ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Αθήνα, 15-05-2012
Αριθ. Πρωτ.: Γ/ΕΞ/3499/15-05-2012

Α Π Ο Φ Α Σ Η ΑΡ.59/2012

(Τμήμα)

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα συνεδρίασε εκτάκτως σε σύνθεση Τμήματος στην έδρα της την 05/04/2012 και ώρα 10:00, εξ' αναβολής από 06/03/2012 και 03/04/2012 και σε συνέχεια της από 20/03/2012 συνεδρίασης, μετά από πρόσκληση του Προέδρου της, προκειμένου να εξετάσει την υπόθεση που αναφέρεται στο ιστορικό της παρούσας. Παρέστησαν οι Γεώργιος Μπατζαλέξης, Αναπληρωτής Πρόεδρος, κωλυομένου του Προέδρου της Αρχής Πέτρου Χριστόφορου, και τα αναπληρωματικά μέλη Γρηγόριος Λαζαράκος, ως εισηγητής, και Πέτρος Τσαντίλας, σε αντικατάσταση των τακτικών μελών Αναστασίου-Ιωάννη Μεταξά, και Αναστάσιου Πράσσου, αντίστοιχα, οι οποίοι, αν και εκλήθησαν νομίμως εγγράφως δεν παρέστησαν λόγω κωλύματος. Δεν παρέστησαν αν και εκλήθησαν νομίμως εγγράφως ο Δημήτριος Μπριόλας, τακτικό μέλος και ο Χαράλαμπος Ανθόπουλος, αναπληρωματικό μέλος. Παρόντες χωρίς δικαίωμα ψήφου ήταν ο Γεώργιος Ρουσόπουλος και Ανάργυρος Χρυσάνθου, πληροφορικοί ελεγκτές, ως βοηθοί εισηγητές και η Ειρήνη Παπαγεωργοπούλου, υπάλληλος του τμήματος διοικητικών και οικονομικών υποθέσεων, ως γραμματέας.

Η Αρχή έλαβε υπόψη της τα παρακάτω:

Στις ../5/2011 διαπιστώθηκε, κατόπιν δημοσιευμάτων στον τύπο και σχετικών αναρτήσεων στο διαδίκτυο (διαδικτυακή έκδοση του περιοδικού Pcworld, άρθρο με τίτλο «Θύμα hacking το Ελληνικό site της Sony Music», διαθέσιμο στην ιστοσελίδα (…….), ότι υπήρξε περιστατικό παραβίασης προσωπικών δεδομένων (εφεξής

«περιστατικό») των εγγεγραμμένων χρηστών του διαδικτυακού τόπου της εταιρείας Sony Music Entertainment A.E. (εφεξής «Sony»). Στοιχεία για την παραβίαση είχαν ήδη αναρτηθεί από την προηγούμενη ημέρα σε ιστοσελίδες όπου δραστηριοποιούνται ομάδες "hacker" ή δημοσιεύονται στοιχεία για αυτούς[1]. Τμήμα των δεδομένων που παραβιάστηκαν αναρτήθηκε στην ιστοσελίδα ……., όπου φαίνονται και τα ακριβή πεδία της βάσης δεδομένων που παραβιάστηκαν. Επίσης, σε ανάλογες δημοσιεύσεις[2] αναφέρεται η παραβίαση από hacker ονόματι «…….», ο οποίος παραμόρφωσε μια ιστοσελίδα από το διαδικτυακό τόπο της Sony. Η παραβίαση αυτή έγινε, σύμφωνα με τη δημοσίευση των hacker, στις ../05/2011 σε σελίδα του διαδικτυακού τόπου της Sony που αφορά την καλλιτέχνιδα Α και συγκεκριμένα στη διεύθυνση ιστού …….

Η Αρχή ζήτησε από τη Sony, με το υπ' αριθμ. πρωτ. Γ/ΕΞ/3575/23-05-2011 έγγραφό της, να παράσχει διευκρινίσεις σχετικά με το περιστατικό και τις σχετικές με αυτό ενέργειές της. Ειδικότερα, η εταιρεία κλήθηκε να διευκρινίσει: *«α) την ακριβή χρονική στιγμή που έλαβε χώρα το περιστατικό, β) τον αριθμό των ατόμων των οποίων τα προσωπικά δεδομένα διέρρευσαν (υποκείμενα των δεδομένων), γ) το είδος των προσωπικών δεδομένων που διέρρευσαν, δ) τον τρόπο και τον χρόνο κατά τον οποίο η εταιρεία εντόπισε τη διαρροή, ε) την πολιτική ασφαλείας και τα λοιπά τεχνικά και οργανωτικά μέτρα ασφαλείας που ακολουθεί η εταιρεία για την προστασία των προσωπικών δεδομένων των χρηστών του διαδικτυακού τόπου, στ) τους λόγους που οδήγησαν στην διαρροή (π.χ. συγκεκριμένες τεχνικές ελλείψεις) και την ανάρτηση των προσωπικών δεδομένων στην παραπάνω ιστοσελίδα, ζ) τις ενέργειες της εταιρείας για την αντιμετώπιση του περιστατικού, συμπεριλαμβανομένων των τεχνικών και οργανωτικών μέτρων που έχουν ληφθεί ή πρόκειται να ληφθούν, η) τυχόν ενημέρωση των υποκειμένων των δεδομένων σχετικά με τη διαρροή, στην οποία προέβη η εταιρεία ώστε να μετριασθούν οι κίνδυνοι της διαρροής»*. Η Sony, με την υπ. αρ. πρωτ. Γ/ΕΙΣ/3639/25-05-2011 επιστολή της, παρείχε απαντήσεις στα ερωτήματα της Αρχής, δηλώνοντας ότι:

1. «*Η ακριβής χρονική στιγμή που έλαβε χώρα το περιστατικό διερευνάται από την Sony Music Entertainment A.E., δεδομένου ότι την 22^{α} Μαΐου 2011, ημέρα Κυριακή, ενημερώθηκε η εταιρεία από το γραφείο της στο Τόκυο ότι hackers ανήρτησαν, την ιδία ως άνω ημέρα, ανακοίνωση σε ιστοσελίδα τους για γεγονός παράνομης πρόσβασης που κατά την άνω ανάρτηση έλαβε χώρα την ..Μαΐου 2011*»
2. «*Ο αριθμός των χρηστών, των οποίων τα δεδομένα φέρεται να διέρρευσαν, ανέρχεται σε 8385*».

[1] Βλ. ενδεικτικά …….
[2] Βλ. ……

3. «*Τα δεδομένα που διέρρευσαν αφορούν σε όνομα χρήστη (user name), κωδικούς πρόσβασης (password) για την είσοδο στην συγκεκριμένη ιστοσελίδα, διευθύνσεις email και τηλεφωνικούς αριθμούς. Σημειωτέον ότι τα παραπάνω δεδομένα δεν υπήρχαν νια όλους τους χρήστες αλλά μόνο για όσους είχαν συμπληρώσει, με δική τους ευθύνη, τα σχετικά αυτά πεδία.*»
4. «*Η διαρροή επιβεβαιώθηκε τεχνικά το πρωί της 23ης Μαΐου 2011 από τον τεχνικό ασφαλείας της εταιρείας φιλοξενίας- hosting «Χ» (IPHost)*».
5. «*Την φιλοξενία των ιστοσελίδων που φέρεται ότι επλήγησαν έχει αναλάβει η εταιρεία «Χ» (IPHost), η οποία είναι υπεύθυνη για την αναβάθμιση του φιλαξενητή (server) σύμφωνα με τα εκάστοτε μέτρα ασφαλείας και την τεχνική υποστήριξη του λειτουργικού συστήματος (operating system) και του υλισμικού (hardware). Ο φιλοξενητής βρίσκεται στο DC* LAMDA Hellix *στο Κορωπί κάτω από δίκτυο της εταιρείας IPHost, προστατεύεται δε με τείχος προστασίας, το οποίο επιτρέπει συγκεκριμένες και μόνο συνδέσεις. Η πρόσβαση στη βάση δεδομένων επιτρέπεται μόνο εσωτερικά του δικτύου. Την υλοποίηση των ιστοσελίδων που φιλοξενούνται στον ανωτέρω φιλοξενητή (server) και την ανανέωση και συντήρηση αυτών έχει αναλάβει η εταιρεία «Ψ».*
6. «*Η Sony Music Entertainment A.E. βρίσκεται στο στάδιο διερεύνησης της παράνομης πρόσβασης και θα ενημερώσει την Αρχή για τα αποτελέσματα της.*»
7. «*Η Sony Music Entertainment A.E αμέσως μόλις πληροφορήθηκε το παράνομο γεγονός, και συγκεκριμένα την 22^{α} Μαΐου 2011, έδωσε εντολή σε όλους τους αρμοδίους (εταιρεία κατασκευής ιστοσελίδων και εταιρεία φιλοξενίας-hosting) για άμεση απενεργοποίηση όλων των ιστοσελίδων που ήταν στην επίμαχη πλατφόρμα. Συγχρόνως, η Sony Music Entertainment A.E επέτυχε το πρωί της 24ης Μαΐου 2011 την απενεργοποίηση της ιστοσελίδας των hackers που είχε παράνομα αναρτήσει τα δεδομένα. Η Sony Music Entertainment A.E παρακολουθεί συνεχώς τυχόν νέα ανάρτηση ώστε να λάβει τα αναγκαία μέτρα.*»
8. «*Η Sony Music Entertainment A.E εξέδωσε σχετική ανακοίνωση μέσω του Τύπου αλλά και σε άνω από 15.000 ιστοσελίδες παγκοσμίως. Ως εκ τούτου οι χρήστες έχουν ήδη και επαρκώς ενημερωθεί.*»

Με την υπ' αριθμ. πρωτ. Γ/ΕΞ/3785/31-05-2011 εντολή του Αναπληρωτή Προέδρου της Αρχής, διατάχθηκε η διενέργεια ελέγχου στην Sony. Ο έλεγχος πραγματοποιήθηκε την 1/6/2011 στις εγκαταστάσεις της εταιρείας LAMDA Hellix A.E., …….. όπου φιλοξενούνται τα ηλεκτρονικά αρχεία των εξυπηρετητών διαδικτύου της Sony, από τους

υπαλλήλους του Τμήματος Ελεγκτών της Γραμματείας της Αρχής, Αθηνά Μπούρκα, Γεώργιο Ρουσόπουλο και Ανάργυρο Χρυσάνθου (εφεξής «ομάδα ελέγχου»).

Κατά τον επιτόπιο έλεγχο, η ομάδα ελέγχου πραγματοποίησε αρχικά συνέντευξη με τους αρμόδιους υπαλλήλους που είχε ορίσει ο υπεύθυνος επεξεργασίας και στη συνέχεια διενήργησε επιτόπιο τεχνικό έλεγχο. Ο έλεγχος εστιάστηκε στα παρακάτω βασικά σημεία: α) την τεχνική περιγραφή του συστήματος το οποίο υποστηρίζει τον διαδικτυακό τόπο του υπεύθυνου επεξεργασίας, στη διεύθυνση http://www.sonymusic.gr/, β) τις κατηγορίες των δεδομένων προσωπικού χαρακτήρα που υφίστανται επεξεργασία μέσω του παραπάνω διαδικτυακού τόπου, γ) την περιγραφή του συγκεκριμένου περιστατικού παραβίασης προσωπικών δεδομένων και των πιθανών επιπτώσεών του στα υποκείμενα των δεδομένων, δ) τα μέτρα ασφάλειας που είχε λάβει ο υπεύθυνος επεξεργασίας πριν από το περιστατικό, ε) τον τρόπο με τον οποίο ο υπεύθυνος επεξεργασίας αντιμετώπισε το περιστατικό. Στο πλαίσιο του ελέγχου ζητήθηκε από τον υπεύθυνο επεξεργασίας να παραδώσει στην ομάδα ελέγχου μια σειρά πειστηρίων (εντύπων και ηλεκτρονικών – εφεξής «Πειστήρια»).

Μετά από την ολοκλήρωση του επιτόπιου ελέγχου, η ομάδα ελέγχου συνέταξε τα Πρακτικά του ελέγχου (εφεξής «Πρακτικά»), στα οποία καταγράφονται οι απαντήσεις/διευκρινήσεις του υπεύθυνου επεξεργασίας, οι επιτόπιες παρατηρήσεις της ομάδας ελέγχου και η λίστα με τα Πειστήρια. Τα Πρακτικά απεστάλησαν στις 6/6/2011 με μήνυμα ηλεκτρονικού ταχυδρομείου στον υπεύθυνο επεξεργασίας για υποβολή σχολίων ή/και παρατηρήσεων. Στις 10/06/2011 τα Πρακτικά οριστικοποιήθηκαν με το υπ. αρ. πρωτ. Γ/ΕΞ/4123/10-06-2011 έγγραφο της Αρχής. Για την ολοκλήρωση του ελέγχου ο υπεύθυνος επεξεργασίας απέστειλε τα υπ. αρ. πρωτ. Γ/ΕΙΣ/4544/30-06-2011, Γ/ΕΙΣ/5528/10-08-2011 και Α/ΕΙΣ/324/11-10-2011 συμπληρωματικά έγγραφα αναφορικά με την υπόθεση.

Στη συνέχεια, η ομάδα ελέγχου μελέτησε τα Πρακτικά σε συνδυασμό με τα Πειστήρια και συνέταξε Πόρισμα, το οποίο υπέβαλε στην Αρχή με το υπ. αρ. πρωτ. Γ/ΕΙΣ/8485/16-12-2011 έγγραφο. Στο Πόρισμα της ομάδας ελέγχου καταγράφονται μεταξύ άλλων τα ευρήματα αναφορικά με μέτρα ασφάλειας ή/και διαδικασίες προστασίας προσωπικών δεδομένων του υπεύθυνου επεξεργασίας που συντέλεσαν στο να συμβεί το συγκεκριμένο περιστατικό, καθώς και με τις διαδικασίες αντιμετώπισης του περιστατικού από τον υπεύθυνο επεξεργασίας, καθώς και οι προτεινόμενες από την ομάδα ελέγχου συστάσεις για την αντιμετώπιση των κινδύνων που δημιουργούνται.

Όπως διαπιστώνεται από το Πόρισμα και καταγράφεται στα ευρήματα:

- Το περιστατικό παραβίασης προσωπικών δεδομένων συνέβη στις 7 και 8/5/2011 με αρχική παραβίαση της ιστοσελίδας …….. Κατά την επίθεση χρησιμοποιήθηκε το λογισμικό Havij[3], το οποίο εκμεταλλεύεται αδυναμίες του λογισμικού που εκτελείται στην πλευρά του εξυπηρετητή ιστοσελίδων για να αποκτήσει τη δυνατότητα εκτέλεσης ερωτημάτων και εντολών στη βάση δεδομένων (τεχνική γνωστή ως «SQL Injection»). Η παραβίαση αφορά προσωπικά δεδομένα 8385 εγγραμμένων χρηστών του διαδικτυακού τόπο της Sony. Τα δεδομένα αυτά περιλαμβάνουν: όνομα χρήστη, ονοματεπώνυμο, εταιρεία, διεύθυνση ηλεκτρονικού ταχυδρομείου, αριθμό τηλεφώνου, κωδικό πρόσβασης και ημερομηνία εγγραφής.
- Από την στιγμή που έγινε αντιληπτό το περιστατικό, ο διαδικτυακός τόπος κατέστη άμεσα ανενεργός από τη Sony, ενώ δόθηκε πλήρης πρόσβαση σε όλα τα αρχεία του διαδικτυακού τόπου σε εξειδικευμένο συνεργάτη (Guidance Software Inc) της μητρικής εταιρείας (Sony Music), ως πραγματογνώμονα, ο οποίος ανέλαβε να αναλύσει και να αξιολογήσει το περιστατικό. Κατά τη χρονική στιγμή του ελέγχου, η Sony δεν είχε προβεί σε άλλα τεχνικά ή οργανωτικά μέτρα για την αντιμετώπιση του συγκεκριμένου περιστατικού ή άλλων ανάλογων περιστατικών στο μέλλον. Τα συμπεράσματα της ανάλυσης της Guidance Software Inc υποβλήθηκαν στην Αρχή, και επιβεβαίωσαν τα ευρήματα του Πορίσματος, ως προς το εξεταζόμενο περιστατικό παραβίασης προσωπικών δεδομένων.
- Πριν την απενεργοποίηση του διαδικτυακού τόπου της Sony διαπιστώθηκαν επιτυχείς προσπάθειες πρόσβασης στον διαδικτυακό τόπο της Sony με χρήση των αναρτηθέντων στο διαδίκτυο στοιχείων των χρηστών (υποκλοπή ταυτότητας).
- Ο διαδικτυακός τόπος της Sony υπέστη 2 αλλοιώσεις. Η πρώτη από αυτές τις αλλοιώσεις δεν σχετιζόταν με το περιστατικό αλλά με εγγραφές που παρέπεμπαν σε φαρμακευτικά προϊόντα και περιείχαν κεκαλυμμένο κώδικα, ο οποίος μεταφόρτωνε άλλο κώδικα λογισμικού από απομακρυσμένο ιστότοπο με σκοπό να εγκαταστήσει στους υπολογιστές των επισκεπτών κακόβουλο λογισμικό. Η δεύτερη και πιο πρόσφατη αλλοίωση δημοσιεύτηκε σε ιστοσελίδα ……. και έγινε αντιληπτή από τους υπεύθυνους της εταιρείας, αποκαλύπτοντας κατά τον τρόπο αυτό το περιστατικό παραβίασης προσωπικών δεδομένων.

[3] Βλ. ……..

- Ο διαδικτυακός τόπος της Sony είχε κενά ασφάλειας, τα οποία, μεταξύ άλλων, επιτρέπουν:
  1. επιθέσεις τύπου SQL Injection και Cross-site Scripting (XSS).
  2. μεταφόρτωση κώδικα λογισμικού από απομακρυσμένο ιστότοπο
  3. υποκλοπή ονομάτων χρήστη και κωδικών πρόσβασης, καθώς και περιεχομένου (πχ. στοιχεία χρηστών) της βάσης δεδομένων
  4. ενδεχόμενη πρόσβαση σε φαινομενικά προστατευμένους καταλόγους του διακομιστή
  5. ενδεχόμενη πρόσβαση στον διακομιστή από μη εγκεκριμένες IP διευθύνσεις, ακόμα και μέσω μη ασφαλών πρωτοκόλλων.

Η Sony κλήθηκε, με το υπ' αριθμ. Γ/ΕΞ/1232/20-02-2012 έγγραφο της Αρχής, νομίμως σε ακρόαση ενώπιον της Αρχής στη συνεδρίαση της 06/03/2012 για να δώσει περαιτέρω διευκρινίσεις και να εκθέσει τις απόψεις της επί του Πορίσματος της Αρχής, το οποίο της επιδόθηκε μαζί με την κλήση της από την Αρχή για ακρόαση. Η Sony ζήτησε λόγω αποχής των δικηγόρων της Ελλάδας από τα καθήκοντα τους την Τρίτη 6/03/2012 και έλαβε από την Αρχή αναβολή για τη συζήτηση της υπόθεσης την Τρίτη 20/03/2012, προκειμένου να μπορεί να παραστεί δια των νομίμων αντιπροσώπων της στη συζήτηση της υπόθεσης. Στη συνεδρίαση της Αρχής, την 20/03/2012, παρέστησαν νομίμως η Β, νόμιμη εκπρόσωπος της Sony, Σ. Πηλαδάκης και Κ. Γαβρίλογλου, δικηγόροι της Sony, καθώς επίσης και ο Γ, υπάλληλος της Sony αρμόδιος για ζητήματα πληροφορικής. Η Sony υπέβαλε και σχετικό υπόμνημα εκθέτοντας και εγγράφως τις θέσεις της με το υπ' αριθμ. πρωτ. Γ/ΕΙΣ/2210/23-03-2011 έγγραφό της, το οποίο εξετάστηκε από την Αρχή, κατά την συνεδρίαση του Τμήματος, την 05/04/2012.

Η Αρχή, αφού άκουσε τον εισηγητή της υπόθεσης και έλαβε υπόψη όλα τα στοιχεία του φακέλου, μετά και από διεξοδική συζήτηση,

ΣΚΕΦΘΗΚΕ ΣΥΜΦΩΝΑ ΜΕ ΤΟ ΝΟΜΟ

1. 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.

2. Ως περιστατικό παραβίασης προσωπικών δεδομένων θεωρείται κάθε περίπτωση παραβίασης της ασφάλειας των δεδομένων στο πλαίσιο του χρησιμοποιούμενου συστήματος επεξεργασίας, όπως τυχαία ή αθέμιτη καταστροφή, τυχαία απώλεια, αλλοίωση, απαγορευμένη διάδοση ή πρόσβαση και κάθε άλλη μορφή αθέμιτης επεξεργασίας.

3. Η Αρχή κρίνει ότι για να πληρούνται σε διαδικτυακούς τόπους, οι οποίοι τηρούν προσωπικά δεδομένα, οι προϋποθέσεις που θέτει το άρθρο 10 παρ. 3 του νόμου 2472/1997 αναφορικά με τη λήψη κατάλληλων οργανωτικών και τεχνικών μέτρων ασφάλειας θα πρέπει να ισχύουν τουλάχιστον τα ακόλουθα:

- Ο υπεύθυνος επεξεργασίας οφείλει να χρησιμοποιεί τεχνικές ασφαλούς συγγραφής κώδικα, ειδικά για το λογισμικό εφαρμογών που χρησιμοποιείται για την επεξεργασία προσωπικών δεδομένων, όπως για παράδειγμα η μη επιστροφή μηνυμάτων λάθους με χρήσιμες πληροφορίες από τον διακομιστή της βάσης δεδομένων, το φιλτράρισμα της εισαγωγής του χρήστη με την «απόρριψη» ειδικών χαρακτήρων, κα[4]. Επίσης, οφείλει να φροντίζει για τη συντήρηση των εφαρμογών του και την άμεση διόρθωση κάθε κενού ασφαλείας που εντοπίζεται, είτε από τους δικούς του προληπτικούς ελέγχους, είτε από τρίτους. Σε περίπτωση που χρησιμοποιεί εκτελούντες την επεξεργασία, οφείλει να περιλαμβάνει σχετικές προβλέψεις στις μεταξύ τους συμβάσεις, τόσο στα στάδια σχεδιασμού, υλοποίησης και παράδοσης των εφαρμογών που χρησιμοποιεί, όσο και στο στάδιο παραγωγικής λειτουργίας τους.
- Ο υπεύθυνος επεξεργασίας οφείλει να ελέγχει περιοδικά την ορθότητα του περιεχομένου των ιστοσελίδων, οι οποίες φιλοξενούνται στον διαδικτυακό του τόπο, και να εξασφαλίζει ότι δεν φιλοξενείται στη σελίδα του κώδικας τρίτων χωρίς την έγκρισή του, ώστε να αποφεύγεται οποιαδήποτε πιθανότητα παραβίασης προσωπικών δεδομένων των επισκεπτών ή χρηστών της ιστοσελίδας.
- Ο υπεύθυνος επεξεργασίας οφείλει να φροντίζει ώστε οι κωδικοί πρόσβασης που χρησιμοποιούνται σε εφαρμογές διαθέσιμες στο κοινό να αποθηκεύονται με κατάλληλη κρυπτογράφηση. Το επίπεδο της κρυπτογράφησης πρέπει να είναι τέτοιο που να εξασφαλίζει ότι σε περίπτωση διαρροής δεδομένων κανείς τρίτος

[4] Βλ. ενδεικτικά ……..

δεν θα μπορέσει να βρει τους κωδικούς πρόσβασης με γνωστές μεθόδους (π.χ. αποθήκευση hash με ασφαλή αλγόριθμο, ανθεκτικότητα σε επιθέσεις τύπου λεξικού).

- Ο υπεύθυνος επεξεργασίας θα πρέπει να εφαρμόζει κατάλληλα μέτρα ασφάλειας, όπως η μη επιστροφή μηνυμάτων λάθους με χρήσιμες πληροφορίες, η χρήση λογαριασμού χρήστη με περιορισμένα δικαιώματα σε επίπεδο διαδικτυακής εφαρμογής, κ.α.[5]
- Ο υπεύθυνος επεξεργασίας οφείλει να τηρεί και να εφαρμόζει απαρεγκλίτως τα μέτρα της πολιτικής ασφάλειάς του και να βεβαιώνεται για την εφαρμογή αυτών στις διαδικτυακές του εφαρμογές.
- Ο υπεύθυνος επεξεργασίας οφείλει να διασφαλίζει ότι ο εκτελών την επεξεργασία τηρεί τους όρους της πολιτικής ασφάλειας στο μέτρο που αυτή τον αφορά (τον εκτελούντα), όπως π.χ. αναφορικά με την ασφαλή συγγραφή κώδικα, κανόνες πρόσβασης στα συστήματα, διαχείριση περιστατικών ασφαλείας, μέτρα φυσικής ασφάλειας, κλπ. Όταν η επεξεργασία γίνεται εκτός των εγκαταστάσεων του υπεύθυνου επεξεργασίας, ο υπεύθυνος θα πρέπει να εξασφαλίζει ότι ο εκτελών παρέχει επίπεδο ασφαλείας τουλάχιστον ανάλογο με αυτό που ορίζεται στην πολιτική ασφάλειας του υπευθύνου.
- Ο υπεύθυνος επεξεργασίας οφείλει να φροντίζει ώστε τα αρχεία καταγραφής να επιβλέπονται ανά τακτά διαστήματα από αρμόδιο πρόσωπο (π.χ. διαχειριστή ή/και υπεύθυνο ασφαλείας) για τυχόν ανίχνευση και αναγνώριση αθέμιτων ενεργειών, ενώ επίσης πρέπει να διασφαλίζεται η ακεραιότητά τους. Τα μηνύματα σφάλματος που καταγράφονται πρέπει να εκτιμούνται καταλλήλως. Η συχνότητα του ελέγχου πρέπει να είναι ανάλογη με τις υφιστάμενες απειλές.
- Ο υπεύθυνος επεξεργασίας οφείλει να φροντίζει ώστε η πληροφορία που τηρείται στα αρχεία καταγραφής προστατεύεται κατάλληλα και δεν περιλαμβάνει συνθηματικά χρηστών σε αναγνώσιμη μορφή. Αυτό μπορεί να επιτευχθεί είτε με διαφορετική συγγραφή του κώδικα της ιστοσελίδας, είτε με διαφορετική ρύθμιση της εφαρμογής του εξυπηρετητή IIS, είτε με εφαρμογή κατάλληλης κρυπτογράφησης. Το επίπεδο της κρυπτογράφησης πρέπει να είναι τέτοιο που να εξασφαλίζει ότι σε περίπτωση διαρροής δεδομένων κανείς τρίτος δεν θα μπορέσει

[5] Βλ. …….

να βρει τους κωδικούς πρόσβασης με γνωστές μεθόδους (π.χ. αποθήκευση hash με ασφαλή αλγόριθμο, ανθεκτικότητα σε επιθέσεις τύπου λεξικού).

- Ο υπεύθυνος επεξεργασίας οφείλει να εξασφαλίζει ότι δεν επιτρέπεται, μέσω εξυπηρετητών FTP, η δημιουργία αρχείων ή καταλόγων από μη αυθεντικοποιημένους χρήστες. Επιπλέον, η πρόσβαση στους καταλόγους του εξυπηρετητή διαδικτύου πρέπει να περιορίζεται στους αρμόδιους χρήστες.
- Ο υπεύθυνος επεξεργασίας πρέπει να επιτρέπει την απομακρυσμένη πρόσβαση εξουσιοδοτημένων στελεχών δικών του ή των εκτελούντων την επεξεργασία σε πόρους του συστήματος που περιέχουν προσωπικά δεδομένα, μόνο όταν αυτό είναι απολύτως απαραίτητο. Ο υπεύθυνος επεξεργασίας πρέπει να διαθέτει συγκεκριμένη διαδικασία διαχείρισης των απομακρυσμένων προσβάσεων που να εξασφαλίζει ότι ουδείς τρίτος έχει τη δυνατότητα απομακρυσμένης πρόσβασης.

4. Το συγκεκριμένο περιστατικό αποτελεί περιστατικό παραβίασης προσωπικών δεδομένων των εγγεγραμμένων χρηστών του διαδικτυακού τόπου της Sony. Τα δεδομένα αυτά αποτελούν απλά προσωπικά δεδομένα, κατά την έννοια του αρ. 2 στοιχ. α ν. 2472/1997. Η βαρύτητα του περιστατικού αυξάνεται από το γεγονός ότι α) το περιστατικό αφορά μεγάλο αριθμό ατόμων (8385 εγγεγραμμένοι χρήστες), β) τα δεδομένα που διέρρευσαν γνωστοποιήθηκαν σε μεγάλο αριθμό ατόμων (μέσω διαδικτύου) και αποτέλεσαν αντικείμενο επιτυχών προσπαθειών υποκλοπής ταυτότητας, γ) υπήρχαν πρότερα περιστατικά ασφάλειας, τα οποία δεν έγιναν ποτέ αντιληπτά, δ) η επίθεση στη Sony ήταν η 8^{η} παγκοσμίως κατά του ομίλου Sony, με την 1^{η} να έχει γίνει στις 4/4/2011 και την 7^{η} στις 21/5/2011[6], άρα η εταιρεία ήταν εν γνώσει της ότι υφίσταται διαδικτυακές επιθέσεις διεθνώς και ε) στα δεδομένα που διέρρευσαν περιλαμβάνονται και κωδικοί πρόσβασης χρηστών, συνοδευόμενοι τόσο από όνομα χρήστη όσο και από διεύθυνση ηλεκτρονικού ταχυδρομείου, καθιστώντας κατ' αυτόν τον τρόπο εφικτή τη μη εξουσιοδοτημένη πρόσβαση στους συγκεκριμένους αλλά και σε άλλους λογαριασμούς των χρηστών σε διάφορες ηλεκτρονικές υπηρεσίες του διαδικτύου, καθώς πολλοί χρήστες συνηθίζουν να χρησιμοποιούν κοινούς κωδικούς πρόσβασης και κοινά ονόματα χρηστών για διαφορετικές ηλεκτρονικές υπηρεσίες, στις οποίες διατηρούν λογαριασμό.

5. Από το Πόρισμα προκύπτει ότι το περιστατικό διευκολύνθηκε από ανεπάρκεια των μέτρων ασφάλειας της Sony. Πιο συγκεκριμένα η εταιρεία είχε μεν λάβει μέτρα ασφάλειας

[6] Βλ. ……..

καθώς α) τηρούσε αρχεία καταγραφής για τον διαδικτυακό της τόπο και την υπάρχουσα υποδομή, β) είχε μια γενική πολιτική ασφάλειας, γ) λάμβανε σχεδόν καθημερινά αντίγραφα ασφαλείας, δ) εφάρμοζε έλεγχο πρόσβασης αναφορικά με τους εγγεγραμμένους χρήστες του διαδικτυακού της τόπου αλλά και με τους χρήστες, οι οποίοι υποστήριζαν το σύστημα, ε) είχε διαρκή υποστήριξη τόσο σε επίπεδο υποδομής όσο και σε επίπεδο εφαρμογών και περιεχομένου και στ) είχε την υποδομή για να χρησιμοποιήσει τεχνικές VPN για απομακρυσμένη πρόσβαση στον εξυπηρετητή του διαδικτυακού τόπου για λόγους υποστήριξης Παρόλα αυτά, από τα στοιχεία που γνωστοποιήθηκαν στην Αρχή, και όπως προκύπτει από το Πόρισμα: α) τα αρχεία καταγραφής δεν παρακολουθούνταν από την Sony με αποτέλεσμα να μη γίνουν αντιληπτές επιθέσεις και παραβιάσεις ασφάλειας σε διάστημα 3 ετών, β) η πολιτική ασφαλείας δεν εφαρμόστηκε στον διαδικτυακό τόπο της Sony, γ) οι κωδικοί πρόσβασης των εγγεγραμμένων χρηστών του διαδικτυακού τόπου της Sony δεν ήταν κρυπτογραφημένοι, δ) παρά την ύπαρξη διαρκούς υποστήριξης σε επίπεδο εφαρμογών η Sony δεν είχε διασφαλίσει το απαιτούμενο επίπεδο ασφάλειας των δεδομένων κατά την επεξεργασία τους από τον εκτελούντα την επεξεργασία και ειδικά κατά την ανάπτυξη του κώδικα λογισμικού του διαδικτυακού τόπου της, με αποτέλεσμα ο τελευταίος να είναι ευάλωτος σε επιθέσεις τύπου SQL Injection και Cross-site Scripting (XSS) και ε) η δυνατότητα πρόσβασης μέσω VPN δεν έχει χρησιμοποιηθεί ποτέ. Τα ανωτέρω διευκολύνουν τη μη εξουσιοδοτημένη πρόσβαση στα παραπάνω δεδομένα.

6. Παρά τις ανωτέρω ελλείψεις, η Αρχή συνεκτιμά ότι η Sony έλαβε αμέσως μέτρα για την αντιμετώπιση του περιστατικού. Ειδικότερα, μετά τη διαπίστωση του περιστατικού ο διαδικτυακός τόπος κατέστη άμεσα ανενεργός, ενώ δόθηκε πλήρης πρόσβαση σε όλα τα αρχεία του διαδικτυακού τόπου σε εξειδικευμένο συνεργάτη (Guidance Software Inc) της μητρικής εταιρείας (Sony Music), ως πραγματογνώμονα, ο οποίος ανέλαβε να αναλύσει και να αξιολογήσει το περιστατικό. Ο διαδικτυακός τόπος της παραμένει μέχρι τη στιγμή της παρούσης ανενεργός σε αναμονή της απόφασης της Αρχής και της εκ νέου υλοποίησης του σε άλλη, πιο ασφαλή πλατφόρμα με βάση τις οδηγίες της μητρικής εταιρείας του ομίλου Sony. Η Sony ενημέρωσε για το συμβάν μέσω ανακοίνωσης στον τύπο, ενημέρωση η οποία θα ήταν πληρέστερη αν συνοδευόταν από μήνυμα ηλεκτρονικού ταχυδρομείου προς τους εγγεγραμμένους χρήστες. Η Sony πέτυχε, εντός δύο ημερών από την ίδια διαπίστωση του περιστατικού και εντός τριών ημερών από την ανάρτηση των διαρρευσάντων δεδομένων από τους hackers την απενεργοποίηση της ιστοσελίδας των hackers που είχε παράνομα αναρτήσει τα δεδομένα Στο δελτίο τύπου περιέγραψε το είδος των προσωπικών δεδομένων που διέρρευσαν και ανέφερε ότι σε αυτά δεν περιλαμβάνονταν δεδομένα πιστωτικών καρτών.

7. Η Sony, καθ' όλη τη διάρκεια διερεύνησης του περιστατικού από την Αρχή ήταν απόλυτα συνεργάσιμη με την Αρχή παρέχοντας διευκρινίσεις σε ότι της ζητήθηκε από την ομάδα ελέγχου.

8. Λαμβάνοντας υπόψη όλα τα παραπάνω, προκύπτει ότι η Sony, παρότι περιόρισε κατά το δυνατόν την έκταση της διαρροής των δεδομένων και έλαβε μέτρα για την αντιμετώπιση παρόμοιων προβλημάτων στο μέλλον, παραβίασε το άρθρο 10 παρ. 3 ν. 2472/1997.

ΓΙΑ ΤΟΥΣ ΛΟΓΟΥΣ ΑΥΤΟΥΣ

Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, συνεκτιμώντας και τα οικονομικά στοιχεία της εταιρείας, όπως εκτίθενται στο σχετικό υπόμνημα επιβάλλει στη Sony με βάση το άρθρο 21 παρ. 1 στοιχ. β' του Ν. 2472/1997 πρόστιμο δέκα χιλιάδων Ευρώ (10.000€) για μη λήψη κατάλληλων οργανωτικών και τεχνικών μέτρων ασφάλειας, σύμφωνα με τα οριζόμενα στο άρθρο 10 παρ. 3 του νόμου 2472/1997, η οποία οδήγησε σε περιστατικό παραβίασης προσωπικών δεδομένων των εγγεγραμμένων χρηστών του διαδικτυακού τόπου της.

Ο Αναπληρωτής Πρόεδρος **Η γραμματέας**

Γεώργιος Μπατζαλέξης **Ειρήνη Παπαγεωργοπούλου**