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.

Για την προστασία του φορέα σας προτείνονται τα παρακάτω:

1. Τήρηση backup των συστημάτων εκτός δικτύου και ύπαρξη δοκιμασμένης μεθόδου αποκατάστασής του.
2. Ενημέρωση των λογισμικών που χρησιμοποιούνται με τις τελευταίες εκδόσεις.
3. Τήρηση ενημερωμένης λίστας εξωτερικών και εσωτερικών επαφών σε περίπτωση ανάγκης.
4. Ύπαρξη σχεδίου αποκατάστασης με συγκεκριμένους ρόλους και στρατηγική.
5. Περιορισμός των προσωπικών συσκευών ώστε να μην έχουν πρόσβαση σε υπηρεσιακά δίκτυα όπου δεν είναι απαραίτητο.
6. Χρήση λογαριασμών χρηστών με περιορισμένα δικαιώματα κι όχι δικαιώματα διαχειριστή.
7. Αποφυγή χρήσης προσωπικών εφαρμογών και ιστοσελίδων (email, chat, μέσα κοινωνικής δικτύωσης) από υπηρεσιακούς υπολογιστές.
8. Ενημέρωση των χρηστών για τους κινδύνους που ελλοχεύουν και τις καλές πρακτικές.

Ενδεικτικές πηγές πληροφόρησης για μέτρα προστασίας και προετοιμασίας από επιθέσεις τύπου ransomware:

- https://www.cisa.gov/ransomware-guides-and-services
- https://csrc.nist.gov/Projects/ransomware-protection-and-response
- https://www.bleepingcomputer.com/news/security/cisa-fbi-share-guidance-for-victims-of-kaseya-ransomware-attack/
- https://www.enisa.europa.eu/publications/ransomware
- https://www.trendmicro.com/en_gb/what-is/ransomware/ransomware-attack.html