Οι επιθέσεις τύπου ransomware είναι ένας τύπος επιθέσεων όπου οι επιτιθέμενοι αποκτούν πρόσβαση στο πληροφοριακό σύστημα και κρυπτογραφούν τα αρχεία/δεδομένα που βρίσκουν εκεί. Στη συνέχεια, τα θύματα ενημερώνονται μέσω μηνύματος για την καταβολή λύτρων και οδηγίες αποπληρωμής τους. Εάν δεν καταβληθούν τα λύτρα, υπάρχει η απειλή να πωληθούν ή να διαρρεύσουν τα δεδομένα, σε ιστοσελίδες που ελέγχονται από τους επιτιθέμενους.

Προτεινόμενες οδηγίες για την αυστηρή τήρηση των κάτωθι από τους χρήστες:

Α) Διαπιστευτήρια (username/ password)

Αλλαγή κωδικού πρόσβασης ανά τακτά χρονικά διαστήματα (σχετικές οδηγίες στο **Παράρτημα Ι**).

- Μη γνωστοποίηση κωδικού (password) σε τρίτους. Σε διαφορετική περίπτωση, θα πρέπει να γίνει άμεση αλλαγή αυτού.
- Μη τοποθέτηση διαπιστευτηρίων σε εμφανές ή προσβάσιμο από τρίτους, σημείο.

Β) Υπηρεσιακά έγγραφα:

- Αποθήκευση, υπηρεσιακών εγγράφων σε κεντρικούς κοινόχρηστους φακέλους του φορέα, όπου υφίστανται, για τους οποίους θα λαμβάνονται σε καθημερινή βάση, offline αντίγραφα ασφαλείας.
- Τήρηση εφεδρικών αντιγράφων ασφαλείας (σε CD, DVD, εξωτερικό δίσκο), εγγράφων, που αποθηκεύονται στους σταθμούς εργασίας, με ευθύνη των χρηστών τους.

Γ) Εξωτερικές συσκευές:

Έλεγχος συσκευών για ιούς σύμφωνα με τις οδηγίες του **Παραρτήματος ΙΙ**, πριν την χρήση τους και αναφορά τυχόν ευρημάτων στους Υπεύθυνους Συστημάτων του φορέα σας.

Δ) Διαδίκτυο/ ηλεκτρονικό ταχυδρομείο:

- Χρήση διαδικτύου/ ηλεκτρονικού ταχυδρομείου μόνο για υπηρεσιακούς λόγους.
- Αποφυγή ανοίγματος ηλεκτρονικών μηνυμάτων, url και επισυναπτόμενων αρχείων από άγνωστους αποστολείς, καθώς υπάρχει κίνδυνος υποκλοπής στοιχείων ή μόλυνσης του δικτύου Η/Υ με ιό.
- Αποφυγή χρήσης μέσων κοινωνικής δικτύωσης (π.χ. facebook, twitter κ.α.) εκτός και αν υπάρχουν αποδεδειγμένες υπηρεσιακές ανάγκες.
- Αποφυγή χρήσης υπηρεσιών άμεσων μηνυμάτων (Instant messaging).

Ε) Ενημέρωση λογισμικών σταθμών εργασίας με τις τελευταίες εκδόσεις (σχετικές οδηγίες στο **Παράρτημα ΙΙΙ**).

ΣΤ) Λοιπά:

- Αναφορά στους Υπεύθυνους Συστημάτων του φορέα σας, τυχών δυσλειτουργιών, παραβιάσεων ή μη-εξουσιοδοτημένης χρήσης του σταθμού εργασίας και του ηλεκτρονικού ταχυδρομείου.
- Κλείδωμα (Ctrl+Alt+Del → Κλείδωμα) των σταθμών εργασίας, όταν απομακρύνονται οι χρήστες από το γραφείο τους.
- Κλείσιμο (shut down) των σταθμών εργασίας, όταν οι χρήστες αποχωρούν από την εργασία τους.
- Μεταφόρτωση (download), εγκατάσταση ή εκτέλεση επιπρόσθετων προγραμμάτων στους σταθμούς εργασίας, μετά από ενημέρωση και συναίνεση με τους Υπεύθυνους Συστημάτων του φορέα σας.
- Αποφυγή εγκατάστασης και χρήσης λογισμικών απομακρυσμένης πρόσβασης, για την εξ αποστάσεως διαχείριση/ χρήση/ υποστήριξη συστατικών του δικτύου Η/Υ, από τρίτους.

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

Email επικοινωνίας: ICTsupport@justice.gov.gr