Συμβουλές ασφαλείας για επιχειρήσεις/οργανισμούς:

- Είναι σημαντικό να έχουμε **ξεκάθαρες πολιτικές** για την πρόσβαση σε εταιρικές δομές, καθώς και το ποιος θα πρέπει να κληθεί σε περίπτωση περιστατικού.
- Δημιουργούμε **διαδικασίες διαχείρισης περιστατικών** ασφαλείας.
- Χρησιμοποιούμε επιπλέον μέτρα όταν πρόκειται για **έγκριση και υπογραφή εγγράφων** από τους προϊσταμένους της επιχείρησης / οργανισμού.
- Παίρνουμε μέτρα, όπως **κρυπτογράφηση σκληρών δίσκων, προστασία ιδιωτικότητας οθόνης** από τρίτους, ισχυρή αυθεντικοποίηση και έλεγχος των φορητών μέσων αποθήκευσης.

- Διατηρούμε το **λογισμικό ενημερωμένο,** συμπεριλαμβανομένου του φυλλομετρητή ιστοσελίδων (browser), του προγραμμάτος antivirus / antimalware και του λειτουργικού συστήματος.
- **Δημιουργούμε διαδικασίες** εξ αποστάσεως απενεργοποίησης πρόσβασης σε συσκευές που χάθηκαν ή κλάπηκαν και διαγραφής του περιεχομένου τους.
- Διασφαλίζουμε ότι οι **υπάλληλοί μας είναι ενημερωμένοι και σωστά εκπαιδευμένοι** σε θέματα κυβερνοασφάλειας.
- Εφαρμόζουμε **εσωτερικές διαδικασίες** σχετικά με τη διενέργεια πληρωμών.

- **Ελέγχουμε τις πληροφορίες** που αναρτώνται στην ιστοσελίδα της επιχείρησης / οργανισμού μας, περιορίζουμε τις πληροφορίες και επιδεικνύουμε **ιδιαίτερη προσοχή** σχετικά με τις πληροφορίες στα μέσα κοινωνικής δικτύωσης. Δεν παραλείπουμε κανένα βήμα και **δεν υποκύπτουμε σε πιέσεις.**
- Λαμβάνουμε τακτικά **αντίγραφα ασφαλείας** τα οποία διατηρούμε σε ασφαλές σημείο και όχι διαρκώς συνδεδεμένα στα πληροφοριακά συστήματα.
- Εφαρμόζουμε διαδικασία για την **επαλήθευση της νομιμότητας αιτημάτων** διενέργειας πληρωμών που λαμβάνονται μέσω e-mail.
- Δεν ξεχνάμε και την **φυσική ασφάλεια** (προστασία προσωπικού, εγκαταστάσεων, εξοπλισμού και πόρων).

CYBER CRIME DIVISION
ΔΙΩΞΗ ΗΛΕΚ/ΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

Η ΑΣΦΑΛΗΣ ΠΛΟΗΓΗΣΗ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΕΙΝΑΙ ΥΠΟΘΕΣΗ ΟΛΩΝ ΜΑΣ

CYBER ALERT
ΔΙΩΞΗ ΗΛΕΚ/ΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ
111 88

Για περισσότερες πληροφορίες :

ΕΠΙΚΟΙΝΩΝΙΑ

Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος – Cyber Crime Division
Λ. Αλεξάνδρας 173, Αμπελόκηποι, Αθήνα, Τ.Κ. 11522
e-mail: **ccu@cybercrimeunit.gov.gr**, Τηλ.: **11188**

Υποδιεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος Βορείου Ελλάδας
Μοναστηρίου 326, Θεσσαλονίκη, Τ.Κ. 54121
e-mail: **ydheve@cybercrimeunit.gov.gr**, Τηλ.: **11188**

Ενημερωθείτε για θέματα ασφαλούς πλοήγησης στο Διαδίκτυο στο **cyberkid.gov.gr** και στο **www.cyberalert.gr**

Cyberkid.gov.gr
CyberAlertGR
Cyberalert.gr
CyberAlertGR
Cyber Alert

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Προστασίας του Πολίτη

ΕΛΑΣ Επόμενο Βήμα

Αρχηγείο Ελληνικής Αστυνομίας

CYBER ALERT
ΔΙΩΞΗ ΗΛΕΚ/ΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ
111 88

#ασφαλής_επιχείρηση / οργανισμός_στο_διαδίκτυο

Προστατεύουμε την επιχείρηση/τον οργανισμό μας στο Διαδίκτυο

Προστατεύουμε την επιχείρηση / οργανισμό μας στο Διαδίκτυο!

Το εύρος ευκαιριών που επιδιώκουν να εκμεταλλευτούν οι εγκληματίες του κυβερνοχώρου είναι εντυπωσιακό. Οι σημαντικότερες τάσεις είναι οι ακόλουθες:

- **Μόλυνση πληροφοριακών συστημάτων** με λογισμικό τύπου ransomware, για κρυπτογράφηση αρχείων και απαίτηση πληρωμής «λύτρων».
- **Εκμετάλλευση ευπαθειών συστημάτων** και εφαρμογών για την εγκατάσταση και διασπορά κακόβουλου λογισμικού, το οποίο κατά περίπτωση οδηγεί σε:
  - **υποκλοπή διαπιστευτηρίων χρηστών** (username & password).
  - **υποκλοπή δεδομένων καρτών** πληρωμών και λογαριασμών web banking.
  - **διαρροή δεδομένων προσωπικού χαρακτήρα.**
  - **διαρροή εμπιστευτικών / απόρρητων** πληροφοριών.

- Επιθέσεις με **χρήση δικτύων συσκευών** που έχουν μολυνθεί με κακόβουλο λογισμικό εν αγνοία των χρηστών τους (botnets).
- **Παράνομη νομιμοποίηση εσόδων** παραδοσιακών ή εικονικών νομισμάτων.
- **Απάτες με τη μέθοδο του ενδιάμεσου** (man-in-the middle) παρεμβαίνοντας σε τμήματα επικοινωνίας μεταξύ συναλλασσόμενων επιχειρήσεων / οργανισμών και πείθοντας τους υπαλλήλους να καταθέσουν χρήματα σε άλλους τραπεζικούς λογαριασμούς.
- **Απάτες με εταιρικό e-mail**, στις οποίες ένας εξουσιοδοτημένος υπάλληλος εξαπατάται προκειμένου να εξοφλήσει ένα πλαστό τιμολόγιο ή να πραγματοποιήσει μια μη εγκεκριμένη μεταφορά πίστωσης από τον εταιρικό λογαριασμό της επιχείρησης.
- **Εξαπάτηση εργαζομένων**, προμηθευτών και πελατών με την αξιοποίηση τεχνικών κοινωνικής μηχανικής (social engineering).

Συμβουλές για επιχειρήσεις ηλεκτρονικού εμπορίου:

Προετοιμάζουμε την επιχείρησή μας!

- **Κατοχυρώνουμε** το εμπορικό σήμα και το λογότυπο της επιχείρησής μας.
- **Επενδύουμε** σε μια πλατφόρμα ηλεκτρονικού εμπορίου υψηλής ποιότητας.
- Γνωρίζουμε αυτό που πουλάμε. **Επιλέγουμε** αξιόπιστη μέθοδο αποστολής των προϊόντων μας και μέθοδο λήψης πληρωμών.
- Για να πουλήσουμε αγαθά ή υπηρεσίες διαδικτυακά, θα πρέπει να έχουμε **συμφωνία με πιστωτικό ίδρυμα** που εκκαθαρίζει τις πληρωμές (acquirer).

Ορίζουμε τις άμυνές μας

- Συζητάμε τις επιλογές μας με το πιστωτικό ίδρυμα (acquirer): **διατηρούμε ενημερωμένο το λογισμικό μας**, χρησιμοποιούμε ισχυρούς κωδικούς πρόσβασης και εγκαθιστούμε τείχος προστασίας και λογισμικό προστασίας από κακόβουλο λογισμικό.
- **Χρησιμοποιούμε διαθέσιμα εργαλεία** για τη διαχείριση της δραστηριότητας των πελατών μας, για να προσδιορίσουμε εάν είναι γνήσιοι ή όχι.
- **Ενημερωνόμαστε** για τις τάσεις απατών στην περιοχή μας.
- Βεβαιωνόμαστε ότι η επιχείρησή μας **συμμορφώνεται με την ισχύουσα νομοθεσία** για την επεξεργασία δεδομένων προσωπικού χαρακτήρα.
- Βεβαιωνόμαστε ότι διαθέτουμε **σχέδιο διαχείρισης συμβάντων** και άμεσης ανάκαμψης από μια επίθεση, υιοθετώντας τεχνικά και οργανωτικά μέτρα.
- Συλλέγουμε και **αναλύουμε πληροφορίες** από ανοιχτές πηγές του διαδικτύου σχετιζόμενες με την επιχείρηση /οργανισμό μας.
- **Εκπαιδεύουμε – ενημερώνουμε** το προσωπικό σε θέματα κυβερνοασφάλειας.
- Ορίζουμε **υπεύθυνους πληροφοριακών συστημάτων** / ομάδες αντιμετώπισης περιστατικών ασφαλείας.

Πραγματοποιούμε συναλλαγές με ασφάλεια

- Ενημερωνόμαστε για τα **πρωτόκολλα ασφαλείας 3D Secure** για ασφαλείς πληρωμές.
- Επαληθεύουμε τη **γνησιότητα των πελατών μας.**
- Εάν συναντήσουμε οποιαδήποτε παράνομη δραστηριότητα, **επικοινωνούμε με την Αστυνομία.**

Ενέργειες σε περίπτωση κυβερνοεπίθεσης:

- Άμεση **ενημέρωση αρμόδιων Αρχών** και στελεχών Οργανισμού.
- **Περιορισμός επιπλέον ζημίας.**
- **Συλλογή και διαφύλαξη** σχετικών αποδεικτικών στοιχείων.
- **Αποφυγή αλλοίωσης** των δεδομένων κατά τη συλλογή.
- Λήψη αντιγράφων των αρχείων καταγραφής του συστήματος ή / και των λογισμικών διαχείρισης δεδομένων.
- Σημαντικό να αποδεικνύεται η **αντικειμενικότητα, η λογική αλληλουχία και η ακεραιότητα** των αποδεικτικών στοιχείων.
- Απαραίτητη η **λεπτομερής παρουσίαση** της διαδικασίας απόκτησης των στοιχείων αυτών, επιδεικνύοντας όλες τις διεργασίες μέσω των οποίων αυτά αποκτήθηκαν.

Συμβουλές ασφαλείας στον κυβερνοχώρο για εργαζομένους:

- **Αποφεύγουμε να κάνουμε χρήση των εταιρικών συσκευών για ιδιωτικές δραστηριότητες.**
- **Χρησιμοποιούμε συσκευές και λογισμικό που παρέχονται από την επιχείρηση / οργανισμό για να έχουμε πρόσβαση σε δεδομένα της επιχείρησης / οργανισμού.**
- **Χρησιμοποιούμε ισχυρούς κωδικούς πρόσβασης (εάν είναι εφικτό password managers ή two-step verification).**
- **Συνδεόμαστε με το εταιρικό δίκτυο μόνο μέσω εταιρικού VPN.**
- **Δεν επιτρέπουμε σε μέλη της οικογένειάς μας να αποκτούν πρόσβαση στον εταιρικό εξοπλισμό. Ασφαλίζουμε το οικιακό μας δίκτυο.**
- **Αν εντοπίσουμε ασυνήθιστη ή ύποπτη δραστηριότητα σε οποιαδήποτε συσκευή χρησιμοποιούμε για την εξ αποστάσεως εργασία, επικοινωνούμε άμεσα με την εταιρεία μας μέσω των ενδεδειγμένων καναλιών.**
- **Εφαρμόζουμε αυστηρά τις υφιστάμενες διαδικασίες ασφαλείας σχετικά με τη διενέργεια πληρωμών.**
- Καθορίζουμε **μοναδικά σημεία επικοινωνίας** με επιχειρήσεις στις οποίες πραγματοποιούμε πληρωμές ανά τακτά χρονικά διαστήματα.
- Χρησιμοποιούμε τη **μέθοδο SLAM** για να αποτρέψουμε επιθέσεις ηλεκτρονικού ψαρέματος (phishing): 1) Sender: Ελέγχουμε τη διεύθυνση (email) του αποστολέα, 2) Links: Τοποθετούμε το δείκτη του ποντικιού και ελέγχουμε αν υπάρχουν σύνδεσμοι πριν κάνουμε κάποιο κλικ, 3) Attachment: **Δεν ανοίγουμε συνημμένα από κάποιον που δεν γνωρίζουμε** ή συνημμένα που δεν περιμένουμε, 4) Message: Ελέγχουμε το περιεχόμενο του μηνύματος και προσέχουμε για κακή γραμματική ή ορθογραφικά λάθη.
- Είμαστε **ιδιαίτερα επιφυλακτικοί** εάν ένα μήνυμα ηλεκτρονικού ταχυδρομείου ιδρύματος πληρωμών μας ζητά ευαίσθητες πληροφορίες (π.χ. τον κωδικό πρόσβασης του τραπεζικού μας λογαριασμού web banking).
- **Είμαστε σε επαγρύπνηση** για αιτήματα που αφορούν οικονομικές συναλλαγές. Ελέγχουμε προσεκτικά τα μηνύματα ηλεκτρονικού ταχυδρομείου, συγκρίνουμε τη διεύθυνση με τα προηγούμενα πραγματικά μηνύματα από την τράπεζα συνεργασίας μας.

- **Δεν επιλέγουμε απευθείας ηλεκτρονικούς συνδέσμους** (links) και δεν μεταφορτώνουμε (download) επισυναπτόμενα αρχεία, αντίθετα πληκτρολογούμε τη διεύθυνση του ηλεκτρονικού συνδέσμου (url) στον φυλλομετρητή ιστοσελίδων (browser) που χρησιμοποιούμε.
- Σε περίπτωση οποιασδήποτε αμφιβολίας, **ελέγχουμε την ιστοσελίδα ή τηλεφωνούμε άμεσα στην τράπεζα συνεργασίας μας.**
- **Φορητές συσκευές αποθήκευσης δεδομένων** (π.χ. USB sticks) μπορεί να συνιστούν πηγή μόλυνσης, ενώ είναι πολύ εύκολο ακόμα και να χαθούν (μαζί με τυχόν πολύτιμα αρχεία που περιέχουν). Χρησιμοποιούμε πρόγραμμα κρυπτογράφησης ή και κλειδώματος των αρχείων!
- **Ελέγχουμε πάντα με προσοχή τις διευθύνσεις ηλεκτρονικού ταχυδρομείου** όταν διαχειριζόμαστε ευαίσθητες πληροφορίες ή όταν πραγματοποιούμε μεταφορές χρημάτων!
- **Ιδιαίτερη προσοχή στη χρήση των μέσων κοινωνικής δικτύωσης** και ειδικότερα αν το επάγγελμά μας συνδέεται με διαχείριση ευαίσθητων δεδομένων! Γνωρίζουμε ποιες πληροφορίες μοιραζόμαστε στα μέσα κοινωνικής δικτύωσης.