ΕΝΗΜΕΡΩΣΗ ΣΧΕΤΙΚΑ ΜΕ ΠΕΡΙΣΤΑΤΙΚΟ ΠΑΡΑΒΙΑΣΗΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Ενημέρωση σχετικά με κακόβουλη ενέργεια (διαδικτυακή επίθεση) στις 29/8/2024.

Ο σκοπός της παρούσας ενημέρωσης είναι να παρουσιάσει τα δεδομένα που ενδέχεται να διέρρευσαν στο σκοτεινό διαδίκτυο και να σας υποδείξει τα μέτρα που μπορείτε να λάβετε για να προστατευτείτε από τυχόν κακόβουλες ενέργειες τρίτων, οι οποίοι δύναται να επιδιώξουν να εκμεταλλευτούν τα προσωπικά σας δεδομένα για παράνομους ή επιζήμιους σκοπούς.

Η ενημέρωση των φυσικών προσώπων που ενδέχεται να επηρεάστηκαν από το συμβάν πραγματοποιείται αυτή τη χρονική στιγμή, διότι έπρεπε να προηγηθεί έρευνα για την αιτία που προκάλεσε το περιστατικό παραβίασης και άμεσες ενέργειες τόσο για την αντιμετώπισή του όσο και για τον περιορισμό των συνεπειών του, ενέργειες οι οποίες απαιτούσαν υψηλό φόρτο επεξεργασίας και αρκετό χρόνο. Ωστόσο αξίζει να σημειωθεί ότι όλα τα φυσικά πρόσωπα που επικοινώνησαν άμεσα με την Εταιρία σχετικά με τη λήψη του κακόβουλου email ενημερώθηκαν άμεσα για το περιστατικό και τους δόθηκαν οδηγίες για την αντιμετώπισή του. Η παρούσα ενημέρωση αφορά όσους χρήστες έλαβαν το κακόβουλο email και δεν επικοινώνησαν άμεσα με την Εταιρία (δεδομένου ότι είναι πρακτικά αδύνατον να γνωρίζουμε σε ποιους συγκεκριμένα στάλθηκε το κακόβουλο μήνυμα).

Η εταιρεία εφάρμοσε όλα τα απαραίτητα τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλίσει όσο το δυνατόν περισσότερο τον περιορισμό των συνεπειών της παραβίασης.

Δεν απαιτείται καμία ενέργεια από την πλευρά των φυσικών προσώπων σε συνέχεια αυτής της ενημέρωσης.

Τι συνέβη;

Η εταιρεία Megalab Α.Ε., και συγκεκριμένα πλήθος εσωτερικών και εξωτερικών χρηστών, έλαβε στις 29-8-2024 μήνυμα ηλεκτρονικού ταχυδρομείου, το οποίο φέρεται να ξεκίνησε από πιστοποιημένη εσωτερική ηλεκτρονική διεύθυνση «ag.anargiri@megalab.info».

Εντός του περιεχομένου του μηνύματος, υπήρχε σύνδεσμος (link) μέσω του οποίου οι παραλήπτες «καλούνται» να συνδεθούν στην πλατφόρμα αποθήκευσης αρχείων στο σύννεφο Dropbox, ώστε να λάβουν ένα αρχείο. Ο εν λόγω σύνδεσμος διαμοιράστηκε από AWS (amazon web services) υπηρεσίες και

δεν έχει καμία σχέση με τη Dropbox. Πρόκειται για μία κακόβουλη και μαζική διαδικτυακή επίθεση, η οποία είχε στόχο -με πρόσχημα το διαμοιρασμό αρχείου- να υποκλέψει αναγνωριστικά εισόδου χρηστών (username & password).

Κατηγορίες προσωπικών δεδομένων που παραβιάστηκαν και μπορεί να διέρρευσαν

Τα προσωπικά δεδομένα που παραβιάστηκαν είναι οι Διευθύνσεις Ηλεκτρονικού Ταχυδρομείου των παραληπτών του κακόβουλου email. Δεδομένα που ενδεχομένως διέρρευσαν είναι τα αναγνωριστικά εισόδου των χρηστών (username & password).

Ενέργειες που έγιναν προς αντιμετώπισή του περιστατικού

Στο πλαίσιο της αντιμετώπισης της πρόσφατης κυβερνοεπίθεσης, οι αρμόδιες υπηρεσίες της εταιρείας έλαβαν άμεσα και αποφασιστικά μέτρα για την αντιμετώπισή της και την άμεση αποκατάσταση των πληροφοριακών συστημάτων που επηρεάστηκαν.

Τα μέτρα αυτά περιλαμβάνουν τεχνικές παρεμβάσεις που πραγματοποιήθηκαν με σκοπό την ενίσχυση της ασφάλειας των πληροφοριακών συστημάτων της εταιρείας έναντι μελλοντικών κυβερνοαπειλών.

Επιπλέον πραγματοποιήθηκε αναπροσαρμογή υφιστάμενων διαδικασιών για την καλύτερη διαχείριση και πρόληψη αντίστοιχων περιστατικών.

Επίσης,, ενισχύθηκε η συνεργασία με εξειδικευμένους εξωτερικούς φορείς και εταιρείες κυβερνοασφάλειας για την παροχή συμβουλευτικών υπηρεσιών και την ενίσχυση της προστασίας των δεδομένων.

Τέλος, η Εταιρία γνωστοποίησε το περιστατικό στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.

Ποιες είναι οι ενδεχόμενες συνέπειες της διαρροής για εσάς;

Καταρχάς οφείλουμε να σας ενημερώσουμε ότι δεν μας έχει αναφερθεί κάποια ανεπιθύμητη συνέπεια από τους παραλήπτες του κακόβουλου email που επικοινώνησαν με την Εταιρία. Στην απευκταία περίπτωση που διέρρευσαν τα αναγνωριστικά εισόδου της διεύθυνσης ηλεκτρονικού ταχυδρομείου σας, οι ενδεχόμενοι κίνδυνοι είναι οι εξής:

Κίνδυνος Απάτης και Κακόβουλης Χρήσης: Οι διαρροές δεδομένων μπορούν να οδηγήσουν σε απάτες και κακόβουλη χρήση των προσωπικών πληροφοριών από επιτήδειους ή εγκληματίες.

Παραβίαση της Ιδιωτικής Ζωής: Οι διαρροές δεδομένων μπορούν να οδηγήσουν σε σοβαρή παραβίαση της ιδιωτικής ζωής, καθώς προσωπικές πληροφορίες μπορεί να διαρρεύσουν σε μη εξουσιοδοτημένα άτομα ή φορείς.

Κίνδυνος Ψευδούς Ταυτοποίησης: Οι διαρροές δεδομένων μπορούν να οδηγήσουν σε πιθανή ιδιοποίηση ταυτότητας από κακόβουλους δράστες, οι οποίοι δύνανται να χρησιμοποιήσουν ευαίσθητες πληροφορίες που έχουν διαρρεύσει, όπως ΑΦΜ, ΑΔΤ και ΑΜΚΑ για την πραγματοποίηση παράνομων ενεργειών.

Ποια είναι τα μέτρα που μπορείτε να λάβετε για να προστατευτείτε

Ιδιαίτερη προσοχή σε πιθανές απάτες: Θα πρέπει να είστε προσεκτικοί σε πιθανές απάτες που μπορεί να σχετίζονται με τη χρήση των προσωπικών σας δεδομένων και να αναφέρετε άμεσα οποιαδήποτε ύποπτη δραστηριότητα.

Ιδιαίτερη προσοχή στις αιτήσεις ταυτοποίησης: Θα πρέπει να εξετάζετε προσεκτικά κάθε αίτηση ταυτοποίησης που γίνεται στο όνομά σας και να επιβεβαιώνετε την εγκυρότητά της πριν παραχωρήσετε οποιαδήποτε προσωπική πληροφορία.

Ιδιαίτερη προσοχή σε επιθέσεις κοινωνικής μηχανικής (social engineering): Μην παρέχετε προσωπικά στοιχεία μέσω τηλεφώνου ή email, ακόμα κι αν το αίτημα φαίνεται να προέρχεται από αξιόπιστους φορείς, όπως τράπεζες. Πάντα να επιβεβαιώνετε την ταυτότητα του αιτούντος φορέα μέσω των επίσημων καναλιών επικοινωνίας του. Η Εταιρία, όπως και οι τράπεζες, δεν θα ζητήσει ποτέ το συνθηματικό πρόσβασης σε υπηρεσίες μέσω email ή τηλεφώνου.

Παρακολούθηση των λογαριασμών σας (ηλεκτρονικό ταχυδρομείο, κοινωνικά δίκτυα) για πιθανές ύποπτες προσβάσεις. **Συνιστάται η αλλαγή του κωδικού εισόδου στο λογαριασμό σας.**

Λήψη μέτρων προστασίας από ανεπιθύμητες τηλεφωνικές κλήσεις: Σε περίπτωση που αρχίσετε να λαμβάνετε ανεπιθύμητες εμπορικές κλήσεις, εξετάστε την πιθανότητα εγγραφής σας μέσω των σχετικών νόμιμων διαδικασιών στο μητρώο του άρθρου 11 παρ. 2 Ν. 3471/2006.

Ζητούμε συγνώμη για τυχόν αναστάτωση που μπορεί να σας προκάλεσε το εν λόγω περιστατικό. Σας ευχαριστούμε για την κατανόησή σας και τη συνεργασία σας καθ' όλη τη διάρκεια αυτής της διαδικασίας.

Εκ της Διοικήσεως της εταιρείας,

Γεώργιος Δημοτσάντος

4 Σεπτεμβρίου 2024