Ελληνικό Ανοικτό Πανεπιστήμιο

Διευκρινιστικές ερωταπαντήσεις για την υπόθεση διαρροής προσωπικών δεδομένων της 25ης Οκτωβρίου 2024

1. ***Ποιο χρονικό διάστημα και πόσες επιθέσεις έχει δεχθεί το πληροφοριακό σύστημα του Ελληνικού Ανοικτού Πανεπιστημίου;***

Όπως και άλλοι δημόσιοι και ιδιωτικοί φορείς, έχουμε γίνει στόχος αρκετών κυβερνοεπιθέσεων στο παρελθόν, τις οποίες αποκρούσαμε με επιτυχία. Αυτή που δεν μπορέσαμε να αποκρούσουμε ήταν αυτή της 25ης Οκτωβρίου 2024.

2. ***Που οφείλεται η ευαλωτότητα του πληροφοριακού συστήματος;***

Θα πρέπει να σημειωθεί ότι κανένα πληροφοριακό σύστημα δεν είναι αδιαπέραστο καθώς οι κυβερνοεγκληματίες διαρκώς βρίσκουν τρόπους να παρακάμπτουν ακόμα και πολύ προηγμένα συστήματα ασφαλείας. Το ερώτημα λοιπόν είναι με ποιους τρόπους επικαιροποιείται διαρκώς η ασφάλεια της πληροφοριακής υποδομής ενός οργανισμού, καθιστώντας την λιγότερο ευάλωτη. Αν και το σύστημά μας είχε πολύ υψηλό επίπεδο ασφάλειας, δεν κατάφερε να αποτρέψει την συγκεκριμένη επαγγελματική επίθεση.

3. ***Γιατί η υπόθεση δημοσιοποιήθηκε πέντε μήνες μετά την αναφερόμενη επίθεση;***

Η υπόθεση δεν δημοσιοποιήθηκε τώρα. Είχαν προηγηθεί τέσσερεις ανακοινώσεις με τις οποίες γινόταν ενημέρωση με βάση τα στοιχεία τα οποία ήταν διαθέσιμα. Ο λόγος που αναρτήθηκε η (5η κατά σειρά) ανακοίνωση σε αυτή τη χρονική στιγμή, είναι ότι οφείλαμε πρώτα να ολοκληρώσουμε μια σειρά εσωτερικών ενεργειών αλλά και συνεργασιών με τους αρμόδιους θεσμικούς φορείς, προκειμένου να υπάρχει ολοκληρωμένη εικόνα. Η τελευταία ενέργεια ήταν η μήνυση κατά αγνώστων και ακολούθησε η συγκεκριμένη ανακοίνωση. Σε κάθε περίπτωση η ενημέρωση πραγματοποιήθηκε με βάση τα υπάρχοντα δεδομένα και με τον κατάλληλο βαθμό τεκμηρίωσης.

4. ***Τι έκταση είχε η διαρροή σε σχέση με τον συνολικό όγκο των δεδομένων;***

Διέρρευσαν 813GB, που αντιστοιχούν σε ποσοστό της τάξης του 2 με 2.5% των δεδομένων του ΕΑΠ. Συνεπώς η διαρροή ήταν πολύ μικρή σε σχέση με το συνολικό μέγεθος των δεδομένων.

5. ***Τι δεδομένα αφορά η κυβερνοεπίθεση; Ποια από αυτά είναι ευαίσθητα;***

Από αρχική ανάλυση των ανακτηθέντων δεδομένων (βλ. παρακάτω) προκύπτει ότι αυτά αφορούν, κυρίως, σε ονοματεπώνυμα, αριθμούς κινητού τηλεφώνου και διευθύνσεις ηλεκτρονικού ταχυδρομείου. Στο ανακτημένο μέρος του αρχείου, δεδομένα όπως ΑΦΜ και διευθύνσεις κατοικίας φαίνεται να υπάρχουν σε πολύ περιορισμένη έκταση.

6. ***Που βρίσκονται τα δεδομένα που κλάπηκαν και κατά πόσο είναι ανακτήσιμα;***

Τα δεδομένα βρίσκονται στο «σκοτεινό διαδίκτυο» (darkweb) με όσες δυσκολίες αυτό συνεπάγεται για τις δυνατότητες ελέγχου και ανάκτησης. Μέχρι σήμερα, έχει καταστεί εφικτή η ανάκτηση μόνο ενός μικρού μέρους του αρχείου (περίπου 65 GB). Επισημαίνεται ρητά ότι η ανάκτηση αυτού του αρχείου πραγματοποιήθηκε από το Ίδρυμα και όχι από τρίτους.

7. ***Σε τι ενέργειες έχει προβεί το ΕΑΠ από τη στιγμή που αντιλήφθηκε τη διαρροή;***

- Το ΕΑΠ ήταν από την πρώτη στιγμή σε συνεννόηση με τις αρμόδιες αρχές (Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, Εθνική Αρχή Κυβερνοασφάλειας, Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος, Υπουργείο Παιδείας) συμμορφώθηκε πλήρως με όλες τις υποδείξεις των και ακολούθησε τις διεθνώς ενδεδειγμένες καλύτερες πρακτικές.
- Η Διοίκηση του Πανεπιστημίου, με διαδοχικές ανακοινώσεις αλλά και με μεγάλη προσοχή και αίσθημα ευθύνης, ενημέρωνε το κοινό για την κατάσταση και τις ενέργειες που έχουν πραγματοποιηθεί.
- Το ΕΑΠ έχει προχωρήσει σε περαιτέρω αναβάθμιση των σχετικών υποδομών και του επιπέδου προστασίας των προσωπικών δεδομένων.
- Το ΕΑΠ προχώρησε σε μήνυση κατ' αγνώστων για το συγκεκριμένο περιστατικό.

8. ***Ποιοι είναι οι κίνδυνοι για τα πρόσωπα των οποίων τα δεδομένα έχουν κλαπεί;***

Το ΕΑΠ έχει ενημερώσει αναλυτικά για τους κινδύνους που διατρέχουν τα πρόσωπα των οποίων τα δεδομένα **ενδεχομένως** να έχουν διαρρεύσει, αλλά και για τις ενέργειες που θα πρέπει να κάνουν προκειμένου να είναι προστατευμένα τα προσωπικά τους δεδομένα. Μόλις όμως ολοκληρωθεί η ανάλυση και σε περίπτωση που διαπιστωθεί διαρροή ευαίσθητων προσωπικών δεδομένων, θα υπάρξει εξατομικευμένη ενημέρωση των άμεσα ενδιαφερομένων.

9. ***Ζητήθηκαν λύτρα από αυτούς που οργάνωσαν την κυβερνοεπίθεση; Τι έχει απαντήσει το ΕΑΠ;***

Πράγματι ζητήθηκαν λύτρα. Πρόκειται για επίθεση ransomware. Από την πλευρά του ΕΑΠ δεν υπήρξε καμία επικοινωνία ούτε διαπραγμάτευση με τους εγκληματίες.

10. ***Πως σκέφτεστε να αντιμετωπίσετε ενδεχόμενες μηνύσεις από πρώην ή νυν φοιτητές;***

Θα ακολουθηθεί βεβαίως η νόμιμη διαδικασία. Προτρέπουμε πάντως τους ενδιαφερόμενους να περιμένουν πρώτα την τεκμηριωμένη ενημέρωσή μας.

11. ***Έχει αναβαθμιστεί το σύστημα κυβερνοασφάλειας του ΕΑΠ και σε τι ενέργειες έχει προβεί για την θωράκιση της πληροφοριακής σας υποδομής στο μέλλον από αντίστοιχες κακόβουλες ενέργειες;***

Αναβαθμίσαμε το σύστημα προστασίας, λαμβάνοντας υπόψη τις νέες συνθήκες που διαμορφώθηκαν. Υπάρχει διαρκής εγρήγορση και ετοιμότητα, αν και καμία πληροφοριακή υποδομή δεν είναι 100% προστατευμένη.

12. ***Πως μπορεί κάποιος να ενημερωθεί για την κατάσταση των δεδομένων του και αν έχει πέσει θύμα της κυβερνοεπίθεσης; Έχετε δημιουργήσει κάποια γραμμή ή σύστημα υποστήριξης και πληροφόρησης;***

Μόλις ολοκληρωθεί η ανάλυση και επιβεβαιωθεί ποια ακριβώς προσωπικά δεδομένα έχουν διαρρεύσει και ποια υποκείμενα επηρεάζονται, θα ακολουθήσει εξατομικευμένη ενημέρωση προς τους άμεσα ενδιαφερόμενους. Σε περίπτωση που τα δεδομένα κάποιου/ας περιλαμβάνονται στη διαρροή, θα λάβει προσωπική ειδοποίηση με αναλυτικές πληροφορίες σχετικά με τα προσωπικά δεδομένα που επηρεάστηκαν. Επιπλέον, θα υπάρξει νέα, γενική ανακοίνωση όταν ολοκληρωθεί η διαδικασία διερεύνησης και ανάλυσης όλων των διαθέσιμων στοιχείων.

13. ***Τι μέτρα ασφάλειας μπορεί να πάρει κάποιος ή κάποια που μπορεί να έχει πέσει θύμα της κυβερνοεπίθεσης;***

- Αλλάξτε, άμεσα, τους κωδικούς πρόσβασης στους λογαριασμούς σας (ηλεκτρονικού ταχυδρομείου και υπηρεσιών μητρώου). Συνιστάται η χρήση ενός μοναδικού και ισχυρού κωδικού, με τουλάχιστον 10 χαρακτήρες που να περιλαμβάνει συνδυασμό κεφαλαίων και πεζών γραμμάτων, αριθμών και συμβόλων. Επιπλέον, προτείνεται η τακτική αλλαγή του κωδικού, ιδανικά κάθε έξι μήνες.
- Αποφύγετε τη χρήση του ίδιου κωδικού πρόσβασης σε πολλαπλές υπηρεσίες.
- Να είστε προσεκτικοί με emails ή τηλεφωνικές κλήσεις που ζητούν προσωπικά στοιχεία ή οικονομικές πληροφορίες.
- Μην ανοίγετε συνδέσμους και μην κατεβάζετε συνημμένα από άγνωστες ή ύποπτες πηγές.
- Παρακολουθείτε τις συναλλαγές σας για τυχόν μη εξουσιοδοτημένες κινήσεις και ενημερώστε, άμεσα, την τράπεζά σας, σε περίπτωση ύποπτης δραστηριότητας.
- Χρησιμοποιήστε λογισμικό προστασίας από κακόβουλο λογισμικό και διατηρήστε το ενημερωμένο.
- Περιορίστε τη δημοσίευση προσωπικών πληροφοριών σε δημόσιες πλατφόρμες και κοινωνικά δίκτυα.
- Ρυθμίστε ειδοποιήσεις για ύποπτες συνδέσεις ή δραστηριότητα στους λογαριασμούς σας.
- Ενημερώστε, άμεσα, τον πάροχο υπηρεσιών σας εάν παρατηρήσετε ύποπτη δραστηριότητα σε προσωπικούς ή επαγγελματικούς σας λογαριασμούς.
- Σε περίπτωση που αρχίσετε να λαμβάνετε ανεπιθύμητες, εμπορικές κλήσεις, εξετάστε την πιθανότητα εγγραφής σας, μέσω των σχετικών, νόμιμων διαδικασιών στο μητρώο της παρ. 2, άρθρου 11, Ν. 3471/2006.
- Σε περίπτωση που λαμβάνετε ενοχλητικά, διαφημιστικά email, μηνύματα ή μηνύματα τα οποία δε σχετίζονται με την εκπαιδευτική διαδικασία στις ηλεκτρονικές διευθύνσεις που σας έχουν δοθεί από το Ε.Α.Π., παρακαλούμε να τα γνωστοποιείτε στο Γραφείο Δικτυακών και Πληροφοριακών Υπηρεσιών, προωθώντας τα εν λόγω μηνύματα στην email διεύθυνση abuse@eap.gr, έτσι ώστε να λαμβάνονται όλα τα απαραίτητα μέτρα.