ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΑΡΧΗ ΔΙΑΣΦΑΛΙΣΗΣ ΤΟΥ ΑΠΟΡΡΗΤΟΥ ΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ

Μαρούσι, 28-06-2023

Αριθ. Πρωτ.: 2355

ΑΝΑΡΤΗΤΕΑ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

ΑΠΟΦΑΣΗ
(Αριθμ. 300/2023)

ΘΕΜΑ*:* Έγκριση της από 21.04.2023 Έκθεσης διενέργειας εκτάκτου ελέγχου στις εγκαταστάσεις της εταιρείας **«VODAFONE – ΠΑΝΑΦΟΝ ΑΕΕΤ»** σε συνέχεια του περιστατικού ασφαλείας με αριθμ. πρωτ. ΑΔΑΕ 2205/02.08.2021 και κλήση σε ακρόαση της εταιρείας με αντικείμενο τον έλεγχο ενδεχόμενης παραβάσεως της κείμενης νομοθεσίας περί απορρήτου των επικοινωνιών ενόψει του εν λόγω περιστατικού.

Την Τετάρτη, 21η Ιουνίου 2023, η Ολομέλεια της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών, παρισταμένων του Προέδρου κ. Χρήστου Ράμμου, του Αντιπροέδρου, κ. Μιχαήλ Σακκά, των τακτικών μελών κ.κ. Δημητρίου Βέργαδου, Νικολάου Παπαδάκη, Γεωργίου Μπακάλη και Αικατερίνης Παπανικολάου, καθώς και του αναπληρωματικού μέλους κας Βασιλικής Διαμαντοπούλου, η οποία προσήλθε προς αναπλήρωση του τακτικού μέλους κου Στέφανου Γκρίτζαλη, ο οποίος δεν προσήλθε λόγω κωλύματος, αν και είχε νομίμως και εμπροθέσμως προσκληθεί, συνήλθε σε συνεδρίαση προκειμένου αφενός να εγκρίνει την από 21.04.2023 Έκθεση διενέργειας εκτάκτου ελέγχου στις εγκαταστάσεις της εταιρείας «VODAFONE ΠΑΝΑΦΟΝ ΑΕΕΤ» κατόπιν της υπ' αριθμ. πρωτ. ΑΔΑΕ 2205/02.08.2021 αναφοράς περιστατικού σχετικά με συμβάν μη ζητηθείσας από τον νόμιμο συνδρομητή αντικατάστασης κάρτας sim στη σύνδεση κινητής τηλεφωνίας του, αφετέρου να αποφασίσει επί της ενδεχόμενης κλήσης σε ακρόαση της εν λόγω εταιρείας, με αντικείμενο τον έλεγχο της ενδεχόμενης παραβάσεως της κείμενης νομοθεσίας περί προστασίας του απορρήτου των επικοινωνιών.

Ειδικότερα:

Α. Στην Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών (Α.Δ.Α.Ε.) υπεβλήθη περιστατικό ασφάλειας από την εταιρεία «VODAFONE -ΠΑΝΑΦΟΝ Α.Ε.Ε.Τ.» με το με αρ. πρωτ. ΑΔΑΕ 2205/02.08.2021 έγγραφο αναφορικά με παραβίαση προσωπικών δεδομένων συνδρομητή και ειδικότερα με πραγματοποίηση αλλαγής κάρτας e-sim, κατόπιν σχετικού αιτήματος μέσω του λογαριασμού «My Account» του web portal ως μία οργανωμένη προσπάθεια απάτης SIM SWAP.

Για τη διερεύνηση του εν λόγω περιστατικού, με την υπ' αριθμ. 369/2021 Απόφαση της Ολομέλειας της Α.Δ.Α.Ε., ορίστηκε Ομάδα Ελέγχου η οποία ολοκλήρωσε το έργο της με τη σύνταξη της συνημμένης από

21.04.2023 «Έκθεσης Διενέργειας Εκτάκτου Ελέγχου στην εταιρεία VODAFONE ΠΑΝΑΦΟΝ ΑΕΕΤ σε συνέχεια του περιστατικού ασφαλείας με αριθμό πρωτοκόλλου ΑΔΑΕ 2205/02.08.2021».

Τα αποτελέσματα της εν λόγω έκθεσης ελέγχου έχουν ως εξής:

«Γ. <u>ΕΞΕΤΑΣΗ ΣΤΟΙΧΕΙΩΝ - ΑΠΟΤΕΛΕΣΜΑΤΑ ΕΛΕΓΧΟΥ</u>

Από τα στοιχεία του φακέλου, τον έλεγχο και τα δεδομένα που τέθηκαν υπόψη της ΟΕ, προκύπτουν τα ακόλουθα:

1. Η εταιρεία προσκόμισε τη διαδικασία (Συνημμένο 1 του Σχετικού 4) με την οποία εξυπηρετείται το αίτημα ενεργοποίησης e-SIM, που ήταν σε ισχύ κατά την ημερομηνία του περιστατικού (22.07.2021), με ειδική αναφορά στον τρόπο ενεργοποίησης μέσω της εφαρμογής My Account, σημειώνοντας ότι από τις 26/07/2021, η ενεργοποίηση της eSIM είναι προσωρινά μη διαθέσιμη μέσα από το My Account web portal της εταιρείας, όπως έχει αναρτηθεί και στο εσωτερικό κανάλι ενημέρωσης της εταιρείας. Αναφορικά με τους τρόπους ενεργοποίησης της esim κατά την ημερομηνία του περιστατικού, η εταιρεία δήλωσε ότι: «Η ενεργοποίηση της esim μπορούσε να γίνει μέσω του my account web portal και μέσω του my account application. Για το web portal η υπηρεσία ενεργοποιήθηκε στις 22.07.2021 και διακόπηκε αμέσως μετά την ενημέρωση ότι προέκυψε το συγκεκριμένο περιστατικό. Έκτοτε, η υπηρεσία αυτή δεν είναι διαθέσιμη μέσω του web portal. Για το my account application απαιτείτο η σταδιακή αυτοματοποιημένη ενημέρωση της εφαρμογής, η οποία για το σύνολο των χρηστών ολοκληρώθηκε επτά με δέκα ημέρες αργότερα από τις 22.07.2021. Η υπηρεσία μέσω του my account application σταμάτησε να παρέχεται στις 04.08.2021 κατόπιν σχετικού περιστατικού που συνέβη μέσω του application και ενεργοποιήθηκε ξανά στις 19.01.2022, με επιπρόσθετα μέτρα ασφάλειας (ενεργοποίηση μόνο μέσα από 4G δίκτυο και όχι μέσω WiFi, ενεργοποίηση της e-sim μετά από 12 ώρες με ταυτόχρονη αποστολή ενημερωτικών στον χρήστη που αιτήθηκε την αλλαγή και επιπλέον 4 ώρες για την ενεργοποίηση λήψης των SMS).»

2. Η διαδικασία Λογικής Πρόσβασης που ισχύει για τους συνδρομητές ή χρήστες (….), όπως αναφέρεται στην εγκεκριμένη, με την Απόφαση 132/2016 της ΑΔΑΕ, πολιτική ασφάλειας της εταιρείας σύμφωνα με δήλωση της κατά τη διάρκεια του επιτόπιου ελέγχου, έχει επικαιροποιηθεί σε σχέση με αυτή που ίσχυε κατά την ημερομηνία εκδήλωσης του περιστατικού. Η εταιρεία απέστειλε τη Διαδικασία Λογικής Πρόσβασης που ίσχυε κατά την ημερομηνία του περιστατικού (αρχείο «….», συνημμένο στο Σχετικό 6), καθώς και την έκδοση της Διαδικασίας Λογικής Πρόσβασης που ισχύει την τρέχουσα χρονική στιγμή (….) συνημμένο στο Σχετικό 6). Στην διαδικασία που ίσχυε κατά την ημερομηνία εκδήλωσης του συγκεκριμένου περιστατικού δεν εντοπίστηκε από την ΟΕ συγκεκριμένη ενότητα/σελίδα όπου περιγράφεται ο μηχανισμός ταυτοποίησης συνδρομητών και συνεπώς παρουσιάζεται απόκλιση από τα όσα προβλέπονται στην ενότητα 5.5 της εγκεκριμένης πολιτικής εταιρείας αναφορικά με τους συνδρομητές ή χρήστες (άρθρο 6.5 του Κανονισμού 165/2011 της Αρχής).

3. Η εταιρεία δήλωσε ότι δεν υπάρχει παρεμβολή υπάλληλου ή συνεργάτη της εταιρείας για την εξυπηρέτηση αιτήματος ενεργοποίησης e-SIM μέσω του λογαριασμού My Account. Τα σχετικά αιτήματα ολοκληρώνονταν με αυτοματοποιημένο τρόπο (Σημείο 2 του Σχετικού 4).

4. Αναφορικά με την ημερομηνία ενεργοποίησης της υπηρεσίας My Account καθώς και την ημερομηνία τελευταίας αλλαγής password από τον θιγόμενο, η εταιρεία στο Σημείο 3 του Σχετικού 4 απάντησε ότι: «Δεν υπάρχει καταχωρημένη η ημερομηνία εγγραφής και ενεργοποίησης της υπηρεσίας (λογαριασμού) My Account για τον θιγόμενο συνδρομητή. Όπως προκύπτει από την παρακάτω Εικόνα 2 από τα συστήματα της εταιρείας μας τελευταία καταχωρημένη αλλαγή του κωδικού πρόσβασης είναι η 14-12-2021 και ώρα 13:35.» Κατά τη διάρκεια του επιτόπιου ελέγχου η εταιρεία δήλωσε επιπλέον ότι ο συγκεκριμένος λογαριασμός στην υπηρεσία my account ενεργοποιήθηκε στις 17.02.2013 και παρέδωσε σχετική τεκμηρίωση (Συνημμένο 1 του Σχετικού 5).

5. Σχετικά με τον τρόπο αποθήκευσης των user name και passwords των χρηστών στον web server, η εταιρεία κατά τη διάρκεια του επιτόπιου ελέγχου δήλωσε ότι διατηρούνται σε μορφή hashed. Στη συνέχεια στο Σημείο 4 του Σχετικού 6 δήλωσε: «Όσον αφορά στον τρόπο αποθήκευσης των user names και passwords των χρηστών στον web server, χρησιμοποιείται hashing αλγόριθμος και πιο συγκεκριμένα ο αλγόριθμος "….".».

6. Σχετικά με την τακτική αλλαγή του κωδικού πρόσβασης, η εταιρεία δήλωσε ότι οι χρήστες ενημερώνονται από την εταιρεία και απευθύνεται σχετική σύσταση να αλλάζουν τον κωδικό πρόσβασης (password) κάθε έξι (6) μήνες. Ωστόσο, δεν υπάρχει διαθέσιμη η πληροφορία για το πότε ενημερώθηκε ο χρήστης τελευταία φορά για την αναγκαιότητα αλλαγής. Επιπροσθέτως, η εταιρεία δήλωσε ότι δίνεται η δυνατότητα ο χρήστης να επιλέξει να μην αλλάξει κωδικό πρόσβασης. Σε αυτή την περίπτωση εμφανίζεται σχετικό ενημερωτικό μήνυμα με αναφορά στους κινδύνους και τις ενδεχόμενες συνέπειες από τη μη αλλαγή κωδικού (Σημείο 4 του Σχετικού 4). Όσον αφορά στην τελευταία αλλαγή password του θιγόμενου συνδρομητή πριν το συμβάν, η εταιρεία στο Σημείο 5 του Σχετικού 6 δήλωσε ότι: «Η πληροφορία δεν είναι διαθέσιμη στα συστήματά μας, καθώς οποιαδήποτε αλλαγή στο password του θιγόμενου συνδρομητή ενδέχεται να έχει πραγματοποιηθεί σε προγενέστερη χρονική στιγμή από τον ορισμένο χρόνο διατήρησης της εταιρεία μας.» . Σε ερώτημα της ΟΕ, κατά τη διάρκεια του επιτόπιου ελέγχου, αν αλλάζει υποχρεωτικά το password σε τακτά χρονικά διαστήματα, η εταιρεία απάντησε ότι οι χρήστες ενημερώνονται ανά εξάμηνο για την ανάγκη αλλαγής του password, δήλωσε ωστόσο ότι η αλλαγή δεν είναι υποχρεωτική. Επιπρόσθετα, η εταιρεία δήλωσε ότι ελέγχεται συστημικά αν έχει παρέλθει το εξάμηνο από την τελευταία αλλαγή του password κάθε φορά που ο χρήστης χρησιμοποιεί την εφαρμογή, είτε μέσω του application, είτε μέσω του portal.

7. Σχετικά με τον τρόπο που αποδίδονται τα username και password για την υπηρεσία my account, η εταιρεία απάντησε ότι τα username και password ορίζονται από το χρήστη της εφαρμογής κατά την ενεργοποίηση της υπηρεσίας και ο χρήστης ταυτοποιείται με χρήση one time password (OTP). Ο ίδιος μηχανισμός ταυτοποίησης χρησιμοποιείται και κατά την αλλαγή password λόγω απώλειας. Σχετικά με τα

κριτήρια που απαιτούνται για τον ορισμό του password, η εταιρεία δήλωσε ότι τα σχετικά κριτήρια εμφανίζονται στον χρήστη κατά τη διαδικασία ορισμού/αλλαγής του password (7-20 αριθμούς ή Λατινικούς χαρακτήρες, τουλάχιστον 2 τύπους χαρακτήρων και να μην περιέχει Ελληνικούς χαρακτήρες ή το όνομα χρήστη).

8. Όσον αφορά στα αρχεία καταγραφής της ενεργοποίησης και της απενεργοποίησης της επίμαχης eSIM από τα συστήματα της εταιρείας, έχουν εντοπιστεί εγγραφές στο σύστημα διαχείρισης πελατών (CRM) οι οποίες παρουσιάζονται στην εικόνα 6 στο σημείο 5 του σχετικού 4. Σύμφωνα με αυτές η πρώτη αλλαγή έγινε στις 16:14:30 της 22.07.2021 μέσω ηλεκτρονικής επικοινωνίας και η δεύτερη αλλαγή στις 19:18:17 της ίδιας ημέρας κατόπιν επίσκεψης σε φυσικό καττάστημα.

9. Οι προσβάσεις που προκύπτουν στα συστήματα εξυπηρέτησης πελατών αναφορικά με τον αριθμό σύνδεσης 6948821402, για την ημερομηνία 22.07.2021, παρατίθενται με επεξήγηση των σχετικών εγγραφών (Εικόνα 5, Σημείο 6 του Σχετικού 4). Αναλυτικότερα, την 22/07/2021 και ώρα 16:31:54 γίνεται επικοινωνία μέσω της υπηρεσίας live chat με θέμα την e-SIM, κατά την οποία, όταν ζητούνται τα στοιχεία ταυτοποίησης όπως ορίζει η διαδικασία, ο συνδρομητής αποσυνδέεται από την υπηρεσία live chat. Την 22/07/2021 και ώρα 16:35:56 γίνεται επικοινωνία μέσω της υπηρεσίας live chat με θέμα την μη δυνατότητα λήψης μηνυμάτων στην e-SIM. Κατόπιν ταυτοποίησης του συνδρομητή γίνεται ενημέρωση ότι, σύμφωνα με τη διαδικασία, η ενεργοποίηση της e-SIM όπως και όλες οι τροποποιήσεις sim, ενεργοποιούν αυτόματα για λόγους ασφαλείας φραγή εισερχομένων μηνυμάτων για 2 ώρες από το αίτημα. Την 22/07/2021 και ώρα 17:50:43 πραγματοποιείται κλήση στο τμήμα εξυπηρέτησης πελατών της εταιρείας μας με θέμα την κάρτα SIM η οποία είχε κλειδωθεί και την αναζήτηση του PUK. Την 22/07/2021 και ώρα 19:23:17 πραγματοποιείται κλήση στο τμήμα εξυπηρέτησης πελατών της εταιρείας όπου αναφέρεται η μη ζητηθείσα αλλαγή της κάρτας sim.

10. Η ακριβής ημέρα και ώρα ενεργοποίησης της κάρτας e-SIM για την υπ' αριθμόν 6948821402 σύνδεση κινητής τηλεφωνίας, της οποίας η αλλαγή αναφέρθηκε ως μη ζητηθείσα από τον συνδρομητή, είναι η 22/07/2021 (και ώρα 16:14:30), ενώ η απενεργοποίηση της εν λόγω κάρτας sim πραγματοποιήθηκε την ίδια ημέρα, ήτοι την 22/07/2021 (και ώρα 19:10:12), (Εικόνα 6, Σημείο 7 του Σχετικού 4).

11. Σχετικά με τον αριθμό των εισερχόμενων και εξερχόμενων επικοινωνιών ανά είδος (ενδεικτικά κλήσεις, SMS, data) της σύνδεσης …. κατά το χρονικό διάστημα από την ενεργοποίηση της e-SIM έως την έκδοση νέας κάρτας SIM και την παράδοσή της στον συνδρομητή η εταιρεία στο Σημείο 8 του Σχετικού 4 δήλωσε ότι: «Το πλήθος των εισερχόμενων και εξερχόμενων επικοινωνιών της υπ' αριθμόν …. σύνδεσης κινητής τηλεφωνίας κατά το χρονικό διάστημα από την ενεργοποίηση της e-SIM (22/07/2021 και ώρα 16:14:30) έως την έκδοση νέας κάρτας SIM (την 22/07/2021 και ώρα 19:10:12), είναι 102 εγγραφές και ειδικότερα αφορούν σε: 1 εισερχόμενη αναπάντητη κλήση, 1 εισερχόμενη κλήση (για την οποία έχουν παραχθεί 2 cdrs), 2 εξερχόμενες κλήσεις, 28 επιτυχημένες αποστολές sms προς τον αριθμό … (25 εκ των οποίων A2P), 42 εγγραφές που αφορούν sms που έχουν παραδοθεί στον αριθμό … με επιτυχία από το κέντρο μηνυμάτων (smsc), 27 εγγραφές (25 εκ των οποίων A2P) εισερχόμενων sms που ενδέχεται να

αντιστοιχούν σε λιγότερα από 27 μοναδικά sms, καθώς το κέντρο μηνυμάτων (smsc) ενδέχεται να σπάσει ένα sms σε 2 CDR, 0 εξερχόμενα sms και 0 καταγραφές χρήσης υπηρεσίας δεδομένων».

12. Αναφορικά με τα τεχνικά και οργανωτικά μέτρα που ανέφερε στο Σχετικό 1 ότι πρόκειται να λάβει η εταιρεία, δήλωσε ότι: «Έχουν υλοποιηθεί όλα τα αναφερόμενα τεχνικά και οργανωτικά μέτρα. Ειδικότερα, η επικαιροποίηση των διαδικασιών αντικατάστασης των καρτών SIM/ e-SIM είναι συνεχής, έχει ήδη λάβει χώρα από την εταιρεία μας ήδη από το έτος 2020 και λαμβάνει χώρα όποτε κρίνεται αναγκαίο. Έχει ήδη θεσπιστεί ως υποχρεωτικός έλεγχος στα αιτήματα αντικατάστασης κάρτας η εκ μέρους μας τηλεφωνική επικοινωνία με τον αιτούντα συνδρομητή / κάτοχο της SIM, προκειμένου να επιβεβαιωθεί το υποβληθέν αίτημα, στις περιπτώσεις αιτήματος μέσω καταστημάτων (στο νούμερο που ζητείται αντικατάσταση καθώς και στο τηλέφωνο επικοινωνίας στην καρτέλα του πελάτη). Έχει καταργηθεί η διαδικασία αντικατάστασης SIM κάρτας για πελάτες λιανικής, μέσω του τηλεφωνικού κέντρου εξυπηρέτησης πελατών. Μετά την αντικατάσταση κάρτας SIM πραγματοποιείται σε κάθε περίπτωση φραγή εισερχομένων sms για διάστημα 2 ωρών. Έχει γίνει ενημέρωση και εκπαίδευση των υπεύθυνων και των υπαλλήλων των καταστημάτων σχετικά με τη διαδικασία αντικατάστασης SIM και τη συνακόλουθη ανάγκη πλήρους συμμόρφωσης και εφαρμογής των διαδικασιών. Ιδίως όσον αφορά στα ψηφιακά κανάλια της εταιρείας μας και ειδικότερα μέσω της mobile εφαρμογής My Vodafone App έχει υιοθετηθεί μηχανισμός αυθεντικοποίησης με χρήση δύο παραγόντων (2 factor authentication - One Time Password σε συνδυασμό με τα υφιστάμενα στοιχεία αυθεντικοποίησης). Αναφορικά με την υπηρεσία My Account που είναι προσβάσιμη μέσω browser/web όπως ήδη αναφέραμε και στο σημείο 1, η εταιρεία μας προέβη σε άμεση αναστολή της διάθεσης της υπηρεσίας e-SIM και από τις 26/07/2021 η ενεργοποίηση της e-SIM είναι μη διαθέσιμη μέσα από το την εν λόγω υπηρεσία. Επιπλέον δεν υπάρχει δυνατότητα αλλαγής κάρτας από τα ψηφιακά κανάλια σε περίπτωση απώλειας ή κλοπής και η εξυπηρέτηση γίνεται μόνο από καταστήματα.» (Σημείο 9 του Σχετικού 4).

13. Η εταιρεία κοινοποίησε στην ΑΔΑΕ την επιστολή προς τον θιγόμενο συνδρομητή Μέδρο Πρόδρομο (Συνημμένο 2 του Σχετικού 4).

14. Σχετικά με οποιοδήποτε άλλο στοιχείο έχει προκύψει από τη διερεύνηση του περιστατικού (π.χ. εκτιμώμενη αιτία εκδήλωσης περιστατικού, κτλ) σύμφωνα με τη διαδικασία της εταιρείας για τη διαχείριση των περιστατικών ασφάλειας και τη διάταξη του άρθρου 9.2.3 του Κανονισμού για τη Διασφάλιση του Απορρήτου των Ηλεκτρονικών Επικοινωνιών (Απόφαση 165/2011 της Αρχής), η εταιρεία δήλωσε ότι: «Από τη διερεύνηση του εν λόγω περιστατικού προέκυψε ότι η εκτιμώμενη αιτία εκδήλωσής του έγκειται αφενός σε πρότερη πλήρη γνώση (μη σχετιζόμενη με τη Vodafone) και πρόσβαση από άγνωστο άτομο σε προσωπικά στοιχεία του συνδρομητή, όπως ενδεικτικά αριθμός σύνδεσης κινητής τηλεφωνίας και κωδικούς (username και password) του λογαριασμού My account. Η γνώση και η εν λόγω πρόσβαση στα πιο πάνω προσωπικά στοιχεία του συνδρομητή αποτέλεσε την μοναδική αιτία για την οποία το εν λόγω άγνωστο τρίτο άτομο κατάφερε να υπερκεράσει τους θεσπισμένους μηχανισμούς ελέγχου και τα τεχνικά και οργανωτικά μέτρα της εταιρείας μας. Τέλος, επισημαίνεται ότι οι προσπάθειες απάτης και κλοπής

στοιχείων πολιτών έχουν εξελιχθεί ραγδαία με χρήση τόσο κοινωνικής μηχανικής (social engineering) όσο και εξειδικευμένης τεχνολογίας, υφαρπάζοντας όλα τα απαραίτητα στοιχεία και παρακάμπτοντας με αυτόν το τρόπο την διαδικασία ταυτοποίησης, με τελικό σκοπό την διενέργεια παράνομων συναλλαγών». (Σημείο 11 του Σχετικού 4).

15. Σχετικά με την τεχνολογία που χρησιμοποιείται στην web εφαρμογή και την έκδοση του web server που εξυπηρετεί την υπηρεσία, η εταιρεία απάντησε ότι βασίζεται σε τεχνολογία της Oracle, ενώ για τη συγκεκριμένη έκδοση αυτού κατά την ημερομηνία του περιστατικού, καθώς και τη σημερινή η εταιρεία δήλωσε ότι: «Οι τεχνολογίες που χρησιμοποιούνται στο Hosting Environment (web application servers) είναι οι ακόλουθες: …..).» (σημείο 1 του σχετικού 6). Κατά τη διάρκεια του ελέγχου η εταιρεία δήλωσε ότι ο web server διατηρείται ενημερωμένος, καθώς και ότι κάθε 6 μήνες, ή και νωρίτερα εφόσον υπάρξει κάποια σημαντική αλλαγή, πραγματοποιείται penetration test στην εφαρμογή. Η εταιρεία απέστειλε (συνημμένο του σχετικού 6) penetration test που είχε πραγματοποιηθεί πριν τις 22-07-2021 (…), καθώς και τα penetration tests που πραγματοποιήθηκαν στη συνέχεια (….), αναφέροντας ότι για όλα τα ευρήματα των ανωτέρω ελέγχων που έχουν χαρακτηριστεί ως υψηλού κινδύνου έχουν πραγματοποιηθεί διορθωτικές ενέργειες.

16. Η διαχείριση του web server κατά δήλωση της εταιρείας γίνεται από την ίδια και εφόσον προκύψει ανάγκη υπάρχει υποστήριξη από τη συνεργάτη της εταιρεία, …. Η εταιρεία απέστειλε συνημμένα στο Σχετικό 6 τη σύμβαση υποστηρικτικών υπηρεσιών της εταιρείας με την εταιρεία ….

17. Σχετικά με την ταυτοποίηση του χρήστη κατά την επικοινωνία του με την εταιρεία στις 22.07.2021 και ώρα 16:35, μέσω live chat, η εταιρεία ανέφερε ότι αυτή πραγματοποιήθηκε μέσω επιβεβαίωσης του ονοματεπώνυμου και του ΑΔΤ και απέστειλε τα σχετικά αποδεικτικά screenshot του live chat τα οποία, σύμφωνα με την εταιρεία, διατηρούνται για ένα χρόνο (Σημείο 7 του Σχετικού 6). Ο χρήστης, κατά την επικοινωνία αυτή, αφού πρώτα ταυτοποιήθηκε δίνοντας στον εκπρόσωπο της εταιρείας ονοματεπώνυμο και ΑΔΤ, ζήτησε να γίνει άρση φραγής πριν το προβλεπόμενο από την διαδικασία της εταιρείας χρόνο (2ώρες). Το αίτημα του δεν έγινε δεκτό και τερμάτισε την επικοινωνία.

18. Αναφορικά με ερώτημα της Ο.Ε., κατά τον επιτόπιο έλεγχο, αν κατά τη χρήση της υπηρεσίας my account για την ενεργοποίηση esim μέσω portal υπήρχε OTP ή άλλος σχετικός μηχανισμός, η εταιρεία απάντησε ότι δεν υπήρχε κατά το διάστημα των 2 ημερών που η υπηρεσία ήταν διαθέσιμη. Για την ενεργοποίηση esim μέσω application, η εταιρεία απάντησε ότι τέθηκε σε εφαρμογή η χρήση OTP αμέσως μετά την εμφάνιση του εν λόγω περιστατικού.

Δ. ΣΥΜΠΕΡΑΣΜΑΤΑ

Από τον έλεγχο που διενεργήθηκε και την εξέταση του συνόλου των στοιχείων του περιστατικού ασφάλειας με αρ. πρωτ. ΑΔΑΕ 2205/02.08.2021 προκύπτουν οι διαπιστώσεις που αναφέρονται αναλυτικά στην ενότητα Γ της παρούσας Έκθεσης.

Ειδικότερα:

α) Πραγματοποιήθηκε ενεργοποίηση e-sim σε μη εξουσιοδοτημένο πρόσωπο. Σχετικά με τον αριθμό των εισερχόμενων και εξερχόμενων επικοινωνιών ανά είδος (ενδεικτικά κλήσεις, SMS, data) της σύνδεσης …. κατά το χρονικό διάστημα από την ενεργοποίηση της e-SIM έως την έκδοση νέας κάρτας SIM και την παράδοσή της στον συνδρομητή η εταιρεία στο Σημείο 8 του Σχετικού 4 δήλωσε ότι: «Το πλήθος των εισερχόμενων και εξερχόμενων επικοινωνιών της υπ' αριθμόν …. σύνδεσης κινητής τηλεφωνίας κατά το χρονικό διάστημα από την ενεργοποίηση της e-SIM (22/07/2021 και ώρα 16:14:30) έως την έκδοση νέας κάρτας SIM (την 22/07/2021 και ώρα 19:10:12), είναι 102 εγγραφές και ειδικότερα αφορούν σε: 1 εισερχόμενη αναπάντητη κλήση, 1 εισερχόμενη κλήση (για την οποία έχουν παραχθεί 2 cdrs), 2 εξερχόμενες κλήσεις, 28 επιτυχημένες αποστολές sms προς τον …. (25 εκ των οποίων A2P), 42 εγγραφές που αφορούν sms που έχουν παραδοθεί στον αριθμό …. με επιτυχία από το κέντρο μηνυμάτων (smsc), 27 εγγραφές (25 εκ των οποίων A2P) εισερχόμενων sms που ενδέχεται να αντιστοιχούν σε λιγότερα από 27 μοναδικά sms, καθώς το κέντρο μηνυμάτων (smsc) ενδέχεται να σπάσει ένα sms σε 2 CDR, 0 εξερχόμενα sms και 0 καταγραφές χρήσης υπηρεσίας δεδομένων».

β) Στη διαδικασία λογικής πρόσβασης …. (Συνημμένο του Σχετικού 6) της εγκεκριμένης με την Απόφαση 132/2016 της ΑΔΑΕ Πολιτικής Ασφάλειας της εταιρείας δεν περιλαμβάνεται ο μηχανισμός ταυτοποίησης συνδρομητών, κατά παράβαση των προβλεπόμενων στην παρ. 6.5.1 του Κανονισμού 165/2011 της Αρχής, όπου ρητώς προβλέπεται ότι: *«το υπόχρεο πρόσωπο οφείλει να διατηρεί αρχείο που αναφέρει αναλυτικά τους μηχανισμούς ελέγχου πρόσβασης και αυθεντικοποίησης που χρησιμοποιούνται για την πρόσβαση των συνδρομητών ή χρηστών του στις υπηρεσίες ή/και τα δίκτυα που παρέχει.»*.».

Β. Ενόψει των αποτελεσμάτων της από 21.04.2023 «Έκθεσης Διενέργειας Εκτάκτου Ελέγχου στην εταιρεία VODAFONE ΠΑΝΑΦΟΝ ΑΕΕΤ σε συνέχεια του περιστατικού ασφαλείας με αριθμό πρωτοκόλλου ΑΔΑΕ 2205/02.08.2021», προκύπτει η ακόλουθη ενδεχόμενη παράβαση της κείμενης νομοθεσίας περί προστασίας του απορρήτου των επικοινωνιών εκ μέρους της εταιρείας «VODAFONE ΠΑΝΑΦΟΝ ΑΕΕΤ»:

Παραβίαση της διάταξης του άρθρου 6.5.1 του Κανονισμού για τη Διασφάλιση του Απορρήτου των Ηλεκτρονικών Επικοινωνιών (Απόφαση 165/2011 της Α.Δ.Α.Ε.) και της ενότητας 5.5 της Πολιτικής Ασφάλειας της εταιρείας.

Όπως προέκυψε κατά τη διενέργεια του ελέγχου του επίμαχου περιστατικού, στη διαδικασία λογικής πρόσβασης P-207 της Πολιτικής Ασφάλειας της εταιρείας (Access & Authentication DR_v2.1 έκδοση 2.1), όπως αυτή παραδόθηκε συνημμένη στο υπ' αριθμ πρωτ. ΑΔΑΕ ΕΜΠ 231/27-06-2022 έγγραφό της, δεν περιλαμβάνεται ο μηχανισμός ταυτοποίησης συνδρομητών, κατά παράβαση των προβλεπόμενων στην παρ. 6.5.1 του Κανονισμού 165/2011 της Αρχής, όπου ρητώς προβλέπεται ότι: *«το υπόχρεο πρόσωπο οφείλει να διατηρεί αρχείο που αναφέρει αναλυτικά τους μηχανισμούς ελέγχου πρόσβασης και αυθεντικοποίησης που χρησιμοποιούνται για την πρόσβαση των συνδρομητών ή χρηστών του στις υπηρεσίες ή/και τα δίκτυα που παρέχει.»*. Όπως, μάλιστα αναγνωρίζει η ίδια η εταιρεία στο υπ' αριθμ.

πρωτ. ΑΔΑΕ ΕΜΠ 367/11-10-2022 έγγραφο που είχε αποστείλει στην Α.Δ.Α.Ε. επ' αφορμής αντίστοιχου με το επίμαχο περιστατικού, ο μηχανισμός ταυτοποίησης συνδρομητών εξειδικεύεται μόνο στη νεότερη έκδοση της εν λόγω διαδικασίας, η οποία, ωστόσο, δεν ίσχυε στο χρόνο εμφάνισης του εν θέματι περιστατικού. Η αναλυτική καταγραφή των μηχανισμών λογικής πρόσβασης των συνδρομητών στα ΠΕΣ της εταιρείας που παρέχουν πρόσβαση σε δεδομένα επικοινωνίας παρέχει την απαιτούμενη τεκμηρίωση για την πραγματοποίηση της πρόσβασης, ελέγχεται, εξάλλου, ως προς την αποτελεσματικότητά της από την Αρχή. Τουναντίον, η έλλειψη αυτής καθιστά ανέφικτο τον έλεγχο εκ μέρους της Αρχής των αρχών και των προϋποθέσεων ταυτοποίησης των συνδρομητών και πρόσβασής τους στα δεδομένα επικοινωνίας τους.

Γ. Κατόπιν των παραπάνω, και έχοντας υπόψη:

1. Το ν.3115/2003 «Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών» (ΦΕΚ Α΄ 47/2003), όπως ισχύει, και ιδίως τα άρθρα 1, 6, 7 και 11 αυτού,
2. Το ν.3471/2006 «Προστασία δεδομένων προσωπικού χαρακτήρα και της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών» (ΦΕΚ Α'133), όπως ισχύει, και ιδίως τα άρθρα 4, 12 και 13 αυτού,
3. Το ν.3674/2008 «Ενίσχυση του θεσμικού πλαισίου διασφάλισης του απορρήτου της τηλεφωνικής επικοινωνίας και άλλες διατάξεις» (ΦΕΚ Α' 136/10.07.2008), όπως ισχύει, και ιδίως τα άρθρα 2, 3, 6,8 και 11 αυτού,
4. Την Απόφαση της ΑΔΑΕ υπ' αριθμ. 165/2011 (ΦΕΚ Β' 2715/17-11-2011),
5. Τις διατάξεις της υπ'αριθμ. 44/31.10.2003 Απόφασης της Α.Δ.Α.Ε. «Κανονισμός Εσωτερικής Λειτουργίας της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών (Α.Δ.Α.Ε.)» (ΦΕΚ Β' 1642/7.11.2003), όπως ισχύει, και ιδίως τα άρθρα 4 και 6 αυτής,
6. Την υπ' αριθμ. 16887/17-03-2016 Απόφαση του Υπουργού Δικαιοσύνης, Διαφάνειας και Ανθρωπίνων Δικαιωμάτων (ΦΕΚ Υ.Ο.Δ.Δ. 151/21-03-2016), περί συγκρότησης της Αρχής Διασφάλισης του Απορρήτου των Επικοινωνιών,
7. Την υπ' αριθ. 34051/29.05.2019 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,
8. Την υπ' αριθμ. 58347/21-12-2020 Απόφαση του Υπουργού Δικαιοσύνης (ΦΕΚ Υ.Ο.Δ.Δ. 1066/24-12-2020) περί διορισμού νέων μελών στην Αρχή Διασφάλισης του Απορρήτου των Επικοινωνιών,
9. Το με αρ. πρωτ. ΑΔΑΕ 2205/02.08.2021 έγγραφο της εταιρείας «VODAFONE ΠΑΝΑΦΟΝ ΑΕΕΤ»,
10. Την υπ' αριθμ. 296/2021 εισήγηση προς την Ολομέλεια της Α.Δ.Α.Ε.,
11. Την υπ' αριθμ. 369/2021 Απόφαση της Ολομέλειας της Α.Δ.Α.Ε.,

12. Τη με αρ. πρωτ. ΑΔΑΕ ΕΜΠ 114/21.03.2022 επιστολή της Α.Δ.Α.Ε. προς την εταιρεία «VODAFONE ΠΑΝΑΦΟΝ ΑΕΕΤ»,
13. Το με αρ. πρωτ. ΑΔΑΕ ΕΜΠ-152/12.04.2022 έγγραφο της εταιρείας «VODAFONE ΠΑΝΑΦΟΝ ΑΕΕΤ»,
14. Το υπ' αριθμ. πρωτ. ΑΔΑΕ ΕΜΠ 205/14.06.2022 πρακτικό διενέργειας εκτάκτου ελέγχου στις εγκαταστάσεις της εταιρείας «VODAFONE ΠΑΝΑΦΟΝ ΑΕΕΤ»,
15. Τη με αρ. πρωτ. ΑΔΑΕ ΕΜΠ 310/13.09.2022 επιστολή της Α.Δ.Α.Ε. προς την εταιρεία «VODAFONE ΠΑΝΑΦΟΝ ΑΕΕΤ»,
16. Το με αρ. πρωτ. ΑΔΑΕ ΕΜΠ-231/27.06.2022 έγγραφο της εταιρείας «VODAFONE ΠΑΝΑΦΟΝ ΑΕΕΤ»,
17. Την από 21.04.2023 «Έκθεση Διενέργειας Εκτάκτου Ελέγχου στην εταιρεία VODAFONE ΠΑΝΑΦΟΝ ΑΕΕΤ σε συνέχεια του περιστατικού ασφαλείας με αριθμό πρωτοκόλλου ΑΔΑΕ 2205/02.08.2021» (συνημμένο 1),
18. Την υπ' αριθμ. 235/2023 εισήγηση προς την Ολομέλεια της Α.Δ.Α.Ε.,
19. Το πρακτικό της από 21 Ιουνίου 2023 συνεδρίασης της Ολομέλειας της Α.Δ.Α.Ε.,

Η ΑΡΧΗ ΔΙΑΣΦΑΛΙΣΗΣ ΤΟΥ ΑΠΟΡΡΗΤΟΥ ΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ (ΑΔΑΕ)

ΑΠΟΦΑΣΙΖΕΙ

Α) Εγκρίνει την από 21.04.2023 «Έκθεση Διενέργειας Εκτάκτου Ελέγχου στην εταιρεία VODAFONE ΠΑΝΑΦΟΝ ΑΕΕΤ σε συνέχεια του περιστατικού ασφαλείας με αριθμό πρωτοκόλλου ΑΔΑΕ 2205/02.08.2021».

Β) Καλεί σε Ακρόαση την εταιρεία **«VODAFONE ΠΑΝΑΦΟΝ ΑΕΕΤ»** ενώπιον της Ολομέλειας της Α.Δ.Α.Ε., με αντικείμενο τον έλεγχο της ενδεχόμενης παράβασης της κείμενης νομοθεσίας περί απορρήτου των επικοινωνιών, όπως αναλυτικά εκτίθεται ανωτέρω στα σημεία Α και Β, δια της υποβολής έγγραφου υπομνήματος ενώπιον της Αρχής έως την **31η Ιουλίου 2023, ημέρα Δευτέρα και ώρα 15.00 μ.μ.,** σύμφωνα με τα οριζόμενα στη διάταξη της παρ. 3 του άρθρου 4 του Κανονισμού Εσωτερικής Λειτουργίας της Α.Δ.Α.Ε., όπως τροποποιήθηκε με την υπ' αριθμ. 29/2020 Απόφαση της Αρχής (ΦΕΚ Β΄ 423/12-02-2020).

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

Επίσης, καλείται η εταιρεία να προσκομίσει, συνημμένα στο προαναφερθέν έγγραφο υπόμνημά της, τα πρόσφατα οικονομικά της στοιχεία.

Επισημαίνεται, τέλος, ότι σύμφωνα με το άρθρο 6 παρ. 3 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 ισχύει, ο ενδιαφερόμενος μπορεί να υποβάλει αίτημα δημοσιότητας της διαδικασίας.

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΑΡΧΗ ΔΙΑΣΦΑΛΙΣΗΣ ΤΟΥ ΑΠΟΡΡΗΤΟΥ ΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ

Η παρούσα απόφαση να επιδοθεί στην εταιρεία «VODAFONE ΠΑΝΑΦΟΝ ΑΕΕΤ»,.

Κρίθηκε και αποφασίστηκε την 21η Ιουνίου 2023.

ΣΥΝΗΜΜΕΝΑ: 1
Η από 21.04.2023 «Έκθεση Διενέργειας Εκτάκτου Ελέγχου στην εταιρεία VODAFONE ΠΑΝΑΦΟΝ ΑΕΕΤ σε συνέχεια του περιστατικού ασφαλείας με αριθμό πρωτοκόλλου ΑΔΑΕ 2205/02.08.2021».

Ο Πρόεδρος

Χρ. Ράμμος