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

Μαζική διαρροή προσωπικών δεδομένων από το ΕΕΤΑΑ

Αθήνα, 24-4-2025

Στις 10 Μαρτίου 2025 αναρτήθηκε στον ιστότοπο της ΕΕΤΑΑ η παρακάτω έκτακτη ανακοίνωση[1]:

> *"Η ΕΛΛΗΝΙΚΗ ΕΤΑΙΡΕΙΑ ΤΟΠΙΚΗΣ ΑΝΑΠΤΥΞΗΣ ΚΑΙ ΑΥΤΟΔΙΟΙΚΗΣΗΣ Α.Ε. (ΕΕΤΑΑ ΑΕ) σας ενημερώνει ότι τα πληροφοριακά της συστήματα, έχουν τεθεί εκτός λειτουργίας λόγω κυβερνοεπίθεσης. Περαιτέρω, σας ενημερώνουμε ότι καταβάλλεται κάθε δυνατή προσπάθεια για την όσο το δυνατόν ταχύτερη αποκατάσταση της ομαλής λειτουργίας των εν λόγω συστημάτων."*

Το παραπάνω κείμενο 45 λέξεων δεν αποτελεί απόσπασμα, είναι ολόκληρη η αρχική ανακοίνωση. Δύο ημέρες αργότερα, στις 12 Μαρτίου, αναρτήθηκε σε συνέχεια νεότερη ανακοίνωση[2] όπου μεταξύ άλλων αναφέρονται:

> *"Η ΕΛΛΗΝΙΚΗ ΕΤΑΙΡΕΙΑ ΤΟΠΙΚΗΣ ΑΝΑΠΤΥΞΗΣ ΚΑΙ ΑΥΤΟΔΙΟΙΚΗΣΗΣ Α.Ε. (ΕΕΤΑΑ ΑΕ) δέχτηκε κυβερνοεπίθεση στο διάστημα από 01/3/2025 έως 05/3/2025, οπότε και διαπιστώθηκε από τα αρμόδια στελέχη της Δ/νσης Πληροφορικής της Εταιρείας. Στο πλαίσιο αυτό, εξετάζεται το ενδεχόμενο να έχουν παραβιαστεί και προσωπικά δεδομένα ωφελούμενων των προγραμμάτων και των δράσεων που διαχειρίζεται η ΕΕΤΑΑ ΑΕ. (...)"*

Με βάση τα παραπάνω, προκύπτει ότι η πρώτη δημόσια ανακοίνωση του περιστατικού έγινε περίπου **μία εβδομάδα αργότερα**, καθιστώντας αυτό το χρονικό παράθυρο "ανοικτό" για τυχόν εκμετάλλευση από τρίτους εναντίον των θιγόμενων πολιτών.

1 https://www.eetaa.gr/nea-anakoinoseis/ektakti-anakoinosi-kyvernoepithesi-2/

2 https://www.eetaa.gr/nea-anakoinoseis/anakoinosi-schetika-me-tin-kyvernoepithesi/

Αντίθετα, στην ανακοίνωση αναφέρεται ότι εκ μέρους της ΕΕΤΑΑ ενημερώθηκαν αρμοδίως:

- Εντός 48 ωρών, οι Υπεύθυνοι Επεξεργασίας των σχετικών προγραμμάτων και δράσεων.
- Εντός 72 ωρών, η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (ΑΠΔΠΧ) και το Υπουργείο Εσωτερικών.
- "Άμεσα" (χωρίς ακριβή αναφορά χρόνου), η Εθνική Αρχή Κυβερνοασφάλειας (ΕΑΚ).

Συνεπώς, προκύπτει ότι η δημοσιοποίηση του περιστατικού έγινε πολύ αργότερα από την ενημέρωση των αρμόδιων φορέων, όπως η ΑΠΔΠΧ και η ΕΑΚ, χωρίς να προκύπτει κάποιος άμεσος λόγος για αυτή την καθυστέρηση.

Σημειώνεται ότι ούτε στην αρχική ανακοίνωση (10/3), ούτε και στην αμέσως επόμενη (12/3) αναφέρεται κάποιο συγκεκριμένο στοιχείο ως προς τα υποκείμενα (κατηγορίες πολιτών-αιτούμενων), το περιεχόμενο ή την έκταση του περιστατικού. Επιπλέον, εφόσον πρόκειται για περίπτωση άμεσης έκθεσης-υποκλοπής προσωπικών δεδομένων, αλλά ενδεχομένως και ευαίσθητων προσωπικών δεδομένων με έμμεσο τρόπο[3], τα υποκείμενα θα έπρεπε να ενημερωθούν στο συντομότερο δυνατό χρόνο προκειμένου να ληφθούν ανάλογα μέτρα προφύλαξης, στα οποία η ίδια η ΕΕΤΑΑ αναφέρεται πολύ αργότερα (11/4).

Η κρισιμότητα του περιστατικού, καθώς και η παραπάνω διαπίστωση περί ανάγκης άμεσης ενημέρωσης των πολιτών από την πρώτη στιγμή (κάτι που δεν έγινε), αναδείχθηκε πολύ αργότερα, όταν στις 23 Απριλίου το θέμα έγινε ευρύτερα γνωστό στο κοινό μέσω δημοσιευμάτων[4,5,6] και αφού προηγήθηκε απάντηση (ΕΕΤΑΑ, αρ. πρωτ. 10056/28-3-2025) σε σχετική επίκαιρη ερώτηση στη Βουλή (αρ.πρωτ. 4053/19-3/2025). Το πλήρες περιστατικό γνωστοποιήθηκε εκ μέρους της ΕΕΤΑΑ με νεότερη συμπληρωματική ανακοίνωση[7] στις 11 Απριλίου, όπου για πρώτη φορά αναφέρονται στοιχεία ως προς το περιεχόμενο της επίθεσης, τις κατηγορίες πολιτών-αιτούμενων που αφορούν και τις πιθανές συνέπειες ως αποτέλεσμα αυτής.

Σύμφωνα με τα παραπάνω στοιχεία, τα οποία ήρθαν στη δημοσιότητα περίπου **50 ημέρες μετά το περιστατικό**, προκύπτει ότι η επίθεση ήταν τύπου κρυπτογράφησης περιεχομένου (ransomware) και αφορά ως και **2,5 εκατομμύρια πολίτες**, συμπεριλαμβανομένων και *"...παιδιών σχολικής ηλικίας, εφήβων και ατόμων με αναπηρία.."*, συνεπώς συμπεριλαμβάνει και **ευαίσθητα** προσωπικά δεδομένα, σύμφωνα με το Γενικό Κανονισμό Προστασίας Δεδομένων (GDPR). Τα δεδομένα αυτά αντλήθηκαν από αιτήσεις δικαιούχων προς την ΕΕΤΑΑ τα τελευταία τουλάχιστον **10 χρόνια**, καθιστώντας το περιστατικό **μια από τις σοβαρότερες και μεγαλύτερης έκτασης επιθέσεις υποδομής στη χώρα τα τελευταία χρόνια**.

Από την αναλυτική απάντηση εκ μέρους της ΕΕΤΑΑ στις 28/3 επιβεβαιώνονται τα εξής:

- Πρόκειται για επίθεση τύπου κρυπτογράφησης περιεχομένου (ransomware).
- Στο περιεχόμενο περιλαμβάνονται και **ευαίσθητα** προσωπικά δεδομένα.

3 https://www.edpb.europa.eu/sme-data-protection-guide/data-protection-basics_el

4 https://www.newsbreak.gr/ellada/870325/chakers-eklepsan-afm-amka-mechri-kai-ta-ivan-politon-i-kyvernisi-omologise-tin-kyvernoepithesi-stin-eetaa/

5 https://www.alfavita.gr/koinonia/475682_kybernoepithesi-sok-stin-eetaa-dierreysan-prosopika-dedomena-25-ekat-goneon-kai

6 https://www.lawspot.gr/nomika-nea/paraviasi-dedomenon-stin-eetaa-enimerosi-apo-ypoyrgeio-koinonikis-synohis-kai-oikogeneias

7 https://www.eetaa.gr/nea-anakoinoseis/syblиromatiki-anakoinosi-gia-paraviasi-dedomenon-prosopikou-charaktira/

- Η παραβίαση έγινε σε **εσωτερική υποδομή**, όχι σε εξωτερική υπηρεσία (cloud), δηλαδή σε αποκλειστική νομική και τεχνική ευθύνη της ΕΕΤΑΑ.
- Από το Σάββατο 1/3 μέχρι και την Τετάρτη 5/3 *"...το περιστατικό βρισκόταν ακόμη σε εξέλιξη, χωρίς να είναι δυνατός ο περιορισμός του."* (σελ. 3).
- Λόγω της παραπάνω αδυναμίας, το σύστημα τέθηκε σκόπιμα και καθολικά εκτός λειτουργίας, με αποτέλεσμα να καταστεί **αδύνατη για μεγάλο διάστημα η διερεύνηση** τόσο της προέλευσης, όσο και της έκτασης της επίθεσης (σελ. 3).
- Η εσωτερική διερεύνηση κατέδειξε ότι η επίθεση πραγματοποιήθηκε μέσω παράνομης πρόσβασης σε εσωτερικό Σύστημα Διαχείρισης Βάσεων Δεδομένων (RDBMS), από όπου και **επεκτάθηκε** σε περαιτέρω διακομιστές (σελ. 4).
- Αναφέρεται ότι *"υπάρχει η δυνατότητα επαναφοράς και ανασύστασης των Βάσεων Δεδομένων που επλήγησαν"* (σελ. 4), όμως δεν εξηγείται το γιατί αυτό δεν κατέστη δυνατό να συμβεί για πολλές ημέρες μετά το περιστατικό. Συγκεκριμένα, στην ανακοίνωση της ΕΕΤΑΑ στις 12/3, αλλά και στην απάντηση στις 28/3, αναφέρει ότι *"...καταβάλει εργώδη προσπάθεια για την όσο το δυνατόν ταχύτερη αποκατάσταση της ομαλής λειτουργίας των πληροφοριακών της συστημάτων (...), το αργότερο έως 31 Μαρτίου 2025."* Συνεπώς, προκύπτει ότι **τρεις και πλέον εβδομάδες μετά το περιστατικό** τα εσωτερικά συστήματα δεν έχουν ακόμη επανέλθει πλήρως και αξιόπιστα.
- Η έκταση της επίθεσης εκτιμάται σε 700.000 αιτήσεις σε βάθος 10 ετών και ως και 2,5 εκατομμύρια υποκείμενα (θιγόμενους πολίτες). Επιβεβαιώνεται έτσι ότι πρόκειται για επιτυχημένη κυβερνοεπίθεση ιστορικών διαστάσεων για τη χώρα μας.
- Αναφέρεται (σελ. 7) ότι η ΕΕΤΑΑ έχει εκπονήσει την προβλεπόμενη από το νόμο Πολιτική Προστασίας Προσωπικών Δεδομένων, χωρίς όμως να εξηγεί τις παραπάνω παραλείψεις, καθυστερήσεις και αδυναμία άμεσης αντιμετώπισης του περιστατικού σύμφωνα με το εν λόγω σχέδιο δράσης, συνεπώς τη **μη ορθή εφαρμογή της**.
- Στο πλέγμα των *"οργανωτικών και τεχνικών μέτρων"* (σελ. 7) αναφέρονται μια σειρά μέτρα φυσικής προστασίας χώρων και εξοπλισμού, όχι όμως και τη συστηματική συντήρηση των εγκατεστημένων συστημάτων με ενημερώσεις ασφαλείας, από όπου κατά συντριπτική πλειοψηφία προέρχονται παρόμοιες επιθέσεις από τρίτους εκτός του χώρου. Συνεπώς, δεν είναι σαφές αν υπήρχε και εφαρμοζόταν κανονικά μια τέτοια πολιτική ή αν αντίθετα αυτός ήταν πιθανόν ο τρόπος πραγματοποίησης της επίθεσης (attack vector).
- Αναφέρονται η συνεργασία με συμβουλευτική εταιρία σε θέματα κυβερνοασφάλειας και η διενέργεια αξιολογήσεων ευαλωτότητας (vulnerability assessment), χωρίς όμως το πότε έγιναν, με τι περιεχόμενο, με τι αποτελέσματα και τι διορθωτικά μέτρα ελήφθησαν στη συνέχεια.
- Συγκεκριμένα, αναφέρεται ως παράδειγμα ένα *"πεπαλαιωμένο σύστημα"* (legacy platform) του οποίου *"...η ευαλωτότητα είχε διακριβωθεί μέσω των προαναφερθέντων ελέγχων"*. Όμως, δεν αναφέρεται ποια ακριβώς μέτρα ελήφθησαν και, κυρίως, αν και κατά πόσο αυτό έχει συνάφεια με το συγκεκριμένο περιστατικό παραβίασης.

- Αναφέρεται (σελ. 10) ως μέτρο ανάκαμψης η εγκατάσταση firewalls και malware protection *"σε κάθε εξυπηρετητή και σταθμό εργασίας"*, χωρίς να διευκρινίζεται αν κάτι τέτοιο προϋπήρχε και απέτυχε ή δεν υπήρχε καθόλου ως μέτρο. Και στις δύο περιπτώσεις, πρόκειται για τη σοβαρότερη ίσως αμέλεια που μπορεί να συμβεί σε τεχνικό επίπεδο σε σχέση με την προστασία της ασφάλειας εσωτερικών υποδομών.

Είναι χαρακτηριστικό ότι η ίδια η ΕΕΤΑΑ στην τρίτη κατά σειρά ανακοίνωσή της στις 11/4 αναφέρεται στα αποτελέσματα του περιστατικού και στις πιθανές συνέπειες για τους θιγόμενους πολίτες. Επιπλέον, αναφέρεται ότι *"...Είναι γεγονός ότι οι κυβερνοεπιθέσεις αλλά και οι εν γένει απειλές που συνδέονται με το ψηφιακό έγκλημα, αποτελούν μία δυσάρεστη αλλά αναπόδραστη πραγματικότητα, άρρηκτα συνδεδεμένη με τον σύγχρονο τρόπο ζωής."* Παρόλα αυτά, η ίδια η ΕΕΤΑΑ φαίνεται **απροετοίμαστη να αντιμετωπίσει εγκαίρως και αποφασιστικά τέτοιου είδους περιστατικά, παρότι σύμφωνα με την ίδια είναι αναμενόμενα**.

Σημειώνεται ότι η παράνομη απόκτηση πρόσβασης και γνωστοποίησης κρίσιμων προσωπικών δεδομένων, ακόμη και αν σε πρώτο στάδιο δεν χαρακτηρίζονται "ευαίσθητα" βάσει του ΓΚΠΔ, πιθανά οδηγεί σε **κλιμάκωση της πρόσβασης** σε αυτά μέσω "κλοπής ταυτότητας" (identity theft).

Για παράδειγμα, η απόκτηση ενός πλήρους συνόλου ατομικών δεδομένων όπως ΑΔΤ, ΑΦΜ, ΑΜΚΑ, διεύθυνση email, τραπεζικοί λογαριασμοί (IBAN), κτλ, είναι δυνατό να επιτρέψει την πρόσβαση σε άλλες ηλεκτρονικές πλατφόρμες από όπου θα αντληθούν ακόμη περισσότερα δεδομένα, όπως ιατρικά και φορολογικά, να υποβληθούν αιτήματα απόκτησης βεβαιώσεων και πιστοποιητικών, να πραγματοποιηθούν τραπεζικές συναλλαγές, κ.ο.κ.

Είναι πραγματικά λυπηρό να αναγκαζόμαστε ως Ένωση Πληροφορικών Ελλάδας (ΕΠΕ), ξανά και ξανά, **περίπου μία φορά κάθε λίγες εβδομάδες**, να αναφερόμαστε σε ανάλογα περιστατικά και να επισημαίνουμε τα προφανή.

Όπως αναφέρει και η ίδια η ΕΕΤΑΑ, δεν πρόκειται για κάποια μακρινή πιθανότητα αλλά για τη σύγχρονη πραγματικότητα. Περιστατικά κυβερνοεπιθέσεων σε κρατικές υποδομές και πληροφοριακά συστήματα δεν είναι κάτι που ίσως κάποτε συμβεί, είναι **βέβαιο** ότι θα συμβεί και πρόκειται απλά για ζήτημα χρόνου. Αποδεικνύεται ότι, παρά τις εξαγγελίες, τις δικές μας προειδοποιήσεις και τα πραγματικά αποτελέσματα, οι αρμόδιοι φορείς φαίνεται να θεωρούν το συγκεκριμένο ζήτημα της προστασίας των δεδομένων των πολιτών μάλλον εξαιρετικά χαμηλής προτεραιότητας. Σε αντίθετη περίπτωση, πρόκειται για αποδεδειγμένη και επαναλαμβανόμενη **ανεπάρκεια της αντίληψης της κρισιμότητας του ζητήματος** και της ανάλογης οργάνωσης των δημόσιων υποδομών σε επίπεδο τεχνικό και προσωπικού.

Ως ο πλέον αρμόδιος επιστημονικός και επαγγελματικός φορέας του κλάδου, είμαστε υποχρεωμένοι να συνεχίσουμε να επισημαίνουμε τα προφανή, δυστυχώς πολύ τακτικότερα από όσο επιθυμούμε με αφορμή μία ακόμη επιτυχημένη κυβερνοεπίθεση και μαζική διαρροή προσωπικών δεδομένων πολιτών.

Καλούμε τα συναρμόδια υπουργεία, ιδιαιτέρως το Υπουργείο Ψηφιακής Διακυβέρνησης, καθώς και κάθε φορέα του ευρύτερου Δημοσίου με κατά το νόμο ευθύνη προστασίας των δεδομένων των πολιτών, να εφαρμόσουν τα προβλεπόμενα και να διασφαλίσουν τα δικαιώματα όλων μας. Όπως πάντα, είμαστε στη διάθεσή τους για οποιαδήποτε συνδρομή.

Το Διοικητικό Συμβούλιο
της Ένωσης Πληροφορικών Ελλάδας

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