ΣΧΟΛΗ ΟΙΚΟΝΟΜΙΚΩΝ ΕΠΙΣΤΗΜΩΝ ΚΑΙ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ

ΤΜΗΜΑ ΔΙΟΙΚΗΤΙΚΗΣ ΕΠΙΣΤΗΜΗΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ

ΠΠΣ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ ΜΕΣΟΛΟΓΓΙ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

«ΑΝΑΠΤΥΞΗ ΔΙΑΔΙΚΤΥΑΚΟΥ ΣΕΜΙΝΑΡΙΟΥ ΜΕ ΣΤΟΧΟ ΤΗΝ ΕΝΗΜΕΡΩΣΗ ΔΙΟΙΚΗΤΙΚΩΝ ΥΠΑΛΛΗΛΩΝ ΣΕ ΘΕΜΑΤΑ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ»

ΑΝΔΡΙΑΝΑ ΜΑΡΙΑ ΚΑΛΑΡΙΔΗ ΚΑΙ ΑΝΙΣΑ ΛΑΜΙ

Μεσολόγγι 2020

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΑΤΡΩΝ

ΣΧΟΛΗ ΟΙΚΟΝΟΜΙΚΩΝ ΕΠΙΣΤΗΜΩΝ ΚΑΙ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ

ΤΜΗΜΑ ΔΙΟΙΚΗΤΙΚΗΣ ΕΠΙΣΤΗΜΗΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ

ΠΠΣ ΔΙΟΙΚΗΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ ΜΕΣΟΛΟΓΓΙ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΑΝΑΠΤΥΞΗ ΔΙΑΔΙΚΤΥΑΚΟΥ ΣΕΜΙΝΑΡΙΟΥ ΜΕ ΣΤΟΧΟ ΤΗΝ ΕΝΗΜΕΡΩΣΗ ΔΙΟΙΚΗΤΙΚΩΝ ΥΠΑΛΛΗΛΩΝ ΣΕ ΘΕΜΑΤΑ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ

ΑΝΔΡΙΑΝΑ ΜΑΡΙΑ ΚΑΛΑΡΙΔΗ ΚΑΙ ΑΝΙΣΑ ΛΑΜΙ

Επιβλέπων καθηγητής ή καθηγήτρια

[ΒΑΣΙΛΕΙΟΣ ΣΤΕΦΑΝΗΣ]

Μεσολόγγι 2020

UNIVERSITY OF PATRAS

SCHOOL OF ECONOMICS & BUSINESS

DEPARTMENT OF MANAGEMENT SCIENCE AND TECHNOLOGY

FORMER DEPARTMENT OF BUSINESS ADMINISTRATION AT MESSOLONGHI

THESIS

ICT Security – Developing an online course for administration staff

ANDRIANA MAPIA KALARIDI AND ANISA LAMI

Messolonghi 2020

Η έγκριση της πτυχιακής εργασίας από το Τμήμα Διοικητικής Επιστήμης και Τεχνολογίας του Πανεπιστημίου Πατρών δεν υποδηλώνει απαραιτήτως και αποδοχή των απόψεων του συγγραφέα εκ μέρους του Τμήματος.

ΠΕΡΙΛΗΨΗ

Στη σύγχρονη ανθρωπότητα η μάθηση αποτελεί βασικό στοιχείο της καθημερινότητας μας και όλοι δικαιούνται ίσες ευκαιρίες σε αυτή. Ωστόσο, επειδή οι συνθήκες δεν είναι πάντα ευνοϊκές για να συμβεί αυτό, τα τελευταία χρόνια έχει δοθεί μεγάλος βάρος στην ανάπτυξη της ηλεκτρονικής μάθησης ως ένα μέσο το οποίο θα βοηθήσει να λυθούν αν όλα τα περισσότερα προβλήματα που παρουσιάζοντα. Μερικά από αυτά είναι διάφορες περιπτώσεις όπου η μάθηση είναι αδύνατον να συμβεί λόγο έντονης κακοκαιρίας, λόγο απομακρυσμένων και δυσπρόσιτων τοποθεσιών η και ακόμα απρόβλεπτων συνθηκών που εμποδίζουν την συνύπαρξη του καθηγητή και του εκπαιδευόμενου στον ίδιο χώρο.

Για αυτούς τους λόγους, σε παγκόσμιο επίπεδο έχει επικεντρωθεί η έρευνα στην ανάπτυξη του τομέα της ηλεκτρονικής μάθησης (e-learning) καθώς και του τομέα των προηγμένων μαθησιακών τεχνολογιών.

Η ηλεκτρονική μάθηση όπως εύκολα μπορούμε να συμπεράνουμε είναι η διαδικασία με την οποία η μάθηση γίνεται μέσω υπολογιστή και χωρίς να είναι απαραίτητη η φυσική παρουσία στον ίδιο χώρο του εκπαιδευτή με τον εκπαιδευόμενο. Πρόκειται δηλαδή για εκπαίδευση εξ-αποστάσεως. Αυτή μπορεί να είναι σύγχρονη ή ασύγχρονη. Δηλαδή, μπορεί να συμβαίνει είτε σε ζωντανή μετάδοση είτε ηχογραφημένα. Ο εκπαιδευτής μπορεί να παρουσιάσει το μάθημά του και ο εκπαιδευόμενος θα μπορεί να ανατρέξει σε αυτό οποιαδήποτε στιγμή μπορεί ή θέλει.

Αυτό δεν σημαίνει πως η ηλεκτρονική μάθηση θα αντικαταστήσει τη κλασική μέθοδο εκπαίδευσης αλλά μπορεί να αποτελέσει ένα σημαντικό βοήθημα διευκόλυνσης για όταν κρίνεται απαραίτητο. Επίσης, η ηλεκτρονική μάθηση θα μπορούσε να αποτελεί και ένα τρόπο με τον οποίο θα δινόταν πρόσβαση στους εκπαιδευόμενους σε έξτρα βοηθητικό υλικό που θα τους βοηθούσε στην εκπαίδευσή τους.

Αυτή τη στιγμή η πλατφόρμα ηλεκτρονικής εκπαίδευσης που χρησιμοποιείται από τα περισσότερα πανεπιστήμια και εκπαιδευτικά ιδρύματα της χώρας ,μας είναι το moodle. Αυτός είναι και ο λόγος που επιλέξαμε σε αυτή την πτυχιακή να αναλύσουμε αυτή τη πλατφόρμα, να δείξομε ποιος ο ρόλος της και οι λειτουργίες της καθώς και ποιες δυνατότητες παρέχονται και στους εκπαιδευόμενους αλλά και στους εκπαιδευτές.

ABSTRACT

In modern humanity, learning is a key element of our daily lives and everyone is entitled to equal opportunities. However, because conditions are not always conducive to this happening, in recent years much emphasis has been placed on the development of e-learning as a means of helping to solve all the problems that have arisen. Some of these are various cases where learning is impossible due to severe bad weather, remote and inaccessible locations or even unpredictable conditions that prevent the coexistence of teacher and student in the same area.

For these reasons, global research has focused on the development of the e-learning sector as well as the advanced learning technology sector.

E-learning as we can easily conclude is the process by which learning is done through a computer and without the need for physical presence in the same area of the instructor as the learner. In other words, it is distance learning. This can be modern or asynchronous. That is, it can occur either live or recorded. The instructor can present his / her lesson and the trainee will be able to refer to it at any time he / she can or wants.

This does not mean that e-learning will replace the classical method of education, but it can be an important facilitator for when it is deemed necessary. E-learning could also be a way to give learners access to extra support material that would help them in their education.

Currently the e-learning platform used by most universities and educational institutions in the country, is our moodle. This is the reason why we chose in this dissertation to analyze this platform, to show what its role and functions are, as well as what possibilities are provided to both trainees and trainers.

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ

ΠΣ - πληροφοριακό σύστημα

ΕΙΣΑΓΩΓΗ

Η ραγδαία ανάπτυξη των τεχνολογιών της πληροφορίας και των επικοινωνιών του διαδικτύου αλλά και των έξυπνων συσκευών έχουν ως αποτέλεσμα η σύγχρονη καθημερινότητα των ανθρώπων όσον αφορά τον τρόπο που επικοινωνούν και εκπαιδεύονται να έχει αλλάξει σε τεράστιο βαθμό σε σχέση με τα παλαιότερα χρόνια. Οι αυξημένες απαιτήσεις που υπάρχουν σήμερα για περισσότερη αυτονομία και ευελιξία όσον αφορά τον τόπο, το χρόνο αλλά και το ρυθμό που γίνεται η μάθηση έχουν οδηγήσει στην δημιουργία ενός νέου είδους εκπαίδευσης, τη λεγόμενη ηλεκτρονική μάθηση.

Η συγκεκριμένη έννοια ουσιαστικά εκφράζει την προσπάθεια για αξιοποίηση των πλεονεκτημάτων που προσφέρει η εξ' αποστάσεως εκπαίδευση αλλά ταυτόχρονα, υποστηρίζει και τη προσπάθεια για την εξάπλωση και διεύρυνση των γνώσεων μεταξύ των μαθητών σε όλο τον κόσμο.

Η έννοια αυτή δεν αποτελεί νέο φαινόμενο, καθώς ίχνη της είναι εφικτό να εντοπιστούν Ήδη από την περίοδο του '80 είχε αρχίσει να εμφανίζεται η συγκεκριμένη έννοια και πλέον έχει φτάσει σε ένα σημείο που η διάδοση της την καθιστά σε μία από τις πιο διαδεδομένες μεθόδους που χρησιμοποιείται από τα περισσότερα εκπαιδευτικά ιδρύματα.. Γενικότερα, ο μεγάλος αριθμός ορισμών που έχουν αποδοθεί στο συγκεκριμένο όρο φανερώνει και το πόσο πολύπλοκο χαρακτήρα έχει και πόσο δύσκολο είναι να περιοριστεί και να αποδοθεί ένας και μόνο απλούστερος ορισμός ο οποίος θα περιέχει τα κυριότερα χαρακτηριστικά.

1 ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

1.1 Θεμελιώδης Έννοιες

Όπως όλοι γνωρίζουμε πλέον είναι ότι η έννοια της ασφάλειας των πληροφορικών συστημάτων (information system security) έχει τρείς βασικές έννοιες:

- Εμπιστευτικότητα (Confidentiality)
- Ακεραιότητα (Integrity),
- Διαθεσιμότητα (Availability)

1.1.1 Εμπιστευτικότητα (Confidentiality)

Η εμπιστευτικότητα είναι η πιο σημαίνει πρόληψη μη εξουσιοδοτημένης (unauthorized) αποκάλυψης πληροφοριών, δηλαδή πρόληψη από μη εξουσιοδοτημένη ανάγνωση. Επομένως σημαίνει ότι τα δεδομένα ενός υπολογιστικού συστήματος, καθώς και τα διακινούμενα μεταξύ των υπολογιστών δεδομένα, αποκαλύπτονται μόνο σε εξουσιοδοτημένα άτομα. Αυτό αφορά όχι μόνο την προστασία από μη εξουσιοδοτημένη αποκάλυψη των δεδομένων αυτών καθαυτών αλλά ακόμη και από το γεγονός ότι τα δεδομένα απλώς υπάρχουν. Έτσι για παράδειγμα, το γεγονός ότι κανείς έχει φάκελο εγκληματία είναι συχνά το ίδιο σημαντικό όπως και οι λεπτομέρειες για το έγκλημα που διαπράχθηκε. (Liebeherr, El Zarki.2004)

1.1.2 Ακεραιότητα (Integrity)

Την ακεραιότητα μπορούμε γενικά να την ορίσουμε ως την απαίτηση να είναι τα πράγματα όπως πρέπει να είναι. Στην πληροφορική, ακεραιότητα σημαίνει πρόληψη μη εξουσιοδοτημένης μεταβολής πληροφοριών, δηλαδή, πρόληψη από μη εξουσιοδοτημένη εγγραφή ή διαγραφή, που περιλαμβάνει και της μη εξουσιοδοτημένης δημιουργίας δεδομένων.

1.1.3 Διαθεσιμότητα (Availability)

Διαθεσιμότητα ονομάζουμε την ιδιότητα του να είναι προσπελάσιμες και χωρίς αδικαιολόγητη καθυστέρηση οι υπηρεσίες ενός πληροφοριακού συστήματος (ΠΣ) όταν τις χρειάζεται μια εξουσιοδοτημένη οντότητα. Αυτό σημαίνει ότι οι εξουσιοδοτημένοι χρήστες των υπολογιστικών συστημάτων και των επικοινωνιακών μέσων δεν αντιμετωπίζουν προβλήματα άρνησης εξυπηρέτησης (denial of service) όταν επιθυμούν να προσπελάσουν

τους πόρους του συστήματος. Η διαθεσιμότητα καλύπτει περιοχές πέρα από το φυσικό σκοπό της ασφάλειας. Για παράδειγμα, ένα μεγάλο μέρος της τεχνολογίας που απαιτείται για τη διασφάλιση της διαθεσιμότητας προέρχεται από άλλες περιοχές, όπως fault – tolerant computing.(Γκριτζαλης,2003)

1.2 Τι είναι ασφάλεια πληροφοριακών συστημάτων

Η έννοια της ασφάλειας ενός πληροφοριακού συστήματος έχει να κάνει με την ικανότητα ενός συστήματος να προστατεύει τις πληροφορίες του από αλλοιώσεις και καταστροφές, καθώς και από μη εξουσιοδοτημένη χρήση των πόρων του. Σχετίζεται επίσης με την ικανότητά του να παρέχει σωστές και αξιόπιστες πληροφορίες, οι οποίες είναι διαθέσιμες στους εξουσιοδοτημένους χρήστες κάθε φορά που τις αναζητούν. Η λειτουργία αυτή στηρίζεται στη λήψη μέτρων τα οποία διασφαλίζουν την ακεραιότητα και την εμπιστευτικότητα των δεδομένων, καθώς και την αδιάλειπτη λειτουργία του υπολογιστικού συστήματος. (Weber,2010)

1.2.1 Τύποι Απειλών Ασφάλειας

Η προέλευσή των απειλών κατατάσσονται στις τρεις ακόλουθες κατηγορίες:

- Φυσικές απειλές: Αυτές οι καταστροφές (φωτιά, πλημμύρα κλπ.) δεν είναι πάντα δυνατόν να αποτραπούν. Όμως είναι σημαντικό η εκδήλωση παρόμοιων γεγονότων να διαπιστώνεται έγκαιρα, ώστε να ελαχιστοποιούνται οι πιθανότητες σημαντικών ζημιών. Όπως επίσης σημαντικό είναι να αποφεύγονται ενέργειες που αυξάνουν την πιθανότητα εκδήλωσής τους (όπως για παράδειγμα, το κάπνισμα). Τέλος, η ετοιμότητα χρήσης εφεδρικού συστήματος, σε συνδυασμό με τη λήψη τακτικών εφεδρικών αρχείων (back - ups) για τα κρίσιμα δεδομένα, περιορίζει τις πιθανές δραματικές συνέπειες.
- Ακούσιες απειλές: Προκαλούνται είτε από αστοχίες υλικού ή λογισμικού (HW/SW failures), είτε από άγνοια ή αδιαφορία του ανθρώπινου παράγοντα. Ο λόγος που υπάρχουν τέτοιες απειλές είναι η έλλειψη σωστής εκπαίδευσης, είτε είναι απλοί χρήστες είτε είναι διαχειριστές των συστημάτων. Επίσης να επισημάνουμε ότι το ποσοστό των προβλημάτων που δημιουργούνται από άγνοια στα πληροφοριακά συστήματα είναι πολύ μεγαλύτερο από εκείνο που οφείλεται σε κακή πρόθεση.

- Εκούσιες απειλές: Είναι οι απειλές αυτές που απασχολούν περισσότερο τη δημοσιότητα. Στην κατηγορία αυτή, οι κακόβουλοι χρήστες μπορεί να ανήκουν στο εσωτερικό του συστήματος (insiders), για παράδειγμα κάποιοι δυσαρεστημένοι υπάλληλοι. Είναι όμως πιθανό οι απειλές να προέρχονται από κάποιους επίδοξους εισβολείς που είναι εξωτερικοί χρήστες (outsiders). Στη περίπτωση αυτή η επιτυχία των επιθέσεων εξαρτάται κυρίως από τα μέσα που διαθέτουν δηλαδή το χρόνο, την υπολογιστική ισχύ, τις γνώσεις, τα άτομα, τα χρήματα, τις συσκευές και τα εξαρτήματα. Οι κακοήθεις χρήστες μπορεί να επιδιώκουν εκδίκηση, οικονομικό κέρδος, αναγνώριση ή λόγω ιδιοσυγκρασίας απλά τη δημιουργία προβληματικών καταστάσεων και τη διάπραξη βανδαλισμών. (Πομπόρτσης 2003).

1.2.2 Λειτουργίες και χειρισμοί ασφάλειας

Τα μέτρα προστασίας (controls) ή αντίμετρα (countermeasures) είναι όλες εκείνες οι διαδικασίες, τεχνικές, ενέργειες και συσκευές που περιορίζουν τις ευπάθειες ενός Πληροφοριακού Συστήματος (ΠΣ). Οι διαφορετικοί τύποι αντίμετρων έχουν ως αποτέλεσμα την ανάλυση του προβλήματος της ασφάλειας πληροφοριακών στις ακόλουθες συνιστώσες:

- ❖ Φυσική ασφάλεια συστήματος (physical security): Δηλαδή στην προστασία ολόκληρου του σχετικού εξοπλισμού του υπολογιστή από φυσικές καταστροφές, όπως κλοπή, βανδαλισμοί, πλημμύρες, φωτιά κλπ. 21
- ❖ Ασφάλεια Υπολογιστικού Συστήματος (computer security): Δίνουμε έμφαση στην προστασία εκείνων των πληροφοριών του υπολογιστή που διαχειρίζεται άμεσα το λειτουργικό σύστημα (προγράμματα εφαρμογών, αρχεία δεδομένων, κ.α.). Αναφερόμαστε κυρίως στις συγκεκριμένες υπηρεσίες των λειτουργικών συστημάτων που καθορίζουν το ποιος και το πώς θα έχει το δικαίωμα να έχει πρόσβαση στα δεδομένα και τις εφαρμογές που φιλοξενεί το υπολογιστικό σύστημα.
- ❖ Ασφάλεια Βάσεων Δεδομένων (database security): Αναφέρεται στην ικανότητα του συστήματος να εφαρμόσει μια πολιτική προστασίας των περιεχομένων μιας βάσης δεδομένων, στην οποία διευκρινίζεται ποιοι εξουσιοδοτούνται να δουν ή / και να τροποποιήσουν τα προστατευμένα δεδομένα.

- ❖ Ασφάλεια Δικτύων Επικοινωνιών (network security): Σε αυτήν την φάση αναφερόμαστε στην προστασία των πληροφοριών κατά τη μετάδοσή τους μέσω των τηλεφωνικών, δορυφορικών ή άλλων δικτύων, όπως είναι τα τοπικά δίκτυα και το Internet. (Γκριτζαλης,2003)

1.2.3 Τρόποι παραβίασης της ασφάλειας

- Στις έννοιες παραβάσεις ασφαλείας (security breaches) υπολογιστικών συστημάτων σχετίζονται με τις έννοιες των εκθέσεων, ευπαθειών, απειλών και χειρισμών, ως εξής:
- Η Έκθεση (Exposure) περιλαμβάνει αποκάλυψη των δεδομένων, μεταβολές των δεδομένων, άρνηση νόμιμης προσπέλασης για υπολογισμούς. Παραδείγματα εκθέσεων σε κίνδυνο είναι:
    - η μη εξουσιοδοτημένη αποκάλυψη δεδομένων
    - η μη εξουσιοδοτημένη τροποποίηση δεδομένων
    - η άρνηση θεμιτής προσπέλασης υπολογιστικών πόρων
- Η Ευπάθεια (Vulnerability) είναι μια αδυναμία στο σύστημα ασφάλειας που μπορούμε να την αξιοποιήσουμε για την πρόκληση απωλειών ή ζημιών.
- Η Απειλή (Threat) για ένα υπολογιστικό σύστημα είναι μια κατάσταση όπου υπάρχει η πιθανότητα πρόκλησης απωλειών ή ζημιών. Παραδείγματα απειλών είναι:
    - ανθρώπινες επιθέσεις,
    - φυσικές καταστροφές,
    - ακούσια ανθρώπινα λάθη,
    - εσωτερικές ατέλειες του εξοπλισμού ή του λογισμικού.
- Ο Χειρισμός ή Έλεγχος (Control) είναι ένα προστατευτικό μέτρο που μειώνει μια απειλή του υπολογιστικού συστήματος.

Οι βασικές απειλές για την ασφάλεια ενός υπολογιστικού συστήματος είναι η διακοπή, η μεταβολή, η κλοπή, και η παραποίηση. Πιο αναλυτικά:

- Η Διακοπή (Interruption) συμβαίνει όταν ένα στοιχείο του συστήματος χάνεται ή γίνεται μη διαθέσιμο.
- Η Μεταβολή (Modification) συμβαίνει όταν κάποιο μη εξουσιοδοτημένο μέρος εκτός του ότι έχει καταφέρει να έχει προσπέλαση, παραποιεί (tampers) ένα στοιχείο.
- Η Κλοπή (Interception) συμβαίνει όταν κάποιο μη εξουσιοδοτημένο μέρος έχει καταφέρει να έχει προσπέλαση σε ένα στοιχείο.
- Η Παραποίηση (Fabrication) συμβαίνει όταν κάποιο μη εξουσιοδοτημένο μέρος παραποιεί αντικείμενα σε ένα υπολογιστικό σύστημα. (Henmi, 2006)

1.2.4 Η Ασφάλεια και η προστασία ενός Π.Σ

Τα μέτρα προστασίας (controls) ή αντίμετρα (countermeasures) είναι όλες εκείνες οι διαδικασίες, τεχνικές, ενέργειες και συσκευές που περιορίζουν τις ευπάθειες ενός Πληροφοριακού Συστήματος (ΠΣ).

Οι διαφορετικοί τύποι αντίμετρων έχουν ως αποτέλεσμα την ανάλυση του προβλήματος της ασφάλειας πληροφοριακών στις ακόλουθες συνιστώσες:

- Φυσική ασφάλεια συστήματος (physical security): Αναφέρεται στην προστασία ολόκληρου του σχετικού εξοπλισμού του υπολογιστή από φυσικές καταστροφές, όπως κλοπή, βανδαλισμοί, πλημμύρες, φωτιά κλπ.
- Ασφάλεια Υπολογιστικού Συστήματος (computer security): Αναφέρεται στην προστασία εκείνων των πληροφοριών του υπολογιστή που διαχειρίζεται άμεσα το λειτουργικό σύστημα (προγράμματα εφαρμογών, αρχεία δεδομένων, κ.α.). Επικεντρώνεται κυρίως στις συγκεκριμένες υπηρεσίες των λειτουργικών συστημάτων που καθορίζουν το ποιος και το πώς θα δικαιούται να προσπελάσει τα δεδομένα και τις εφαρμογές που φιλοξενεί το υπολογιστικό σύστημα.
- Ασφάλεια Βάσεων Δεδομένων (database security): Αναφέρεται στην ικανότητα του συστήματος να εφαρμόσει μια προκαθορισμένη πολιτική προστασίας των περιεχομένων μιας βάσης δεδομένων, στην οποία

διευκρινίζεται ποιοι εξουσιοδοτούνται να δουν ή / και να τροποποιήσουν τα προστατευμένα δεδομένα.

- Ασφάλεια Δικτύων Επικοινωνιών (network security): Αναφέρεται στην προστασία των πληροφοριών κατά τη μετάδοσή τους μέσω των τηλεφωνικών, δορυφορικών ή άλλων δικτύων, όπως είναι τα τοπικά δίκτυα και το Internet.(Liebeherr, El Zarki.2004)

1.2.5 Επίπεδα προστασίας των πληροφοριακών συστημάτων

Γενικά, υπάρχουν τέσσερις βασικοί τρόποι άμυνας οι οποίοι μπορεί να βοηθήσουν ώστε να υπάρξει επαρκής ασφάλεια σε ένα πληροφοριακό σύστημα (ΠΣ):

- Μέτρα προσπέλασης συστήματος: Με αυτό το μέτρο εξασφαλίζουμε ότι οι μη εξουσιοδοτημένοι χρήστες δεν μπορούν να εισάγονται (log in) στο σύστημα.
- Μέτρα προσπέλασης δεδομένων: Σε αυτήν τη φάση ελέγχουμε ποιος μπορεί να έχει πρόσβαση σε ποια δεδομένα και με ποιο σκοπό. Οι εφαρμογές βάσεων δεδομένων τυπικά απαιτούν έναν υψηλό βαθμό λεπτομέρειας (granularity) του ελέγχου προσπέλασης.
- Διαχείριση συστήματος και ασφάλειας: Εκτέλεση των off – line διαδικασιών που διαμορφώνουν ή επιβάλλουν ένα ασφαλές σύστημα, ορίζοντας ξεκάθαρα τις υπευθυνότητες του διαχειριστή συστήματος, εκπαιδεύοντας τους χρήστες κατάλληλα και ελέγχοντας ότι οι διαδικασίες ασφάλειας τηρούνται από τους χρήστες.
- Σχεδιασμός συστήματος: Αξιοποίηση βασικών χαρακτηριστικών και δυνατοτήτων ασφάλειας του υλικού και του λογισμικού.

Οι βασικοί τύποι μέτρων (controls) για την πρόληψη της εκμετάλλευσης των ευπαθειών ενός πληροφοριακού συστήματος είναι:

- Κρυπτογράφηση (encryption): Αλλάζουμε τα δεδομένα ώστε να είναι ακατάληπτα από τον εξωτερικό παρατηρητή, με αυτόν τον τρόπο οι υποκλοπές και η πιθανότητα για τροποποιήσεις σχεδόν εκμηδενίζεται.

- Μέτρα Λογισμικού (software controls): Τα προγράμματα πρέπει να είναι όσο το δυνατόν πιο ασφαλή και αξιόπιστα ώστε να αποτρέπουν εξωτερικές επιθέσεις. Τα μέτρα προγραμμάτων περιλαμβάνουν:

    - Μέτρα ανάπτυξης (development controls): Είναι τα πρότυπα (standards) σύμφωνα με τα οποία σχεδιάζονται, κωδικοποιούνται, ελέγχονται και συντηρούνται τα προγράμματα.
    - Μέτρα λειτουργικού συστήματος (operating system controls): Αφορά τους περιορισμούς που επιβάλλονται από το λειτουργικό σύστημα που έχει σκοπό την προστασία κάθε χρήστη από τους υπόλοιπους χρήστες.
    - Μέτρα μέσα στα προγράμματα (internal program controls): Τα μέτρα αυτά επιβάλλουν περιορισμούς ασφάλειας, όπως για παράδειγμα βάζουμε κάποιους περιορισμούς για να μπορεί κάποιος να προσπέλαση σε ένα σύστημα διαχείρισης βάσης δεδομένων (ΣΔΒΔ).

- Μέτρα Υλικού (hardware controls): Έχουν ανακαλυφθεί αρκετές συσκευές για να βοηθούν στην ασφάλεια υπολογιστών. Αυτές ποικίλλουν από την υλοποίηση της κρυπτογράφησης με υλικό μέχρι τις συσκευές για επιβεβαίωση της ταυτότητας των χρηστών.
- Φυσικά Μέτρα Υλικού (physical controls): Τα φυσικά μέτρα είναι από τα πιο εύκολα, πιο αποτελεσματικά και λιγότερο δαπανηρά μέτρα για την ασφάλεια των πληροφοριακών συστημάτων και των συστημάτων βάσεων δεδομένων (για παράδειγμα, κλειδαριές στις πόρτες, φύλακες, αντίγραφα ασφάλειας, κ.α.).
- Πολιτικές Ασφάλειας (security policies): Μερικά άλλα μέτρα αποτελούν αντικείμενο πολιτικής, όπως για παράδειγμα ο έλεγχος προσπέλασης. Παρά τα προβλήματα διαχείρισης σε μεγάλους και εξελισσόμενους οργανισμούς, οι πολιτικές ελέγχου προσπέλασης πρέπει να προσαρμόζονται στις επιμέρους συνθήκες και απαιτήσεις ασφάλειας του κάθε πληροφοριακού συστήματος.

1.2.5.1 Φυσική ασφάλεια του πληροφοριακού συστήματος

Η φυσική ασφάλεια αφορά το 'φυσικό περιβάλλον' (για παράδειγμα τα κτίρια και τους χώρους των μηχανογραφικών κέντρων (computer rooms)). Μια πρώτη άμυνα ενάντια σε πιθανές εισβολές παρέχουν τα κλασσικά μέσα προστασίας, όπως ο έλεγχος της φυσικής προσπέλασης, (οι φύλακες, οι βιομετρικές συσκευές, οι αντικλεπτικοί συναγερμοί, κ.α.). (Πομπόρτσης 2003).

Περιλαμβάνει τα παρακάτω βασικά θέματα προστασίας:

- Προστασία των χώρων του Κέντρου Πληροφορικής και ιδιαίτερα του computer room (π.χ. ελεγχόμενη πρόσβαση).
- Προστασία του υλικού (hardware) από οποιαδήποτε απειλή, βλάβη ή ανθρώπινη απροσεξία.
- Προστασία των εφεδρικών αντιγράφων (backup) του λογισμικού συστήματος των προγραμμάτων εφαρμογών (βιβλιοθηκών, πακέτων) και των δεδομένων του οργανισμού.
- Εγκατάσταση συστημάτων προστασίας, όπως για παράδειγμα συστήματος αδιάλειπτης λειτουργίας (U.P.S), συστήματος πυρόσβεσης με αδρανές αέριο, κ.α.

Παραδείγματα πιθανών κινδύνων (security threats):

1. Βλάβη ή καταστροφή υλικού (hardware).
2. Απώλεια δεδομένων.
3. Αλλαγή δηλωμένων χαρακτηριστικών των περιφερειακών συσκευών.
4. Λανθασμένα αποτελέσματα.
5. Λανθασμένες εκτυπώσεις

Παραδείγματα βασικών μέτρων προστασίας (counter - measures):

- Έλεγχος και απαγόρευση της μη εξουσιοδοτημένης πρόσβασης σε ευαίσθητους χώρους, όπως τα computer room, τα τερματικά, οι βιβλιοθήκες ταινιών και δίσκων, κ.λπ.

- ❖ Δημιουργία πινάκων εξουσιοδότησης που απεικονίζουν το δικαίωμα πρόσβασης του κάθε χρήστη (κατηγορίας χρηστών) στους διάφορους πόρους του συστήματος (δίσκους, ταινίες, αρχεία ή πίνακες βάσεων δεδομένων, κ.λπ.).
- ❖ Στατιστική παρακολούθηση των παραβιάσεων της ασφάλειας του πληροφοριακού συστήματος.
- ❖ Προσεκτική επιλογή και σωστή διοικητική εποπτεία των εργαζομένων στο Κέντρο Πληροφορικής
- ❖ Δημιουργία χώρων εργασίας που ικανοποιούν τις βασικές προϋποθέσεις ασφάλειας (προστασία από πιθανές φυσικές καταστροφές, συνθήκες κατάλληλου φωτισμού και κλιματισμού κ.λπ.).
- ❖ Τήρηση ασφαλών δομικών προδιαγραφών με συστήματα πυρόσβεσης, πυρασφαλή δωμάτια ή χώρους φύλαξης αρχείων κ.λ.π.

1.2.6 Πολιτική ασφάλειας στην ευαισθησία πληροφοριών

Για να μπορούμε να γνωρίζουμε κατά πόσον ένα υπολογιστικό σύστημα παρέχει την αναμενόμενη ασφάλεια, πρέπει να μπορούμε να διατυπώσουμε το τι είναι αυτή η ασφάλεια. Οι απαιτήσεις ασφάλειας ενός υπολογιστικού συστήματος προσδιορίζονται διαμέσου μιας πολιτικής ασφάλειας. (Stajano, Anderson,2002).

Η πολιτική ασφάλειας (security policy) ενός υπολογιστικού συστήματος είναι ένα σύνολο από αρχές (principles) και οδηγίες υψηλού επιπέδου (high level guidelines) που αφορούν τη σχεδίαση και διαχείριση συστημάτων ασφάλειας.

Μια πολιτική ασφάλειας εκφράζεται με κανόνες (rules) που ρυθμίζουν πως ελέγχονται τα συμμετέχοντα μέρη και πως λαμβάνονται οι αποφάσεις για προσπέλαση. Συνήθως επιβάλλονται από διάφορους μηχανισμούς ασφάλειας, οι οποίοι μπορούν να καταταγούν στις παρακάτω κατηγορίες:

- o αναγνώριση (identification),
- o αυθεντικότητα (authentication),
- o εξουσιοδότηση (authorization),
- o έλεγχο προσπέλασης (access control),

- ακεραιότητα (integrity),
- συνέπεια (consistency),
- επίβλεψη (auditing).

Οι μηχανισμοί ασφάλειας (security mechanisms) είναι χαμηλού επιπέδου λειτουργίες λογισμικού και υλικού που μπορούν να διαμορφώνονται κατάλληλα για την υλοποίηση μιας πολιτικής ασφάλειας.(Liebeherr, El Zarki.2004)

Το λεξιλόγιο TCSEC ορίζει μια πολιτική ασφάλειας ως 'το σύνολο νόμων, κανόνων και πρακτικών που ρυθμίζουν πως ένας οργανισμός διαχειρίζεται, προστατεύει και κατανέμει ευαίσθητες πληροφορίες'. Ομοίως, το λεξιλόγιο ITSEC ορίζει τον όρο πολιτική ασφάλειας ως 'το σύνολο νόμων, κανόνων και πρακτικών που ρυθμίζουν πως τα στοιχεία διαχειρίζονται, προστατεύονται και κατανέμονται μέσα σε έναν οργανισμό χρηστών'.

Μια πολιτική ασφάλειας ορίζεται τυπικά στη βάση των όρων υποκείμενα και αντικείμενα. Ένα υποκείμενο είναι κάτι ενεργό στο σύστημα, όπως για παράδειγμα οι χρήστες (users), οι διεργασίες (processes) και τα προγράμματα (programs). Αντικείμενο είναι κάτι στο οποίο ενεργεί το υποκείμενο. Παραδείγματα αντικειμένων είναι τα αρχεία (files), οι κατάλογοι (directories), οι συσκευές (devices), οι υποδοχές (sockets) και τα παράθυρα (windows). (Henmi, 2006)

1.3 Ασφάλεια σε περιβάλλον διαδικτύου

1.3.1 Δίκτυα και Internet

Δίκτυο είναι μια ομάδα υπολογιστών συνδεδεμένων μεταξύ τους είτε ενσύρματα είτε ασύρματα, η οποία επιτρέπει σε πολλούς ανθρώπους να ανταλλάσουν πληροφορίες και να διαμοιράζονται εξοπλισμό. Με την διασύνδεση ενός συνόλου υπολογιστών, ένα δίκτυο επικοινωνιών σχηματίζεται με τρόπο τέτοιο ώστε, να μπορούν να ανταλλάσουν πληροφορίες. Η επικοινωνία των υπολογιστών επιτυγχάνεται με την ανταλλαγή μηνυμάτων ειδικής φόρμας ακολουθώντας ειδικούς κανόνες (πρωτόκολλα) ώστε να μπορούν να τα ερμηνεύουν όλοι οι υπολογιστές που διαθέτουν τις αντίστοιχες προβλέψεις υπό μορφή υλικού (π.χ. κάρτας δικτύου) και λογισμικού (π.χ. πρωτόκολλο TCP/IP). (Πομπόρτσης 2003).

Η απλούστερη μορφή δικτύου λαμβάνει χώρα όταν οι υπολογιστές συνδέονται ανά δύο απ' ευθείας με μια τηλεπικοινωνιακή ζεύξη σημείου προς σημείο. Εκτός από πολύ απλές

περιπτώσεις αυτό δεν είναι και τόσο χρήσιμη λύση διότι δεν είναι γενικεύσιμη. Οι υπολογιστές μπορεί να βρίσκονται πολύ μακριά ο ένας από τον άλλον, ώστε να μην δικαιολογείται το κόστος της απ' ευθείας σύνδεσης. Ανάλογα με την τοποθεσία των υπολογιστών που συνδέονται, ένα δίκτυο χαρακτηρίζεται ως:

- Τοπικό Δίκτυο (Local Area Network – LAN).
- Μητροπολιτικό Δίκτυο (Metropolitan Area Network – MAN).
- Δίκτυο Ευρείας Περιοχής (Wide Area Network – WAN).
- Προσωπικά δίκτυα (PAN).
- Διαδίκτυο

1.3.2 Θέματα ασφάλειας δικτύων και κατανεμημένων συστημάτων

Το πρόβλημα της ασφάλειας των πληροφοριών είναι ιδιαίτερα σημαντικό στα σύγχρονα δίκτυα υπολογιστών. Η χρησιμοποίηση όλο και πιο προχωρημένων τεχνικών και τεχνολογιών όπως για παράδειγμα οι σύγχρονες βάσεις δεδομένων και τα σύγχρονα δίκτυα, προσφέρει αναμφισβήτητα σημαντικά πλεονεκτήματα και δυνατότητες, αυξάνει όμως ταυτόχρονα σημαντικά τα προβλήματα τα σχετικά με την προστασία και τη διαθεσιμότητα των πληροφοριών.

Η ασφάλεια αποτελεί αναγκαία συνθήκη και είναι απαραίτητη, σε συνδυασμό με τις άλλες βασικές προϋποθέσεις λειτουργίας όπως η ποιότητα και η απόδοση, για την εξασφάλιση της εύρυθμης λειτουργίας μιας επιχείρησης ή ενός οργανισμού. Αυτό είναι ιδιαίτερα σημαντικό σήμερα όπου πολύ συχνά το σύνολο των παρερχομένων υπηρεσιών μιας επιχείρησης στηρίζεται στην πληροφορική (π.χ. πάνω από το 80% των υπηρεσιών μιας τράπεζας).

Η έννοια της ασφάλειας ενός Δικτύου Υπολογιστών σχετίζεται με την ικανότητα μιας επιχείρησης ή ενός οργανισμού να προστατεύει τις πληροφορίες του από τυχόν αλλοιώσεις και καταστροφές, καθώς και από μη εξουσιοδοτημένη χρήση των πόρων του. Σχετίζεται επίσης με την ικανότητά του να παρέχει ορθές και αξιόπιστες πληροφορίες, οι οποίες είναι διαθέσιμες στους εξουσιοδοτημένους χρήστες κάθε φορά που τις αναζητούν. Η ικανότητα αυτή στηρίζεται στη λήψη μέτρων τα οποία διασφαλίζουν την ακεραιότητα και την εμπιστευτικότητα των δεδομένων, καθώς και την αδιάλειπτη λειτουργία του δικτύου. (Stajano, Anderson,2002).

1.3.3 Ασφάλεια στο διαδίκτυο

Σύμφωνα με τον προηγούμενο ορισμό της ασφάλειας, η ασφάλεια στα δίκτυα υπολογιστών έχει να κάνει με την πρόληψη και ανίχνευση μη εξουσιοδοτημένων ενεργειών των χρηστών του δικτύου καθώς και την λήψη μέτρων.

Ποιο συγκεκριμένα η ασφάλεια στα δίκτυα υπολογιστών σχετίζεται με:

- Πρόληψη (prevention): Την λήψη δηλαδή μέτρων για να προληφθούν φθορές των μονάδων ενός δικτύου υπολογιστών.
- Ανίχνευση (detection): Την λήψη μέτρων για την ανίχνευση του πότε, πώς και από ποιον προκλήθηκε φθορά σε μία από τις παραπάνω μονάδες.
- Αντίδραση (reaction): Την λήψη δηλαδή μέτρων για την αποκατάσταση ή ανάκτηση των συστατικών ενός δικτύου.

Η ασφάλεια δικτύων και πληροφοριών μπορεί ακόμη να οριστεί ως η δυνατότητα ενός δικτύου ή συστήματος πληροφοριών να αντισταθεί, σε δεδομένο επίπεδο αξιοπιστίας, σε τυχαία συμβάντα ή κακόβουλες ενέργειες που θέτουν σε κίνδυνο τη διάθεση, την επαλήθευση ταυτότητας, την ακεραιότητα και την τήρηση του απορρήτου των δεδομένων που έχουν αποθηκευτεί ή μεταδοθεί καθώς και τις συναφείς υπηρεσίες που παρέχονται είτε είναι προσβάσιμες μέσω των δικτύων και συστημάτων αυτών. (Weber,2010)

Η προστασία ενός δικτύου το οποίο συνδέεται και με το Internet είναι ένα θέμα που καλούνται να αντιμετωπίσουν οι σύγχρονες επιχειρήσεις και οργανισμοί. Είναι γενικά αποδεκτό σήμερα ότι η έννοια της ασφάλειας των δικτύων υπολογιστών αλλά και των πληροφοριακών συστημάτων γενικότερα, συνδέεται στενά με τρεις βασικές έννοιες:

- Διαθεσιμότητα {Availability}
- Εμπιστευτικότητα {Confidentiality}
- Ακεραιότητα {Integrity}

1.3.4 Εντοπισμός και διαχείριση των κινδύνων

Η πρόσβαση στο Διαδίκτυο σήμερα δεν είναι ακίνδυνη, ανεξάρτητα από τον τρόπο χρήσης των υπηρεσιών του. Υπάρχουν κακόβουλοι χρήστες και αρκετές δυνατότητες πρόκλησης ζημιών τόσο στο επίπεδο του χρησιμοποιούμενου λογισμικού και υλικού, όσο και σε προσωπικό επίπεδο.

1.3.4.1 Πρόκληση ζημιών στο υπολογιστικό σύστημα

Ο κύριος κίνδυνος πρόκλησης ζημιών στο υπολογιστικό σύστημα ενός ανύποπτου χρήστη είναι η μόλυνση του συστήματος με κάποιον ιό. Η μόλυνση γίνεται όταν ο χρήστης καλείται να λάβει κάποιο αρχείο, φαινομενικά αθώο, όπως ένα κείμενο ή μια φωτογραφία και, όταν δοκιμάσει να το χρησιμοποιήσει, ο ιός αναλαμβάνει δράση επιμολύνοντας το σύστημα και μπορεί να καταστρέψει αρχεία ή το σκληρό δίσκο του συστήματος. Άλλες φορές είναι δυνατή η αποστολή ιού απευθείας από τον ιστότοπο που επισκέπτεται ο χρήστης, χωρίς να εμφανισθεί κάποια ένδειξη λήψης αρχείου.(Liebeherr, El Zarki.2004)

Η περίπτωση αυτή εκμεταλλεύεται κενά ασφαλείας στο λογισμικό του χρήστη (φυλομετρητή ή Λειτουργικό Σύστημα). Παρόμοιας δράσης είναι και ένα πρόγραμμα που αποκαλείται worm (κατά λέξη μετάφραση σκουλήκι). Είναι παρόμοιο σε αποτέλεσμα με τον ιό, αλλά, αντίθετα από αυτόν, δεν απαιτεί την "προσκόλλησή" του σε ένα αρχείο, έχοντας έτσι περισσότερη αυτονομία. Η βλάβη που προκαλεί το worm δεν είναι τόσο ευρεία στο σύστημα, όσο στο δίκτυο σύνδεσης, επειδή καταναλώνει σημαντικό εύρος ζώνης (bandwidth). Άλλος κίνδυνος είναι ο Δούρειος Ίππος, ένα πρόγραμμα που ξεγελά το χρήστη του, ο οποίος χρησιμοποιώντας το νομίζει ότι εκτελεί κάποια εργασία, ενώ στην πραγματικότητα εκτελεί κάποια άλλη, συνήθως εγκατάσταση άλλων κακόβουλων προγραμμάτων. Αντίθετα από τους ιούς, οι δούρειοι ίπποι δεν επιμολύνουν αρχεία.

1.3.4.2 Πρόκληση ζημιών σε προσωπικά δεδομένα

Στην κατηγορία αυτή υπάγονται τόσο οι δούρειοι ίπποι που προαναφέρθηκαν, όσο και κακόβουλα μηνύματα ηλεκτρονικού ταχυδρομείου. Με τον τρόπο αυτό όχι μόνον είναι δυνατό να κλαπούν προσωπικά δεδομένα κάποιου χρήστη, όπως ο αριθμός ταυτότητάς του ή το ΑΦΜ του, όσο και, πιο σημαντικό, αριθμοί πιστωτικών καρτών, λογαριασμών Τραπέζης κτλ.

Ανάλογη μέθοδος ακολουθείται και από ορισμένους ιστοτόπους, στους οποίους ο ανύποπτος χρήστης καταχωρεί παρόμοια στοιχεία παραγγέλλοντας ένα προϊόν, το οποίο όχι μόνο δε θα λάβει ποτέ, αλλά τα δεδομένα του μπορούν να χρησιμοποιηθούν από τους δημιουργούς του ιστοτόπου για να πραγματοποιήσουν οι ίδιοι αγορές, χρεώνοντας τον "πελάτη" τους. Η μέθοδος υφαρπαγής προσωπικών δεδομένων μέσω ηλεκτρονικού ταχυδρομείου αποκαλείται "Phishing" (παραφθορά της λέξης fishing = ψάρεμα). (Weber,2010)

1.3.4.3 Διαχείριση κινδύνων

Υπάρχουν τρεις τρόποι προστασίας, οι οποίοι θα πρέπει να χρησιμοποιούνται σε συνδυασμό για τη διαχείριση των κίνδυνων δικτύου:

- Χρήση τείχους προστασίας (firewall)
- Χρήση λογισμικού προστασίας ενάντια σε ιούς και προγράμματα κατασκοπείας (spyware).
- Συνεχής ενημέρωση των χρηστών.

1.3.4.3.1 Τείχος προστασία

Τα τείχη προστασίας χρησιμοποιούνται τόσο από μεμονωμένους καταναλωτές όσο και από μεγάλες επιχειρήσεις, είτε ως λογισμικό είτε ως υλικό, για τη σάρωση πακέτων δεδομένων που εισέρχονται και εξέρχονται από τον υπολογιστή μέσω του διαδικτύου. Εάν το φίλτρο του τείχους προστασίας αιχμαλωτίζει τυχόν ύποπτα πακέτα, δεν τους επιτρέπεται η πρόσβαση στο σύστημα σου και στο ιδιωτικό δίκτυο.

Τα τείχη προστασίας είναι ζωτικής σημασίας για την διακοπή της επικίνδυνης ή δόλιας κίνησης από το δίκτυο. Αποκλείουν συγκεκριμένα προγράμματα από την πρόσβαση στο διαδίκτυο εάν η δραστηριότητα θεωρείται υπερβολικά επικίνδυνη. Το 2019, κάθε μηχάνημα χρειάζεται ένα τείχος προστασίας, γι ‘αυτό τα εταιρικά τμήματα πληροφορικής έχουν κατά κανόνα σαν προτεραιότητα την εγκατάσταση τείχους προστασίας ως βασικό πυρήνα της εταιρικής ασφάλειας στον κυβερνοχώρο. (Πομπόρτσης 2003).

1.3.4.3.2 Λογισμικό προστασίας (Antivirus)

Το antivirus είναι ένα πρόγραμμα που έχει σχεδιαστεί για την προστασία των χρηστών και των συσκευών τους από δυνητικούς επιβλαβείς ιούς υπολογιστών, κακόβουλο λογισμικό και άλλες κυβερνοαπειλές. Είναι σημαντικό τόσο οι επιχειρήσεις όσο και οι οικιακοί χρήστες να προστατεύονται από ιούς και άλλες επιθέσεις που θα μπορούσαν να διαταράξουν, να επιβραδύνουν, ακόμα και να καταστρέψουν τη συσκευή τους. Το antivirus είναι το βασικό εργαλείο που βοηθάει στην ασφαλή και ομαλή λειτουργία του υπολογιστή και των άλλων συσκευών σας.

Τα διάφορα antivirus διαφέρουν σε ότι αφορά τις μεθόδους τους, ωστόσο όλα έχουν τον ίδιο στόχο: να προστατέψουν τις συσκευές σας

Αφού το antivirus εγκατασταθεί, λειτουργεί στο παρασκήνιο, εκτελώντας τακτικές σαρώσεις και ελέγχους στις συσκευές σας, παρακολουθώντας τα αρχεία, τα προγράμματα και τις ιστοσελίδες για πιθανές απειλές. Το antivirus ανιχνεύει οποιαδήποτε κακόβουλη ή απειλητική συμπεριφορά θα μπορούσε να θεωρηθεί ως μορφή κακόβουλου λογισμικού, αφαιρώντας το από τη συσκευή σας όσο το δυνατόν γρηγορότερα, ενώ εργάζεται για να αποτρέψει μελλοντικές επιθέσεις.

Το antivirus έχει σχεδιαστεί για να προστατεύει τους χρήστες από κυβερνοαπειλές, όπως:

- Malware
- Ransomware
- Spam
- Trojan Horses
- Adware
- Spyware

2 ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΩΝ ΣΤΟ ΕΡΓΑΣΙΑΚΟ ΠΕΡΙΒΑΛΛΟΝ

2.1 Εισαγωγή

Οι εταιρείες καθημερινά ασχολούνται με τη συλλογή, αποθήκευση επεξεργασία και διακίνηση πληροφοριών στα πλαίσια της εκτέλεσης των επιχειρησιακών τους λειτουργιών. Συνεπώς, καταλαβαίνουμε πόσο μεγάλη σημασία παίζει η προστασία των διάφορων πληροφοριών και των συστημάτων επεξεργασίας τους ώστε να επιτύχει τους στόχους τις η εταιρία.

Για να εξασφαλιστεί η εύρυθμη λειτουργία μιας εταιρίας σε συνδυασμός με την ασφαλή λειτουργία των πληροφοριακών συστημάτων η Διοίκηση κάθε εταιρίας προβαίνει στις κατάλληλες ενέργειες που θα συμβάλουν στην επίτευξη αυτού του στόχου. Πρόκειται, ουσιαστικά, για διάφορα μέτρα σε τεχνικό και οργανωτικό επίπεδο τα οποία στοχεύουν στην εξασφάλιση της ακεραιότητας, της διαθεσιμότητας αλλά και της εμπιστευτικότητας των πληροφοριών που επεξεργάζεται. Επιπρόσθετα, εφαρμόζονται πολιτικές και διαδικασίες στα πλαίσια των οποίων:

- Ορίζονται οι οργανωτικές δομές που είναι απαραίτητες για την παρακολούθηση θεμάτων σχετικών με την Ασφάλεια Πληροφοριών
- Ορίζονται τα τεχνικά μέτρα ελέγχου και περιορισμού της πρόσβασης σε πληροφορίες και πληροφοριακά συστήματα
- Καθορίζεται ο τρόπος διαβάθμισης των πληροφοριών ανάλογα με τη σπουδαιότητα και την αξία τους
- Περιγράφονται οι απαραίτητες ενέργειες προστασίας των πληροφοριών κατά τα στάδια της επεξεργασίας, αποθήκευσης και διακίνησής τους
- Καθορίζονται οι τρόποι ενημέρωσης και εκπαίδευσης των υπαλλήλων και των συνεργατών της εταιρείας σε θέματα Ασφάλειας Πληροφοριών
- Προσδιορίζονται οι τρόποι αντιμετώπισης περιστατικών Ασφάλειας Πληροφοριών

- Περιγράφονται οι τρόποι με τους οποίους διασφαλίζεται η ασφαλής συνέχεια των επιχειρησιακών λειτουργιών της εταιρείας σε περιπτώσεις δυσλειτουργίας πληροφοριακών συστημάτων ή σε περιπτώσεις καταστροφών

2.2 Τρόποι ασφάλειας στον εργασιακό περιβάλλον

Οι τρόποι που εξασφαλίζουν την ασφάλεια στον εργασιακό τομέα αναφέρονται ως Αντίμετρα, και αφορούν όλες τις διαδικασίες, τις τεχνικές, τις ενέργειες και τις συσκευές που περιορίζουν τις ευπάθειες και τις απειλές του πληροφοριακού συστήματος, καθώς και το Πλάνο Υλοποίησης τους.

Τα αντίμετρα χωρίζονται σε τέσσερις μεγάλες κατηγορίες:

1. Πρόληψη (Prevention): η προσφυγή σε μέτρα που προσπαθούν να μειώσουν τον κίνδυνο.
2. Διασφάλιση (Ensuring): εργαλεία, έλεγχοι και στρατηγικές που διασφαλίζουν την συνεχή αποτελεσματικότητα των παρόντων αντιμέτρων.
3. Ανίχνευση (Detection): η προσφυγή σε προγράμματα και τεχνικές για την έγκαιρη ανίχνευση, αναχαίτιση και αντιμετώπιση περιστατικών.
4. Επαναφορά (Reinstatement): διαδικασίες που στοχεύουν στην γρήγορη επαναφορά σε ένα ασφαλές περιβάλλον έπειτα από ρήξη ασφαλείας και στην έρευνα της αιτίας που την προκάλεσε.

Για την επιτυχή εφαρμογή της πολιτικής ασφαλείας, το σχέδιο ασφαλείας πρέπει να περιλαμβάνει και συγκεκριμένες διαδικασίες συνεχούς ενημέρωσης με επισκοπήσεις – επιθεωρήσεις της εφαρμογής του, ώστε με τις κατάλληλες αναθεωρήσεις να είναι πάντα ενημερωμένο (up-to-date) σε σχέση με τις τεχνολογικές εξελίξεις και τις αλλαγές στην εταιρεία. (Γκριτζαλης,2003)

Ολοκληρώνοντας το σχέδιο ασφάλειας της εταιρείας θα ακολουθήσουν τα εξής:

1. Κατάρτιση αναλυτικού σχεδίου έκτακτης ανάγκης, το οποίο θα περιλαμβάνει σχέδιο ανάκαμψης από καταστροφή (disaster recovery plan)
2. Κατάρτιση σχεδίου αποκατάστασης λειτουργίας (contingency action plan).

3. Εγκατάσταση και τακτική ενημέρωση προγραμμάτων antivirus για τον έλεγχο προσωπικών υπολογιστών και αποθηκευτικών μέσων.
4. Τακτικός έλεγχος του χρησιμοποιούμενου λογισμικού και των αρχείων του συστήματος. Οποιαδήποτε αλλαγή θα πρέπει να ερευνάται.
5. Ο έλεγχος αρχείων και αποθηκευτικών μέσων για ιούς πριν από την χρήση τους.
6. Ο έλεγχος των εισερχόμενων ηλεκτρονικών μηνυμάτων για ιούς. Ο συγκεκριμένος έλεγχος μπορεί να γίνει σε διάφορα σημεία του συστήματος, όπως τους εξυπηρετητές ηλεκτρονικού ταχυδρομείου, τους προσωπικούς υπολογιστές κλπ.
7. Την εκπαίδευση των χρηστών και ύπαρξη διαδικασιών για την αντιμετώπιση ιών.
8. Την ύπαρξη σχεδίου επιχειρησιακής συνέχειας στην περίπτωση εκτεταμένων ζημιών στο σύστημα από ιούς.
9. Την ύπαρξη διαδικασιών για έλεγχο της ακρίβειας της πληροφόρησης για ιούς

Η εισαγωγή (προσθήκη μηχανισμών) ασφαλείας σε ένα πληροφοριακό σύστημα είναι ένα δύσκολο και περίπλοκο έργο. Για την ελληνική πραγματικότητα ίσως η πλέον σημαντική δυσκολία οφείλεται στο σημαντικό κόστος της ασφάλειας. (Weber,2010)

2.3 Ευαισθησίες – κίνδυνοι

Ως απειλή μπορεί να θεωρηθεί οποιαδήποτε πιθανή ενέργεια ή ένα γεγονός που μπορεί να προκαλέσει την απώλεια ενός ή περισσοτέρων ιδιοτήτων-χαρακτηριστικών ασφαλείας ενός πληροφοριακού συστήματος. Οι απειλές που εντοπίζονται στα πληροφοριακά συστήματα, δεν προέρχονται μόνο από κακόβουλες ενέργειες που προκαλούνται από εξωτερικές ή εσωτερικές οντότητες, αλλά συμπεριλαμβάνουν και σχεδιαστικά λάθη ή μη ηθελημένες ενέργειες που μπορούν να οδηγήσουν το πληροφοριακό σύστημα σε μη εκπλήρωση των στόχων του.

Η ανάλυση επικινδυνότητας (risk analysis) είναι η διαδικασία αναγνώρισης κινδύνων και ο υπολογισμός επικινδυνότητας. Η εκτίμηση επικινδυνότητας (risk assessment) είναι η

διαδικασία αξιολόγησης της υπολογισμένης επικινδυνότητας σε σχέση με τα κριτήρια αξιολόγησης της σημαντικότητάς τους.

Η συνολική διαδικασία ανάλυσης και εκτίμησης επικινδυνότητας αποτελεί την αποτίμηση επικινδυνότητας. Η αποτίμηση και διαχείριση επικινδυνότητας (risk assessment and management) στηρίζεται στην αρχή ότι απόλυτη ασφάλεια δεν είναι δυνατό να υπάρξει, άρα το καλύτερο που μπορεί να γίνει είναι να εξισορροπηθεί η έκταση των πιθανών κινδύνων με κόστος εφαρμογής των κατάλληλων αντιμέτρων (countermeasures). Επομένως, χρειαζόμαστε μεθοδολογίες που επιτρέπουν τη μέτρηση των κινδύνων και την έκφρασή τους σε κοινές μονάδες μέτρησης με την αποτελεσματικότητα των αντιμέτρων, ώστε να είναι δυνατή η σύγκρισή τους. (Πομπόρτσης 2003).

Γι' αυτό το λόγο πρέπει να υπολογιστεί η επικινδυνότητα ενός συστήματος ως συνάρτηση των εξής παραγόντων:

- Της αξίας των περιουσιακών του στοιχείων
- Της φύσης και του βαθμού των ευπαθειών του
- Της φύσης και της πιθανότητας εμφάνισης απειλών εναντίον του
- Της φύσης και έντασης των επιπτώσεων που θα έχουν οι απειλές αν πραγματοποιηθούν

2.4 Τρόποι εκπαίδευσης προσωπικού για την ασφάλεια πληροφοριών

Η εκπαίδευση του προσωπικού σε θέματα προστασίας προσωπικών δεδομένων, καθώς και σε ειδικές σχετικές με ασφάλεια λειτουργίες του πληροφοριακού συστήματος (π.χ. χρήση μη προβλέψιμων κωδικών πρόσβασης και συνθηματικών, τρόπο εντοπισμού και αναφοράς των περιστατικών παραβίασης της ασφαλείας, σωστή χρήση των e-mail και των αποσπώμενων μέσων αποθήκευσης) είναι ιδιαιτέρως σημαντική για την ορθή εφαρμογή των οργανωτικών και τεχνικών μέτρων ασφαλείας.

Η εκπαίδευση κατά την πρόσληψη πρέπει να περιλαμβάνει κατ' ελάχιστο την κοινοποίηση στους εργαζόμενους της πολιτικής ασφαλείας, για την οποία πρέπει κατά το δυνατόν να διαπιστωθεί ότι είναι πλήρως κατανοητή από όλους, καθώς επίσης και των διαδικασιών διαχείρισης περιστατικών παραβίασης δεδομένων και ανάκαμψης από καταστροφές, εφόσον άπτονται των αρμοδιοτήτων τους. (Convery, 2004)

Σκόπιμο θα ήταν να υπάρχει εταιρικός δικτυακός τόπος (web portal) στον οποίον θα είναι αναρτημένη η περιγραφή των βασικών διαδικασιών ασφαλείας που πρέπει να γνωρίζουν τα μέλη του προσωπικού. Θα πρέπει επίσης η εκπαίδευση να συνεχίζεται και μετά την πρόσληψη, είτε σε σημαντικές αλλαγές των διαδικασιών ασφαλείας είτε κατά την εμφάνιση σημαντικών θεμάτων ασφαλείας. Επίσης, ως προς το σκοπό της εκπαίδευσης κρίνεται σκόπιμη η κατάρτιση ειδικότερων ενημερωτικών εντύπων.

Τέλος, πρέπει να παρέχεται στο προσωπικό που έχει αναλάβει τη διαχείριση της ασφάλειας διαρκής εξειδικευμένη εκπαίδευση σχετικά με τις τεχνολογικές εξελίξεις στο χώρο της ασφάλειας πληροφοριών.

2.5 Πολιτική ασφάλειας

Όταν αναφερόμαστε στη πολιτική ασφάλειας των Πληροφοριακών Συστημάτων, μιλάμε ουσιαστικά για το σκοπό και τους στόχους της ασφάλειας, όλες αυτές τις οδηγίες, διαδικασίες, κανόνες ρόλους και υπευθυνότητες που έχουν άμεση σχέση με την προστασία των ΠΣ ενός οργανισμού

Η διατύπωση της Πολιτικής Ασφάλειας γίνεται συνήθως σε ένα έγγραφο, το οποίο θα πρέπει να γνωρίζουν και να εφαρμόζουν όλοι οι χρήστες των ΠΣ. Οι οδηγίες και οι διαδικασίες που περιλαμβάνονται στην Πολιτική Ασφάλειας υλοποιούνται με την εφαρμογή των μέτρων προστασίας ή ασφάλειας (security measures, security controls)

Η Πολιτική Ασφάλειας μαζί με το σύνολο των μέτρων προστασίας αποτελούν το Σχέδιο Ασφάλειας (Security Plan) για τα πληροφοριακά συστήματα ενός οργανισμού.

2.5.1 Πολιτική ασφαλείας στη χρήση email

Η πολιτική ασφάλειας στη χρήση email ορίζει τους παρακάτω κανόνες που πρέπει να τηρούνται ευλαβικά για την αποφυγή κινδύνων :

1. Οι mail servers πρέπει να είναι παραμετροποιημένοι με τέτοιο τρόπο ώστε να εμποδίζεται η υπερφόρτωσή τους με τον περιορισμό των μηνυμάτων ανά mailbox, της χρήσης μεγάλων λιστών παραληπτών και την αυτόματη ανίχνευση και ακύρωση email loops.

2. Τα emails πρέπει να ελέγχονται για (α) Κακόβουλα συνημμένα (β) Φράσεις συσχετισμένες με κακόβουλο λογισμικό (γ) Απαγορευμένες λέξεις (π.χ. αισχρές, προσβλητικές ή ρατσιστικές)
3. Οι mail servers πρέπει να παρέχουν προστασία με το να (α) Αποκλείουν μηνύματα που θεωρούνται μη επιθυμητά (spam) (π.χ. χρησιμοποιώντας κάποια black list με μη επιθυμητούς ιστότοπους ή mail list servers) (β) Ελέγχουν την ακεραιότητα των μηνυμάτων ως προς την πληρότητα του περιεχόμενού τους. (π.χ. ένα μήνυμα να περιλαμβάνει όλα τα απαραίτητα headers.) (γ) Μην προωθούν αυτόματα emails προς εξωτερικούς παραλήπτες
4. Στα συστήματα ανταλλαγής email καλό είναι να χρησιμοποιούνται ψηφιακές υπογραφές.
5. Θα πρέπει να μην επιτρέπεται η απομακρυσμένη πρόσβαση στα emails του φορέα, εκτός του χώρου του.
6. Καλό είναι να μη χρησιμοποιείται webmail, καθώς προκαλεί περισσότερες τρωτότητες σε ένα σύστημα ανταλλαγής email.

Θα πρέπει να μην επιτρέπεται η χρήση email του φορέα για προσωπικούς / μη επαγγελματικούς λόγους του χρήστη.

2.5.2 Πολιτική ασφαλείας στη χρήση anti-virus

Η πολιτική ασφαλείας στη χρήση anti-virus ορίζει πως:

Πρέπει να υπάρχει εγκατεστημένη ολοκληρωμένη λύση λογισμικού προστασίας σε όλα τα συστήματα που είναι ευαίσθητα σε επιθέσεις κακόβουλου λογισμικού – ειδικά σε αυτά που έχουν πρόσβαση στο Διαδίκτυο.

1. Το λογισμικό προστασίας, εκτός από τους παραπάνω γενικούς κανόνες για λογισμικό, επιπλέον πρέπει να:
    a) Ενημερώνεται κάθε μέρα και με αυτόματο τρόπο.
    b) Προβλέπει προστασία από κάθε είδος κακόβουλου λογισμικού: ιοί, worms, trojan horses, rootkits, spyware και adware.

c) Είναι ρυθμισμένο να ελέγχει: τη μνήμη του Η/Υ, τα εκτελέσιμα αρχεία, τα προστατευμένα και κρυφά αρχεία, τα αφαιρούμενα μέσα αποθήκευσης (CDs / DVDs / USB συσκευές), την εισερχόμενη και εξερχόμενη δικτυακή κίνηση του φορέα. Γενικά μέτρα προστασίας πληροφοριακών συστημάτων από ηλεκτρονικές επιθέσεις

d) Είναι ρυθμισμένο να πραγματοποιεί ελέγχους σε πραγματικό χρόνο και όχι μετά από απαίτηση του χρήστη

e) Ενημερώνει έγκαιρα και αποτελεσματικά σε περίπτωση που ανακαλύψει ύποπτο λογισμικό

f) Απομονώνει το ύποπτο λογισμικό για περαιτέρω ανάλυση

g) Απομακρύνει το κακόβουλο λογισμικό και σχετικά αρχεία

h) Εξασφαλίζει ότι δεν υπάρχει δυνατότητα να απενεργοποιούνται σημαντικές ρυθμίσεις και να μην ελαχιστοποιείται η λειτουργικότητα

i) Διαθέτει μηχανισμό ειδοποίησης για την περίπτωση που είναι ανενεργό

2. Πρέπει να πραγματοποιείται τακτικός έλεγχος στα logs του λογισμικού προστασίας.
3. Δεν πρέπει να επιτρέπεται η εγκατάσταση λογισμικού από οποιονδήποτε χρήστη, αλλά από τον διαχειριστή (Administrator).
4. Δεν πρέπει να επιτρέπεται η χρήση αφαιρούμενων μέσων αποθήκευσης σε κρίσιμα συστήματα.
5. Εάν είναι απαραίτητη η χρήση αφαιρούμενων μέσων αποθήκευσης, πρέπει να απενεργοποιείται η δυνατότητα αυτόματης εκκίνησης (autorun).

2.5.3 Πολιτική ασφάλειας στη χρήση PASSWORDS

Σχετικά με τους κωδικούς ασφαλείας ισχύει πως:

1. Πρέπει να χρησιμοποιούνται κωδικοί ασφαλείας, όπου είναι δυνατόν.
2. Οι κωδικοί ασφαλείας πρέπει να είναι προσωπικοί για κάθε χρήστη.

3. Καλό είναι να επιλέγεται διαφορετικός κωδικός ασφαλείας για κάθε λογαριασμό, όταν χρησιμοποιούνται πολλοί λογαριασμοί από τον ίδιο χρήστη.
4. Οι κωδικοί ασφαλείας καλό είναι να έχουν μήκος τουλάχιστον 10 χαρακτήρων και να συμπεριλαμβάνουν αλφαριθμητικούς χαρακτήρες, πεζά και κεφαλαία καθώς και σημεία στίξης.
5. Οι κωδικοί ασφαλείας δεν πρέπει να καταγράφονται, γι' αυτό καλό είναι να τα απομνημονεύουμε.
6. Οι κωδικοί ασφαλείας καλό είναι να αλλάζουν περιοδικά, αλλά όχι σε λιγότερο χρονικό διάστημα από ένα μήνα, καθώς έτσι ενισχύεται η χρήση εύκολων κωδικών ή η καταγραφή τους.

2.5.3.1 Παράδειγμα επιλογής κωδικού ασφαλείας

Ένας τρόπος επιλογής κωδικού ασφαλείας με τα παραπάνω χαρακτηριστικά είναι η χρήση κάποια φράσης, όπου χρησιμοποιούνται επιλεκτικά οι χαρακτήρες της. Οι χαρακτήρες αυτοί επιπλέον μεταλλάσσονται σε αριθμητικούς και σημεία στίξης, ενώ πεζά εναλλάσσονται με κεφαλαία με κάποιο εύκολο αλγόριθμο. (Convery, 2004)

Π.χ. Φράση: "This is a very strong password, which protects my account!"

Αλγόριθμος: Επιλέγεται κάθε πρώτος χαρακτήρας, όπου a αντικαθίσταται με @, όπου i αντικαθίσταται με 1 και όπου p χρησιμοποιείται το κεφαλαίο P. Κωδικός: T1@vsP,wPm@!

2.5.4 Πολιτική ασφαλείας στην χρήση SERVERS

Οι διαδικτυακοί διακομιστές (web servers) θα πρέπει να:

A. Βρίσκονται διαχωρισμένοι από τα εσωτερικά δίκτυα (π.χ. εφαρμογή «Αποστρατικωποιημενης Ζώνης» - D.M.Z.)
B. Εκτελούνται σε "dedicated" υπολογιστές, που δεν εκτελούν άλλες εφαρμογές (π.χ. βάσεις δεδομένων, e-mail)
C. Εκτελούν τις εφαρμογές με περιορισμένα δικαιώματα, αφαιρώντας τη δυνατότητα εκτέλεσης με δικαιώματα διαχειριστή

D. Είναι παραμετροποιημένοι έτσι ώστε να μην εκτελούνται σενάρια (scripts) από μη εξουσιοδοτημένους χρήστες.

E. Ελέγχονται, ώστε να είναι απενεργοποιημένες περιττές διεργασίες κι υπηρεσίες

F. Είναι παραμετροποιημένοι, ώστε να διατηρούνται αρχεία καταγραφής συμβάντων (logs) για μεγάλο χρονικό διάστημα, τουλάχιστον δώδεκα (12) μηνών.

Οι συνδέσεις μεταξύ των διαδικτυακών διακομιστών και των "back office" συστημάτων (π.χ. διακομιστών βάσεων δεδομένων) πρέπει να:

a) Προστατεύονται με τείχη προστασίας

b) Περιορίζονται μόνο σε επιτρεπτές υπηρεσίες, απαραίτητες για τις εφαρμογές

c) Βασίζονται σε αξιόπιστες διεπαφές (application programming interfaces - APIs)

d) Προστατεύονται με τη χρήση αμοιβαίας αυθεντικότητας

Δεν πρέπει να υπάρχει άλλος τρόπος σύνδεσης σε back office συστήματα από χρήστες των εφαρμογών, εκτός μέσω του διαδικτυακού διακομιστή.

Οι λογαριασμοί χρηστών που χρησιμοποιούνται για τη σύνδεση διαδικτυακών διακομιστών και "back office" συστημάτων πρέπει να έχουν τα λιγότερα δυνατά δικαιώματα, αφαιρώντας έτσι τη δυνατότητα σύνδεσης με δικαιώματα διαχειριστή.

Η πληροφορία που χρησιμοποιείται στις εφαρμογές αυτές πρέπει να προστατεύεται από μη επιτρεπτή αποκάλυψη ή αλλοίωση με

a) Τον έλεγχο των δεδομένων εισόδου σε επίπεδο χρήστη αλλά και διακομιστή

b) Την κρυπτογράφηση ευαίσθητων δεδομένων κατά τη μεταφορά τους και την αποθήκευσή τους

c) Την προστασία αρχείων που περιέχουν ρυθμίσεις διασύνδεσης, με την τοποθέτησή τους σε τοποθεσίες με περιορισμένη πρόσβαση και περιορισμένα δικαιώματα.

Το περιεχόμενο των ιστοτόπων καλό είναι να:

a) Τοποθετείται σε διαφορετικό δίσκο από το λειτουργικό σύστημα

b) Προστατεύετε με την ρύθμιση των δικαιωμάτων των αρχείων

c) Ενημερώνεται από εξουσιοδοτημένα άτομα με εγκεκριμένα εργαλεία (π.χ. με SSH ή SFTP από καθορισμένη IP διεύθυνση)

d) Ελέγχεται η ακεραιότητά του, ότι οι σύνδεσμοί του είναι έγκυροι και λειτουργικοί και ότι δεν έχουν εισαχθεί τρωτότητες από σενάρια (scripts) ή «κρυφά» πεδία φόρμας. (Γκριτζαλης,2003)

3 ΗΛΕΚΤΡΟΝΙΚΗ ΜΑΘΗΣΗ ΩΣ ΤΡΟΠΟΣ ΕΚΠΑΙΔΕΥΣΗΣ

3.1 Εισαγωγή στην ηλεκτρονική μάθηση

Διαφοροποιημένες έννοιες έχουν χρησιμεύσει με στόχο να οριοθετήσουν τη μάθηση η οποία υλοποιείται σε απευθείας σύνδεση με το διαδίκτυο, κάτι το οποίο κάνει δύσκολη την ανάπτυξη ενός ευρύτερου ορισμού. Μελετητές συμφωνούν πως ένας ενιαίος ορισμός για τη συγκεκριμένη έννοια δεν έχει βρεθεί ακόμα. Όροι οι οποίοι χρησιμεύουν τις περισσότερες φορές για μάθηση σε σύνδεση στο διαδίκτυο είναι το elearning, το internet learning, το virtual learning, το distance learning κλπ. (Τζιμογιάννης, 2017)

Γενικότερα, ο συγκεκριμένος ορισμός είναι σημαντικό να περιέχει τη διανομή περιεχομένου διαμέσου διαδικτύου, Intranet, Extranet, δορυφορική εκπομπή, διακρατική τηλεόραση κλπ. Οι διαφοροποιημένες ορολογίες υποδηλώνουν τη σύλληψη μιας παρόμοιας εκπαιδευτικής εμπειρίας. Ακόμα, εκθέτουν την άποψη πως ο εκάστοτε εκπαιδευόμενος βρίσκεται σε απόσταση από τον εκάστοτε εκπαιδευτή, πως ο εκπαιδευόμενος κάνει χρήση ενός είδους τεχνολογίας (τις περισσότερες φορές έναν Η/Υ) με στόχο την πρόσβαση στο εκπαιδευτικό υλικό αλλά και πως ο εκπαιδευόμενος κάνει χρήση της τεχνολογίας με στόχο να καταφέρει να αλληλεπιδράσει με τον εκπαιδευτή και άλλους εκπαιδευόμενους, και πως προσφέρεται κάποιο είδος στήριξης στους εκπαιδευόμενους.(Καμπουράκης, Λουκής, 2015)

Εικόνα 1: Εισαγωγή Νέων Τεχνολογιών (Ορφανουδάκης, 2016)

Με τον ενεργό ρόλο εμπειρογνωμόνων από όλο τον κόσμο υλοποιήθηκε πριν μερικά χρόνια ένα ερευνητικό έργο, που στόχο είχε να οριοθετήσει έναν καθορισμένο ορισμό αυτής της έννοιας. Για το συγκεκριμένο σκοπό, υλοποιήθηκαν δυο βασικές ερευνητικές δράσεις. Αρχικά, υλοποιήθηκε μια εκτεταμένη βιβλιογραφική ανασκόπηση σε ότι είχε να κάνει με τον παραπάνω ορισμό, αντλώντας πληροφορίες από επιστημονικά περιοδικά, ειδικούς ιστότοπους και βιβλία. (Clark, Mayer, 2016)

Δεύτερον, μια μελέτη στάλθηκε με στόχο να συλλεχθούν οι απόψεις αναγνωρισμένων εμπειρογνωμόνων στον εκπαιδευτικό και στον τεχνολογικό κλάδο. Τα αποτελέσματα της συγκεκριμένης έρευνας επιβεβαιώνουν τη βασική υπόθεση της εν λόγω μελέτης σε ότι είχε να κάνει με τη δυσκολία ανάπτυξης ενός ενιαίου, δίχως αποκλεισμούς ορισμού της έννοιας αυτής που θα γίνει αποδεκτή από το μεγαλύτερο ποσοστό της σύγχρονης επιστημονικής κοινότητας.(E.R. Mayer, 2014)

Εικόνα 2: Εκπαιδευτικός Σχεδιασμός στην Εξ Αποστάσεως Εκπαίδευση (Ορφανουδάκης, 2016)

Το συμπέρασμα της παραπάνω έρευνας ήταν πως οι πιο καθοριστικοί λόγοι για την παραπάνω κατάσταση είναι πως τόσο ο όρος αυτός όσο και της κοινωνίας βρίσκονται σε ρευστή κατάσταση και η έννοια γίνεται κατανοητό από αρκετές και διαφορετικές οπτικές γωνίες και χρησιμεύει με διαφοροποιημένες σημασίες. Ο πιο κοινά αποδεκτός ορισμός που

χρησιμοποιείται μέχρι και σήμερα παρουσιάζεται παρακάτω.(Σοφός, Κώστα, Παράσχου, 2015)

Ο πιο κοινά αποδεκτός ορισμός είναι πως η ηλεκτρονική μάθηση αποτελεί μια σύγχρονη προσέγγιση στη διδασκαλία και στη μαθησιακή δράση, η οποία ως επί το πλείστον αντιπροσωπεύει το σύνολο είτε τμήμα του εκπαιδευτικού μοντέλου. Το μοντέλο αυτής της μορφής υλοποιείται και εστιάζει στη χρησιμοποίηση των ηλεκτρονικών μέσων και συσκευών σαν χρήσιμα εργαλεία, με στόχο τη βελτίωση της πρόσβασης στην εκπαιδευτική δράση, την επικοινωνία καθώς επίσης και την αλληλεπίδραση. Όλα τα παραπάνω παίζουν καθοριστικό ρόλο στην υιοθέτηση καινούριων τακτικών κατανόησης και ανάπτυξης της σύγχρονης μαθησιακής δράσης. (Τζιμογιάννης, 2017)

3.2 Πλεονεκτήματα και μειονεκτήματα ηλεκτρονικής μάθησης

Έρευνες έχουν δείξει πως η συγκεκριμένη μορφή μάθησης διαφοροποιείται σε μεγάλο βαθμό από τη βασισμένη σε σχολική αίθουσα εκπαιδευτική δράση από αρκετές και διαφορετικές απόψεις. Συνεπώς, η μετατροπή μιας παραδοσιακής σειράς μαθημάτων σε ηλεκτρονική μάθηση είναι δυνατόν να αφορά μια πολύπλοκη προσπάθεια, όπου χρειάζεται ακριβής σχεδιασμός, παρακολούθηση αλλά και έλεγχος με στόχο να καταστεί η συγκεκριμένη δράση αποδοτική και οικονομική.(E.R. Mayer, 2014)

Εικόνα 3: Πλεονεκτήματα Ηλεκτρονικής Μάθησης (Makri, Vlachopoulos, 2017)

Ανάμεσα στα αρκετά θετικά δεδομένα της ηλεκτρονικής μάθησης είναι εφικτό να απαριθμήσουμε τα παρακάτω. Γενικά αποτελεί μια οικονομική τακτική διάδοση γνώσης. Επίσης, είναι σημαντικό το γεγονός πως ο εκάστοτε εκπαιδευόμενος ακολουθεί τον δικό του ρυθμό τηλεκπαίδευσης και το γεγονός πως είναι γρηγορότερο (οι εκπαιδευόμενοι έχουν τη δυνατότητα να παραβλέψουν το υλικό το οποίο γνωρίζουν ήδη). (Σοφός, Κώστα, Παράσχου, 2015)

Ένα εξίσου σημαντικό πλεονέκτημα είναι το γεγονός πως η ύλη του μαθήματος έχει προκαθορισμένη συνοχή. Επίσης, η συγκεκριμένη μορφή μάθησης δρα ασύγχρονα και έχει την ευχέρεια να αναβαθμιστεί εύκολα και άμεσα εάν υπάρξουν σημαντικά ζητήματα ενώ ταυτόχρονα έχει την ευχέρεια να προσαρμοστεί εύκολα για μεγάλες ομάδες εκπαιδευόμενων. Εξίσου σημαντικά οφέλη είναι πως είναι στον τόπο και στον χρόνο που επιθυμούν οι εκπαιδευόμενοι.(Clark, Mayer, 2016)

Δυο ακόμα εξίσου σημαντικά οφέλη είναι η αμεσότερη εξέλιξη εκμάθησης και το γεγονός πως οι εκπαιδευόμενοι παρακολουθούν μια διαδικτυακή σειρά μαθημάτων και έχουν τη δυνατότητα να εισχωρήσουν σε ένα δίχως ρίσκο περιβάλλον προσομοίωσης όπου έχουν την ευχέρεια να κάνουν λάθη δίχως να εκθέτουν άμεσα τον εαυτό τους, και εν τέλει να λαμβάνουν την ανάδραση των επιπτώσεων των πρακτικών τους. (Καμπουράκης, Λουκής, 2015)

Από την άλλη πλευρά, τα κυριότερα ελαττώματα και οι κίνδυνοι της μάθησης αυτής της μορφής είναι εφικτό να συμπεριλάβουν τα παρακάτω. Αρχικά, είναι εφικτό να κοστίσει αρκετά για να αναπτυχθεί, χρειάζεται καινούριες ικανότητες των παραγωγών, χρειάζεται να είναι επικερδές βάσει με τον δείκτη ROI κλπ. Ακόμα, η αντίστοιχη τεχνολογία είναι εφικτό να αναπτύξει στον εκπαιδευόμενο το αίσθημα του φόβου, ενώ ταυτόχρονα είναι συγκεχυμένη αφού στερείται τμήμα της άτυπης κοινωνικής αλληλεπίδρασης της παραδοσιακής μεθόδου εκμάθησης.(Α. Τζιμογιάννης, 2017)

Σε συνδυασμό με όλα τα παραπάνω υφίσταται και ο κίνδυνος η τεχνολογία να είναι δαπανηρή, όχι απαραίτητα, ειδικά σε περίπτωση προηγμένου οπτικού περιεχομένου. Ακόμα, η τακτική αυτής της μορφής απαιτεί περισσότερη υπευθυνότητα αλλά και αυτοπειθαρχία για τον εκάστοτε φοιτητή με στόχο να κατορθώσει να συμβαδίσει με την πιο ελεύθερη και δίχως περιορισμούς δράση κατάρτισης.

Φυσικά, τα οφέλη και τα ελαττώματα τα οποία αναλύθηκαν παραπάνω δεν είναι απαραιτήτως αναπόφευκτα. Με προσεκτική ανάπτυξη και καλό προγραμματισμό, τα πιο πολλά από τα παραπάνω ελαττώματα είναι εφικτό να υπερνικηθούν, ενώ δίχως ακριβές και ενημερωμένο εκπαιδευτικό σχέδιο κανένα από τα παραπάνω οφέλη δεν είναι εφικτό να κατορθωθεί. (Σοφός, Κώστα, Παράσχου, 2015)

3.3 Moocs

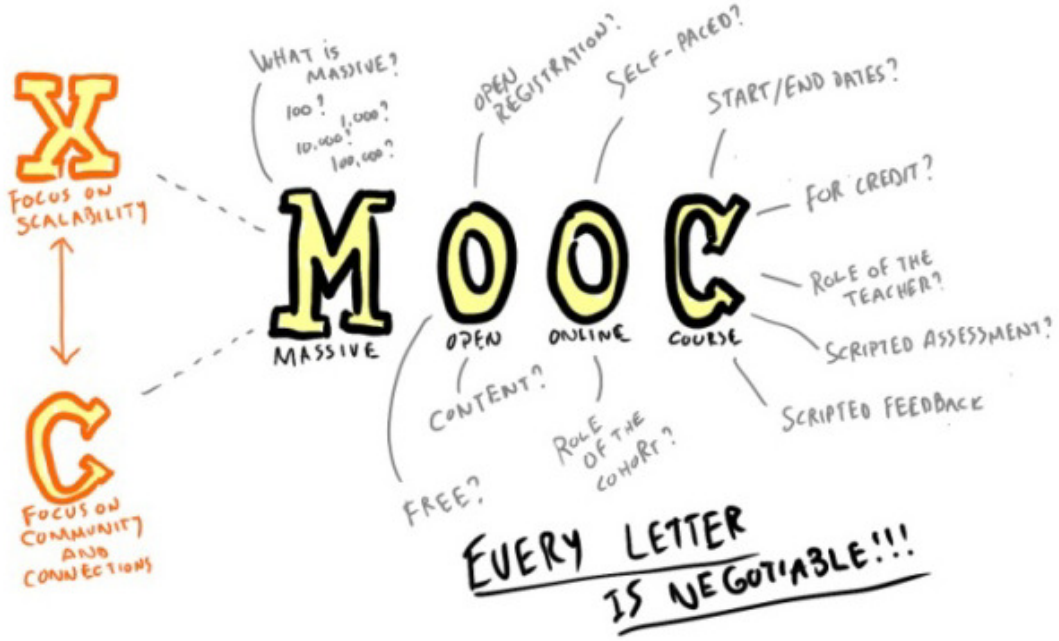
Η συγκεκριμένη έννοια παρά τη σύντομη ιστορία της βρέθηκε στο επίκεντρο του ενδιαφέροντος της διεθνούς εκπαιδευτικής κοινότητας, με κυριότερη συνέπεια να χαρακτηριστούν σαν ένα φαινόμενο, την περίοδο του 2012 και να αναγνωριστούν σαν μια σύγχρονη καινοτόμα δράση και τάση διαμέσου του κινήματος ανοιχτών εκπαιδευτικών πόρων. Η εν λόγω έννοια εισήχθη για $1^{η}$ φορά από τον Cormier την περίοδο του 2008.(Breslow, Pritchard, DeBoer, Stump, Ho, Seaton, 2013)

Μέχρι και σήμερα δεν υφίσταται σαφής ορισμός τους και τις πιο πολλές φορές η προσέγγιση γίνεται περιγραφικά. Σύμφωνα με έρευνες αφορά διαδικτυακές σειρές μαθημάτων που έχουν σχεδιαστεί και αναπτυχθεί για τεράστιο σύνολο συμμετεχόντων και είναι διαθέσιμες στον οποιονδήποτε αρκεί να έχει πρόσβαση στο διαδίκτυο. Γενικότερα, είναι ανοιχτά σε όλους δίχως καθορισμένα κριτήρια εγγραφής και προσφέρουν διαδικτυακά ολοκληρωμένη δωρεάν εκπαιδευτική εμπειρία. (Depover, Arsenti, Komis, 2016)

Στα κυριότερα γνωρίσματά τους περιέχονται η μαζικότητα, η ανοικτότητα, διαδικτυακή πρόσβαση καθώς επίσης και τα μαθήματα. Τα συγκεκριμένα γνωρίσματα θα αναλυθούν και σε επόμενη ενότητα, αλλά αυτό το οποίο είναι σημαντικό να γνωρίζουμε είναι πως οι 4 αυτές διαστάσεις περιλαμβάνουν τεράστιο επίπεδο ασάφειας και είναι εφικτό να προσεγγιστούν τόσο υπό τη στενή όσο και την ευρεία έννοιά τους, όπως μπορούμε να διακρίνουμε από την εικόνα 1.4 που ακολουθεί.(Marshall, 2013)

Στη βιβλιογραφία της χώρας μας αναφέρονται σαν Μαζικά Ανοικτά Διαδικτυακά Μαθήματα (Massive Open Online Courses) και αφορούν μαθήματα τα οποία προσβλέπουν στον ενεργό ρόλο των εκπαιδευόμενων χωρίς κανέναν περιορισμό και παρέχουν ανοικτή πρόσβαση διαμέσου της χρήσης του διαδικτύου. Εκτός από τα κλασσικά μέσα, όπως είναι για παράδειγμα η χρήση βίντεο, διαλέξεων, τεστ προόδου κλπ, τα μαθήματα αυτής της μορφής προσφέρουν στον εκάστοτε διαδικτυακό χειριστή την ευχέρεια συμμετοχής σε συζητήσεις, οι οποίες ευνοούν την ανοικοδόμηση μιας διαδραστικής κοινότητας για τους εκπαιδευόμενους,

τους εκπαιδευτικούς κλπ. Τα συγκεκριμένα μαθήματα αποτελούν μια πρόσφατη εξέλιξη στην εξ αποστάσεως εκπαίδευση.(Dalipi, Yayilgan, Imran, Kastrati, 2016)



Εικόνα 4 Moocs https://www.flickr.com/photos/mathplourde/8448541815

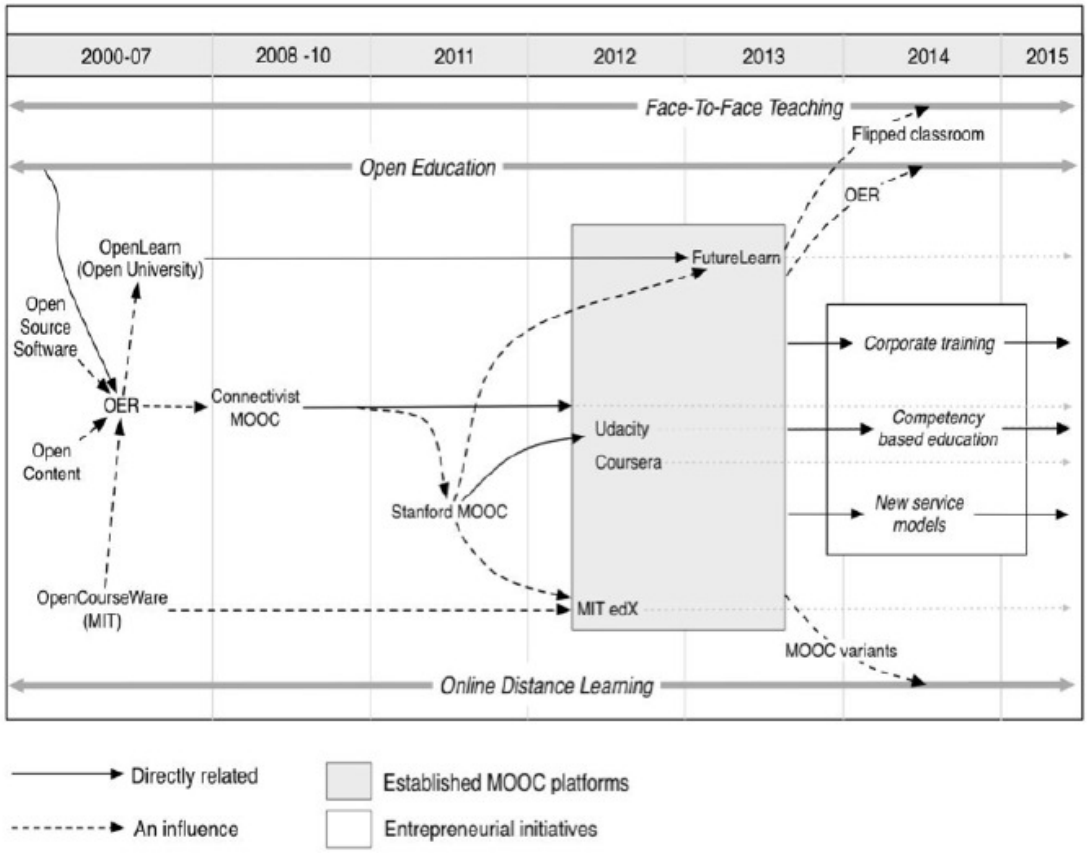
Παρά το γεγονός πως τα αρχικά μαθήματα αυτής της μορφής τις περισσότερες φορές επισήμαιναν τα γνωρίσματα της ανοικτής πρόσβασης όπως για παράδειγμα ο κοννεκτιβισμός και η ελεύθερη χρήση του περιεχομένου, της δομής και τω μαθησιακών σκοπών με στόχο την προώθηση της επαναχρησιμοποίησης τω διαφορετικών μέσων εκμάθησης και κατάρτισης, μερικά από τα πιο σύγχρονα μαθήματα αυτής της μορφής δρουν με κλειστές άδειες με στόχο τη χρησιμοποίηση των υλικών τα οποία χρησιμεύουν στη σειρά των μαθημάτων τους, ενώ ταυτόχρονα συντηρούν την ελεύθερη πρόσβαση των εκπαιδευόμενων στο περιεχόμενο των μαθημάτων.(Daniel, 2012)

Με τη συγκεκριμένη έννοια, τις περισσότερες φορές αναφερόμαστε στη μαθησιακή εμπειρία την οποία αποκομίζουν οι χειριστές του διαδικτύου κάνοντας χρήση αυτής της μορφής των μαθημάτων. Αρχικά, επομένως, ο χειριστής, αφού υλοποιήσει την εγγραφή του στο συγκεκριμένο σύστημα και συνδεθεί σε αυτό κάνοντας χρήση των κωδικών εισόδου και ασφαλείας, αποκτά πρόσβαση στον κατάλογο των παρεχόμενων μαθημάτων της εκάστοτε πλατφόρμας. (Kaplan, Haenlein, 2016)

Ο χειριστής είναι ελεύθερος να διαλέξει το μάθημα είτε τα μαθήματα τα οποία επιθυμεί και τον ενδιαφέρουν. Στη συνέχεια, ύστερα από τη δήλωση συμμετοχής του σε αυτό εντάσσεται στην ηλεκτρονική τάξη, κάτι το οποίο σημαίνει πως παρακολουθεί σύντομες βίντεο διαλέξεις, συμπληρώνει διαδραστικά τεστ και έχει ενεργό ρόλο σε ομάδες συζητήσεως με άλλους μαθητές είτε εκπαιδευτικούς. (Daniel, Cano, Cervera, 2015)

Τέλος, η παρακολούθηση του εκάστοτε μαθήματος λογίζεται σαν επιτυχημένη, μονάχα στην περίπτωση στην οποία ο χειριστής παραδώσει όλες τις εργασίες και λάβει τελική βαθμολογία. Παρά το γεγονός πως η συμμετοχή στο εκάστοτε μάθημα είναι δωρεάν, η παραλαβή ενός πιστοποιητικού επιμόρφωσης έχει σαν βασικότερο κριτήριο, σε πολλές περιπτώσεις, την καταβολή ενός χρηματικού ποσού. (Μπραΐλας, 2018)

Παρά το γεγονός αυτό, όμως, εξαιρετικά καθοριστικό είναι το γεγονός πως αρκετές πλατφόρμες αυτής της μορφής (όπως είναι για παράδειγμα η πλατφόρμα Coursera) αξιοποιώντας κατάλληλα τις αρχές της κυρίαρχης μάθησης δεν επιτρέπουν στον εκάστοτε χειριστή να προχωρήσει σε ένα θέμα δίχως να κατανοήσει πλήρως το προηγούμενο. Αυτός είναι και ο βασικότερος λόγος που παρέχεται υποστήριξη με τη μορφή τυχαίων εκδόσεων ενός διαγωνίσματος, προκειμένου να διαβάσει ξανά και να προσπαθήσει ξανά είτε της αξιολόγησης μιας εργασίας από ομότιμους.(Papamitsiou, Economides, 2014)



Εικόνα 5 Χρονοδιάγραμμα Ανάπτυξης Συστημάτων Ανοικτής Εκπαίδευσης και MOOCs (Yuan, Powell, 2015)

Γενικότερα, θα μπορούσε να ειπωθεί πως τα συγκεκριμένα μαθήματα αποτελούν ένα χρήσιμο μέσο το οποίο παίζει καθοριστικό ρόλο στη διευκόλυνση της ανάπτυξης, της διανομής και χρησιμοποίησης της γνώσης μέσα από συνεργατικές κοινότητες αλλά και σύγχρονα δίκτυα μάθησης. Έρευνες αναφέρουν πως η συγκεκριμένη ιδέα αναπτύχθηκε με ραγδαίους ρυθμούς, καθώς εστιάζει στον ενεργό ρόλο και στη συνεργασία η οποία εξελίσσεται ανάμεσα σε εκπαιδευόμενους και εκπαιδευτικούς και όχι τόσο στα παραδοσιακά μέσα διδασκαλίας μαθημάτων τα οποία χρησιμεύουν από άλλες πλατφόρμες (όπως για παράδειγμα μαγνητοσκοπημένες διαλέξεις κλπ) (Khalil, Ebner, 2016)

3.3.1 Κατηγορίες Moocs

Η κυριότερη προϋπόθεση διάκρισης των μαθημάτων αυτής της μορφής έχει άμεση σχέση με την παιδαγωγική προσέγγιση την οποία χρησιμοποιούν. Γενικότερα, όμως, ο διαχωρισμός των συγκεκριμένων μαθημάτων είναι εφικτό να υλοποιηθεί σύμφωνα με αρκετά και

διαφορετικά κριτήρια όπως είναι για παράδειγμα ο φορέας ο οποίος τα παρέχει (όπως για παράδειγμα πανεπιστήμια, επιχειρήσεις κλπ), το κόστος κλπ.(Daniel, Cano, Cervera, 2015)

Όπως ήδη αναφέρθηκε παραπάνω, η πιο διαδεδομένη διάκριση η οποία εντοπίζεται, γίνεται με βασική παράμετρο τη θεωρία μάθησης στην οποία βασίζονται και περιέχει 2 σημαντικά είδη που είναι τα Connectivist Moocs (είτε όπως καλούνται εν συντομία cMOOCs) και τα eXtention MOOCs (είτε όπως καλούνται και αυτά εν συντομία xMOOCs).(Breslow, Pritchard, DeBoer, Stump, Ho, Seaton, 2013)

Πίνακας 1: Κατηγορίες MOOCs (Marshall, 2013

xMOOCs	**Ιδιότητες**	**cMOOCs**
Επεκτασιμότητα	Μαζικά	Κοινότητα και ανάπτυξη δικτύων
Ανοιχτή πρόσβαση και περιορισμένες άδειες χρήσης υλικών	Ανοικτά	Ανοικτή πρόσβαση και ανοιχτές άδειες χρήσης υλικών
Ατομική εκμάθηση σε μια μόνο πλατφόρμα	Online	Εκμάθηση διαμέσου δικτύων μέσω διαφορετικών πλατφόρμων και υπηρεσιών
Απόκτηση γνώσεων και ικανοτήτων μέσα από ένα πρόγραμμα φοίτησης	Μάθημα	Ανάπτυξη κοινών πρακτικών, γνώσης και κατανόησης

Τα πρώτα εξ αυτών αναγνωρίζονται σαν η $1^{η}$ γενιά των μαθημάτων αυτής της μορφής και θέτοντας στο επίκεντρο της μάθησης τον εκάστοτε μαθητή, βασίζονται στη θεωρία μάθησης η οποία αναφέρεται σαν κονεκτιβισμός. Βάσει με την παραπάνω θεωρία, η ανάπτυξη γνώσης και η μάθηση τις περισσότερες φορές κατορθώνεται διαμέσου συνεργατικής αλληλεπίδρασης και ενεργούς παρέμβασης στο περιεχόμενο της διδασκαλίας, αναπτύσσοντας με αυτόν τον τρόπο μη τυποποιημένα δίκτυα υποστήριξης της μαθησιακής δράσης. (Dalipi, Yayilgan, Imran, Kastrati, 2016)

Τα συγκεκριμένα μαθήματα έχουν σαν βασικότερο σκοπό την προαγωγή της συνεργασίας ανάμεσα στους μαθητές και τη βελτίωση του ίδιου του μαθήματος. Ο μαθητής στον οποία αποδίδεται ενεργός ρόλος έχει την ευχέρεια να οριοθετεί ο ίδιος στόχους και να οργανώνει

μόνος του σύμφωνα με τις προσωπικές του απαιτήσεις και επιθυμίες τη μέθοδο μάθησης.(Depover, Arsenti, Komis, 2016)

Πίνακας 2: Βασικά Γνωρίσματα Κατηγοριών MOOCs (Dalipi, Yayilgan, Imran, Kastrati, 2016)

Βασικά χαρακτηριστικά	**xMOOCs**	**CMOOCs**
Θεωρίες μάθησης	Γνωστικός συμπεριφορισμός	Κονεκτιβισμός
Διδακτικές προσεγγίσεις	Προσανατολισμός προς το γνωστικό αντικείμενο	Προσανατολισμός προς τη μαθησιακή δράση
Προσέγγισης μάθησης	Μεταφορά δεδομένων	Ανταλλαγή γνώσεων ανάμεσα στους σπουδαστές
Αλληλεπίδραση	Περιορισμένη αλληλεπίδραση	Εκπαιδευόμενου-εκπαιδευόμενου, εκπαιδευόμενου-περιεχόμενο, εκπαιδευόμενου-εκπαιδευτικού
Ρόλος του σπουδαστή	Αποδέκτης	Δημιουργός
Ρόλος εκπαιδευτικού	Είναι αρμόδιος για την ανάπτυξη περιεχομένου και δράσεων μέσω συντονισμού και επίβλεψης	Συμμαθητής (αναπτύσσει περιεχόμενο και βάζει στόχους σε συνεργασία με τους άλλους εκπαιδευόμενους
Περιεχόμενο	Επικεντρώνετε στην γνώση	Επικεντρώνετε στη δράση
Αξιολόγηση	Τεστ πολλαπλών επιλογών, κουίζ, αυτοματοποιημένη αξιολόγηση από ομότιμους	Δεν υφίσταται επίσημη αξιολόγηση (ανατροφοδότηση από όσους συμμετέχουν)
Εκπαιδευτικό υλικό	Βίντεο διαλέξεις, αναγνώσεις κειμένων, διαφάνειες, αρχεία	Social media, συστήματα διαχείρισης μάθησης (πχ

	ήχου κλπ	Moodle), βίντεο και δράσεις τις οποίες αναπτύσσουν οι σπουδαστές

Με τον τρόπο αυτόν κατορθώνεται η συνεργατική μάθηση, η παραγωγή καθώς επίσης και η διάχυση της γνώσης, υποστηριζόμενες από την τεχνολογία και τα σύγχρονα κοινωνικά δίκτυα, τα οποία προσφέρουν την ευχέρεια ανάπτυξης διαδικτυακών κοινοτήτων με στόχο την επίλυση καθοριστικών ζητημάτων αλλά και τον εντοπισμό κατάλληλων απαντήσεων. Με τη χρησιμοποίηση διαφοροποιημένων μέσων και χρήσιμων εργαλείων αυτής της μορφής (όπως είναι για παράδειγμα το Facebook, τα ιστολόγια κλπ), οι εκπαιδευόμενοι που έχουν ενεργό ρόλο δρουν σαν εκπαιδευόμενοι και εκπαιδευτές παράλληλα, καθώς καταρτίζονται αλλά και διδάσκουν. (Daniel, 2012)

Από την άλλη πλευρά, σε ότι έχει να κάνει με την 2^{η} κατηγορία που αναφέρθηκε παραπάνω, είναι σημαντικό να τονιστεί πως αποτελούν την 2^{η} γενιά και είναι η πιο διαδεδομένη κατηγορία της σύγχρονης εποχής, καθώς εστιάζει σε διαφοροποιημένες θεωρίες μάθησης. Η κατηγορία αυτή έχει στο επίκεντρό της το αντικείμενο και το περιεχόμενο της διδασκαλίας. (Kaplan, Haenlein, 2016),

Οι διδακτικοί στόχοι είναι οριοθετημένοι από τον εκάστοτε εκπαιδευτικό, ενώ ο ρόλος ο οποίος αποδίδεται στον εκάστοτε μαθητή είναι περισσότερο παθητικός. Τα μαθήματα αυτής της μορφής έχουν σαν κυριότερο στόχο τη διάχυση της γνώσης με μαζικά γνωρίσματα και δομημένες τακτικές. Έκαναν για πρώτη φορά την εμφάνισή τους την περίοδο του 2011. Στόχος τους από την αρχή ήταν η παροχή εκπαιδευτικών υπηρεσιών αντιγράφοντας την παραδοσιακή μέθοδο διδασκαλίας και περιείχαν δράσεις όπως η αξιολόγηση για την εκτίμηση του παραγόμενου αποτελέσματος. (Μπραϊλας,2018)

Γενικότερα, προσφέρουν δομημένα δεδομένα και στοιχεία όπως αυτό είναι δυνατόν να κατορθωθεί με την προβολή σειράς βίντεο με τη μορφή μαγνητοσκοπημένων διαλέξεων και τις περισσότερες φορές είναι εφικτό να συνδυαστούν με διαγωνίσματα, κουίζ κλπ, η υλοποίηση των οποίων αποτελεί μορφή αυτό-αξιολόγησης. Το επίπεδο αλληλεπίδρασης το οποίο προσφέρουν είναι πολύ μικρό εξαιτίας του τεράστιου συνόλου όσων συμμετέχουν ενώ η επικοινωνία τις περισσότερες φορές είναι εξαιρετικά περιορισμένη καθώς αφορά μονάχα

εκείνη η οποία προσφέρεται από το σύστημα διαχείρισης μάθησης το οποίο χρησιμοποιείται. (Papamitsiou, Economides, 2014)

Πίνακας 3 : Αλλαγές που επήλθαν με τα MOOCs (Σαλματζίδης, 2016)

ΠΡΙΝ	**ΜΕΤΑ**
Εκπαίδευση σαν κοινωνικό αγαθό	Εμπορευματοποίηση της εκπαίδευσης (σύμφωνα με το μοντέλο το οποίο ακολουθείται)
Πανεπιστήμιο σαν βασικός μέτοχος της παροχής εκπαίδευσης	Καινούριοι μέτοχοι (πάροχοι τεχνολογικής πλατφόρμας, εξεταστικά κέντρα πιστοποίησης κλπ)
Πτυχίο	Πιστοποίηση
Συνολική γνώση επιστημονικών πεδίων	Μεμονωμένη συγκέντρωση επαγγελματικών ικανοτήτων
Συμβατική αξιολόγηση εργασιών	Αυτοματοποιημένες εξετάσεις
Αριθμός μελών ΔΕΠ προσαρμοσμένος στο σύνολο των εκπαιδευόμενων και τις αίθουσες	Ελάττωση του διδακτικού ανθρώπινου δυναμικού υψηλών βαθμίδων και ανοδική τάση του βοηθητικού προσωπικού για τις διεκπεραιωτικές δράσεις
Αίθουσες διδασκαλίας	Ευζωνικό δίκτυο και υπηρεσίες cloud
Συμβατική αξιολόγηση εργασιών	Αυτοματοποιημένες εξετάσεις
Αριθμός μελών ΔΕΠ προσαρμοσμένος στο σύνολο των εκπαιδευόμενων και τις αίθουσες	Ελάττωση του διδακτικού ανθρώπινου δυναμικού υψηλών βαθμίδων και ανοδική τάση του βοηθητικού προσωπικού για τις διεκπεραιωτικές δράσεις
Αίθουσες διδασκαλίας	Ευζωνικό δίκτυο και υπηρεσίες cloud

3.3.2 Χαρακτηριστικά Moocs

Τα συγκεκριμένα μαθήματα έχουν βασικά γνωρίσματα τα οποία είναι τόσο θετικά όσο και αρνητικά. Τα θετικά έχουν προέλευση από την υπόσχεση παροχής δωρεάν, υψηλού επιπέδου και σε τεράστια κλίμακα πανεπιστημιακών μαθημάτων. Το συγκεκριμένο γεγονός ως επί το πλείστον προέρχεται από τις πρόσφατες τεχνολογικές αλλαγές, αλλά και από την απορρέουσα αίσθηση πως η τεχνολογία έχει την ευχέρεια να παρέχει εν τέλει καθορισμένες δυνατότητες σε όλες τις βαθμίδες και κυρίως στην τριτοβάθμια εκπαίδευση.(Yuan, Powell, 2015)

Ακόμα, τα μαθήματα αυτής της μορφής αναδύουν ένα αίσθημα δημοκρατικής και ελεύθερης προσβασιμότητας στη σύγχρονη εκπαιδευτική δράση αλλά και τη νοοτροπία πως οι ικανότητες για κατάρτιση είναι σημαντικό να μην περιορίζονται μονάχα σε λίγους προνομιούχους. Τα μαθήματα αυτά παρέχουν γνώση δίχως περιορισμούς. (Makri, Vlachopoulos, 2017)

Κυριότερη επίπτωση όλων των παραπάνω είναι πως οι εκπαιδευόμενοι από όλα σχεδόν τα μέρη του πλανήτη έχουν την ευχέρεια να κάνουν χρήση εξίσου αυτών των μαθησιακών ευκαιριών, υπερνικώντας την ποικιλομορφία των γλωσσών, τα διαφοροποιημένα εκπαιδευτικά υπόβαθρα, τις κοινωνικές αλλά και πολιτιστικές διαφοροποιήσεις και τις ανισότητες, οι οποίες υφίστανται στον διεθνή πληθυσμό. Στη σημερινή εποχή, οι εκπαιδευτές επισημαίνουν πως πλέον υφίσταται η δυνατότητα εκπαίδευσης όχι μονάχα σε 40 εκπαιδευόμενους αλλά και σε 40 χιλιάδες ταυτόχρονα εξαιτίας της ραγδαίας τεχνολογικής ανάπτυξης.(Τζιμογιάννης, 2017)

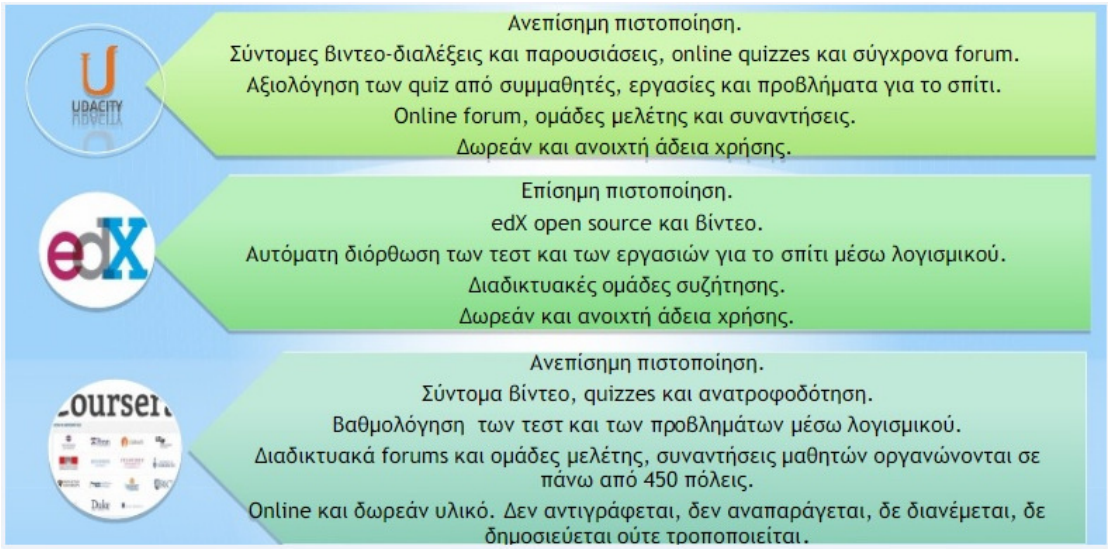
Τα κυριότερα γνωρίσματα αυτών των μαθημάτων είναι η **μαζικότητα** (δηλαδή αφορά μαζικά επεκτάσιμα μαθήματα, τα οποία αναπτύσσονται για πάρα πολλούς χρήστες και είναι εφικτό να έχουν ενεργό ρόλο πολλές χιλιάδες εκπαιδευόμενοι), η **προσβασιμότητα** (απαιτείται ένας Η/Υ, με πρόσβαση στο διαδίκτυο και στον παγκόσμιο ιστό αλλά και ένας ελάχιστος ψηφιακός αλφαβητισμός) και η **ευελιξία** (η δράση της διδασκαλίας προσαρμόζεται στο χρονοδιάγραμμα των εκπαιδευόμενων, δεν υφίστανται επίσημες απαιτήσεις εγγραφής και ως επί το πλείστον οι φοιτητές έχουν την ευχέρεια να σταματήσουν την εγγραφή για οποιαδήποτε λόγο δίχως καμία συνέπεια). (Daniel, Cano, Cervera, 2015)

Εξίσου σημαντικό γνώρισμα είναι η **διαφορετική βαθμολογία** (γίνεται χρήση αυτοματοποιημένων συστημάτων βαθμολόγησης), η **μηδαμινή χρησιμοποίηση βιβλίων**, η

αλληλεπίδραση ανάμεσα στους εκπαιδευόμενους (δεδομένου πως ενθαρρύνεται ο ενεργός ρόλος σε κοινότητες συνομιλίας και επικοινωνίας με το σχηματισμό τοπικών ομάδων διερεύνησης) καθώς επίσης και διάφορα **ηθικά θέματα** (σε ό,τι έχει να κάνει με αυτό το κομμάτι, τα πιο πολλά μαθήματα αυτής της μορφής δεν απαιτούν πιστοποίηση ταυτότητας και φυσικά αφορούν άτομα με διαφορετικό ήθος).(Depover, Arsenti, Komis, 2016).

3.3.3 Δομή και παροχή online μαθημάτων

Η πιο συχνή διάρκεια μιας σειράς μαθημάτων αυτής της μορφής κυμαίνεται από 6 έως και 12 εβδομάδες ενώ το εκάστοτε μάθημα είναι προσβάσιμο όλο το 24ωρο για 7 ημέρες την βδομάδα. Το πιο μεγάλο τμήμα του περιεχομένου προσφέρεται με ασύγχρονες τακτικές, δηλαδή οι εκπαιδευόμενοι έχουν την ευχέρεια να έχουν πρόσβαση στον προσωπικό τους χρόνο και με το δικό τους ρυθμό. Παρά το γεγονός αυτό, όμως, κάποιες φορές είναι εφικτό να υφίστανται προαιρετικές διαλέξεις σε ζωντανή μετάδοση (όπως για παράδειγμα συμβαίνει με διαδικτυακά σεμινάρια τα οποία απαιτούν από όλους όσους έχουν ενεργό ρόλο να τις παρακολουθούν εντός μιας καθορισμένης ημερομηνίας αλλά και ώρας).(Dalipi, Yayilgan, Imran, Kastrati, 2016)



Εικόνα 6: Κυριότερες Πλατφόρμες MOOCs https://www.academia.edu/34449165/MOOC_-_%CE%9C%CE%B9%CE%B1_%CF%83%CF%8D%CE%BD%CF%84%CE%BF%CE%BC%CE%B7_%CE%B5%CF%80%CE%B9%CF%83%CE%BA%CF%8C%CF%80%CE%B7%CF%83%CE%B7

Μια τυπική ακολουθία μαθημάτων μετατρέπεται σε MOOC με την υποστήριξη μιας σειράς βίντεο με μικρή διάρκεια (5-10 λεπτά) ενώ η κατανόηση του περιεχομένου των συγκεκριμένων μαθημάτων από τους εκπαιδευόμενους αξιολογείται κατά κύριο λόγο μέσω τεστ ερωτήσεων πολλαπλής επιλογής. Ένα καθοριστικό γνώρισμα των εν λόγω μαθημάτων είναι και οι εργασίες. Οι εκπαιδευόμενοι χρειάζεται να αναρτούν τις εργασίες τους στην διαδικτυακή πλατφόρμα και αυτές αξιολογούνται και βαθμολογούνται αυτόματα (όταν είναι εφικτό) είτε διαμέσου της υποστήριξης άλλων εκπαιδευόμενων (όπου ο εκάστοτε εκπαιδευόμενος αξιολογεί τους άλλους βαθμολογώντας τις εργασίας τους σύμφωνα με ένα καθορισμένο υπόδειγμα αξιολόγησης). (Yuan, Powell,2015)

Ένα ακόμα εξίσου σημαντικό δεδομένο των μαθημάτων αυτής της μορφής είναι οι διαδικτυακοί τόποι δημόσιων συζητήσεων, στους οποίους υφίσταται η δυνατότητα ανάρτησης ερωτημάτων από τους εκπαιδευόμενους και απάντησης από άλλους σπουδαστές. Τις περισσότερες φορές, δεν υφίσταται κατάλληλα κριτήρια για τον ενεργό ρόλο σε τέτοια μαθήματα, εκτός από το να έχει κάποιος πρόσβαση στο διαδίκτυο. (Breslow, Pritchard, DeBoer, Stump, Ho, Seaton, 2013)

Πρωτοβουλίες	Κερδοσκοπικές	Ελεύθερη πρόσβαση	Τέλος πιστοποίησης	Παροχή εκπαιδευτικών πιστωτικών μονάδων
eDX	X	✓	✓	X
Coursera	✓	✓	✓	X ✓
Udacity	✓	✓	✓	X ✓
Udemy	✓	X ✓	✓	X ✓
P2PU	✓	✓	✓	X

✓: Διαθέσιμο χαρακτηριστικό, X: Δεν αποτελεί χαρακτηριστικό, X, ✓: Χαρακτηριστικό εν μέρει διαθέσιμο

Εικόνα:7 Σύγκριση Πλατφόρμων Παροχής MOOCs (Καλογιαννάκης, Παπαδάκης, 2014)

Τις πιο πολλές φορές, επίσης, το εκπαιδευτικό υπόβαθρο των εκπαιδευόμενων δεν παίζει κανέναν απολύτως ρόλο. Οι εκπαιδευόμενοι τις περισσότερες φορές δεν απαιτείται καν να αγοράσουν βιβλία για τα εν λόγω μαθήματα, λόγω του ότι το υλικό ανάγνωσης περιέχεται στο περιεχόμενο των συγκεκριμένων μαθημάτων είτε υφίσταται η ευχέρεια διασύνδεσης με κείμενα ανοιχτής πρόσβασης. (Marshall, 2013)

Οι κυριότεροι πάροχοι αυτών των μαθημάτων είναι το edx, το courser καθώς επίσης και το udacity. Εκτός από αυτούς, όμως, υφίστανται και άλλοι πάροχοι αυτής της μορφής όπως είναι για παράδειγμα το FutureLearn και το Udemy. Το πρώτο εξ αυτών που θα αναλυθεί διεξοδικά και σε επόμενο κεφάλαιο αποτελεί μια μεγάλη ανοιχτή διαδικτυακή πλατφόρμα

μαθημάτων, η οποία αναπτύχθηκε την περίοδο του 2012 με στόχο να φιλοξενήσει διαδικτυακά μαθήματα πανεπιστημιακού επιπέδου σε ένα μεγάλο σύνολο διαφοροποιημένων επιστημονικών τομέων που αφορούσαν ένα παγκόσμιο κοινό δίχως κόστος. (Depover, Arsenti,Komis, 2016)

Από την άλλη πλευρά το Coursera αποτελεί μια κερδοσκοπική εκπαιδευτική τεχνολογική επιχείρηση, η οποία προσφέρει μαθήματα αυτής της μορφής και αναπτύχθηκε από το Πανεπιστήμιο του Στάνφορντ. Συνεργάζεται με αρκετούς εκπαιδευτικούς οργανισμούς τριτοβάθμιας εκπαίδευσης, με κυριότερο στόχο να παρέχει διαδικτυακά κάποια από τα μαθήματά τους, όπως είναι για παράδειγμα η φυσική, η μηχανική, η ιατρική κλπ. Την περίοδο του 2013 αναπτύχθηκε και η εφαρμογή του για κινητά τηλέφωνα. (Mayer, 2014)

Από την άλλη πλευρά, το Udacity αποτελεί έναν κερδοσκοπικό εκπαιδευτικό οργανισμός, ο οποίος αναπτύχθηκε με στόχο την παροχή μαθημάτων αυτής της μορφής. Βάσει μελετών, η προέλευση του συγκεκριμένου ονόματος έχει προέλευση από τη θέληση της επιχείρησης να είναι τολμηρή για τους εκπαιδευόμενους. Το Udemy, από την άλλη μεριά, αναπτύχθηκε από τους Bali και Caglar, αναπτύσσοντας μια πλατφόρμα η οποία καλούσε ανθρώπους (και όχι οργανισμούς) με στόχο να παρέχουν διαδικτυακά μαθήματα. (Khalil, Ebner, 2016)

Τέλος, το FutureLearn αποτελεί μια μεγάλη πλατφόρμα αυτής της μορφής, η οποία αναπτύχθηκε την περίοδο του 2012. Σαν επιχείρηση εντάσσεται στο Ανοικτό Πανεπιστήμιο του Ηνωμένου Βασιλείου. Αποτελεί την 1^{η} πλατφόρμα αυτής της μορφής του Ηνωμένου Βασιλείου και από τα τέλη του 2013 συμμετέχουν 26 πανεπιστήμια. Σε αντίθεση με άλλες πλατφόρμες αυτής της μορφής περιέχει 3 εταίρους εκτός πανεπιστημίου που είναι το Βρετανικό Μουσείο, το Βρετανικό Συμβούλιο καθώς επίσης και η Βρετανική Βιβλιοθήκη. (Yuan, Powell, 2015)

Πίνακας 4: Πλεονεκτήματα και μειονεκτήματα βασικότερων παρόχων (Kaplan, Haenlein, 2016)

COURSERA	**UDACITY**	**EdX**
Πλεονεκτήματα	**Πλεονεκτήματα**	**Πλεονεκτήματα**
Τεράστια γκάμα από μαθήματα τα οποία καλύπτουν αρκετούς και διαφορετικούς θεματικούς	Σύνδεση μέσω social media (όπως το Facebook και το Twitter)	Καλή ποικιλία από μαθήματα τα οποία καλύπτουν διαφοροποιημένες θεματικές περιοχές

κλάδους		
Σχεδόν όλα τα μαθήματα παρέχουν πιστοποίηση	Εξαιρετικά διαδραστικά μαθήματα φροντιστηριακής μορφής	Πιστοποιητικά παρακολούθησης προσφέρονται για όλα τα μαθήματα
Μειονεκτήματα	**Μειονεκτήματα**	**Μειονεκτήματα**
Δεν είναι διαθέσιμα για άμεση εγγραφή όλα τα μαθήματα τα οποία διαφημίζονται	Περιορισμένο φάσμα μαθημάτων	Δεν είναι όλα τα μαθήματα τα οποία διαφημίζονται διαθέσιμα για άμεση εγγραφή
Με στόχο την επίτευξη της πιστοποίησης είναι σημαντικό να πληρούνται όλες οι προθεσμίες των μαθημάτων	Δεν παρέχονται σήμερα όλες οι μορφές μετάφρασης σε ξένες γλώσσες	Οι εκτιμώμενες εβδομαδιαίες ώρες και προθεσμίες είναι εφικτό να είναι δύσκολο για κάποια άτομα να τις τηρήσουν

3.3.4 Σύγκριση moodle και edx

Το Moodle και το edX είναι ηλεκτρονικές πλατφόρμες μάθησης ανοιχτού κώδικα σχεδιασμένες για διαφορετικές παιδαγωγικές εφαρμογές και στοχεύουν σε διαφορετικό κοινό και διαφορετικές περιπτώσεις εκμάθησης. Το γεγονός πως πρόκειται για πλατφόρμες ανοιχτού κώδικα σημαίνει πως με τη συμβολή της εκάστοτε κοινότητας συνεχώς αλλάζουν με στόχο τη βελτίωσή τους ανάλογα με τις απαιτήσεις των χρηστών.

Οι διαφορές τους είναι ορατές ακόμα και μέσω της επίσημης περιγραφής κάθε πλατφόρμας. Το open edX περιγράφει τον εαυτό του ως "ένα σύστημα διαχείρισης μαθημάτων ελεύθερου και ανοιχτού κώδικα (CMS) που χρησιμοποιείται σε όλο τον κόσμο για να φιλοξενήσει Μαθήματα Ανοικτού Διαδικτύου Μαζικής Επικοινωνίας (MOOC), καθώς και μικρότερες κατηγορίες και εκπαιδευτικές ενότητες". Ενώ το Moodle περιγράφει τον εαυτό του ως μια πλατφόρμα "καθοδηγούμενη από την κοινωνική κατασκευαστική παιδαγωγική" που "παρέχει ένα ισχυρό σύνολο εργαλείων βασιζόμενα σε μαθητές και περιβάλλοντα συνεργατικής μάθησης που ενδυναμώνουν τόσο τη διδασκαλία όσο και τη μάθηση".

Τόσο το Moodle όσο και το Open edX υπάρχουν χρόνια στο χώρο της μάθησης. Το Moodle πρωτοεμφανίστηκε στην ηλεκτρονική σκηνή μάθησης πριν από 15 χρόνια, ενώ το Open edX ξεκίνησε πιο πρόσφατα το 2013.

3.3.4.1 Κοινό που στοχεύουν

Το Moodle και το Open edX σχεδιάστηκαν αρχικά με τους εκπαιδευτικούς στο μυαλό τους. Ωστόσο, με την πάροδο των ετών, κάθε πλατφόρμα έχει αποκλίνει για να εξυπηρετήσει διαφορετικά ακροατήρια.

Το Moodle φτιάχτηκε σύμφωνα με το παραδοσιακό μοντέλο της αίθουσας διδασκαλίας, όπου τα μεγέθη των τάξεων στο διαδίκτυο κυμαίνονταν συνήθως μεταξύ των 5-30 σπουδαστών. Με ένα ευρύ φάσμα πελατών που επικεντρώνονται κυρίως στην τριτοβάθμια εκπαίδευση, συμπεριλαμβανομένου του κρατικού πανεπιστημίου της Νέας Υόρκης και της Σχολής Οικονομικών του Λονδίνου, το Moodle εξακολουθεί να έχει ισχυρή παρουσία στον κόσμο της ακαδημαϊκής κοινότητας.

3.3.4.2 Χρηστικότητα

Η εγκατάσταση του Open edX σε μορφή MOOC επιτρέπει επίσης περισσότερη διαδραστική συμμετοχή από μια απλή τάξη στο διαδίκτυο. Το Open edX σας επιτρέπει να προσθέτετε αλληλεπιδραστικά στοιχεία στα μαθήματά σας μέσω plugins XBlock, τα οποία παρέχουν σχεδόν άπειρη ευελιξία στο Open edX. Στην πραγματικότητα, τα XBlocks είναι ένας μεγάλος λόγος για την απήχηση του Open eXX σε συγγραφείς, διαχειριστές και εκπαιδευτές που είναι μέλη διάφορων οργανισμών κάθε μορφής και μεγέθους.

Παρόλο που και το Moodle και το Open edX επιτρέπουν τη προσθήκη λειτουργιών όπως βίντεο, κουίζ και εξετάσεις, το Moodle διαθέτει μια μεγαλύτερη βιβλιοθήκη plug-in διαθέσιμη για τους χρήστες. Αλλά όπου το Moodle κερδίζει σε ποσότητα, το Open edX κερδίζει σε ποιότητα, με τα XBlocks να ενσωματώνονται άψογα στην εμπειρία δημιουργίας και με το να είναι πολύ πιο εύκολο στο σχεδιασμό.

Η Κοινότητα αποτελεί ένα σημαντικό μέρος της επιλογής μιας πλατφόρμας και τόσο το Open edX όσο και το Moodle έχουν διαφορετικές αλλά δραστήριες κοινότητες που καθοδηγούν την κατεύθυνση που αναπτύσσετε η πλατφόρμα. Η κοινότητα Moodle εξελίχθηκε από την βάση της εκπαίδευσης K-12, ενώ η κοινότητα Open eXX προέκυψε από

την τριτοβάθμια εκπαίδευση, με την ιδέα να μοιράζονται πιο σύνθετες και προηγμένες πληροφορίες μέσω των MOOC.

Το Moodle είναι μια σταθερή πλατφόρμα, αλλά ορισμένοι χρήστες βρίσκουν τις λειτουργίες της λίγο αφύσικες και η εμφάνιση του site μπορεί να δίνει την αίσθηση λίγο παρωχημένης. Επιπλέον, η Moodle επέλεξε να μην δώσει προτεραιότητα στο να είναι φιλική προς τα κινητά ή τα API, γεγονός που καθιστά τα πράγματα δύσκολα για ορισμένους χρήστες. Το open edX έχει καλύτερη χρηστικότητα και χρησιμοποιεί API που κάνουν ακόμα πιο εύκολη τη χρήση. Επιπλέον, υπηρεσίες όπως το Tahoe του Appsembler υπάρχουν στο Open edX για να βοηθήσουν στην επίβλεψη των τεχνικών πτυχών και να επιτρέψουν ακόμα ευκολότερη χρήση της πλατφόρμας.

Μερικές φορές οι διαφορές μεταξύ δύο προϊόντων καθίστανται σαφείς ακόμα και από το ποιος χρησιμοποιεί τα προϊόντα. Τα κορυφαία ιδρύματα όπως το MIT, το Χάρβαρντ και το Stanford, καθώς και μεγάλες καινοτόμες εταιρείες όπως το Google, οι υπηρεσίες Amazon Web Services και η IBM χρησιμοποιούν το Open EdX. Οι χρήστες του Moodle περιλαμβάνουν το κρατικό πανεπιστήμιο της Νέας Υόρκης, το London School of Economics και εταιρείες όπως η Shell.

3.3.4.3 Συμπέρασμα

Τόσο το Moodle όσο και το Open edX είναι εξαιρετικές πλατφόρμες και το καθένα έχει τα δικά του πλεονεκτήματα. Τελικά, η επιλογή της σωστής πλατφόρμας έρχεται στην ακόλουθη ερώτηση: είστε ένας σύγχρονος χρήστης με ένα ευρύ φάσμα περιπτώσεων χρήσης που ξεπερνούν την παραδοσιακή μάθηση στην τάξη ή είστε εκπαιδευτικός που αναζητά μια παραδοσιακή εμπειρία της τάξης στο διαδίκτυο; Το Moodle είναι η σωστή επιλογή για ανθρώπους που δεν ενδιαφέρονται για το πώς φαίνεται η πλατφόρμα, αλλά ενδιαφέρονται πολύ για το ακροατήριο K-12 και αισθάνονται πιο διατεθειμένοι να δημιουργήσουν παραδοσιακές εμπειρίες.

Ωστόσο, αν ψάχνετε για κάτι που έχει μια πιο ενημερωμένη αίσθηση, που είναι προσανατολισμένη σε μια τεράστια βάση χρηστών και κάτι που έχει πολλή ευελιξία, τότε το Open edX είναι η σωστή επιλογή για εσάς.

Από την άλλη, το Open edX σχεδιάστηκε για τον κόσμο του MOOC της διαδικτυακής και αυτό-ρυθμιζόμενης μάθησης. Το open edX απευθύνεται σε μεγάλης κλίμακας ακροατήρια,

όπου η πλατφόρμα μπορεί εύκολα να κλιμακωθεί από λίγους μαθητές σε εκατομμύρια μαθητευόμενους. Εξαιτίας αυτού, η πλατφόρμα επέδρασε πέρα από τα παραδοσιακά ακροατήρια στην τριτοβάθμια εκπαίδευση και εξαπλώθηκε σε εταιρείες, κυβερνητικούς οργανισμούς, μη κερδοσκοπικούς οργανισμούς και μικρές επιχειρήσεις. Χαρακτηριστικά παραδείγματα πελατών αποτελούν οι εταιρίες Starbucks, MongoDB, RedisLabs καθώς και πολλές άλλες.

4 ΑΝΑΠΤΥΞΗ ΔΙΑΔΙΚΤΥΑΚΟΥ ΣΕΜΙΝΑΡΙΟΥ ΣΤΗΝ ΠΛΑΤΦΟΡΜΑ MOODLE

4.1 Γενικά στοιχεία Moodle

Το Moodle είναι μια πλατφόρμα μάθησης που έχει σχεδιαστεί για να παρέχει στους εκπαιδευτικούς, τους διαχειριστές και τους εκπαιδευόμενους ένα ενιαίο δυνατό, ασφαλές και ολοκληρωμένο σύστημα για τη δημιουργία εξατομικευμένων μαθησιακών περιβαλλόντων. Πρόκειται για λογισμικό το οποίο είτε μπορείτε να κατεβάσετε στον δικό σας διακομιστεί ιστού ή να ζητήσετε βοήθεια από κάποιον από τους γνωστούς συνεργάτες της Moodle.

Το Moodle κατασκευάζεται από το έργο Moodle, το οποίο διευθύνεται και συντονίζεται από το Moodle HQ, το οποίο χρηματοδοτείται από ένα δίκτυο περισσότερων από 80 εταιρειών παροχής υπηρεσιών Moodle Partner παγκοσμίως.

Συντηρώντας δεκάδες χιλιάδες περιβάλλοντα μάθησης παγκοσμίως, το Moodle αποτελεί έμπιστο εργαλείο για ιδρύματα και οργανισμούς μεγάλους και μικρούς, όπως το Shell, το London School of Economics, το Πανεπιστήμιο της Νέας Υόρκης, η Microsoft και το Open University. Ο παγκόσμιος αριθμός των περισσότερων από 90 εκατομμυρίων χρηστών της Moodle σε ακαδημαϊκή και επιχειρηματική χρήση καθιστά την πλατφόρμα μάθησης που χρησιμοποιείται περισσότερο παγκοσμίως.

4.2 Χαρακτηριστικά Moodle

Το απλά σχεδιασμένο περιβάλλον, χαρακτηριστικά drag-and-drop και καλά τεκμηριωμένοι πόροι μαζί με συνεχείς βελτιώσεις ευχρηστίας καθιστούν το Moodle εύκολο στην εκμάθηση και χρήση.

Επίσης, το Moodle παρέχεται δωρεάν ως λογισμικό ανοιχτού κώδικα, στο πλαίσιο της Γενικής Δημόσιας Άδειας GNU. Οποιοσδήποτε μπορεί να προσαρμόσει, να επεκτείνει ή να τροποποιήσει το Moodle τόσο για εμπορικά όσο και για μη εμπορικά έργα χωρίς αμοιβή αδειοδότησης και να επωφεληθεί από την αποδοτικότητα του κόστους, την ευελιξία και άλλα πλεονεκτήματα της χρήσης του. Η προσέγγιση ανοιχτού κώδικα του σχεδίου Moodle σημαίνει ότι το Moodle αναθεωρείται συνεχώς και βελτιώνεται ώστε να ανταποκρίνεται στις τρέχουσες και εξελισσόμενες ανάγκες των χρηστών του.

Οι πολύγλωσσες δυνατότητες του Moodle εξασφαλίζουν ότι δεν υπάρχουν γλωσσικοί περιορισμοί στη μάθηση στο διαδίκτυο. Η κοινότητα του Moodle έχει αρχίσει να μεταφράζει το Moodle σε περισσότερες από 120 γλώσσες (και αυξάνονται), ώστε οι χρήστες να μπορούν εύκολα να εγκαταστήσουν τον Moodle ισότοπο τους, καθώς και πολλούς πόρους, υποστήριξη και συζητήσεις σε διάφορες γλώσσες.

Επιπρόσθετα, το Moodle παρέχει το πιο ευέλικτο σετ εργαλείων που υποστηρίζει τόσο προγράμματα συνδυασμένης μάθησης όσο και 100% online μαθήματα. Διαμορφώνοντας το Moodle υπάρχει η δυνατότητα της ενεργοποίησης ή απενεργοποίησης των βασικών λειτουργιών καθώς και της εύκολης ενσωμάτωσης όλων όσων χρειάζονται για ένα μάθημα χρησιμοποιώντας το πλήρες φάσμα των ενσωματωμένων λειτουργιών, συμπεριλαμβανομένων των εξωτερικών συνεργατικών εργαλείων όπως φόρουμ, wiki, chat και blogs.

Τέλος, το Moodle είναι βασισμένο στο διαδίκτυο και έτσι μπορεί να αποκτηθεί πρόσβαση από οπουδήποτε στον κόσμο. Με μια προεπιλεγμένη διασύνδεση συμβατή με το κινητό και συμβατότητα μεταξύ των browsers, το περιεχόμενο της πλατφόρμας Moodle είναι εύκολα προσβάσιμο και συνεπές σε διαφορετικά προγράμματα περιήγησης και μηχανές ιστού.

Παράλληλα, εγγυάται τη διασφάλιση της ασφάλειας των δεδομένων και της δηκτικότητας των χρηστών καθώς οι έλεγχοι ασφαλείας ενημερώνονται και εφαρμόζονται συνεχώς σε διαδικασίες ανάπτυξης και λογισμικού για προστασία από μη εξουσιοδοτημένη πρόσβαση, απώλεια δεδομένων και κακή χρήση. Το Moodle μπορεί εύκολα να αναπτυχθεί σε ένα ιδιωτικό ασφαλές σύννεφο ή διακομιστή για πλήρη έλεγχο.

4.3 Δομή Moodle

Η μπροστινή σελίδα ενός ιστότοπου Moodle - η σελίδα που φτάνετε από το πρόγραμμα περιήγησής σας - συνήθως περιλαμβάνει πληροφορίες για το ίδρυμα και μπορεί να προσαρμοστεί σε μεγάλο βαθμό. (Σημειώστε ότι είναι επίσης δυνατό να κλειδώσετε την πρώτη σελίδα προς τα κάτω, ώστε το μόνο που θα μπορεί ο χρήστης να βλέπει όταν κάνει κλικ στο URL της Moodle είναι μια οθόνη σύνδεσης).

Ο τρόπος με τον οποίο οι χρήστες συμμετέχουν σε μια τοποθεσία Moodle εξαρτάται από την εγκατάσταση: ενδέχεται να τους δοθούν στοιχεία σύνδεσης. μπορεί να τους επιτραπεί να κάνουν τους λογαριασμούς τους, ή να συνδεθούν αυτόματα από άλλο σύστημα.

Η βασική δομή του Moodle οργανώνεται γύρω από τα μαθήματα. Αυτά είναι βασικά σελίδες ή περιοχές εντός του Moodle όπου οι εκπαιδευτικοί μπορούν να παρουσιάσουν τους μαθησιακούς τους πόρους και δραστηριότητες στους μαθητές. Μπορούν να έχουν διαφορετικές διατάξεις, αλλά συνήθως περιλαμβάνουν μια σειρά κεντρικών τμημάτων όπου εμφανίζονται τα υλικά και πλευρικά μπλοκ που προσφέρουν επιπλέον χαρακτηριστικά ή πληροφορίες.

Τα μαθήματα μπορούν να περιέχουν περιεχόμενο για σπουδές ενός έτους, μία μόνο σύνοδο ή άλλες παραλλαγές ανάλογα με το δάσκαλο ή την εγκατάσταση. Μπορούν να χρησιμοποιηθούν από έναν δάσκαλο ή να μοιραστούν από μια ομάδα καθηγητών.

Ο τρόπος με τον οποίο οι σπουδαστές εγγράφονται σε μαθήματα εξαρτάται από την εγκατάσταση για παράδειγμα, μπορούν να εγγραφούν αυτομάτως, να εγγραφούν με το χέρι από τον δάσκαλό τους ή αυτόματα από το διαχειριστή.

Τα μαθήματα είναι οργανωμένα σε κατηγορίες για παράδειγμα : Μαθήματα Φυσικής, Χημείας και Βιολογίας ενδέχεται να εμπίπτουν στην κατηγορία Επιστήμη, για παράδειγμα.

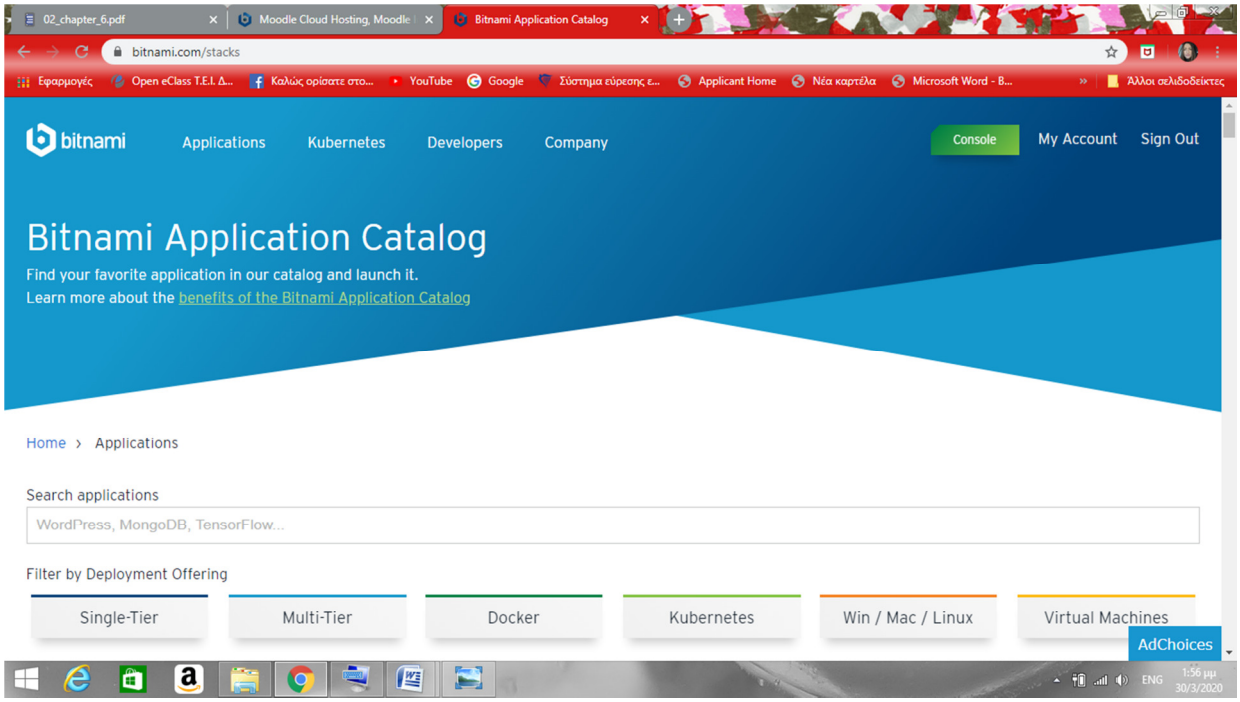
Δεν εισάγετε το Moodle με το ρόλο του "δάσκαλου" ή "φοιτητή". Όλοι όσοι συνδεθούν στο Moodle δεν έχουν ειδικά προνόμια μέχρι να τους δοθούν ρόλοι από τον διαχειριστή ανάλογα με τις ανάγκες τους σε μεμονωμένα μαθήματα ή πλαίσια.

Τέλος, ένας συνδεδεμένος χρήστης μπορεί να έχει πρόσβαση σε περιοχές του Moodle, όπως τα μαθήματα ή το προφίλ του, αυτό βέβαια εξαρτάτε από το ρόλο τους. Κάθε χρήστης έχει τον δικό του προσαρμόσιμο πίνακα ελέγχου.

4.4 Εγκατάσταση Moodle

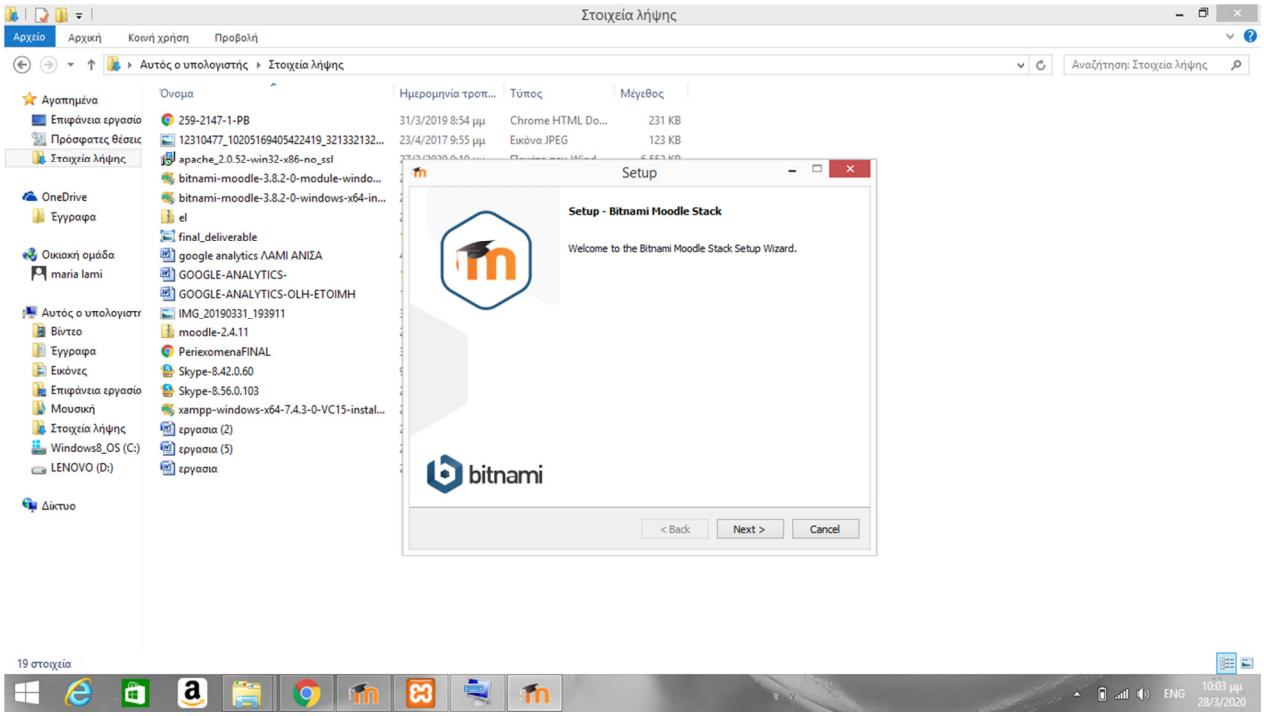
Στη συνέχεια, θα αναλύσουμε την διαδικασία εγκατάστασης του Moodle με χρήση του Bitnami. Το Bitnami είναι μια βιβλιοθήκη δημοφιλών εφαρμογών εξυπηρετητών (server applications) και περιβαλλόντων ανάπτυξης τα οποία μπορούν να εγκατασταθούν είτε τοπικά σε προσωπικό υπολογιστή, είτε σε μια εικονική μηχανή (virtual machine), είτε στο cloud .Μπορεί να χρησιμοποιηθεί σε λειτουργικά συστήματα Windows, OS X και διανομές Linux (συμπεριλαμβανομένων των Fedora, Ubuntu, CentOS, Debian, κ.α.).

Αφού γίνει αρχικά η σύνδεση στην ιστοσελίδα του Bitnami, μπορεί στη συνέχεια να επιλεγεί το Moodle από τη βιβλιοθήκη με τις εφαρμογές (https://bitnami.com/stacks) (Εικόνα 1) και να πραγματοποιηθεί λήψη του επιθυμητού πακέτου εγκατάστασης. Το Bitnami Moodle Stack είναι ένα δωρεάν πακέτο εγκατάστασης που απλοποιεί κατά πολύ τη διαδικασία εγκατάστασης, καθώς συμπεριλαμβάνει εκδόσεις MySQL, PHP και Apache που είναι έτοιμες να εκτελεστούν χωρίς κάποια ρύθμιση.



Εικόνα 8

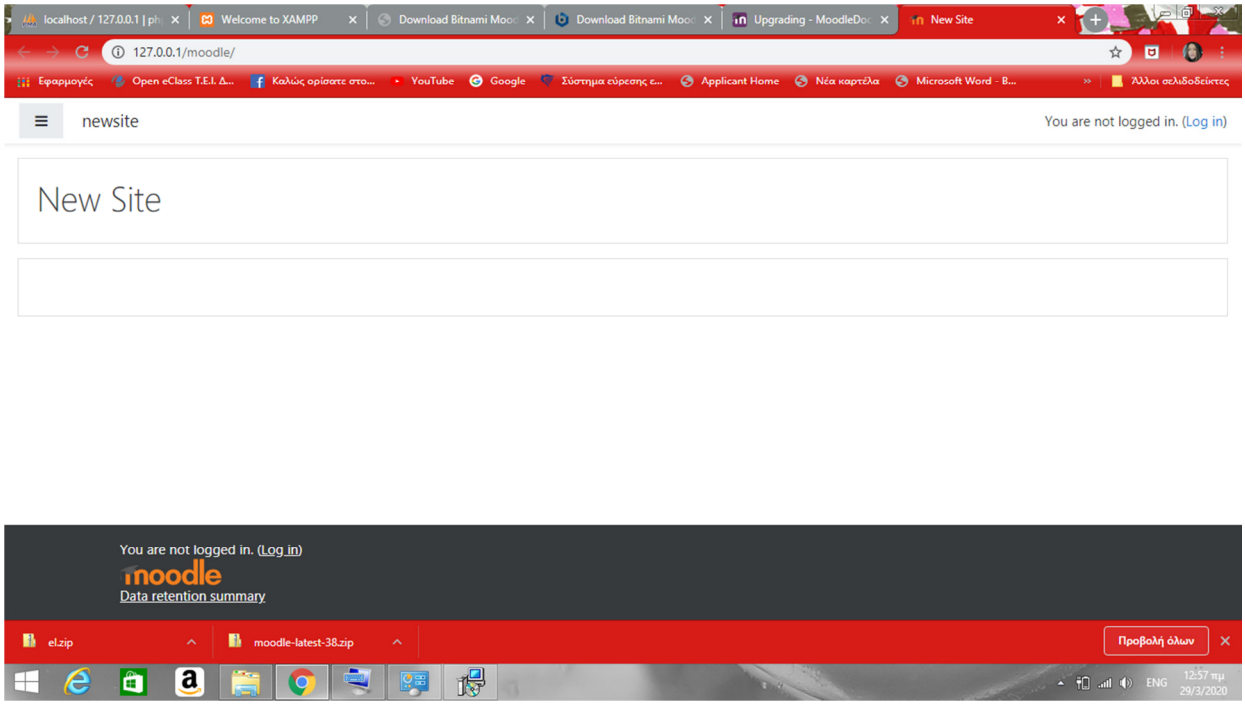
Αφού γίνει η λήψη της Bitnami θα κάνουμε το setup για εγκατάσταση στον υπολογιστή μας όπως βλέπουμε και στη παρακάτω εικόνα.(Εικόνα 9)



Εικόνα 9

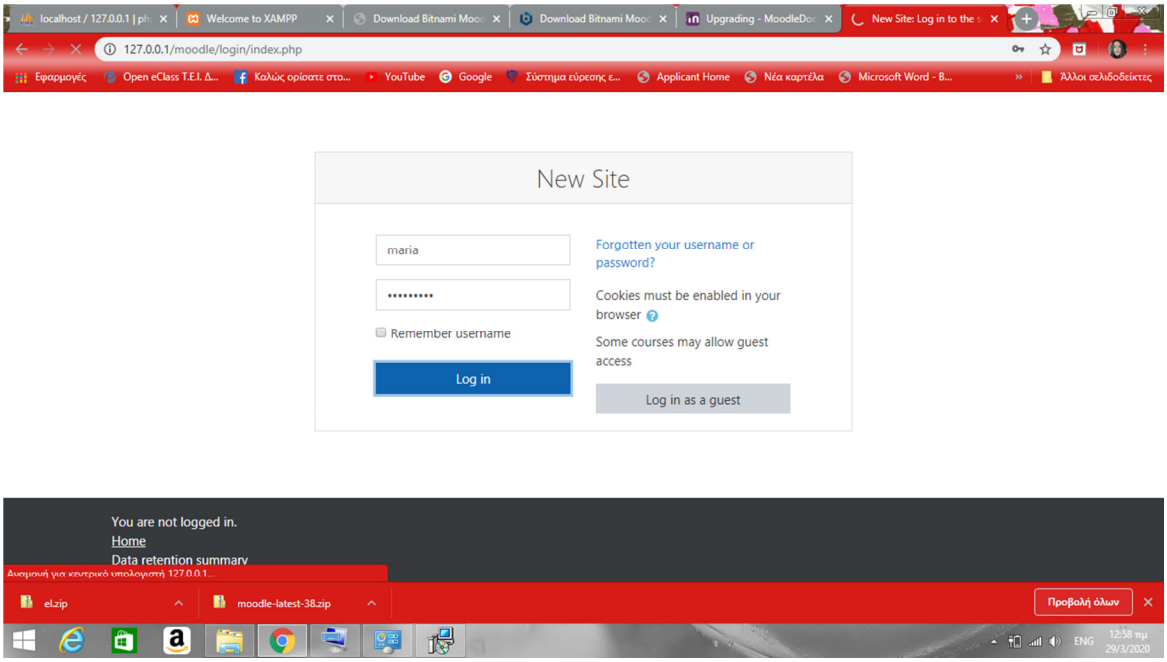
Εφόσον πραγματοποιηθεί το setup μας εμφανίζετε αυτή η σελίδα (Εικόνα10)

Που φανερώνει ότι έγινε η εγκατάσταση της moodle με διεύθυνση http://127.0.0.1/moodle/\

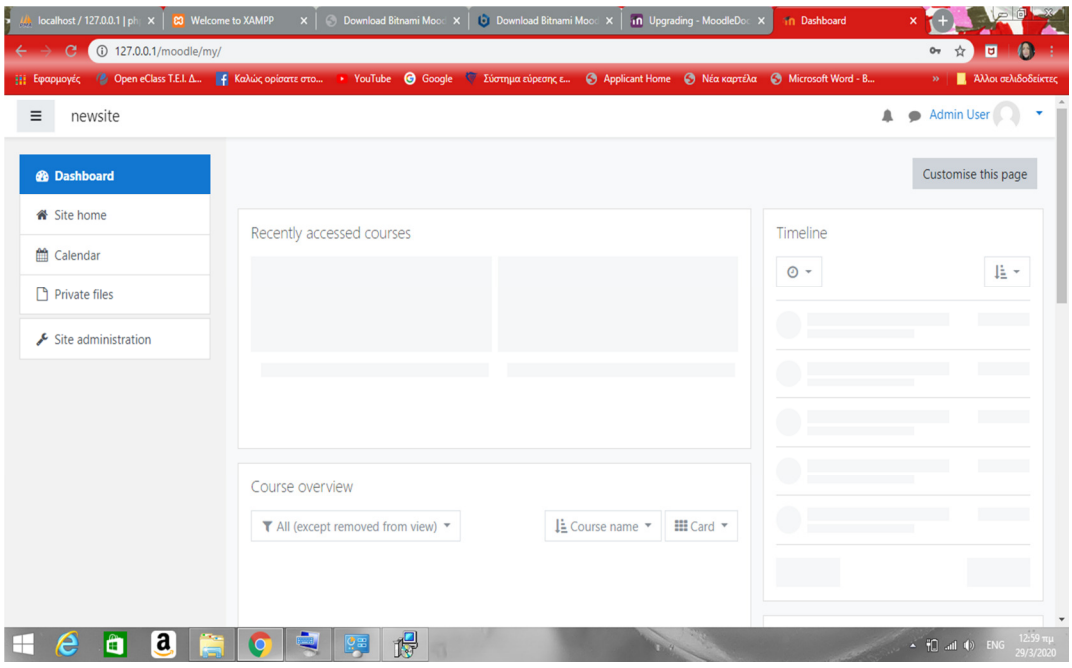


Εικόνα 10

Έπειτα δημιουργούμε το λογαριασμό μας όπως βλέπουμε στην παρακάτω εικόνα. (εικόνα 11) Μόλις κάνουμε την εγγραφή μας βλέπουμε την αρχική πλατφόρμα της moodle. Εκεί μπορούμε να κάνουμε οποιαδήποτε εργασία (εικόνα 12)

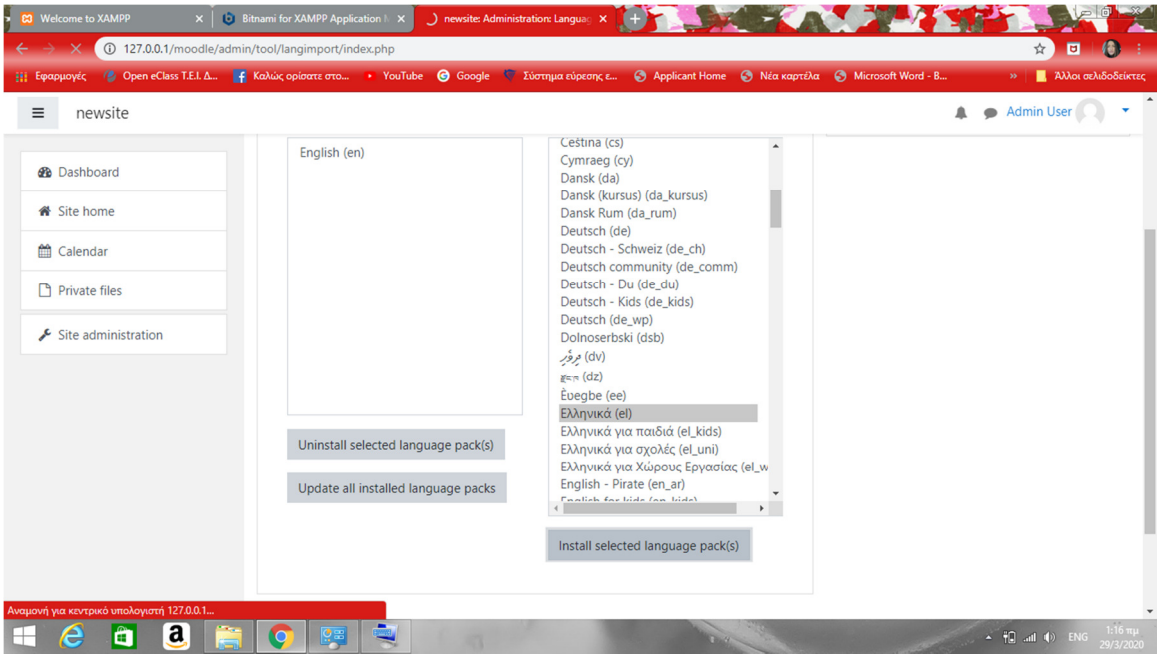


Εικόνα 11

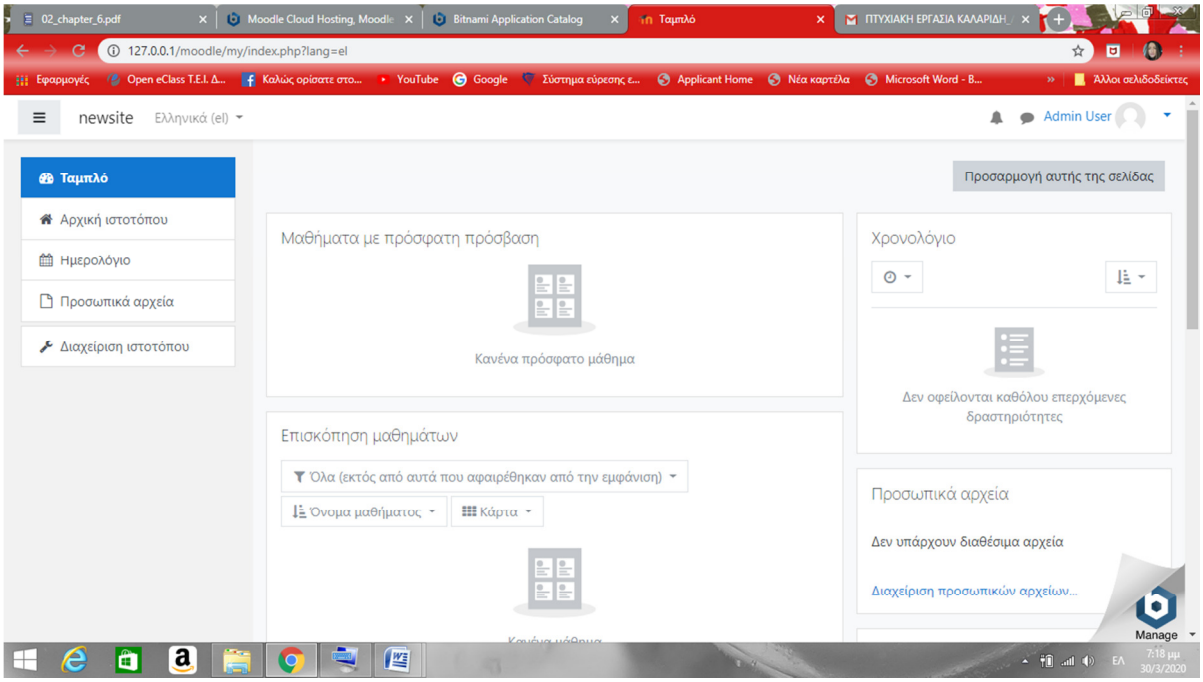


Εικόνα 12

Επειδή η πλατφόρμα είναι στα αγγλικά θα πάμε να εγκαταστήσουμε τα ελληνικά (εικόνα 13). Στις ρύθμισης γλώσσας βρίσκουμε τα ελληνικά και κάνουμε την εγκατάσταση. Έπειτα η πλατφόρμα είναι έτοιμη και στα ελληνικά .Αυτή λοιπόν είναι τελική εμφάνιση της σελίδας μας στην moodle όπου εκεί θα δημιουργήσουμε τα μαθήματα (εικόνα 14)



Εικόνα 13



Εικόνα 14

4.5 Το moodle στην ελληνική πραγματικότητα

Σήμερα υπάρχουν παγκοσμίως 54 Moodle Partners, που υποστηρίζουν τους χρήστες και τους διαχειριστές της πλατφόρμας σε όλα τα επίπεδα. Το 2010 η εταιρία Διαδραστικές Τεχνολογίες Μάθησης και Πολιτισμού έγινε ο Moodle Partner στην Ελλάδα. Γίνεται λοιπόν εμφανής η δυναμική που έχει η μεγάλη κοινότητα του Moodle, η οποία ολοένα και διευρύνεται, εξελίσσοντας το λογισμικό και τις προσφερόμενες υπηρεσίες.

Ο Moodle Partner της Ελλάδας μπορεί να προσφέρει υπηρεσίες όπως:

- η εγκατάσταση και παραμετροποίηση μια πλατφόρμας Moodle,
- η αναβάθμιση της πλατφόρμας από την μία έκδοση στην άλλη,
- η σχεδίαση μοναδικών themes,
- η παροχή υποστήριξης στην χρήση του Moodle,
- η σχεδίαση νέων λειτουργιών που να ικανοποιεί τις ιδιαίτερες απαιτήσεις που μπορεί να έχει κάποιος οργανισμός,
- η εκπαίδευση χρηστών για τη χρήση της πλατφόρμας αλλά και παροχή ενός πτυχίου, το οποίο μπορούν να εκδώσουν μόνοι οι Moodle Partners, για την πιστοποίηση των γνώσεων ενός καθηγητή στην χρήση του Moodle. Το

πτυχίο αυτό αναγνωρίζεται από την επίσημη κοινότητα του Moodle, και είναι γνωστό ως Πιστοποίηση Δημιουργού Μαθημάτων (Moodle Course Creator Certification).

- Στις υπηρεσίες υποστήριξης, περιλαμβάνονται και συμβουλευτικές υπηρεσίες όπως της εκπαίδευσης χρηστών για τη σωστή χρήση εργαλείων συγγραφής εκπαιδευτικού υλικού, τον εκπαιδευτικό σχεδιασμό, την οργάνωση των μαθημάτων κλπ, ακόμη και η υλοποίηση εκπαιδευτικού υλικού για τις ανάγκες ενός μαθήματος.

Εκτός από τον πιστοποιημένο Moodle Partner στην Ελλάδα, υπάρχει και η ελληνική κοινότητα υποστήριξης του Moodle η οποία είναι διαθέσιμη για κάθε ενδιαφερόμενο στην παρακάτω διεύθυνση https://moodle.org/course/view.php?id=49. Σε αυτή τη σελίδα μπορείτε να βρείτε ελληνικά γραμμένα σχέδια μαθήματος, οδηγοί βοήθειας και υποστήριξης.

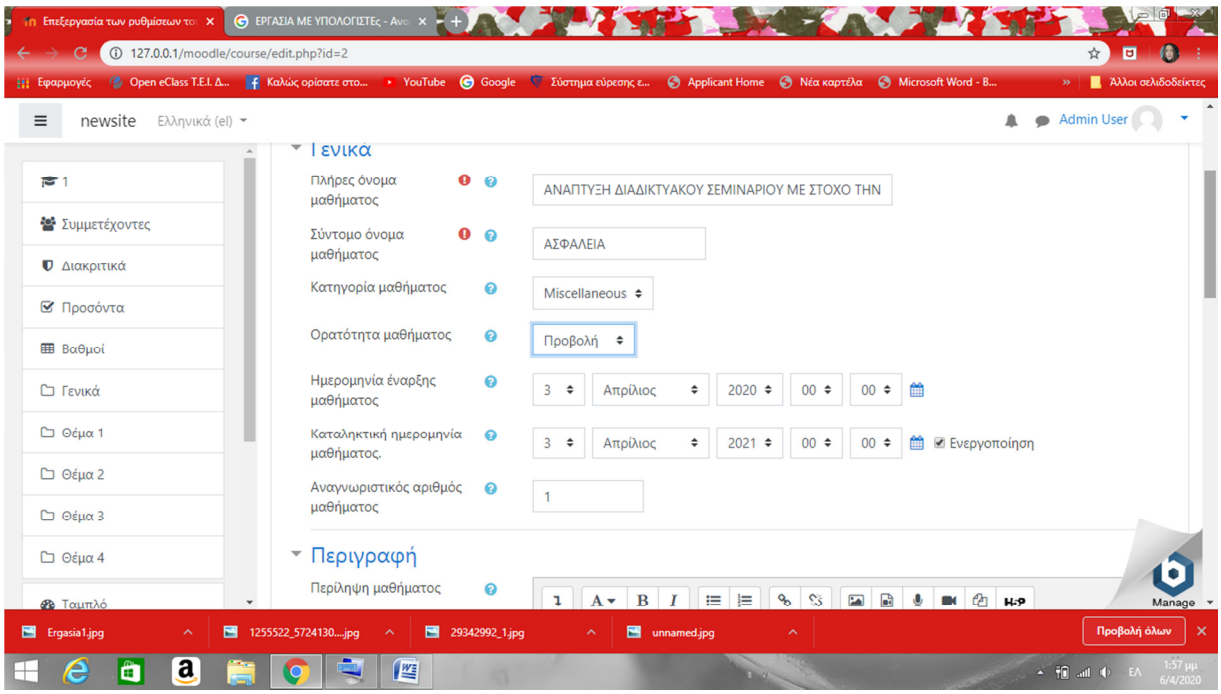
Τόσο από την εξέλιξη που έχει και τις εκδόσεις της ίδιας της πλατφόρμας, όσο και από την έντονη κινητικότητα ειδικών ηλεκτρονικής μάθησης και των εκπαιδευτικών σχεδιαστών και των μηχανικών λογισμικού, δημιουργείται έντονο ενδιαφέρον για την πλατφόρμα Moodle. Όλα αυτά συνετέλεσαν ώστε να εξελιχθεί στην πιο δημοφιλής, ανοικτού κώδικα, εκπαιδευτική λύση.

Το Moodle είναι ένα σύστημα με ολοένα αυξανόμενες και βελτιούμενες υπηρεσίες που διεισδύει σε χώρους αντικαθιστώντας πολυδάπανες εμπορικές λύσεις. Είναι θέμα χρόνου η επικράτησή του ως το πλέον κατάλληλο σύστημα υποστήριξης της μαθησιακής διαδικασίας σε όλα τα επίπεδα.

5 ΠΑΡΟΥΣΙΑΣΗ ΔΙΑΔΙΚΤΥΑΚΟΥ ΣΕΜΙΝΑΡΙΟΥ ΑΣΦΑΛΕΙΑΣ ΠΛΗΡΟΦΟΡΙΩΝ ΣΕ MOODLE

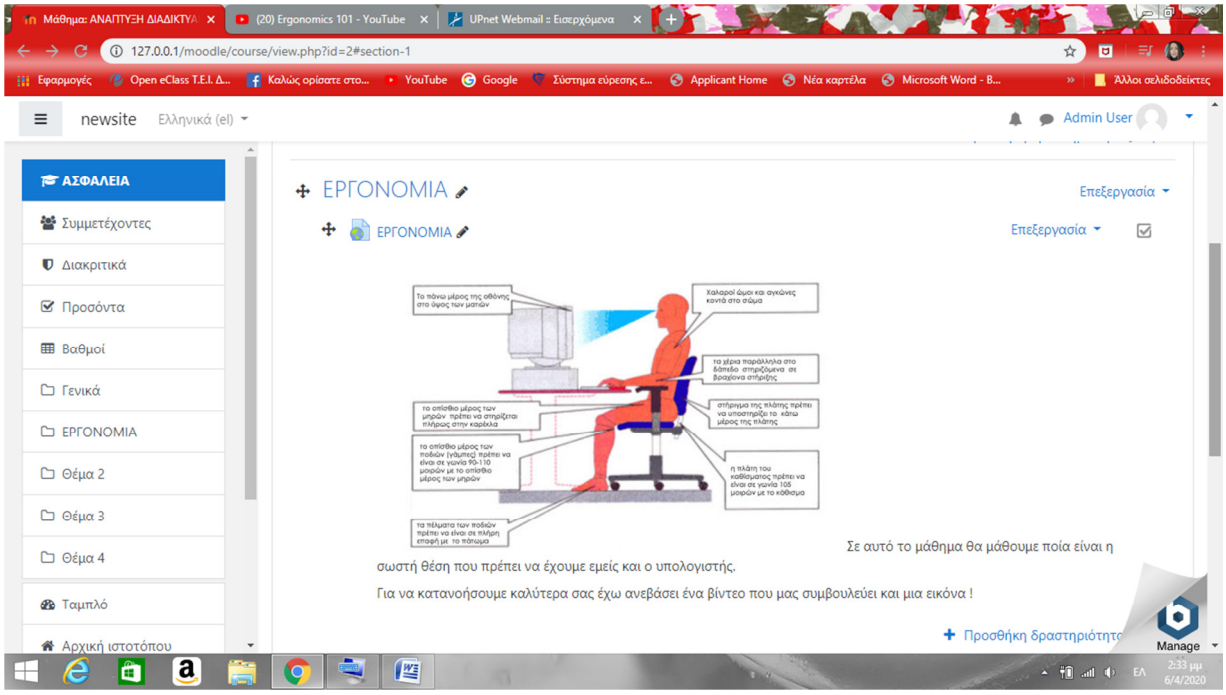
Σε αυτό το κεφάλαιο θα παρουσιαστή η δημιουργία ενός μαθήματος στην πλατφόρμα της Moodle όπου θα μπορούμε να ανεβάσουμε διάφορα εκπαιδευτικά αρχεία ώστε να υλοποιήσουμε ένα διαδικτυακό σεμινάριο Ασφάλειας Πληροφοριών.

Για το λόγο αυτό δημιουργήσαμε ένα μάθημα στην πλατφόρμα τις Moodle που το ονομάσαμε <<ανάπτυξη διαδικτυακού σεμιναρίου με στόχο την ενημέρωση διοικητικών υπαλλήλων σε θέματα ασφάλειας πληροφοριών>> . (Εικόνα 15) Μέσα σε αυτό το μάθημα λοιπόν φτιάξαμε έξη θέματα προς συζήτηση σύμφωνα με τις παρακάτω εικόνες.



Εικόνα 15

Το πρώτο θέμα του σεμιναρίου μας είναι η εργονομία (Εικόνα 16) . Σε αυτό το θέμα έχουμε ανεβάσει ένα βίντεο και μια εικόνα που σκοπό έχουμε να ενημερώσουμε το προσωπικό για την κατάλληλη θέση που πρέπει να έχει τόσο ο υπάλληλος όσο και η κατάλληλη θέση που πρέπει να έχει και ο υπολογιστής .



Εικόνα 16

Το δεύτερο θέμα του σεμιναρίου μας είναι η ασφάλεια κατά την πλοήγηση στον παγκόσμιο ιστό. Σε αυτό το θέμα θα μάθουμε ποιοι είναι οι κίνδυνοι που υπάρχουν κατά την πλοήγηση μας στον παγκόσμιο αυτόν ιστό. (Εικόνα 17) Για να αναπτύξουμε αυτό το θέμα συλλέξαμε κάποιες πληροφορίες για το πώς μπορούμε να είμαστε ασφαλείς στο διαδίκτυο και ποιοί είναι οι κίνδυνοι που έχουμε κατά την πλοήγηση μας σε αυτόν το παγκόσμιο ιστό.

Αρχικά θα μιλήσουμε ποια είναι τα βασικά μέτρα που πρέπει να έχουμε κατά την πλοήγηση μας:

1. Τα άτομα που γνωρίζουμε στο Διαδίκτυο δεν είναι πάντοτε αυτά που ισχυρίζονται ότι είναι , μπορεί να μας λένε ψέματα για να κερδίσουν την εμπιστοσύνη μας.
2. Δεν δίνουμε ποτέ τα προσωπικά μας στοιχεία, ούτε αποκαλύπτουμε σε άλλους χρήστες του Διαδικτύου πληροφορίες που αφορούν τους φίλους μας, την οικογένειά μας ή στην εργασία μας.
3. Δεν δίνουμε σε κανέναν του κωδικούς πρόσβασης (password) που χρησιμοποιούμε.
4. Κάνουμε προσεκτικές αγορές μέσου του Διαδικτύου για την αγορά προϊόντων και δεν δίνουμε στοιχεία που φορούν πιστωτικές κάρτες.
5. Είμαστε προσεκτική ως προς την αποδοχή όσων διαβάζουμε στο Διαδίκτυο ή αυτών που μας λένε οι άλλοι χρήστες του, πριν το υποβάλουμε στην κρίση μας.

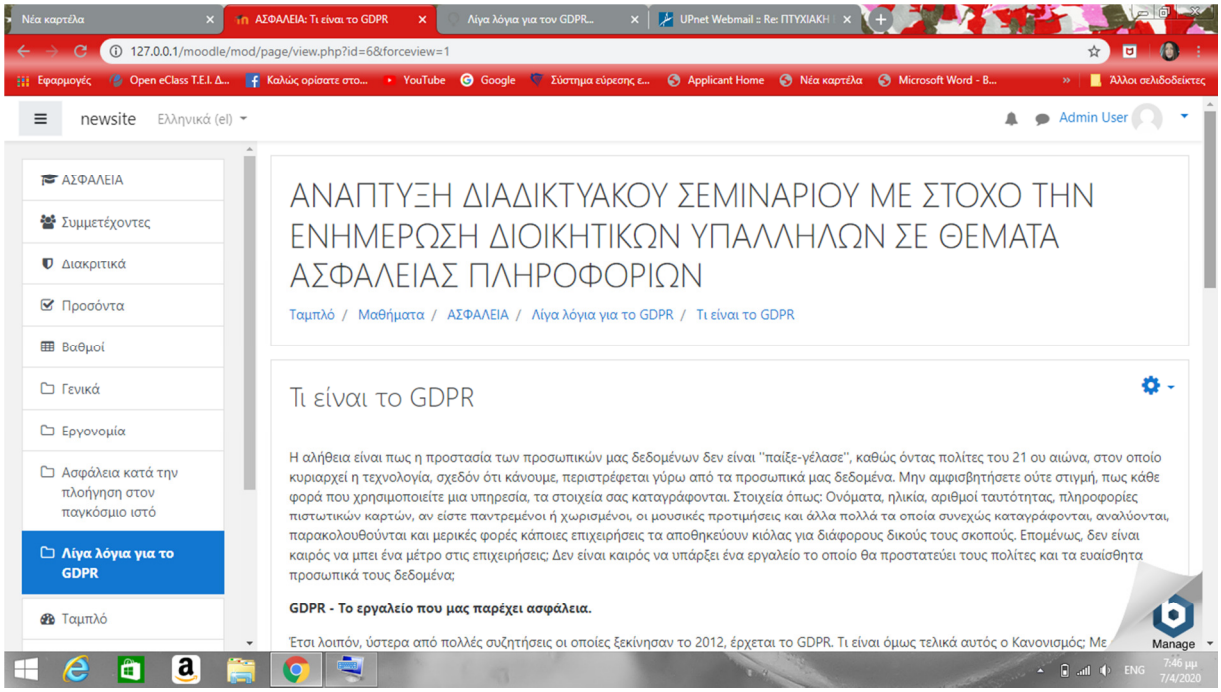
6. Το ίδιο παράνομη πράξη θεωρείται και η διακίνηση προγραμμάτων υπολογιστών (Software), εκτός και αν ανήκουν στην κατηγορία του Ελεύθερου Λογισμικού (Open source Software).
7. Προσέχουμε τα μηνύματα (e-mail) και επισυναπτόμενα αρχεία από άγνωστους αποστολείς με περίεργα θέματα (subject) ή χωρίς θέμα. Συνήθως περιέχουν ιούς και να προκαλέσουν σοβαρά προβλήματα στον υπολογιστή μας.
8. Δεν χρησιμοποιούμε οποιοιδήποτε προγράμματα στο Διαδίκτυο που είναι δωρεάν. Δεν είναι όλα τα προγράμματα ασφαλή.

Οι βασικοί κίνδυνοι που υπάρχουν σε αυτόν τον ιστό είναι τα εξής:

- Κατά την πλοήγηση στους χώρους του Διαδικτύου είναι καλό να έχουμε υπόψη μας τα παρακάτω:
- Το Διαδίκτυο είναι κυρίως μια κοινωνία ανθρώπων και κρύβει τους ίδιους κινδύνους που κρύβει κάθε κοινωνία, ιδιαίτερα όταν διευκολύνεται στο έπακρο ο τρόπος επικοινωνίας των ανθρώπων μεταξύ τους.
- Οι πληροφορίες ου υπάρχουν στο Διαδίκτυο δεν είναι πάντα έγκυρες.
- Δεν κοινοποιούμε ποτέ τα προσωπικά μας στοιχεία (ονοματεπώνυμο, διεύθυνση, τηλέφωνο, φωτογραφία, κωδικοί πρόσβασης, αριθμός πιστωτικών καρτών, e-mail κ.λπ.) είναι καλό να αποφεύγεται.
- Σε αυτήν τη διεύθυνση http://www.safeline.gr/ έχουμε ίσως τη μοναδική ελληνική ανοικτή γραμμή για καταγγελία παράνομου περιεχομένου στο διαδίκτυο. Μη διστάσετε να την χρησιμοποιήσετε.

Εικόνα 17

Το τρίτο θέμα του σεμιναρίου μας είναι να μάθουμε για το GDPR τι είναι και γιατί είναι πολύ σημαντικό για τις επιχειρήσεις.(Εικόνα18) Το GDPR είναι πολύ σημαντικό για του υπαλλήλους για να μπορούν να αισθάνονται ασφαλείς .Γιατί σε περίπτωση παραβιάσεις των προσωπικών τους δεδομένων σημαντικές ποινές σε περίπτωση μη συμμόρφωσης, ανάλογα με το μέγεθος της ζημιάς. Συγκεκριμένα, τα πρόστιμα κυμαίνονται από 10-20 εκατομμύρια ευρώ έως 4% του συνολικού ετήσιου κύκλου εργασιών της επιχείρησης για παραβίαση των δεδομένων. Επομένως, αν ένας πελάτης ζητήσει τα δεδομένα του και δεν τα λάβει, αν υπάρξει παράνομη συγκέντρωση πληροφοριών ή μεταφορά προσωπικών δεδομένων προς τρίτους, το DGPR θα είναι εκεί για να τιμωρήσει αυτές τις επιχειρήσεις.



Εικόνα 18

Το τέταρτο θέμα του σεμιναρίου μας είναι το email και πως πρέπει να ήμαστε ασφαλείς κατά την χρήση του μιας και είναι ένα από το πιο σημαντικό μέσω που όλος ο πλανήτης πλέον χρησιμοποιεί στην καθημερινότητα του. (Εικόνα 19) Το e-mail έχει τρία βασικά χαρακτηριστικά

- Το φάκελο του μηνύματος
- Την επικεφαλίδα του
- Το κυρίως σώμα του μηνύματος

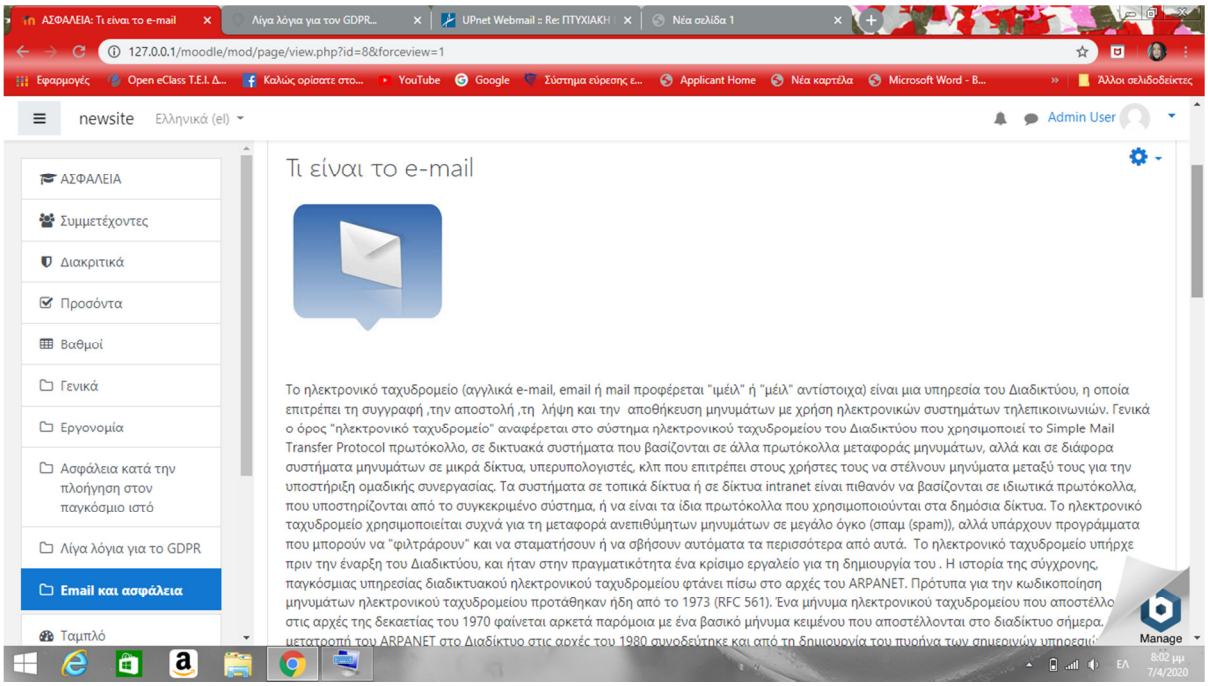
Πως χρησιμοποιούμε όμως το e-mail. Το ηλεκτρονικό αυτό μήνυμα το χρησιμοποιούμε για να ανταλλάξουμε μηνύματα φωτογραφίες και οποιεσδήποτε άλλες πληροφορίες και αν θέλουμε μέσα σε λίγα μόλις λεπτά για αυτό το λόγο πρέπει να είμαστε πάρα πολύ προσεκτική. Επίσης μέσω του ηλεκτρονικού ταχυδρομείου μπορούμε να προωθήσουμε ένα μήνυμα που μας έχουν στείλει απευθείας σε κάποιον άλλο παραλήπτη προωθώντας το. Μπορούμε να ενημερωθούμε για προσφορές και διάφορα γεγονότα μέσω του e-mail μας.

Για όλα αυτά δεν είναι ανάγει κάποιος να είναι στον υπολογιστή του αρκεί να έχει κάνει εγκατάσταση της εφαρμογής στο κινητό του και όλα αυτά γίνονται ακόμα πιο εύκολα.

Συμβουλές για την ασφάλεια

Για να είναι πάντα ασφαλής ο λογαριασμός σας, προσέξτε τα εξής 6 πράγματα: Προστατεύστε τον κωδικό σας: Μη χρησιμοποιείτε πουθενά αλλού τον κωδικό πρόσβασης σας. Μην κοινοποιείτε ποτέ τον προσωπικό σας κωδικό πρόσβασης. Πρέπει να είστε το μοναδικό άτομο που το γνωρίζει. Προσπαθήστε να μην περιλαμβάνετε το όνομά σας ή συνηθισμένες λέξεις. Ο κωδικός πρόσβασης σας πρέπει να είναι τέτοιες που να μην μπορεί κάποιος να το μαντέψει εύκολο.

1. Χρησιμοποιήστε τις επιπλέον λειτουργίες ασφαλείας.
2. Βεβαιωθείτε ότι οι λογαριασμοί email που χρησιμοποιείτε είναι ασφαλείς.
3. Να αποσυνδέεστε πάντοτε όταν χρησιμοποιείτε κοινόχρηστο υπολογιστή. Αν το ξεχάσετε μπορείτε να αποσυνδεθείτε απολακτισμένα.
4. Να χρησιμοποιείτε πάντοτε λογισμικό προστασίας από τους ιούς στον υπολογιστή σας:
    a. Για Windows
    b. Για Mac OS
5. Σκεφτείτε καλά πριν πατήσετε ή κατεβάσετε κάτι.

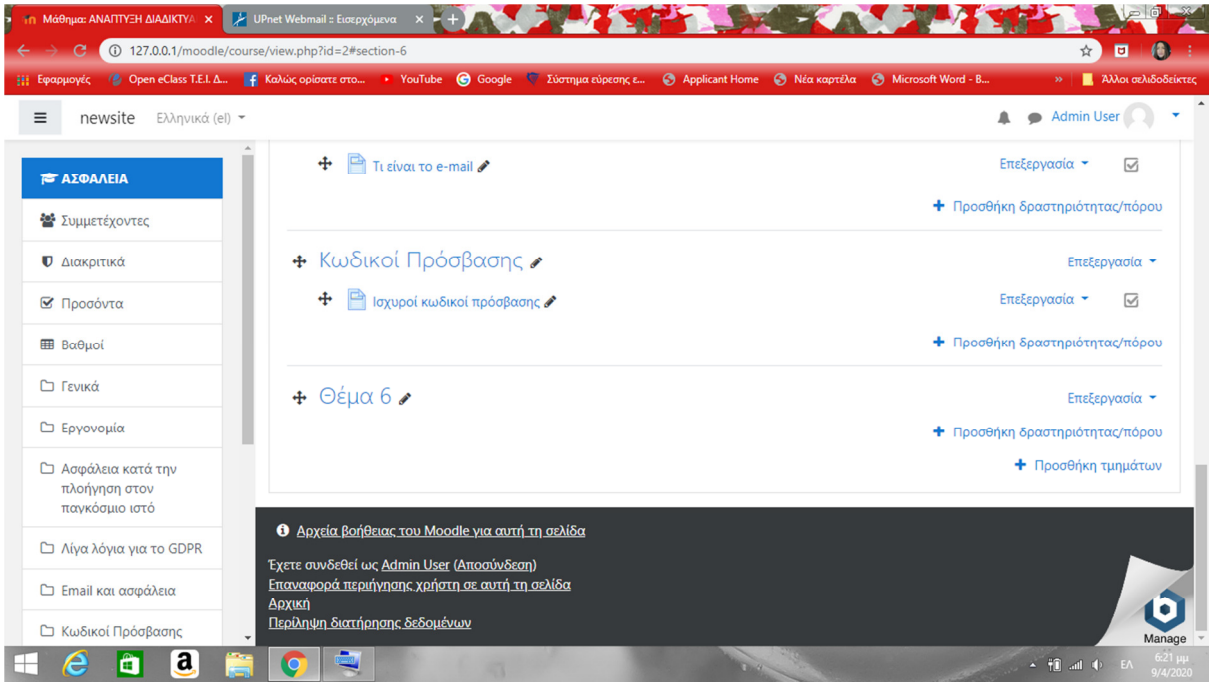


Εικόνα 19

Το πέμπτο θέμα του σεμιναρίου μας είναι οι κωδικοί προσβάσεις. Σε αυτό το θέμα θα μάθουμε γιατί πρέπει ο καθένας μας να είναι πολύ προσεκτικός όσο αφορά τους κωδικούς προσβάσεις μας και τρόποι που μπορούμε να προστατεύουμε αυτούς τους κωδικούς . (Εικόνα 20) Το σημαντικότερο κομμάτι της δημιουργίας λογαριασμού αποτελεί η θέσπιση κωδικού πρόσβασης (password). Ο μυστικός κωδικός αποτελεί το «κλειδί» για την είσοδο στο προσωπικό μας προφίλ, καθώς η διεύθυνση ηλεκτρονικού ταχυδρομείου (που συνήθως προτιμάται ως username) είναι κοινή γνώση. Η διαδικασία εύρεσης του κατάλληλου password δεν πρέπει να χαρακτηρίζεται από βαρεμάρα και ταχύτητα, αλλά από συνειδητές επιλογές και επιτυχή εύρεση του ιδανικού.

Συμβουλές για ισχυρό κωδικό πρόσβασης

- Πρέπει να είναι εκτενείς
- Δεν χρειάζεται να βγάζουν νόημα
- Πρέπει να περιλαμβάνουν σύμβολα, νούμερα και κεφαλαία
- Δεν πρέπει να περιλαμβάνουν προσωπικές πληροφορίες
- Δεν πρέπει ΠΟΤΕ να επαναχρησιμοποιούμε τους ίδιους κωδικούς
- Δεν πρέπει να γνωρίζουν και άλλοι (πχ φίλοι, οικογένεια) τους κωδικούς



Εικόνα 20

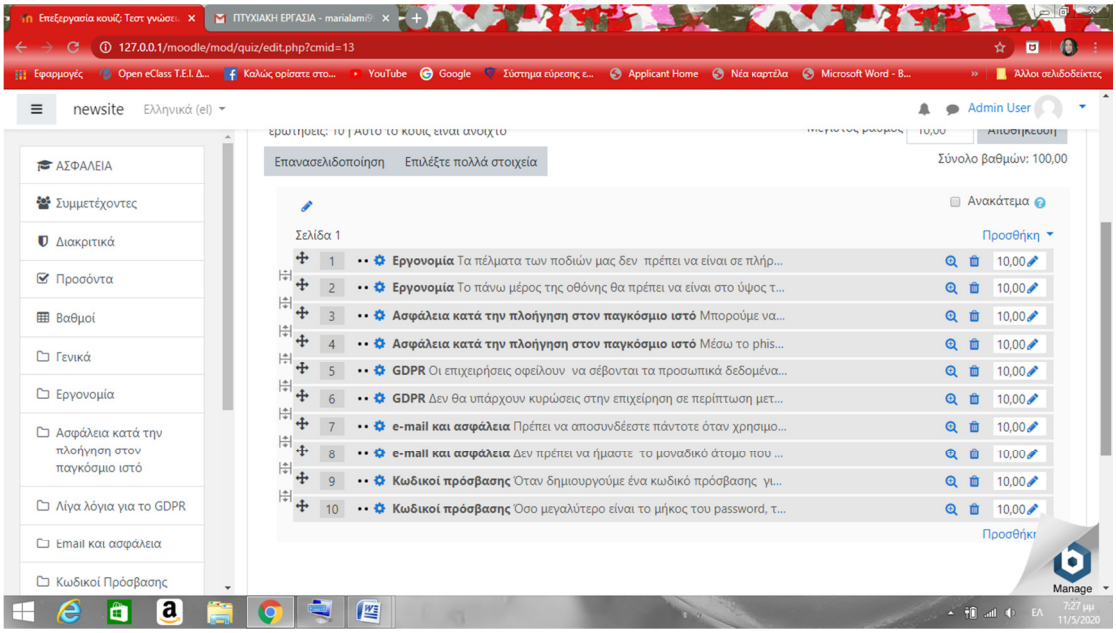
Τέλος δημιουργήσαμε λοιπόν το κουίζ γνώσεων για να μπορεί ο αναγνώστης να τεστάρει τις γνώσει του πάνω στα θέματα που αναπτύξαμε. Τα βήματα που ακολουθήσαμε για την δημιουργία του είναι τα εξής. (Εικόνα 21)

1. Αρχικά φτιάξαμε τις ερωτήσεις. (Πίνακας 1)
2. Επιλέξαμε δύο ερωτήσεις από το κάθε θέμα .
3. Γράψαμε τις ερωτήσεις.
4. Αποφασίσαμε ότι ο αναγνώσεις θα μπορεί να απαντήσει με Σωστό η Λάθος.
5. Έτσι λοιπόν κατά την διάρκεια της γραφής των ερωτήσεων έπρεπε να θέσουμε εμείς ποιά είναι η απάντηση αν δηλαδή είναι σωστή ή λάθος.
6. Ως επιπλέον ρυθμίσεις επιλέξαμε ότι ο μέγιστος αριθμός βαθμολογίας θα είναι το 10 και ο ελάχιστος το 0.
7. Επίσης μετά την ολοκλήρωση του τεστ από τον αναγνώστη θα του εμφανίζετε και ο χρόνος που έκανε για να απαντήσει σε αυτές της ερωτήσεις .(Εικόνα 22)

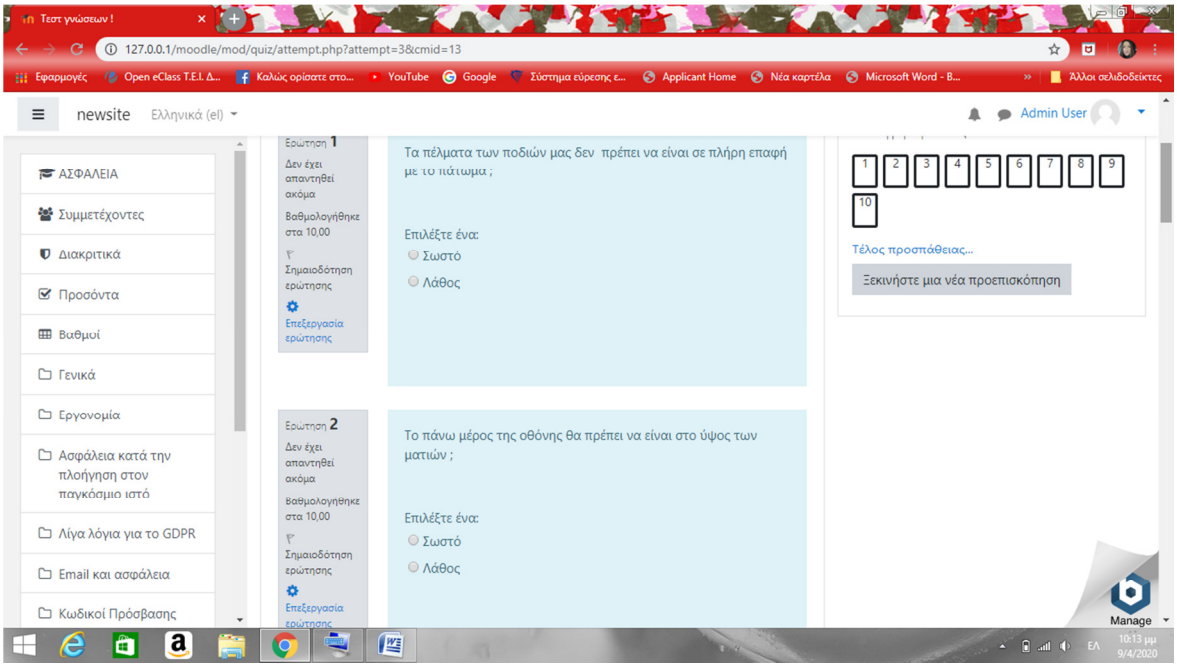
Στο παρακάτω πίνακα έχουμε τις ερωτήσεις που δημιουργήσαμε πριν τις ενσωματώσουμε στην πλατφόρμα μας στην moodle με τη σωστή τους απάντηση.

Πίνακας 5:Κατάλλογος ερωτήσεων

Ερωτήσεις	**Απαντήσεις**
Τα πέλματα των ποδιών μας δεν πρέπει να είναι σε πλήρη επαφή με το πάτωμα ;	ΛΑΘΟΣ
Το πάνω μέρος της οθόνης θα πρέπει να είναι στο ύψος των ματιών ;	ΣΩΣΤΟ
Μπορούμε να εμπιστευόμαστε οτιδήποτε και βλέπουμε και διαβάζουμε στο διαδίκτυο ;	ΛΑΘΟΣ
Μέσω το phishing, οι χάκερ μπορούν να σας κλέψουν τα προσωπικά σας δεδομένα ;	ΣΩΣΤΟ
Οι επιχειρήσεις οφείλουν να σέβονται τα προσωπικά δεδομένα των εργαζομένων τους ;	ΣΩΣΤΟ
Δεν θα υπάρχουν κυρώσεις στην επιχείρηση σε περίπτωση μεταφοράς προσωπικών δεδομένων σε τρίτους ;	ΛΑΘΟΣ
Πρέπει να αποσυνδέεστε πάντοτε όταν χρησιμοποιείτε κοινόχρηστο υπολογιστή;	ΣΩΣΤΟ
Δεν πρέπει να ήμαστε το μοναδικό άτομο που το γνωρίζει των κωδικό πρόσβασης;	ΛΑΘΟΣ
Όταν δημιουργούμε ένα κωδικό πρόσβασης για να το θυμόμαστε χρησιμοποιούμε ότι είναι πιο εύκολο για εμάς όπως(πχ (123)) ;	ΛΑΘΟΣ
Όσο μεγαλύτερο είναι το μήκος του password, τόσο δυσκολότερο έργο είναι για τους hackers ;	ΣΩΣΤΟ



Εικόνα 21



Εικόνα 22

6 ΣΥΜΠΕΡΑΣΜΑΤΑ/ ΑΠΟΤΕΛΕΣΜΑΤΑ/ ΕΠΙΛΟΓΟΣ

Σε μία εποχή που η αξία της πληροφορίας διακρίνεται ως ένα εξαιρετικά ισχυρό χαρακτηριστικό, η πρόκληση για τη μετατροπή του παραδοσιακού τρόπου λειτουργίας μιας επιχείρησης ή ενός οργανισμού σε μια αυτοματοποιημένη διαδικασία και με παράλληλη χρήση της πληροφορικής, είναι έντονη και απασχολεί την παγκόσμια κοινότητα.

Η ανάγκη για την εγκατάσταση ενός ολοκληρωμένου πληροφοριακού συστήματος σε μία επιχείρηση είναι πλέον αναπόφευκτη, αφού ικανοποιεί τις ανάγκες της, συγχωνεύοντας και τυποποιώντας τις βασικές επιχειρηματικές διαδικασίες της και αναπτύσσει ένα ενιαίο πλαίσιο λειτουργίας και επικοινωνίας.

Ωστόσο, όλο αυτό δημιουργεί και κινδύνους με αποτέλεσμα η ασφάλεια δικτύων να αποκτά όλο και μεγαλύτερη σημασία, εν όψει των διάφορων επιθέσεων, που καθιστούν την περίμετρο ασφαλείας λιγότερο αποτελεσματική αλλά και ταυτόχρονα πολύ ευάλωτη. Αναφέραμε ένα μεγάλο είδος απειλών σε συστήματα καθώς και διάφορους τρόπους με τους οποίους μπορούν να αντιμετωπιστούν.

Έπειτα, έγινε ξεχωριστή αναφορά στην ηλεκτρονική μάθηση ως τρόπο εκπαίδευσης καθώς ανάλυση της πλατφόρμας Moodle η οποία αποτελεί αυτή τη στιγμή τη πιο διαδομένη λύση για την υλοποίηση της.

Τέλος, έγινε και περιγραφή ενός υποθετικού σεναρίου όπου δημιουργήθηκε στη πλατφόρμα Moodle ένα διαδικτυακό σεμινάριο για την ενημέρωση πάνω στην ασφάλεια πληροφοριών.

ΒΙΒΛΙΟΓΡΑΦΙΑ

- Α. Τζιμογιάννης, (2017), Ηλεκτρονική μάθηση: Θεωρητικές προσεγγίσεις και εκπαιδευτικοί σχεδιασμοί, Εκδόσεις Κριτική, Αθήνα.
- Γ. Καμπουράκης, Ε. Λουκής, (2015), e-*λεκτρονική μάθηση*, Εκδόσεις Κλειδάριθμος, Αθήνα.
- Θ. Ορφανουδάκης, (2016), Εκπαιδευτικά μέσα και μεθοδολογίες για την μαζική κατάρτιση και ανοικτή πρόσβαση στην γνώση: Η εμπειρία των μαζικών ανοικτών διαδικτυακών μαθημάτων, Ελληνικό Ανοικτό Πανεπιστήμιο, Εργαστήριο Εκπαιδευτικού Υλικού & Εκπαιδευτικής Μεθοδολογίας.
- C.R. Clark, E.R. Mayer, (2016), *e-Learning and the Science of Instruction: Proven Guidelines for Consumers and Designers of Multimedia Learning,* 4th Edition, Wiley.
- E.R. Mayer, (2014), *The Cambridge Handbook of Multimedia Learning*, 2nd Edition, University of California, Santa Barbara.
- Α. Σοφός, Α. Κώστα, Β. Παράσχου, (2015), *Online Εξ Αποστάσεως Εκπαίδευση*, Εκδόσεις Κάλλιπος, Αθήνα.
- A. Makri, D. Vlachopoulos, (2017), *Ηλεκτρονική μάθηση: η πολυσημία και πολυπλοκότητα της έννοιας: Μία συστηματική βιβλιογραφική επισκόπηση*, European University Cyprus.
- L. Breslow, D.E. Pritchard, J. DeBoer, G.S. Stump, A.D. Ho, D.T. Seaton, (2013), *Studying learning in the worldwide classroom: Research into edX's first MOOC,* Research & Practice in Assessment, 8(2), pp. 12-26.
- C. Depover, T. arsenti, V. Komis, (2016), *Μαζικά Ανοικτά Διαδικτυακά Μαθήματα (MOOC): Φύση, προκλήσεις και προοπτικές*, Εκδόσεις Κλειδάριθμος, Αθήνα.
- S. Marshall, (2013), *Evaluating the Strategic and Leadership Challenges of MOOCs,* MERLOT Journal of Online Learning and Teaching, 9(2), pp. 24-37.

- F. Dalipi, S.Y. Yayilgan, A.S. Imran, Z. Kastrati, (2016), *Towards Understanding the MOOC Trend: Pedagogical Challenges and Business Opportunities,* In International Conference on Learning and Communication Technologies, Springer International Publishing.
- J. Daniel, (2012), *Making sense of MOOCs: Musings in a maze of myth, paradox and possibility,* Journal of Interactive Media in Education, 3(2), pp. 2-19.
- A.M. Kaplan, M. Haenlein, (2016), *Higher education and the digital revolution: About MOOCs, SPOCs, social media, and the Cookie Monster*, Business Horizons, 59(3), pp. 43-58.
- J. Daniel, E.V. Cano, M.G. Cervera, (2015), *The Future of MOOCs: Adaptive Learning or Business Model? RUSC,* Universities and Knowledge Society Journal, 12(1), pp. 65-74.
- Α.Β. Μπραϊλας, (2018), *Η μάθηση στο χρονοτόπο του διαδικτύου: κοινότητες, ψηφιακή κουλτούρα, wilipedia & MOOCs*, Εκδόσεις Γρηγόρης, Αθήνα.
- M. Khalil, M. Ebner, (2016), *Learning Analytics in MOOCs: Can Data Improve Students Retention and Learning?,* In EdMedia: World Conference on Educational Media and Technology, pp. 580-589.
- Z. Papamitsiou, A.A. Economides, (2014), *Learning Analytics and Educational Data Mining in Practice: A Systematic Literature Review of Empirical Evidence,* Educational Technology & Society, 17(4), pp. 48-65.
- Jorg Liebeherr, Magda El Zarki.(2004) Mastering Networks An Internet Lab Manual. Pearson Addison Wesley.
- L. Yuan, S. Powell, (2015), Partnership Model for Entrepreneurial Innovation in Open Online Learning, University of Bolton, Bolton.
- J. Daniel, E.V. Cano, M.G. Cervera, (2015), *The Future of MOOCs: Adaptive Learning or Business Model? RUSC,* Universities and Knowledge Society Journal, 12(1), pp. 65-74.
- A. Henmi, M. L. A. S. C. C., (2006). Firewall Policies and VPN Configurations. s.l.:Syngress Publishing.

- Δημήτρης Γκριτζαλης, Σ. Γ. Σ. Κ., (2003). Ασφάλεια Δικτύων υπολογιστών. Αθήνα: Παπασωτηριου.
- Πομπόρτσης Ανδρέας, Π. Γ., (2003). Ασφάλεια Δικτύων Υπολογιστών. Αθήνα: Τζιόλα.
- Douglas E. Comer. (2007) Δίκτυα και διαδίκτυα υπολογιστών και εφαρμογές τους στο Internet. Εκδόσεις Κλειδάριθμος.
- James F. Kurose, Keith W. Ross. (2008) Δικτύωση Υπολογιστών Προσέγγιση από Πάνω προς τα Κάτω. Εκδόσεις Μ. Γκιούρδας.
- Stajano, F., & Anderson, R. (2002). The Resurrecting Duckling: security issues for ubiquitous computing. Computer, 35(4), 22–26. http://doi.org/10.1109/MC.2002.1012427
- Weber, R. H. (2010). Internet of Things – New security and privacy challenges. Computer Law & Security Review, 26(1), 23–30. http://doi.org/10.1016/j.clsr.2009.11.008
- Convery, S. (2004). Network security architectures. Indianapolis, IN: Cisco Press.
- https://static.eudoxus.gr/books/25/chapter-5425.pdf
- http://www.efthymiadis.gr/default.aspx?lang=el-GR&page=455
- http://www.nis.gr/npimages/docs/Genika%20Metra%20Prostasias%20Cert.pdf

Πνευματικά δικαιώματα

Δηλώνω ρητά ότι, σύμφωνα με το άρθρο 8 του Ν. 1599/1988 και τα άρθρα 2,4,6 παρ. 3 του Ν. 1256/1982, η παρούσα εργασία αποτελεί αποκλειστικά προϊόν προσωπικής εργασίας και δεν προσβάλλει κάθε μορφής πνευματικά δικαιώματα τρίτων και δεν είναι προϊόν μερικής ή ολικής αντιγραφής, οι πηγές δε που χρησιμοποιήθηκαν περιορίζονται στις βιβλιογραφικές αναφορές και μόνον.

ΑΝΔΡΙΑΝΑ ΚΑΛΑΡΙΔΗ

ΑΝΙΣΑ ΛΑΜΙ

2020