#ασφάλεια_πληροφοριών_ &_βιομηχανική_κατασκοπία

όταν κάθε επιχείρηση βάλλεται ηλεκτρονικά

Η ΑΣΦΑΛΗΣ ΠΛΟΗΓΗΣΗ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΕΙΝΑΙ ΥΠΟΘΕΣΗ ΟΛΩΝ ΜΑΣ

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Εσωτερικών και Διοικητικής Ανασυγκρότησης

ΑΡΧΗΓΕΙΟ ΕΛΛΗΝΙΚΗΣ ΑΣΤΥΝΟΜΙΑΣ

CYBER CRIME DIVISION
ΔΙΩΞΗ ΗΛΕΚ/ΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

Ο πολύτιμος δεκάλογος της επιχείρησής σας

Antivirus - Antimalware

Θα πρέπει να υπάρχει πρόγραμμα προστασίας από ιούς (Antivirus) και πρόγραμμα προστασίας από κακόβουλο λογισμικό (Antimalware), ενημερωμένα για όλες τις τρέχουσες απειλές.

Firewall

Με τη χρήση του firewall, μπορείτε να παρακολουθείτε και να εντοπίζετε τυχόν ασυνήθιστη συμπεριφορά ενός επιμέρους προγράμματος. Το firewall αποτελεί την καρδιά τής πολιτικής ασφαλείας, γιατί φιλτράρει την κίνηση του δικτύου της επιχείρησης.

Intrusion Prevention System

Το Σύστημα Ελέγχου Επιθέσεων (Intrusion Prevention System) ψάχνει για ιούς, αλλά και παρακολουθεί τα συστήματά σας για οποιαδήποτε ασυνήθιστη δραστηριότητα.

Χρήστες

Πολιτική πρόσβασης χρηστών στο δίκτυο της επιχείρησης. Έλεγχος της πρόσβασης των χρηστών στο δίκτυο της επιχείρησης μέσω:
Authentication: Αυθεντικοποίηση των χρηστών Επιβεβαίωση της ταυτότητας των χρηστών.
Authorization: Καθορισμός επιτρεπόμενων ενεργειών για κάθε χρήστη.
Accounting: Δημιουργία αρχείου ενεργειών για κάθε χρήστη (τι ενέργειες έκανε και πότε).

Απομακρυσμένη πρόσβαση χρηστών. Οποιοσδήποτε χρήστης θα πρέπει να συνδέεται στο δίκτυό σας μέσω κατάλληλου Εικονικού Ιδιωτικού Δικτύου **(Virtual Private Network-VPN)** με τα ακολουθούμενα επίπεδα ασφαλείας.

Εκπαίδευση χρηστών, ώστε όλοι οι χρήστες να καταλαβαίνουν τη σπουδαιότητα της πιστής εφαρμογής των κανόνων ασφαλείας. Κάποιοι κανόνες ασφαλείας, ενδεικτικά, μπορεί να είναι: να σβήνουν τον υπολογιστή πριν την απομάκρυνση από το γραφείο τους και να χρησιμοποιούν ισχυρούς κωδικούς ασφαλείας (passwords). Επιπλέον, το σύστημα δεν θα πρέπει να επιτρέπει σε έναν χρήστη να έχει πρόσβαση στο δίκτυο αν δεν έχει χρησιμοποιήσει ισχυρό password.
Έλεγχος των αδειών χρήσης λογισμικού. Οι χρήστες δεν θα πρέπει να κατεβάζουν οποιοδήποτε λογισμικό κατά βούληση, γιατί μπορεί να θέσουν σε κίνδυνο το δίκτυο της επιχείρησής σας.
Εφαρμογή πολιτικής πρόσβασης των χρηστών και στο έντυπο υλικό της επιχείρησης.
Εφαρμογή κυρώσεων σε όποιον χρήστη δεν εφαρμόζει την πολιτική ασφαλείας της επιχείρησης.

Πολιτική ασφαλείας στις χρησιμοποιούμενες συσκευές

Διαμόρφωση κρίσιμων συσκευών ώστε να μην υποστηρίζουν τη χρήση φορητών συσκευών μεταφοράς δεδομένων, π.χ. USB.
Μην επιτρέπετε σε άτομα εκτός επιχείρησης, όπως επισκέπτες, να συνδέονται στο δίκτυο της επιχείρησής σας. Σε αντίθετη περίπτωση, θα πρέπει να ακολουθούν το δικό σας επίπεδο ασφαλείας. Θα πρέπει, δηλαδή, να γίνεται έλεγχος της πρόσβασης στο δίκτυο από φορητές ασύρματες συσκευές, όπως κινητά τηλέφωνα ή ταμπλέτες (tablets) κ.λπ.
Χρήση λογισμικού Data Loss Prevention (DLP) για την αποφυγή περιπτώσεων διαρροής κρίσιμων δεδομένων της επιχείρησης.

Περιορισμός της έκτασης πρόσβασης

Θα πρέπει να υπάρχουν δικλίδες ασφαλείας, ώστε, αν κάποιος εισβολέας καταφέρει να εισχωρήσει σε κάποιο τμήμα του δικτύου σας, να μην μπορεί αυτομάτως να εισχωρήσει και σε όλο το δίκτυο.

Γνώση των αδυναμιών του δικτύου σας

Δεν υπάρχει το τέλειο σύστημα ασφαλείας, γι' αυτό θα πρέπει ο υπεύθυνος ασφαλείας της επιχείρησης να γνωρίζει τα τρωτά σημεία του και τις περιοχές που παρουσιάζουν τον μεγαλύτερο κίνδυνο, και να απαγορεύεται η πρόσβαση σ' αυτές.

Κατοχύρωση Διπλωμάτων Ευρεσιτεχνίας

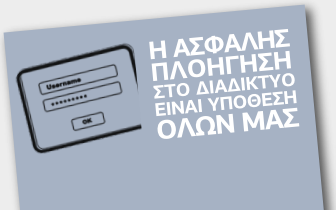
Διασφάλιση των κρίσιμων δεδομένων της επιχείρησης με Διπλώματα Ευρεσιτεχνίας, όπου είναι εφικτό.

Παρακολούθηση του φυσικού χώρου της επιχείρησής σας με χρήση καμερών ασφαλείας

Εκτίμηση του κόστους

Θα πρέπει να δίνεται ιδιαίτερη σημασία στην εκτίμηση του κόστους για την ασφάλεια της επιχείρησης και να συνυπολογίζεται στον προϋπολογισμό της επιχείρησης, αφού είναι κρίσιμο στοιχείο για την υπόστασή της.

Αν πέσετε θύμα βιομηχανικής κατασκοπίας, ενημερώστε αμέσως την Υπηρεσία μας, καλώντας στο τηλέφωνο 11188 ή μέσω e-mail **ccu@cybercrimeunit.gov.gr.**



#ασφάλεια_πληροφοριών_ &_βιομηχανική_ κατασκοπία

όταν κάθε επιχείρηση βάλλεται ηλεκτρονικά

Ορισμός. Με τον όρο βιομηχανική κατασκοπία, σε επίπεδο επιχειρήσεων, εννοούμε τη **συλλογή πολύτιμων δεδομένων εταιρειών είτε από άλλες εταιρείες που αποσκοπούν στη βελτίωση των συγκριτικών πλεονεκτημάτων τους, είτε από ιδιώτες-hackers.**

Bold Ogilvy & Mather

ΕΠΙΚΟΙΝΩΝΙΑ

Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος - Cyber Crime Division
Λ. Αλεξάνδρας 173, Αμπελόκηποι, Αθήνα, Τ.Κ. 11521
e-mail: ccu@cybercrimeunit.gov.gr, Τηλ.: 11188, Fax: 2106476462

Βρείτε μας στα:

www.cyberkid.gr

www.facebook.com/cyberkid.gov.gr

www.cyberalert.gr

www.facebook.com/CyberAlertGR

twitter.com/cyberalertgr