ΣΥΛΛΟΓΟΣ ΔΕΠ ΠΑΝΕΠΙΣΤΗΜΙΟΥ ΑΙΓΑΙΟΥ

ΑΝΟΙΚΤΗ ΕΠΙΣΤΟΛΗ ΚΕΝΤΡΙΚΟΥ ΣΥΜΒΟΥΛΙΟΥ ΣΥΛΛΟΓΟΥ ΔΕΠ ΠΑΝΕΠΙΣΤΗΜΙΟΥ ΑΙΓΑΙΟΥ ΠΡΟΣ ΤΗ ΔΙΟΙΚΗΣΗ ΠΑΝΕΠΙΣΤΗΜΙΟΥ ΑΙΓΑΙΟΥ

22 Ιουνίου 2024

Σχετικά με την ενημέρωση (14/06/2024) από τον Υπεύθυνο Προστασίας Δεδομένων του Πανεπιστημίου Αιγαίου περί της διαρροής προσωπικών δεδομένων

Ύστερα από δημοσιεύσεις σε έντυπο και διαδικτυακό τύπο, την 1η Δεκεμβρίου 2023 ενημερωθήκαμε με μήνυμα στο Aegean Global List από τον Πρύτανη του Πανεπιστημίου Αιγαίου ότι «*αναρτήθηκαν στο Dark Web δεδομένα αποθηκευμένα σε εξυπηρετητές του Πανεπιστημίου τα οποία παρανόμως αποκτήθηκαν, ενδεχομένως τον Μάρτιο του 2023, όταν οι υπολογιστικές μας υποδομές υπέστησαν κυβερνοεπίθεση από άγνωστους […] Μόλις ολοκληρωθεί η έρευνά μας και έχουμε απολύτως ξεκάθαρη εικόνα θα ενημερώσουμε με προσωπικό μήνυμα όσες και όσους από σας των οποίων προσωπικά δεδομένα συμπεριλαμβάνονται στο συγκεκριμένο σύνολο δεδομένων. Παράλληλα λαμβάνουμε όλα τα απαραίτητα τεχνικά και οργανωτικά μέτρα τόσο για τον περιορισμό των επιπτώσεων της διαρροής όσο και για την περαιτέρω θωράκιση της προστασίας των υπολογιστικών μας συστημάτων*.»

Έκτοτε μεσολάβησε διάστημα πέραν του εξαμήνου χωρίς -εξ όσων γνωρίζουμε- κάποιο μέλος της Πανεπιστημιακής κοινότητας να λάβει κάποια ειδική ενημέρωση. Από την Παρασκευή 14 Ιουνίου πάρα πολλά μέλη της πανεπιστημιακής κοινότητας του Αιγαίου (διδάσκοντες, διοικητικοί, φοιτητές) αλλά και συνεργάτες του Πανεπιστημίου (όπως π.χ. εξωτερικοί συνεργάτες που απασχολούνται σε ερευνητικά έργα), λαμβάνουν από τον Υπεύθυνο Προστασίας Δεδομένων του Πανεπιστημίου Αιγαίου προσωποποιημένη ενημέρωση σχετικά με τη διαρροή προσωπικών δεδομένων στο σκοτεινό διαδίκτυο (Dark Web) που έλαβε χώρα στις 23/11/2023, αναφέροντας τα προσωπικά δεδομένα που έχουν «διαρρεύσει». Στη συνέχεια ακολουθεί ένα γενικού χαρακτήρα κείμενο για το ποιες είναι οι ενδεχόμενες συνέπειες της διαρροής για εμάς και ποια είναι τα μέτρα που μπορούμε να λάβουμε για την προστασία μας.

Το περιεχόμενο της προσωποποιημένης ενημέρωσης δημιούργησε απορίες και τεράστια ανησυχία στη μεγάλη πλειοψηφία των μελών της κοινότητας που έλαβαν το μήνυμα. Ενδεικτικά αναφέρεται ότι η «διαρροή» προσωπικών δεδομένων, περιλαμβάνει υποσύνολα ή σύνολα δεδομένων ατόμων, όπως: Ιδιότητα στο Πανεπιστήμιο, ΑΦΜ, ΑΜΚΑ, αριθμός ΔΑΤ ή Διαβατηρίου, Ημερομηνία Γέννησης, Υπογραφή, έως και IBAN τραπεζικών λογαριασμών.

Εμείς ως Σύλλογος λαμβάνουμε καθημερινά μηνύματα είτε ηλεκτρονικά, είτε τηλεφωνικά, με τα οποία οι συνάδελφοι εκδηλώνουν την έντονη ανησυχία τους και θέτουν σ΄εμάς ερωτήματα που προκύπτουν άμεσα από την «προσωποποιημένη ενημέρωση» που έλαβαν. Σας παραθέτουμε μερικά απ΄αυτά, γιατί είσαστε οι αρμόδιοι να παρέχετε λεπτομερή ενημέρωση και τις απαιτούμενες απαντήσεις:

- Γιατί δεν υπήρξε εγκαίρως, αμέσως μετά την εκδήλωση του περιστατικού, ενημέρωση προς το σύνολο της Πανεπιστημιακής Κοινότητας, με οδηγίες ανάλογες με αυτές που μας έστειλαν τώρα, αφού ήταν εξ αρχής γνωστός ή έστω διαγνώσιμος ο τεράστιος όγκος της δεδομένων ώστε να λάβουμε όλοι μέτρα προστασίας και να είμαστε υποψιασμένοι έναντι

ενδεχόμενης κακόβουλης χρήσης των δεδομένων μας (απάτη, κλοπή ταυτότητας κ.α.); Αντιθέτως, το μεγάλο διάστημα που μεσολάβησε έως την ατομική ενημέρωση οδήγησε πολλούς συναδέλφους στην εσφαλμένη εντύπωση ότι τα δικά τους προσωπικά στοιχεία δεν κατέστησαν γνωστά σε τρίτους, πιθανότατα κακόβουλους, και μάλιστα σε απροσδιόριστο αριθμό προσώπων.

- Σημειώνεται, ότι εκ των υστέρων, πολλοί συνδυάζουν την αυξημένη αποστολή μηνυμάτων spam ή ακόμα και απόπειρες υφαρπαγής προσωπικών στοιχείων ή απάτης που αντιμετώπισαν στο διάστημα αυτό με το περιστατικό ασφάλειας.
- Ποια μέτρα λήφθηκαν αναφορικά α) με τη διερεύνηση του περιστατικού και β) με τη λήψη μέτρων από τη στιγμή που έγινε αντιληπτή η παραβίαση του Νοεμβρίου 2023 και μέχρι τώρα; Η γενική αναφορά σε «άμεσα και αποφασιστικά μέτρα» κρίνεται σαφής και επαρκής όταν αναφερόμαστε σε τέτοιας έκτασης παραβίαση με άδηλες συνέπειες για όσους έχουν εκτεθεί τα δεδομένα τους; Ποια είναι η αιτιολογία για τη μεσολάβηση τόσο μεγάλου χρονικού διαστήματος, από τον εντοπισμό του περιστατικού και μέχρι την -εν τέλει μαζική- ανακοίνωση;
- Υπάρχει σαφής εικόνα για το ποια προσωπικά δεδομένα έχουν διαρρεύσει και καταστεί γνωστά σε μη δικαιούμενα πρόσωπα; Όταν πρόκειται για προσωποποιημένη ενημέρωση πως νοείται η αναφορά «ΑΔΤ ή Διαβατηρίου»; Υπάρχει σαφής εικόνα για τα αρχεία/ βάσεις που αποτέλεσαν στόχο της επίθεσης από τα οποία αντλήθηκαν και τα επιμέρους δεδομένα;
- Πώς δικαιολογείται ότι δεν κρίθηκε αναγκαία η κατεπείγουσα ενημέρωση τουλάχιστον των μελών της Πανεπιστημιακής Κοινότητας των οποίων διέρρευσε το IBAN του ή στοιχεία των τραπεζικών τους λογαριασμών;
- Γιατί ενώ έχουν συμβεί διαδοχικά σοβαρά περιστατικά παραβίασης δεν έχει υπάρξει ενημέρωση των χρηστών για τις πρακτικές προστασίας των συστημάτων τους;
- Τα παραπάνω ερωτήματα ευλόγως γεννούν σοβαρές επιφυλάξεις σχετικά με το εύρος των δεδομένων που έχουν διαρρεύσει, καθώς πολλά μέλη της Πανεπιστημιακής Κοινότητας εκφράζουν την ανησυχία ότι ενδεχομένως έχουν διαρρεύσει και κοινολογηθεί περισσότερα δεδομένα που μπορεί να αφορούν π.χ. την οικογενειακή κατάσταση, στοιχεία τρίτων προσώπων (όπως μέλη οικογένειας κλπ.). Μπορεί η Διοίκηση του Πανεπιστημίου ύστερα από την – υποθέτουμε – ενδελεχή έρευνα 8 μηνών να επιβεβαιώσει ότι η επίθεση και οι συνέπειές της αφορούν μόνο τα στοιχεία για τα οποία ενημερωθήκαμε;
- Γνωρίζουμε μετά την έρευνα που έγινε ποια μηχανήματα παραβιάστηκαν και ποια στοιχεία ήταν αποθηκευμένα σ΄αυτά;
- Οι οδηγίες που εστάλησαν δεν είναι εξειδικευμένες, αλλά περιγράφουν τις καλές πρακτικές για την ασφάλεια των δεδομένων. Ποια μέτρα ή ποιες κατηγορίες μέτρων έχουν συγκεκριμένα ληφθεί ή σχεδιάζονται για την αποφυγή παρόμοιων περιστατικών, εκτός από την περιοδική αλλαγή κωδικού που αποτελεί το μόνο ορατό για την κοινότητα μέτρο έως τώρα;
- Ποια μέτρα υπήρχαν όταν εκδηλώθηκε η επίθεση στα συστήματα του Πανεπιστημίου Αιγαίου; Εάν υπήρχαν, υπάρχει επαρκής αιτιολογία και τεκμηρίωση γιατί αποδείχτηκαν ανεπαρκή ως προς την ασφάλεια συστημάτων και πληροφοριών; Ποια ήταν εκείνα τα μέτρα ασφάλειας που είχαν ληφθεί μετά την προηγούμενη κυβερνοεπίθεση του Μαρτίου 2023 και επέτρεψαν να συμβεί και η επόμενη, του Νοεμβρίου 2023;
- Γιατί δεν ενημερωθήκαμε από την αρμόδια πανεπιστημιακή αρχή, τον Υπεύθυνο Επεξεργασίας Δεδομένων, δηλ. το Πανεπιστήμιο όπως εκπροσωπείται από το αρμόδιο όργανο διοίκησής του όπως ορίζει ο Γενικός Κανονισμός Προστασίας Δεδομένων, και λάβαμε μήνυμα από τον Υπεύθυνο Προστασίας Δεδομένων του Πανεπιστημίου Αιγαίου;

- Ποιο όργανο του Πανεπιστημίου (Πρύτανης, Αντιπρυτάνεις;) έχει ως αρμοδιότητα την ασφάλεια συστημάτων, πληροφοριών και δικτύων και την διασφάλιση της εφαρμογής της νομοθεσίας για την προστασία δεδομένων; Επικουρούνται ή υποστηρίζονται από κάποια άλλα όργανα και επιτροπές και εάν ναι από ποια, με ποια σύνθεση και ποιες αρμοδιότητες;
- Πώς σχεδιάζει να αντιμετωπίσει το Ίδρυμα ενδεχόμενες προσφυγές στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα ή στα Δικαστήρια από τρίτους, όπως φοιτητές, συνεργάτες κ.λπ., τα στοιχεία των οποίων επίσης διέρρευσαν και επικοινωνούν με τα αντίστοιχα Τμήματα και μέλη ΔΕΠ διαμαρτυρόμενοι;
- Τι μπορεί να σημαίνει για τη λειτουργία του Πανεπιστημίου μας, ότι ενώ δεν έχουν αναφερθεί τόσο σοβαρά παρόμοια περιστατικά σε άλλα ελληνικά Πανεπιστήμια, στο Πανεπιστήμιο Αιγαίου συνέβησαν δύο φορές, σε διάστημα μερικών μηνών;

Αξιότιμε κύριε Πρύτανη
Θεωρούμε ότι απαιτείται άμεσα να συγκαλέσετε μια ανοικτή Σύγκλητο με όλα τα μέλη της κοινότητας ή μια ανοικτή συζήτηση για να απαντηθούν όχι μόνο αυτά τα ερωτήματα που λάβαμε εμείς αλλά όλα τα ερωτήματα των άμεσα ενδιαφερομένων και να δοθούν όλες οι διευκρινίσεις που απαιτούνται. Η κοινότητα πρέπει να αποκαταστήσει τη ζημία που έχει υποστεί και να νοιώσει ασφαλής μετά το περιστατικό που έλαβε χώρα και μετά το περιεχόμενο της προσωποποιημένης ενημέρωσης που έλαβαν οι συνάδελφοι που δημιούργησε πολύ μεγάλη ανησυχία.