

Ενημέρωση σχετικά με περιστατικό ασφάλειας πληροφοριακών συστημάτων

Στο πλαίσιο της υπεύθυνης και διαφανούς ενημέρωσης των πελατών (πρώην, υφιστάμενων και δυνητικών) και χρηστών των υπηρεσιών μας, η ΕΦΑ ΕΝΕΡΓΕΙΑΚΗ ΕΤΑΙΡΙΑ ΦΥΣΙΚΟΥ ΑΕΡΙΟΥ ΜΟΝΟΠΡΟΣΩΠΗ Α.Ε. («ΕΦΑ») σας ενημερώνει σχετικά με περιστατικό κυβερνοασφάλειας που επηρέασε πληροφοριακή υποδομή στην οποία φιλοξενούνταν η ιστοσελίδα της Εταιρείας και η ηλεκτρονική πλατφόρμα MyEFA.

Το περιστατικό

Σύμφωνα με τα αποτελέσματα της τεχνικής διερεύνησης που πραγματοποιήθηκε μετά τον εντοπισμό του περιστατικού, διαπιστώθηκε κακόβουλη δραστηριότητα στον επηρεαζόμενο διακομιστή κατά το χρονικό διάστημα από 30 Απριλίου 2026 έως και 8 Μαΐου 2026.

Ειδικότερα, στις 30 Απριλίου 2026 και ώρα 16:28 καταγράφηκε η πρώτη επιβεβαιωμένη εκμετάλλευση ευπάθειας ασφαλείας του λογισμικού διαχείρισης του διακομιστή από μη εξουσιοδοτημένο τρίτο, μέσω της οποίας κατέστη δυνατή η απόκτηση αυξημένων δικαιωμάτων πρόσβασης (root access). Η τελευταία διαπιστωμένη κακόβουλη δραστηριότητα καταγράφηκε στις 8 Μαΐου 2026 και ώρα 23:24.

Κατά την τεχνική διερεύνηση εντοπίστηκαν, μεταξύ άλλων, επανειλημμένες μη εξουσιοδοτημένες προσβάσεις με αυξημένα δικαιώματα, αλλαγές στοιχείων πρόσβασης, δημιουργία μη εξουσιοδοτημένων λογαριασμών, απομακρυσμένη εκτέλεση εντολών και δημιουργία κακόβουλων αρχείων (webshells) και μηχανισμών διατήρησης της μη εξουσιοδοτημένης πρόσβασης στον επηρεαζόμενο διακομιστή.

Η ΕΦΑ έλαβε γνώση της ύπαρξης του προβλήματος στις 4 Μαΐου 2026, κατόπιν δυσλειτουργίας και μη διαθεσιμότητας της ιστοσελίδας και της πλατφόρμας MyEFA. Ακολούθησε, σε συνεργασία με τους τεχνικούς συνεργάτες της Εταιρείας, διερεύνηση του περιστατικού και λήψη μέτρων περιορισμού και αποκατάστασης.

Στο πλαίσιο αυτό, πραγματοποιήθηκε εξειδικευμένη τεχνική διερεύνηση, κατά την οποία αναλύθηκαν τα διαθέσιμα τεχνικά στοιχεία και αρχεία καταγραφής, με σκοπό, μεταξύ άλλων, τον προσδιορισμό της μεθόδου παραβίασης, της έκτασης του περιστατικού και της τυχόν εξαγωγής δεδομένων.

Λόγω του επιπέδου της μη εξουσιοδοτημένης πρόσβασης, δεν μπορεί να αποκλειστεί το ενδεχόμενο πρόσβασης σε προσωπικά δεδομένα που βρίσκονταν στην επηρεαζόμενη υποδομή. Ωστόσο, από την τεχνική διερεύνηση δεν προέκυψαν ενδείξεις μαζικής εξαγωγής δεδομένων ούτε ενδείξεις σημαντικής μεταφοράς αρχείων ή πρόσβασης στους αποθηκευμένους λογαριασμούς πελατών. Λόγω των περιορισμών των διαθέσιμων τεχνικών καταγραφών, το

ενδεχόμενο μη εξουσιοδοτημένης πρόσβασης σε προσωπικά δεδομένα δεν μπορεί να αποκλειστεί πλήρως.

Προσωπικά δεδομένα που ενδέχεται να έχουν επηρεαστεί

Το περιστατικό ενδέχεται να αφορά υφιστάμενους και πρώην πελάτες της ΕΦΑ, υφιστάμενους πελάτες που ήταν παράλληλα εγγεγραμμένοι χρήστες της ηλεκτρονικής πλατφόρμας MyEFA, καθώς και δυνητικούς πελάτες που είχαν καταχωρίσει τα στοιχεία τους μέσω της ιστοσελίδας της Εταιρείας.

Οι κατηγορίες προσωπικών δεδομένων που ενδέχεται να έχουν επηρεαστεί διαφοροποιούνται ανάλογα με την κατηγορία στην οποία ανήκει κάθε πρόσωπο και ειδικότερα περιλαμβάνουν:

- **Για τους υφιστάμενους και πρώην πελάτες:** προσωπικά δεδομένα που περιλαμβάνονται στους λογαριασμούς φυσικού αερίου (ΛΦΑ), οι οποίοι ήταν αποθηκευμένοι σε μορφή PDF στην επηρεαζόμενη υποδομή.
- **Για τους υφιστάμενους πελάτες που ήταν παράλληλα χρήστες της πλατφόρμας MyEFA** όνομα, επώνυμο, διεύθυνση ηλεκτρονικού ταχυδρομείου (email), Αριθμός Φορολογικού Μητρώου (ΑΦΜ), αριθμός παροχής (ΗΚΑΣΠ), όνομα χρήστη, κωδικός πρόσβασης σε προστατευμένη μορφή, καθώς και προσωπικά δεδομένα που περιλαμβάνονται στους λογαριασμούς φυσικού αερίου σε μορφή PDF.
- **Για τους δυνητικούς πελάτες:** ονοματεπώνυμο, αριθμός τηλεφώνου και διεύθυνση ηλεκτρονικού ταχυδρομείου (email).

Περαιτέρω, μέσω του αριθμού παροχής, κατά την εκάστοτε προβολή της εφαρμογής MyEFA αντλούνται μέσω API πληροφορίες που αφορούν τον εκάστοτε πελάτη, όπως διεύθυνση, πληροφορίες επικοινωνίας, υπόλοιπο λογαριασμών, συναλλαγές και ιστορικό λογαριασμών. Οι πληροφορίες αυτές δεν αποθηκεύονται στην πλατφόρμα MyEFA, αλλά αντλούνται μέσω API κατά την εκάστοτε προβολή τους στην εφαρμογή.

Επισημαίνεται ότι στοιχεία καρτών πληρωμών και IBAN δεν αποθηκεύονται στην πλατφόρμα MyEFA. Οι κωδικοί πρόσβασης των χρηστών αποθηκεύονται σε προστατευμένη μορφή με τη χρήση πρόσθετου μηχανισμού ασφαλείας (salt) και δεν είναι απευθείας ανακτήσιμοι από τη βάση δεδομένων.

Ενέργειες για την αντιμετώπιση του περιστατικού

Μετά τον εντοπισμό του περιστατικού, η ΕΦΑ προχώρησε άμεσα, σε συνεργασία με εξειδικευμένους τεχνικούς συνεργάτες, στη λήψη μέτρων για τον περιορισμό και την αντιμετώπισή του και στην απομόνωση της επηρεαζόμενης πληροφοριακής υποδομής.

Παράλληλα, πραγματοποιήθηκε εξειδικευμένη τεχνική διερεύνηση του περιστατικού, στο πλαίσιο της οποίας εξετάστηκαν τα διαθέσιμα αρχεία καταγραφής και λοιπά τεχνικά στοιχεία του επηρεαζόμενου διακομιστή, με σκοπό τον προσδιορισμό του τρόπου και της έκτασης της παραβίασης, τον εντοπισμό τυχόν μη εξουσιοδοτημένης παρουσίας στο σύστημα και τη διερεύνηση ενδεχόμενης εξαγωγής δεδομένων.

Περαιτέρω, ελήφθησαν και δρομολογήθηκαν πρόσθετα μέτρα ενίσχυσης της ασφάλειας της πληροφοριακής υποδομής, ιδίως ως προς τον περιορισμό των προνομιακών δικαιωμάτων πρόσβασης, την ενίσχυση των μηχανισμών αυθεντικοποίησης και ελέγχου πρόσβασης, την προστασία του διακομιστή από κακόβουλες ενέργειες και τη βελτίωση της παρακολούθησης και καταγραφής συμβάντων ασφαλείας.

Η ΕΦΑ συνεχίζει να παρακολουθεί την ασφάλεια των συστημάτων της και να εφαρμόζει τα αναγκαία τεχνικά και οργανωτικά μέτρα για την ενίσχυση της προστασίας της πληροφοριακής της υποδομής και τον περιορισμό του κινδύνου επανάληψης αντίστοιχου περιστατικού.

Το περιστατικό γνωστοποιήθηκε στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, σύμφωνα με τις προβλέψεις του Γενικού Κανονισμού για την Προστασία Δεδομένων.

Πιθανές συνέπειες για τα επηρεαζόμενα πρόσωπα

Με βάση τα μέχρι σήμερα διαθέσιμα στοιχεία της τεχνικής διερεύνησης, δεν έχει επιβεβαιωθεί εξαγωγή ή κακόβουλη χρήση προσωπικών δεδομένων. Ωστόσο, δεδομένου ότι δεν μπορεί να αποκλειστεί πλήρως το ενδεχόμενο μη εξουσιοδοτημένης πρόσβασης σε προσωπικά δεδομένα που βρίσκονταν στην επηρεαζόμενη υποδομή, υφίσταται ενδεχόμενος κίνδυνος τα δεδομένα αυτά να χρησιμοποιηθούν για στοχευμένες απόπειρες εξαπάτησης ή ηλεκτρονικής απάτης (phishing).

Ειδικότερα, ένας μη εξουσιοδοτημένος τρίτος θα μπορούσε να επιχειρήσει να αξιοποιήσει πληροφορίες που αφορούν τη σχέση του πελάτη με την ΕΦΑ, προκειμένου να καταστήσει μία παραπλανητική επικοινωνία περισσότερο πειστική και να επιχειρήσει να αποσπάσει πρόσθετα προσωπικά στοιχεία, κωδικούς πρόσβασης ή οικονομικές πληροφορίες.

Για τον λόγο αυτό, συνιστάται αυξημένη προσοχή σε τυχόν ύποπτα μηνύματα ηλεκτρονικού ταχυδρομείου, SMS ή τηλεφωνικές επικοινωνίες που εμφανίζονται ως προερχόμενες από την ΕΦΑ ή άλλο σχετικό φορέα και ζητούν την παροχή προσωπικών, οικονομικών ή άλλων εμπιστευτικών πληροφοριών.

Τι συνιστούμε να κάνετε

Για προληπτικούς λόγους, συνιστούμε στους δυνητικούς, υφιστάμενους και πρώην πελάτες και χρήστες της διαδικτυακής ιστοσελίδας της πλατφόρμας MyEFA να επιδεικνύουν αυξημένη προσοχή σε τυχόν μηνύματα ηλεκτρονικού ταχυδρομείου (email), SMS ή τηλεφωνικές

επικοινωνίες που εμφανίζονται ως προερχόμενες από την ΕΦΑ ή άλλο σχετικό φορέα και ιδίως όταν μέσω αυτών ζητείται η γνωστοποίηση προσωπικών ή οικονομικών στοιχείων ή κωδικών πρόσβασης.

Ειδικότερα, συνιστάται:

- να ελέγχετε προσεκτικά την ταυτότητα και τη διεύθυνση του αποστολέα πριν ανταποκριθείτε σε οποιαδήποτε επικοινωνία,
- να μην ακολουθείτε συνδέσμους και να μην ανοίγετε συνημμένα αρχεία που περιλαμβάνονται σε ύποπτα ή μη αναμενόμενα μηνύματα,
- να μη γνωστοποιείτε μέσω email, SMS ή τηλεφώνου κωδικούς πρόσβασης ή άλλα εμπιστευτικά στοιχεία κατόπιν σχετικού αιτήματος,
- να είστε ιδιαίτερα επιφυλακτικοί απέναντι σε επικοινωνίες που επικαλούνται στοιχεία της σχέσης σας με την ΕΦΑ προκειμένου να εμφανιστούν ως αυθεντικές,
- να χρησιμοποιείτε ισχυρούς και διαφορετικούς κωδικούς πρόσβασης για κάθε ηλεκτρονική υπηρεσία και, εφόσον χρησιμοποιείτε τον ίδιο κωδικό πρόσβασης του MyEFA και σε άλλες υπηρεσίες, να προβείτε προληπτικά στην αλλαγή του,
- σε περίπτωση που διαπιστώσετε ύποπτη επικοινωνία ή δραστηριότητα που φαίνεται να σχετίζεται με την ΕΦΑ ή τα στοιχεία σας, να μην ανταποκριθείτε σε αυτήν και να επικοινωνήσετε με την ΕΦΑ μέσω των επίσημων διαύλων επικοινωνίας της.

Η ΕΦΑ θα συνεχίσει να παρακολουθεί την εξέλιξη του περιστατικού και, εφόσον προκύψουν νεότερα στοιχεία που απαιτούν τη λήψη πρόσθετων μέτρων από τους επηρεαζόμενους, θα προβεί σε σχετική ενημέρωση.

Επισημαίνεται ότι η ΕΦΑ πρόκειται να συγχωνευθεί με τη Metlen Energy & Metals ΜΟΝΟΠΡΟΣΩΠΗ Α.Ε., με την ολοκλήρωση της σχετικής διαδικασίας να αναμένεται εντός του Σεπτεμβρίου 2026.

Για οποιαδήποτε ερώτηση σχετικά με το παρόν περιστατικό ή την προστασία των προσωπικών σας δεδομένων, έως την ολοκλήρωση της συγχώνευσης, μπορείτε να επικοινωνείτε με τον Υπεύθυνο Προστασίας Δεδομένων (DPO) της ΕΦΑ (Δικηγορική Εταιρεία ΖΑΧΟΣ Δ.-ΠΑΠΑΜΙΜΙΚΟΣ Α. & ΣΥΝΕΡΓΑΤΕΣ) στην ηλεκτρονική διεύθυνση gdpr@efaenergy.gr.

Μετά την ολοκλήρωση της συγχώνευσης, για οποιοδήποτε ζήτημα αφορά την προστασία των προσωπικών σας δεδομένων, καθώς και για πληροφορίες ή διευκρινίσεις σχετικά με το παρόν περιστατικό, μπορείτε να απευθύνεστε στον Υπεύθυνο Προστασίας Δεδομένων (DPO) της METLEN Energy & Metals A.E. στην ηλεκτρονική διεύθυνση DPO@metlen.com.

Για περισσότερες πληροφορίες σχετικά με τη συγχώνευση και τις σχετικές εταιρικές μεταβολές, μπορείτε να ανατρέξετε στον ακόλουθο σύνδεσμο <https://www.protergia.gr/eksuphrethsh-pelatwn/suxnes-erwthseis-efa-energy>.