ΕΝΩΣΗ ΠΛΗΡΟΦΟΡΙΚΩΝ ΕΛΛΑΔΑΣ

Ένωση Πληροφορικών Ελλάδας
Λυκούργου 1 & Αιόλου (1ος όροφος)
ΤΚ 10551, Αθήνα
http://www.epe.org.gr
e-mail: info@epe.org.gr
Τηλέφωνο: (+30) 211 3332456

Δελτιο Τυπου

Ξανά "επίθεση hackers" στην τράπεζα θεμάτων;

Αθήνα, 22-5-2025

Νωρίς το πρωί της Τετάρτης 21/5/2025 οι εκπαιδευτικοί που είχαν επωμιστεί τις διαδικασίες επικοινωνίας με την πλατφόρμα της Τράπεζας Θεμάτων Διαβαθμισμένης Δυσκολίας (ΤΘΔΔ) του Ινστιτούτου Εκπαιδευτικής Πολιτικής (ΙΕΠ) στα πλαίσια των σχολικών εξετάσεων διαπίστωσαν ότι **το σύστημα ήταν εκτός λειτουργίας**.

Για περίπου **δύο ώρες** η επικοινωνία και η διεκπεραίωση των διαδικασιών ήταν αδύνατη, ενώ υπήρξαν αναφορές ότι δεν υπήρχε δυνατότητα ούτε τηλεφωνικής επικοινωνίας. Σύμφωνα με τα δημοσιεύματα[1]:

"...ο πρόεδρος του ΙΕΠ Σπύρος Δουκάκης δήλωσε στο esos.gr ότι το πρόβλημα δεν είναι του ΙΕΠ αλλά γενικότερο καθώς ούτε η Γενική Γραμματεία Πληροφορικών συστημάτων λειτουργεί."

Σχεδόν δύο ώρες αργότερα από τις πρώτες αναφορές του προβλήματος διαπιστώθηκε ότι:

"...οι Διευθυντές των Λυκείων μπορούν να εισέλθουν στην Τράπεζα Θεμάτων όχι με τους κωδικούς του σχολείου αλλά με κωδικούς του taxisnet."

Αργότερα την ίδια μέρα ο υπουργός Ψηφιακής Διακυβέρνησης κ. Δημήτρης Παπαστεργίου βρέθηκε στην ΕΡΤ όπου και δήλωσε επίσημα[2] ότι το πρόβλημα οφείλεται σε:

"...κυβερνοεπίθεση κυρίως στο υπουργείο Παιδείας η οποία αντιμετωπίστηκε πολύ γρήγορα από του ανθρώπους του gov.gr".

1 https://www.esos.gr/arthra/93498/katerreyse-i-trapeza-thematon-panikos-sta-lykeia-problima-lythike-meta-apo-2-ores

2 https://www.ertnews.gr/eidiseis/ellada/d-papastergiou-gia-trapeza-thematon-sto-ertnews-i-kyvernoepithesi-antimetopistike-poly-grigora-i-anakoinosi-tou-yp-paideias/

Σχεδόν ταυτόχρονα δημοσιεύτηκε[3] ότι:

"...το θέμα λύθηκε γρήγορα με άμεση παρέμβαση της υπουργού Παιδείας Σοφίας Ζαχαράκη η οποία ήρθε σε επαφή με τον κεντρικό μηχανισμό ταυτοποίησης και διαβαθμισμένης πρόσβασης των χρηστών."

Λίγο αργότερα σύμφωνα με την επίσημη ανακοίνωση του Υπουργείου Παιδείας[4]:

"...Η προσωρινή δυσλειτουργία σχετιζόταν με τον κεντρικό μηχανισμό ταυτοποίησης και διαβαθμισμένης πρόσβασης των χρηστών."

Και λίγες ώρες αργότερα, σύμφωνα με δημοσιεύματα[5]:

"...ο γενικός γραμματέας του ΥΠΑΙΘΑ κ.Ι.Κατσαρός με νέα του εγκύκλιο, ορίζει ότι τις ημέρες διενέργειας των παραπάνω εξετάσεων και δύο (2) ώρες προ της έναρξης αυτών πρέπει να υπάρχει προσωπικό υποστήριξης επιφορτισμένο να δίδει απαντήσεις για θέματα που τυχόν αναφύονται σχετικά με την Τ.Θ.Δ.Δ. και την επιλογή θεμάτων εξετάσεων από τα Λύκεια. Με τον τρόπο αυτόν το υπουργείο επιχειρεί να αντιμετωπίσει οποιαδήποτε επόμενη κυβερνοεπίθεση, δεδομένου ότι πρόβλημα εκδηλώθηκε σήμερα και στο Πανελλήνιο Σχολικό Δίκτυο."

Σύμφωνα με τα παραπάνω, το Υπουργείο δηλώνει ότι:

- Υπήρξε "κυβερνοεπίθεση" στην οποία οφείλεται το πρόβλημα πρόσβασης παντού, σε όλα τα διασυνδεδεμένα συστήματα (σχολικό δίκτυο και ΓΓΠΣ).
- Το πρόβλημα εντοπίζεται στο σύστημα ταυτοποίησης των χρηστών κατά την είσοδό τους.
- Το πρόβλημα λύθηκε με ένα τηλεφώνημα της υπουργού Παιδείας στην αρμόδια υπηρεσία.
- Τυχόν νέο παρόμοιο πρόβλημα θα αντιμετωπιστεί έχοντας πρόσθετο *"προσωπικό υποστήριξης επιφορτισμένο να δίδει απαντήσεις".*

Είμαστε υποχρεωμένοι να θυμίσουμε ότι τόσο οι δηλώσεις εκ μέρους του υπουργείου ("κυβερνοεπίθεση"), όσο και η φύση του προβλήματος (ταυτοποίηση χρηστών), δείχνουν να είναι **ακριβώς ταυτόσημα με το ίδιο περιστατικό τον Μάιο του 2023**. Με άλλα λόγια, για δεύτερη φορά κάποιοι "χάκερς" καταφέρνουν να προσβάλλουν **το ίδιο υποσύστημα, με τον ίδιο τρόπο και τα ίδια αποτελέσματα**, απλά σε μικρότερη διάρκεια χρονικά.

3 https://www.alfavita.gr/ekpaideysi/478518_amesi-parembasi-tis-sofias-zaharaki-gia-tin-apokatastasi-tis-leitoyrgias-tis

4 https://www.alfavita.gr/ekpaideysi/478524_sto-stohastro-haker-i-trapeza-thematon-d-papastergioy-egine-kybernoepithesi

5 https://www.alfavita.gr/ekpaideysi/478573_oi-fylakes-tis-trapezas-thematon-egkyklios-ypaitha-orizei-prosopiko-ypostirixis

Το κατά πόσο ένα τέτοιο ενδεχόμενο είναι ή όχι πιθανό έχει αναλυθεί επαρκώς στην ανακοίνωση της ΕΠΕ τότε[6], με διαπιστώσεις και ερωτήματα για τα οποία **ουδέποτε δόθηκαν απαντήσεις από τους αρμόδιους φορείς**.

Ανεξάρτητα από το τι πραγματικά συνέβη αυτή τη φορά, ξανά "κυβερνοεπίθεση", θα πρέπει να διευκρινίσουμε το εξής: Από το 2023 **έχουμε κουραστεί να ακούμε για δήθεν πολυπρόσωπες ομάδες από hackers** που στοχεύουν τα Πληροφοριακά Συστήματα του ΙΕΠ. Για όποιον δεν το γνωρίζει, ενημερώνουμε ότι ακόμη κι ένας μαθητής του τομέα Πληροφορικής των ΕΠΑΛ, ο οποίος ίσως να μην έχει διάθεση να γράψει εξετάσεις εκείνη την ημέρα, μπορεί να δοκιμάσει μια επίθεση τύπου DDoS, χρησιμοποιώντας κάποιο έτοιμο σενάριο κελύφους (shell script) από τα πολλά που κυκλοφορούν ως εκπαιδευτικά παραδείγματα στο διαδίκτυο. Φυσικά, εξίσου εύκολα μπορεί μια τέτοια επίθεση να προληφθεί ή να αντιμετωπιστεί καθώς συμβαίνει, αν υπάρχει η κατάλληλη προετοιμασία, υποδομή και τεχνική εκπαίδευση του προσωπικού.

Αυτό που αξίζει να αναφερθεί σε εκείνο περιστατικό είναι ότι τότε, αμέσως μετά, είχαν ανακοινωθεί μια σειρά μέτρα και τεχνικές αναβαθμίσεις, μεταξύ των οποίων[7]:

- Το ΙΕΠ είχε αναθέσει σε ιδιωτική εταιρεία να κάνει στοχευμένες βελτιώσεις στην υποδομή.
- Μεταφορά του περιεχομένου σε cloud υποδομή της Amazon, ειδικά με χρήση της υπηρεσίας AWS S3.
- Παραμετροποίηση του AWS Content Delivery Network ώστε να προστατεύεται από κακόβουλες επιθέσεις (DDoS attacks).
- Μεταφορά των υφιστάμενων php εφαρμογών σε cloud υποδομή της AWS.
- Υλοποίηση εναλλακτικού τρόπου διασύνδεσης με στοιχεία του TAXIS καθώς και διασύνδεση αυτού με το υφιστάμενο σύστημα.
- Μελέτη Εφαρμογής - Ανάλυση Απαιτήσεων.
- Μελέτη Ασφάλειας.
- Μελέτη Ιδιωτικότητας - Συμμόρφωση με Γενικό Κανονισμό Προστασίας Προσωπικών Δεδομένων (GDPR).
- Σχέδιο Ανάκαμψης από Καταστροφές (Disaster Recovery Plan).

Για τα παραπάνω **προβλέφθηκε κονδύλι ύψους 595.200 ευρώ** και πλάνο άμεσης υλοποίησης, ώστε *"...να μην επαναληφθούν τα ίδια στο μέλλον"*.

Η εργασία των εκπαιδευτικών και, κυρίως, το μέλλον των μαθητών και εξετάσεις τους στα σχολεία είναι θέματα που δεν αφήνουν περιθώρια για πολλά λόγια και

6 https://www.epe.org.gr/ola-ta-arthra/deltio-typoy-psifiaki-ellada-20-i-kybernitiko-denial-of-service

7 https://www.esos.gr/arthra/93498/katerreyse-i-trapeza-thematon-panikos-sta-lykeia-problima-lythike-meta-apo-2-ores

αοριστίες. Ολοι πρέπει να **σοβαρευτούν** και να κατανοήσουν τις ευθύνες που φέρει η θέση και υπογραφή τους.

Η ΕΠΕ ζητά από το ΥΠΑΙΘΑ, το ΙΕΠ και κάθε άλλο αρμόδιο φορέα να μας **πληροφορήσουν δημόσια και άμεσα** για το πλήρες περιεχόμενο των παρακάτω, σε σχέση με τις παραπάνω χρηματοδοτούμενες δράσεις:

1. Παραδοτέο Π.1.1 Μελέτη Εφαρμογής
2. Παραδοτέο Π2.2 Σενάρια Ελέγχου Λογισμικού και Πλάνο Δοκιμών Ελέγχου
3. Παραδοτέο Π2.3 Έκθεση αποτελεσμάτων διενέργειας ελέγχων
4. Παραδοτέο Π3.1 Τεύχος αποτελεσμάτων Δοκιμαστικής Λειτουργίας
5. Παραδοτέο Π5.1 Μελέτη Ασφαλείας (“Μελέτη ασφαλείας καθώς και αναγνωρισμένοι κίνδυνοι”
6. Παραδοτέο Π5.2 Μελέτη Απόδοσης (“Πίνακας απόδοσης σε συνθήκες υψηλού φόρτου (stress tests)”)

Από τα παραπάνω παραδοτέα, εφόσον είναι τεχνικώς επαρκή, πλήρη και τεκμηριωμένα, είναι βέβαιο ότι μπορεί να διαπιστωθεί αν και κατά πόσο η κατάσταση της υποδομής της ΤΘΔΔ θα έπρεπε σήμερα να είναι σε καλύτερη κατάσταση και αξιοπιστία σε σχέση με το 2023.

Επιπλέον, ως ΕΠΕ **αιτούμαστε δημόσια** και αναμένουμε να αποκτήσουμε πρόσβαση στα παρακάτω:

1. Την επίσημη αναφορά περιστατικού (incident report) που βάσει νόμου ο φορέας υποχρεούται να υποβάλλει πάραυτα στην ΑΠΔΠΧ, στην ΑΔΑΕ και σε κάθε άλλη συναρμόδια Αρχή σε ανάλογα περιστατικά.
2. Την έκθεση-πιστοποίηση συμμόρφωσης της πλατφόρμας ΤΘΔΔ με τα πρότυπα και τις υποχρεώσεις που προβλέπονται στον κανονισμό NIS2 της ΕΕ[8].
3. Μελέτη Ασφάλειας (βλ. παραπάνω).
4. Μελέτη Ιδιωτικότητας - Συμμόρφωση με Γενικό Κανονισμό Προστασίας Προσωπικών Δεδομένων (GDPR) (βλ. παραπάνω).
5. Την τρέχουσα έκδοση του εγχειριδίου “Σχέδιο Ανάκαμψης από Καταστροφές (Disaster Recovery Plan)” (βλ. παραπάνω).
6. Την τρέχουσα Πολιτική Ασφάλειας που ο αρμόδιος φορέας υποχρεούται να τηρεί και να εφαρμόζει, συμπεριλαμβανομένων και των τυποποιημένων διαδικασιών ανταπόκρισης σε περιστατικά ασφάλειας ή διαθεσιμότητας των υπηρεσιών του.
7. Την τεχνική έκθεση-αξιολόγηση της εφαρμογής των δύο παραπάνω κατά τη διάρκεια και αμέσως μετά την εξέλιξη του περιστατικού.

8 https://digital-strategy.ec.europa.eu/el/policies/nis2-directive

8. Τα αντίστοιχα τεχνικά δεδομένα που να τεκμηριώνουν όλα τα παραπάνω, ανωνυμοποιημένα αν απαιτείται για λόγους προστασίας της ιδιωτικότητας.

Σχετικά με το τελευταίο σημείο, παραθέτουμε αυτούσια τη σχετική διατύπωση στην ανακοίνωση[9] της ΕΠΕ το 2023 και η οποία δεν απαντήθηκε ποτέ:

> *"...Είμαστε βέβαιοι ότι η ελληνική Δικαιοσύνη, με τη συνδρομή της Δίωξης Ηλεκτρονικού Εγκλήματος, θα εντοπίσει τα αίτια που προκάλεσαν το πρόβλημα. Καλούμε τους αρμόδιους φορείς να δημοσιοποιήσουν αναλυτικά τα ευρήματα της έρευνας όταν ολοκληρωθεί. Καλούμε επίσης όλους τους συναρμόδιους φορείς και υπηρεσίες να πράξουν τα δέοντα για την άμεση δημοσιοποίηση στοιχείων ως προς τα τεχνικά χαρακτηριστικά της φερόμενης επίθεσης μόλις αυτά γίνουν διαθέσιμα, όπως ενδεικτικά το είδος των αιτημάτων που έγιναν προς τους εξυπηρετητές - ενδεικτικά GET/POST/PATCH requests, είδος/μέγεθος και ταχύτητα μετάδοσης payload, προορισμός/endpoint διεύθυνσης προορισμού, κλπ. Τα στοιχεία αυτά θα επιτρέψουν τη μελέτη της περίπτωσης από τους τεχνικούς άλλων οργανισμών με σκοπό την κατανόηση των αδυναμιών και την υλοποίηση μεθόδων αποφυγής παρόμοιων προβλημάτων στο μέλλον..."*

Ως ΕΠΕ, δηλώνουμε δημόσια ότι διαθέτουμε τόσο την επιστημονική επάρκεια και τεχνολογική εμπειρία, όσο και την πρόθεση, να μελετήσουμε προσεκτικά τα παραπάνω τεκμήρια και να εκθέσουμε επίσης **δημόσια τη γνωμοδότησή μας**, ειδικότερα σε σχέση με τα παρακάτω βασικά ερωτήματα:

- Πως διαπιστώνεται και πως τεκμηριώνεται ότι πρόκειται για ένα ακόμα περιστατικό "κυβερνοεπίθεσης", στο ίδιο υποσύστημα, με τον ίδιο τρόπο, ξανά με επιτυχία;
- Πως ακριβώς ξοδεύτηκαν τα 595.200 ευρώ ακριβώς για αυτό το σκοπό, δηλαδή να διαπιστωθούν οι ελλείψεις και να βελτιωθεί η αξιοπιστία της ΤΘΔΔ;
- Ποιος αναλαμβάνει την ευθύνη για την "επιτυχία" των δύο μέχρι τώρα "κυβερνοεπιθέσεων" και για όποια πιθανόν ακολουθήσει στο μέλλον;

Παραμένουμε στη διάθεση της Πολιτείας και των αρμόδιων Αρχών, εφόσον ζητηθεί η συνδρομή μας σε σχέση με τα παραπάνω.

9 https://www.epe.org.gr/ola-ta-arthra/deltio-typoy-psifiaki-ellada-20-i-kybernitiko-denial-of-service

ΕΝΩΣΗ ΠΛΗΡΟΦΟΡΙΚΩΝ ΕΛΛΑΔΑΣ

Το Διοικητικό Συμβούλιο
της Ένωσης Πληροφορικών Ελλάδας

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