29 / 6 / 2022

Η Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων μας ενημέρωσε για τα παρακάτω:

1. Σας γνωρίζουμε ότι παρατηρείται έξαρση κακόβουλων επιθέσεων τύπου Ransomware (λυτρισμικό), κατά τις οποίες οι κακόβουλοι υποκλέπτουν και κρυπτογραφούν τα αρχεία του οργανισμού στα οποία αποκτούν πρόσβαση και στη συνέχεια ζητούν λύτρα για να μην τα διαρρεύσουν.

*2. Τονίζεται η ανάγκη τήρησης αντιγράφων ασφαλείας (backup) των κρίσιμων αρχείων και των εξυπηρετητών (servers) **εκτός δικτύου** (**offline backup**) ως το αποτελεσματικότερο μέτρο ανάκαμψης από επιθέσεις τύπου ransomware. Σε περίπτωση που δεν τηρείτε offline backups των κρίσιμων συστημάτων σας, υπάρχει ισχυρή σύσταση να προβείτε σε αυτό.*

3. Προτεινόμενα μέτρα επαύξησης προστασίας:

α. Τήρηση backup των συστημάτων εκτός δικτύου και ύπαρξη στρατηγικής αποκατάστασής τους.

β. Έλεγχος των security logs της περιμέτρου για ασυνήθιστες ενέργειες όπως πολλαπλές αποτυχημένες προσπάθειες σύνδεσης, συνδέσεις σε ports που δε σχετίζονται με την τυπική ροή δεδομένων, δραστηριότητα σάρωσης ή απαρίθμησης ports και ασυνήθιστη δραστηριότητα σε λογαριασμούς επαυξημένων δικαιωμάτων (privileged).

γ. Διατήρηση αρχείων καταγραφής δραστηριότητας των συσκευών δικτύου.

δ. Ενημέρωση των λογισμικών που χρησιμοποιούνται με τις τελευταίες εκδόσεις.

ε. Προετοιμασία σχεδίου αποκατάστασης με συγκεκριμένους ρόλους.

στ. Χρήση ενημερωμένου λογισμικού προστασίας από ιούς.

ζ. Αποφυγή ανοίγματος άγνωστων αρχείων ή πρόσβασης σε άγνωστους συνδέσμους παρά μόνο αφού ελεγχθούν προσεκτικά (scan) από λογισμικά προστασίας από ιούς.

η. Να επιτρέπεται η εγκατάσταση μόνο εγκεκριμένων εφαρμογών.

θ. Περιορισμός των προσωπικών συσκευών ώστε να μην έχουν πρόσβαση σε υπηρεσιακά δίκτυα όπου δεν είναι απαραίτητο.

ι. Χρήση λογαριασμών χρηστών με περιορισμένα δικαιώματα κι όχι δικαιώματα διαχειριστή.

ια. Αποφυγή χρήσης προσωπικών εφαρμογών και ιστοσελίδων (email, chat, μέσα κοινωνικής δικτύωσης) από υπηρεσιακούς υπολογιστές.

ιβ. Ενημέρωση των χρηστών για τους κινδύνους που ελλοχεύουν και τις καλές πρακτικές.

4. Σε περίπτωση που ο οργανισμός σας έχει μολυνθεί, προτείνονται οι παρακάτω ενέργειες:

α. Προσδιορισμός και άμεση απομόνωση των συστημάτων που έχουν μολυνθεί. Συγκεκριμένα:

(1) Αποσύνδεση δικτύου μολυσμένων συστημάτων και υποδικτύων.

(2) Στην περίπτωση που δεν είναι εφικτή η αποσύνδεση υποδικτύων, επιβάλλεται όπως η απενεργοποίηση του δικτύου να γίνει σε επίπεδο κεντρικού switch.

(3) Στην περίπτωση που δεν μπορεί να απομονωθεί το ιδιο το δίκτυο, η απομόνωση μπορεί να γίνει με αποσύνδεση των Ethernet καλωδίων ή των Wi-Fi συνδέσεων των μολυσμένων μηχανημάτων.

β. Καταγραφή της έκτασης της μόλυνσης, με προσεκτικό έλεγχο του δικτύου, shared folders, για τυχόν επέκταση της μόλυνσης.

γ. Φωτογράφιση « ransomware note».

δ. Λήψη αντιγράφου μνήμης μολυσμένων σταθμών εργασίας και αντίστοιχων δίσκων .

ε. Αλλαγή κωδικών των online λογαριασμών, αφού απομονωθεί η μόλυνση.

στ. Αποφυγή επικοινωνίας με συνεργαζόμενους φορείς με χρήση του προσβεβλημένου συστήματος (π.χ. mail) για αποφυγή επέκτασης της μόλυνσης. Χρησιμοποιείστε άλλα κανάλια επικοινωνίας (π.χ. τηλέφωνο).

ζ. Άμεση αναφορά του συμβάντος στην Ομάδα Αντιμετώπισης Ηλεκτρονικών Επιθέσεων - ΕΘΝΙΚΟ CERT για τεχνική αρωγή.

5. Μπορείτε να βρείτε πληροφορίες για βέλτιστες πρακτικές και στο Εγχειρίδιο Κυβερνοασφάλειας στον παρακάτω σύνδεσμο:
hxxps://mindigital[.]gr/wp-content/uploads/2021/06/Εγχειρίδιο-Κυβερνοασφάλειας.pdf

Η υπηρεσία μας παραμένει στη διάθεσή σας για κάθε περαιτέρω διευκρίνιση / πληροφορία που αφορά τα παραπάνω θέματα.

Email επικοινωνίας: ICTsupport@justice.gov.gr