ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Αθήνα, 07-07-2015

Αριθ. Πρωτ.: Γ/ΕΞ/6300-1/07-07-2015

Α Π Ο Φ Α Σ Η ΑΡ. 85 / 2015

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα συνήλθε μετά από πρόσκληση του Προέδρου της σε τακτική συνεδρίαση στην έδρα της την 9-06-2015, σε συνέχεια της από 26-05-2015 τακτικής συνεδρίασής της, προκειμένου να εξετάσει την υπόθεση που αναφέρεται στο ιστορικό της παρούσας. Παρέστησαν οι Π. Χριστόφορος, Πρόεδρος της Αρχής, και τα τακτικά μέλη της Αρχής Λ. Κοτσαλής, Αν.-Ιωάν. Μεταξάς, Δ. Μπριόλας, Κ. Χριστοδούλου, Π. Τσαντίλας, καθώς επίσης και το αναπλ. μέλος της Αρχής Π. Ροντογιάννης, ως εισηγητής. Το τακτικό μέλος Α. Συμβώνης, αν και προσκλήθηκε νομίμως, δεν προσήλθε λόγω κωλύματος. Στη συνεδρίαση παρέστησαν, επίσης, με εντολή του Προέδρου, οι Κ. Λιμνιώτης, και Λ. Ρούσσος, ειδικοί επιστήμονες-πληροφορικοί, ως βοηθοί εισηγητή. Επίσης, παρέστη, με εντολή του Προέδρου, και η Ε. Παπαγεωργοπούλου, υπάλληλος του Διοικητικού-Οικονομικού Τμήματος της Αρχής, ως γραμματέας. Ο βοηθός εισηγητή Ι. Λυκοτραφίτης, ειδικός επιστήμων-πληροφορικός, δεν παρέστη στη συνεδρίαση αυτή (της 9-06-2015) λόγω κωλύματος.

Η Αρχή έλαβε υπόψη της τα παρακάτω:

Ο Ευρωπαϊκός Οργανισμός για την Ασφάλεια των Δικτύων και Πληροφοριών (European Union Network and Information Security Agency – εφεξής ENISA) ενημέρωσε την Αρχή, με το υπ' αριθμ. πρωτ. Γ/ΕΙΣ/6300/17-10-2014 έγγραφό του, για περιστατικό διαρροής δεδομένων πιστωτικών καρτών τριών ατόμων τα οποία πραγματοποίησαν, από ξεχωριστές τοποθεσίες (διαφορετικά κράτη) ηλεκτρονική κράτηση στο ξενοδοχείο Royal Olympic επί της οδού Αθ. Διάκου 28-34, 11743, Αθήνα. Συγκεκριμένα, ο ENISA διοργάνωσε στο εν

λόγω ξενοδοχείο ένα συνέδριο (workshop) στο διάστημα 22-23 Οκτωβρίου 2014, και οι συμμετέχοντες σε αυτό μπορούσαν να πραγματοποιήσουν ηλεκτρονικά κράτηση για τη διαμονή τους στο συγκεκριμένο ξενοδοχείο. Όπως επισημαίνεται στο ανωτέρω έγγραφο του ENISA, τρεις εκ των συμμετεχόντων στο εν λόγω συνέδριο, οι οποίοι είχαν ήδη προβεί σε ηλεκτρονική κράτηση έχοντας συμπληρώσει –ηλεκτρονικά– στοιχεία των πιστωτικών τους καρτών, ενημερώθηκαν εκ των υστέρων για ηλεκτρονικές διαδικτυακές συναλλαγές που είτε έγιναν είτε έγινε σχετική απόπειρα να γίνουν από αγνώστους με τα στοιχεία των καρτών τους. Συγκεκριμένα, με βάση τα επισυναπτόμενα μηνύματα ηλεκτρονικού ταχυδρομείου στο ως άνω έγγραφο του ENISA:

α) Ο Α από τη Γερμανία ενημέρωσε τον ENISA ότι άγνωστος επιχείρησε να πραγματοποιήσει αγορά ύψους 1200 € δίνοντας στοιχεία της πιστωτικής του κάρτας που ο ίδιος είχε χρησιμοποιήσει λίγες μέρες νωρίτερα για την ηλεκτρονική κράτηση στο ξενοδοχείο (ο ίδιος ενημερώθηκε για την απόπειρα αυτή από την Τράπεζά του),

β) Η Β από τη Σλοβενία ενημέρωσε τον ENISA ότι άγνωστος πραγματοποίησε ηλεκτρονική αγορά ύψους 500 €, για διαδικτυακό παιχνίδι, δίνοντας στοιχεία της πιστωτικής της κάρτας που η ίδια είχε χρησιμοποιήσει λίγες μέρες νωρίτερα για την ηλεκτρονική κράτηση στο ξενοδοχείο[1], ενώ μετέπειτα έγιναν και άλλες δύο απόπειρες αγοράς μέσω αυτής της κάρτας από άγνωστο αλλά η Τράπεζά της εν τω μεταξύ την είχε καταστήσει άκυρη,

γ) Ο Γ ενημέρωσε επίσης τον ENISA ότι είχε αντίστοιχο πρόβλημα με τη δική του πιστωτική κάρτα (χωρίς να αναφέρει περισσότερες λεπτομέρειες).

Όπως προκύπτει επίσης από το ως άνω έγγραφο, ο ENISA επικοινώνησε με το ξενοδοχείο, τόσο τηλεφωνικά όσο και μέσω ηλεκτρονικού ταχυδρομείου, αναφέροντας τα εν λόγω περιστατικά.

Κατόπιν των ανωτέρω, η Αρχή ζήτησε από το ξενοδοχείο Royal Olympic (εφεξής, υπεύθυνος επεξεργασίας), με το υπ' αριθμ. πρωτ. Γ/ΕΞ/6300-1/20-10-2014 έγγραφό της, τις απόψεις του επί των ανωτέρω, θέτοντας ιδίως τα ακόλουθα ερωτήματα: α) αν εξέτασε την έκτασή του (πλήθος χρηστών των οποίων τα δεδομένα εκτέθηκαν, είδος δεδομένων, χρονικό διάστημα που το εν λόγω πρόβλημα ήταν σε ισχύ), β) σε περίπτωση που εντοπίστηκε συγκεκριμένο πρόβλημα, αν προέβη σε ενέργειες για την αποκατάστασή του, γ) αν προέβη σε κατάλληλη ενημέρωση λοιπών πελατών του που έχουν πραγματοποιήσει κράτηση μέσω της ίδιας ηλεκτρονικής πλατφόρμας. Με το ίδιο έγγραφο, η Αρχή ζήτησε την παροχή αναλυτικών πληροφοριών σχετικά με τη γενικότερη επεξεργασία προσωπικών δεδομένων

[1] Η σχετική ιστοσελίδα που χρησιμοποίησε για την κράτησή της ήταν η https://royalolympic.reserve-online.net/?bkcode=ENISA&checkin=2014-10-21

που πραγματοποιείται στο πλαίσιο ηλεκτρονικών κρατήσεων, όπως για το είδος των προσωπικών δεδομένων που τηρούνται, τη ροή της πληροφορίας από τη στιγμή που εισάγεται από τους πελάτες μέχρι την ολοκλήρωση της διαδικασίας της κράτησης, τα στοιχεία εταιρειών με τις οποίες ο υπεύθυνος επεξεργασίας συνεργάζεται στο πλαίσιο αυτό, τα τεχνικά μέτρα ασφάλειας που υλοποιούνται για την εν λόγω επεξεργασία συνολικά και, ειδικότερα, αν διαθέτει ο υπεύθυνος επεξεργασίας ή οι συνεργαζόμενες εταιρείες πιστοποίηση PCI/DSS.

Ακολούθως, ο υπεύθυνος επεξεργασίας απάντησε στην Αρχή με το υπ' αριθμ. πρωτ. Γ/ΕΙΣ/6668/04-11-2014 έγγραφό του, στο οποίο σημειώνονται τα εξής:

α) Ενημέρωσε αμέσως τον πάροχο της πλατφόρμας ηλεκτρονικών κρατήσεων WebHotelier (εφεξής σύστημα), από τον οποίο και θα πρέπει –όπως δήλωσε– να υπάρξουν οι απαντήσεις για τις ενέργειες στις οποίες έχει προβεί, καθώς επίσης και για τους λάθος χειρισμούς που οδήγησαν στη διαρροή προσωπικών δεδομένων.

β) Επικοινώνησε τόσο με τον ENISA, όσο και με τους τρεις προαναφερθέντες συνέδρους, για τη συλλογή πληροφοριών. Στο διάστημα αυτό των τεσσάρων ημερών, πιστοποιήθηκαν τρία επιπλέον κρούσματα απάτης μέσω του ENISA.

Στη συνέχεια, η εταιρεία WebHotelier Holdings LTD (εφεξής, WebHotelier), δια του εκπροσώπου της και μετόχου αυτής Δ, απέστειλε στην Αρχή το υπ' αριθμ. πρωτ. Γ/ΕΙΣ/256/19-01-2015 έγγραφο, με το οποίο αναφέρει ότι επηρεάστηκαν περί τους 20-25 χρήστες –βάσει της πληροφορίας που τους μετέφερε το ξενοδοχείο– καθώς επίσης και ότι το πρόβλημα διήρκεσε για διάστημα μικρότερο του εικοσιτετραώρου. Αναφέρει επίσης ότι εκλάπησαν δεδομένα πιστωτικών καρτών από ενεργές κρατήσεις που υπήρχαν στο σύστημα – όπου ενεργή νοείται μία μη ακυρωμένη κράτηση για την οποία δεν έχει γίνει αναχώρηση (check-out). Η WebHotelier περιγράφει επίσης και τις ενέργειες στις οποίες προέβη μετά το συμβάν, για την ενίσχυση της ασφάλειας του συστήματος, ενώ διευκρινίζει ότι το σύστημα κρατήσεων είναι πιστοποιημένο κατά PCI/DSS επιπέδου 3 και τηρεί όλους τους κανόνες διαδικτυακής ασφάλειας.

Δεδομένου ωστόσο ότι, μετά και τις ως άνω απαντήσεις, πολλά ζητήματα δεν αποσαφηνίστηκαν, η Αρχή με το υπ' αριθμ. πρωτ. Γ/ΕΞ/533/29-01-2105 έγγραφό της τόσο προς τον υπεύθυνο επεξεργασίας όσο και προς τη WebHotelier, ζήτησε περισσότερες διευκρινίσεις επί των κάτωθι ζητημάτων: α) ποια είναι επακριβώς η ροή της πληροφορίας, από τη στιγμή που οι πελάτες εισάγουν μέσω του σχετικού διαδικτυακού τόπου τα δεδομένα τους, προκειμένου να πραγματοποιήσουν κράτηση στο ξενοδοχείο, μέχρι την ολοκλήρωση

της διαδικασίας της κράτησης), β) ποια επακριβώς ήταν η ευπάθεια στη συνολική επεξεργασία των δεδομένων, η οποία οδήγησε στην εν λόγω διαρροή, καθώς επίσης και πώς διασφαλίζεται ότι τα μέτρα που εκ των υστέρων λήφθηκαν την αντιμετωπίζουν, γ) αν υπήρξε κατάλληλη ενημέρωση των πελατών εκείνων που πραγματοποίησαν κράτηση μέσω της ίδιας ηλεκτρονικής πλατφόρμας. Με το ίδιο έγγραφο η Αρχή ζήτησε τη χορήγηση αντιγράφου της πιστοποίησης κατά PCI/DSS. Ακολούθως, η WebHotelier απάντησε με το υπ' αριθμ. πρωτ. Γ/ΕΙΣ/1397/04-03-2015 έγγραφο, ενώ ο υπεύθυνος επεξεργασίας με το υπ' αριθμ. πρωτ. Γ/ΕΙΣ/1472/06-03-2015 έγγραφο.

Από το σύνολο όλων των ανωτέρω απαντήσεων, προκύπτουν τα εξής:

1. Οι πελάτες εισάγουν τα δεδομένα τους (ονοματεπώνυμο, διεύθυνση ηλεκτρονικού ταχυδρομείου, τηλέφωνο και στοιχεία πιστωτικής κάρτας) σε περιβάλλον που παρέχει η WebHotelier. Τα δεδομένα μεταφέρονται με ασφάλεια και αποθηκεύονται κρυπτογραφημένα, για λογαριασμό της WebHotelier, σε διακομιστή της Amazon (PCI Level 1).
2. Ο υπεύθυνος επεξεργασίας έχει πρόσβαση στα δεδομένα μέσω κωδικών πρόσβασης που του παρέχει η WebHotelier. Ο υπεύθυνος επεξεργασίας καταχωρεί την κράτηση στο ξενοδοχειακό πρόγραμμα Fidelio και μετά την αναχώρηση του πελάτη τα στοιχεία διαγράφονται. Σύμφωνα με την υπ' αριθμ. πρωτ. Γ/ΕΙΣ/1397/04-03-2015 απάντηση της WebHotelier, τα δεδομένα μπορούν να διαγράφονται είτε αυτόματα με την αναχώρηση του πελάτη είτε χειροκίνητα από τον υπεύθυνο επεξεργασίας με την πραγματοποίηση της χρέωσης.
3. Κανείς τρίτος, ούτε υπάλληλος της WebHotelier, δεν έχει πρόσβαση στα στοιχεία πληρωμής.

Κατά την άποψη του υπεύθυνου επεξεργασίας (βλ. υπ' αριθ. πρωτ. Γ/ΕΙΣ/6668/04-11-2014 και Γ/ΕΙΣ/1472/06-03-2015 έγγραφα), το ξενοδοχείο δεν ευθύνεται για την ως άνω διαρροή δεδομένων. Κατά την άποψη της WebHotelier (βλ. υπ' αριθ. πρωτ. Γ/ΕΙΣ/256/19-01-2015 και Γ/ΕΙΣ/1397/04-03-2015 έγγραφα), η διερεύνηση του συμβάντος κατέδειξε ότι εντοπίστηκε χρήστης με διαδικτυακή διεύθυνση (διεύθυνση IP) εξωτερικού, ο οποίος είχε γνώση των διαπιστευτηρίων (όνομα χρήστη και κωδικό πρόσβασης) συγκεκριμένου χρήστη του ξενοδοχείου, με αποτέλεσμα να εισέλθει στο σύστημα και να υποκλέψει προσωπικά δεδομένα πελατών. Επίσης, επισημαίνει ότι, με βάση τα αρχεία καταγραφής (log files), η σύνδεση ήταν επιτυχής με την πρώτη προσπάθεια, που σημαίνει ότι ήταν εκ των προτέρων

εις γνώσιν του ο κωδικός. Η πηγή της διαρροής των κωδικών δεν μπορεί να διευκρινιστεί, αλλά σημειώνεται από τη WebHotelier ότι δεν μπορεί να είναι από την ίδια την εταιρεία, αφού τα δεδομένα τηρούνται σε μορφή κρυπτογραφημένη και μη ανακτήσιμη. Η WebHotelier σημειώνει επίσης ότι δεν υπήρξε ανάλογο περιστατικό σε άλλον πελάτη/πελάτες της (σημειώνεται ότι η εταιρεία έχει ως πελάτες περισσότερα από 2600 ξενοδοχεία, σε πλέον των 30 χωρών).

Σημειώνεται επίσης ότι στο τελευταίο έγγραφο του υπευθύνου επεξεργασίας αναφέρεται ότι όλοι οι σύνεδροι ενημερώθηκαν –χωρίς να διευκρινίζονται λεπτομέρειες επί του τρόπου και είδους της ενημέρωσής τους– καθώς επίσης και ότι καταγράφηκαν έξι (6) κρούσματα απάτης σε διάστημα 4 ημερών (αριθμός που δεν συμφωνεί με τον αριθμό που αναφέρει η WebHotelier στην αρχική απάντησή της στην Αρχή).

Περαιτέρω, στο υπ' αριθμ. πρωτ. Γ/ΕΙΣ/1397/04-03-2015 έγγραφο η WebHotelier επισημαίνει ότι το εν λόγω περιστατικό θα μπορούσε να έχει αποτραπεί αν είχε τοποθετηθεί, με πρωτοβουλία του ξενοδοχείου, κατάλληλο φίλτρο έτσι ώστε η πρόσβαση στο σύστημα να είναι δυνατή μόνο από τη διαδικτυακή διεύθυνση του ξενοδοχείου η οποία είναι στατική (δηλαδή σταθερή και όχι μεταβαλλόμενη) – ενώ επισημαίνει ότι η WebHotelier παρέχει τη δυνατότητα να είναι επιτρεπτή η πρόσβαση στα στοιχεία πληρωμής μόνο από συγκεκριμένες διαδικτυακές διευθύνσεις, η οποία όμως δεν αξιοποιήθηκε. Επιπλέον, η WebHotelier σημειώνει ότι δεν εφαρμοζόταν ως πρακτική από το ξενοδοχείο η άμεση διαγραφή στοιχείων καρτών πληρωμής μετά τον έλεγχο εγκυρότητάς τους, γινόταν ωστόσο αυτόματη διαγραφή μετά την αναχώρηση των πελατών.

Τα μέτρα που ελήφθησαν από τη WebHotelier, μετά το εν λόγω περιστατικό, είναι τα εξής: α) υποχρεωτική αλλαγή των κωδικών πρόσβασης σε όλους τους χρήστες, β) τοποθέτηση IP φίλτρου στις IP διευθύνσεις που δύνανται να έχουν πρόσβαση στο σύστημα, έτσι ώστε προσβάσεις να είναι εφικτές μόνο από τη στατική IP διεύθυνση του υπευθύνου επεξεργασίας, γ) διαβάθμιση χρηστών ανάλογα με την προσβασιμότητα σε κρίσιμα δεδομένα, δ) έναρξη διαδικασίας για απευθείας σύνδεση με Τραπεζικά Ιδρύματα για την εκκαθάριση των συναλλαγών, ε) απαγόρευση σύνδεσης σε λογαριασμό του ξενοδοχείου από IP διεύθυνση εκτός Ελλάδας.

Η WebHotelier περιγράφει επίσης, στο ως άνω της έγγραφο, λίστα με λειτουργίες ασφαλείας που ήταν σε εφαρμογή πριν και μετά το συμβάν, όπως κρυπτογράφηση επικοινωνιών, ασφάλεια έναντι γνωστών επιθέσεων (Heartbleed, Poodle, Beast), πλήρη καταγραφή κάθε επιτυχημένης ή αποτυχημένης προσπάθειας σύνδεσης στο σύστημα, περιορισμό εισόδου στο σύστημα και πρόσβασης σε δεδομένα πιστωτικών καρτών βάσει IP

διεύθυνσης (ο υπεύθυνος επεξεργασίας δεν αξιοποιούσε, όπως προαναφέρθηκε, τις συγκεκριμένες δυνατότητες), πραγματοποίηση ελέγχων ασφαλείας από την TrustWave κάθε μήνα, ενώ επίσης τα συστήματα της WebHotelier έχουν λάβει πιστοποίηση κατά PCI DSS (level 3). Στο ίδιο έγγραφο η WebHotelier επισυνάπτει τόσο τα αποτελέσματα από έλεγχο ανίχνευσης ευπαθειών που διενέργησε η TrustWave στις 26-01-2015 (όπου καταδεικνύεται η μη ανίχνευση ευπαθειών), καθώς επίσης και το σχετικό πιστοποιητικό PCI DSS. Σημειώνεται ωστόσο ότι στο πιστοποιητικό αυτό δεν αναφέρεται αν πρόκειται για πιστοποιητικό επιπέδου 3, ενώ στο διαδικτυακό τόπο της Webhotelier (και ειδικότετα, στο διαδικτυακό σύνδεσμο https://www.webhotelier.net/features, αναφέρεται ότι η εταιρεία είναι πιστοποιημένη κατά το πρότυπο PCI/DSS επιπέδου 2).

Στη συνέχεια, η Αρχή απηύθυνε νέα επιμέρους ερωτήματα τόσο προς τον υπεύθυνο επεξεργασίας (με το υπ' αριθμ. πρωτ. Γ/ΕΞ/2230/08-04-2015 έγγραφό της) όσο και προς τη WebHotelier (με το υπ' αριθμ. πρωτ. Γ/ΕΞ/2231/08-04-2015 έγγραφό της), αναφορικά με ειδικά ζητήματα τα οποία είτε δεν είχαν καλυφθεί πλήρως είτε ανέκυψαν από τις προηγούμενες απαντήσεις. Ειδικότερα, με τα ως άνω έγγραφα η Αρχή ζήτησε διευκρινίσεις περί: α) του συστήματος (ηλεκτρονικής πλατφόρμας) που παρέχει η WebHotelier στον υπεύθυνο επεξεργασίας για τη διαχείριση των κρατήσεων των πελατών, ως προς το αν είναι προσβάσιμη σε οποιονδήποτε γνωρίζει τη σχετική διαδικτυακή διεύθυνση (URL) αυτής (αν είναι δηλαδή web-based εφαρμογή), β) του αριθμού των λογαριασμών χρηστών (όνομα πρόσβασης – κωδικός πρόσβασης) των υπαλλήλων του υπευθύνου επεξεργασίας που συνδέονται στην ανωτέρω πλατφόρμα, καθώς και ειδικότερα περί των συνθηματικών αυτών, γ) του ακριβούς είδους προσωπικών δεδομένων στα οποία αποκτούσε κανείς πρόσβαση μέσω των ως άνω συνθηματικών (αν π.χ. αποκτούσε πρόσβαση σε δεδομένα των πελατών που πραγματοποίησαν κράτηση μόνο για το συγκεκριμένο συνέδριο που διοργάνωνε ο ENISA ή και στα δεδομένα οποιουδήποτε άλλου είχε πραγματοποιήσει –ανεξάρτητα του συνεδρίου– ηλεκτρονική κράτηση, ποια επακριβώς προσωπικά δεδομένα πελατών προσπελαύνονται κτλ.), δ) του ακριβούς αριθμού ατόμων των οποίων τα δεδομένα διέρρευσαν – δεδομένου ότι στο υπ' αριθμ. πρωτ. Γ/ΕΙΣ/6668/04-11-2014 έγγραφο του υπευθύνου επεξεργασίας αναφέρεται ότι καταγράφηκαν έξι (6) κρούσματα απάτης σε διάστημα τεσσάρων (4) ημερών, ενώ η εταιρεία WebHotelier αναφέρει στο υπ' αριθμ. πρωτ. Γ/ΕΙΣ/256/19-01-2015 έγγραφό της ότι επηρεάστηκαν περί τους 20-25 πελάτες, κατόπιν ενημέρωσης που είχε από τον υπεύθυνο επεξεργασίας, ε) του τρόπου ενημέρωσης όλων όσων τα προσωπικά δεδομένα εκτέθηκαν λόγω του περιστατικού, καθώς και του ακριβούς

περιεχομένου της ενημέρωσης αυτής, στ) του χρόνου πραγματοποίησης της διαγραφής των δεδομένων των πελατών από το σύστημα. Τόσο ο υπεύθυνος επεξεργασίας, όσο και η εταιρεία WebHotelier απέστειλαν εγγράφως τις νέες απαντήσεις τους με τα υπ' αριθμ. πρωτ. Γ/ΕΙΣ/2428/28-04-2015 και Γ/ΕΙΣ/2429/28-04-2015 έγγραφά τους – στη δε απάντηση του υπεύθυνου επεξεργασίας επισυνάπτεται –κατόπιν σχετικού αιτήματος της Αρχής– και η σύμβαση που έχει συνάψει με την εταιρεία RezLogic Cyprus LTD, αντικείμενο της οποίας είναι η παροχή της υπηρεσίας WebHotelier[2].

Από τις ως άνω απαντήσεις, προκύπτουν τα εξής:

α) Η ηλεκτρονική πλατφόρμα που παρέχει η WebHotelier στον υπεύθυνο επεξεργασίας είναι διαδικτυακή (web-based), και η διεύθυνση του σχετικού διαδικτυακού τόπου είναι https://hotel.webhotelier.net/. Το ξενοδοχειακό πρόγραμμα Fidelio είναι ανεξάρτητο πρόγραμμα για την καταχώριση κρατήσεων.

β) Το σύστημα προσφέρει τη δυνατότητα χρήσης απεριόριστου αριθμού λογαριασμών χρηστών ανά ξενοδοχείο. Η WebHotelier παρέχει αρχικά, σε κάθε πελάτη της (ξενοδοχείο), ένα λογαριασμό με οδηγίες για το πώς μπορούν να δημιουργηθούν νέοι λογαριασμοί, για κάθε υπάλληλο που χρειάζεται πρόσβαση. Στους χρήστες της πλατφόρμας παρέχεται η δυνατότητα αλλαγής των κωδικών πρόσβασης. Ως προς την επιλογή των κωδικών πρόσβασης, η WebHotelier επισημαίνει ότι ήταν σε ισχύ έλεγχος της πολυπλοκότητάς τους –τόσο για τα αρχικά, όσο και για αυτά που μπορούσε εκ των υστέρων να επιλέξει ο χρήστης– χωρίς όμως να διευκρινίζονται τα κριτήρια βάσει των οποίων ένα συνθηματικό δεν γίνεται αποδεκτό ως ανασφαλές/προβλέψιμο. Αναφέρεται μόνο ότι χρησιμοποιείται βάση δεδομένων με χιλιάδες κωδικούς που χρησιμοποιούνται συχνά, των οποίων η επιλογή δεν γίνεται δεκτή, ενώ επίσης, όταν γίνεται αλλαγή κωδικού, απαγορεύεται η εισαγωγή κωδικών που έχουν χρησιμοποιηθεί στο παρελθόν. Σε περίπτωση τριών συνεχόμενων αποτυχημένων προσπαθειών σύνδεσης, το σύστημα «κλειδώνει» το συγκεκριμένο λογαριασμό χρήστη και ο χρήστης υποχρεούται να αλλάξει τον κωδικό πρόσβασής του με αποστολή e-mail στην ηλεκτρονική διεύθυνση που έχει δηλώσει ο χρήστης.

Την περίοδο που συνέβη το περιστατικό παραβίασης δεδομένων, υπήρχαν δύο διαφορετικοί λογαριασμοί χρηστών για το ξενοδοχείο (υπεύθυνο επεξεργασίας) για σύνδεση στην πλατφόρμα. Οι κωδικοί πρόσβασης αυτών δεν ήταν οι αρχικά ορισμένοι από τη WebHotelier αλλά είχαν μεταβληθεί από τους υπαλλήλους-χρήστες του υπευθύνου

[2] Κατόπιν τηλεφωνικής επικοινωνίας με τον Δ στις 4/5/2015, και όπως επιβεβαιώθηκε μετέπειτα και κατά την ακρόαση του Δ στη συνεδρίαση της Αρχής στις 26/5/2015, προκύπτει ότι η εταιρεία Webhotelier Holdings LTD είναι υπεύθυνη για τα πνευματικά δικαιώματα της πλατφόρμας Webhotelier. Άλλες εταιρείες –όπως εν προκειμένω η RezLogic– αναλαμβάνουν την προώθηση αυτής.

επεξεργασίας. Σημειώνεται ότι το σύστημα παρέχει τη δυνατότητα «απομνημόνευσης» των κωδικών πρόσβασης (επιλογή «Remember Me»), αφήνοντας στη δικαιοδοσία του χρήστη την επιλογή.

γ) Με τη γνώση των ανωτέρω κωδικών, αποκτούσε κανείς πρόσβαση στα δεδομένα των πελατών του ξενοδοχείου που είχαν ενεργές κρατήσεις (δηλ. είχαν πραγματοποιήσει κράτηση αλλά δεν είχαν κάνει, κατά τη συγκεκριμένη περίοδο, αναχώρηση (check-out)), ανεξαρτήτως του αν η κράτηση αφορούσε το συγκεκριμένο συνέδριο ή όχι.

δ) Ως προς τον αριθμό των πελατών του υπευθύνου επεξεργασίας των οποίων τα δεδομένα διέρρευσαν, η WebHotelier στο υπ' αριθμ. πρωτ. Γ/ΕΙΣ/2429/28-04-2015 έγγραφό της αναφέρει ότι δεν είναι σε θέση να γνωρίζει ποιοι πελάτες είχαν αναφέρει παράπονα στην διεύθυνση του ξενοδοχείου, και σε κάθε περίπτωση το νούμερο που έχει δηλωθεί από τον υπεύθυνο επεξεργασίας είναι και το πλέον αξιόπιστο. Ο υπεύθυνος επεξεργασίας, με το υπ' αριθμ. πρωτ. Γ/ΕΙΣ/2428/28-04-2015 έγγραφό του, αναφέρει ότι τα επιβεβαιωμένα κρούσματα απάτης είναι έξι (6) – ενώ η εκτίμηση για 20-25 πελάτες έγινε λαμβάνοντας υπόψη όλους τους σύνεδρους του συγκεκριμένου συνεδρίου, μια και ήταν το ίδιο πιθανό να έχουν υπάρξει θύματα απάτης.

ε) Το είδος των προσωπικών δεδομένων των πελατών που μπορούσε κανείς να προσπελάσει με τη σύνδεσή του στη συγκεκριμένη ηλεκτρονική πλατφόρμα, ήταν το όνομα, επώνυμο, τηλέφωνο επικοινωνίας, ηλεκτρονική διεύθυνση (email), στοιχεία πιστωτικής κάρτας (αριθμός, αριθμός ασφαλείας CVV, ημερομηνία λήξης, ονοματεπώνυμο κατόχου), ενώ προαιρετικά οι πελάτες μπορούσαν να έχουν εισάγει και την ταχυδρομική τους διεύθυνση.

στ) Ως προς την ενημέρωση όλων των πελατών του υπευθύνου επεξεργασίας των οποίων τα δεδομένα διέρρευσαν, ο υπεύθυνος επεξεργασίας με το υπ' αριθμ. πρωτ. Γ/ΕΙΣ/2428/28-04-2015 έγγραφό του επαναλαμβάνει τα όσα είχε ήδη αναφέρει και στο αρχικό Γ/ΕΙΣ/6668/04-11-2014 έγγραφό του – δηλαδή, ότι έγινε μέσω του υπευθύνου του συνεδρίου από την πλευρά του ENISA (Ε), ο οποίος ήταν ο συνδετικός κρίκος επικοινωνίας με τους συνέδρους, αλλά και πιο γρήγορος τρόπος επαφής για άμεση ενημέρωση. Δεν αναφέρει αν τελικά ενημερώθηκαν όλοι όσων τα δεδομένα βρίσκονταν στο σύστημα εκείνη τη στιγμή – ανεξαρτήτως του αν για αυτούς παρατηρήθηκε κρούσμα ή όχι– ενώ επίσης δεν γίνεται καμία αναφορά σε περιπτώσεις κρατήσεων άλλων, πέραν αυτών για το συγκεκριμένο συνέδριο.

ζ) Η αυτόματη διαγραφή δεδομένων πιστωτικής κάρτας γίνεται μετά την αναχώρηση (check-out) του πελάτη. Δεν πραγματοποιήθηκε «χειροκίνητη» (μη αυτόματη) διαγραφή.

Το ξενοδοχείο Royal Olympic (επιχείρηση ΟΛΥΜΠΙΩΝ ΞΕΝΟΔΟΧΕΙΩΝ ΑΕ) κλήθηκε νομίμως, με το υπ' αριθμ. πρωτ. Γ/ΕΞ/2705/12-05-2015 έγγραφο της Αρχής, σε ακρόαση ενώπιον της Αρχής στη συνεδρίαση της 26-05-2015, ως υπεύθυνος επεξεργασίας, για να δώσει περαιτέρω διευκρινίσεις και να εκθέσει διεξοδικά τις απόψεις του επί των ανωτέρω. Για την ίδια συνεδρίαση κλήθηκε, με το υπ' αριθμ. πρωτ. Γ/ΕΞ/2706/12-05-2015, και ο Δ, μέτοχος της εταιρείας WebHotelier και ιδιοκτήτης της εταιρείας Ψ, η οποία είναι –κατά δήλωσή του– υπεργολάβος εταιρεία για την τεχνική υποστήριξη των χρηστών του συστήματος της WebHotelier στην Ελλάδα. Με το ίδιο έγγραφο ζητήθηκε να προσκομισθούν στην Αρχή αντίγραφα από τα αρχεία καταγραφής των διαδικτυακών προσβάσεων στην εφαρμογή κατά το διάστημα της διαρροής, που να τεκμηριώνουν το είδος και το πλήθος των μη εξουσιοδοτημένων προσβάσεων στην εφαρμογή, καθώς και τις σχετικές διαδικτυακές διευθύνσεις (διευθύνσεις IP) από τις οποίες πραγματοποιήθηκαν οι προσβάσεις. Το σχετικό αντίγραφο υποβλήθηκε στην Αρχή με το υπ' αριθμ. πρωτ. Γ/ΕΙΣ/2979/26-05-2015 έγγραφο.

Στη συνεδρίαση της 26-05-2015, παρέστησαν νομίμως, ως εκπρόσωπος του υπευθύνου επεξεργασίας, ο ΣΤ, νομικός σύμβουλος, καθώς επίσης και ο Δ, ως εκπρόσωπος της WebHotelier αλλά και της υπεργολάβου εταιρείας Ψ. Κατά την ακρόαση, οι ως άνω εκπρόσωποι εξέθεσαν προφορικά τις απόψεις τους. Κατόπιν της ακρόασης, τόσο ο υπεύθυνος επεξεργασίας όσο και ο Δ κατέθεσαν εμπροθέσμως σχετικά υπομνήματα (αρ. πρωτ. Γ/ΕΙΣ/3115/02-06-2015 και Γ/ΕΙΣ/3116/02-06-2015 αντίστοιχα).

Στο υπόμνημα του υπευθύνου επεξεργασίας αναφέρονται τα εξής: α) Η επιχείρηση λειτουργεί από το 1969, χωρίς να έχει αντιμετωπίσει ποτέ παρόμοιο ή ανάλογο περιστατικό απάτης, β) Το εν λόγω περιστατικό έλαβε χώρα στις 14-10-2014 και η επιχείρηση έλαβε γνώση στις 15-10-2014 αρχικώς μέσω τηλεφώνου και ακολούθως μέσω ηλεκτρονικού ταχυδρομείου από τον Ε εκ μέρους του ENISA. Αρχικά αναφέρθηκαν τρεις περιπτώσεις απάτης και στη συνέχεια προέκυψαν άλλες τρεις, όπου όλες αφορούσαν συμμετέχοντες στο εν λόγω συνέδριο του ENISA. Επακολούθησε ηλεκτρονική αλληλογραφία τόσο με τον Ε όσο και με τα άτομα των οποίων τα δεδομένα διέρρευσαν (η σχετική αλληλογραφία επισυνάπτεται στο εν λόγω υπόμνημα). γ) Το συνέδριο έλαβε χώρα λίγες μέρες μετά το συμβάν –συγκεκριμένα από 21-10-2015 μέχρι και 24-10-2015– οπότε και δεν εστάλη στους λοιπούς συμμετέχοντες αυτού σχετική ηλεκτρονική αλληλογραφία ενημερωτική για το περιστατικό που έλαβε χώρα, αλλά ρωτήθηκαν όλοι –συνολικά 20 άτομα– κατά τη διάρκεια του εν λόγω συνεδρίου, δ) Το ξενοδοχειακό πρόγραμμα Fidelio δεν ήταν διασυνδεδεμένο με την πλατφόρμα της WebHotelier, ε) Ο κωδικός πρόσβασης του χρήστη που φέρεται να χρησιμοποιήθηκε για την επίθεση ασφαλείας που προκάλεσε το εν λόγω περιστατικό

παραβίασης δεδομένων ήταν ο «…», στ) Ο υπεύθυνος επεξεργασίας προέβη σε όλες τις διαδικασίες ασφαλείας που του υποδείχθηκαν από τον υπεργολάβο και πάροχο τεχνικής υποστήριξης της πλατφόρμας WebHotelier[3]. Τέλος, ο υπεύθυνος επεξεργασίας καταλήγει ότι άμεσα (εντός μηνός) προχωρεί στην υπογραφή σχετικής σύμβασης με Τράπεζα, ώστε να εξαντλήσει τη δυνατότητα που του παρέχεται από την αγορά για βέλτιστη ασφάλεια των συναλλαγών με πιστωτικές κάρτες.

Από την πλευρά του ο Δ, με το ως άνω υπόμνημά του επαναλαμβάνει τις λειτουργίες ασφαλείας της πλατφόρμας της WebHotelier που ήταν σε ισχύ κατά την περίοδο που έλαβε χώρα το εν λόγω περιστατικό, ενώ αναφορικά με τους νέους μηχανισμούς ασφαλείας μετά το περιστατικό αναφέρει ότι στο εξής θα πραγματοποιείται: α) Διαβάθμιση χρηστών ανάλογα με την προσβασιμότητα σε κρίσιμα δεδομένα, β) Έναρξη διαδικασίας για την απευθείας σύνδεση με Τραπεζικά Ιδρύματα για την εκκαθάριση των συναλλαγών, γ) Υποστήριξη αυθεντικοποίησης δύο παραγόντων (two-factor authentication) για όλους τους χρήστες, δ) «Κλείδωμα» (Lock-out) του λογαριασμού του χρήστη σε περίπτωση τριών αποτυχημένων προσπαθειών πρόσβασης.

Η Αρχή, μετά από εξέταση των προαναφερομένων στοιχείων και μνεία των λεχθέντων κατά τη συνεδρίαση της 26-05-2015, άκουσε τον εισηγητή και τις διευκρινίσεις των βοηθών εισηγητή, οι οποίοι στη συνέχεια αποχώρησαν πριν από τη διάσκεψη και τη λήψη απόφασης, κατόπιν διεξοδικής συζήτησης,

ΣΚΕΦΘΗΚΕ ΣΥΜΦΩΝΑ ΜΕ ΤΟ ΝΟΜΟ

1. Το άρθρο 2 του ν. 2472/1997, ορίζει ότι «δεδομένα προσωπικού χαρακτήρα» είναι «κάθε πληροφορία που αναφέρεται στο υποκείμενο των δεδομένων». «Υποκείμενο των δεδομένων» είναι «το φυσικό πρόσωπο στο οποίο αναφέρονται τα δεδομένα, και του οποίου η ταυτότητα είναι γνωστή ή μπορεί να εξακριβωθεί, δηλαδή μπορεί να προσδιορισθεί αμέσως ή εμμέσως, ιδίως βάσει αριθμού ταυτότητας ή βάσει ενός η περισσότερων συγκεκριμένων στοιχείων που χαρακτηρίζουν την υπόστασή του από άποψη φυσική, βιολογική, ψυχική, οικονομική, πολιτιστική, πολιτική ή κοινωνική». Ως εκ τούτου, σημειώνεται ότι τα δεδομένα πιστωτικών καρτών, βάσει των ανωτέρω, αποτελούν δεδομένα προσωπικού χαρακτήρα.

[3] Οι οποίες διαδικασίες ωστόσο δεν κατονομάζονται στο εν λόγω υπόμνημα

Στο ίδιο άρθρο επίσης ορίζεται ως επεξεργασία δεδομένων προσωπικού χαρακτήρα «κάθε εργασία ή σειρά εργασιών που πραγματοποιείται, από το Δημόσιο ή από νομικό πρόσωπο δημοσίου δικαίου ή ιδιωτικού δικαίου ή ένωση προσώπων ή φυσικό πρόσωπο με ή χωρίς τη βοήθεια αυτοματοποιημένων μεθόδων και εφαρμόζονται σε δεδομένα προσωπικού χαρακτήρα, όπως η συλλογή, η καταχώριση, η οργάνωση, η διατήρηση ή αποθήκευση, η τροποποίηση, η εξαγωγή, η χρήση, η διαβίβαση, η διάδοση ή κάθε άλλης μορφής διάθεση, η συσχέτιση ή ο συνδυασμός, η διασύνδεση, η δέσμευση (κλείδωμα), η διαγραφή, η καταστροφή».

Περαιτέρω, ως υπεύθυνος επεξεργασίας ορίζεται οποιοσδήποτε καθορίζει το σκοπό και τον τρόπο επεξεργασίας των δεδομένων προσωπικού χαρακτήρα, όπως φυσικό ή νομικό πρόσωπο, δημόσια αρχή ή υπηρεσία ή οποιοσδήποτε άλλος οργανισμός, ενώ ως εκτελών την επεξεργασία ορίζεται οποιοσδήποτε επεξεργάζεται δεδομένα προσωπικού χαρακτήρα για λογαριασμό του υπευθύνου επεξεργασίας (φυσικό ή νομικό πρόσωπο, δημόσια αρχή ή υπηρεσία ή οποιοσδήποτε άλλος οργανισμός).

Με βάση τα ανωτέρω, για τη συγκεκριμένη επεξεργασία των προσωπικών δεδομένων των πελατών του ξενοδοχείου, υπεύθυνος επεξεργασίας είναι το ξενοδοχείο Royal Olympic, ενώ η εταιρεία RezLogic Cyprus Ltd, η οποία παρέχει την πλατφόρμα ηλεκτρονικών κρατήσεων της WebHotelier στο ξενοδοχείο, αποτελεί εκτελούσα την επεξεργασία[4]. Περαιτέρω, και η εταιρεία WebHotelier Holdings LTD που αναπτύσσει την εν λόγω πλατφόρμα, αποτελεί επίσης εκτελούσα την επεξεργασία.

2. Το άρθρο 10, παρ. 3 του ν. 2472/1997 ορίζει ότι ο υπεύθυνος επεξεργασίας οφείλει να λαμβάνει τα κατάλληλα οργανωτικά και τεχνικά μέτρα για την ασφάλεια των δεδομένων και την προστασία τους από τυχαία ή αθέμιτη καταστροφή, τυχαία απώλεια, αλλοίωση, απαγορευμένη διάδοση ή πρόσβαση και κάθε άλλη μορφή αθέμιτης επεξεργασίας. Αυτά τα μέτρα πρέπει να εξασφαλίζουν επίπεδο ασφαλείας ανάλογο προς τους κινδύνους που συνεπάγεται η επεξεργασία και η φύση των δεδομένων που είναι αντικείμενο της επεξεργασίας. Στο ίδιο άρθρο αναφέρεται ότι ο υπεύθυνος επεξεργασίας οφείλει να επιλέγει πρόσωπα με αντίστοιχα επαγγελματικά προσόντα που παρέχουν επαρκείς εγγυήσεις από

[4] Όπως επισημαίνεται στη Γνώμη 1/2010 της Ομάδας Εργασίας του Άρθρου 29, «*το γεγονός ότι η σύμβαση και αναλυτικοί συναλλακτικοί όροι της καταρτίζονται από τον πάροχο των υπηρεσιών και όχι από τον υπεύθυνο της επεξεργασίας δεν αποτελεί από μόνο του επαρκή βάση για να εξαχθεί το συμπέρασμα ότι ο πάροχος των υπηρεσιών πρέπει να θεωρηθεί υπεύθυνος της επεξεργασίας, στον βαθμό που ο υπεύθυνος της επεξεργασίας αποδέχθηκε ελεύθερα τους συμβατικούς όρους, αποδεχόμενος έτσι την πλήρη ευθύνη για αυτούς. Στο ίδιο πνεύμα, η ανισότητα διαπραγματευτικής ισχύος μεταξύ ενός μικρού υπευθύνου της επεξεργασίας δεδομένων και μεγάλων παρόχων υπηρεσιών δεν πρέπει να θεωρείται δικαιολογία για τον υπεύθυνο της επεξεργασίας ώστε να δεχθεί συμβατικές ρήτρες και όρους οι οποίοι δεν είναι σύμφωνοι προς τη νομοθεσία για την προστασία των δεδομένων*»

πλευράς τεχνικών γνώσεων και προσωπικής ακεραιότητας για την τήρηση του απορρήτου. Η σχετική ανάθεση γίνεται υποχρεωτικά εγγράφως. Οι υποχρεώσεις του άρθρου αυτού βαρύνουν επίσης και τον εκτελούντα την επεξεργασία.

Ειδικά για την ασφάλεια σε ηλεκτρονικές πληρωμές, σημείο αναφοράς αποτελεί το διεθνώς αναγνωρισμένο πρότυπο ασφαλείας Payment Card Industry Data Security Standard (PCI/DSS). Το PCI/DSS αναπτύχθηκε από το ανοιχτό παγκόσμιο forum Payment Card Industry Security Standards Council για να ενισχύσει την ασφάλεια των δεδομένων του κατόχου πιστωτικών καρτών μέσω της υιοθέτησης ενιαίων μέτρων ασφαλείας παγκοσμίως. Το πρότυπο αυτό απευθύνεται σε όλους τους φορείς που εμπλέκονται στην επεξεργασία πληρωμών με πιστωτική κάρτα, συμπεριλαμβανομένων των εμπόρων, των φορέων παροχής υπηρεσιών, καθώς και όλων των μερών που αποθηκεύουν, επεξεργάζονται ή μεταδίδουν δεδομένα κατόχων καρτών[5]. Σημειώνεται ότι το πρότυπο PCI/DSS προβλέπει ότι ο αριθμός ασφαλείας (CVC/CVV) της πιστωτικής κάρτας δεν πρέπει να αποθηκεύεται, ακόμα και αν πρόκειται για τήρησή του σε κρυπτογραφημένη μορφή[6].

3. Ως περιστατικό παραβίασης προσωπικών δεδομένων θεωρείται κάθε περίπτωση παραβίασης της ασφάλειας των δεδομένων όπως τυχαία ή παράνομη καταστροφή, απώλεια, αλλοίωση, μη εξουσιοδοτημένη διάδοση ή προσπέλαση και κάθε άλλη μορφή αθέμιτης επεξεργασίας δεδομένων προσωπικού χαρακτήρα που διαβιβάσθηκαν, αποθηκεύτηκαν ή υποβλήθηκαν κατά οποιονδήποτε άλλον τρόπο σε επεξεργασία στο πλαίσιο του χρησιμοποιούμενου συστήματος επεξεργασίας (βλ. επίσης και άρθρο 2 του ν. 3471/2006 για την προστασία των προσωπικών δεδομένων στον τομέα των ηλεκτρονικών επικοινωνιών, όπως τροποποιήθηκε με το ν. 4070/2012).

Το συγκεκριμένο περιστατικό αφορά στη διαρροή προσωπικών δεδομένων πελατών του υπεύθυνου επεξεργασίας –συμπεριλαμβανομένων δεδομένων πιστωτικών καρτών– σε άγνωστους τρίτους. Ως εκ τούτου αποτελεί περιστατικό παραβίασης των προσωπικών δεδομένων των εν λόγω χρηστών, καθώς τα προσωπικά δεδομένα τους διέρρευσαν σε μη εξουσιοδοτημένα πρόσωπα. Μάλιστα, από την εν λόγω διαρροή υπήρξαν εξαιρετικά δυσμενείς συνέπειες για τα υποκείμενα των δεδομένων (χρεώσεις, αλλά και απόπειρες χρεώσεων, στις πιστωτικές τους κάρτες) – ενώ σε κάθε περίπτωση, η διαρροή των στοιχείων των πιστωτικών καρτών σε αγνώστους μπορεί ανά πάσα στιγμή στο μέλλον να πλήξει τα

[5] https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf

[6] Στο πρότυπο PCI/DSS οι αριθμοί ασφαλείας θεωρούνται ως «κρίσιμα» δεδομένα ταυτοποίησης (sensitive authentication data), και ως προς αυτά αναφέρεται το εξής: «*Do not store sensitive authentication data after authorization (even if encrypted)* (…).*It is permissible for issuers and companies that support issuing services to store sensitive authentication data if there is a business justification and the data is stored securely*»

υποκείμενα των δεδομένων, εφόσον αυτά δεν έχουν αντιληφθεί την εν λόγω διαρροή.

4. Από την εξέταση του φακέλου της υπόθεσης, προκύπτει ότι γενεσιουργό αιτία του εν λόγω περιστατικού αποτέλεσε το γεγονός ότι άγνωστος χρήστης συνδέθηκε απομακρυσμένα στην ηλεκτρονική πλατφόρμα που διαθέτει η εκτελούσα την επεξεργασία προς τον υπεύθυνο επεξεργασίας, γνωρίζοντας έναν κωδικό πρόσβασης χρήστη του τελευταίου. Με βάση το αρχείο καταγραφής των προσβάσεων στην εν λόγω πλατφόρμα που υπεβλήθη στην Αρχή με το υπ' αριθμ. πρωτ. Γ/ΕΙΣ/2979/26-05-2015 έγγραφο που αφορά στις προσβάσεις από 29 Σεπτεμβρίου μέχρι 5 Νοεμβρίου 2014, φαίνεται ότι η εν λόγω απομακρυσμένη πρόσβαση πραγματοποιήθηκε στις 13-10-2014 με τον κωδικό πρόσβασης του χρήστη με όνομα «Χ» (αφού είναι η μοναδική καταχώρηση στο εν λόγω αρχείο, που αντιστοιχεί σε μη ελληνική διαδικτυακή διεύθυνση του συνδεόμενου χρήστη). Δεν υπάρχουν αρχεία καταγραφής αναφορικά με τις ενέργειες στις οποίες προέβη ο χρήστης, εντός του συστήματος, από τη στιγμή της σύνδεσής του, καθώς την χρονική περίοδο που συνέβη το περιστατικό δεν τηρούνταν τέτοια αρχεία. Ωστόσο, όπως δηλώνει ο εκπρόσωπος της WebHotelier στα έγγραφά του, με τη σύνδεση αυτή αποκτήθηκε πρόσβαση σε στοιχεία πελατών του υπευθύνου επεξεργασίας οι οποίοι είχαν πραγματοποιήσει ηλεκτρονικά κράτηση και οι κρατήσεις ήταν ενεργές (ο αριθμός των οποίων, όπως επισημαίνει ο εκπρόσωπος της WebHotelier στο ως άνω έγγραφό του, ήταν 227 κατά τη στιγμή του περιστατικού). Δεδομένου ότι οι προσβάσεις αυτές πραγματοποιήθηκαν από διαδικτυακή διεύθυνση (IP) εξωτερικού, φαίνεται ότι πιθανότατα, η εν λόγω σύνδεση έγινε απευθείας στο σύστημα από απομακρυσμένο υπολογιστή που ήταν υπό τον έλεγχο του επιτιθέμενου και όχι μέσω υπολογιστή υπαλλήλου του υπευθύνου επεξεργασίας. Η επιτυχής πρόσβαση πραγματοποιήθηκε ωστόσο με χρήση ενός από τους δύο συνολικά διαθέσιμους λογαριασμούς χρήστη των υπαλλήλων του ξενοδοχείου – βάσει των αρχείων καταγραφής της WebHotelier, ο κωδικός πρόσβασης του οποίου μάλιστα ήταν εις γνώσιν μόνο του υπευθύνου επεξεργασίας. Σημειώνεται ότι ο εν λόγω κωδικός πρόσβασης («…») που χρησιμοποιούνταν δεν μπορεί να χαρακτηριστεί ως απόλυτα ασφαλής (αφού αποτελείται από έξι μόνο αλφαριθμητικά στοιχεία, εκ των οποίων τα δύο πρώτα ταυτίζονται με τους αρχικούς χαρακτήρες του ονόματος του χρήστη του λογαριασμού «Χ»). Δεδομένου ότι δεν προσκομίστηκε πλήρες και αναλυτικό αρχείο καταγραφής των επιτυχών ή ανεπιτυχών προσβάσεων στον εξυπηρετητή διαδικτύου της εφαρμογής, ο τρόπος διαρροής και της μη εξουσιοδοτημένης πρόσβασης δεν μπορεί να τεκμηριωθεί με ακρίβεια. Για παράδειγμα δεν μπορεί να τεκμηριωθεί ότι το ξενοδοχείο δεν αποτέλεσε στόχο διαδικτυακής επίθεσης, περίπτωση στην οποία θα έπρεπε να ληφθεί η αντίστοιχη προστασία μέσω κατάλληλου

διαδικτυακού εξοπλισμού (π.χ. τείχος προστασίας). Αντιστοίχως, δεδομένου ότι δεν προσκομίστηκαν περισσότερα αρχεία καταγραφής ή σχέδια ασφάλειας και πληροφοριακής υποδομής του υπευθύνου επεξεργασίας, παρότι συζητήθηκε κατά την ακρόαση, δεν μπορεί να αποκλειστεί το ενδεχόμενο ο κωδικός ασφαλείας που χρησιμοποιήθηκε κατά την πρόσβαση να υποκλάπηκε μέσω κοινωνικής μηχανικής (social engineering) ή τοπικής πρόσβασης στον υπολογιστή του υπαλλήλου του ξενοδοχείου π.χ. μέσω τεχνικών παραπλάνησης μέσω ηλεκτρονικού ταχυδρομείου (spear phishing) και εκτέλεσης κακόβουλου κώδικα (π.χ. keylogger).

Σε κάθε περίπτωση, σημειώνεται ότι εάν δεν είχε τηρηθεί στο σύστημα το σύνολο των στοιχείων της πιστωτικής κάρτας (αριθμός κάρτας, αριθμός ασφαλείας αυτής, ημερομηνία λήξης), τότε οι συνέπειες –από το ως άνω περιστατικό– για τα υποκείμενα των δεδομένων θα εξακολουθούσαν μεν να ήταν σοβαρές αλλά όχι στον ίδιο μεγάλο βαθμό – αφού, δεν θα ήταν το ίδιο μεγάλος ο κίνδυνος παράνομης χρήσης των πιστωτικών καρτών, τα στοιχεία των οποίων θα είχαν διαρρεύσει, για την πραγματοποίηση ηλεκτρονικών συναλλαγών μέσω καρτών όπου ζητούνται όλα τα στοιχεία αυτών, όπως περιγράφονται ανωτέρω. Εξάλλου, η συμμόρφωση με το προαναφερθέν πρότυπο PCI/DSS προβλέπει τη μη τήρηση του αριθμού ασφαλείας CCV/CVV.

Σημειώνεται ότι –όπως προαναφέρθηκε– η Webhotelier, με το υπ' αριθμ. πρωτ. Γ/ΕΙΣ/1397/04-03-2015 έγγραφό της υπέβαλε στην Αρχή το πιστοποιητικό PCI/DSS (το οποίο έχει χορηγηθεί από την εταιρεία TrustWave). Ωστόσο, όπως προκύπτει και από την επισυναπτόμενη, στο ίδιο έγγραφο, αναφορά ελέγχου ανίχνευσης ευπαθειών που πραγματοποίησε η TrustWave στη WebHotelier (βάσει του αποτελέσματος της οποίας φαίνεται ότι εκδόθηκε το ως άνω πιστοποιητικό), ο έλεγχος αυτός δεν συνεπάγεται την καθολική συμμόρφωση της εταιρείας με το πρότυπο PCI/DSS[7].

Πέρα από τα ανωτέρω, επισημαίνεται ότι ο υπεύθυνος επεξεργασίας δεν είχε θέσει σε εφαρμογή την τεχνική δυνατότητα που υπήρχε να επιτρέπονται μόνο εκείνες οι προσβάσεις που επιχειρούνται από συγκεκριμένες στατικές IP διευθύνσεις που του ανήκαν – σημειώνεται ότι, αν αυτή η δυνατότητα είχε τεθεί σε εφαρμογή, φαίνεται ότι το ανωτέρω περιστατικό ασφαλείας θα είχε αποτραπεί. Περαιτέρω, δεν τηρούνταν αρχεία καταγραφής για τις ενέργειες των χρηστών εντός του συστήματος πέραν των προσπαθειών πρόσβασης σε αυτό, γεγονός που δυσχεραίνει την εκ των υστέρων διερεύνηση του περιστατικού, αφού δεν μπορεί

[7] Συγκεκριμένα, αναφέρεται στην αναφορά αυτή: «This scan does not represent WebHotelier Holdings Ltds overall compliance status with PCI DSS or provide any indication of compliance with other PCI DSS requirements».

να διαπιστωθεί σε ποιες ακριβώς ενέργειες προέβη ο επιτιθέμενος που πραγματοποίησε παράνομη πρόσβαση στην εν λόγω διαδικτυακή πλατφόρμα.

5. Ο υπεύθυνος επεξεργασίας δεν προέβη σε άμεση ενημέρωση όλων των συμμετεχόντων του συνεδρίου (είκοσι τον αριθμό, όπως δηλώθηκε), παρά μόνο μετά από λίγες μέρες κατά τη φυσική παρουσία αυτών στους χώρους του ξενοδοχείου για το συνέδριο. Επίσης, ο υπεύθυνος επεξεργασίας δεν ανέφερε στην Αρχή με το υπόμνημά του τυχόν διαδικασία ενημέρωσης που ακολούθησε για λοιπούς πελάτες του, πέραν των ως άνω συνέδρων, τα στοιχεία των οποίων ήταν αποθηκευμένα στη διαδικτυακή πλατφόρμα της WebHotelier κατά την επίμαχη χρονική περίοδο. Κατά την ακρόασή του δήλωσε ότι ενημερώθηκαν όλοι –χωρίς να προσδιορίζει λεπτομέρειες επί της ενημέρωσης– καθώς επίσης και ότι δεν αναφέρθηκε ποτέ κανένα άλλο περιστατικό.

Ανεξάρτητα από το ζήτημα της ενημέρωσης των υποκειμένων των δεδομένων, σημειώνεται ότι ο υπεύθυνος επεξεργασίας έθεσε σε εφαρμογή διαδικασίες αντιμετώπισης του περιστατικού, τόσο με τις ενέργειες στις οποίες προέβη για την αποκατάστασή του (βλ. ιστορικό της παρούσας), όσο και με την επικοινωνία που είχε με τον ENISA αλλά και με τα υποκείμενα των δεδομένων που δήλωσαν ότι είχαν διαρρεύσει τα δεδομένα τους.

6. Με βάση τα ανωτέρω –βλ. Σημεία 3-5– προκύπτει ότι ο υπεύθυνος επεξεργασίας δεν υιοθέτησε τα πλέον ενδεδειγμένα μέτρα για την ασφάλεια της επεξεργασίας, κατά παράβαση του άρθρου 10 του ν. 2472/1997.

Σημειώνεται επίσης ότι οι υποχρεώσεις του άρ. 10 για την ασφάλεια της επεξεργασίας βαρύνουν και τον εκτελούντα την επεξεργασία. Το εφαρμοστέο δίκαιο όσον αφορά την ασφάλεια της επεξεργασίας είναι το εθνικό δίκαιο του Κράτους Μέλους στο οποίο είναι εγκαταστημένος ο εκτελών την επεξεργασία – εν προκειμένω, για την εταιρεία WebHotelier Holdings LTD, το κυπριακό δίκαιο.

7. Εν όψει της παράβασης που διαπιστώθηκε και του γεγονότος ότι δεν υπήρξε αμέσως ενημέρωση όλων όσων τα δεδομένα τέθηκαν σε κίνδυνο, και λαμβάνοντας επίσης υπόψη τόσο το ότι ο υπεύθυνος επεξεργασίας προχώρησε στη λήψη μέτρων ενίσχυσης της ασφάλειας, σε συνδυασμό με το ότι έχει δρομολογηθεί διαδικασία αναβάθμισης του περιβάλλοντος ηλεκτρονικών κρατήσεων σύμφωνη με τα πρότυπα ασφαλείας (απευθείας σύνδεση με ασφαλές περιβάλλον τραπεζικού ιδρύματος), η Αρχή κρίνει ομόφωνα ότι πρέπει να επιβληθεί στον υπεύθυνο επεξεργασίας η προβλεπόμενη στο άρθρο 21 παρ. 1 στοιχ. β΄ του ν. 2472/1997 κύρωση που αναφέρεται στο διατακτικό της παρούσας για μη λήψη κατάλληλων οργανωτικών και τεχνικών μέτρων ασφάλειας, σύμφωνα με τα οριζόμενα στο άρθρο 10 του νόμου 2472/1997, η οποία οδήγησε σε περιστατικό παραβίασης προσωπικών

δεδομένων.

ΓΙΑ ΤΟΥΣ ΛΟΓΟΥΣ ΑΥΤΟΥΣ

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, λαμβάνοντας υπόψη τα παραπάνω,

1. Επιβάλλει, με βάση τα άρθρα 19 παρ. 1 στοιχ. στ΄ και 21 ν. 2472/1997, στην εταιρεία «ΟΛΥΜΠΙΩΝ ΞΕΝΟΔΟΧΕΙΩΝ ΑΕ», με διακριτικό τίτλο Royal Olympic, πρόστιμο πέντε χιλιάδων (5000) ευρώ για την ανωτέρω περιγραφόμενη παράβαση του ν. 2472/1997.
2. Απευθύνει προειδοποίηση στην ως άνω εταιρεία όπως λάβει αμελλητί τα απαραίτητα μέτρα για την ασφάλεια της επεξεργασίας, σύμφωνα με το άρ. 10 του ν. 2472/1997. Στα μέτρα αυτά θα πρέπει να συμπεριλαμβάνεται η αναδιαμόρφωση του συστήματος ηλεκτρονικών κρατήσεων έτσι ώστε να μην τηρούνται, από τον υπεύθυνο επεξεργασίας, οι αριθμοί ασφαλείας (CVC/CVV) των πιστωτικών καρτών των πελατών του, καθώς επίσης και η εκπαίδευση του προσωπικού ως προς την ασφαλή χρήση των υπολογιστών τους και την προστασία των δεδομένων που επεξεργάζονται μέσω αυτών.

Ο Πρόεδρος **Η γραμματέας**

Πέτρος Χριστόφορος **Ειρήνη Παπαγεωργοπούλου**