ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ ΕΡΕΥΝΑΣ ΚΑΙ ΘΡΗΣΚΕΥΜΑΤΩΝ
ΙΝΣΤΙΤΟΥΤΟ ΕΚΠΑΙΔΕΥΤΙΚΗΣ ΠΟΛΙΤΙΚΗΣ

Κατσούλας Ν., Όροβας Χ., Παναγιωτίδης Σ.

ΛΕΙΤΟΥΡΓΙΚΑ ΣΥΣΤΗΜΑΤΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Β' Τάξη ΤΟΜΕΑΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΕΠΑ.Λ.

ΟΔΗΓΙΕΣ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

ΙΝΣΤΙΤΟΥΤΟ ΕΚΠΑΙΔΕΥΤΙΚΗΣ ΠΟΛΙΤΙΚΗΣ
Πρόεδρος: **Γκλαβάς Σωτήριος**

ΓΡΑΦΕΙΟ ΕΡΕΥΝΑΣ, ΣΧΕΔΙΑΣΜΟΥ ΚΑΙ ΕΦΑΡΜΟΓΩΝ Β΄
Προϊστάμενος: **Μάραντος Παύλος**
Επιστημονικά Υπεύθυνος: **Δρ. Τσαπέλας Θεοδόσιος**, Σύμβουλος Β΄ Πληροφορικής ΙΕΠ.

ΣΥΓΓΡΑΦΙΚΗ ΟΜΑΔΑ:
Κατσούλας Νικόλαος, Εκπαιδευτικός Πληροφορικής
Δρ. Όροβας Χρήστος, Εκπαιδευτικός Πληροφορικής
Παναγιωτίδης Σωτήρης, Εκπαιδευτικός Πληροφορικής

ΕΠΙΜΕΛΕΙΑ - ΣΥΝΤΟΝΙΣΜΟΣ ΟΜΑΔΑΣ:
Κωτσάκης Σταύρος, Σχολικός σύμβουλος πληροφορικής

ΦΙΛΟΛΟΓΙΚΗ ΕΠΙΜΕΛΕΙΑ:
Δελής Φίλιππος, Εκπαιδευτικός Φιλόλογος

ΠΕΡΙΕΧΟΜΕΝΑ

Πρόλογος

Αγαπητοί συνάδελφοι,

Οι σημειώσεις που εκπονήθηκαν πρόσφατα για το μάθημα Λειτουργικά Συστήματα και Ασφάλεια Πληροφοριακών Συστημάτων της Β' Τάξης των ειδικοτήτων «Τεχνικός Εφαρμογών Πληροφορικής», «Τεχνικός Εφαρμογών Λογισμικού» και «Τεχνικός Η/Υ και Δικτύων» του Τομέα Πληροφορικής των ΕΠΑ.Λ αποτελούν ένα συμπλήρωμα και μια προσπάθεια ανανέωσης του περιεχομένου του αντίστοιχου βιβλίου.

Ακολουθούν το νέο αναλυτικό πρόγραμμα σπουδών του μαθήματος και προσθέτουν δύο νέα κεφάλαια αφιερωμένα στην Ασφάλεια Πληροφοριακών Συστημάτων και στη χρήση των εικονικών μηχανών για πειραματισμούς στο εργαστήριο.

Σε μια προσπάθεια ομαλής μετάβασης στο νέο περιεχόμενο οι σημειώσεις ακολουθούν το υπάρχον βιβλίο στα περισσότερα σημεία στα οποία δεν υπάρχουν σημαντικές αλλαγές ενώ ενσωματώνουν σύγχρονες δραστηριότητες όπου αυτό είναι απαραίτητο.

Είναι κατανοητό ότι η ταυτόχρονη χρήση δύο εγχειριδίων ίσως να προκαλέσει σύγχυση σε συναδέλφους εκπαιδευτικούς αλλά και στους μαθητές. Για αυτό το λόγο ο τρέχον οδηγός έχει ως στόχο να βοηθήσει στην αναγκαία αντιστοίχιση της ύλης μεταξύ των σημειώσεων και του βιβλίου και να προτείνει διδακτικές προσεγγίσεις με βάση το νέο αναλυτικό πρόγραμμα σπουδών. Τα κεφάλαια του τρέχοντος οδηγού ακολουθούν τις ενότητες του νέου ΑΠΣ και δίνουν τις απαραίτητες οδηγίες.

Αυτό που θα πρέπει να γίνει κατανοητό είναι ότι ο λόγος συγγραφής των σημειώσεων είναι η ανανέωση κάποιων σημείων της ύλης και όχι η πλήρης αντικατάσταση της. Είναι η υποβοήθηση του έργου του εκπαιδευτικού και όχι η δυσχέρανση του. Ο τελικός κριτής του μέσου και της διαδικασίας η οποία θα χρησιμοποιηθεί παραμένει πάντα ο εκπαιδευτικός του μαθήματος που γνωρίζει καλύτερα από όλους τις ιδιαιτερότητες και τις εκπαιδευτικές ανάγκες της τάξης του.

Οι συγγραφείς

Ενότητα 1

Βασικές Εισαγωγικές Έννοιες

Χρόνος: 12 ώρες (4Θ + 8Ε)

Η ενότητα αυτή αντιστοιχεί στην πρώτη ενότητα του προηγούμενου αναλυτικού προγράμματος σπουδών και παρέχονται επίσης τέσσερις επιπλέον ώρες δηλαδή από τις 8 ώρες έχει πάει στις 12 συνολικά θεωρία και εργαστήριο.

Η αντιστοίχιση της ύλης γίνεται σύμφωνα με τον παρακάτω πίνακα:

Βασικές Εισαγωγικές Έννοιες	
Κεφάλαια και παράγραφοι από σημειώσεις	Κεφάλαια και παράγραφοι από βιβλίο
Κεφάλαιο 1	Μέρος Α, Κεφάλαιο 1

Στις σημειώσεις ακολουθείται σε γενικές γραμμές το πρώτο κεφάλαιο του βιβλίου ενώ δίνεται έμφαση στη διαφοροποίηση του Λογισμικού Συστήματος από το Λογισμικό Εφαρμογών, στην έννοια του ανοικτού λογισμικού και επίσης αναφέρονται όροι όπως η υπολογιστική πλέγματος (grid computing) και νέφους (cloud computing).

Προτάσεις για την κατανομή της ύλης σε διδακτικές ώρες

Θεωρία

α/α	Περιεχόμενο
1	Ρόλος και αναγκαιότητα Λειτουργικών Συστημάτων Παράγραφοι 1.1, 1.2 και 1.3 από σημειώσεις (εναλλακτικά παράγραφοι 1.1 και 1.1.1, σελίδα 16 από βιβλίο). Ερωτήσεις 1,2,3,4, 17, 18, 19
2	Δομικά μέρη ενός Λ.Σ Παράγραφοι 1.4, 1.5, 1.6 από σημειώσεις (εναλλακτικά παράγραφοι 1.1.2, 1.1.3, 1.1.4, σελίδες 17-18 από βιβλίο). Ερωτήσεις 5,8,9
3	Κατηγορίες Λ.Σ Παράγραφος 1.7 από σημειώσεις (εναλλακτικά παράγραφοι 1.1.5, 1.1.6, 1.2.2 από βιβλίο). Ερωτήσεις 11, 14, 15, 16

4	Ιστορική αναδρομή και σύνοψη κεφαλαίου Παράγραφος 1.8 από σημειώσεις (εναλλακτικά 1.2.1 από βιβλίο). Ερωτήσεις 6, 7, 10, 12, 13

Εργαστήρια

Οι εννέα δραστηριότητες που προτείνονται στο 1ο κεφάλαιο των σημειώσεων μπορούν να κατανεμηθούν ομοιόμορφα στα οκτώ εργαστήρια που αντιστοιχούν σε αυτή την ενότητα. Ο στόχος είναι η εξοικείωση με

- τις δυνατότητες που μας παρέχει ένα λειτουργικό σύστημα,
- την διαδικασία εκκίνησης του,
- την κλήση εφαρμογών και
- την παραμετροποίηση του περιβάλλοντος εργασίας.

Προτείνεται η χρήση ομαδοσυνεργατικών δραστηριοτήτων και του εποικοδομητισμού ως κύρια διδακτική προσέγγιση. Σε συνεργασία με τους υπεύθυνους των εργαστηρίων μπορείτε να πειραματιστείτε με την εκκίνηση χωρίς σκληρό δίσκο εξηγώντας τα μηνύματα που εμφανίζονται, την χρήση δισκέττας εκκίνησης (αν υπάρχει δυνατότητα), την χρήση CD εκκίνησης (για Ubuntu κυρίως). Επίσης μπορείτε να δείξετε παραδείγματα από διαμόρφωση BIOS (ή UEFI) όσον αφορά τις δραστηριότητες προ εκκίνησης του λειτουργικού συστήματος.

Μπορείτε επίσης να ετοιμάσετε ένα CD εκκίνησης με την εργαλειοθήκη Hiren's (http://www.hirensbootcd.org/download/) και να δείξετε τις δυνατότητες που παρέχονται. Συνιστάται όμως μεγάλη προσοχή στη χρήση των εργαλείων που περιέχονται σε αυτό.

Ενότητα 2

Οργάνωση Συστήματος Αρχείων

Χρόνος: 21 ώρες (7Θ + 14Ε)

Η ενότητα αυτή αντιστοιχεί στην ενότητα «Οργάνωση του συστήματος αρχείων» του προηγούμενου αναλυτικού προγράμματος σπουδών. Οι ώρες που αντιστοιχούν είναι περίπου ίδιες και στα δύο ΑΠΣ. Έτσι με το νέο διατίθενται 21 ώρες έναντι 22 του προηγούμενου.

Η αντιστοίχιση της ύλης γίνεται σύμφωνα με τον παρακάτω πίνακα:

Διαχείριση Συστήματος Αρχείων	
Κεφάλαια και παράγραφοι από σημειώσεις	Κεφάλαια και παράγραφοι από βιβλίο
Κεφάλαιο 2	Μέρος Α, παράγραφος 2.1 Μέρος Β-Κεφάλαια 3 και 4

Στις σημειώσεις επιχειρήθηκε να δοθεί μια ενημερωμένη εικόνα της οργάνωσης του συστήματος αρχείων με αναφορά σε σύγχρονα μέσα αποθήκευσης (USB flash disks, SSD) και στη χρήση διαμερισμάτων στα οποία μπορούν να διαχωρισθούν οι σκληροί δίσκοι. Η παρουσίαση των εντολών και των χειρισμών που μπορούν να πραγματοποιηθούν γίνεται με αναφορά στο βιβλίο που χρησιμοποιείται καθώς υπάρχει μικρή διαφοροποίηση τους.

Προτάσεις για την κατανομή της ύλης σε διδακτικές ώρες

Θεωρία

α/α	Περιεχόμενο
1	Εισαγωγή στη διαχείριση αρχείων και Σύστημα Αρχείων Παράγραφοι 2.1.1, 2.1.2 και 2.1.3 από Σημειώσεις (εναλλακτικά παράγραφοι 2.1.1, 2.1.2 και 2.1.3 από βιβλίο).
2	Τι προσφέρει το Σύστημα Αρχείων Παράγραφοι 2.1.4 από Σημειώσεις (εναλλακτικά 2.1.4 και 2.1.5 από βιβλίο)
3	Τύποι αρχείων και Κατανομή αρχείων σε συσκευές Παράγραφοι 2.1.5 και 2.2 από Σημειώσεις (εναλλακτικά 2.1.7 και 2.1.8 από βιβλίο)
4	Φυσική οργάνωση δίσκων και χωρισμός τους σε διαμερίσματα Παράγραφοι 2.3 και 2.3.1 από Σημειώσεις
5	Είδη Συστημάτων αρχείων και Προσπέλαση δίσκων Παράγραφοι 2.3.2 και 2.4 από Σημειώσεις (εναλλακτικά για την 2.4 μόνο, η 2.1.10

	του βιβλίου)
6	Καταχώρηση περιοχών του δίσκου Παράγραφοι 2.4.1 από Σημειώσεις (εναλλακτικά η 2.1.11 από βιβλίο)
7	Κατακερματισμός και Ασφάλεια συστήματος Παράγραφοι 2.4.2 και 2.5 από Σημειώσεις (εναλλακτικά για την 2.4.2 η 2.1.12 του βιβλίου)

Εργαστήρια

α/α	Δραστηριότητα	Βοηθητικό υλικό
1	Παραδείγματα της Παρ. 2.1.6 βιβλίου (Windows)	
2	Πίνακας Ελέγχου, Διαχείριση ενέργειας (Windows)	
3	Παραδείγματα της Παρ. 2.1.6 βιβλίου (Linux) Ρυθμίσεις Συστήματος (Πίνακας Ελέγχου), Διαχείριση ενέργειας (Linux)	
4	Δραστηριότητς 1-7 των σημειώσεων. Για την 6η (σε Windows): άνοιγμα του Windows Explorer επιλογή Υπολογιστής προβολή: Λεπτομέρειες δεξί κλικ στην γραμμή με |Όνομα | Τύπος | επιλογή από το μενού που θα ανοίξει *Σύστημα Αρχείων*	
5	Μέρος Β' βιβλίου – 3.2, 3.2.1, 3.2.6 και 3.2.8	http://www.it.uom.gr/teaching/linux/linux_gr_card-1.pdf
6	Μέρος Β' βιβλίου – 3.2.9 και 3.2.10	
7	Μέρος Β' βιβλίου – 5 και 3.2.5	https://www.washington.edu/computing/unix/vi.html
8	Μέρος Β' βιβλίου – 3.2.2	
9	Μέρος Β' βιβλίου – 3.2.3 και 3.2.7	
10	Μέρος Β' βιβλίου – 3.2.12	https://en.wikipedia.org/wiki/Chmod
11	Μέρος Β' βιβλίου – 4.1 και 4.2	
12	Μέρος Β' βιβλίου – 6.1.1	
13	Μέρος Β' βιβλίου – 7.1.1	
14	Μέρος Β' βιβλίου – 7.1.2	

Ενότητα 3

Διεργασίες και Διαχείριση κεντρικής μνήμης

Χρόνος: 12 ώρες (4Θ + 8Ε)

Η ενότητα αυτή συμπεριλαμβάνει την ενότητα Διαχείρισης Κεντρικής Μνήμης και τις διεργασίες από τα ειδικά θέματα του προηγούμενου προγράμματος σπουδών. Έχει δοθεί έμφαση στη χρήση παραδειγμάτων και δραστηριοτήτων από δύο γνωστά λειτουργικά συστήματα, τα Windows 7 (με δυνατότητα χρήσης και των XP) και το Ubuntu 12.04.

Η αντιστοίχιση της ύλης γίνεται σύμφωνα με τον παρακάτω πίνακα:

Διεργασίες και διαχείριση Κεντρικής Μνήμης	
Κεφάλαια και παράγραφοι από σημειώσεις	Κεφάλαια και παράγραφοι από βιβλίο
Παράγραφοι 3.1, 3.2	Μέρος Α, Κεφάλαιο 4
Παράγραφος 3.3	Μέρος Α, Κεφάλαιο 5

Καθώς ο συνολικός χρόνος έχει μειωθεί από τις 14 (και περισσότερο) ώρες στις 12 προτείνεται μια νέα κατανομή της ύλης σε διδακτικές ώρες όπως αναλύεται στη συνέχεια.

Προτάσεις για την κατανομή της ύλης σε διδακτικές ώρες

Θεωρία

α/α	Περιεχόμενο
1	Διεργασίες Παράγραφοι 3.1, 3.2, 3.2.1 και 3.2.2 από σημειώσεις (εναλλακτικά παράγραφος 4.1, σελίδες 72 και 73, από βιβλίο). Ερωτήσεις 1-10.
2	Συγχρονισμός και χρονοδρομολόγηση Παράγραφοι 3.2.3 και 3.2.4 από σημειώσεις (εναλλακτικά παράγραφοι 4.1.1 και 4.1.2, σελίδες 74-77, από βιβλίο). Ερωτήσεις 11-15.
3	Διαχείριση Μνήμης Παράγραφοι 3.3, 3.3.1 και 3.3.2 από σημειώσεις (εναλλακτικά παράγραφοι 5.1, 5.2, 5.3, 5.4, 5.5 και 5.6, σελίδες 82-86, από βιβλίο). Ερωτήσεις 16-19.
4	Σελιδοποίηση και κατάτμηση

	Παράγραφος 3.3.3 από σημειώσεις (εναλλακτικά παράγραφοι 5.7, 5.8 και 5.9, σελίδες 86-92, από βιβλίο). Ερωτήσεις 20-24.

Εργαστήρια

α/α	Περιεχόμενο
Εργαστήρια 1,2,3 και 4	Δραστηριότητες 1, 2, 3 ,6 και 8. Ειδικότερα για τη δραστηριότητα 6 μπορείτε να «κατεβάσετε» από το διαδίκτυο και την έκδοση του Process Explorer για Linux. Πειραματιστείτε ιδιαίτερα με την προτεραιότητα των διεργασιών.
Εργαστήρια 5,6,7,8	Δραστηριότητες 4, 5 και 9. Επαναλάβετε την δραστηριότητα 6 αναφερόμενοι τώρα και στις πληροφορίες σχετικά με τη μεταγωγή περιβάλλοντος που σας παρέχονται από το πρόγραμμα.

Ενότητα 4

Διαχείριση Συσκευών Ε/Ε

Χρόνος: 6 ώρες (2Θ + 4Ε)

Η ενότητα αυτή αντιστοιχεί στην ενότητα «Διαχείριση Εισόδου-Εξόδου (I/O)» του προηγούμενου αναλυτικού προγράμματος σπουδών. Η αντιστοίχηση της ύλης ανάμεσα στο βιβλίο και τις σημειώσεις είναι η εξής:

Διαχείριση Συσκευών Ε/Ε	
Κεφάλαια και παράγραφοι από σημειώσεις	Κεφάλαια και παράγραφοι από βιβλίο
Κεφάλαιο 4	Μέρος Α, Κεφάλαιο 3

Για αυτή την ενότητα οι ώρες στο προηγούμενο ΑΠΣ ήταν 16 και στο τρέχον είναι 6. Προτείνεται λοιπόν η νέα κατανομή της ύλης σε διδακτικές ώρες να είναι όπως φαίνεται στη συνέχεια.

Προτάσεις για την κατανομή της ύλης σε διδακτικές ώρες

Θεωρία

α/α	Περιεχόμενο
1	Είσοδος/Έξοδος και Περιφερειακές Συσκευές Παράγραφοι 4.1 και 4.2 από σημειώσεις (εναλλακτικά παράγραφοι 3.1.1, 3.1.2 και 3.1.3, σελίδες 60-62, από βιβλίο). Ερωτήσεις 1-4. Ένα ενδιαφέρον και μάλλον διασκεδαστικό βίντεο σχετικά με την επικοινωνία Υλικού και Λογισμικού που μπορείτε να προβάλλετε στην αίθουσα μέσω του YouTube είναι το *https://www.youtube.com/watch?v=rNl9ol_rPMs (How Does Hardware and Software Communicate?)*
2	Ελεγκτές και διαχείριση συσκευών από το Λ.Σ Παράγραφοι 4.3 και 4.4 από σημειώσεις (εναλλακτικά παράγραφοι 3.1.4, 3.2 και 3.3, σελίδες 63-65, από βιβλίο). Ερωτήσεις 5-8.

Εργαστήρια

α/α	Περιεχόμενο

Εργαστήρια 1,2	Δραστηριότητες 1, 2, 3 ,7 και 8.
Εργαστήρια 3,4	Δραστηριότητες 4,5,6 ,9 και 10. Για την δραστηριότητα 4 θα είναι χρήσιμο αν είχατε κάποια μη λειτουργική συσκευή που θα μπορούσατε να χρησιμοποιήσετε ως εποπτικό υλικό (πχ παλιό πληκτρολόγιο ή ποντίκι κτλ) Για την δραστηριότητα 6 συνεννοηθείτε με τον υπεύθυνο εργαστηρίου ή/και το οικείο ΚΕΠΛΗΝΕΤ και προμηθευτείτε μια εναλλακτική κάρτα γραφικών που μπορείτε να χρησιμοποιήσετε. Τοποθετείστε πρώτα την κάρτα χωρίς τους οδηγούς για να παρατηρήσετε την συμπεριφορά του Η/Υ. Συνεχίστε με την διαδικασία εύρεσης και εγκατάστασης των κατάλληλων οδηγών ως συλλογική δραστηριότητα στην τάξη.

Ενότητα 5

Ασφάλεια Πληροφοριακών Συστημάτων

[20 Ώρες - 8Θ + 12Ε]

Σκοπός της ενότητας είναι να δουν συνοπτικά οι μαθητές όλες τις παραμέτρους της Ασφάλειας ενός Πληροφοριακού Συστήματος και όχι η σε βάθος γνώση όλων αυτών γιατί αυτό θα απαιτούσε ολόκληρο βιβλίο.

Επιπλέον πληροφορίες, βοηθήματα και συζητήσεις μπορούν να αναζητηθούν στα Blogs:

1. http://blogs.sch.gr/virtualization
2. http://blogs.sch.gr/infosec

Στη συνέχεια της ενότητας όπου υπάρχει αναφορά σε ΛΣ Linux θα αντιστοιχεί το Ubuntu Linux και για ΛΣ Windows έκδοση των Windows 7 και μεταγενέστερη.

Θ	Εργ	Περιεχόμενο
1	1	5.1 Εισαγωγή 5.1.1 Ιστορικά στοιχεία 5.1.2 Ορισμοί
1		5.2 Βασικές έννοιες 5.2.1 Απειλές κατά των δεδομένων (Data threats) 5.2.2 Βασικές αρχές ασφαλείας Πληροφοριακών Συστημάτων
1	3	5.2.3 Έλεγχος Πρόσβασης (Access Control) 5.2.3.1Πιστοποίηση Ταυτότητας και Εξουσιοδότηση 5.2.3.2 Εφαρμογή Ελέγχου Πρόσβασης
1	1	5.2.4 Διαχείριση Ασφαλείας Πληροφοριακού Συστήματος 5.2.4.1 Διαχείριση Κινδύνου ή Επικινδυνότητας (Risk management)
1	1	5.2.4.2 Σχέδιο Ασφαλείας (Security Plan) 5.2.4.3 Σχεδιασμός Επαναφοράς από Καταστροφή (Disaster Recovery) και Επιχειρησιακής Συνέχειας (Business Continuity)
1	3	5.3 Ασφάλεια Λογισμικού 5.3.1 Λογισμικό κακόβουλης χρήσης (malware) 5.3.2 Λογισμικό προστασίας από κακόβουλο λογισμικό (antivirus) 5.3.3 Ενημερώσεις λειτουργικών συστημάτων και εφαρμογών (updates)
1	1	5.3.4 Κρυπτογραφία (cryptography)
1	1	5.4 Ασφάλεια Δικτύων 5.4.1 Τοίχος Προστασίας (firewall)
	1	5.4.2 Εικονικό ιδιωτικό δίκτυο (VPN – Virtual Private Network) 5.4.3 Σύστημα Ανίχνευσης Εισβολής (IDS – Intrusion Detection System)
		5.5 Φυσική Ασφάλεια
8	12	Σύνολο ωρών

5.1 Εισαγωγή

5.1.1 Ιστορικά στοιχεία

Στην ενότητα αυτή υπάρχουν διάφορα ιστορικά γεγονότα που έχουν σχέση με την Ασφάλεια Πληροφοριών. Το κυριότερο από αυτά είναι η δημιουργία των Ομάδων Αντιμετώπισης Περιστατικών Ασφαλείας (CERT) γιατί είναι σήμερα μια από τις σημαντικότερες πηγές πληροφόρησης για θέματα προστασίας Πληροφοριακών Συστημάτων.

Δραστηριότητα 1

Πληροφορίες για τον Άλαν Τούριγκ: συμβολή στην αποκρυπτογράφηση των μηνυμάτων της μηχανής Αίνιγμα (ταινία *Το παιχνίδι της μίμησης* - The imitation game 2014), μηχανή Τούριγκ (υπολογιστικές μηχανές), τεχνητή νοημοσύνη (τεστ Τούριγκ), βραβείο Τούριγκ (ίσως το αντίστοιχο του Βραβείου Νόμπελ στον χώρο της πληροφορικής)

Δραστηριότητα 3

Σχετικές πληροφορίες μπορούν να βρεθούν στην ιστοσελίδα της Αστυνομίας http://tinyurl.com/ecrime-gr και http://www.safeline.gr/kataggelies/statistika-stoiheia.

Πρόσθετες δραστηριότητες:

Αναζήτηση πληροφοριών για την Κρυπτεία Σκυτάλη, τον Κώδικα του Καίσαρα και για τον Κέβιν Μίτνικ.

Δικτυογραφία: 1, 2, 3

5.1.2 Ορισμοί

Ως παράδειγμα Πληροφοριακού Συστήματος μπορεί να δοθεί και αυτό των νοσοκομείων και κλινικών στο οποίο καταχωρείται το ιστορικό των ασθενών που τα επισκέπτονται.

Ιδιαίτερη βαρύτητα χρειάζεται: η Ασφάλεια Πληροφοριακών Συστημάτων, το Ηλεκτρονικό Έγκλημα και η Κοινωνική Μηχανική (Ηλεκτρονικό Ψάρεμα https://el.wikipedia.org/wiki/Phishing, Κλοπή Ταυτότητας και των επιπτώσεών της http://www.safekids.gr/ασφάλεια/κλοπή-ταυτότητας-εφήβων)

Δικτυογραφία: 11 (http://tinyurl.com/ecrime-gr), 26, 27

5.2 Βασικές έννοιες

Στην ενότητα αυτή παρουσιάζονται οι Βασικές Έννοιες της Ασφάλειας Πληροφοριακών Συστημάτων.

5.2.1 Απειλές κατά των δεδομένων (Data threats)

Σκοπός της ενότητας είναι η κατανόηση των κινδύνων που διατρέχουν τα δεδομένα ενός οργανισμού και των συνεπειών που μπορεί να έχει η διαρροή ή η τροποποίησή τους. Για παράδειγμα, η διαρροή ενός μηχανολογικού σχεδίου μπορεί να έχει οικονομικές επιπτώσεις, ενώ ιατρικών εξετάσεων να έχει κοινωνικές επιπτώσεις. Η τροποποίηση μιας ιατρικής διάγνωσης μπορεί να βάλει σε κίνδυνο ακόμα και ανθρώπινες ζωές.

5.2.2 Βασικές αρχές ασφαλείας Πληροφοριακών Συστημάτων

Ιδιαίτερα σημαντική ενότητα καθώς η τήρηση των Βασικών Αρχών που περιγράφονται είναι επιδιωκόμενος στόχος και στους προσωπικούς υπολογιστές των μαθητών.
Για παράδειγμα: δεν επιθυμούν να δουν προσωπικές φωτογραφίες και μηνύματα ηλεκτρονικού ταχυδρομείου τους (Εμπιστευτικότητα), να τους τροποποιήσουν μια εργασία που θα παραδώσουν (Ακεραιότητα) χωρίς την συγκατάθεσή τους, και να μπορούν να χρησιμοποιούν τον Η/Υ όποτε τον χρειάζονται (Διαθεσιμότητα).

5.2.3 Έλεγχος Πρόσβασης (Access Control)

Δραστηριότητα 4

- Σε Windows ΛΣ γίνεται με δεξί κλικ πάνω στο φάκελο/αρχείο και επιλογή Κοινή Χρήση.
- Για να έχει ο Η/Υ με Windows πρόσβαση σε κοινόχρηστο φάκελο ή εκτυπωτή που βρίσκετε σε Η/Υ με Linux θα πρέπει πρώτα να εγκατασταθεί και παραμετροποιηθεί κατάλληλα ο Samba Server στον δεύτερο (https://help.ubuntu.com/lts/serverguide/samba.html)

Δραστηριότητα 5

A. Ο Καταγραφέας Συμβάντων (Event Viewer) βρίσκεται στα Εργαλεία Διαχείρισης αλλά και κάνοντας δεξί κλικ στο εικονίδιο Υπολογιστής / Διαχείριση / Εργαλεία Συστήματος / Προβολή Συμβάντων / Αρχεία Καταγραφής / Ασφάλεια

B. Στο αρχείο καταγραφής /var/log/*auth.log* υπάρχουν πληροφορίες για όλες τις <u>εξουσιοδοτήσεις</u> που δόθηκαν ή απέτυχαν στο σύστημα (πχ. και από sudo, ssh κτλ). Μπορούν να εντοπιστούν αυτές από το ενσωματωμένο πρόγραμμα του Ubuntu, το gnome-system-log. Επίσης, μπορούν να περιηγηθούν μέσα στο *auth.lo, πχ.* με την εντολή $vi /var/log/auth.log ή να φιλτράρουν μόνο τις επιθυμητές γραμμές με την *grep* δίνοντας για παράδειγμα*:*
$*grep '(lightdm:session)' /var/log/auth.log* **|** grep opened
$*grep sudo /var/log/auth.log* **|** grep *COMMAND*)

Υπάρχει η εντολή *last* στο Linux που δείχνει μόνο τις συνδέσεις/αποσυνδέσεις και επανεκκινήσεις στο σύστημα.

5.2.3.1 Πιστοποίηση Ταυτότητας και Εξουσιοδότηση

Η χρήση του συνδυασμού ΟνόμαΧρήστη/Κωδικού (Username/Password) είναι ο συνηθέστερος τρόπος απόκτησης εξουσιοδότησης για πρόσβαση σε κάποιο σύστημα (Η/Υ, Ηλεκτρονικό Ταχυδρομείο, διαδικτυακές τραπεζικές συναλλαγές κ.λπ.). Θα πρέπει να τονισθεί πόσο σημαντικό είναι να υπάρχουν κωδικοί που δεν θα μπορούν να τους μαντεύσουν εύκολα όσοι το προσπαθήσουν.

Ενδεικτικές ιστοσελίδες με πληροφορίες για προτάσεις δημιουργίας ισχυρών κωδικών και έλεγχό τους:

1. http://windows.microsoft.com/en-us/windows7/tips-for-creating-strong-passwords-and-passphrases
2. http://dide.sam.sch.gr/keplinet/index.php/articles-menu-item/technical-menu-item/157-safe-password-instructions
3. https://blog.kaspersky.com/password-check/

Δραστηριότητα 6

Ακολουθώντας της οδηγίες των παραπάνω ιστοσελίδων μπορούν να δημιουργήσουν ισχυρούς κωδικούς αλλά και ελέγξουν το πόσο ισχυροί είναι (δεν είναι απαραίτητη η επίτευξη 100% στο τεστ του συνδέσμου 3 ή στο τεστ που προτείνεται στο τέλος του συνδέσμου 2)

Σημαντικό είναι να μάθουν και για την ύπαρξη προγραμμάτων διαχείρισης κωδικών (Password managers) σε κρυπτογραφημένη μορφή και τον τρόπο χρήσης τους. Γνωστό τέτοιο πρόγραμμα Ανοιχτού Λογισμικού είναι το Keepass. Ακολουθεί η παρουσίασή του από την ομάδα Διανομή Ασφάλειας http://secure-distro.cti.gr/index.php/el/ του ΙΤΥΕ ΔΙΟΦΑΝΤΟΣ: https://www.youtube.com/watch?v=GChv4nhoRuw

5.2.3.2 Εφαρμογή Ελέγχου Πρόσβασης

Μορφή ACL συστήματος αρχείων μπορεί να θεωρηθεί και το αποτέλεσμα της *chmod* γιατί το περιέχει Ιδιοκτήτη και Προνόμια: Χρήστη (User), Ομάδας (Group), Άλλων (Others).

Στις ACL δικτύου μπορούν να παρουσιαστούν παραδείγματα από iptables (linux firewall), Router και Squid proxy server που μπορούν να βρεθούν εύκολα στο διαδίκτυο.

Παραδείγματα:

- http://www.cisco.com/c/en/us/support/docs/ip/access-lists/26448-ACLsamples.html#allowselecthost
- https://help.ubuntu.com/community/IptablesHowTo
- http://www.cyberciti.biz/tips/linux-iptables-examples.html (δείτε το #10)
- http://blogs.sch.gr/span/squid-conf-block-ads-and-downloading/

Το Active Directory συνήθως υπάρχει σε Διακομιστή Windows των εργαστηρίων.

Το LDAP μπορεί να βρεθεί σε Εικονική Μηχανή (Virtual Machine) στο διαδίκτυο. Αναζητήστε Εικονική Μηχανή OpenLdap ή μεταβείτε στο http://blogs.sch.gr/virtualization.

Δραστηριότητα 7

Τρόπο χρήσης του AD μπορείτε να βρείτε στις σελίδες:

1. http://ts.sch.gr/docs/odigies-egkatastasis-diaxirisis

2. http://ts.sch.gr/wiki/Windows/Server_Client/Αρχιτεκτονική

5.2.4 Διαχείριση Ασφαλείας Πληροφοριακού Συστήματος

Η ενότητα αυτή είναι κυρίως θεωρητική όμως το περιεχόμενό της είναι ιδιαίτερα σημαντικό γιατί παρουσιάζει σύντομα τον τρόπο διατήρησης του επιθυμητού επιπέδου ασφαλείας ενός Πληροφοριακού Συστήματος καθώς και τον τρόπο Επαναφοράς του σε λειτουργία μετά από κάποια καταστροφή.

Δραστηριότητα 8

Να δοθεί όσος χρόνος χρειαστεί για την κατανόηση του τρόπου λήψης Αντιγράφων Ασφαλείας.

Δικτυογραφία: 4, 5, 6, 7, 8, 30

5.3 Ασφάλεια Λογισμικού

5.3.1 Λογισμικό κακόβουλης χρήσης (Malware)

Πρόσθετα μπορεί να αναφερθούν πληροφορίες και για τον Ransomware:

1. Δικτυογραφία 25,
2. http://www.safer-internet.gr/δίωξη-ηλεκτρονικού-εγκλήματος-οδηγο
3. http://tinyurl.com/grpolice-ransomware

Δικτυογραφία: 1, 2, 23, 25

5.3.2 Λογισμικό προστασίας από κακόβουλο λογισμικό (antivirus)

Να επισημανθεί πως αυτού του είδους τα προγράμματα είναι απαραίτητα την σημερινή εποχή και πως η επιλογή ενός δοκιμασμένου σε εργαστήρια (και όχι από φήμες) είναι επιβεβλημένη. Η ομαδική αγορά αδειών μπορεί να οδηγήσει το κόστος ανά άδεια σε έκπτωση ακόμη και πάνω από 50% της αρχικής τιμής αγοράς.

Παράδειγμα ενδεικτικών τιμών από ένα τέτοιο πρόγραμμα με ενσωματωμένο Antivirus + Antimalware + Antispam + Firewall + Parental Control + Anti-Phishing:

1 άδεια για 1 χρόνο 28€	5 άδειες για 1 χρόνο 80€ (16€ / άδεια τον χρόνο)
1 άδεια για 2 χρόνια 44€	5 άδειες για 2 χρόνια 125€ (12,5€ τον χρόνο)

Ενδεικτική ιστοσελίδα συγκριτικών δοκιμών: http://www.av-comparatives.org

Δραστηριότητα 9

Ο ιός του συνδέσμου είναι αβλαβής και προσφέρεται για απόκτηση εμπειρίας από τους μαθητές στον τρόπο με τον οποίο αντιδρά (μηνύματα) το Πρόγραμμα Προστασίας σε περίπτωση εντοπισμού ενός ιού.

5.3.3 Ενημερώσεις λειτουργικών συστημάτων και εφαρμογών (updates)

Σημαντικότατο τμήμα της ασφάλειας ενός συστήματος είναι οι ενημερώσεις του ΛΣ αλλά και των εγκατεστημένων εφαρμογών σε αυτό.

Με την εγκατάσταση ενός ΛΣ ο αυτόματος έλεγχος είναι ή προτείνεται να ενεργοποιηθεί.

Σε ΛΣ Windows η ρύθμισή του βρίσκεται στον Πίνακα Ελέγχου (Control Panel).

Σε ΛΣ Linux υπάρχει πρόγραμμα σε γραφικό περιβάλλον από το οποίο μπορεί να γίνει ενημέρωση και των εγκατεστημένων προγραμμάτων ή επιλογή μόνο των επιθυμητών πακέτων. Από τη γραμμή εντολών μπορεί να γίνει συνολική ενημέρωση με τις εντολές:

1. $sudo apt-get update (ενημέρωση της λίστας με τις τελευταίες εκδόσεις των πακέτων)
2. $sudo apt-get upgrade (αναβάθμιση όλων των πακέτων ανεξαιρέτως)

Τα εγκατεστημένα προγράμματα σε ΛΣ Windows συνήθως έχουν τον έλεγχο για ενημερώσεις στο μενού Βοήθεια και η ρύθμιση για αυτόματο έλεγχο γίνεται συχνά μέσα από τις ρυθμίσεις του προγράμματος. Τις περισσότερες ενημερώσεις λόγω ευπαθειών τις έχουν το Flash Player

και η Java. Οι ρυθμίσεις για αυτόματο ή χειροκίνητο έλεγχο υπάρχουν στον Πίνακα Ελέγχου (όταν είναι εγκατεστημένα).
Σε ΛΣ Linux η ενημέρωση προγραμμάτων μπορεί να γίνει από το πρόγραμμα γενικής ενημέρωσης με την επιλογή μόνο του επιθυμητού ή από την γραμμή εντολών:

$sudo apt-get update
$sudo apt-get –only-upgrade install <*ΟΝΟΜΑ ΠΑΚΕΤΟΥ*>
Όπου *ΟΝΟΜΑ ΠΑΚΕΤΟΥ* μπορεί να είναι για παράδειγμα:
firefox, flashplugin-installer (ο FlashPlayer μόνο μέχρι την 11.2 υπάρχει) κ.λπ.

Για την Java εκτελέστε τις εντολές:

```
$ sudo add-apt-repository ppa:webupd8team/java
$ sudo apt-get update
$ sudo apt-get install oracle-java8-installer
```

Δραστηριότητα 10
Εφαρμόστε τις παραπάνω οδηγίες.

5.3.4 Κρυπτογραφία (cryptography)

Ψηφιακή Υπογραφή
Δικτυογραφία: 9, 16, 28, 29, 32, 37
Δραστηριότητα 12

Κρυπτογράφηση
Το Bitlocker (ενσωματωμένη κρυπτογράφηση Windows) είναι διαθέσιμο:
Win7 Enterprise και Ultimate - Win8.1 Enterprise και Pro
Για να μπορούν να διαβαστούν κρυπτογραφημένα αρχεία σε άλλους Η/Υ χρειάζονται τα εξής βήματα: http://windows.microsoft.com/el-gr/windows-vista/share-encrypted-files
Δραστηριότητες 11, 13

5.4 Ασφάλεια Δικτύων

(Δοκιμαστικά αν υπάρχει χρόνος μπορεί να χρησιμοποιηθεί για τον εντοπισμό και την αξιολόγηση ευπαθειών το OpenVAS http://www.openvas.org/about.html και η έτοιμη Εικονική Μηχανή που διαθέτουν στη σελίδα http://www.openvas.org/vm.html.
ΠΡΟΣΟΧΗ στη σελίδα http://www.openvas.org/compendium/preparing-the-microsoft-windows-target.html στη γραμμή «For Windows XP it is important that "Easy Filesharing" is switched off.»)

5.4.1 Τοίχος Προστασίας (firewall)

Δραστηριότητα 14
Σε ΛΣ Windows βρείτε και ενεργοποιήστε/απενεργοποιήστε την χρήση Απομακρυσμένης Επιφάνειας Εργασίας (RDP):
http://windows.microsoft.com/el-gr/windows7/allow-remote-desktop-connections-from-outside-your-home-network

Σε ΛΣ Linux εκτελέστε από Τερματικό την εντολή *$gufw* και ακολουθήστε τα βήματα:

1. Ενεργοποιήστε το Firewall από το κουμπί Κατάσταση
2. Κλικ στο +
3. Πολιτική: Αποδοχή
4. Κατεύθυνση: Εισερχόμενη
5. Κατηγορία: Δίκτυο
6. Υποκατηγορία: Απομακρυσμένη Πρόσβαση
7. Εφαρμογή: RDP
8. Πατήστε το κουμπί Προσθήκη
9. Κλείσιμο
10. Θα εμφανιστεί στο κύριο παράθυρο του προγράμματος η προσθήκη που μόλις έγινε

Επιπλέον πληροφορίες: http://tinyurl.com/gufw-examples

5.4.2 Εικονικό ιδιωτικό δίκτυο (VPN – Virtual Private Network)

Δραστηριότητα 15
Αν δεν υπάρχει κάποιος Router που να υποστηρίζει VPN συνδέσεις δοκιμάστε να κατεβάστε μια Εικονική Μηχανή (VM) με το OpenVPN από τη σελίδα http://tinyurl.com/vm-openvpn

5.4.3 Σύστημα Ανίχνευσης Εισβολής (IDS – Intrusion Detection System)

Για περισσότερες πληροφορίες δείτε την σελίδα
https://en.wikipedia.org/wiki/Intrusion_detection_system

5.5 Φυσική Ασφάλεια

Στη Φυσική Ασφάλεια θα πρέπει να δίνεται, επίσης, βαρύτητα γιατί εκτός από την φυσική πρόσβαση ανθρώπων υπάρχουν πολλοί κίνδυνοι όπως είναι οι πλημμύρες, υπερβολική ζέστη και διακοπές ρεύματος οι οποίες είναι αναπόφευκτες.

Για τις διακοπές ρεύματος, οι οποίες μπορούν να συμβούν σε μεγάλες γεωγραφικές περιοχές και κατά περιόδους συχνά, θα πρέπει να λαμβάνονται μέτρα όπως αυτά των UPS ή και γεννητριών ρεύματος. Υπάρχουν UPS που μπορούν να συνδεθούν με λογισμικό σε Η/Υ (μέσω USB ή Serial Port) το οποίο να ενημερώνει τους αρμόδιους με SMS ή e-mail όταν γίνεται διακοπή ρεύματος οποιαδήποτε ώρα της ημέρας. Επίσης υπάρχουν γεννήτριες ρεύματος που μπορούν να μπαίνουν σε λειτουργία αυτόματα μετά την πάροδο κάποιου χρονικού διαστήματος χωρίς παροχή από το κύριο δίκτυο παροχής ρεύματος.

Ενότητα 6

Ειδικά θέματα

[10 Ώρες - 2Θ + 8Ε]

Θ	Εργ	Περιεχόμενο
2	8	6 Ειδικά θάματα 6.1 Εικονικές Μηχανές

Η χρήση Εικονικών Μηχανών (VM) προσφέρει εκτός των ευκολιών μετακίνησης, λήψης αντιγράφων ασφαλείας και ανεξαρτησίας τους από το υλικό, και έναν ασφαλή τρόπο δοκιμών εγκαταστάσεων ΛΣ και λογισμικού.

Δραστηριότητα 2

Γ) VirtualBox. Για να τεθεί ένας Εικονικός Δίσκος σε κατάσταση Immutable (αμετάβλητη, δηλαδή μη μόνιμης εγγραφής) θα πρέπει πρώτα να αποσυδενθεί από την μηχανή στην οποία ανήκει:

Αποσύνδεση δίσκου:

1. Επιλογή της Μηχανής που θέλουμε να θέσουμε τον δίσκο σε Immutable
2. Settings / Storage / και επιλογή του δίσκου (πχ κάτω από τον SATA Controller)
3. Επιλέγουμε το σύμβολο Πλην (αποσύνδεση)

Μετατροπή του δίσκου σε Immutable

1. File / Virtual Media Manager / καρτέλα Hard Disks
2. Επιλογή του δίσκου που θέλουμε να βάλουμε σε κατάσταση Immutable
3. Επιλογή Modify
4. Επιλογή Immutable

Επανασύνδεση δίσκου στη Μηχανή

1. Επιλογή Μηχανής στην οποία θα επανασυνδέσουμε τον δίσκο
2. Settings / Storage / SATA Controler.
   Όταν επιλεχθεί αυτός τότε εμφανίζονται δεξιά του 2 σύμβολα, CD και HD με + πάνω τους.
3. Επιλογή του HD (με το +)
4. Επιλογή *Choose existing disk*
5. Επιλογή του δίσκου

Από το σημείο αυτό και μετά όσες αλλαγές γίνονται θα χάνονται **μόνο** όταν θα «σβήσει» (Shutdown) η Εικονική Μηχανή, θα παραμένουν όμως σε επανεκκινήσεις (Reboot).

Δραστηριότητα 4

Με τη χρήση του VMware Converter μπορεί να γίνει η μετατροπή ενός φυσικού Η/Υ σε Εικονική Μηχανή και η αποθήκευσή του σε έναν εξωτερικό USB δίσκο (πχ).
https://my.vmware.com/web/vmware/evalcenter?p=converter (θέλει δωρεάν εγγραφή)

Οι Συγγραφείς