ΕΞΑΙΡΕΤΙΚΑ ΕΠΕΙΓΟΝ

Ενημέρωση για κλιμάκωση επιθέσεων ransomware

Κατόπιν ενημέρωσης από το Τμήμα Κυβερνοασφάλειας του Υπουργείου Εσωτερικών σχετικά με την **ιδιαίτερα ανησυχητική κλιμάκωση των επιθέσεων ransomware** (λυτρισμικού), που επισημαίνει η Εθνική Υπηρεσία Πληροφοριών το τελευταίο χρονικό διάστημα, εφιστούμε την προσοχή όλων των υπαλλήλων και παρακαλούμε για αυξημένη επαγρύπνηση.

Το ransomware είναι μια μορφή κακόβουλου λογισμικού (malware) που έχει σχεδιαστεί για να κρυπτογραφεί αρχεία από μια συσκευή, καθιστώντας τα αρχεία, καθώς και τα συστήματα που βασίζονται σε αυτά, μη προσβάσιμα. Οι κακόβουλοι δράστες στη συνέχεια απαιτούν λύτρα (συνήθως σε κρυπτονομίσματα) προκειμένου να δοθεί το κλειδί αποκρυπτογράφησης και να αποκατασταθεί η πρόσβαση στα δεδομένα.

Με την πάροδο του χρόνου, οι κακόβουλοι δράστες έχουν προσαρμόσει τις τακτικές τους ώστε να είναι πιο καταστροφικές και επιβλαβείς. Συχνά προβαίνουν και σε εξαγωγή (exfiltration) δεδομένων των θυμάτων, ώστε να τα πιέσουν να πληρώσουν, απειλώντας ότι θα δημοσιοποιήσουν τα κλεμμένα δεδομένα.

Μπορούν να προσδιοριστούν διάφοροι τύποι ransomware, ανάλογα με τα δεδομένα που στοχεύουν: ορισμένοι τύποι κρυπτογραφούν αρχεία, άλλοι κλειδώνουν την οθόνη του χρήστη, ενώ πιο εξελιγμένες μορφές επεμβαίνουν στα αρχεία που χρησιμοποιούνται για την εκκίνηση των συστημάτων, εμποδίζοντας την εκκίνησή τους. Υπάρχουν επίσης εκδόσεις που στοχεύουν servers και εταιρικά δίκτυα, καθώς και ransomware που πλήττει φορητές συσκευές μέσω κακόβουλων εφαρμογών. Κοινός στόχος όλων είναι η απαίτηση λύτρων για την αποκατάσταση της πρόσβασης.

Το ransomware μπορεί να κατεβεί σε έναν υπολογιστή ανοίγοντας ένα συνημμένο ηλεκτρονικού ταχυδρομείου, κάνοντας κλικ σε μια διαφήμιση, πατώντας ένα σύνδεσμο ή ακόμα και όταν επισκεπτόμαστε έναν ιστότοπο που έχει ενσωματωμένο κακόβουλο λογισμικό.

> **Για το λόγο αυτό, πρέπει να είστε ιδιαίτερα προσεκτικοί κατά την πλοήγησή σας στο διαδίκτυο και όταν λαμβάνετε ύποπτα μηνύματα ηλεκτρονικού ταχυδρομείου** από αποστολέα άγνωστο σε εσάς, από αποστολέα του οποίου ο λογαριασμός προσομοιάζει οπτικά με αυθεντικό ή από αποστολέα από χώρα προέλευσης στην οποία δεν έχετε επαφές.

Συστάσεις για την προστασία σας

Κρατήστε το λειτουργικό σύστημα και τα λογισμικά ενημερωμένα.

Χρησιμοποιήστε αξιόπιστο, ενεργό και ενημερωμένο antivirus.

Μην χρησιμοποιείτε πειρατικό λογισμικό.

Δημιουργήστε συχνά αντίγραφα ασφαλείας (backups).

Διατηρήστε τα backup εκτός σύνδεσης (offline).

Να είστε προσεκτικοί με ύποπτα email και συνδέσμους. Μην ακολουθείτε συνδέσμους (links) ή διευθύνσεις (URLs) και μην ανοίγετε επισυναπτόμενα αρχεία που λαμβάνετε μέσω email ή εφαρμογές αν δεν προέρχονται από έμπιστους αποστολείς ή αν δεν είστε σίγουροι για την ασφάλεια του περιεχομένου τους.

Χρησιμοποιήστε ισχυρούς, μοναδικούς κωδικούς για κάθε λογαριασμό ή εφαρμογή.

Όπου είναι εφικτό, χρησιμοποιήστε πολυπαραγοντικό έλεγχο ταυτότητας, διότι θωρακίζει την ασφάλεια πρόσβασης απαιτώντας ένα επιπλέον επίπεδο επαλήθευσης.

Μην γνωστοποιείτε στοιχεία πρόσβασης και κωδικούς σε τρίτους.

Μισαρίδης Θανάσης
Προϊστάμενος
Γενική Διεύθυνση Ψηφιακής Λειτουργίας
Περιφέρεια Νοτίου Αιγαίου