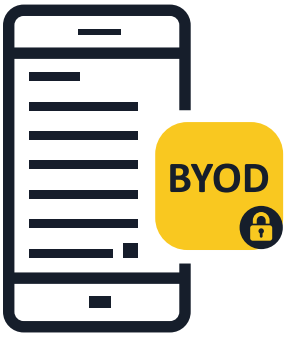
MOBILE MALWARE

ΣΥΜΒΟΥΛΕΣ ΓΙΑ ΕΠΑΓΓΕΛΜΑΤΙΕΣ & ΕΠΙΧΕΙΡΗΣΕΙΣ

1 Ενημερώστε το προσωπικό σας για τις απειλές κατά τη χρήση φορητών συσκευών

- Η χρήση των προσωπικών φορητών συσκευών και για επαγγελματικούς σκοπούς εγκυμονεί κινδύνους. Μια επίθεση, που αρχικά έχει στόχο την προσωπική φορητή συσκευή ενός εργαζόμενου, θα μπορούσε να επηρεάσει σοβαρά και την επιχείρηση. Μια φορητή συσκευή είναι ένας υπολογιστής και θα πρέπει να προστατεύεται με όμοιες μεθόδους.



2 Εφαρμόστε εταιρική πολιτική για το bring-your-own-device (BYOD – «φέρε τη δική σου συσκευή»)

- Οι εργαζόμενοι που χρησιμοποιούν τις προσωπικές τους φορητές συσκευές για να προσπελάσουν εταιρικά δεδομένα και συστήματα (ακόμα και emails, ημερολόγια ή λίστες επαφών) οφείλουν να ακολουθούν τις πολιτικές της εταιρείας. Επιλέξτε με προσοχή τις τεχνολογίες που θα χρησιμοποιηθούν για τη διαχείριση και ασφάλεια των φορητών συσκευών και υπενθυμίστε στους εργαζομένους την ανάγκη να είναι προσεκτικοί.

3 Συμπεριλάβετε πολιτικές ασφάλειας για φορητές συσκευές στο ισχύον συνολικό πλαίσιο ασφάλειας

- Αν μια συσκευή δε ανταποκρίνεται στις πολιτικές ασφαλείας, δε θα πρέπει να επιτρέπεται η σύνδεσή της στο εταιρικό δίκτυο, ούτε η πρόσβασή της σε εταιρικά δεδομένα. Οι εταιρείες θα πρέπει να αναπτύξουν τις δικές τους λύσεις Mobile Device Management (MDM) ή Enterprise Mobility Management (EMM).
- Συμπληρωματικά, είναι εξίσου χρήσιμη η εγκατάσταση μιας λύσης Mobile Threat Defence, που θα παρέχει διευρυμένη ορατότητα και σχετική ενημέρωση για τα επίπεδα απειλών σε εφαρμογές, δίκτυα και λειτουργικά συστήματα.

4 Αποφύγετε τη χρήση δημόσιων Wi-Fi δικτύων για πρόσβαση σε εταιρικά δεδομένα

- Κατά κανόνα, τα δημόσια Wi-Fi δίκτυα δεν θεωρούνται ασφαλή. Αν ένας εργαζόμενος προσπελαύνει εταιρικά δεδομένα χρησιμοποιώντας ένα ελεύθερο Wi-Fi δίκτυο σε ένα αεροδρόμιο ή μια καφετέρια, τα δεδομένα αυτά θα μπορούσαν να εκτεθούν σε κακόβουλους χρήστες. Προτείνεται οι εταιρείες να αναπτύξουν πολιτικές «αποτελεσματικής χρήσης» προς αυτή την κατεύθυνση.

5 Ενημερώνετε τακτικά τα λειτουργικά συστήματα και τις εφαρμογές

- Τονίστε στους εργαζόμενους της εταιρείας την ανάγκη να εγκαθιστούν ενημερώσεις λογισμικού και ασφαλείας για το λειτουργικό σύστημα των φορητών τους συσκευών, αμέσως μόλις ειδοποιηθούν για τη διαθεσιμότητα αυτών. Ειδικά για τα λειτουργικά Android, αναζητήστε τις πολιτικές ενημερώσεων που ακολουθούν οι κατασκευαστές των συσκευών και οι πάροχοι υπηρεσιών κινητής τηλεφωνίας. Έχοντας εγκατεστημένες τις πιο πρόσφατες ενημερώσεις, διασφαλίζετε όχι μόνο την ασφάλεια των συσκευών, αλλά και την βέλτιστη και αποδοτικότερη λειτουργία τους.

6 Εγκαταστήστε εφαρμογές μόνο από αξιόπιστες πηγές

- Οι εταιρείες θα πρέπει να επιτρέπουν στους εργαζόμενους την εγκατάσταση εφαρμογών μόνο από επίσημες πηγές για εκείνες τις φορητές συσκευές που συνδέονται στα εταιρικά δίκτυα. Εξετάστε την επιλογή δημιουργίας ενός εταιρικού καταστήματος εφαρμογών μέσω του οποίου οι τελικοί χρήστες θα μπορούν να έχουν πρόσβαση, να μεταφορτώνουν και να εγκαθιστούν εφαρμογές εγκεκριμένες από την εταιρεία. Συμβουλευτείτε έναν προμηθευτή λύσεων ασφαλείας για έτοιμα προϊόντα ή δημιουργήστε τη δική σας πλατφόρμα ενδοεταιρικά.

7 Jailbreak: σε καμία περίπτωση!

- Με τον όρο jailbreak αναφερόμαστε στη διαδικασία αφαίρεσης των περιορισμών ασφαλείας που έχουν ορισθεί από τον πωλητή του λειτουργικού συστήματος, ώστε να μπορεί κάποιος να έχει πλήρη πρόσβαση στο λειτουργικό σύστημα και στα χαρακτηριστικά του. Το jailbreak της συσκευής εξασθενεί την ασφάλειά της, δημιουργώντας κενά ασφάλειας που ενδεχομένως δεν είναι άμεσα εμφανή. Δε θα πρέπει να επιτρέπεται η χρήση στο εταιρικό περιβάλλον συσκευών που έχουν υποστεί jailbreak.

8 Εξετάστε εναλλακτικές λύσεις αποθήκευσης στο cloud

- Οι χρήστες φορητών συσκευών συχνά επιθυμούν να έχουν πρόσβαση σε σημαντικά έγγραφα όχι μόνο μέσω του εταιρικού τους υπολογιστή, αλλά και μέσα από τα ιδιωτικά τους smartphones ή tablets, όταν βρίσκονται εκτός γραφείου. Οι εταιρείες πρέπει να εξετάσουν τη δημιουργία συστημάτων ασφαλούς cloud αποθήκευσης και συγχρονισμού αρχείων, για να ικανοποιήσουν τις ανάγκες αυτές στο πλαίσιο της μέγιστης δυνατής ασφάλειας.

9 Ενθαρρύνετε το προσωπικό σας να εγκαταστήσει λογισμικό ασφάλειας για φορητές συσκευές

- Όλα τα λειτουργικά συστήματα κινδυνεύουν να μολυνθούν. Βεβαιωθείτε ότι οι εργαζόμενοι χρησιμοποιούν, εφόσον υπάρχει διαθέσιμο, λογισμικό ασφάλειας για φορητές συσκευές, το οποίο ανιχνεύει και προστατεύει από malware, spyware και κακόβουλες εφαρμογές, αλλά και αντικλεπτικές λύσεις και λύσεις προστασίας της ιδιωτικότητας.

EUROPOL EC3 European Cybercrime Centre

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ
Υπουργείο Εσωτερικών και Διοικητικής Ανασυγκρότησης
ΑΡΧΗΓΕΙΟ ΕΛΛΗΝΙΚΗΣ ΑΣΤΥΝΟΜΙΑΣ

CYBER CRIME DIVISION
ΔΙΩΞΗ ΗΛΕΚ/ΝΙΚΟΥ ΕΓΚΛΗΜΑΤΟΣ

#MobileMalware