



ΕΤΕΚ: Συμβουλές προστασίας από κυβερνοεπιθέσεις

Το Επιστημονικό Τεχνικό Επιμελητήριο (ΕΤΕΚ) παρέχει συμβουλές για προστασία από κυβερνοεπιθέσεις, ενόψει της αλματώδους αύξησης που παρουσιάζει ο αριθμός των κυβερνοεπιθέσεων. Το Επιμελητήριο συμβουλεύει όπως χρησιμοποιείται ισχυρός κωδικός πρόσβασης με τουλάχιστον 8 χαρακτήρες που να περιλαμβάνει κεφαλαία γράμματα (Α-Ζ), πεζά γράμματα (α-ζ), αριθμούς (0-9) και σύμβολα (!, #, \$, κ.λπ.), αποφεύγεται η χρήση του ίδιου κωδικού για πρόσβαση σε διαφορετικές υπηρεσίες, αλλαγή κωδικού πρόσβασης για κάθε υπηρεσία σε τακτά χρονικά διαστήματα (τουλάχιστον μια φορά ανά 3 μήνες), αποφυγή ενεργοποίησης απομνημόνευσης του κωδικού πρόσβασης κατά τη χρήση προγραμμάτων πλοήγησης, αποφυγή μοιράσματος κωδικού πρόσβασης, όπου είναι εφικτό, να γίνεται ενεργοποίηση ελέγχου ταυτότητας δύο παραγόντων (2-factor authentication). Δηλαδή, να γίνεται χρήση διαφορετικών μορφών αναγνώρισης για πρόσβαση σε μια υπηρεσία. Π.χ., πέραν του κωδικού πρόσβασης να απαιτείται και παραλαβή επιπλέον κωδικού μέσω sms, ή άλλης εφαρμογής authenticator.

Επίσης εισηγείται να μην ανοίγονται αρχεία τα οποία επισυνάπτονται σε ηλεκτρο-

νικά μηνύματα που έχουν σταλεί, αν δεν επιβεβαιωθεί προηγουμένως ότι προέρχονται από αποστολέα της εμπιστοσύνης του χρήστη, να αποφεύγεται το άνοιγμα άγνωστων αρχείων, μηνυμάτων ή συνδέσμων, να μην απαντώνται ηλεκτρονικά μηνύματα που ζητούν ευαίσθητες πληροφορίες, όπως για παράδειγμα αριθμούς λογαριασμών, ταυτότητας, πιστωτικής κάρτας, ή κωδικούς πρόσβασης, να αποφεύγεται πλοήγηση σε ιστοσελίδες που δεν είναι γνωστές, ή συνδέσμους σε email, sms, διαφημίσεις και άλλες εφαρμογές, να κατεβάζονται εφαρμογές σε φορητές συσκευές από επίσημα καταστήματα και όχι από προγράμματα περιήγησης, να τηρούνται συχνά εφεδρικά αντίγραφα όλων των σημαντικών σας εγγράφων/αρχείων, είτε σε φυσικά εξωτερικά μέσα αποθήκευσης (usb sticks, εξωτερικοί σκληροί δίσκοι, κ.τ.λ.) είτε σε υπηρεσίες νέφους εμπιστοσύνης.

Επιπλέον συστήνει όπως σε περίπτωση αντιγράφων σε φυσικά μέσα αποθήκευσης, να τηρούνται τα μέσα αυτά σε ασφαλισμένο χώρο και για επιπλέον προστασία των αντιγράφων ασφαλείας, να διατηρούνται επιπρόσθετα αντίγραφα σε άλλη τοποθεσία, ή/και σε διαφορετικό μέσο.