**Ένωση Πληροφορικών Ελλάδας**
Τ.Θ. 13801
ΤΚ 10310, Αθήνα
http://www.epe.org.gr
e-mail: info@epe.org.gr
Τηλέφωνο/Fax: 211 7907675



# ΔΕΛΤΙΟ ΤΥΠΟΥ

## 28η Ιανουαρίου – Παγκόσμια Ημέρα Προστασίας Προσωπικών Δεδομένων

Αθήνα, 27-1-2017

Η 28η Ιανουαρίου έχει οριστεί ως η Παγκόσμια Ημέρα Προστασίας των Προσωπικών Δεδομένων[1] (Data Protection / Data Privacy Day). Στην Ευρώπη γιορτάζεται ως Πανευρωπαϊκή Ημέρα Προστασίας Δεδομένων (European Data Protection Day – EDPD)[2,3] και σηματοδοτεί συμβολικά την υπογραφή της Σύμβασης 108 του Συμβουλίου της Ευρώπης[4,5] το 2006 για την προστασία των προσωπικών δεδομένων στην Ε.Ε.

Στη σημερινή ψηφιακή εποχή η καθημερινότητα των πολιτών, των επιχειρήσεων και ολόκληρων των κοινωνιών ρυθμίζεται καθοριστικά από τον τρόπο παραγωγής, αποθήκευσης, επεξεργασίας και μετάδοσης δεδομένων κάθε μορφής, από απλές ενέργειες όπως η επικύρωση εισιτηρίου στο μετρό μέχρι τα βιομετρικά στοιχεία στα σύγχρονα διαβατήρια. Κάθε πακέτο πληροφορίας αποτελεί από μόνο του αγαθό (commodity) και ταυτόχρονα μέσο συναλλαγής με φορείς και υπηρεσίες. Επιπλέον, χαρακτηρίζει με τρόπο συστηματικό, λεπτομερή και σε βάθος χρόνου, κάθε εταιρική

1 https://en.wikipedia.org/wiki/Data_Privacy_Day
2 http://www.coe.int/en/web/portal/28-january-data-protection-day
3 https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/Events
4 http://www.coe.int/en/web/portal/28-january-data-protection-day-factsheet
5 https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680078b37

οντότητα και κάθε άτομο ξεχωριστά. Επομένως η διασφάλιση της προστασίας και της σωστής χρήσης των δεδομένων αυτών είναι ζήτημα ζωτικής σημασίας σε κάθε επίπεδο.

Δυστυχώς η εκπαίδευση των πολιτών και η εγρήγορση των θεσμών σε νομοθετικό και εκτελεστικό επίπεδο βρίσκονται ακόμα σε πολύ πρώιμο στάδιο. Μαζικές διαρροές δεδομένων από δημόσιους και ιδιωτικούς φορείς γίνονται δημόσια γνωστές μόνο σε πολύ μικρό ποσοστό[6,7,8] και μόνο εφόσον συνοδεύονται από επίσημες καταγγελίες σχετικής οικονομικής απάτης (π.χ. χρήση πλαστών πιστωτικών καρτών). Σύμφωνα με πρόσφατη μελέτη[9], το 54% των εταιριών εξακολουθούν να είναι ανέτοιμες και να λειτουργούν εκτός του Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR) της Ευρωπαϊκής Ένωσης. Ταυτόχρονα, οι πολίτες εξακολουθούν να αγνοούν σε μεγάλο βαθμό ακόμα και τις βασικές οδηγίες προστασίας των δικών τους προσωπικών δεδομένων. Το γεγονός αυτό, σε συνδυασμό με τη ραγδαία αύξηση των ηλεκτρονικών συναλλαγών[10], υποχρεωτικά πλέον βάσει του πρόσφατου Νόμου[11], δημιουργούν συνθήκες εξαιρετικά αυξημένου ρίσκου, όχι μόνο για την κλοπή προσωπικών δεδομένων αλλά και για ηλεκτρονική απάτη.

Δεν είναι ασυνήθιστο ένας χρήστης υπηρεσιών ηλεκτρονικής τραπεζικής (e-banking) να χρησιμοποιεί τη φορητή του συσκευή ως μέσο αποθήκευσης αυτόματων κωδικών πρόσβασης και πρόσθετης πιστοποίησης πρόσβασης για τις συναλλαγές (Transaction Authentication Number – TAN) και ταυτόχρονα να έχει ρυθμίσει τη συσκευή αυτή έτσι ώστε να συνδέεται αυτόματα σε οποιοδήποτε ασύρματο δίκτυο (WiFi) εντοπίσει, ακόμα και χωρίς να υπάρχει πρωτόκολλο ασφάλειας/κρυπτογράφησης (WPAx ή έστω WEP). Το αποτέλεσμα είναι οποιασδήποτε να μπορεί όχι μόνο να υποκλέψει τα στοιχεία πρόσβασης κατά τη διάρκεια ηλεκτρονικών συναλλαγών, αλλά να υλοποιήσει πολύ εύκολα, σε οποιοδήποτε σημείο εν κινήσει, επιθέσεις διαμεσολάβησης, παρεμβολής ψευδούς ταυτότητας ή διαμεσολάβησης (man-in-the-

6 http://www.reuters.com/article/us-britain-banks-cyber-idUSKBN12E0NQ
7 https://eandt.theiet.org/content/articles/2016/10/uk-banks-under-constant-cyber-attack-but-dont-report-incidents/
8 https://www.ecb.europa.eu/pub/pdf/other/4th_card_fraud_report.en.pdf
9 http://www.sepe.gr/gr/research-studies/article/8290518/oi-mises-etaireies-anetoimes-gia-to-neo-geniko-kanonismo-prostasias-dedomenon/
10 http://www.bankofgreece.gr/Pages/el/Statistics/paymentsystems/cards.aspx
11 Ν.4446/2016, ΦΕΚ 240 Α'/22.12.2016 - https://is.gd/sLHl6O

middle[12] & eavesdropping attacks[13]) προσποιούμενος το server της τράπεζας. Αντίστοιχα, οι νέες χρεωστικές και πιστωτικές κάρτες ασύρματων συναλλαγών που εκδίδουν οι τράπεζες μπορεί να έχουν κατά κανόνα πολύ χαμηλό όριο συναλλαγών (τυπικά όχι πάνω από 150 ευρώ), όμως τα πρωτόκολλα αυτόματης ανταλλαγής δεδομένων στις συναλλαγές αποτελούν αποδεδειγμένα σημαντικό ρίσκο για τη διαρροή προσωπικών δεδομένων του κατόχου, σε οποιοδήποτε σημείο βρίσκεται, ακόμα και όταν μετακινείται έχοντας απλά την κάρτα στην τσέπη του[14].

Στην Ελλάδα η πρόσφατη τροποποίηση του Ποινικού Κώδικα περιλαμβάνει αρκετές βελτιώσεις σε σχέση με το ηλεκτρονικό έγκλημα και την προστασία των προσωπικών δεδομένων στο Διαδίκτυο[15]. Παρόλα αυτά, όπως έχει επισημανθεί εδώ και πολλούς μήνες από την ΕΠΕ[16], τα νομοθετήματα των τελευταίων λίγων ετών έχουν γίνει με ελάχιστη ή καθόλου μελέτη ως προς την προστασία έναντι διαρροών δεδομένων και ηλεκτρονικής απάτης. Ως παράδειγμα, επισημαίνεται η μεγαλύτερη μαζική διαρροή δεδομένων από το TAXIS[17] το 2013, για την οποία η ΓΓΠΣ καταδικάστηκε τελεσίδικα από την ΑΠΔΠΧ για βαρύτατη αμέλεια με το μέγιστο προβλεπόμενο πρόστιμο[18]. Επιπροσθέτως, με την πρόσφατη αναβάθμιση της ΓΓΔΕ σε ανεξάρτητη Αρχή, η ΑΑΔΕ απέκτησε πλήρη και αποκλειστική χρήση των δεδομένων και του λογισμικού του TAXIS (μεταξύ άλλων)[19]. Αυτό δημιουργεί εν δυνάμει σημαντικό πρόβλημα θεσμικού ελέγχου ως προς πιθανές αντίστοιχες περιπτώσεις διαρροών και παραβιάσεων ασφαλείας, καθώς το υπουργείο Οικονομικών είναι μεν ο εποπτεύον φορέας σε αυτά τα ζητήματα, όμως η ΑΑΔΕ ως ανεξάρτητη Αρχή έχει βάσει Νόμου και κατά προτεραιότητα αυτόνομες εσωτερικές διαδικασίες ελέγχων αντί από εξωτερικό φορέα.

12 https://en.wikipedia.org/wiki/Man-in-the-middle_attack
13 https://technet.microsoft.com/en-us/library/cc959354.aspx
14 http://www.dailymail.co.uk/sciencetech/article-2948212/Will-victim-digital-pickpockets-Hacker-reveals-easy-steal-credit-card-numbers-air-SECONDS.html
15 https://www.epe.org.gr/index.php?id=19&tx_ttnews%5Btt_news%5D=11217&cHash=9a759d621ed4cc069d8db3eacd38efec
16 https://www.epe.org.gr/index.php?id=19&tx_ttnews%5Btt_news%5D=9181&cHash=54c1d1c803e4305fafc8bba26cc654cc
17 "Σοβαρές ελλείψεις στο σύστημα προστασίας δεδομένων" (Καθημερινή, 13/9/2015) -- http://is.gd/crWcDG
18 ΑΠΔΠΧ απόφαση 98/2013: Γ/ΕΞ/5276, 9-8-2013.
19 Ν.4389/2016 (ΦΕΚ 94Α'/27-5-2016), άρθρο 37: "Διαχείριση δεδομένων και συστημάτων" -- http://www.et.gr/images/stories/2016/fek_a94_2016/20160100094.pdf

ΕΝΩΣΗ ΠΛΗΡΟΦΟΡΙΚΩΝ ΕΛΛΑΔΑΣ

Για την ΕΠΕ το ζήτημα της ψηφιακής ασφάλειας και της ανάδειξής του ως ένα από τα σημαντικότερα στη σύγχρονη Κοινωνία της Πληροφορίας αποτελεί θεσμικό θέμα και στρατηγικό στόχο. Ο πρόσφατος σχολιασμός μας[20] ως προς την αναβολή αναβάθμισης ασφάλειας (TLS 1.2) στα συστήματα στη ΓΓΠΣ βοήθησε τελικά στην υλοποίηση, έστω και καθυστερημένα, της ενίσχυσης της ασφάλειας του TAXIS. Ταυτόχρονα, ως ΕΠΕ έχουμε ήδη καταθέσει τις παρατηρήσεις[21] μας σχετικά με την υιοθέτηση και ραγδαία ενίσχυση της χρήσης πλαστικού χρήματος και ηλεκτρονικών συναλλαγών, όχι μόνο σε τεχνικό επίπεδο ασφάλειας, αλλά και σε ό,τι αφορά τις σημαντικές επιβαρύνσεις για τους χρήστες. Σε θεσμικό επίπεδο, η ΕΠΕ κατέθεσε σε δημόσια διαβούλευση και πρόσφατα ενσωμάτωσε πλήρως στο Καταστατικό & Εσωτ. Κανονισμό της τον πρώτο Κώδικα Δεοντολογίας για την Πληροφορική (ΚΔΠ)[22,23] στην Ελλάδα. Σημαντικό παράγοντα στον ΚΔΠ και πρώτο ως προτεραιότητα, πέρα και πάνω από οτιδήποτε άλλο, έχει τεθεί το δημόσιο συμφέρον ("public good") - μέρος του οποίου είναι σαφέστατα και η προστασία των προσωπικών δεδομένων όλων των πολιτών, τόσο σε ατομικό επίπεδο, όσο και σε σχέση με όποιο δημόσιο ή ιδιωτικό οργανισμό τα διαχειρίζεται.

Ως ΕΠΕ εξακολουθούμε να στηρίζουμε κάθε προσπάθεια ανάδειξης του ζητήματος της ψηφιακής ασφάλειας, της προστασίας των προσωπικών δεδομένων και της εγρήγορσης πολιτών και φορέων προς αυτή την κατεύθυνση. Παραμένουμε στη διάθεση όλων, ως επιστημονικά και τεχνικά αρμόδιος φορέας, για αντίστοιχες δράσεις.

Το Διοικητικό Συμβούλιο
της Ένωσης Πληροφορικών Ελλάδας

URL: http://www.epe.org.gr , mailto:info@epe.org.gr

20 https://www.epe.org.gr/index.php?id=19&tx_ttnews%5Btt_news%5D=11362&cHash=df983fde80f8b0a00ebb48d22da65fed
21 https://www.epe.org.gr/index.php?id=19&tx_ttnews%5Btt_news%5D=11248&cHash=ef64993ad1af9fb97e00808ad8f362e2
22 https://www.epe.org.gr/index.php?id=19&tx_ttnews%5Btt_news%5D=11187&cHash=8cbc9a8a1bdc6e90f0e48a4e2c6599a6
23 "Κώδικας Δεοντολογίας Πληροφορικών" (ΕΠΕ) -- https://is.gd/Zc16ri