ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ
ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ

Η χρήση έξυπνων συσκευών στο χώρο εργασίας: Ασφάλεια και προσωπικά δεδομένα

Ανάργυρος Χρυσάνθου, MSc., Ειδικός Επιστήμων ΑΠΔΠΧ

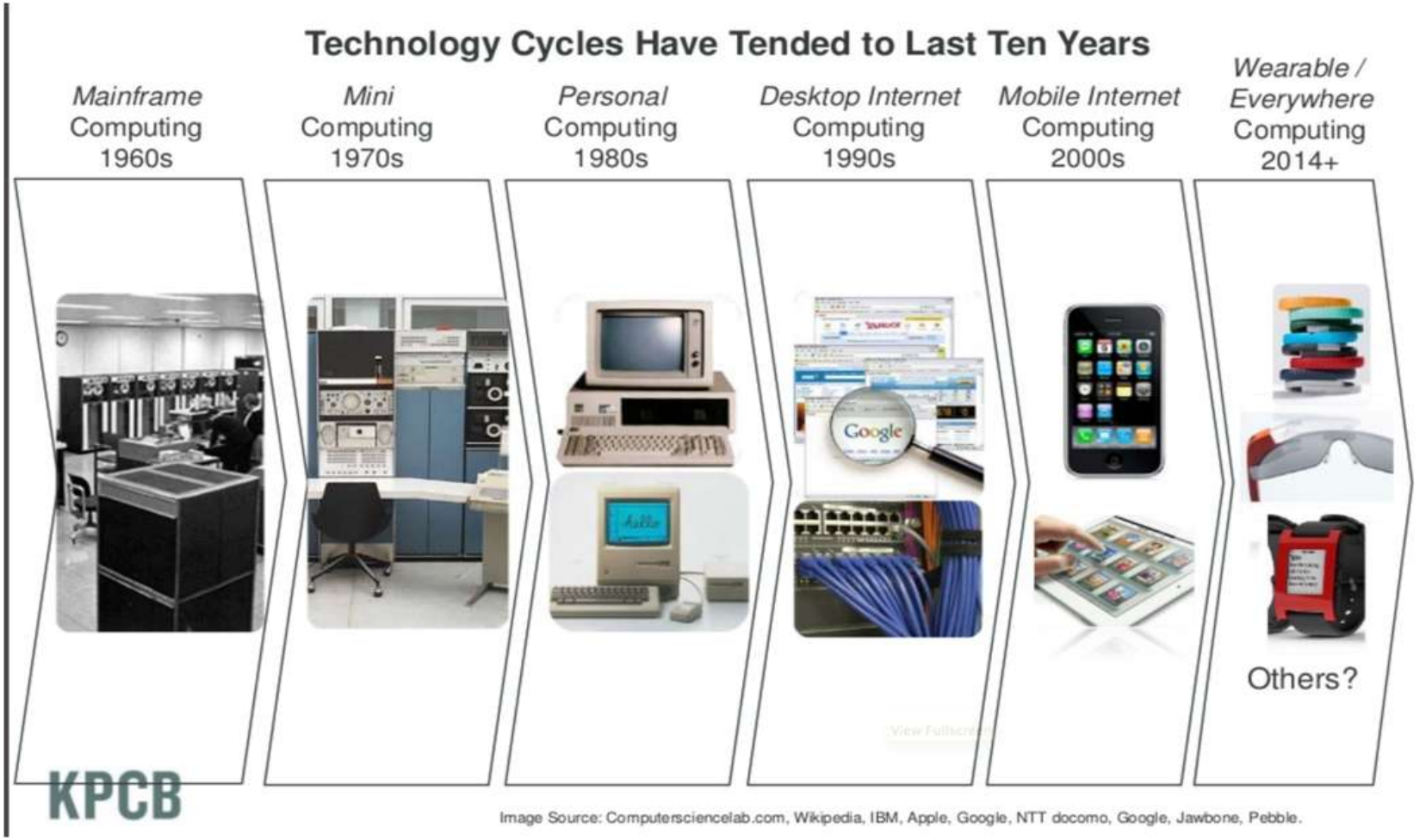
Δομή Παρουσίασης

Α. Χρυσάνθου

- Εισαγωγή
- Γιατί να χρησιμοποιήσω τη δική μου συσκευή;
- Είναι ασφαλές; Ποιοι είναι οι κίνδυνοι;
- Τι μέτρα ασφάλειας πρέπει να λάβω;
- Συμπεράσματα

Η εξέλιξη των τεχνολογιών πληροφορικής

Α. Χρυσάνθου



KPCB Internet Trends 2013
http://www.slideshare.net/kleinerperkins/kpcb-internet-trends-2013

3

Η εποχή του “mobile computing”

- Έξυπνες συσκευές (κινητά τηλέφωνα, τηλεοράσεις)
- Διαρκής πρόσβαση στο Διαδίκτυο
- Ένα «Σύννεφο» διαθέσιμων εφαρμογών

Η ζωή μας έχει αλλάξει

  - **Ο εργασιακός μας χώρος;;;**

Ο εργασιακός μας χώρος

- Έξυπνες συσκευές
  - Κινητά
  - Tablets
- Laptops
- Netbooks
- Ασύρματες κάρτες δικτύου
- Webcams
- Προσωπική ιδιοκτησία
  - Υπαλλήλων
- Μεταφερόμενοι
- Απομακρυσμένη εργασία

BYOD – Ορισμοί

- *"Bring Your Own Device (BYOD) is exactly what its moniker implies: the growing trend for employees to use personally-owned smartphones, tablets, laptops and other platforms to access corporate applications like email and databases; and to create, store and manage corporate data using these devices".*

(Osterman Research, 2012, Putting IT Back in Control of BYOD, http://www.slideshare.net/mosterman/putting-it-back-in-control-of-byod)

«Η πρακτική, με βάση την οποία οι υπάλληλοι μιας επιχείρησης χρησιμοποιούν, για εταιρικούς λόγους, ιδιόκτητες συσκευές (έξυπνα τηλέφωνα, tablets, φορητούς υπολογιστές και άλλες πλατφόρμες) για πρόσβαση σε εταιρικές εφαρμογές, όπως ηλεκτρονικό ταχυδρομείο και βάσεις δεδομένων, αλλά και για δημιουργία, αποθήκευση και διαχείριση εταιρικών δεδομένων.»

Γιατί να χρησιμοποιήσω τη δική μου συσκευή (1/2);

- **Γιατί….**
  - «**συμφέρει**» τον εργοδότη μου
    - Οικονομία κόστους
      - Μείωση εξόδων υλικού / λογισμικού
      - Χρήση ενδεχομένως «καλύτερου» εξοπλισμού
      - Αξιοποίηση της ομάδας πληροφορικής σε άλλα καθήκοντα

ΟΙ ΧΡΗΣΤΕΣ ΥΠΟΣΤΗΡΙΖΟΥΝ ΚΑΙ «ΠΡΟΣΕΧΟΥΝ» ΚΑΛΥΤΕΡΑ ΤΙΣ **ΔΙΚΕΣ ΤΟΥΣ** ΣΥΣΚΕΥΕΣ

Γιατί να χρησιμοποιήσω τη δική μου συσκευή (2/2);

- **Γιατί….**
  - με κάνει «ευτυχισμένο» ως εργαζόμενο
- Μπορώ να δουλεύω
  - όποτε χρειάζεται
  - από όπου θέλω
  - στη **δική μου** συσκευή
- Και φυσικά…
  - Να είμαι πιο παραγωγικός
  - Όντας πιο ευέλικτος

ManageEngine, 2012

Είναι ασφαλές; Ποιοι είναι οι κίνδυνοι;

- **B**ring **Y**our **O**wn **D**evice or....
  - **B**ring **Y**our **O**wn **D**isaster????
- BYOD
  - Οφέλη
  - Κίνδυνοι ασφάλειας πληροφοριών

Η «περίμετρος» έχει αλλάξει

- Ασφάλεια
  - Δεδομένων
  - Δικτύου
  - Φυσική
- Σε ένα περιβάλλον
  - Αναρίθμητες «δικτυωμένες» μη εταιρικές συσκευές
  - Συνεχώς μεταφερόμενες
  - Ετερογενή λειτουργικά συστήματα
  - Αμέτρητες εφαρμογές (Apps)
  - Πολυάριθμοι ιοί

Τα έξυπνα τηλέφωνα είναι…

- Ελκυστικοί στόχοι
  - Μπορούν να
    - «υποκλέψουν» εταιρικά δεδομένα
    - αποτελέσουν σημείο εισόδου σε εταιρικά δίκτυα
    - «κρυφακούσουν»
    - «παράσχουν» λίστες επαφών, στοιχεία κλήσεων, μηνύματα, κ.α.
    - φανερώσουν στοιχεία τοποθεσίας

  Ή απλά…

    - να κλαπούν / χαθούν

Τα δεδομένα στο έξυπνο τηλέφωνο μου είναι ασφαλή…

ΜΟΝΟ ΕΓΩ ΤΟ ΧΡΗΣΙΜΟΠΟΙΩ…

- Μόνο;;;;
- Πόσες εφαρμογές (apps) έχεις εγκαταστήσει;
- Ξέρεις τι ακριβώς κάνουν;
- Τι δικαιώματα τους έχεις δώσει;
- Έχεις ελέγξει για ποιο λόγο τα χρειάζονται;
- Τι δεδομένα συλλέγουν για σένα;
- Συλλέγουν πχ. μόνο δεδομένα θέσης (GPS);

Πλαστή εφαρμογή Instagram (2012)

- Διαθέσιμη σε μη εγκεκριμένο κατάστημα με apps
- Οικονομικό όφελος;;;
  - Αποστολή sms
  - Στο παρασκήνιο
- Andr/Boxer-F

http://nakedsecurity.sophos.com/2012/04/18/fake-instagram-app-android-malwar/

Το app μου είναι «εγκεκριμένο»

- iOS and Android virus
  - Google Play
  - Apple App Store
- Trojan
- Υποκλοπή λίστας επαφών
- Sms Spam
- Αποστολέας
  - Τηλέφωνο χρήστη
  - Sms -> App URL

(http://www.securelist.com/en/blog/208193641/Find_and_Call_Leak_and_Spam)

Έδωσα δικαιώματα…

- Τι μπορώ να πάθω;
  - Αποστολή premium sms (Fake Instagram App)
  - Κλοπή πνευματικής ιδιοκτησίας / διαρροή δεδομένων (Hand of Thief)
  - Κλοπή στοιχείων αυθεντικοποίησης (PowerZeus - KINS)
  - Επιθέσεις κοινωνικής μηχανικής σε εταιρικά e-mail
  - Εταιρική Κατασκοπεία (Red October)
  - Παρακολούθηση κινήσεων
  - Πιθανές κυρώσεις (διοικητικές & μη)

Εξίσου σημαντικά…

- Έξυπνες συσκευές
  - Περιορισμένες δυνατότητες ασφάλειας
  - Μειωμένο επίπεδο ασφάλειας (jailbroken / rooted)
  - Τέλος υποστήριξης
  - Ετερογενή δίκτυα
  - Αυτόματη σύνδεση
  - Αντίγραφα ασφαλείας στο «σύννεφο»
  - Διαμοιρασμός με οικεία πρόσωπα
  - Μη «εταιρικής» ιδιοκτησίας

http://www.apartmenttherapy.com/is-free-wi-fi-safe-172250

Η «περίμετρος» έχει αλλάξει…

- Η ασφάλεια πληροφοριών **όχι**…

«Ορίζεται ως η διατήρηση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας της πληροφορίας. Επιπρόσθετα, μπορούν να περιληφθούν στην ασφάλεια πληροφοριών και άλλες ιδιότητες όπως η αυθεντικότητα, η υπευθυνότητα (accountability), η μη-αποποίηση (non-repudiation) και η αξιοπιστία.» (ISO 27001:2005)

- Νέες «έξυπνες» συσκευές στο δίκτυο => Νέα μέτρα ασφάλειας
  - Συνέπεια μιας μελέτης επικινδυνότητας
- **Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών**
  - Αντιμετώπιση νέων κινδύνων ασφάλειας

Τι μέτρα ασφάλειας πρέπει να λάβω; (1/4)

- Εκπαίδευση
  - Συνεχής
  - Με διάφορους τρόπους
    - Εισαγωγική εβδομάδα
    - Αλλαγές Πολιτικών
    - Αφίσες
- **Στόχος**: Ευαισθητοποίηση χρηστών

Τι μέτρα ασφάλειας πρέπει να λάβω; (2/4)

- Πολιτική Ορθής (αποδεκτής) χρήσης «κινητών» συσκευών (ενδεικτικά)
  - Διαγραφή δεδομένων (device wiping)
  - Αποθήκευση δεδομένων
  - Κρυπτογράφηση
  - Προστασία από ιομορφικό λογισμικό
  - Εγκατάσταση εφαρμογών (apps)
  - Σύνδεση στο δίκτυο
  - Απομακρυσμένος εντοπισμός συσκευής
  - Απενεργοποίηση λειτουργιών με βάση τοποθεσία (geofencing)
  - Απομακρυσμένη πρόσβαση

http://www.eweek.com/imagesvr_ce/7287/048313deactivatingtitle.jpg

Τι μέτρα ασφάλειας πρέπει να λάβω; (3/4)

- Ενδεικτικά
  - Υποχρεωτική δήλωση συσκευής
  - Έλεγχος ασφάλειας συσκευής
    - Απαγόρευση χρήσης εφαρμογών από μη εγκεκριμένα app stores
    - Απαγόρευση χρήσης rooted / jailbroken συσκευών
  - Απαγόρευση εφαρμογών cloud
  - Χρήση PINs και Passcodes (Μήκος > 4, αλφαριθμητικό)
  - Διαγραφή δεδομένων μετά από 10 αποτυχημένους κωδικούς (wipe)
  - Ενεργοποίηση απομακρυσμένου εντοπισμού συσκευής

http://www.askdavetaylor.com/how_to_use_find_my_iphone_apple_ipad_ipod_touch/

Τι μέτρα ασφάλειας πρέπει να λάβω; (4/4)

- Έλεγχος συμμόρφωσης ρυθμίσεων συσκευών με πολιτική BYOD
- Εκτέλεση εταιρικών εφαρμογών σε secure containers ή σε περιβάλλον Virtual Hosted Desktop (VHD)
- Απομακρυσμένη σύνδεση μόνο με VPN
- Απενεργοποίηση μέτρων ασφαλείας (πχ. content filtering) εκτός εταιρείας
- Υποστήριξη χρηστών / συσκευών (έστω συμβουλευτικά)

Θέματα ιδιωτικότητας

Α. Χρυσάνθου

- Προσωπικά δεδομένα
  - Φωτογραφίες, βίντεο, προσωπικά e-mail, κτλ
  - Ιστορικό πλοήγησης, στοιχεία αυθεντικοποίησης
  - Φορολογικά στοιχεία
- Συμμετοχή υπαλλήλων / HR στη διαμόρφωση της πολιτικής BYOD
- Λήψη μέτρων ασφάλειας
- Σεβασμός της αρχής της αναλογικότητας
- Σαφής σκοπός ελέγχου συσκευών
- Σύμφωνη γνώμη εργαζομένων
- Μη παρακολούθηση εργαζομένου
- Διαχωρισμός εταιρικών / προσωπικών δεδομένων

Τι πρέπει να ξέρουν οι χρήστες;

- Όχι χρήση λογαριασμών ηλ. ταχυδρομείου για ανάκτηση πρόσβασης σε άλλες υπηρεσίες από έξυπνα κινητά
- Όχι αποκάλυψη των μέτρων προστασίας της συσκευής
- Όχι άνοιγμα ύποπτων μηνυμάτων
- Σε περίπτωση απώλειας / κλοπής
  - Ενημέρωση εταιρείας
  - Προσπάθεια εντοπισμού
  - Απομακρυσμένη διαγραφή
  - Αφαίρεση δικαιωμάτων συσκευής (πχ. σύνδεση με iTunes, πρόσβαση σε αντίγραφα ασφαλείας σε iCloud)

Συμπεράσματα

- Οι «έξυπνες» κινητές συσκευές είναι «**εδώ**»
- Περίμετρος: Ποτέ ξανά η ίδια
- Σε συνεχή επιφυλακή
  - Χρήστες
  - Οργανισμοί

http://blog.etelesolv.com/bid/104155/Managing-IT-Costs-in-a-BYOD-Environment

Βιβλιογραφία (1/2)

- Article 29 Data Protection Working Party, Opinion 02/2013 on apps on smart devices, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf
- Article 29 Data Protection Working Party, Opinion 13/2011 on Geolocation services on smart mobile devices, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp185_en.pdf
- Information Law Group, Bring Your Own Device Security and Privacy Legal Risks, http://www.isaca-denver.org/Conferences/RMISC/Presentations/301-Legal_Implications_of_BYOD.pdf
- Kaspersky Labs, Mobile Security and BYOD for Dummies http://www.kaspersky.com/business-security/byod-for-dummies

Βιβλιογραφία (2/2)

- SecureState, Android vs. Apple iOs Security Showdown, http://www.slideshare.net/agent0x0/the-android-vs-apple-ios-security-showdown
- UK Information Commissioner Office, Bring Your Own Device Guidance, http://www.ico.org.uk/~/media/documents/library/Data_Protection/Practical_application/ico_bring_your_own_device_byod_guidance.ashx
- Αρχή Προστασίας Δεδομένων, Πολιτική ασφάλειας, σχέδιο ασφάλειας, σχέδιο ανάκαμψης από καταστροφές, http://www.dpa.gr/pls/portal/url/ITEM/B6F5DCC88FD8EC4AE040A8C07C24572A
- Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, Οδηγία 115/2001 για την επεξεργασία δεδομένων των εργαζομένων, http://www.dpa.gr/pls/portal/url/ITEM/BD66D8402E549E88E040A8C07C242BC7

Ευχαριστώ για την προσοχή σας