Κεφάλαιο 8

Ασφάλεια των πληροφοριακών συστημάτων

ΜΑΘΗΣΙΑΚΟΙ ΣΤΟΧΟΙ

- Για ποιον λόγο είναι τα πληροφοριακά συστήματα ευάλωτα σε καταστροφή, σφάλματα και κακή χρήση;
- Ποια είναι η επιχειρηματική αξία της ασφάλειας και του ελέγχου;
- Ποια είναι τα συστατικά στοιχεία ενός οργανωσιακού πλαισίου δράσης για την ασφάλεια και τον έλεγχο;
- Ποια είναι τα σημαντικότερα εργαλεία και τεχνολογίες για την προστασία των πληροφοριακών πόρων;

ΜΑΘΗΣΙΑΚΟΙ ΣΤΟΧΟΙ

Πρόσθετο υλικό για μελέτη

1.The Booming Job Market in IT Security (Η εκρηκτική ανάπτυξη της αγοράς εργασίας στον τομέα της ασφάλειας ΤΠ)

2.The Sarbanes Oxley Act (Νόμος Sarbanes Oxley)

3.Computer Forensics (Ηλεκτρονική εγκληματολογία)

4.General and Application Controls for Information Systems (Γενικά μέτρα ελέγχου και μέτρα ελέγχου εφαρμογών στα ΠΣ)

5.Management Challenges of Security and Control (Προκλήσεις ασφάλειας και ελέγχου σε διοικητικό επίπεδο)

6.Software Vulnerability and Reliability (Ευπάθεια και αξιοπιστία του λογισμικού)

Βίντεο

Περ. Μελέτη 1: Stuxnet and Cyberwarfare (Το σκουλήκι Stuxnet και ο κυβερνοπόλεμος)

Περ. Μελέτη 2: Cyberespionage: The Chinese Threat (Κυβερνοκατασκοπεία: Η κινεζική απειλή)

Περ. Μελέτη 3: IBM Zone Trusted Information Channel (Ο Δίαυλος Έμπιστων Πληροφοριών Ζώνης της IBM)

Βίντεο 1: Sony PlayStation Hacked; Data Stolen from 77 Million Users (Παραβίαση των λογαριασμών του Sony PlayStation και κλοπή δεδομένων από 77 εκατομμύρια χρήστες)

Βίντεο 2: Zappos Working to Correct Online Security Breach (Η Zappos προσπαθεί να αποκαταστήσει την παραβίαση των ηλεκτρονικών συστημάτων της)

Βίντεο 3: Meet the Hackers: Anonymous Statement on Hacking SONY (Ιδού οι χάκερ: Δήλωση των Anonymous για την παραβίαση της SONY)

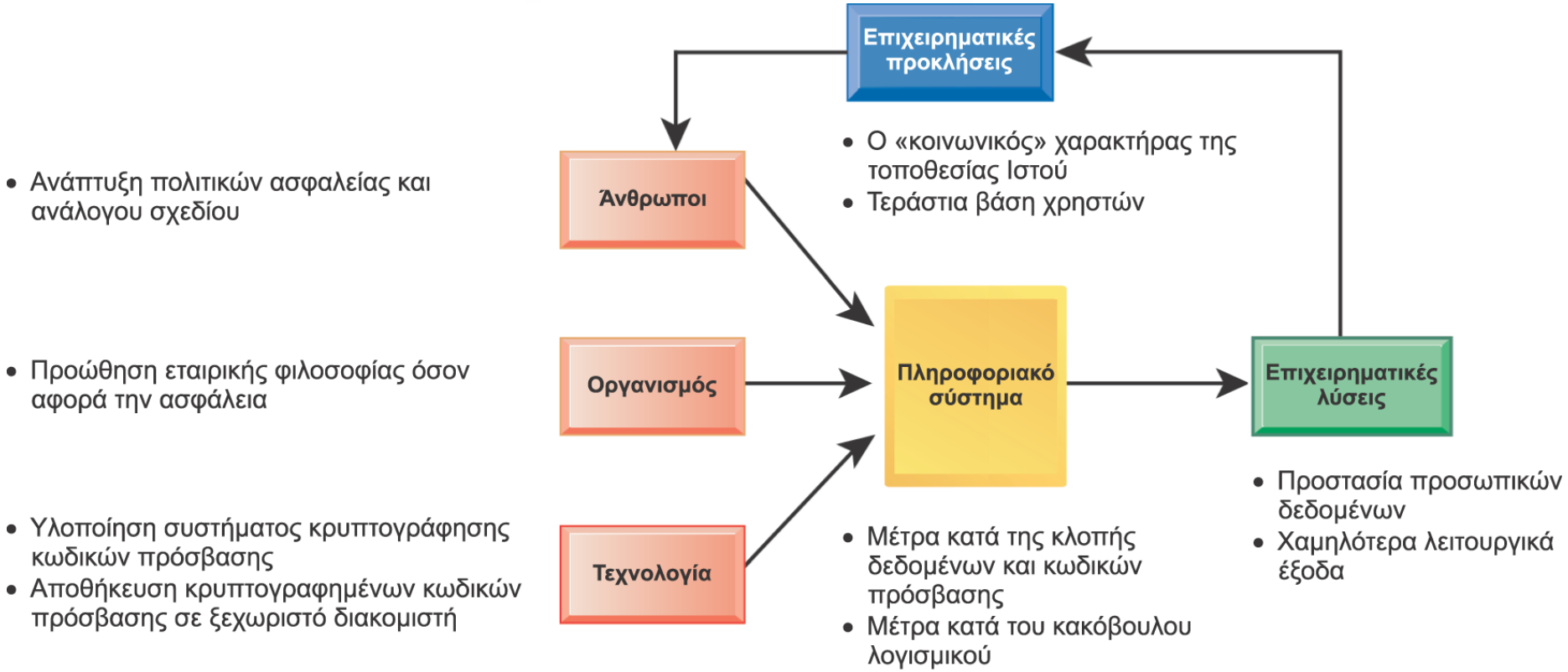
Έχετε λογαριασμό στο LinkedIn; Φυλαχτείτε!

- **LinkedIn:**
  - Ένα από τα μεγαλύτερα κοινωνικά δίκτυα στον κόσμο, με περισσότερα από 225 εκατομμύρια χρήστες
  - Ως ευρέως διαδεδομένο μέσο κοινωνικής δικτύωσης, αποτελεί στόχο για τους χάκερ
  - Παρωχημένες διαδικασίες ασφαλείας
- **Πρόβλημα**
  - Μια παραβίαση των ηλεκτρονικών συστημάτων οδήγησε στην αποκάλυψη 6,5 εκατομμυρίων κωδικών πρόσβασης
  - Σπίλωση φήμης
  - Μηνύσεις ύψους πολλών εκατομμυρίων δολαρίων

Έχετε λογαριασμό στο LinkedIn; Φυλαχτείτε!

- **Αν και η πολιτική ασφαλείας του LinkedIn ήταν επαρκής πριν από μερικά χρόνια, εν έτει 2012 αποδείχθηκε εντελώς ανεπαρκής**
  - Δεν προέβλεπε:
    - Την ύπαρξη ενός διευθυντή ασφαλείας
    - Έστω και την ελάχιστη προστασία των κωδικών πρόσβασης με κρυπτογράφηση
    - Τη χρήση μεθόδων «εμπλουτισμού» (salting) των κωδικών πρόσβασης
- **Η περιπτωσιολογική μελέτη εξηγεί: Την έλλειψη υπαιτιότητας των εταιρειών που ασχολούνται με τις υπηρεσίες κοινωνικής δικτύωσης, ως αιτία για τις χαλαρές πολιτικές ασφάλειας**
- **Η περιπτωσιολογική μελέτη δείχνει: Την ανάγκη για συνεχή ενημέρωση και επικαιροποίηση της πολιτικής ασφαλείας**

Έχετε λογαριασμό στο LinkedIn; Φυλαχτείτε!



Ευάλωτα συστήματα και κατάχρηση

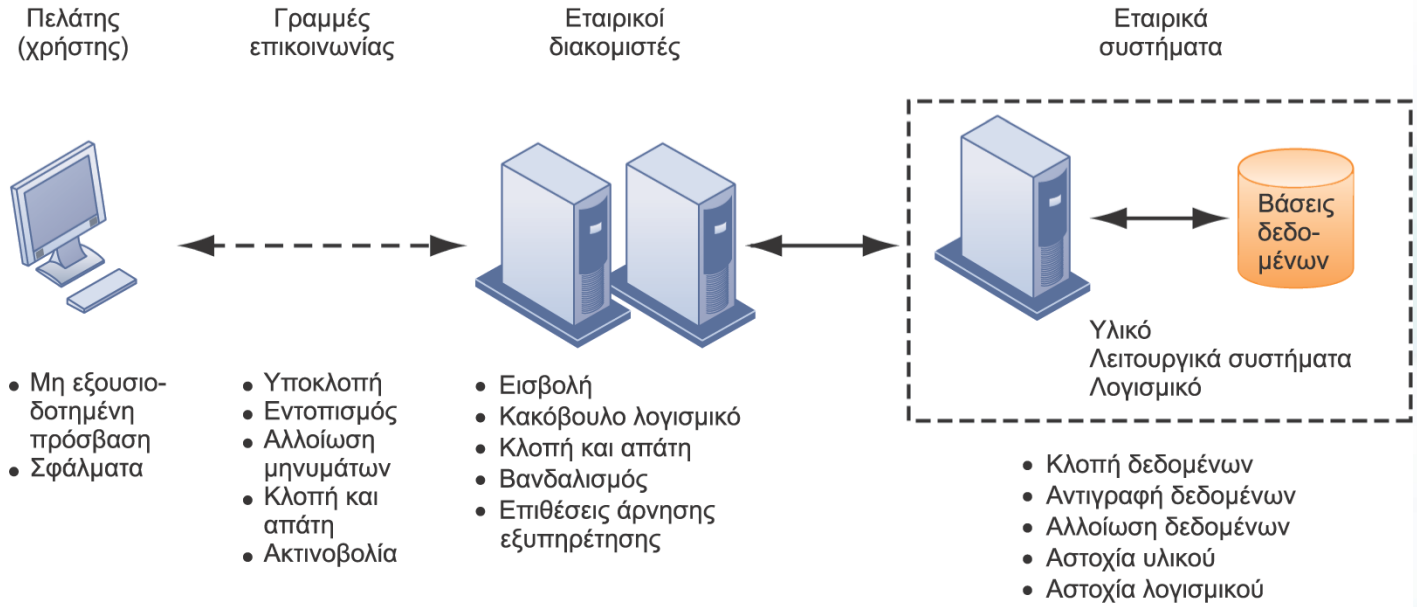
- **Ένας υπολογιστής που είναι συνδεδεμένος στο Διαδίκτυο χωρίς μέτρα προστασίας μπορεί να απενεργοποιηθεί σε δευτερόλεπτα**
- **Ασφάλεια:**
  - Το σύνολο των πολιτικών, των διαδικασιών και των τεχνικών μέτρων που χρησιμοποιούνται προκειμένου να εμποδιστεί η μη εξουσιοδοτημένη πρόσβαση, αλλοίωση, κλοπή ή υλική ζημιά των πληροφοριακών συστημάτων από παρείσακτους
- **Μέτρα ελέγχου (controls):**
  - Οι μέθοδοι, πολιτικές και οργανωσιακές διαδικασίες που εγγυώνται την ασφάλεια των περιουσιακών στοιχείων του οργανισμού, την ακρίβεια και αξιοπιστία των αρχείων του, και την εκ μέρους του τήρηση των κανόνων διαχείρισης

Γιατί είναι ευάλωτα τα συστήματα

- **Προβλήματα στο υλικό**
  - Βλάβες, σφάλματα στη ρύθμιση των παραμέτρων, ζημιά από ακατάλληλη χρήση ή από εγκληματική ενέργεια
- **Προβλήματα στο λογισμικό**
  - Σφάλματα στον κώδικα, σφάλματα στην εγκατάσταση, μη εξουσιοδοτημένες αλλαγές
- **Καταστροφές**
  - Πτώση τάσης, πλημμύρες, πυρκαγιές, κ.ο.κ.
- **Χρήση δικτύων και υπολογιστών εκτός του ελέγχου της επιχείρησης**
  - Εγχώριοι ή εξωχώριοι προμηθευτές
  - Φορητές συσκευές

Ευάλωτα συστήματα και κατάχρηση

Σύγχρονες προκλήσεις για την ασφάλεια και ευάλωτα σημεία



Εικόνα 8-1

Η αρχιτεκτονική κάθε ιστοπαγούς εφαρμογής περιλαμβάνει κατά κανόνα έναν πελάτη Ιστού, έναν διακομιστή και εταιρικά πληροφοριακά συστήματα συνδεδεμένα με βάσεις δεδομένων. Το καθένα από αυτά τα στοιχεία θέτει προκλήσεις σε επίπεδο ασφάλειας και εισάγει ευάλωτα σημεία στα συστήματα. Πλημμύρες, πυρκαγιές, διακοπές ρεύματος και άλλα προβλήματα με την τροφοδοσία ηλεκτρικού ρεύματος μπορούν να προκαλέσουν διαταραχές σε οποιοδήποτε σημείο του δικτύου.

Ευάλωτα συστήματα και κατάχρηση

- **Αδύνατα σημεία στο Διαδίκτυο**
  - **Ανοιχτό σε όλους**
  - **Λόγω του μεγέθους του, κάθε κατάχρηση μπορεί να έχει εκτενή επίδραση**
  - **Η χρήση σταθερών διευθύνσεων στο Διαδίκτυο σε συνδυασμό με τις μόνιμες συνδέσεις διευκολύνουν την ταυτοποίηση ενός χρήστη από τους χάκερ**
  - **Συνημμένα αρχεία μέσω ηλεκτρονικού ταχυδρομείου, λήψη αρχείων, κοινή χρήση αρχείων**
  - **Χρήση του ηλεκτρονικού ταχυδρομείου για την επικοινωνία εμπορικών μυστικών**
  - **Τα μηνύματα στις υπηρεσίες άμεσων μηνυμάτων δεν έχουν επαρκή ασφάλεια, είναι εύκολο να υποκλαπούν**

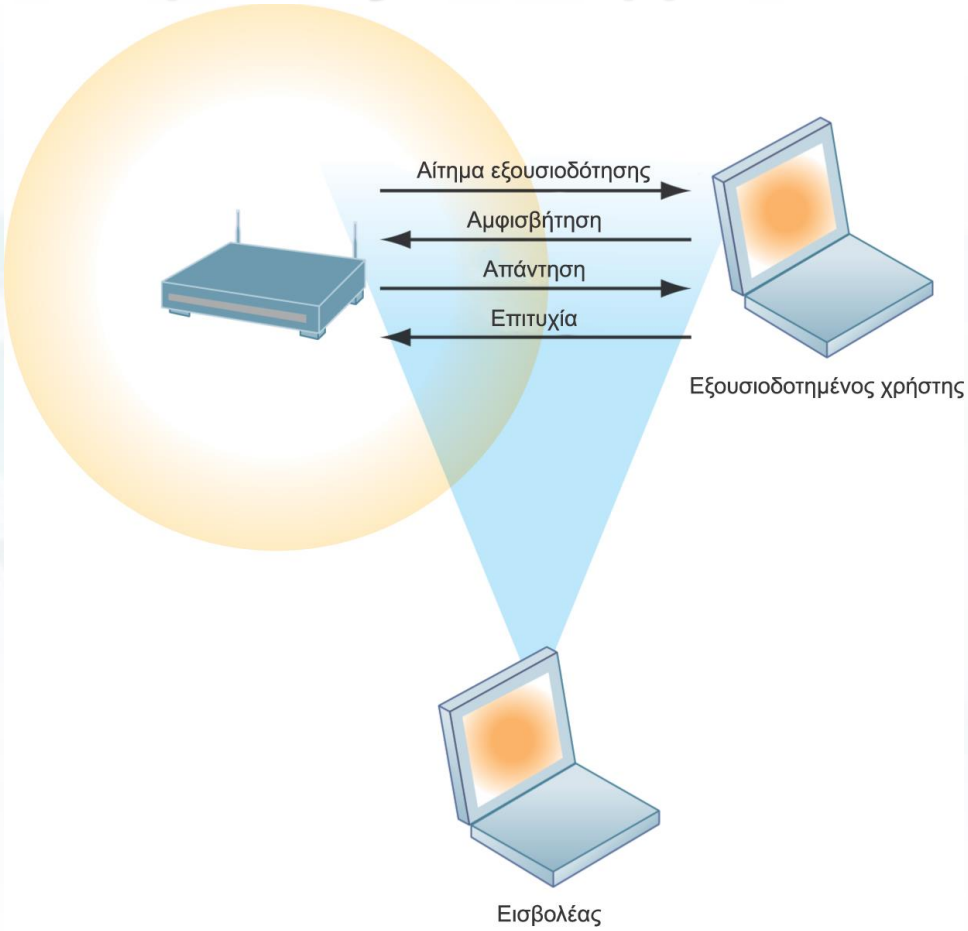
Ευάλωτα συστήματα και κατάχρηση

- **Προβλήματα ασφάλειας σε ασύρματα δίκτυα**
  - **Οι ζώνες ραδιοσυχνοτήτων σαρώνονται εύκολα**
  - **Αναγνωριστικά συνόλου υπηρεσιών (SSID)**
    - Προσδιορίζουν τα σημεία πρόσβασης στο δίκτυο Wi-Fi.
    - Μεταδίδονται πολλές φορές.
  - **Περιπολία εντοπισμού (war driving)**
    - Οι «ωτακουστές» περνούν με το αυτοκίνητό τους δίπλα από κτίρια και προσπαθούν να παρεισφρύσουν στην κυκλοφορία δεδομένων από ασύρματα δίκτυα
    - Η πρόσβαση στο SSID δίνει πρόσβαση στους πόρους του δικτύου
  - **Πλαστά σημεία πρόσβασης**

Προβλήματα ασφάλειας σε ασύρματα δίκτυα

Εικόνα 8-2

Σε πολλά ασύρματα δίκτυα, είναι εύκολο για τους εισβολείς να διεισδύσουν χρησιμοποιώντας προγράμματα εντοπισμού (sniffers), ώστε να αποκτήσουν μια διεύθυνση και να προσπελάσουν τους πόρους του δικτύου χωρίς κατάλληλη εξουσιοδότηση.



Κακόβουλο λογισμικό: Ιοί, σκουλήκια, δούρειοι ίπποι και κατασκοπευτικό λογισμικό

- **Κακόβουλο λογισμικό (malware)**
  - **Ιός (virus)**
    - Κακόβουλο πρόγραμμα λογισμικού που προσκολλάται σε άλλα προγράμματα λογισμικού ή αρχεία δεδομένων προκειμένου να εκτελεστεί
  - **Σκουλήκι (worm)**
    - Ανεξάρτητο πρόγραμμα που αντιγράφεται από τον έναν υπολογιστή στον άλλον μέσω δικτύου
  - **Δούρειος ίππος (Trojan horse)**
    - Πρόγραμμα λογισμικού το οποίο εμφανίζεται ακίνδυνο, αλλά κάνει κάτι διαφορετικό από το αναμενόμενο.

Ευάλωτα συστήματα και κατάχρηση

Κακόβουλο λογισμικό: Ιοί, σκουλήκια, δούρειοι ίπποι και κατασκοπευτικό λογισμικό

- **Επίθεση με προσθήκη κακόβουλου κώδικα SQL (SQL injection attack)**
- **Κατασκοπευτικό λογισμικό (spyware)**
  - Μικρά προγράμματα που εγκαθίστανται λαθραία σε υπολογιστές, όπου παρακολουθούν τη δραστηριότητα περιήγησης του χρήστη στον Ιστό και παρουσιάζουν διαφημίσεις
- **Προγράμματα καταγραφής πληκτρολογήσεων (key loggers)**
  - Καταγράφουν κάθε πλήκτρο που πατά ο χρήστης στον υπολογιστή, προκειμένου να υποκλέψουν σειριακούς αριθμούς λογισμικού και κωδικούς πρόσβασης, ή να εξαπολύσουν επιθέσεις στο Διαδίκτυο

Χάκερ και ηλεκτρονική εγκληματικότητα

- **Χάκερ και κράκερ**
- **Στις δραστηριότητές τους συμπεριλαμβάνονται:**
  - **Η εισβολή σε συστήματα**
  - **Η κλοπή αγαθών και υπηρεσιών**
  - **Η πρόκληση βλαβών σε συστήματα**
  - **Ο κυβερνοβανδαλισμός—**Η σκόπιμη διατάραξη, αλλοίωση ή καταστροφή τοποθεσιών Ιστού ή εταιρικών πληροφοριακών συστημάτων

Χάκερ και ηλεκτρονική εγκληματικότητα

- **Παραπλάνηση (spoofing)**
  - Οι χάκερ επιχειρούν να κρύψουν την πραγματική τους ταυτότητα παραπλανώντας τους χρήστες-στόχους, με μια πλαστή διεύθυνση ηλεκτρονικού ταχυδρομείου ή υποδυόμενοι κάποιον άλλον
  - Ανακατεύθυνση ενός συνδέσμου του Ιστού σε διεύθυνση διαφορετική από την επιδιωκόμενη, προς μια τοποθεσία Ιστού που υποδύεται την επιδιωκόμενη
- **Πρόγραμμα εντοπισμού (sniffer)**
  - Είδος προγράμματος το οποίο παρακολουθεί τις πληροφορίες που διακινούνται διαμέσου ενός δικτύου
  - Επιτρέπει στους χάκερ να κλέβουν ιδιωτικές πληροφορίες, συμπεριλαμβανομένων μηνυμάτων ηλεκτρονικού ταχυδρομείου, εταιρικών αρχείων, κ.ο.κ.

Χάκερ και ηλεκτρονική εγκληματικότητα

- **Επίθεση άρνησης εξυπηρέτησης (Denial-of-service attack, DoS)**
  - Κατακλυσμός ενός διακομιστή με πολλές χιλιάδες ψευδή μηνύματα ή αιτήματα εξυπηρέτησης με σκοπό την κατάρρευση του δικτύου.
- **Κατανεμημένη επίθεση άρνησης εξυπηρέτησης (distributed denial-of-service attack, DDoS)**
  - Χρήση πολλών υπολογιστών σε επίθεση DoS
  - **Δίκτυο ρομπότ (botnet)**
    - Δίκτυα υπολογιστών-«ζόμπι» που έχουν προσβληθεί από κακόβουλο λογισμικό

Χάκερ και ηλεκτρονική εγκληματικότητα

- **Ηλεκτρονική εγκληματικότητα**
  - Κάθε παραβίαση του ποινικού δικαίου που περιλαμβάνει γνώση της τεχνολογίας των υπολογιστών προκειμένου να διαπραχθεί, να ερευνηθεί ή να ασκηθεί σχετική δίωξη
  - **Ο υπολογιστής μπορεί να είναι ο στόχος μιας εγκληματικής ενέργειας:**
    - Παραβίαση του απόρρητου χαρακτήρα προστατευμένων μηχανοργανωμένων δεδομένων
    - Μη εξουσιοδοτημένη πρόσβαση σε σύστημα υπολογιστών
  - **Ο υπολογιστής μπορεί να είναι το όργανο μιας εγκληματικής ενέργειας:**
    - Κλοπή εμπορικών μυστικών
    - Χρήση ηλεκτρονικού ταχυδρομείου για απειλές ή όχληση

Περ. Μελέτη: Οργανισμοί
Το «μεγάλο κόλπο» στον 21ο αιώνα

- **Διαβάστε την περιπτωσιολογική μελέτη και μετά συζητήστε τις παρακάτω ερωτήσεις:**
  - Να περιγράψετε τα ευάλωτα σημεία ασφαλείας τα οποία εκμεταλλεύθηκαν οι χάκερ.
  - Ποιοι ανθρώπινοι, οργανωσιακοί και τεχνολογικοί παράγοντες συνέβαλαν σε αυτά τα προβλήματα;
  - Ποιες λύσεις υπάρχουν για το πρόβλημα αυτό; Πόσο δύσκολο είναι να τεθούν σε εφαρμογή; Γιατί;

Χάκερ και ηλεκτρονική εγκληματικότητα

- **Κλοπή ταυτότητας**
  - Ο απατεώνας υποκλέπτει καίρια προσωπικά δεδομένα (τον αριθμό κοινωνικής ασφάλισης, τον αριθμό της άδειας οδήγησης ή αριθμούς πιστωτικών καρτών), με σκοπό να υποδυθεί κάποιον άλλον
- **Ηλεκτρονικό «ψάρεμα» (phishing)**
  - Δημιουργία πλαστών τοποθεσιών Ιστού ή αποστολή μηνυμάτων ηλεκτρονικού ταχυδρομείου όμοιων με μηνύματα αναγνωρισμένων επιχειρήσεων, που ζητούν από τους χρήστες τα εμπιστευτικά προσωπικά τους δεδομένα
- **«Πονηροί δίδυμοι» (evil twins)**
  - Ασύρματα δίκτυα που προσποιούνται ότι προσφέρουν φερέγγυες συνδέσεις μέσω Wi-Fi στο Διαδίκτυο

Χάκερ και ηλεκτρονική εγκληματικότητα

- **«Εκτροφή» (pharming)**
  - Η εκτροφή (κυριολεκτική απόδοση, αλλά στην ουσία μέθοδος παραπλάνησης) ανακατευθύνει τον χρήστη σε μια πλαστή ιστοσελίδα, έστω κι αν αυτός πληκτρολογεί τη σωστή διεύθυνση ιστοσελίδας στον φυλλομετρητή του
- **Απάτη των κλικ (click fraud)**
  - Άτομο ή πρόγραμμα υπολογιστή ανοίγει μια διαδικτυακή διαφήμιση με δόλιο σκοπό, χωρίς να έχει πρόθεση να μάθει περισσότερα για τον διαφημιζόμενο ή να αγοράσει κάτι, αλλά μόνο να αυξήσει τις καταγεγραμμένες εμφανίσεις της διαφήμισης
- **Παγκόσμιες απειλές**
  - **Κυβερνοτρομοκρατία & Κυβερνοπόλεμος**

Εσωτερικές απειλές: Εργαζόμενοι

- **Οι απειλές για την ασφάλεια ενός οργανισμού προέρχονται συχνά μέσα από τους ίδιους τους κόλπους του.**
  - **Εσωτερική πληροφόρηση**
  - **Πλημμελείς διαδικασίες ασφαλείας**
    - Έλλειψη γνώσεων από μέρους των χρηστών
  - **Κοινωνική μηχανική (social engineering):**
    - Παραπλάνηση χρηστών ώστε να αποκαλύψουν αυτοβούλως τους κωδικούς πρόσβασής τους· οι δράστες προσποιούνται ότι είναι καλοπροαίρετοι χρήστες ή μέλη εταιρείας και ότι χρειάζονται κάποιες πληροφορίες

Ευπάθεια του λογισμικού

- **Το εμπορικό λογισμικό έχει ελαττώματα που δημιουργούν αδυναμίες ασφάλειας.**
  - Κρυφά σφάλματα (ελαττώματα στον κώδικα του προγράμματος)
    - Ο στόχος των μηδενικών ελαττωμάτων είναι ανέφικτος επειδή δεν μπορεί να γίνει απόλυτα διεξοδική δοκιμή των μεγάλων προγραμμάτων
  - Τα ελαττώματα ανοίγουν τα δίκτυα σε εισβολείς
- **Διορθωτικές εκδόσεις (patches):** Μικρά τμήματα λογισμικού από τους προμηθευτές τα οποία διορθώνουν τα ευπαθή σημεία
  - Αλλά τα προγράμματα λογισμικού που χρησιμοποιούνται είναι τόσα πολλά που παρουσιάζονται ευπαθή σημεία με ταχύτερους ρυθμούς απ' ό,τι κυκλοφορούν διορθωτικές εκδόσεις

Η επιχειρηματική αξία της ασφάλειας και του ελέγχου

- Η παύση της λειτουργίας των υπολογιστικών συστημάτων μπορεί να οδηγήσει σε εκτενή ή και πλήρη παύση της επιχειρηματικής δραστηριότητας.
- Οι επιχειρήσεις είναι πια πιο ευάλωτες από ποτέ.
- Μια παραβίαση ασφαλείας μπορεί να υπονομεύσει σχεδόν άμεσα την αγοραία αξία της επιχείρησης.
- Τα ελλιπή μέτρα ασφαλείας και ελέγχου εγείρουν και ζητήματα υπαιτιότητας.

Νομικές και κανονιστικές απαιτήσεις για τη διαχείριση ηλεκτρονικών εγγράφων

- Οι εταιρείες έχουν πλέον νέες νομικές υποχρεώσεις για τη διατήρηση και αποθήκευση των ηλεκτρονικών εγγραφών, καθώς και για την προστασία του προσωπικού απορρήτου
  - **Νόμος HIPAA:** κανόνες για την ιατρική ασφάλεια και το προσωπικό απόρρητο
  - **Νόμος Gramm-Leach-Bliley:** Επιβάλλει στα χρηματοπιστωτικά ιδρύματα να εξασφαλίζουν την ασφάλεια και την εμπιστευτικότητα των δεδομένων των πελατών τους
  - **Νόμος Sarbanes-Oxley:** Επιβάλλει την ευθύνη των εταιρειών και των διευθυντικών στελεχών τους να διασφαλίζουν την ακρίβεια και την ακεραιότητα των χρηματοπιστωτικών πληροφοριών που χρησιμοποιούν εσωτερικά και που δημοσιεύουν εξωτερικά

Ηλεκτρονικά αποδεικτικά στοιχεία και ηλεκτρονική εγκληματολογία

- **Συχνά, τα αποδεικτικά στοιχεία είναι σε ψηφιακή μορφή**
  - Δεδομένα αποθηκευμένα σε αποθηκευτικές συσκευές υπολογιστών, μηνύματα ηλεκτρονικού ταχυδρομείου, άμεσα μηνύματα και συναλλαγές ηλεκτρονικού εμπορίου μέσω του Διαδικτύου
- **Ο κατάλληλος έλεγχος των δεδομένων μπορεί να εξοικονομήσει χρόνο και χρήμα όταν η επιχείρηση κληθεί να απαντήσει σε αίτημα των διωκτικών αρχών**
- **Ηλεκτρονική εγκληματολογία (computer forensics):**
  - Η επιστημονική συλλογή, εξέταση, πιστοποίηση, διατήρηση και ανάλυση δεδομένων από μέσα αποθήκευσης υπολογιστών, ώστε να μπορούν να χρησιμοποιηθούν ως αποδεικτικά στοιχεία σε δικαστήριο
  - Περιλαμβάνει την ανάκτηση κρυφών ή περιβάλλοντων δεδομένων (μη ορατά στον μέσο χρήστη)

Δημιουργία ενός πλαισίου δράσης για την ασφάλεια και τον έλεγχο

- **Μέτρα ελέγχου πληροφοριακών συστημάτων**
  - **Γενικά μέτρα ελέγχου**
    - Αφορούν τον σχεδιασμό, την ασφάλεια και τη χρήση των προγραμμάτων υπολογιστών, καθώς και τη γενικότερη ασφάλεια των αρχείων δεδομένων σε ολόκληρο τον οργανισμό.
    - Εφαρμόζονται σε όλες τις μηχανογραφημένες εφαρμογές.
    - Αποτελούνται από συνδυασμό υλικού, λογισμικού και μη αυτόματων διαδικασιών που δημιουργούν ένα συνολικό περιβάλλον ελέγχου.

Δημιουργία ενός πλαισίου δράσης για την ασφάλεια και τον έλεγχο

- **Τύποι γενικών μέτρων ελέγχου**
  - **Μέτρα ελέγχου λογισμικού**
  - **Μέτρα ελέγχου υλικού**
  - **Μέτρα ελέγχου λειτουργίας υπολογιστών**
  - **Μέτρα ελέγχου ασφάλειας δεδομένων**
  - **Μέτρα ελέγχου υλοποίησης**
  - **Διαχειριστικά μέτρα ελέγχου**

Δημιουργία ενός πλαισίου δράσης για την ασφάλεια και τον έλεγχο

- **Μέτρα ελέγχου εφαρμογών (application controls)**
  - Ειδικά μέτρα ελέγχου για κάθε μηχανογραφημένη εφαρμογή, όπως η μισθοδοσία ή η επεξεργασία παραγγελιών.
  - Περιλαμβάνουν αυτοματοποιημένες και μη διαδικασίες.
  - Διασφαλίζουν ότι κάθε εφαρμογή επεξεργάζεται πλήρως και με ακρίβεια μόνον εγκεκριμένα δεδομένα.
  - Σε αυτά συγκαταλέγονται:
    - **Μέτρα ελέγχου της εισόδου**
    - **Μέτρα ελέγχου της επεξεργασίας**
    - **Μέτρα ελέγχου της εξόδου**

Δημιουργία ενός πλαισίου δράσης για την ασφάλεια και τον έλεγχο

- **Εκτίμηση επικινδυνότητας**
  - Προσδιορίζει το επίπεδο κινδύνου για την εταιρεία σε περίπτωση που δεν ελέγχεται επαρκώς μια συγκεκριμένη δραστηριότητα ή διεργασία
    - **Είδη απειλών**
    - **Πιθανότητα εμφάνισης στο έτος**
    - **Πιθανές απώλειες, αξία απειλής**
    - **Εκτιμώμενη ετήσια απώλεια**

Επικίνδυνο γεγονός	Πιθανότητα	Εύρος ζημίας	Εκτιμώμενη ετήσια ζημία
Διακοπή ρεύματος	30%	5 χιλ.–200 χιλ. δολάρια	30.750 δολάρια
Κατάχρηση χρημάτων	5%	1 χιλ.–50 χιλ. δολάρια	1.275 δολάρια
Σφάλματα χρηστών	98%	200 δολάρια–40 χιλ. δολάρια	19.698 δολάρια

Δημιουργία ενός πλαισίου δράσης για την ασφάλεια και τον έλεγχο

- **Πολιτική ασφαλείας**
  - **Κατατάσσει ιεραρχικά τους κινδύνους για τις πληροφορίες**
  - **Ορίζει τους αποδεκτούς στόχους ασφάλειας**
  - **Προσδιορίζει τους μηχανισμούς για την επίτευξη αυτών των στόχων**
  - **Αποτελεί οδηγό για άλλες πολιτικές**
    - Πολιτική αποδεκτής χρήσης (acceptable use policy, AUP)
    - Πολιτική εξουσιοδότησης (authorization policy)
  - **Προβλέψεις για τη διαχείριση ταυτότητας χρηστών**

Δημιουργία ενός πλαισίου δράσης για την ασφάλεια και τον έλεγχο

- **Διαχείριση ταυτότητας χρηστών (identity management)**
  - Επιχειρηματικές διεργασίες και τεχνολογίες που πιστοποιούν την ταυτότητα των εξουσιοδοτημένων χρηστών ενός συστήματος
  - Ορίζει επίπεδα ή ρόλους για τους χρήστες και την πρόσβασή τους
  - Επιτρέπει σε κάθε χρήστη πρόσβαση μόνο σε εκείνα τα τμήματα ενός συστήματος στα οποία επιτρέπεται να εισέλθει αυτός, βάσει του ρόλου του

Δημιουργία ενός πλαισίου δράσης
για την ασφάλεια και τον έλεγχο

Κανόνες ασφάλειας για ένα σύστημα προσωπικού

Εικόνα 8-3

Τα δύο αυτά παραδείγματα αντιστοιχούν σε δύο προφίλ ασφάλειας ή πρότυπα ασφάλειας δεδομένων που μπορεί να υπάρχουν σε ένα σύστημα προσωπικού. Ανάλογα με το προφίλ ασφάλειάς του, κάθε χρήστης έχει ορισμένους περιορισμούς πρόσβασης σε διάφορα συστήματα, τοποθεσίες ή δεδομένα ενός οργανισμού.

ΠΡΟΦΙΛ ΑΣΦΑΛΕΙΑΣ 1

Χρήστης: Υπάλληλος Τμήματος Προσωπικού

Θέση: Διεύθυνση 1

Κωδικοί υπαλλήλων με αυτό το προφίλ: 00753, 27834, 37665, 44116

Περιορισμοί πεδίων δεδομένων	Τύπος πρόσβασης
Δεδομένα όλων των υπαλλήλων μόνο της Διεύθυνσης 1	Ανάγνωση και ενημέρωση
• Δεδομένα ιατρικού ιστορικού	Καμία
• Μισθολογικά δεδομένα	Καμία
• Δεδομένα συνταξιοδοτικού προγράμματος	Καμία

ΠΡΟΦΙΛ ΑΣΦΑΛΕΙΑΣ 2

Χρήστης: Προϊστάμενος Τμήματος Προσωπικού

Θέση: Διεύθυνση 1

Κωδικοί υπαλλήλων με αυτό το προφίλ: 27321

Περιορισμοί πεδίων δεδομένων	Τύπος πρόσβασης
Δεδομένα όλων των υπαλλήλων μόνο της Διεύθυνσης 1	Ανάγνωση μόνο

Σχεδιασμός ανάκαμψης από καταστροφή και σχεδιασμός επιχειρηματικής συνέχειας

- **Σχεδιασμός ανάκαμψης από καταστροφή (disaster recovery planning):** Η διαδικασία της εκπόνησης σχεδίων για την αποκατάσταση των υπολογιστικών υπηρεσιών όταν αυτές διακοπούν

Δημιουργία ενός πλαισίου δράσης
για την ασφάλεια και τον έλεγχο

Σχεδιασμός ανάκαμψης από καταστροφή και σχεδιασμός επιχειρηματικής συνέχειας

- **Σχεδιασμός για τη διασφάλιση της συνέχισης των επιχειρηματικών δραστηριοτήτων (business continuity planning):** Επικεντρώνεται στο πώς μπορεί η εταιρεία να αποκαταστήσει τις επιχειρηματικές λειτουργίες της αφού συμβεί μια καταστροφή
  - Για τα κρίσιμα συστήματα μιας επιχείρησης χρειάζονται και τα δύο σχέδια
  - Ανάλυση επιχειρηματικών συνεπειών για να προσδιοριστεί ο αντίκτυπος της διακοπής λειτουργίας για την επιχείρηση
  - Η διοίκηση πρέπει να ορίσει ποια συστήματα θα αποκατασταθούν πρώτα

Δημιουργία ενός πλαισίου δράσης
για την ασφάλεια και τον έλεγχο

Ο ρόλος της ελεγκτικής εξέτασης

- **Ελεγκτική εξέταση ΠΣΔ**
  - Εξετάζονται το συνολικό περιβάλλον ασφάλειας της επιχείρησης και τα συστήματα ελέγχου που ρυθμίζουν τα επιμέρους πληροφοριακά συστήματα
  - Επιθεωρούνται τεχνολογίες, διαδικασίες, τεκμηρίωση, εκπαίδευση και προσωπικό
  - Μπορεί να γίνει ακόμα και προσομοίωση ενός καταστροφικού γεγονότος για να δοκιμαστεί η απόκριση της τεχνολογίας, του προσωπικού των πληροφοριακών συστημάτων και των εργαζομένων της εταιρείας
  - Απαριθμεί και ιεραρχεί όλες τις αδυναμίες στα μέτρα ελέγχου και εκτιμά την πιθανότητα να παρουσιαστούν
  - Εκτιμά τον οικονομικό και οργανωσιακό αντίκτυπο κάθε απειλής

Δημιουργία ενός πλαισίου δράσης
για την ασφάλεια και τον έλεγχο

Παράδειγμα καταγραφής αδυναμιών από ελεγκτή

Εικόνα 8-4

Αυτός ο πίνακας είναι μια σελίδα από τον κατάλογο αδυναμιών που ενδέχεται να επισημάνει ένας ελεγκτής σε ένα σύστημα παροχής δανείων από μια εμπορική τράπεζα. Αυτή η μορφή αναφοράς βοηθά τους ελεγκτές να καταγράφουν και να αξιολογούν τις αδυναμίες στα μέτρα ελέγχου και δείχνει τα συμπεράσματα των συζητήσεων γι' αυτές με τα διευθυντικά στελέχη, καθώς και τις διορθωτικές ενέργειες των διευθυντικών στελεχών.

Λειτουργία: Προσωπικά δάνεια **Συντάκτης: Γ. Ιακώβου** **Προς: Θ. Βορεάδη**
Υποκατάστημα: Βόλος **Ημ. Δημιουργίας: 16 Ιουνίου 2014** **Ημ. Αναθεώρησης: 28 Ιουνίου 2014**

Φύση προβλήματος και επίδραση	Πιθανότητα σφάλματος		Γνωστοποίηση στη διοίκηση	
	Ναι/Όχι	Αιτιολογία	Ημ. αναφοράς	Ενέργεια διοίκησης
Λογαριασμοί χρηστών που έχουν χάσει τους κωδικούς πρόσβασης	Ναι	Το σύστημα μένει έκθετο σε μη εξουσιοδοτημένους χρήστες εκτός εταιρείας ή σε επιτήδειους	10/5/2014	Να διαγραφούν οι λογαριασμοί από τους οποίους λείπουν οι κωδικοί πρόσβασης.
Το δίκτυο είναι ρυθμισμένο ώστε να επιτρέπει μερικώς την κοινή χρήση αρχείων συστήματος	Ναι	Εκτίθενται κρίσιμα αρχεία του συστήματος σε εχθρούς που καταφέρνουν να συνδεθούν στο δίκτυο	10/5/2014	Να διασφαλιστεί ότι για κοινή χρήση διατίθενται μόνον οι απαιτούμενοι φάκελοι, καθώς και ότι αυτοί οι φάκελοι προστατεύονται με ισχυρούς κωδικούς πρόσβασης.
Οι διορθωτικές εκδόσεις λογισμικού μπορούν να εγκαθίστανται και να ενημερώνουν τα προγράμματα μαζικής παραγωγής χωρίς την τελική έγκριση από την ομάδα Προτύπων και Μέτρων Ελέγχου της εταιρείας	Όχι	Όλα τα προγράμματα μαζικής παραγωγής απαιτούν έγκριση από τη διοίκηση. Η ομάδα Προτύπων και Μέτρων Ελέγχου ορίζει τέτοιες περιπτώσεις ως προσωρινές		

Τεχνολογίες και εργαλεία για την προστασία των πληροφοριακών πόρων

Διαχείριση και πιστοποίηση της ταυτότητας των χρηστών

- Πιστοποίηση ταυτότητας (authentication)
  - Συστήματα με κωδικό πρόσβασης
  - Αναγνωριστικά
  - Έξυπνες κάρτες
  - Βιομετρική πιστοποίηση ταυτότητας
    - Δακτυλικά αποτυπώματα, ίριδα ματιού, φωνητικό δείγμα

Τείχη προστασίας, συστήματα ανίχνευσης εισβολών και λογισμικό κατά των ιών

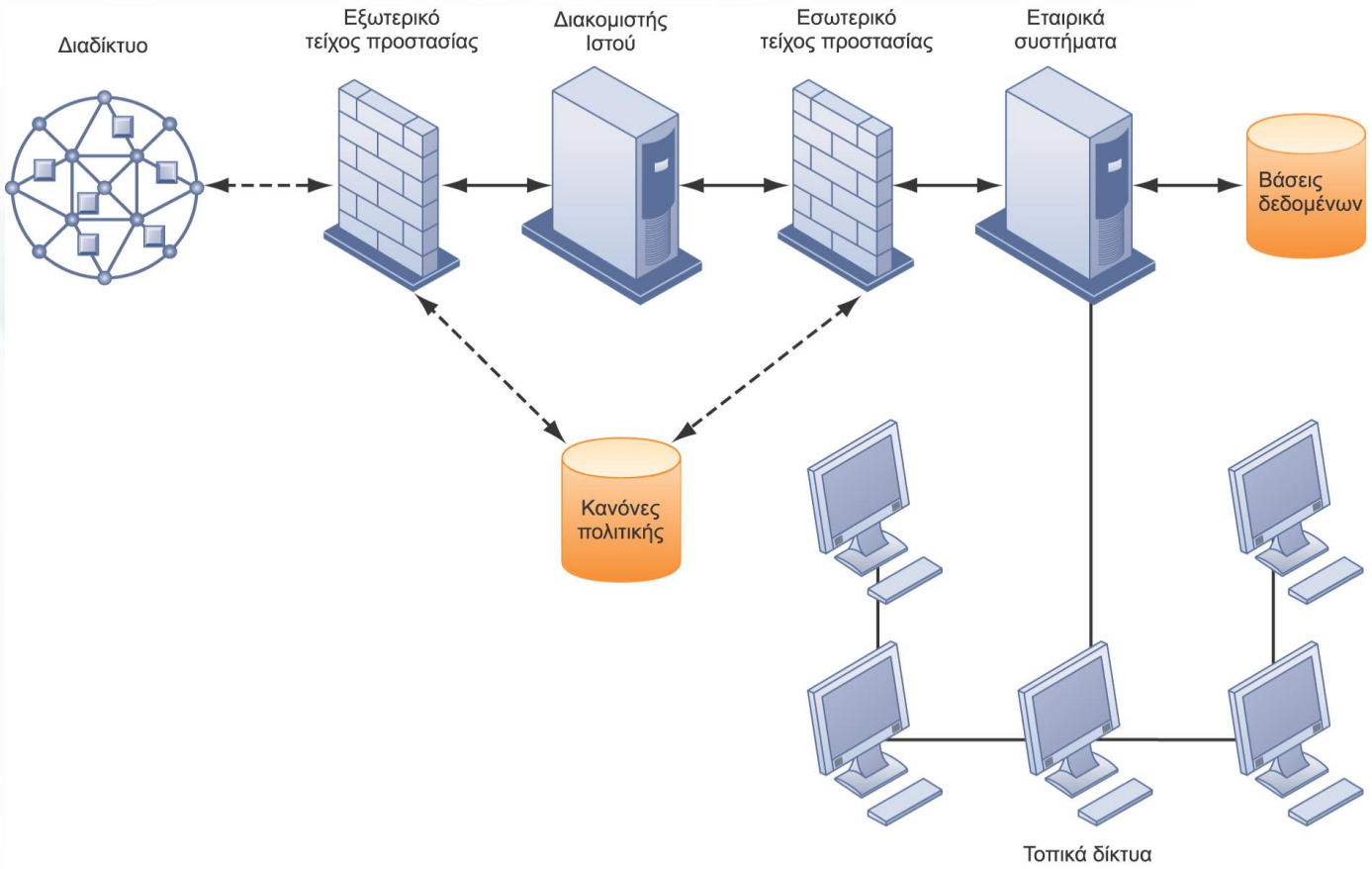
- Τείχος προστασίας (firewall):
  - Συνδυασμός υλικού και λογισμικού που ελέγχει τη ροή της εισερχόμενης και της εξερχόμενης κυκλοφορίας δεδομένων από το δίκτυο
  - Στις τεχνολογίες συγκαταλέγονται:
    - Το φιλτράρισμα πακέτων (packet filtering)
    - Η καταστασιακή επιθεώρηση (stateful inspection)
    - Η μετάφραση διευθύνσεων δικτύου (network address translation, NAT)
    - Το φιλτράρισμα εφαρμογών με διαμεσολαβητή (application proxy filtering)

Τεχνολογίες και εργαλεία για την προστασία των πληροφοριακών πόρων

Ένα εταιρικό τείχος προστασίας

Εικόνα 8-5

Το τείχος προστασίας παρεμβάλλεται ανάμεσα στο ιδιωτικό δίκτυο μιας εταιρείας και στο δημόσιο Διαδίκτυο, ή άλλο μη έμπιστο δίκτυο, για την προστασία από μη εξουσιοδοτημένη κυκλοφορία.



Τεχνολογίες και εργαλεία για την προστασία των πληροφοριακών πόρων

- **Συστήματα ανίχνευσης εισβολών (intrusion detection systems):**
  - Παρακολουθούν τα πιο ευάλωτα σημεία των εταιρικών δικτύων ώστε να ανιχνεύουν και να αποτρέπουν συνεχώς τους εισβολείς.
  - Εξετάζουν τα γεγονότα τη στιγμή που συμβαίνουν, για να ανακαλύπτουν επιθέσεις ασφάλειας που βρίσκονται σε εξέλιξη.
- **Λογισμικό κατά των ιών και αντικατασκοπευτικό λογισμικό (antivirus and antispyware software):**
  - Ελέγχουν αν υπάρχει κακόβουλο λογισμικό στον υπολογιστή και συχνά μπορούν επίσης να απομακρύνουν.
  - Απαιτούν συνεχή ενημέρωση.
- **Συστήματα ενιαίας διαχείρισης απειλών (unified threat management, UTM)**

Ασφάλεια στα ασύρματα δίκτυα

- **Η ασφάλεια WEP βελτιώνεται:**
  - Χρειάζεται να ενεργοποιηθεί
  - Πρέπει να εκχωρηθεί ένα (μοναδικό) όνομα στο SSID του δικτύου
  - Πρέπει να χρησιμοποιείται σε συνδυασμό με την τεχνολογία VPN
- **Η Wi-Fi Alliance οριστικοποίησε το πρότυπο WPA2, το οποίο αντικαθιστά το WEP με ισχυρότερες προδιαγραφές ασφαλείας**
  - Κλειδιά που αλλάζουν συνεχώς
  - Κρυπτογραφημένο σύστημα με κεντρικό διακομιστή πιστοποίησης ταυτότητας

Τεχνολογίες και εργαλεία για την προστασία των πληροφοριακών πόρων

Κρυπτογράφηση και υποδομή δημόσιων κλειδιών

- Κρυπτογράφηση (encryption):
  - Η διαδικασία του μετασχηματισμού απλού κειμένου ή δεδομένων σε κρυπτογραφημένο κείμενο που δεν μπορεί να διαβαστεί από κανέναν παρά μόνο τον προβλεπόμενο παραλήπτη
  - Δύο μέθοδοι κρυπτογράφησης στα δίκτυα
    - Ασφαλές Επίπεδο Υποδοχής (SSL) και το πρωτόκολλο Ασφάλειας Επιπέδου Μεταφοράς (TLS), που διαδέχθηκε το πρώτο
    - Πρωτόκολλο Ασφαλούς Μεταφοράς Υπερκειμένου (Secure Hypertext Transfer Protocol, S-HTTP)

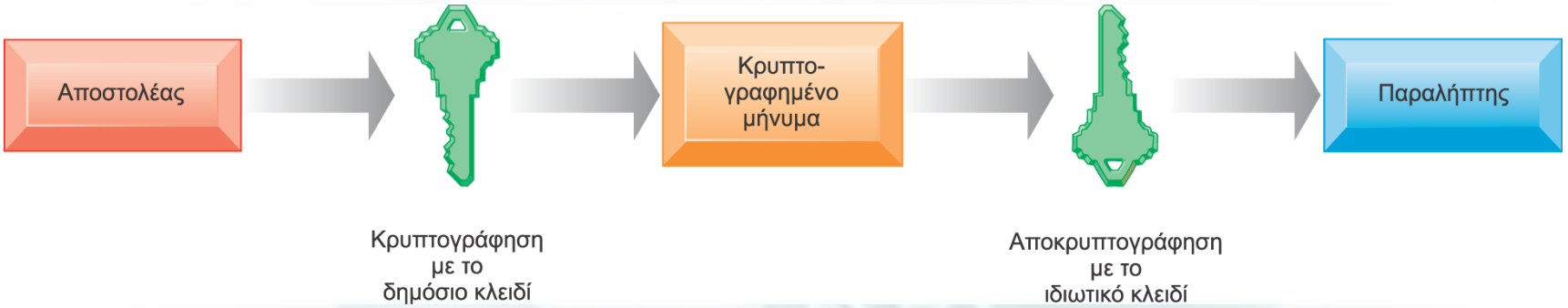
Τεχνολογίες και εργαλεία για την προστασία των πληροφοριακών πόρων

Κρυπτογράφηση και υποδομή δημόσιων κλειδιών

- **Δύο μέθοδοι κρυπτογράφησης**
  - **Κρυπτογράφηση με συμμετρικό κλειδί (symmetric key encryption)**
    - Αποστολέας και παραλήπτης χρησιμοποιούν το ίδιο, κοινό κλειδί
  - **Κρυπτογράφηση με δημόσιο κλειδί (public key encryption)**
    - Βασίζεται στη χρήση δύο κλειδιών: ενός κοινόχρηστου (ή δημόσιου) και ενός ιδιωτικού
    - Ο αποστολέας κωδικοποιεί το μήνυμα με το δημόσιο κλειδί του παραλήπτη
    - Ο παραλήπτης χρησιμοποιεί το ιδιωτικό κλειδί του για να το αποκρυπτογραφήσει

Τεχνολογίες και εργαλεία για την προστασία των πληροφοριακών πόρων

Κρυπτογράφηση με δημόσιο κλειδί



Το σύστημα κρυπτογράφησης με δημόσιο κλειδί μπορεί να θεωρηθεί ως μια σειρά δημόσιων και ιδιωτικών κλειδιών, τα οποία κλειδώνουν τα δεδομένα όταν αυτά μεταδίδονται και τα ξεκλειδώνουν κατά την παραλαβή τους. Ο αποστολέας εντοπίζει το δημόσιο κλειδί του παραλήπτη σε έναν κατάλογο και το χρησιμοποιεί για να κρυπτογραφήσει ένα μήνυμα. Το μήνυμα στέλνεται κρυπτογραφημένο μέσω του Διαδικτύου ή ενός ιδιωτικού δικτύου. Όταν φτάσει στον προορισμό του, ο παραλήπτης αποκρυπτογραφεί τα δεδομένα με το δικό του ιδιωτικό κλειδί και διαβάζει το μήνυμα.

Εικόνα 8-6

Τεχνολογίες και εργαλεία για την προστασία των πληροφοριακών πόρων

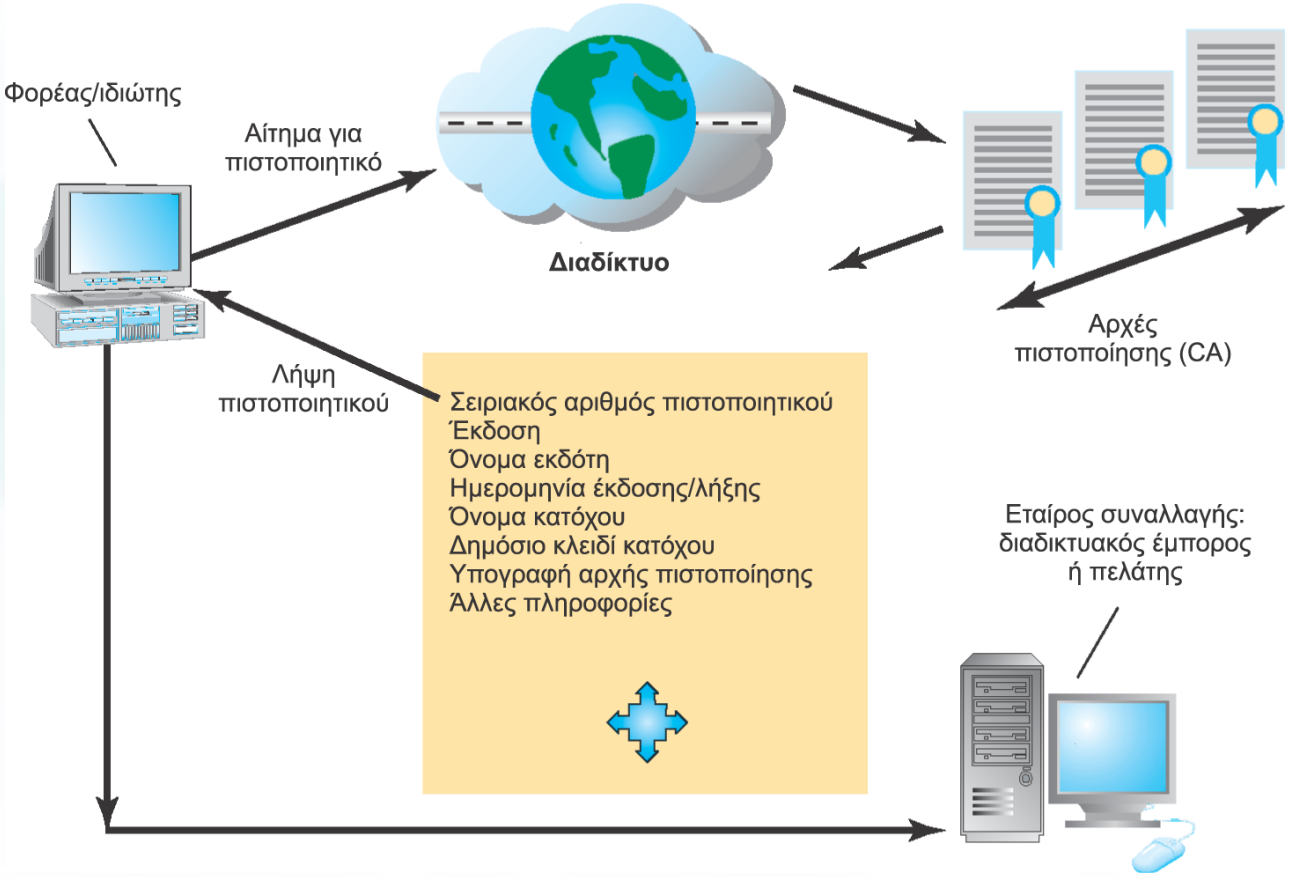
- **Ψηφιακό πιστοποιητικό:**
  - Αρχείο δεδομένων που χρησιμοποιείται για την εξακρίβωση της ταυτότητας χρηστών και ηλεκτρονικών πόρων με στόχο την προστασία σε ηλεκτρονικές συναλλαγές
  - Για την επαλήθευση της ταυτότητας ενός χρήστη χρησιμοποιεί μια αρχή πιστοποίησης (certificate authority, CA)
  - Η αρχή πιστοποίησης επιβεβαιώνει την ταυτότητα του χρήστη και αποθηκεύει τα στοιχεία στον διακομιστή της, ο οποίος δημιουργεί ένα κρυπτογραφημένο ψηφιακό πιστοποιητικό που περιέχει πληροφορίες αναγνώρισης του κατόχου και ένα αντίγραφο του δημόσιου κλειδιού του κατόχου
- **Υποδομή δημοσίων κλειδιών (public key infrastructure, PKI)**
  - Η χρήση κρυπτογράφησης δημόσιου κλειδιού σε συνεργασία με μια αρχή πιστοποίησης
  - Χρησιμοποιείται ευρέως στο η-εμπόριο

Τεχνολογίες και εργαλεία για την προστασία των πληροφοριακών πόρων

Ψηφιακά πιστοποιητικά

Εικόνα 8-7

Τα ψηφιακά πιστοποιητικά χρησιμοποιούνται για να εξακριβώνεται η ταυτότητα ανθρώπων ή ηλεκτρονικών πόρων. Προστατεύουν τις ηλεκτρονικές συναλλαγές προσφέροντας ασφαλείς, κρυπτογραφημένες ηλεκτρονικές επικοινωνίες.



Τεχνολογίες και εργαλεία για την προστασία των πληροφοριακών πόρων

Εξασφάλιση της διαθεσιμότητας των συστημάτων

- **Η άμεση ηλεκτρονική επεξεργασία των συναλλαγών απαιτεί διαθεσιμότητα 100%, χωρίς χρόνο εκτός λειτουργίας.**
- **Συστήματα ανεκτικά σε βλάβες (fault-tolerant computer systems)**
  - Για αδιάλειπτη διαθεσιμότητα, π.χ. στο χρηματιστήριο
  - Περιέχουν πρόσθετα εξαρτήματα υλικού, εφαρμογές λογισμικού και συστήματα παροχής ηλεκτρικού ρεύματος, δημιουργώντας ένα περιβάλλον που προσφέρει συνεχή, αδιάλειπτη υπηρεσία
- **Υπολογιστικά περιβάλλοντα υψηλής διαθεσιμότητας (high-availability computing)**
  - Ανακάμπτουν γρήγορα από κατάρρευση
  - Ελαχιστοποιούν, δεν εξαλείφουν, τον χρόνο εκτός λειτουργίας

Εξασφάλιση της διαθεσιμότητας των συστημάτων

- **Υπολογιστική προσανατολισμένη στην ανάκαμψη (recovery-oriented computing)**
  - Ο σχεδιασμός συστημάτων ώστε να μπορούν να ανακάμπτουν γρήγορα, με δυνατότητες που βοηθούν τους χειριστές να εντοπίζουν με ακρίβεια τις πηγές βλαβών σε πολυστοιχειακά συστήματα και να διορθώνουν εύκολα τα σφάλματά τους
- **Έλεγχος κυκλοφορίας δικτύου**
  - Επιθεώρηση πακέτων σε βάθος (deep packet inspection, DPI) – για τον αποκλεισμό π.χ. βίντεο και μουσικής
- **Εξωτερική ανάθεση ασφάλειας**
  - Πάροχοι υπηρεσιών ασφάλειας (managed security service providers, MSSP)

Ζητήματα ασφάλειας στην υπολογιστική νέφους

- **Υπολογιστική νέφους (cloud computing)**
  - Η υπολογιστική νέφους, που χαρακτηρίζεται από διασπορά, δυσχεραίνει την παρακολούθηση της μη εξουσιοδοτημένης δραστηριότητας
  - Οι χρήστες του νέφους πρέπει να ζητούν τεκμηριωμένες διαδικασίες ασφαλείας και προστασίας του προσωπικού απορρήτου, π.χ. κρυπτογράφηση
  - Σύναψη συμβάσεων επιπέδου παροχής υπηρεσιών (SLA)

Τεχνολογίες και εργαλεία για την προστασία των πληροφοριακών πόρων

Ζητήματα ασφάλειας στην ψηφιακή πλατφόρμα της κινητής τηλεφωνίας και των φορητών συσκευών

- **Κινητή τηλεφωνία και φορητές συσκευές**
  - Εργαλεία διαχείρισης φορητών συσκευών και κινητών: ταυτοποίηση και καταγραφή
  - Τεχνολογία πρόληψης απώλειας δεδομένων
  - Πολιτικές για την ασφάλεια σε φορητές συσκευές και κινητά: περιβάλλον, λογισμικό, διαδικασίες, προϊόντα ασφαλείας
  - Κρυπτογράφηση
  - Μοντέλο BYOD (Bring Your Own Device)
  - Προϊόντα λογισμικού για την προστασία φορητών συσκευών και κινητών

Περ. Μελέτη: Τεχνολογία
BYOD (Bring Your Own Device): Ασφαλές; Όχι και τόσο!

- **Διαβάστε την περιπτωσιολογική μελέτη και μετά συζητήστε τις παρακάτω ερωτήσεις:**
  - Κάποιοι υποστηρίζουν ότι το έξυπνο τηλέφωνο είναι ένας μικρός υπολογιστής στην παλάμη μας. Να συζητήσετε τις συνέπειες αυτής της πρότασης όσον αφορά την ασφάλεια.
  - Ποιοι ανθρώπινοι, οργανωσιακοί και τεχνολογικοί παράγοντες πρέπει να αντιμετωπιστούν στην ασφάλεια των έξυπνων τηλεφώνων;
  - Ποια προβλήματα προκαλούν στις επιχειρήσεις οι αδυναμίες των έξυπνων τηλεφώνων όσον αφορά την ασφάλεια;
  - Ποια μέτρα πρέπει να λάβουν οι μεμονωμένοι χρήστες και οι επιχειρήσεις ώστε να καταστήσουν πιο ασφαλή τα έξυπνα τηλέφωνά τους;

Εξασφάλιση της ποιότητας του λογισμικού

- **Μετρήσεις λογισμικού:** Αντικειμενικές αξιολογήσεις κάθε συστήματος με τη μορφή ποσοτικών στοιχείων, όπως:
  - Πλήθος συναλλαγών
  - Χρόνος απόκρισης
  - Πόσες επιταγές μισθοδοσίας τυπώνονται ανά ώρα
  - Ο αριθμός των γνωστών σφαλμάτων για κάθε εκατό γραμμές κώδικα
- **Έγκαιρες και τακτικές δοκιμές**
- **Περιήγηση (walkthrough):** Η ανασκόπηση των εγγράφων των προδιαγραφών ή του σχεδιασμού από μια μικρή ομάδα προσεκτικά επιλεγμένων καταρτισμένων ατόμων
- **Αποσφαλμάτωση (debugging):** Η διαδικασία εξάλειψης των σφαλμάτων