

Μαρούσι, 04.11.2020
Αρ. Πρωτ.: ~~5555~~

ΑΠΟΦΑΣΗ
(αριθμ:316/2020)
(ΑΝΑΡΤΗΤΕΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ)

Θέμα: Απόφαση επί της από 21.02.2018 Ακρόασης της εταιρείας «ΟΡΓΑΝΙΣΜΟΣ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ ΤΗΣ ΕΛΛΑΔΟΣ Α.Ε.», με αντικείμενο τον έλεγχο ενδεχόμενης παραβάσεως της κείμενης νομοθεσίας περί απορρήτου των επικοινωνιών.

Η Ολομέλεια της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (Α.Δ.Α.Ε.), συνεδρίασε την 04.11.2020, παρισταμένων των κ.κ. Χρήστου Ράμμου, Προέδρου της Αρχής, Μιχαήλ Σακκά, Αντιπροέδρου της Αρχής, του τακτικού μέλους Γεωργίου Μπακάλη και του αναπληρωματικού μέλους Γεωργίου Μισαηλίδη, ο οποίος αντικατέστησε ως εισηγητής της υποθέσεως, το εξελθόν στο θέμα αυτό λόγω υπηρεσιακού κωλύματος τακτικό μέλος κα Αικατερίνη Παπανικολάου, προκειμένου να αποφασίσει επί της από 21.02.2018 Ακρόασης της εταιρείας «ΟΡΓΑΝΙΣΜΟΣ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ ΤΗΣ ΕΛΛΑΔΟΣ Α.Ε.», με αντικείμενο τον έλεγχο ενδεχόμενης παραβάσεως της κείμενης νομοθεσίας περί απορρήτου των επικοινωνιών.

Ο μη παραστάς κατά την από 21.02.2018 ακρόαση Πρόεδρος της ΑΔΑΕ, κ. Χρήστος Ράμμος, δήλωσε ότι ενημερώθηκε για το περιεχόμενο των πρακτικών της ακρόασης, του υποβληθέντος υπομνήματος και για το σύνολο των στοιχείων του φακέλου.

Η ΑΔΑΕ ασχολήθηκε με την παράβαση της κείμενης νομοθεσίας περί απορρήτου των επικοινωνιών από την εταιρεία «ΟΡΓΑΝΙΣΜΟΣ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ ΤΗΣ ΕΛΛΑΔΟΣ Α.Ε.», κατόπιν της υπ' αριθμ. πρωτ.ΑΔΑΕ 953/20.05.2015 καταγγελίας της εταιρείας «~~XXXX~~», στην οποία αναφερόταν ότι στις τερματικές συσκευές routers (CPE), τύπου ZTE H108N που διατίθεται στους συνδρομητές από την εταιρεία ΟΤΕ, πέραν των κωδικών για τη διαχείρισή τους από τον πάροχο, εντοπίστηκαν δύο επιπρόσθετοι κωδικοί πρόσβασης, κοινοί για όλες τις συσκευές (CPE) αυτού του τύπου. Οι κωδικοί αυτοί διατηρούνταν σε μη-



κρυπτογραφημένη μορφή δίνοντας τη δυνατότητα σε τρίτο, που τους γνωρίζει, να αποκτήσει απομακρυσμένη πρόσβαση στη συσκευή (CPE).

Η ακρόαση της εταιρείας «ΟΡΓΑΝΙΣΜΟΣ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ ΤΗΣ ΕΛΛΑΔΟΣ Α.Ε.» έλαβε χώρα ενώπιον της Αρχής, την 21.02.2018.

Η εταιρεία «ΟΡΓΑΝΙΣΜΟΣ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ ΤΗΣ ΕΛΛΑΔΟΣ Α.Ε.» κατέθεσε στην ΑΔΑΕ το υπ' αριθμ. πρωτ. ΑΔΑΕ ΕΜΠ 118/23.05.2018 έγγραφο υπόμνημά της.

Η συζήτηση της υποθέσεως έλαβε χώρα αυθημερόν, καθώς και η λήψη της σχετικής απόφασης.

Ειδικότερα:

ΚΕΦΑΛΑΙΟ Α'

Η Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (ΑΔΑΕ), με την υπ' αριθμ. 326/2017 απόφασή της κάλεσε σε ακρόαση την εταιρεία με την επωνυμία «ΟΡΓΑΝΙΣΜΟΣ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ ΤΗΣ ΕΛΛΑΔΟΣ Α.Ε.» (καλούμενης εφεξής ΟΤΕ), την 21^η Φεβρουαρίου 2018, με αντικείμενο τον έλεγχο της παραβάσεως της κείμενης νομοθεσίας σε σχέση με το απόρρητο των επικοινωνιών. Η εν λόγω ακρόαση αφορούσε στην υπ' αριθμ. πρωτ. ΑΔΑΕ 953/20.05.2015 καταγγελία της εταιρείας «[REDACTED]», στην οποία αναφερόταν ότι στις τερματικές συσκευές routers (CPE)¹, τύπου ZTE H108N που διατίθετο στους συνδρομητές από την εταιρεία ΟΤΕ, πέραν των κωδικών για τη διαχείρισή τους από τον πάροχο, εντοπίστηκαν δύο επιπρόσθετοι κωδικοί πρόσβασης, κοινοί για όλες τις συσκευές (CPE) αυτού του τύπου. Οι κωδικοί αυτοί διατηρούνταν σε μη-κρυπτογραφημένη μορφή δίνοντας τη δυνατότητα σε τρίτο, που τους γνωρίζει, να αποκτήσει απομακρυσμένη πρόσβαση στη συσκευή (CPE).

Η υπ' αριθμ. πρωτ. ΑΔΑΕ 419/06.02.2018 Κλήση μετά της συνημμένης σε αυτήν Απόφασης της ΑΔΑΕ με αριθμό 326/2017 επεδόθη στην εταιρεία νομίμως και εμπροθέσμως, όπως προκύπτει από την υπ' αριθμ. Α-9618/08.02.2018 Έκθεση Επίδοσης. Η εταιρεία παρέστη κατά την ακρόαση της 21^{ης} Φεβρουαρίου 2018 και, εν συνεχεία, η Αρχή της κοινοποίησε τα σχετικά Πρακτικά δια του υπ' αριθμ. πρωτ. ΑΔΑΕ 1328/24.04.2018 εγγράφου της, όπως προκύπτει από την υπ' αριθμ.

¹ ΤΕΡΜΑΤΙΚΗ ΣΥΣΚΕΥΗ (CPE, Customer Premises Equipment). Εξοπλισμός που εγκαθίσταται στο χώρο του συνδρομητή. Πρόκειται για δρομολογητή (router), απαραίτητο για την επικοινωνία δεδομένων (data) και τη πρόσβαση στο διαδίκτυο (internet).

A-9918/03.05.2018 Έκθεση Επίδοσης. Τέλος, η εταιρεία ΟΤΕ υπέβαλε το υπ' αριθμ. πρωτ. ΑΔΑΕ ΕΜΠ 118/23.05.2018 έγγραφο υπόμνημά της.

Εκ των στοιχείων του φακέλου, της από 21.02.2018 ακροάσεως των εκπροσώπων της εταιρείας ΟΤΕ, μετά των δικηγόρων της, του υπ' αριθμ. πρωτ. ΑΔΑΕ ΕΜΠ 118/23.05.2018 υποβληθέντος υπομνήματος και της από 21.11.2016 Έκθεσης Έκτακτης Έρευνας στην εταιρεία ΟΤΕ, προέκυψε ότι η εν θέματι εταιρεία, κατά το χρόνο διεξαγωγής της έκτακτης έρευνας, η οποία έλαβε χώρα κατόπιν της υπ' αριθμ. Πρωτ. ΑΔΑΕ 953/20.05.2015 καταγγελίας της εταιρείας «[REDACTED]», δεν εφάρμοσε τις δέουσες πολιτικές και επιμέρους διαδικασίες, κατά τη διάθεση στους συνδρομητές της, της τερματικής συσκευής (CPE), τύπου ZTE H108N, και δεν ενημέρωσε την ΑΔΑΕ ούτε τους θιγόμενους συνδρομητές που επηρεάστηκαν από το εν λόγω περιστατικό ασφάλειας.

Ενόψει των ανωτέρω ελήφθησαν υπόψη :

1. οι διατάξεις:

- α) του Ν. 3115/2003 (ΦΕΚ 47 Α'/27-2-2003), όπως ισχύει και ιδίως το άρθρο 6 παρ. 1 στοιχ. α', β', γ', δ' ιβ' και παρ. 2 και του άρθρου 11,
- β) του Ν. 3471/2006 (ΦΕΚ 133 Α'/28.6.2006), όπως ισχύει, ιδίως του άρθρου 4 παρ. 2 και του άρθρου 12 παρ. 1, 5 και 6 αυτού, ο οποίος τροποποιήθηκε με το Ν. 4070/2012 (ΦΕΚ 82 Α/2012),
- γ) της υπ' αριθμ. 165/2011 Απόφασης της ΑΔΑΕ «Κανονισμός για την Διασφάλιση Απορρήτου των Ηλεκτρονικών Επικοινωνιών» (ΦΕΚ Β' 2715/17-11-2011), ιδίως του άρθρου 8 «Πολιτική Διαχείρισης και Εγκατάστασης ΠΕΣ», παρ. 8.1 «Σκοπός –Εύρος Πολιτικής», παρ. 8.2.1, παρ. 8.2.3. παρ. του άρθρου 9, 9.1. ,9.2. «Γενικές Απαιτήσεις» 9.2.1., 9.2.2. , 9.2.3. και του άρθρου 11 «Πολιτική Ελέγχου Εφαρμογής της Πολιτικής Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών», παρ. 11.1 αυτής.
- δ) του Ν.3051/2002 «Συνταγματικά κατοχυρωμένες ανεξάρτητες αρχές, τροποποίηση και συμπλήρωση του συστήματος προσλήψεων στο δημόσιο τομέα και συναφείς ρυθμίσεις» (ΦΕΚ Α' 220/2002), όπως ισχύει,
- ε) του Ν. 4055/2012 «Δίκαιη δίκη και εύλογη διάρκεια αυτής» (ΦΕΚ 51/Α/2012) και ιδίως το άρθρο 61 παρ. 1 αυτού,
- στ) της υπ' αριθμ. 44/31.10.2003 Απόφασης της Α.Δ.Α.Ε. «Κανονισμός Εσωτερικής Λειτουργίας



της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών» (ΦΕΚ Β' 1642/7.11.2003), όπως τροποποιήθηκε με την Απόφαση της Α.Δ.Α.Ε. υπ'αριθμ.76/2006 (ΦΕΚ Β' 963/20.7.2006), ιδίως το άρθρο 4 παρ. 3 αυτής,

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

η) του άρθρου 26 παρ.7 του ν.4325/2015 (ΦΕΚ Α' 47/2015),

θ) του άρθρου 55 παρ.10 του Ν. 4339/2015 (ΦΕΚ Α' 133/2015),

ι) του άρθρου 73 του Ν. 4369/2016 (ΦΕΚ Α' 33/2016),

ια) του Ν. 4411/2016 (ΦΕΚ Α'142/03.08.2016),

2. η 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,

3. η υπ' αριθ. 34051/29.05.2018 Απόφαση του Υπουργού Δικαιοσύνης, Διαφάνειας και Ανθρωπίνων Δικαιωμάτων (ΦΕΚ Υ.Ο.Δ.Δ. 326), περί διορισμού Προέδρου της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών, όπως διορθώθηκε στο ορθό με το ΦΕΚ Υ.Ο.Δ.Δ.396/2019,

4. η υπ'αριθ. πρωτ Α.Δ.Α.Ε. ΕΜΠ 126/2013 Πολιτική Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών της εταιρείας ΟΤΕ, η οποία εγκρίθηκε με την υπ'αριθμ. 294/2013 Απόφαση της Α.Δ.Α.Ε, ιδίως η «Πολιτική Διαχείρισης & Εγκατάστασης Συστημάτων» (Εκδοση 1.0-19/11/2012, σελ 13-14), η Πολιτική Διαχείρισης Περιστατικών Ασφάλειας (Εκδοση 1.0-19/11/2012, σελ 15-16) και η «Πολιτική Ελέγχου Εφαρμογής της Πολιτικής Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών» (Εκδοση 1.0-19/11/2012, σελ 19-20),

5. το υπ'αριθμ. πρωτ. ΑΔΑΕ 953/20.05.2015 έγγραφο της εταιρείας «[REDACTED]»,

6. η υπ'αριθμ. 84/2015 Απόφαση της ΑΔΑΕ,

7. η υπ'αριθμ. 264/2015 Απόφαση του Αντιπροέδρου της ΑΔΑΕ,

8. το από 21.09.2015 Πρακτικό Διενέργειας επιτόπιου ελέγχου στις εγκαταστάσεις της εταιρείας ΟΤΕ. μετά συνημμένων αυτού εγγράφων,



9. το υπ' αριθμ. πρωτ. ΑΔΑΕ ΑΠΡ 4003/09.10.2015 έγγραφο της εταιρείας ΟΤΕ, μετά συνημμένων αυτού στοιχείων,
10. το υπ' αριθμ. πρωτ. ΑΔΑΕ 2334/21.10.2015 μήνυμα ηλεκτρονικού ταχυδρομείου της εταιρείας ΟΤΕ,
11. το υπ' αριθμ. πρωτ. ΑΔΑΕ 2674/11.11.2015 έγγραφο της ΑΔΑΕ,
12. το υπ' αριθμ. πρωτ. ΑΔΑΕ ΕΜΠ 20/08.02.2016 έγγραφο της εταιρείας ΟΤΕ, μετά συνημμένων αυτού εγγράφων,
13. η από 21.11.2016 Έκθεση Διενέργειας Εκτάκτου Ελέγχου στην εταιρεία ΟΤΕ,
14. η υπ' αριθμ. 301/09.12.2016 Εισήγηση προς την Ολομέλεια της Αρχής,
15. το πρακτικό της από 14.12.2016 συνεδρίασης της Ολομέλειας της Αρχής,
16. το υπ' αριθμ. πρωτ. ΑΔΑΕ 3119/19.12.2016 έγγραφο της ΑΔΑΕ,
17. το υπ' αριθμ. πρωτ. ΑΔΑΕ ΕΜΠ 3/23.01.2017 έγγραφο της εταιρείας ΟΤΕ,
18. το Απόσπασμα της υπ' αριθμ. 368/2016 Απόφασης της Ολομέλειας της Αρχής,
19. το υπ' αριθμ. πρωτ. ΑΔΑΕ 34/06.03.2017 έγγραφο της ΑΔΑΕ προς την καταγγέλλουσα εταιρεία,
20. η υπ' αριθμ. πρωτ. ΑΔΑΕ 752/14.03.2017 Απόδειξη Παράδοσης Παραλαβής,
21. η υπ' αριθμ. 373/2017 Εισήγηση ενώπιον της Ολομέλειας της Αρχής,
22. το Πρακτικό της από 25.10.2017 συνεδρίασης της Ολομέλειας της Αρχής,
23. η υπ' αριθμ. 326/2017 Απόφαση της Ολομέλειας της Αρχής,
24. η υπ' αριθμ. πρωτ. ΑΔΑΕ 419/06.02.2018 Κλήση σε ακρόαση της εταιρείας, η οποία επεδόθη στην εταιρεία μετά της συνημμένης αυτής υπ' αριθμ. 326/2017 Απόφασης με την υπ' αριθμ. Α-9618/08.02.2018 Έκθεση Επίδοσης της Δικαστικής Επιμελήτριας του Εφετείου Αθηνών κας Γεωργίας Γιωτοπούλου,
25. το πρακτικό της από 21.02.2018 Ακρόασης της εταιρείας, το οποίο επεδόθη σε αυτή με την υπ' αριθμ. Α- 9918/03.05.2018 Έκθεση Επίδοσης της Δικαστικής Επιμελήτριας του Εφετείου Αθηνών κας [REDACTED],
26. το υπ' αριθμ. πρωτ. ΑΔΑΕ 118/23.05.2018 Υπόμνημα της εταιρείας,
27. η υπ' αριθμ. 254/2020 Εισήγηση προς την Ολομέλεια της Αρχής,
28. το πρακτικό της από 04.11.2020 συνεδρίασης της Ολομέλειας,
29. τα πρόσφατα οικονομικά στοιχεία της εταιρείας.

ΚΕΦΑΛΑΙΟ Β΄

Ειδικότερα, επί των ισχυρισμών που προέβαλε η εταιρεία ΟΤΕ τόσο κατά την ακρόασή της, όπως αποτυπώνεται στο από 21.02.2018 Πρακτικό Ακρόασης ενώπιον της Αρχής όσο και στο υπ' αριθμ. Πρωτ. ΑΔΑΕ ΕΜΠ 118/23.05.2018 Υπόμνημά της επισημαίνονται τα ακόλουθα:

Ι. Ως προς την υποβληθείσα ένσταση:***ΠΑΡΑΒΑΣΗ ΤΗΣ ΑΡΧΗΣ ΤΗΣ ΕΥΛΟΓΗΣ ΔΙΑΡΚΕΙΑΣ ΤΗΣ ΔΙΑΔΙΚΑΣΙΑΣ***

Η εταιρεία ισχυρίζεται ότι η παρέλευση δυόμισι ετών από την διενέργεια του Ελέγχου (Σεπτέμβριος 2015) μέχρι τη διενέργεια ακρόασης, έρχεται σε αντίθεση προς την αρχή της χρηστής διοίκησης, έκφανση της οποίας συνιστά η αρχή της δικαιολογημένης εμπιστοσύνης του διοικουμένου και της ασφάλειας δικαίου (βλ. και υπ' αριθμ. Απόφαση 1989/2013 ΣτΕ). Το ως άνω χρονικό διάστημα το οποίο μεσολάβησε μέχρι σήμερα δεν είναι εύλογο. Επομένως, η αδικαιολόγητα μεγάλη διάρκεια για την περάτωση της διοικητικής διαδικασίας, πέραν του ότι είναι αντίθετη σε ρητές διατάξεις του Κώδικα Διοικητικής Διαδικασίας, οδηγεί σε υπέρμετρη καθυστέρηση η οποία από μόνη της συνιστά παραβίαση θεμελιωδών δικαιωμάτων βάσει Συντάγματος και ΕΣΔΑ (βλ. το υπ' αριθμ. Πρωτ. ΑΔΑΕ ΕΜΠ 118/23.05.2018 Υπόμνημα της εταιρείας σελ. 2).

Οι ανωτέρω ισχυρισμοί προβάλλονται αβασίμως, και τούτο διότι σύμφωνα με το ιστορικό της εν θέματι υποθέσεως η ΑΔΑΕ επέδειξε κατά τη διερεύνηση του επίμαχου περιστατικού ασφάλειας συμπεριφορά άκρως συμμορφούμενη με τις αρχές της χρηστής διοίκησης. Τούτο επιβεβαιώνεται από τις ενέργειες της Αρχής, στις οποίες προέβη μετά την ενημέρωσή της για την εκδήλωση του εν θέματι περιστατικού ασφάλειας. Ειδικότερα, αναφορικά με την πάροδο ευλόγου χρόνου από την ενημέρωση της Αρχής με την υπ' αριθμ. πρωτ. ΑΔΑΕ 953/20.05.2015 καταγγελία μέχρι την ακρόαση της ελεγχόμενης εταιρείας (21.02.2018), επισημαίνονται τα ακόλουθα:

Στην ΑΔΑΕ υπεβλήθη το υπ' αριθμ. πρωτ. ΑΔΑΕ 953/20.05.15 έγγραφο της εταιρείας «**██████████**» στο οποίο αναφερόταν ότι στις τερματικές συσκευές (CPE), τύπου ZTE H108N, πέραν των κωδικών για τη διαχείρισή τους από τον πάροχο, έχουν εντοπισθεί δύο επιπρόσθετοι κωδικοί πρόσβασης, κοινοί για όλες τις συσκευές (CPE) αυτού του τύπου. Οι κωδικοί αυτοί διατηρούνταν σε μη-κρυπτογραφημένη μορφή και έδιναν τη δυνατότητα σε τρίτο, που τους γνωρίζει, να αποκτήσει απομακρυσμένη πρόσβαση στη συσκευή (CPE). Σύμφωνα με το



παραπάνω έγγραφο, κατά το χρόνο υποβολής του, ο συγκεκριμένος τύπος τερματικής συσκευής (CPE), διατίθεται από την εταιρεία ΟΤΕ στους πελάτες της.

Κατόπιν τούτων, η ΑΔΑΕ δυνάμει της υπ' αριθμ. 84/27.05.2015 Απόφασης της Ολομέλειας συνέστησε Ομάδα Ελέγχου (ΟΕ) για τη διερεύνηση του εν λόγω περιστατικού ασφάλειας και τη διεξαγωγή ελέγχου σε παρόχους πρόσβασης στο διαδίκτυο που προμηθεύουν τους συνδρομητές τους με συσκευές που εμπλέκονται στο ως άνω περιστατικό. Ειδικότερα, η ΑΔΑΕ διενήργησε έλεγχο σε πέντε (5) παρόχους, ένας εκ των οποίων, ήταν και η εταιρεία ΟΤΕ, οι δε επιτόπιες επισκέψεις έλαβαν χώρα κατά τις ημερομηνίες: 19.06.2015, 09.10.2015 21.09.2015 (αφορά σε επιτόπιο έλεγχο στην εταιρεία ΟΤΕ κατόπιν της υπ' αριθμ. 264/2015 Απόφασης του Αντιπροέδρου της Αρχής), 23.10.2015 και 11.03.2016. Τα αποτελέσματα των διενεργούμενων ελέγχων περιελήφθησαν στην από 21.11.2016 Έκθεση Διενέργειας Εκτάκτου Ελέγχου.

Σημειώνεται ότι μετά την από 19.12.2013 παραίτηση του τότε Προέδρου της Αρχής, κ. Ανδρ. Λαμπρινόπουλου (ΦΕΚ Υ.Ο.Δ.Δ. 19/22.01.2014), σύμφωνα με τη διάταξη του άρθρου 3 παρ. 2 του Ν. 3051/2002, όπως ίσχυε μετά την τροποποίησή του από το άρθρο 61 παρ. 2 του Ν. 4055/2012, η Αρχή συνέχισε να λειτουργεί για ένα εξάμηνο. Εν συνεχεία, την 11.05.2015 δημοσιεύτηκε ο Ν. 4325/2015 (ΦΕΚ Α' 47/11.05.2015), ο οποίος τροποποίησε, εκ νέου, την ανωτέρω διάταξη του Ν. 3051/2002, ορίζοντας ότι η Αρχή συνεχίζει να λειτουργεί νομίμως εάν αποχωρήσει ή εκλείψει κάποιος μέλος της, εφόσον τα λοιπά μέλη επαρκούν για το σχηματισμό απαρτίας, χωρίς τον περιορισμό του εξαμήνου και η Αρχή επαναλειτούργησε νομίμως. Κατόπιν τούτου, δυνάμει της υπ' αριθμ. 84/27.05.2015 Απόφασης της Ολομέλειας συστάθηκε Ομάδα Ελέγχου (ΟΕ) για τη διερεύνηση του εν θέματι περιστατικού ασφάλειας και τη διεξαγωγή ελέγχου σε αρχεία, τράπεζες δεδομένων, έγγραφα, βιβλία, στοιχεία στις εγκαταστάσεις και τον τεχνικό εξοπλισμό των παρόχων πρόσβασης στο διαδίκτυο που προμηθεύουν τους συνδρομητές τους με συσκευές που εμπλέκονται στο καταγγελλόμενο περιστατικό ασφάλειας. Με την υπ' αριθμ. 264/15.09.2015 Απόφαση του Αντιπροέδρου της Αρχής ορίστηκε ΟΕ για τη διενέργεια επιτόπιου ελέγχου στην εταιρεία ΟΤΕ. Ο έλεγχος πραγματοποιήθηκε την 21.09.2015. Πλην όμως, δημοσιεύτηκε ο Ν. 4339/2015 (ΦΕΚ Α' 133/29.10.2015), οπότε και καταργήθηκε η διάταξη του άρθρου 110 παρ. 12 του Ν. 4055/2012 και αποχώρησαν από την Αρχή τα μέλη των οποίων είχε λήξει η θητεία. Έκτοτε, η Αρχή λειτούργησε εκ νέου μετά τον ορισμό της νέας Ολομέλειας, η οποία πραγματοποιήθηκε με την υπ' αριθμ. 16887/17.03.2016 (ΦΕΚ Υ.Ο.Δ.Δ. 151/21.03.2016) Απόφαση του Υπουργού Δικαιοσύνης. Εν συνεχεία, συνετάχθη η από 21.11.2016 Έκθεση

Διενέργειας Εκτάκτου Ελέγχου, η οποία αφορά το σύνολο των διαπιστώσεων της ΟΕ αναφορικά με τον έλεγχο των πέντε παρόχων με πρόσβαση στο διαδίκτυο που προμηθεύουν τους συνδρομητές τους με συσκευές και εμπλέκονται στο καταγγελλόμενο περιστατικό ασφάλειας, η οποία ενεκρίθη από την από 14.12.2016 συνεδρίαση της Ολομέλειας της Αρχής με την υπ' αριθμ. 368/2016 Απόφαση, απόσπασμα της οποίας παρέλαβε η εταιρεία με την υπ' αριθμ. πρωτ. ΑΔΑΕ 752/14.03.2017 Απόδειξη Παράδοσης – Παραλαβής. Επισημαίνεται ότι στην παρ. Δ2 του κεφ. Δ' «ΣΥΜΠΕΡΑΣΜΑΤΑ» της εν λόγω Έκθεσης Εκτάκτου Ελέγχου συμπεριελήφθησαν Οδηγίες/Συστάσεις προς τους πέντε ελεγχόμενους παρόχους ως προς τα μέτρα ασφάλειας που οφείλουν να λαμβάνουν για την ασφάλεια των CPEs που διαθέτουν στους πελάτες τους και την ασφαλή απομακρυσμένη πρόσβαση των παρόχων στον τερματικό εξοπλισμό των συνδρομητών τους (CPEs). Τέλος, με την υπ' αριθμ. 326/2017 Απόφαση της Αρχής εκλήθη η εταιρεία για ακρόαση την 21.02.2018.

Από τα ανωτέρω ουδόλως προκύπτει υπέρβαση των ακραίων εύλογων ορίων που πρέπει να τηρούνται, σύμφωνα με την γενική αρχή της επίκαιρης άσκησης των σχετικών αρμοδιοτήτων από τη Διοίκηση (βλ. Απόφαση Διοικ. Εφ. Αθηνών 3589/2018 Τμήμα 14^ο Τριμελές). Η δε πάροδος αυτού του χρονικού διαστήματος, σε καμία περίπτωση, δεν οφείλεται σε υπαιτιότητα της Αρχής. Ως εκ τούτου, η εταιρεία προσχηματικώς προβάλλει τον εν λόγω ισχυρισμό, δεδομένου ότι τα στοιχεία τεκμηρίωσης της εν θέματι υπόθεσης είχαν ήδη συγκεντρωθεί και γνωστοποιηθεί σε εκείνη κατά το χρόνο διενέργειας του ελέγχου από την Αρχή, ο οποίος έλαβε χώρα αμέσως μετά την ενημέρωση της ΑΔΑΕ για την εκδήλωση του περιστατικού.

Κατόπιν των ανωτέρω, προκύπτει ότι η Αρχή προέβη εγκαίρως σε όλες τις απαιτούμενες ενέργειες, προκειμένου να διερευνήσει το επίμαχο περιστατικό, συγκεντρώνοντας το σύνολο της σχετικής με αυτό πληροφορίας και επισημαίνοντας στην εταιρεία τις αποκλίσεις που είχε διαπιστώσει κατά τον έκτακτο έλεγχο που διενήργησε, με σκοπό τη διασφάλιση του απορρήτου των επικοινωνιών των συνδρομητών της.

Αλλωστε, το δικαίωμα προηγούμενης ακρόασης των διοικουμένων (άρθρο 20 παρ. 2 του Συντάγματος) συνίσταται στη δυνατότητα του διοικουμένου, πριν από την έκδοση δυσμενούς γι' αυτόν ατομικής διοικητικής πράξης, να διατυπώσει τις απόψεις του ενώπιον του αρμοδίου διοικητικού οργάνου, ώστε να επηρεάσει τη λήψη από το όργανο αυτό της σχετικής απόφασης. Συνεπώς, εν προκειμένω, ο εκ του Συντάγματος προβλεπόμενος σκοπός της Αρχής, ήτοι η

διασφάλιση του απορρήτου των επικοινωνιών και η προστασία του απολύτως απαραβίαστου ατομικού δικαιώματος του απορρήτου των επικοινωνιών των συνδρομητών της εταιρείας, επετεύχθη κατά τρόπο άμεσο και αποτελεσματικό δια της έγκαιρης και επισταμένης έρευνας που διεξήχθη από την ΑΔΑΕ αμέσως μετά την ενημέρωσή της για την εκδήλωση του περιστατικού ασφάλειας και, εν συνεχεία, επιδίδοντας στην εταιρεία την Έκθεση Ελέγχου, ενημερώνοντάς την με τον τρόπο αυτόν για τις διαπιστωμένες αποκλίσεις της σε σχέση με την κείμενη νομοθεσία και την εγκεκριμένη από την ΑΔΑΕ Πολιτική Ασφάλειας αυτής.

Τέλος, οι ισχυρισμοί της εταιρείας αναφορικά με την πάροδο ευλόγου χρόνου για τη διεξαγωγή της ακρόασης, κατά παράβαση της αρχής της εύλογης διάρκειας της διαδικασίας, προβάλλονται αβασίμως. Και τούτο διότι η διάταξη του άρθρου 10 παρ. 5 του Κώδικα Διοικητικής Διαδικασίας ορίζει ότι: «οι προθεσμίες για τη Διοίκηση είναι ενδεικτικές, εκτός αν από τις διατάξεις που τις προβλέπουν προκύπτει ότι είναι αποκλειστικές. Οι προθεσμίες για την έκδοση ατομικών διοικητικών πράξεων, δυσμενών για το πρόσωπο που αφορούν αμέσως, είναι αποκλειστικές». Έχει κριθεί από τη νομολογία ότι, ακόμη και ο ρητός χαρακτηρισμός μιας προθεσμίας ως αποκλειστικής, είναι δυνατόν, από τον συνδυασμό των σχετικών με την αρμοδιότητα διατάξεων, να προκύπτει ότι ο χαρακτηρισμός αυτός έχει απλώς την έννοια της έντονης υπόδειξης προς τη Διοίκηση για ταχεία ενέργεια (ΣτΕ 2079/1987, 245/2014, 4480/2014, και πρβλ ΣτΕ 2572, 2758/2015, 3073/2012, 1967/2011 7μελούς, Διοικ. Εφ. Αθ. 3598/2018 -Τμήμα 14^ο Τριμελές). Σε κάθε περίπτωση όμως, εν προκειμένω, δεν προβλέπεται από το Ν. 3115/2003, ο οποίος ορίζει την αρμοδιότητα της ΑΔΑΕ και προβλέπει τη δυνατότητα επιβολής κυρώσεων από αυτήν, προθεσμία για την επιβολή των εν λόγω κυρώσεων. Επομένως, δεν μπορεί να υποστηριχθεί ότι υφίσταται εκ του νόμου συγκεκριμένη προθεσμία για το χρόνο διενέργειας της ακρόασης και την επιβολή κύρωσης από την ΑΔΑΕ, η οποία, βάσει του άρθρου 10 παρ. 5 του Κ.Διοικ. Δ. είναι αποκλειστική ως δυσμενής για το διοικούμενο διοικητική πράξη. Επίσης, η διάταξη του άρθρου 2 του Κ.Διοικ. Δ. στην οποία προβλέπεται ότι τα διοικητικά όργανα οφείλουν να προβαίνουν σε ενέργειες που προβλέπονται από τις ισχύουσες διατάξεις εντός ευλόγου χρόνου, ο οποίος δεν μπορεί να υπερβεί το τρίμηνο, αφορά στη συντέλεση εκ μέρους της Διοίκησης των πράξεων οφειλομένης νόμιμης ενέργειας, όταν η αρμοδιότητά της είναι δεσμία και όχι στην περίπτωση της κύρωτικής αρμοδιότητας της Διοίκησης κατά την οποία ενεργεί κατά διακριτική ευχέρεια. Ως εκ τούτου, η ανωτέρω διάταξη του άρθρου 10 παρ 5 εδ. Β του Κ.Διοικ. Δ. δεν δύναται να συσχετισθεί και να τύχει εφαρμογής επί της διατάξεως του άρθρου 2 του ίδιου Κώδικα, η οποία, αποσκοπούσα μόνο στην επιτάχυνση των διοικητικών ενεργειών, δεν θεσπίζει γενική αποκλειστική

προθεσμία τριών μηνών για την έκδοση δυσμενών διοικητικών πράξεων, η υπέρβαση της οποίας θα καθιστούσε την οικεία αρχή άνευ ετέρου αναρμόδια κατά χρόνο, αλλά υπόδειξη προς τη Διοίκηση για την εντός ευλόγου χρόνου ολοκλήρωση των αυτεπάγγελτων ενεργειών της. Εξάλλου, στην περίπτωση των Ανεξαρτήτων Αρχών δεν εφαρμόζονται οι προθεσμίες του Κώδικα Διοικητικής Διαδικασίας που αφορούν στα συλλογικά διοικητικά όργανα.

II. Αναφορικά με τις αποδιδόμενες παραβάσεις στην απόφαση για κλήση σε ακρόαση.

1) Επί του ιστορικού

Η εταιρεία επί του πραγματικού της εν θέματι υπόθεσης αναφέρει ότι όταν περιήλθε σε γνώση της, στις 17.05.2015, άρθρο δημοσιευμένο στο Site ██████████ ενημερώθηκαν άμεσα οι αρμόδιες υπηρεσίες και ξεκίνησε η σχετική διερεύνηση. Στο πλαίσιο των ενεργειών της εταιρείας βρέθηκαν περίπου 3800 CPEs (Customer Premises Equipment) με ανοιχτή θύρα 80, με απενεργοποιημένο το mini-firewall και ανοιχτή την πρόσβαση στο WAN. Τα συγκεκριμένα CPEs είχαν διατεθεί σε περίπου 756.700 συνδρομητές. Ο τεχνικός έλεγχος της εταιρείας κατέληξε στο συμπέρασμα ότι δεν υπήρξε οποιοσδήποτε κίνδυνος για το απόρρητο των συνδρομητών της και καμία πιθανότητα απομακρυσμένης παρέμβασης μέσω των εν θέματι συσκευών. Κατά τον έλεγχο που διεξήγαγε η Αρχή στις 21.09.2015 ζητήθηκαν και παραδόθηκαν, μεταξύ άλλων: α) Οι κατασκευάστριες εταιρείες CPEs που προμηθεύουν τον ΟΤΕ από 1/1/2013 (ZTE HELLAS COMMUNICATIONS και SERCOMM CORPORATION για τα μοντέλα ZTE-931VII, ZTE-H108NS και SERCOMM-W724-Type-Ci), β) οι τεχνικές προδιαγραφές των CPEs, γ) οι διαδικασίες ελέγχου των CPEs από τον ΟΤΕ σε εργαστηριακό περιβάλλον πριν τη διάθεσή τους στους συνδρομητές που αφορούν τη συμμόρφωση της κατασκευάστριας εταιρείας με τις προδιαγραφές που της έχουν τεθεί. Μετά τη διάθεση από την εταιρεία ZTE του νέου firmware (quick fix) και τις σχετικές δοκιμές, ξεκίνησε, για λόγους αποκλειστικά προληπτικούς, η εγκατάστασή του μέσω της πλατφόρμας TR-069 στα routers, η οποία ολοκληρώθηκε στις 24.06.2015. Στις 26.06.2015 πραγματοποιήθηκε η αποστολή ενημερωτικού email προς τους συνδρομητές που διαθέτουν H108NS (συνημ.1) η οποία αφορούσε στην αλλαγή κωδικού πρόσβασης (βλ. σχετική αναφορά στο υπ' αριθμ. Πρωτ. ΑΔΑΕ ΕΜΠ 118/23.05.2018 Υπόμνημα της εταιρείας σελ. 3 και σχετ. αναφορά στο από 21.02.2018 Πρακτικό Ακρόασης σελ. 3,4, 5,6,7).

Πλην όμως, ο ισχυρισμός της εταιρείας ότι «Ο τεχνικός έλεγχος της εταιρείας μας κατέληξε στο συμπέρασμα ότι δεν υπήρξε οποιοσδήποτε κίνδυνος για το απόρρητο των συνδρομητών της εταιρείας και καμία πιθανότητα απομακρυσμένης παρέμβασης μέσω των εν θέματι συσκευών» έρχεται σε ευθεία αντίθεση με τη δήλωση των εκπροσώπων της κατά τον από 21.09.2015 επιτόπιο έλεγχο σύμφωνα με την οποία η γνώση του δεύτερου λογαριασμού αρκούσε για την απομακρυσμένη πρόσβαση τρίτου, στην περίπτωση που ο χρήστης είχε εν γνώσει του απενεργοποιήσει τους παραπάνω μηχανισμούς ασφάλειας. Επισημαίνεται ότι ο αριθμός των πελατών της που διέθεταν το εν λόγω CPE κατά τον έλεγχο που πραγματοποιήθηκε, ανέρχονταν σε 756.700 περίπου (επί συνόλου πελατειακής βάσης περίπου 1.200.000), εκ των οποίων οι 3.800 είχαν απενεργοποιήσει το mini firewall και είχαν ανοίξει την πρόσβαση στο WAN.

Επίσης ο ισχυρισμός ότι ακολουθήθηκαν «οι διαδικασίες ελέγχου των CPEs από τον ΟΤΕ σε εργαστηριακό περιβάλλον πριν τη διάθεσή τους στους συνδρομητές που αφορούν τη συμμόρφωση της κατασκευάστριας εταιρείας με τις προδιαγραφές που της έχουν τεθεί» δεν επιβεβαιώνεται στο συνημ. 3 του υπ' αριθμ. πρωτ.ΑΔΑΕ ΑΠΡ 4003/09.10.2015 έγγραφο της εταιρείας, καθόσον δεν προκύπτουν οι απαραίτητοι έλεγχοι της εταιρείας στα εν λόγω ZTE CPE (ZTE H108N), δηλαδή οι δοκιμές της διαμόρφωσης των απαιτήσεων ασφάλειας και η έκθεση αποδοχής μετά την επιτυχή ολοκλήρωση των δοκιμών κατά παράβαση των παρ. 8.3.2.1. και 8.3.2.2 της υπ' αριθμ. 165/2011 Απόφασης της Αρχής.

Αναφορικά με το εάν έλαβαν χώρα οι απαιτούμενοι έλεγχοι από την εταιρεία και εάν εντοπίστηκε ο δεύτερος κοινός λογαριασμός πριν την παράδοση των συσκευών στους συνδρομητές της, η εταιρεία κατά την ακρόασή της δήλωσε ότι: «..δεν το πιάσαμε, γιατί δεν μας ενδιέφερε. Εμείς πήραμε αυτά που θέλαμε. Όταν βλέπεις ότι υπάρχει ένα δεύτερο account. Το πιάσαμε πώς; Μπορεί να το έχουμε δει αλλά εμάς αυτό δεν μας έδωσε κάποιο threat ότι υπάρχει εδώ πέρα κάποιο bug ή κάποιο δεύτερο account μέσα. Υπάρχει, το έχω δει απλώς εμένα αυτό δεν μου χτύπησε καμpanάκι γιατί δεν έχω password μέσα να το ενεργοποιήσω και δεν μπορείς να έχεις δύο account στον ίδιο router άρα από την πλευρά της ασφάλειας εμείς το είχαμε τσεκάρει και είπαμε OK, δεχόμαστε ότι υπάρχει και αυτό αλλά δεν είναι κάτι ενεργό, όταν το είδαμε πάλι με τα εργαστήρια, είπαμε βεβαίως, αλλά αυτό είναι κάτι το οποίο εμάς δεν μας απασχολεί γιατί δεν είναι ενεργό..» (βλ. το από 21.02.2018 Πρακτικό Ακρόασης σελ.8).

Πλην όμως, η ανωτέρω δήλωση περί προηγούμενης γνώσης και εντοπισμού του επιπρόσθετου λογαριασμού κατά τις δοκιμές δεν αποδεικνύεται από τα προσκομιζόμενα από την εταιρεία έγγραφα δοκιμών και έρχεται σε αντίθεση με τις δηλώσεις της εταιρείας, τόσο κατά τον επιτόπιο έλεγχο, όσο και στο υπ' αριθμ. Πρωτ. ΑΔΑΕ ΕΜΠΙ 118/23.05.2018 Υπόμνημά της, όπου ρητά αναφέρει ότι ενημερώθηκε για την ύπαρξη του επιπρόσθετου λογαριασμού την 17.05.2015, από άρθρο δημοσιευμένο στο Site [REDACTED]. Ωστόσο, ακόμα και αν είχε εντοπισθεί ο εν λόγω λογαριασμός στα δοκιμαστικά τεστ της εταιρείας, ο ισχυρισμός της εταιρείας ότι η ίδια δεν θορυβήθηκε για την ύπαρξή του διότι «δεν έχω password μέσα να το ενεργοποιήσω» προβάλλεται αβασίμως δεδομένου ότι με τη γνώση του password και της IP διεύθυνσης του συνδρομητή που είχε απενεργοποιήσει το mini firewall δινόταν η δυνατότητα στον κακόβουλο τρίτο να αποκτήσει πρόσβαση στον router.

Επιπροσθέτως, επισημαίνεται ότι σύμφωνα με δηλώσεις της εταιρείας κατά τη διενέργεια της ακρόασης (βλ. το από 21.02.2018 Πρακτικό Ακρόασης σελ 8) ο επίμαχος λογαριασμός που εντοπίστηκε κατά τη διάρκεια των δοκιμών είναι τύπου απλού «user», επομένως μπορεί να χρησιμοποιηθεί από οποιονδήποτε ακόμα και τον συνδρομητή εάν γνωρίζει το όνομα και τον κωδικό πρόσβασής του και αφορά «υπηρεσία» αφού δίνει δυνατότητα πρόσβασης στην υπηρεσία διαχείρισης των CPE. Από τα ανωτέρω προκύπτει ότι για τον εν λόγω λογαριασμό η εταιρεία όφειλε να τηρεί τις προβλεπόμενες στην παρ. 6.5.2. της υπ' αριθμ. 165/2011 Απόφασης της ΑΔΑΕ διαδικασίες διαχείρισης των λογαριασμών πρόσβασης.

Πλην όμως, από το σύνολο των στοιχείων του φακέλου της εν θέματι ακρόασης η εταιρεία δεν προέβη στη σχετική συμμόρφωση, καθώς δεν τηρήθηκε η ορθή διαδικασία για τον τρόπο προσθήκης του λογαριασμού, απόδοσης του ονόματος χρήστη και του κωδικού πρόσβασης σε αυτόν και αποτροπής του εύκολου προσδιορισμού του εν λόγω κωδικού.

Τέλος, ο ισχυρισμός της εταιρείας ότι ενημέρωσε τους συνδρομητές προβάλλεται αβασίμως, δεδομένου ότι το μήνυμα ηλεκτρονικού ταχυδρομείου που απέστειλε την 26.06.2015, δεν αφορούσε το εν θέματι περιστατικό ασφάλειας, ούτε τις προβλεπόμενες από την παρ. 9.2.2. (ι, ια) οδηγίες ή συστάσεις προς τους 3.800 θιγόμενους που είχαν απενεργοποιήσει το mini firewall, αλλά περιορίζεται στην καθιερωμένη, συνήθη, περιοδική προειδοποίηση αλλαγής κωδικού πρόσβασης, λόγω παρέλευσης 6μήνου.



2) Έλλειψη νόμιμης δικαιολογητικής βάσης για επιβολή κύρωσης- Καμία Παραβίαση της εγκεκριμένης με την υπ' αριθμ. 294/2013 απόφασή σας Πολιτικής Ασφάλειας του ΟΤΕ μέσω της παραβίασης επιμέρους διαδικασιών αυτής.

Η εταιρεία ισχυρίζεται ότι: «...δεν συνέτρεξε νόμιμος λόγος ευθύνης του ΟΤΕ, πρωτίστως διότι δεν έλαβε χώρα καμία παράβαση βάσει προϋπάρχοντος και σαφώς καθορισμένου κανόνα δικαίου, ούτε υπήρξε οποιαδήποτε επίπτωση στο απόρρητο των επικοινωνιών. Επιπλέον, δεν υπήρξε οποιοδήποτε κενό ως προς την εφαρμογή της Πολιτικής Διασφάλισης Απορρήτου (ΠΔΑ) του ΟΤΕ» (βλ. το υπ' αριθμ. Πρωτ. ΑΔΑΕ ΕΜΠ 118/23.05.2018 Υπόμνημα της εταιρείας σελ. 3, 4).

Εν προκειμένω, η εταιρεία προβαίνει σε μια γενική επί του θέματος τοποθέτηση. Ωστόσο, οι τερματικές συσκευές (CPEs) αποτελούν σημαντικά δικτυακά συστήματα για την πραγματοποίηση της επικοινωνίας, τα οποία πριν από την παράδοσή τους στους τελικούς συνδρομητές παραμετροποιούνται από τον πάροχο και στη συνέχεια, μετά την παράδοση και εγκατάστασή τους στο χώρο του συνδρομητή, υπόκεινται σε απομακρυσμένη διαχείριση από τον πάροχο (ΟΤΕ). Ως εκ τούτου, οι πάροχοι οφείλουν να λαμβάνουν τα ενδεδειγμένα μέτρα ασφάλειας για την προστασία των τερματικών συσκευών (CPEs) που διαθέτουν στους πελάτες τους, καθώς και για την ασφαλή απομακρυσμένη πρόσβαση των παρόχων στο τερματικό εξοπλισμό των συνδρομητών τους (CPEs). Υπό το πρίσμα αυτό, η ΑΔΑΕ απέστειλε προς τους ελεγχόμενους παρόχους με την από 21.11.2016 Έκθεση Ελέγχου κατευθυντήριες οδηγίες για την ενίσχυση ασφάλειας των εν λόγω συσκευών, οι οποίες εξειδικεύουν τεχνικά τις γενικές απαιτήσεις της υπ' αριθμ. 165/2011 Απόφασης της Αρχής, λόγω της τεχνολογικής τους ιδιαιτερότητας.

Ως προς το ζήτημα της διακινδύνευσης και των επιπτώσεων που είχε το εν θέματι περιστατικό ασφάλειας στο απόρρητο της επικοινωνίας, ο ισχυρισμός της εταιρείας προβάλλεται αβασίμως, λόγω του γεγονότος ότι η ίδια δήλωσε ότι 3.800 συνδρομητές της, οι οποίοι είχαν απενεργοποιήσει το τοίχος ασφαλείας (mini firewall) και είχαν ανοίξει την πρόσβαση στο WAN, με τη γνώση του επιπρόσθετου λογαριασμού πρόσβασης που εντοπίστηκε, ήταν ευάλωτοι και ως εκ τούτου έτιθετο το απόρρητο της επικοινωνίας τους σε διακινδύνευση.

Α. Άρνηση του γεγονότος της διακινδύνευσης του απορρήτου των επικοινωνιών-Δεν συντρέχει λόγος εφαρμογής της ισχύουσας νομοθεσίας αναφορικά με τα περιστατικά ασφάλειας (Ν. 3471/2006, άρθρο 9 Απόφασης 165/2011).

Η εταιρεία ισχυρίζεται ότι δεν συνέτρεξε οποιαδήποτε περίπτωση κατά την οποία θα μπορούσε να στοιχειοθετηθεί περιστατικό ασφάλειας για τους παρακάτω λόγους:

«Γιατί δεν υπήρξε τρόπος να αποκτηθεί πρόσβαση στον δρομολογητή (router) του πελάτη (Custoemer Premises Equipment – CPE), αφού είναι πρακτικά αδύνατο να γίνουν γνωστοί οι κρυπτογραφημένοι – κωδικοί πρόσβασης.(βλ. το υπ’αριθμ. Πρωτ. ΑΔΑΕ ΕΜΠ 118/23.05.2018 Υπόμνημα της εταιρείας σελ. 4)».

Πλην όμως, ο ανωτέρω ισχυρισμός της εταιρείας προβάλλεται αβασίμως. Και τούτο διότι, στο από 21.09.2015 πρακτικό επιτόπιου ελέγχου αναφέρεται ότι η γνώση της δημόσιας IP διεύθυνσης σε συνδυασμό με την απενεργοποίηση των μηχανισμών ασφάλειας της εταιρείας και γνώση του password επέτρεπε την απομακρυσμένη πρόσβαση στους εν λόγω δρομολογητές τρίτων με τη χρήση του επιπρόσθετου λογαριασμού πρόσβασης. Επίσης, η χρήση κρυπτογράφησης, εν προκειμένω, δεν επηρεάζει τη δυνατότητα πρόσβασης τρίτου αφ’ής στιγμής γίνει γνωστός ο κοινός κωδικός που έφεραν τα CPE (ZTE H108N) που είχαν προμηθευτεί από την εταιρεία 756.700 συνδρομητές της.

«Δεν υπήρξε κίνδυνος ασφάλειας για προσωπικά δεδομένα και δεδομένα επικοινωνίας, εφόσον αυτά δεν αποθηκεύονται στις συγκεκριμένες συσκευές. Ειδικότερα, οι routers δεν αποθηκεύουν δεδομένα πελατών (πχ σελίδες που επισκέπτεται ο χρήστης, passwords Internet εφαρμογών κλπ), συνεπώς, τέτοια στοιχεία δεν είναι προσβάσιμα από κανένα λογαριασμό (ούτε μέσω του χρήστη admin).(βλ. το υπ’αριθμ. Πρωτ. ΑΔΑΕ ΕΜΠ 118/23.05.2018 Υπόμνημα της εταιρείας σελ. 4)».

Πλην όμως, ο ως άνω ισχυρισμός είναι αβάσιμος, λόγω του γεγονότος ότι παράνομη πρόσβαση σε μία τερματική συσκευή (CPE) μπορεί να επιφέρει σημαντική διακινδύνευση του απορρήτου, όπως για παράδειγμα ο κακόβουλος χρήστης να καταργήσει το τοπικό ανάχωμα ασφάλειας (firewall) του CPE και από το περιβάλλον διαχείρισης του CPE να αλλάξει τον Σύστημα Ονοματοδοσίας Διαδικτύου (DNS) με αποτέλεσμα η δικτυακή κίνηση του συνδρομητή να διέρχεται από τρίτους διακομιστές (servers) αγνώστου προέλευσης ή ακόμα να εφαρμόσει κανόνες port forwarding στο CPE (ενεργοποίηση συγκεκριμένων θυρών (ports) με σκοπό την απόκτηση πρόσβασης από εφαρμογές που χρειάζονται τις συγκεκριμένες θύρες (ports), ώστε να λειτουργήσουν), με αποτέλεσμα να υπάρξει το ενδεχόμενο παραβίασης των τερματικών συσκευών στο εσωτερικό δίκτυο του συνδρομητή, ιδίως εάν οι συσκευές δεν έχουν

ενεργοποιημένο το δικό τους ανάχωμα ασφάλειας (firewall) ή ενεργοποιημένο κωδικό πρόσβασης.

«Το πλήθος των συνδρομητών, οι οποίοι ενδεχομένως θα μπορούσαν να επηρεαστούν στην περίπτωση που τα ανωτέρω δεν ίσχυαν, γεγονός που αρνούμεθα εξ ολοκλήρου, ήταν πολύ μικρό (0,3% της συνδρομητικής βάσης). Οι συγκεκριμένοι εν γνώσει τους είχαν απενεργοποιήσει τον διπλό μηχανισμό ασφάλειας που είναι εξ ορισμού εγκατεστημένος από τον ΟΤΕ, είχαν παρακάμψει δηλαδή τις αρχικές ρυθμίσεις ασφαλείας. Στους διαδικτυακούς τόπους της εταιρείας υπάρχει σχετική ενημέρωση για τους κινδύνους που υπάρχουν όταν απενεργοποιούνται οι μηχανισμοί ασφάλειας (συν. 2- screenshot από τις οδηγίες για το mini-firewall)(βλ. το υπ' αριθμ. Πρωτ. ΑΔΑΕ ΕΜΠ 118/23.05.2018 Υπόμνημα της εταιρείας σελ. 4)».

Πλην όμως, ο ανωτέρω ισχυρισμός της εταιρείας ενισχύει την αναγκαιότητα λήψης μέτρων από την εταιρεία για την ασφάλεια του δικτύου της και την τήρηση των διαδικασιών που όφειλε να ενεργοποιήσει από την εκδήλωση του εν λόγω περιστατικού ασφάλειας, όπως την υποχρέωση ενημέρωσης των 3.800 θιγόμενων συνδρομητών της, οι οποίοι όντες ανυποψίαστοι για την ύπαρξη επιπρόσθετου κοινού για το σύνολο των CPE (ZTE H108N) κωδικού πρόσβασης προέβησαν σε ενέργειες που ενδεχομένως δεν θα επέλεγαν εάν γνώριζαν τις επιπτώσεις που θα είχαν αυτές στο απόρρητο των επικοινωνιών τους.

«Δεν υπήρξε καμία «ευπάθεια» στο δίκτυο του ΟΤΕ. Η εταιρεία είχε λάβει όλα τα απαιτούμενα μέτρα ασφάλειας για την προστασία των χρηστών του δικτύου της» (βλ. το υπ' αριθμ. Πρωτ. ΑΔΑΕ ΕΜΠ 118/23.05.2018 Υπόμνημα της εταιρείας σελ. 4).

Πλην όμως, ο ανωτέρω ισχυρισμός προβάλλεται αβασίμως. Και τούτο διότι η εταιρεία είτε δεν προέβη σε διαδικασία δοκιμών με σκοπό τη διαμόρφωση των απαιτήσεων ασφάλειας προς την κατασκευάστρια εταιρεία και τη σύνταξη έκθεσης αποδοχής μετά την επιτυχή ολοκλήρωση των δοκιμών αυτών, με αποτέλεσμα το εν θέματι περιστατικό να μην εντοπιστεί και να περιέλθει σε γνώση της εταιρείας από δημοσιευμένο άρθρο, στο διαδίκτυο (σύμφωνα με την αρχική της δήλωση στον επιτόπιο έλεγχο), είτε η ύπαρξη πρόσθετου κωδικού πρόσβασης, κοινού για όλες τις συσκευές CPE (ZTE H108N) δεν αξιολογήθηκε, ορθά από την εταιρεία στο πλαίσιο αποτίμησης κινδύνου κατά το στάδιο των δοκιμών που, κατά μεταγενέστερη δήλωσή της στην ακρόαση,

προηγήθηκαν της παράδοσής τους στους συνδρομητές. Σημειωτέον ότι από το σύνολο των στοιχείων του φακέλου της εν λόγω υπόθεσης, δεν αποδεικνύεται η ορθή εφαρμογή της προβλεπόμενης στις παρ. 8.3.2.1. και 8.3.2.2 της υπ' αριθμ. 165/2011 Απόφασης της Αρχής διαδικασίας. Επίσης, ο ισχυρισμός της εταιρείας ότι η κατασκευάστρια εταιρεία προμηθεύει operators σε όλο τον κόσμο με το συγκεκριμένο «βιομηχανικό setting» (βλ. το από 21.02.2018 Πρακτικό Ακρόασης σελ.5), ουδόλως αιτιολογεί την υποβάθμιση της σπουδαιότητας ύπαρξης κοινού λογαριασμού, και κατ'έπекταση τη μη διαχείριση του εν λόγω συμβάντος ως περιστατικού ασφάλειας, το οποίο είχε ως αποτέλεσμα τη μη ενημέρωση των θιγόμενων συνδρομητών της και της ΑΔΑΕ.

Από τα ανωτέρω συνάγεται ότι οι κοινοί κωδικοί πρόσβασης στις τερματικές συσκευές CPE επέτρεπαν την απομακρυσμένη πρόσβαση σε τρίτο έστω και εάν αυτός δεν γνώριζε τον προσωπικό κωδικό διαχείρισης του κάθε CPE.

Β) Καμία παραβίαση της Πολιτικής Διαχείρισης Περιστατικών Ασφάλειας (σελ. 15-16 της εγκεκριμένης Πολιτικής ασφάλειας του ΟΤΕ) και της Πολιτικής Ελέγχου Εφαρμογής της Πολιτικής Ασφάλειας (σελ. 19-20 της Πολιτικής Ασφάλειας του ΟΤΕ)- Καμία παραβίαση της Πολιτικής Διαχείρισης και Εγκατάστασης Συστημάτων (σελ. 13-14 της Πολιτικής Ασφάλειας του ΟΤΕ).

Η εταιρεία εν προκειμένω ισχυρίζεται ότι τήρησε τις εσωτερικές της διαδικασίες και έλαβε τα απαιτούμενα μέτρα ασφάλειας για την αποφυγή διακινδύνευσης του απορρήτου των επικοινωνιών. Επιπροσθέτως, είχαν ληφθεί όλα τα προσήκοντα μέτρα ασφάλειας και είχαν γίνει όλοι οι απαιτούμενοι έλεγχοι. Τα σχετικά έγγραφα με τις προδιαγραφές ασφάλειας έχουν παραδοθεί κατά τους ελέγχους. Παρά το γεγονός ότι δεν υπήρξε οποιαδήποτε υπόνοια για διακινδύνευση του απορρήτου, ούτε πιθανότητα κινδύνου για το εσωτερικό δίκτυο συνδρομητών, ξεκίνησε άμεσα η κατασκευή νέου firmware, για λόγους επικοινωνιακούς και για την αποφυγή συνέχισης των δημοσιευμάτων. 2) Σύμφωνα με τους γενικώς παραδεκτούς κανόνες ασφάλειας, ήταν αδύνατο να πραγματοποιηθεί οποιαδήποτε παραβίαση/απόκτηση ελέγχου σε router, ακόμα και σε αυτόν που ο χρήστης είχε απενεργοποιήσει τα δύο αναχώματα ασφαλείας, που παρέχονται από την εταιρεία, καθώς α) ο επιπλέον λογαριασμός αφορούσε μόνο στην ύπαρξη ενός ονόματος πρόσβασης (username) στον router, β) ο επίδοξος «εισβολέας» θα έπρεπε να γνωρίζει τον κωδικό πρόσβασης στον λογαριασμό, γεγονός αδύνατο, καθώς αυτός ήταν κρυπτογραφημένος, γ) η

απομακρυσμένη πρόσβαση σε στοχευμένα CPEs θα απαιτούσε και γνώση της δημόσιας IP διεύθυνσής τους, γεγονός επίσης αδύνατο, δ) ακόμα και στην απίθανη περίπτωση ανακάλυψης του κωδικού πρόσβασης, η κακόβουλη ενέργεια δεν θα είχε κανένα απολύτως αποτέλεσμα εφόσον δεν αποθηκεύονται προσωπικά δεδομένα και δεδομένα επικοινωνίας στον router. 3) Δεν υπήρξαν θιγόμενοι συνδρομητές. Τούτο αποδεικνύεται τόσο από την παντελή έλλειψη αναφορών και παραπόνων όσο και από το ίδιο το δημοσίευμα το οποίο δεν φέρει ίχνος απόδειξης για τα διαλαμβανόμενα σε αυτό γεγονότα (βλ. σχετ. αναφορές στο υπ' αριθμ. Πρωτ. ΑΔΑΕ ΕΜΠ118/23.05.2018 Υπόμνημα της εταιρείας σελ. 5, 6).

Πλην όμως, οι ανωτέρω ισχυρισμοί προβάλλονται αβασίμως, για τους λόγους που ήδη έχουν διατυπωθεί ανωτέρω. Επανερχόμενοι στον ισχυρισμό της εταιρείας ότι ήταν αδύνατο να πραγματοποιηθεί οποιαδήποτε παραβίαση/απόκτηση ελέγχου σε router, ακόμα και σε αυτόν που ο χρήστης είχε απενεργοποιήσει τα δύο αναχώματα ασφαλείας, που παρέχονται από την εταιρεία, επισημαίνονται τα ακόλουθα: Ως προς το (α) εφόσον κάποιος γνωρίζει τον κοινό κωδικό πρόσβασης με τη χρήση αυτού μπορεί να αποκτήσει πρόσβαση, ως προς το (β) ο εν λόγω κωδικός πρόσβασης είναι κοινός και εφόσον διαρρεύσει, είναι αδιάφορο εάν είναι κρυπτογραφημένος, ως προς το (γ) στην περίπτωση που τα firewall είναι απενεργοποιημένα ο «εισβολέας» μπορεί να «σκανάρει» τις IP δ/νσεις του ΟΤΕ με αποτέλεσμα αυτές να ανταποκριθούν και άρα ο «εισβολέας» να εντοπίσει τις IP δ/νσεις που έχουν ανταποκριθεί και να εκδηλώσει την επίθεσή του ως προς το δ) εφόσον ο εισβολέας αποκτήσει πρόσβαση δύναται να προβεί σε διάφορες ενέργειες όπως να αλλάξει τοDNS στον router ή να ενεργοποιήσει τη διαδικασία port forwarding.

Τέλος, όπως έχει ήδη επισημανθεί, από τα ανωτέρω συνάγεται ότι οι κοινοί κωδικοί πρόσβασης στις τερματικές συσκευές CPE επέτρεπαν την απομακρυσμένη πρόσβαση σε τρίτο, έστω και εάν αυτός δεν γνώριζε τον προσωπικό κωδικό διαχείρισης του κάθε CPE.

Γ) Καμία παραβίαση του άρθρου 12 Ν. 3471/2006 και του άρθρου 9 της Απόφασης 165/2011 αναφορικά με τη δήθεν μη ενημέρωση των συνδρομητών

Η εταιρεία εν προκειμένω ισχυρίζεται ότι στο άρθρο 12 παρ. 2 ν. 3471/2006 ορίζεται ότι ο φορέας που παρέχει διαθέσιμη στο κοινό υπηρεσία ηλεκτρονικών επικοινωνιών οφείλει να ενημερώσει τους συνδρομητές μόνο εφόσον υπάρχει «ιδιαίτερος κίνδυνος παραβίασης της ασφάλειας του δημοσίου δικτύου». Εν προκειμένω, όπως αποδεικνύεται

από τα ανωτέρω αναφερόμενα, δεν υφίστατο τέτοιος κίνδυνος. Η ως άνω διάταξη υπερέχει της αντίστοιχης διάταξης του άρθρου 2 της υπ' αριθμ. 165/2011 Απόφασής σας (ορισμός του περιστατικού ασφάλειας) και του άρθρου 9 αυτής. Ο πάροχος υποχρεούται να χειριστεί συγκεκριμένο γεγονός ως περιστατικό ασφάλειας και να το ανακοινώσει στην Αρχή Σας και τον συνδρομητή, μόνο αν υφίσταται εύρημα που να συνιστά διακινδύνευση του απορρήτου των επικοινωνιών στο δικό του δίκτυο. Εν προκειμένω δεν έλαβε χώρα τέτοιο περιστατικό. Απαραίτητη προϋπόθεση για την κοινοποίηση ενός περιστατικού είναι επίσης η προηγούμενη στοιχειώδης εκτίμηση της σοβαρότητάς του. Η εσωτερική Διαδικασία Διαχείρισης Περιστατικών ασφάλειας επιβάλλει, πριν την ανάληψη οποιασδήποτε ενέργειας, την αξιολόγηση του βαθμού επικινδυνότητας και προϋποθέτει την ύπαρξη αποδεικτικών στοιχείων. Επικουρικά αναφέρεται ότι οι συνδρομητές ενημερώθηκαν για την αλλαγή κωδικού τους στο πλαίσιο προστασίας των λογαριασμών τους. Σύμφωνα άλλωστε με το άρθρο 12 Ν 3471/2006, ο πάροχος απαλλάσσεται από την υποχρέωση ενημέρωσης, εφόσον έχει λάβει τα κατάλληλα μέτρα ασφάλειας (βλ. σχετ. αναφορά στο υπ' αριθμ. Πρωτ. ΑΔΑΕ ΕΜΠ 118/23.05.2018 Υπόμνημά της εταιρείας σελ. 6, 7).

Πλην όμως, ο ως άνω ισχυρισμός της εταιρείας προβάλλεται αβασίμως. Και τούτο διότι τόσο από τη γενική διάταξη του άρθρου 12 του ν. 3471/2006 όσο και από την ειδική –ως κανονιστική ρύθμιση που αφορά ειδικότερα θέματα τεχνικής φύσεως -του άρθρου 2 της υπ' αριθμ. 165/2011 Απόφασής της ΑΔΑΕ απορρέει η ρητή υποχρέωση των παρόχων να ενημερώνουν τους συνδρομητές τους σε περίπτωση που υπάρχει κίνδυνος παραβίασης της ασφάλειας, η οποία θέτει σε διακινδύνευση το απόρρητο της επικοινωνίας. Εν προκειμένω, η εταιρεία με τους ισχυρισμούς της προσπαθεί να μειώσει τον βαθμό επικινδυνότητας του συμβάντος, το οποίο, όπως είχε αποδεχθεί και η ίδια κατά τον επιτόπιο έλεγχο, ήταν ικανό να παραβιάσει το απόρρητο της επικοινωνίας 3.800 συνδρομητών της που είχαν απενεργοποιήσει το firewall, μη γνωρίζοντας την ύπαρξη του πρόσθετου κοινού για όλες τις συσκευές λογαριασμού πρόσβασης των routers που είχαν προμηθευτεί από την εταιρεία και ο οποίος είχε διαρρεύσει. Οι προαναφερθείσες συνθήκες επιβάλλουν τη χωρίς καθυστέρηση ενημέρωση τόσο των 3.800 συνδρομητών που είχαν απενεργοποιήσει το firewall, όσο και του συνόλου των συνδρομητών της (756.700), δηλαδή οι μεν πρώτοι να το ενεργοποιήσουν και οι δεύτεροι να αποφύγουν οποιαδήποτε ενέργεια που ενδεχομένως θα δημιουργούσε ρωγμές στην ασφάλεια των routers. Ο ισχυρισμός της εταιρείας ότι

δεν ενημέρωσε τους συνδρομητές της, επειδή έλαβε τα κατάλληλα μέτρα ασφάλειας, είναι αβάσιμος, δεδομένου ότι η εταιρεία από την 17.05.2015 που έλαβε γνώση για τη διαρροή του πρόσθετου κοινού κωδικού πρόσβασης, την 22.05.2015 εγκατέστησε διορθωτικό λογισμικό στην ομάδα των πελατών της που είχαν απενεργοποιήσει τους μηχανισμούς ασφάλειας και από την 24.06.2015 ξεκίνησε τη μαζική εγκατάσταση και στους υπόλοιπους συνδρομητές. Όλο αυτό το χρονικό διάστημα, μέχρι την τελική επίλυση του προβλήματος οι συνδρομητές που διέθεταν το συγκεκριμένο μοντέλο router αγνοούσαν τον επαπειλούμενο κίνδυνο λόγω της παράλειψης της εταιρείας να τους ενημερώσει σχετικά. Επισημαίνεται ότι η εταιρεία ουδέποτε ενημέρωσε τους συνδρομητές της για το συγκεκριμένο περιστατικό ασφάλειας, ούτε έδωσε κατευθυντήριες οδηγίες και συστάσεις προστασίας τους, ως όφειλε, το δε μήνυμα ηλεκτρονικού ταχυδρομείου που απέστειλε την 26.06.2015 αφορούσε στην καθιερωμένη, συνήθη, περιοδική προειδοποίηση αλλαγής κωδικού πρόσβασης, λόγω παρέλευσης 6μήνου.

Δ) Παράνομη η όποια επιβολή κύρωσης χωρίς αποδεδειγμένη παραβίαση προϋπάρχοντα κανόνα δικαίου- In Dubio Pro Reo.

Η εταιρεία ισχυρίζεται ότι στο πλαίσιο της διοικητικής διαδικασίας η Αρχή οφείλει να κρίνει μόνο βάσει αποδεδειγμένων πραγματικών περιστατικών και συνδρομής, πέραν πάσης αμφιβολίας νόμιμου λόγου ευθύνης και όχι βάσει απλής πιθανολόγησης. Σε αντίθετη περίπτωση, η όποια κρίση της καθίσταται αυτοδικαίως αστήρικτη, μη νόμιμη και αντίθετη στην αρχή δικαίου in dubio pro reo. Η έλλειψη μιας πραγματικής και διαπιστωμένης αρνητικής επίπτωσης της συμπεριφοράς του ΟΤΕ στο απόρρητο των επικοινωνιών δεν δικαιολογεί την επιβολή εις βάρος του της όποιας διοικητικής κύρωσης (βλ. σχετ. αναφορά στο υπ' αριθμ. Πρωτ. ΑΔΑΕ ΕΜΠ 118/23.05.2018 Υπόμνημα της εταιρείας σελ. 7,8).

Πλην όμως ο ανωτέρω ισχυρισμός προβάλλεται αβασίμως, δεδομένου ότι η εταιρεία, όπως αποδείχθηκε από τον έλεγχο της Αρχής δεν εφήρμοσε συγκεκριμένες πολιτικές και διαδικασίες της εγκεκριμένης από την ΑΔΑΕ Πολιτικής Ασφάλειας («Πολιτική Διαχείρισης & Εγκατάστασης Συστημάτων», «Πολιτική Διαχείρισης Περιστατικών Ασφάλειας», «Πολιτική Ελέγχου Εφαρμογής της Πολιτικής Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών»),

κατά παράβαση του άρθρου 8, ιδίως παρ. 8.2.1, 8.2.3. του άρθρου 9, ιδίως παρ. 9.1., 9.2., 9.2.1, 9.2.2., 9.2.3 του άρθρου 11 της υπ' αριθμ. 165/2011 Απόφασης της ΑΔΑΕ και του ν. 3471/2006, όπως ισχύει με αποτέλεσμα να θέσει σε κίνδυνο το απόρρητο των επικοινωνιών των συνδρομητών της.

Ε) Έλλειψη οποιασδήποτε υπαιτιότητας του ΟΤΕ .

Η εταιρεία ισχυρίζεται ότι στην απίθανη περίπτωση που υπήρχε δυνατότητα αντικανονικής επέμβασης, γεγονός που το αρνείται, δεν υφίσταται η έννοια της υποκειμενικής ευθύνης καθώς η απενεργοποίηση των μηχανισμών ασφάλειας που παρέχονται από τον ΟΤΕ και υπάρχουν στις αρχικές ρυθμίσεις ασφάλειας, γίνονται με πρωτοβουλία του χρήστη. Συνεπώς διακόπτεται οποιοσδήποτε αιτιώδης σύνδεσμος καθώς μεσολαβεί ενέργεια του χρήστη (βλ. σχετ. αναφορά στο υπ' αριθμ. Πρωτ. ΑΔΑΕ ΕΜΠ 118/23.05.2018 Υπόμνημα της εταιρείας σελ. 8).

Πλην όμως, ο ανωτέρω ισχυρισμός είναι αβάσιμος. Και τούτο διότι οι συσκευές (routers) πριν χορηγηθούν στους συνδρομητές ελέγχονται από τον πάροχο, ο οποίος σε συνεννόηση με την κατασκευάστρια εταιρεία θέτει απαιτήσεις και προδιαγραφές σε αυτήν, προκειμένου να είναι οι συσκευές συμβατές με τα συστήματά του και να πληρούν τις προϋποθέσεις ασφάλειας. Στη συνέχεια, ο πάροχος οφείλει να προβεί σε δοκιμές υλοποίησης ή διαμόρφωσης των εν λόγω απαιτήσεων και εφόσον ολοκληρωθεί επιτυχώς η δοκιμαστική λειτουργία να γίνει η αποδοχή των συσκευών. Οι εν λόγω απαιτήσεις και κανόνες ασφάλειας των routers, λόγω και του γεγονότος ότι υπόκεινται σε απομακρυσμένη διαχείριση από τον πάροχο, δεν θα πρέπει να εξαρτώνται ή να επηρεάζονται από τυχόν ενέργειες των συνδρομητών, όπως ενεργοποίηση ή απενεργοποίηση firewall. Σε κάθε περίπτωση, η εταιρεία ΟΤΕ ως πάροχος ηλεκτρονικών επικοινωνιών αδειοδοτημένος από την Πολιτεία υπέχει πρόσθετες υποχρεώσεις έναντι της αυτής, μεταξύ των οποίων και την υποχρέωση διασφάλισης του απορρήτου των επικοινωνιών.

Ενόψει των ανωτέρω, για τις ανωτέρω πλημμέλειες, όπως ανωτέρω αναλύονται στα κεφάλαια Α' και Β' της παρούσας και ειδικότερα για την:

Παράβαση Α: Μη εφαρμογή της «Πολιτικής Διαχείρισης & Εγκατάστασης Συστημάτων» (Έκδοση 1.0-19/11/2012, σελ 13-14 της εγκεκριμένης Πολιτικής Ασφάλειας της εταιρείας ΟΤΕ) (Απόφαση 165/2011 της ΑΔΑΕ άρθρο 8, ιδίως παρ. 8.2.1, 8.2.3. αυτού), της «Πολιτικής Διαχείρισης Περιστατικών Ασφάλειας» (Έκδοση 1.0-19/11/2012, σελ 15-16 της εγκεκριμένης

Πολιτικής Ασφάλειας της εταιρείας ΟΤΕ) (Απόφαση 165/2011 της ΑΔΑΕ άρθρο 9, ιδίως παρ. 9.1., 9.2., 9.2.1, 9.2.2., 9.2.3.) και της «Πολιτικής Ελέγχου Εφαρμογής της Πολιτικής Ασφάλειας για τη Διασφάλιση του Απορρήτου των Επικοινωνιών», (Έκδοση 1.0-19/11/2012, σελ 19-20 της εγκεκριμένης Πολιτικής Ασφάλειας της εταιρείας ΟΤΕ) (Απόφαση 165/2011 της ΑΔΑΕ άρθρο 11), με αποτέλεσμα να θέσει σε κίνδυνο το απόρρητο των επικοινωνιών των συνδρομητών.

Παράβαση Β: Μη ενημέρωση των θιγόμενων συνδρομητών που επηρεάστηκαν από το περιστατικό ασφάλειας κατά παράβαση των προβλεπόμενων στο άρθρο 9 παρ. 9.2.2 στοιχ. (ι) της Απόφασης 165/2011 της ΑΔΑΕ («Πολιτική Διαχείρισης Περιστατικών Ασφάλειας», Έκδοση 1.0-19/11/2012, σελ 15 της εγκεκριμένης Πολιτικής Ασφάλειας της εταιρείας ΟΤΕ) και του Ν. 3471/2006, όπως τροποποιήθηκε και ισχύει.

Παράβαση Γ: Μη ενημέρωση της ΑΔΑΕ για το εν θέματι περιστατικό ασφάλειας κατά παράβαση των προβλεπόμενων στο άρθρο 9 παρ. 9.2.3 της Απόφασης 165/2011 της ΑΔΑΕ («Πολιτική Διαχείρισης Περιστατικών Ασφάλειας», Έκδοση 1.0-19/11/2012, σελ 16 της εγκεκριμένης Πολιτικής Ασφάλειας της εταιρείας ΟΤΕ) και του Ν. 3471/2006, όπως τροποποιήθηκε και ισχύει. (άρθρο 19 του Συντάγματος, Ν. 3115/2003 όπως ισχύει, Ν. 3471/2006, όπως τροποποιήθηκε και ισχύει, Απόφαση 165/2011 της ΑΔΑΕ),

Η ΑΡΧΗ ΔΙΑΣΦΑΛΙΣΗΣ ΤΟΥ ΑΠΟΡΡΗΤΟΥ ΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ
ΑΠΟΦΑΣΙΖΕΙ ΟΜΟΦΩΝΩΣ

Την ύπαρξη ευθύνης της εταιρείας «ΟΡΓΑΝΙΣΜΟΣ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ ΤΗΣ ΕΛΛΑΔΟΣ Α.Ε» (ΟΤΕ), για τις παραβάσεις της κείμενης νομοθεσίας σε σχέση με το απόρρητο των επικοινωνιών, όπως αναλύονται ανωτέρω.

ΕΠΙΒΑΛΛΕΙ ΟΜΟΦΩΝΩΣ

- 1) Για την Α΄ Παράβαση τη διοικητική κύρωση του χρηματικού προστίμου ύψους είκοσι χιλιάδων Ευρώ (20.000 Ευρώ) λαμβάνοντας υπόψη ιδίως την αρχή της αναλογικότητας, τη βαρύτητα της αποδιδόμενης παράβασης, καθώς και τα πρόσφατα οικονομικά στοιχεία της εταιρείας.
- 2) Για την Β΄ Παράβαση τη διοικητική κύρωση του χρηματικού προστίμου ύψους είκοσι χιλιάδων Ευρώ (20.000 Ευρώ) λαμβάνοντας υπόψη ιδίως την αρχή της αναλογικότητας, τη βαρύτητα της αποδιδόμενης παράβασης, καθώς και τα πρόσφατα οικονομικά στοιχεία της εταιρείας.



ΑΔΑΕ

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ

ΑΡΧΗ ΔΙΑΣΦΑΛΙΣΗΣ ΤΟΥ ΑΠΟΡΡΗΤΟΥ ΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ

3) Για την Γ΄ Παράβαση τη διοικητική κύρωση του χρηματικού προστίμου ύψους είκοσι χιλιάδων Ευρώ (20.000 Ευρώ) λαμβάνοντας υπόψη ιδίως την αρχή της αναλογικότητας, τη βαρύτητα της αποδιδόμενης παράβασης, καθώς και τα πρόσφατα οικονομικά στοιχεία της εταιρείας.

Η παρούσα Απόφαση της Α.Δ.Α.Ε. να επιδοθεί στην εταιρεία «ΟΡΓΑΝΙΣΜΟΣ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ ΤΗΣ ΕΛΛΑΔΟΣ Α.Ε.» (ΟΤΕ).

Ο Πρόεδρος

Χρήστος Ράμμος

DataJournalists