχθεί στο σύστημα ο κωδικός πρόσβασης του πραγματικού χρήστη/φυσικού προσώπου σε συμμόρφωση με όσα ορίζονται στο άρθρο 6 παρ. 6.2.1 του Κανονισμού. Σύμφωνα δε, με την προσφεύγουσα, ο έλεγχος πρόσβασης και αυθεντικοποίησης επιτυγχάνεται με τη χρήση ενός λογαριασμού πρόσβασης που αποτελείται από ένα ζεύγος ονόματος χρήστη και κωδικού πρόσβασης, ή άλλου μηχανισμού που εξασφαλίζει αντίστοιχο επίπεδο ασφάλειας, και η διαμόρφωση αυτή αποτελεί την συνήθη και βέλτιστη πρακτική που χρησιμοποιείται (best practice) και αντιμετωπίζει αποτελεσματικά και με ασφαλή τρόπο την τεχνική ιδιαιτερότητα όλων των συστημάτων UNIX να απαιτούν συγκεκριμένες εντολές να εκτελούνται αποκλειστικά μέσω του συστημικού λογαριασμού χρήστη root. Τέλος, ως προς την εν λόγω απόκλιση η προσφεύγουσα ανέφερε την υλοποίηση του συστήματος PAM, μέσω του οποίου δεν υπήρχαν πλέον προσωποποιημένοι λογαριασμοί (accounts), ο κωδικός πρόσβασης του χρήστη root άλλαζε συνεχώς αυτόματα από το σύστημα PAM και για την εκτέλεση εντολών ως root χρειαζόταν ταυτοποίηση δύο παραγόντων από τους φυσικούς διαχειριστές και (στ) [Απόκλιση 6] όλα τα συστήματα SIEM (Security Information - Event Management) στα οποία ανήκε και το XXXXXXXXX ESM, επεξεργάζονται συμβάντα ασφάλειας, τα οποία παράγονται από παραβίαση συγκεκριμένων κανόνων ασφάλειας που έχουν οριστεί, και τα μετατρέπουν σε συναγερμικές ειδοποιήσεις, όταν υπάρχουν ενδείξεις παραβίασης, ενώ η εκτέλεση εντολών σε βάσεις δεδομένων ή σε λειτουργικά συστήματα, από εξουσιοδοτημένους λογαριασμούς χρηστών, δεν παράγουν εν γένει συναγερμικές ειδοποιήσεις, δεδομένου ότι δεν αποτελούν παραβίαση συγκεκριμένου κανόνα ασφάλειας. Συναφώς δε, οι ενέργειες του επιτιθέμενου, και ιδίως οι εντολές αναζήτησης και ανάσυρσης (queries) στη βάση δεδομένων, αποτελούσαν διαχειριστικές ενέργειες, οι οποίες εντάσσονταν πλήρως στις συνήθεις ενέργειες που εκτελεί ένας εξουσιοδοτημένος διαχειριστής στο πλαίσιο της εργασίας του και, υπό την έννοια αυτή, ορθώς δεν σηματοδοτούσαν παραβίαση κανόνων ασφάλειας και αντίστοιχα δεν μετατρέπονταν σε συναγερμικές ειδοποιήσεις. Αντίθετη δε παραμετροποίηση, θα καθιστούσε αδύνατη την καθημερινή εργασία των διαχειριστών, δεδομένου ότι κάθε εντολή αναζήτησης που θα επιχειρούσαν να εκτελέσουν θα παρήγαγε συναγερμικές ειδοποιήσεις, θα εκκινούσε διαδικασία διερεύνησης πιθανού περιστατικού ασφάλειας και θα καθιστούσε έτσι αδύνατη την εκτέλεση συνήθων εργασιών, όπως πχ η βλαβοδιαχείριση. Τέλος, πέραν των ανωτέρω, η προσφεύγουσα προέβαλε ότι κατά την επιμέτρηση της τυχόν επιβλητέας διοικητικής ποινής, η Αρχή όφειλε να λάβει υπόψη τις αρχές της αναλογικότητας και της επιείκειας, και ιδίως το γεγονός ότι της είχε ήδη επιβληθεί διοικητικό πρόστιμο ύψους 6.000.000,00 ευρώ για τα ίδια υπό κρίση πραγματικά περιστατικά από την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ) με την 4/2022 απόφασή της. Ισχυρίσθηκε δε, η προσφεύγουσα ότι τυχόν επιβολή δεύτερης κύρωσης από την ΑΔΑΕ για τα ίδια πραγματικά περιστατικά αποτελεί παραβίαση της αρχής ne bis in idem,. Τέλος, η προσφεύγουσα δήλωσε ότι κοινοποίησε στην ΑΔΑΕ το υπό κρίση περιστατικό, συμμορφούμενη πλήρως με το ισχύον νομοθετικό πλαίσιο, επεσήμανε δε, ότι τα στελέχη της εταιρείας συνεργάστηκαν πλήρως με την Ομάδα Ελέγχου της ΑΔΑΕ κατά τη διάρκεια των επιτόπιων ελέγχων και επέδειξαν θετική ανταπόκριση και τέλος ότι κατά του διενεργήσαντος υπαιτίου την διαδικτυακή επίθεση, η ίδια κατέθεσε την από 16.10.2020 μηνυτήρια αναφορά (4843/ΑΒΜ Ε 2020).

Επειδή, οι προαναφερόμενοι ισχυρισμοί της προσφεύγουσας θεωρήθηκαν στο σύνολό τους ως αβάσιμοι. Ειδικότερα, ως

προς την Απόκλιση 3, η Αρχή εκτίμησε ότι η μη διατήρηση αρχείων καταγραφής για τις ημερομηνίες 6 και 7.7.2020 χρονικά συμπίπτει με το χρονικό διάστημα που εκδηλώθηκε το περιστατικό ασφάλειας και συνεπώς, σχετίζεται με αυτό. Και τούτο διότι σύμφωνα και με την τεχνική αναφορά της προσφεύγουσας «Αναλύοντας τα αρχεία καταγραφής πρωτοκόλλου http από τους εξυπηρετητές της υποδομής Webhosting, εντοπίστηκε ότι στον εξυπηρετητή pvserver01 και ειδικότερα στον φάκελο του ιστοχώρου www.oteplus.gr, είχε εγκατασταθεί εργαλείο λογισμικού που χρησιμοποιείται από χάκερς, με ημερομηνία δημιουργίας των αρχείων την 14/4/2020 ≈13:00.», ενώ τα πρώτα ερωτήματα προς τη βάση δεδομένων του XXXXXXXXX εντοπίσθηκαν από την προσφεύγουσα από τις 7.7.2020, δηλαδή εντός του χρονικού διαστήματος που παρουσιάστηκε η κρίσιμη μη διατήρηση των αρχείων καταγραφής. Ο δε ισχυρισμός της προσφεύγουσας ότι είχε λάβει όλα τα απαραίτητα μέτρα για τη συνεχή συλλογή και αποθήκευση των αρχείων καταγραφής με ασφαλή τρόπο, αλλά ότι δεν υπάρχει κανένα απολύτως σύστημα που να είναι σε υπέρτατο βαθμό θωρακισμένο έναντι τεχνικών αστοχιών και προβλημάτων και ότι επρόκειτο για προσωρινό τεχνικό πρόβλημα που δεν οφείλεται σε υπαιτιότητά της απορρίφθηκε ως αόριστος και ατεκμηρίωτος από την ΑΔΑΕ,με την αιτιολογία ότι δεν επικαλέστηκε συγκεκριμένα στοιχεία από τα οποία να προκύπτει ότι δεν ήταν εφικτή εν προκειμένω η εφαρμογή πιο αποτελεσματικών μέτρων αναφορικά με την τήρηση των εν λόγω αρχείων καταγραφής με όρους ακεραιότητας, εμπιστευτικότητας και διαθεσιμότητας, σύμφωνα με τα προβλεπόμενα στην παράγραφο 5.1.7 της Πολιτικής Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών και στο άρθρο 3 παρ. 3.2.9 του ΚΔΑΗΕ. Η ΑΔΑΕ δέχθηκε ότι τα μέτρα ασφάλειας που επιβάλλονται εν προκειμένω από τις προαναφερόμενες διατάξεις, συνιστούν προεχόντως προληπτικά μέτρα, των οποίων η εφαρμογή στα συστήματα των παρόχων διασφαλίζει, όσο το δυνατόν πιο αποτελεσματικά, το απόρρητο των επικοινωνιών των συνδρομητών και χρηστών των υπηρεσιών τους, με συνέπεια η μη εφαρμογή τους να θέτει σε συνεχή κίνδυνο την προστασία του απορρήτου των επικοινωνιών τους.

Επειδή, περαιτέρω ως προς την Απόκλιση 5, η Αρχή δέχθηκε ότι η προηγούμενη σύνδεση στο σύστημα με προσωποποιημένο λογαριασμό χρήστη και κωδικό εισόδου δεν αναιρούσε την προβλεπόμενη στο άρθρο 6 παρ. 6.2.1 του ΚΔΑΗΕ υποχρέωση να υπάρχει αντίστοιχος μηχανισμός ελέγχου πρόσβασης και αυθεντικοποίησης και για την πρόσβαση στον λογαριασμό «root» με χρήση της εντολής sudo, δεδομένου ότι, κατά τον χρόνο που έλαβε χώρα το επίμαχο περιστατικό, υφίστατο η δυνατότητα και για τους επτά (7) λογαριασμούς χρηστών (μεταξύ αυτών και ο λογαριασμός που χρησιμοποίησε ο επιτιθέμενος), εκτελώντας την εντολή sudo, να συνδεθούν ως χρήστες «root» με πλήρη δικαιώματα, χωρίς δηλαδή κανέναν περιορισμό ανά χρήστη (user), τερματική συσκευή (hostname) και εντολή (command), αλλά με τη δυνατότητα, για όλους αδιακρίτως, και χωρίς χρήση αντίστοιχου επιπρόσθετου κωδικού, να εκτελούν το σύνολο των διαχειριστικών εργασιών και εντολών στο σύστημα. Εξάλλου, για την αντιμετώπιση του ανωτέρω προβλήματος υλοποιήθηκε από την προσφεύγουσα και το σύστημα PAM, μετά το περιστατικό, ώστε να μην υφίστανται πλέον προσωποποιημένοι λογαριασμού (accounts) στα συστήματα, ο κωδικός πρόσβασης του χρήστη root να αλλάζει συνεχώς αυτόματα από το σύστημα αυτό και για την εκτέλεση εντολών root να απαιτείται ταυτοποίηση δύο παραγόντων από τους φυσικούς διαχειριστές.

Επειδή, περαιτέρω, ως προς την Απόκλιση 6, η Αρχή δέχθηκε ότι οι κρίσιμες εντολές,περί των οποίων αποδίδεται στην εταιρεία απόκλιση, δεν αποτελούσαν προγραμματισμένες εντολές αναζήτησης, ούτε εντάσσονταν στις συνήθεις εργασίες με τις οποίες είναι επιφορτισμένος ένας διαχειριστής λειτουργικών συστημάτων γιατί, κατά τη τεχνική κρίση της ΑΔΑΕ, ένας διαχειριστής λειτουργικών συστημάτων είναι υπεύθυνος για τη συντήρηση, τη διαμόρφωση και την αξιόπιστη λειτουργία των λειτουργικών συστημάτων των εξυπηρετητών, και όχι για τη σύνδεση σε βάσεις δεδομένων. Πολλώ δε μάλλον που και η ίδια η προσφεύγουσα αποδέχτηκε ότι υφίστανται μέτρα που επιτρέπουν την υλοποίηση των παραπάνω απαιτήσεων της Πολιτικής της εταιρείας και του ΚΔΑΗΕ, χωρίς να προκαλείται αδυναμία άσκησης της καθημερινής εργασίας των διαχειριστών, λόγω παραγωγής μεγάλου όγκου συναγερμών. Εξάλλου, μεταξύ των διορθωτικών ενεργειών που ελήφθησαν για την αποτροπή παρόμοιων περιστατικών στο μέλλον, από την προσφεύγουσα εγκαταστάθηκαν μηχανισμοί βασισμένοι σε TN/ME για τον εντοπισμό ύποπτων ερωτημάτων σε βάσεις δεδομένων (σύστημα XXXXXXXX).

Επειδή, κατόπιν αυτών, η Ολομέλεια της ΑΔΑΕ με την 225/30.5.2022 απόφαση θεώρησε ότι η προσφεύγουσα υπέπεσε στην παράβαση: α) της διαρροής στοιχείων προσδιοριστικών της εταιρείας και του λογαριασμού πρόσβασης (όνομα χρήστη- κωδικός πρόσβασης) υπαλλήλου της διαχειριστή ΠΕΣ και β) της μη ορθής εφαρμογής του ΚΔΑΗΕ της ΑΔΑΕ και

της Πολιτικής Ασφαλείας για την Διασφάλιση του Απορρήτου των Επικοινωνιών της, λόγω των ως άνω περιγραφέντων 6 αποκλίσεων, κατά παράβαση των οριζόμενων στα άρθρα 2 και 3 του ν. 3674/2008, με περαιτέρω συνέπεια να διαρρεύσουν τα μεταδεδομένα της επικοινωνίας των χρηστών της που προστατεύονται επίσης από το απόρρητο των επικοινωνιών, κατ' άρθρα 2 και 4 του ν. 3471/2006. Εν συνεχεία, η ΑΔΑΕ, αφού έλαβε υπόψη την αρχή της αναλογικότητας, τα πρόσφατα οικονομικά στοιχεία της εταιρείας (1.1.-31.12.2021), καθώς και την βαρύτητα των παραβάσεων επέβαλε στην προσφεύγουσα πρόστιμο : α) για την πρώτη παράβαση 200.000,00 ευρώ και β) για τη δεύτερη 3.000.000,00 ευρώ και τελικώς εν συνόλω 3.200.000,00 ευρώ.

Επειδή, με την κρινόμενη προσφυγή και τους με αρ. καταχ ΠΛ 163/25.9.2024 πρόσθετους λόγους, όπως αναπτύσσονται με το με αρ. καταχ. ΥΠ 23147/21.10.2024 νομίμως κατατεθέν υπόμνημα, η προσφεύγουσα επιδιώκει την ακύρωση, άλλως την τροποποίηση της προσβαλλόμενης 225/30.5.2022 απόφασης της Ολομέλειας της ΑΔΑΕ, ως μη νόμιμης και ουσιαστικά εσφαλμένης. Ειδικότερα, η προσφεύγουσα υποστηρίζει ότι κατά παράβαση της αρχής ne bis in idem της επιβλήθηκε το σχετικό πρόστιμο διότι από την ΑΠΔΠΧ της επιβλήθηκε ήδη πρόστιμο ύψους 6.000.000,00 ευρώ για τα ίδια πραγματικά περιστατικά. Ο εν λόγω ισχυρισμός, όμως βαίνει απορριπτέος ως νόμω αβάσιμος. Και τούτο διότι εν προκειμένω είναι δυνατή η επιβολή στον ίδιο παραβάτη για τα ίδια πραγματικά περιστατικά δύο διοικητικών κυρώσεων από διαφορετικά διοικητικά όργανα ή ανεξάρτητες διοικητικές αρχές, εφόσον η επιβολή τους αποβλέπει στην προστασία διαφορετικών εννόμων αγαθών ιδιαιτέρως σημαντικών, όπως εν προκειμένω είναι το κατοχυρωμένο με ρητή συνταγματική διάταξη, αλλά και διεθνή κείμενα (βλ. άρθρο 8 της ΕΣΔΑ ήδη πδ 76/2022 –Α΄205) ατομικό δικαίωμα του απορρήτου της επικοινωνίας (άρθρο 19 του Συντάγματος) που είναι διάφορο από την προστασία των προσωπικών δεδομένων (άρθρο 9Α του Συντάγματος). Το δε έργο της ΑΔΑΕ είναι αυτοτελές και ανεξάρτητο από τις αρμοδιότητες και ενέργειες άλλων αρχών. Εξάλλου, αντίθετη ερμηνεία θα καθιστούσε ανενεργή την υποχρέωση που έχουν από το Σύνταγμα διαφορετικά κρατικά όργανα να προστατεύουν τους θιγομένους στα ατομικά τους δικαιώματα (ΣτΕ 433/2021 σκ. 10η,1454/2020 σκ. 15η, 1972/2019 σκ. 10η 3473/2017 σκ. 11η -12η).

Επειδή, με τους πρόσθετους λόγους η προσφεύγουσα προβάλλει ειδικότερα ότι μετά την έκδοση της προσβαλλόμενης απόφασης επιβολής προστίμου, κατατέθηκε μήνυση τρίτου προσώπου (ΓΦ του Ι) κατά των υπευθύνων της, η οποία τέθηκε στο αρχείο, κατ' άρθρο 43 του Κώδικα Ποινικής Δικονομίας, ήτοι χωρίς να ασκηθεί ποινική δίωξη κατά του νομίμου εκπροσώπου της, ή άλλων μελών της (σχ. η 1917/2023 Διάταξη του Εισαγγελέα Πρωτοδικών Αθηνών και η 23-5928/5.7.2023 πράξη έγκρισης του Εισαγγελέα Εφετών Αθηνών). Ενόψει αυτών η προσφεύγουσα υποστηρίζει ότι κατ' εφαρμογή του άρθρου 5 παρ. 2 του ΚΔΔ, όπως ισχύει μετά την τροποποίησή του με το άρθρο 17 του ν. 4446/2016 (Α΄240), το Δικαστήριο τούτο, βάσει του τεκμηρίου αθωότητας οφείλει δεσμευόμενο από την ως άνω πράξη θέσεως της μηνύσεως στο αρχείο να ακυρώσει την προσβαλλόμενη απόφαση επιβολής προστίμου. Ο λόγος αυτός της προσφυγής κρίνεται απορριπτέος ως αβάσιμος, για το λόγο ότι η αμετάκλητη περάτωση της ποινικής διαδικασίας για φερόμενο ποινικό αδίκημα εκ μέρους φυσικών προσώπων, ως νομίμων εκπροσώπων ανώνυμης εταιρείας, δεν θεμελιώνει ίδιο δικαίωμα, ούτε άμεσο έννομο συμφέρον στην ανώνυμη εταιρεία, όπως στην προκείμενη περίπτωση στην προσφεύγουσα, να προβάλλει παραβίαση του τεκμηρίου αθωότητας ή και της αρχής ne bis in idem, καθόσον δεν υπάρχει ταυτότητα του φυσικού ή των φυσικών προσώπων κατά των οποίων ασκήθηκε μήνυση, παύθηκε η δίωξη ή περατώθηκε η ποινική διαδικασία με την θέση της υπόθεσης στο αρχείο και του νομικού προσώπου, στο οποίο επιβλήθηκε το διοικητικό πρόστιμο (πρβλ ΣτΕ 1242/2024 σκ.8η και ΕΔΔΑ Απόφαση της 11.1.2007 Μαμιδάκης κατά Ελλάδος, σκέψη 33η / αρ. προσφυγής 35533/2004).

Επειδή, περαιτέρω η προσφεύγουσα προβάλλει ότι η επιβολή σε αυτήν δύο προστίμων συνολικού ύψους 3.200.000,00 ευρώ, σε χρόνο κατά τον οποίο της είχε ήδη επιβληθεί και πρόστιμο ύψους 6.000.000,00 ευρώ από την ΑΠΔΠΧ δυνάμει της 4/2022 απόφασης της τελευταίας για τα ίδια ακριβώς πραγματικά περιστατικά, αντίκειται στην αρχή της αναλογικότητας, κατ' εφαρμογή της οποίας επιβάλλεται συντονισμός των διοικητικών οργάνων και αρχών, προκειμένου η οποιαδήποτε κύρωση να περιορίζεται στο απολύτως απαραίτητο και αναγκαίο βαθμό, δεδομένου ότι η βλάβη που προκαλείται από την επιβολή πολλαπλών διοικητικών κυρώσεων για την ίδια συμπεριφορά, όπως εν προκειμένω, είναι υπέρμετρα επαχθής και υπερβαίνει τον επιδιωκόμενο σκοπό, αφού άλλωστε η διασφάλιση των δεδομένων προσωπικού χαρακτήρα και η προστασία του απορρήτου των επικοινωνιών αποτελούν δυο ειδικότερες εκφάνσεις του αυτού έννομου αγαθού ήτοι της προστασίας της ιδιωτικότητας. Παράλληλα η προσφεύγουσα υποστηρίζει ότι το επαχθές των εν λόγω

κυρώσεων επιτείνεται και εκ του γεγονότος ότι πέραν των ανωτέρω επιβλήθηκε με την ήδη αναφερθείσα απόφαση της ΑΠΔΠΧ πρόστιμο και στον ΟΤΕ ΑΕ ύψους 3.250.000,00 ευρώ, λόγω της συμμετοχής του στον κρίσιμο συμβάν, οπότε το συνολικό ύψος του προστίμου ανέρχεται σε 9.250.000,00 ευρώ. Ο λόγος αυτός της προσφυγής κρίνεται απορριπτέος ως αβάσιμος, υπό την έννοια ότι, καίτοι το ζήτημα του αν η σωρευτική επιβολή διοικητικών κυρώσεων παρίσταται υπέρμετρα επαχθής για τον υπαίτιο παραβάτη, αποτελεί ζήτημα που εκτιμάται στο πλαίσιο της αρχής της αναλογικότητας (βλ. ΣτΕ 3473/2017 σκ. 11), στην υπό κρίση περίπτωση και με βάση τα περιστατικά που διαπιστώθηκαν, την φύση, την έκταση, τη διάρκεια και τη σοβαρότητα της παράβασης, το επιβληθέν με την προσβαλλόμενη απόφαση πρόστιμο κρίνεται ότι δεν αντιστρατεύεται την αρχή της αναλογικότητας, ακόμη και σωρευτικά θεωρούμενο : α) λόγω του όγκου των δεδομένων που διέρρευσαν από τους εξυπηρετητές της προσφεύγουσας, ήτοι (ι) τα δεδομένα κίνησης και οι συντεταγμένες σταθμών βάσης για 4.792.869 μοναδικούς συνδρομητές της, (ιι) ο MSISDN/CLI 6.939.656 χρηστών άλλων εγχώριων παρόχων σταθερής - κινητής τηλεφωνίας που κάλεσαν ή κλήθηκαν από συνδρομητές της προσφεύγουσας και (ιιι) το IMEI και IMSI καθώς και συντεταγμένες σταθμών βάσης για 281.403 συνδρομητές περιαγωγής, προς το υπολογιστικό νέφος και εν συνόλω 12.013.928 χρηστών, που αντιστοιχούν σε αριθμό μεγαλύτερο του μόνιμου πληθυσμού της χώρας που σύμφωνα με την τελευταία απογραφή ανέρχεται σε 10.482.487 (βλ. την από 31.8.2023 απογραφή έτους 2021 της Ελληνική Στατιστικής Αρχής), β) της πλημμελούς και με καθυστέρηση τήρησης της διαδικασίας αλλαγής κωδικών πρόσβασης στους εξυπηρετητές (διαπίστωση το έτος 2018 – συμμόρφωση μέχρι το έτος 2021) και γ) λόγω του ότι η προσφεύγουσα δεν αποδεικνύει ούτε προσκομίζει συγκεκριμένα οικονομικά στοιχεία, ώστε να καταδειχθεί πως οι οικονομικές συνέπειες των σωρευτικά επιβαλλόμενων κυρώσεων εν προκειμένω παρίστανται ιδιαιτέρως δυσμενείς για αυτήν, ώστε να υπερακοντίζουν τον επιδιωκόμενο σκοπό του νομοθέτη, ήτοι του κολασμού του παραβάτη, της διασφάλισης της πιστής τήρησης της κείμενης νομοθεσίας και της αποτροπής παρομοίων παραβάσεων για το μέλλον (πρβλ. ΣτΕ Ολομ.990/2004), ενόψει και του γεγονότος ότι η νομιμότητα της απόφασης της ΑΠΔΠΧ περί επιβολής προστίμου στην προσφεύγουσα έχει αμφισβητηθεί ενώπιον του Συμβουλίου της Επικρατείας, καθώς όπως αναφέρει η προσφεύγουσα έχει ήδη ασκήσει κατ' αυτής την με αριθμό κατάθεσης 701/28.3.2022 αίτηση ακυρώσεως,που εκκρεμεί προς εκδίκαση.

Επειδή, πέραν των ανωτέρω, η προσφεύγουσα προβάλλει ότι μη νομίμως της αποδόθηκε παράβαση του άρθρου 3.2.9 του ΚΔΑΗΕ και της παρ. 5.1.7 της Πολιτικής Ασφαλείας της (Απόκλιση 3), ως προς το τεχνικό πρόβλημα καταγραφής του syslog εξυπηρετητή των δεδομένων εισόδου των χρηστών στον εξυπηρετητή XXXXXXXX. Και τούτο διότι, όπως υποστηρίζει η προσφεύγουσα, το πρόβλημα στον τρόπο καταγραφής των δεδομένων (εγγραφή – επανεγγραφή και διατήρηση για 3 ημέρες των δεδομένων) των χρηστών ήταν τυχαίο, προϋπάρχον του επίμαχου συμβάντος και δεν συνδέονταν με την επίθεση που δέχτηκε το σύστημά της, όπως αβασίμως θεώρησε η ΑΔΑΕ εκτιμώντας ότι το εν λόγω τεχνικό πρόβλημα προέκυψε και για τα αρχεία καταγραφής της 6ης και 7ης.7.2020 και ως εκ τούτου σχετίζεται με αυτήν. Ειδικότερα, η προσφεύγουσα υποστηρίζει ότι το γεγονός ότι υπήρξε πράγματι το διαπιστωθέν τεχνικό πρόβλημα κατά το χρόνο εκδήλωσης της επίθεσης δεν αποδεικνύει ότι τα δυο συμβάντα σχετίζονται, δεδομένου ότι η αρχική σύνδεση του επιτιθέμενου πραγματοποιήθηκε στις 14.4.2020, χωρίς να συμπίπτει χρονικά με το χρόνο διαρροής των δεδομένων μέσω του αρχείου cd.gz στις 8.9.2020, καθώς, υπό την αντίθετη εκδοχή η επίθεση θα είχε εκδηλωθεί νωρίτερα. Ο ισχυρισμός της όμως αυτός, όπως προβάλλεται, βαίνει απορριπτέος ως αβάσιμος. Και τούτο διότι σε κάθε περίπτωση ακόμη και υπό την εκδοχή ότι το διαπιστωθέν εκ των υστέρων πρόβλημα στον syslog εξυπηρετητή δεν υπήρξε αποτέλεσμα της επίθεσης που δέχτηκε η προσφεύγουσα, αλλά τεχνικό πρόβλημα λχ του λογισμικού που χρησιμοποίησε, γεγονός μη αναμφίλεκτο, παντός αποτελεί παράβαση του ως άνω άρθρου 3.2.9 του ΚΔΑΗΕ και προδήλως διευκόλυνε τον επιτιθέμενο και όχι τους εκ των υστέρων επιληφθέντες υπαλλήλους της προσφεύγουσας και του ελέγχοντες υπαλλήλους της ΑΔΑΕ, υπό την έννοια ότι τελικώς, λόγω της σχετικής αστοχίας, αφού εν προκειμένω τα αρχεία διαγράφονταν ανά 3 ημέρες και γινόταν επανεγγραφή, δεν υφίστατο πλήρες αρχείο καταγραφής στον syslog εξυπηρετητή,όπως απαιτεί ο κανονισμός, ο οποίος προβλέπει ρητώς την πλήρη και συνεχή καταγραφή.

Επειδή, η προσφεύγουσα προβάλλει περαιτέρω ότι εσφαλμένως της αποδόθηκε με την προσβαλλόμενη απόφαση παράβαση του άρθρου 6.2.1 του ΚΔΑΗΕ και των παρ. 2.1.1. και 2.2.2 της Πολιτικής Λογικής Πρόσβασης (Απόκλιση 5) ως προς την απόκτηση πρόσβασης στα ΠΕΣ μέσω αυθεντικοποίησης. Υποστηρίζει ειδικότερα, ότι η ΑΔΑΕ παρανόμως θεώρησε ότι εκτός από την σύνδεση στο σύστημα με προσωποποιημένο λογαριασμό χρήστη και κωδικό εισόδου απαιτείται να υπάρχει αντίστοιχος μηχανισμός ελέγχου πρόσβασης και αυθεντικοποίησης και για την πρόσβαση στον

λογαριασμό root με χρήση της εντολής sudo, αφού πρόκειται για επιπλέον μέτρο ασφαλείας που δεν απαιτούνταν από το επικαλούμενο άρθρο 6.2.1 του ΚΔΑΗΕ. Ο λόγος αυτός κρίνεται απορριπτέος ως αβάσιμος και τούτο διότι η πρόσβαση στα ΠΕΣ ενός υπαλλήλου δεν σημαίνει ότι αυτός δύναται άνευ ετέρου να έχει πλήρη δικαιώματα εκτέλεσης όλων ανεξαιρέτως των εντολών που είναι εφικτό να διενεργηθούν, πολλώ δε μάλλον που ειδικά σε λογαριασμούς τύπου root οι χρήστες έχουν δικαιώματα διαχειριστή, οπότε επιβάλλεται η πρόσθετη χρήση μηχανισμών αυθεντικοποίησης. Εξάλλου, ακριβώς για την αποτροπή αντίστοιχων περιστατικών διαρροών, η προσφεύγουσα έθεσε σε εφαρμογή του σύστημα PAM, όπως ανέφερε και η ίδια.

Επειδή, ακολούθως η προσφεύγουσα προβάλλει ότι εσφαλμένως της αποδόθηκε με την προσβαλλόμενη απόφαση παράβαση του άρθρου 8.3.3.1 και 6.3.2.1.γ΄ του ΚΔΑΗΕ και της παρ. 2.4.1. της Πολιτικής Διαχείρισης και Εγκατάστασης Συστημάτων (Απόκλιση 6) ως προς τον μη εντοπισμό και την σήμανση συναγερμού λόγω των σχετικών αιτημάτων που υπέβαλλε ο επιτιθέμενος μέσω του λογαριασμού χρήστη root του υπαλλήλου της επιχείρησης. Ειδικότερα, η προσφεύγουσα υποστηρίζει ότι οι συναγερμοί προκύπτουν από συμβάντα ασφαλείας που παραβιάζουν συγκεκριμένους κανόνες ασφαλείας, οπότε η εκτέλεση εντολών αναζήτησης από λογαριασμούς νόμιμων χρηστών, όπως φαινομενικά συνέβη στην υπό κρίση υπόθεση, δεν μπορούν να γίνουν αντιληπτοί ως παραβίαση και συνεπώς δεν παράγουν αντίστοιχες ειδοποιήσεις και συναγερμούς, ενώ, υπό την αντίθετη παραμετροποίηση των συστημάτων, δεν θα ήταν δυνατή η καθημερινή εργασία των διαχειριστών, όπως λχ η διαχείριση βλαβών. Ενόψει αυτών, η προσφεύγουσα ισχυρίζεται ότι εσφαλμένως η ΑΔΑΕ θεώρησε ότι ένας διαχειριστής λειτουργικών συστημάτων είναι υπεύθυνος για την συντήρηση, την διαμόρφωση και την αξιόπιστη λειτουργία των λειτουργικών συστημάτων των εξυπηρετητών και όχι για την σύνδεση σε βάσεις δεδομένων, αφού η πρόσβαση του επιτιθέμενου πραγματοποιήθηκε με τα διαπιστευτήρια λογαριασμού της βάσης και όχι λογαριασμού διαχειριστή συστήματος. Ο ισχυρισμός αυτός τυγχάνει απορριπτέος ως αβάσιμος, κατά το σκέλος που αφορά την μη παραγωγή συναγερμού για παράνομη δραστηριότητα, καθώς λόγω του εύρους και του είδους των αναζητήσεων, που όπως προέκυψε από την έρευνα ήταν υπερβολικά μεγάλος (μεταδεδομένα 12.013.928 χρηστών – μέγεθος αρχείου περίπου 30gb) και του γεγονότος ότι ένας υπάλληλος της προσφεύγουσας υπέβαλε ένα τέτοιου είδους αίτημα, θα έπρεπε να θεωρηθεί ως μη αιτιολογημένη από το ίδιο το σύστημα, όπως και κατά το δεύτερο του σκέλος διότι ο επιτιθέμενος απέκτησε στοιχεία λογαριασμού χρήστη root, ο οποίος περιλαμβάνονταν μαζί με άλλους (6) σε εκείνους που είχαν την δυνατότητα σύνδεσης στον σχετικό εξυπηρετητή απευθείας, ήτοι χωρίς περαιτέρω αυθεντικοποίηση, με πλήρη δικαιώματα, οπότε η πρόσβαση του επιτιθέμενου, κατ' αυτόν τον τρόπο διευκολύνθηκε, αφού με τον αρχικό λογαριασμό απέκτησε δικαιώματα εντολής sudo χωρίς επιπλέον αυθεντικοποίηση.

Επειδή, ενόψει του γεγονότος ότι δεν προβάλλονται ειδικότερες αιτιάσεις ως προς τις λοιπές αποκλίσεις που διαπιστώθηκαν κατά τον έλεγχο, το Δικαστήριο λαμβάνοντας υπόψη όλα τα ανωτέρω νομικά και πραγματικά δεδομένα και ιδίως: α)το εκτεταμένο εύρος των διαρρευσάντων μεταδεδομένων σε συνδυασμό με το σύνολο των θιγόμενων συνδρομητών, β) ότι εν προκειμένω διέρρευσαν δεδομένα και συνδρομητών έτερων παρόχων -χρηστών περιαγωγής και γ) ότι συνέτρεξαν πολλαπλές αποκλίσεις από τις δέουσες πολιτικές ασφαλείας, ιδίως ως προς την επίκαιρη αλλαγή των κωδικών εισόδου και την εκχώρηση δικαιωμάτων root, όπως και στην παραμετροποίηση του χώρου φιλοξενίας ιστοσελίδων σε σχέση με την διασύνδεση του με τους εφεδρικούς εξυπηρετητές, κρίνει ότι η προσφεύγουσα υπέπεσε στις αποδοθείσες παραβάσεις και το επιβληθέν πρόστιμο για κάθε μία από αυτές κρίνεται δίκαιο και είναι ανάλογο, όσα δε περί του αντιθέτου υποστηρίζονται με την προσφυγή και τους πρόσθετους λόγους είναι απορριπτέα, ως αβάσιμα.

Επειδή, κατ' ακολουθία η προσφυγή και οι πρόσθετοι λόγοι πρέπει να απορριφθούν, να καταπέσει το καταβληθέν παράβολο υπέρ του Δημοσίου, κατ' άρθρο 277 παρ. 9 του ΚΔΔ και να καταλογισθούν στην προσφεύγουσα τα δικαστικά έξοδα της ΑΔΑΕ, οριζόμενα στο ποσό των τριακοσίων σαράντα ενός (341,00) ευρώ, κατ' άρθρο 275 παρ. 1 του ΚΔΔ και Παράρτημα Ι του Κώδικα Δικηγόρων (ν. 4194/2013 - Α΄ 208).

ΔΙΑ ΤΑΥΤΑ

Απορρίπτει την προσφυγή και τους πρόσθετους λόγους.

Διατάσσει την κατάπτωση του παραβόλου υπέρ του Δημοσίου.

Καταλογίζει στην προσφεύγουσα τα δικαστικά έξοδα της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών, ύψους τριακοσίων σαράντα ενός (341) ευρώ.

Η διάσκεψη του Δικαστηρίου έγινε στην Αθήνα στις 15 Νοεμβρίου 2024 και η απόφαση δημοσιεύθηκε στον ίδιο τόπο, σε έκτακτη δημόσια συνεδρίαση στο ακροατήριό του, στις 31 Δεκεμβρίου 2024.

Η ΠΡΟΕΔΡΕΥΟΥΣΑ Ο ΕΙΣΗΓΗΤΗΣ

Κ.ΘΕΟΔΩΡΑΤΟΥ Γ.Δ.Ν. ΤΣΑΠΡΑΖΗΣ

Η ΓΡΑΜΜΑΤΕΑΣ

Κ.ΑΜΕΡΙΚΑΝΗ