

CYBERSECURITY – TIPS

8 ΒΑΣΙΚΟΙ ΚΑΙ ΑΠΑΡΑΙΤΗΤΟΙ ΤΡΟΠΟΙ ΓΙΑ ΝΑ ΠΡΟΣΤΑΤΕΨΕΤΕ ΤΗΝ ΕΠΙΧΕΙΡΗΣΗ ΣΑΣ

**Είστε έτοιμοι να ενισχύσετε την
ασφάλεια της επιχείρησής σας;**

Με περισσότερα από **25** χρόνια εμπειρίας, και γραφεία σε **ΗΠΑ και Ευρώπη**, η εξειδικευμένη ομάδα της EMPIST σχεδιάζει, και υλοποιεί λύσεις **τεχνολογίας**, για τους πελάτες της για πελάτες στους τομείς των **Μεταφορών & Logistics**, της **Ναυτιλίας**, της **Παραγωγής & Μεταποίησης**, της **Υγείας**, των **Οικονομικών** και **Συμβουλευτικών Υπηρεσιών**, των **ΜΚΟ** και άλλων κλάδων.

Οι κυβερνοαπειλές εξελίσσονται διαρκώς, θέτοντας σε κίνδυνο τόσο την ασφάλεια, όσο και τη λειτουργία των επιχειρήσεων. Ωστόσο, με τη σωστή προετοιμασία και τις κατάλληλες λύσεις, μπορείτε να προστατεύσετε κατάλληλα τα δεδομένα σας. Η ασφαλής και αδιάλειπτη πρόσβαση στις πληροφορίες, σε συνδυασμό με προηγμένες τεχνολογικές λύσεις, αποτελεί βασικό πυλώνα για τη σταθερότητα, την ανάπτυξη και την επιτυχία κάθε επιχείρησης.

Δείτε πώς μπορούμε να σας βοηθήσουμε στο empist.com

Για μια ολοκληρωμένη λύση ασφάλειας στο **cybersecurity**, ο οργανισμός σας μπορεί να μας **EMPISTευτεί**

1. Ενεργοποίηση του Multi-Factor Authentication (MFA)

Οι κωδικοί πρόσβασης δεν επαρκούν για την ασφάλειά σας στο σύγχρονο κυβερνοχώρο. Ενεργοποιήστε MFA σε όλους τους επαγγελματικούς και προσωπικούς σας λογαριασμούς για μεγαλύτερη προστασία.

2. Αναβάθμιση της τεχνολογίας

Η παρωχημένη τεχνολογία αυξάνει τα τρωτά σημεία. Επενδύστε σε ενημερωμένα συστήματα, λογισμικό και εξοπλισμό και ενισχύστε την ασφάλεια της επιχείρησής σας.

3. Εγκατάσταση Password Manager

Οι περίπλοκοι κωδικοί είναι απαραίτητοι, αλλά δύσχρηστοι και δύσκολοι στην απομνημόνευσή τους. Γι' αυτό, προτείνουμε τη χρήση προγράμματος διαχείρισης κωδικών.

4. Ξεκινήστε Security Awareness Training

Το 98% των κυβερνοεπιθέσεων περιλαμβάνουν social engineering. Για την αποφυγή τους λοιπόν κρίνεται απαραίτητη όχι μόνο η χρήση κατάλληλης τεχνολογίας, αλλά και η εκπαίδευση των χρηστών. Ενημερώστε και εκπαιδεύστε την ομάδα σας τακτικά για τις νέες απειλές.

5. Δημιουργήστε ένα δικό σας Σχέδιο Ανάκτησης (Recovery plan)

Η διακοπή της επιχειρησιακής λειτουργίας μπορεί να έχει σοβαρό κόστος. Διασφαλίστε την ετοιμότητα της ομάδας σας με ένα αποτελεσματικό σχέδιο ανάκτησης. Εξασφαλίστε την ετοιμότητα της ομάδας σας με ένα εφαρμόσιμο σχέδιο ανάκτησης.

6. Προστατεύστε τις προσωπικές πληροφορίες σας

Μην μοιράζετε τα προσωπικά σας στοιχεία. Όσο περισσότερες πληροφορίες είναι άμεσα διαθέσιμες για εσάς και τους υπαλλήλους σας, τόσο περισσότεροι οι κίνδυνοι να αξιοποιηθούν σε επίθεση κατά της επιχείρησής σας.

7. Back Up

Διασφαλίστε την προστασία των δεδομένων και των λειτουργιών της επιχείρησής σας με ένα αξιόπιστο σύστημα αντιγράφων ασφαλείας. Η σωστή στρατηγική backup είναι το κλειδί για την ταχεία ανάκτηση δεδομένων σε περίπτωση κυβερνοεπίθεσης.

8. Επένδυση στην προληπτική ασφάλεια

Τα antivirus βασίζονται σε γνωστά μοτίβα και δεν αρκούν για προστασία. Επενδύστε σε σύγχρονες λύσεις όπως το EDR (Endpoint Detection & Response) και το MDR (Managed Detection & Response), που βασίζονται στην πρόληψη και προσφέρουν πιο ολοκληρωμένες λύσεις προστασίας.

