Πολιτική Ασφάλειας στο Ολοκληρωμένο Σύστημα Διαχείρισης Ηλεκτρονικών Μαθημάτων «Open eClass»

Γεώργιος Παπαδημητρίου[1], Κωνσταντίνος Λαμπρινουδάκης[2]

[1]MSc Ασφάλεια Ψηφιακών Συστημάτων, Τμήμα Ψηφιακών Συστημάτων Πανεπιστημίου Πειραιώς
georpapajim@gmail.com

[2]Αναπληρωτής Καθηγητής, Τμήμα Ψηφιακών Συστημάτων Πανεπιστημίου Πειραιώς
clam@unipi.gr

Περίληψη

Στο παρόν άρθρο περιγράφεται η πολιτική ασφάλειας που πρέπει να ακολουθηθεί από κάθε εκπαιδευτικό ίδρυμα που φιλοξενεί το Ολοκληρωμένο Σύστημα Διαχείρισης Ηλεκτρονικών Μαθημάτων «Open eClass». Επιπλέον, στο άρθρο αυτό, αναφέρονται οι τύποι επιθέσεων ασφαλείας στους οποίους το πληροφοριακό σύστημα «Open eClass» είναι ευπαθή και προτείνονται τρόποι αντιμετώπισης των επιθέσεων αυτών.

Λέξεις κλειδιά: πολιτική ασφάλειας, Open eClass, επιθέσεις ασφάλειας, αντιμετώπιση επιθέσεων.

1. Εισαγωγή

Τα Συστήματα Διαχείρισης Μάθησης (ΣΔΜ) ή αλλιώς οι πλατφόρμες ηλεκτρονικής μάθησης είναι η βασική τεχνολογική υποδομή λογισμικού για τα περιβάλλοντα ηλεκτρονικής μάθησης και εξ' αποστάσεως εκπαίδευσης και δεν ένα αποθετήριο ψηφιακού υλικού, π.χ. για τις διαφάνειες των διαλέξεων και για τις περιγραφές των εργασιών.

Η αποτελεσματικότητά των ΣΔΜ εξαρτάται από τον άρτιο μαθησιακό σχεδιασμό (learning design), σύμφωνα με τον οποίο ο εκπαιδευόμενος δε θα είναι παθητικός καταναλωτής υλικού αλλά θα είναι ενεργός συμμέτοχος στη μαθησιακή διαδικασία (Ρετάλης, 2011).

Τα ΣΔΜ χρησιμοποιούνται σε όλες τις βαθμίδες εκπαίδευσης (πρωτοβάθμια, δευτεροβάθμια και τριτοβάθμια) και κατάρτισης, επειδή προσφέρουν αρκετά πλεονεκτήματα σε εκπαιδευόμενους, εκπαιδευτές και στους εκπαιδευτικούς οργανισμούς, όπως διαχείριση όλων των μαθησιακών αναγκών, άρση χωρικών και χρονικών περιορισμών.

Υπάρχουν πολλά συστήματα διαχείρισης μάθησης, τόσο εμπορικά όσο και ανοικτού κώδικα. Το «Moodle» είναι το κυρίαρχο ΣΔΜ και ακολουθεί το «Blackboard». Άλλα ευρέως γνωστά ΣΔΜ είναι τα «*Claroline*», «*SumTotal*», «*Saba*», «Desire2Learn (*D2L*)», «*Sakai*».

2. «Open eClass» - Σύστημα Διαχείρισης Ηλεκτρονικών Μαθημάτων

Η πλατφόρμα ηλεκτρονικής μάθησης «Open eClass», είναι η ελληνοποιημένη έκδοση του ΣΔΜ «Claroline» και αποτελεί την πρόταση του ακαδημαϊκού διαδικτύου GUnet, για την υποστήριξη της Υπηρεσίας Ασύγχρονης Τηλεκπαίδευσης. Αναπτύχθηκε και υποστηρίζεται ενεργά από την ομάδα ασύγχρονης τηλεκπαίδευσης του GUnet και διανέμεται ελεύθερα, ως λογισμικό ανοικτού κώδικα σύμφωνα με τη γενική δημόσια άδεια GNU General Public License.

Το λογισμικό «Open eClass» είναι ένα πλήρες και ολοκληρωμένο πρόγραμμα μαθησιακού περιεχομένου. Έχει σχεδιαστεί με προσανατολισμό την ενίσχυση της συμβατικής διδασκαλίας αξιοποιώντας την ήδη σε υψηλό βαθμό αφομοιωμένη στο χώρο της εκπαίδευσης πληροφορική τεχνολογία. Επιπλέον, κώδικα έχει την δυνατότητα περαιτέρω ανάπτυξης και προσαρμογής ανάλογα με τις απαιτήσεις του κάθε εκπαιδευτικού ιδρύματος που το φιλοξενεί, εξαιτίας του ότι είναι λογισμικό ανοικτού κώδικα.

Με δεδομένο το ότι η οργάνωση της μαθησιακής διαδικασίας, οικοδομείται πάνω στο ρόλο του εκπαιδευτικού και στις διαπροσωπικές σχέσεις εκπαιδευτικός-μαθητής, μαθητής-συμμαθητής, η χρήση του λογισμικού «Open eClass» ενισχύει την εκπαιδευτική διαδικασία, προσφέροντας στους συμμετέχοντες ένα δυναμικό περιβάλλον αλληλεπίδρασης και συνεχούς επικοινωνίας εκπαιδευτή – εκπαιδευόμενου, ενώ συγχρόνως επιτρέπει την ηλεκτρονική οργάνωση, αποθήκευση και παρουσίαση του εκπαιδευτικού υλικού, ανεξάρτητα από τους περιοριστικούς παράγοντες του χώρου και του χρόνου της κλασσικής διδασκαλίας.

Τα βασικά στοιχεία που συνθέτουν την λειτουργία του «Open eClass » είναι οι *διακριτικοί ρόλοι των χρηστών* (καθηγητής, εκπαιδευόμενος, διαχειριστής), οι *κατηγορίες των μαθημάτων* (ανοικτά μαθήματα, ανοικτά σε εγγραφή μαθήματα, κλειστά μαθήματα) και τα *στοιχεία που συνθέτουν ένα μάθημα* (ατζέντα, έγγραφα, εργασίες φοιτητών, περιοχή συζητήσεων, ομάδες χρηστών, κουβέντα, σύνδεσμοι, βίντεο, ανακοινώσεις, ασκήσεις αυτοαξιολόγησης, χώρος ανταλλαγής αρχείων, περιγραφή μαθήματος).

3. Πολιτική Ασφαλείας στο Πληροφοριακό Σύστημα «Open eClass»

Η πολιτική ασφάλειας των πληροφοριακών συστημάτων αποτελεί το βασικό εργαλείο για τη διαχείριση της ασφάλειας αυτών. Σκοπός της πολιτικής ασφάλειας είναι η αποφυγή αποκάλυψης πληροφοριών σε μη εξουσιοδοτημένους χρήστες (*εμπιστευτικότητα*), η αποφυγή μη εξουσιοδοτημένης τροποποίησης μιας πληροφορίας (*ακεραιότητα*) και η αποφυγή προσωρινής ή μόνιμης άρνησης διάθεσης της πληροφορίας σε εξουσιοδοτημένους χρήστες (*διαθεσιμότητα*).

Η πολιτική ασφάλειας διατυπώνεται σε ένα έγγραφο, το οποίο θα πρέπει να γνωρίζουν και να εφαρμόζουν υποχρεωτικά όλα τα μέλη του οργανισμού.

Ο οργανισμός με την βοήθεια της πολιτικής ασφάλειας καλείται να επιτύχει:

- Παροχή ποιοτικών υπηρεσιών του πληροφοριακού συστήματος και διασφάλιση της επιχειρησιακής του ικανότητας, στο βαθμό που αυτή εξαρτάται από την εμπιστευτικότητα, την ακεραιότητα και την διαθεσιμότητα πληροφοριών και επικοινωνιών.
- Βελτιστοποίηση της αξιοποίησης της πληροφοριακής υποδομής του.
- Συμμόρφωση με τις απαιτήσεις που απορρέουν από την Ελληνική Νομοθεσία.
- Προστασία της επένδυσης που συνεπάγεται η ανάπτυξη και λειτουργία του Π.Σ.

Η πολιτική ασφάλειας που πρέπει να ακολουθηθεί από κάθε εκπαιδευτικό ίδρυμα που φιλοξενεί το Ολοκληρωμένο Σύστημα Διαχείρισης Ηλεκτρονικών Μαθημάτων «Open eClass», πρέπει να καλύπτει τις ακόλουθες κατηγορίες απαιτήσεων ασφαλείας: *Ζητήματα Προσωπικού*, *Διαχείριση Υλικού και Λογισμικού*, *Φυσική Ασφάλεια*, *Συμμόρφωση με Νομικές Υποχρεώσεις*, *Έλεγχος Πρόσβασης στα Πληροφοριακά Συστήματα*, *Σχέδιο Συνεχής Λειτουργίας*, *Διαδικασίες Διαχείρισης της Πολιτικής Ασφάλειας*, *Οργανωτική Δομή* (Καρύδα, 2004).

3.1 Ρόλοι και Υποχρεώσεις Προσωπικού

3.1.1 Διαχειριστής Ασφάλειας

Διασφαλίζει ότι όλα τα συστήματα «ΙΤ» που χρησιμοποιούνται έχουν αξιολογηθεί δεόντως για τη συμμόρφωση με τις αρχές ασφάλειας και προστατεύονται από την πολιτική ασφάλειας.

Παρακολουθεί τη τήρηση των νόμων, για τη προστασία δεδομένων προσωπικού χαρακτήρα και διασφαλίζει τη φυσική ασφάλεια των υπολογιστών και του σχεδιασμού επιχειρησιακής συνέχειας.

Είναι υπεύθυνος για την παραλαβή όλων των αιτήσεων για την πρόσβαση των υποκειμένων στα δεδομένα τους που διατηρούνται, ελέγχει τις διαδικασίες ολοκλήρωσης αυτών των αιτήσεων, εξασφαλίζει ότι οι πληροφορίες που παρέχονται για τον εντοπισμό των δεδομένων είναι επαρκής και διασφαλίζει τη κοινοποίηση των σχετικών πληροφοριών στους αιτούντες εντός συγκεκριμένου χρονικού διαστήματος (το οποίο πρέπει να καθοριστεί).

Είναι υπεύθυνος για τη διασφάλιση ότι οι εργαζόμενοι είναι ενήμεροι για τις απαιτήσεις της προστασίας δεδομένων προσωπικού χαρακτήρα.

Διατηρεί τις εφαρμογές και τα «sites» ενημερωμένα.

3.1.2 Υπεύθυνος Ασφάλειας

Εστιάζει εντός του οργανισμού σε όλα τα θέματα ασφάλειας «ΙΤ».

Παραλαμβάνει και εξετάζει τις εκθέσεις για περιστατικά ασφάλειας «ΙΤ», προβαίνει στις κατάλληλες πράξεις και διαβιβάζει τις εκθέσεις στον υπεύθυνο «ΙΤ».

Παρέχει ενεργό ρόλο στη δημιουργία και εφαρμογή διαδικασιών που αφορούν την «ΙΤ» ασφάλεια και την ευαισθητοποίηση των εργαζομένων σε θέματα ασφάλειας.

3.1.3 Χρήστες

Υποχρεούνται να τηρούν την πολιτική ασφάλειας.

Υποχρεούνται να συμμορφώνονται με τη νομοθεσία.

Ειδοποιούν άμεσα το διαχειριστή ασφάλειας ή τον υπεύθυνο ασφάλειας αν διαπιστώσουν κάποιο περιστατικό ασφάλειας.

Ενημερώνουν άμεσα τον υπεύθυνο «ΙΤ» για οποιοδήποτε περιστατικό σχετικό με την προστασία δεδομένων προσωπικού χαρακτήρα.

3.2 Διαχείριση Υλικού και Λογισμικού

3.2.1 Έλεγχος Ιών

Κανένα αρχείο από δισκέτα, CD/DVD ή USB δεν πρέπει να μεταφερθεί σε οποιοδήποτε σύστημα αν δεν έχει ελεγχθεί από το τμήμα «ΙΤ».

Δισκέτες, CD/DVD ή USB που χρησιμοποιούνται για την αποστολή αρχείων σε εξωτερικούς χρήστες μπορούν να ελεγχθούν για ιούς πριν αποσταλθούν. Αν απαιτείται τότε το τμήμα «ΙΤ» είναι αρμόδιο για τον έλεγχο.

Όλοι οι servers και οι προσωπικοί υπολογιστές πρέπει να έχουν εγκατεστημένο «antivirus».

Όταν ανιχνευθεί ένας ιός τότε πρέπει να ενημερώνεται άμεσα το τμήμα «IT» που θα προσπαθήσει να «καθαρίσει», να επαναφέρει τον υπολογιστή και να ενημερώσει το «antivirus».

3.2.2 Προστασία Υλικού (hardware) από κλοπή

Το «server room» πρέπει να είναι κλειδωμένο συνέχεια. Η πρόσβαση σε αυτό είναι περιορισμένη και εφόσον απαιτείται πρόσβαση τότε αυτή γίνεται υπό την επίβλεψη αρμόδιου από το τμήμα «IT».

Πρέπει να διατηρείται ένα αρχείο με το «hardware» και το ποιος είναι υπεύθυνος για αυτό.

Δεν επιτρέπεται η μετακίνηση «hardware» χωρίς την έγκριση του υπεύθυνου «IT», εκτός από τους φορητούς υπολογιστές, για τους οποίους είναι υπεύθυνοι οι χρήστες τους.

Για «hardware» που βρίσκεται σε μέρος που είναι τρωτό ή περιέχει δεδομένα προσωπικού χαρακτήρα πρέπει να γίνεται χρήση μέτρων φυσικής ασφάλειας όπως κλείδωμα πορτών.

3.2.3 Προστασία Υλικού από Φθορά Λόγω Ατυχήματος

Πρέπει να γίνεται προσεκτική χρήση φαγητών και ποτών κοντά σε «hardware». Ποτά και φαγητά δεν επιτρέπονται στο «server room».

Η θέση όλου του «hardware» πρέπει να είναι σύμφωνη με τα πρότυπα υγείας και ασφάλειας συμπεριλαμβανόμενης και της σταθερότητας των γραφείων και των ελεύθερων καλωδίων.

Όλοι οι προσωπικοί υπολογιστές και εκτυπωτές πρέπει να είναι απενεργοποιημένοι όταν δεν χρησιμοποιούνται για παρατεταμένες περιόδους, όπως τη νύχτα ή τα σαββατοκύριακα, εξαιρείται ο βασικός εξοπλισμός του «server room».

Μαγνητικά μέσα δεν πρέπει να τοποθετούνται δίπλα σε εκτυπωτές λέιζερ, φωτοτυπικά μηχανήματα ή τηλέφωνα, επειδή μπορεί να προκληθεί φθορά των αποθηκευμένων δεδομένων.

Δισκέτες, CD/DVD, USB πρέπει να ταυτοποιούνται και να φυλάσσονται σε κουτιά ή γραφεία με κλειδαριά.

Δεν πρέπει να εμποδίζονται οι αεραγωγοί των υπολογιστών.

3.2.4 Προστασία των Δεδομένων από Βλάβη Υλικού (hardware)

Αντίγραφα ασφαλείας των δεδομένων και των προγραμμάτων του συστήματος, πρέπει να λαμβάνονται σε τακτική βάση, όπως καθορίζεται από τον υπεύθυνο του πληροφοριακού συστήματος.

Τα δεδομένα δεν πρέπει να κρατούνται σε τοπικό επίπεδο στους υπολογιστές, καθώς αυτό δεν περιλαμβάνεται στην αυτόματη νυχτερινή δημιουργία αντιγράφων ασφαλείας των εξυπηρετητών του δικτύου. Τα δεδομένα πρέπει να αποθηκεύονται σε φακέλους στους εξυπηρετητές του δικτύου.

Τα αντίγραφα ασφαλείας πρέπει να φυλάσσονται με ασφάλεια εκτός του χώρου του κεντρικού «server».

Οι διαδικασίες ανάκτησης των δεδομένων από τα αντίγραφα ασφαλείας πρέπει να ελέγχονται σε τακτική βάση, όπως καθορίζεται από τους υπεύθυνους συντήρησης του πληροφοριακού συστήματος.

3.2.5 Προστασία των Δεδομένων από μη Εξουσιοδοτημένη Πρόσβαση

Πρέπει να εφαρμόζονται έλεγχοι των κωδικών. Οι κωδικοί πρόσβασης πρέπει να είναι τουλάχιστον πέντε χαρακτήρες, να περιλαμβάνουν γράμματα και αριθμούς, να είναι διαφορετικοί από αυτούς που έχουν ήδη χρησιμοποιηθεί, να έχουν δημιουργηθεί από τους χρήστες.

Οι κωδικοί πρόσβασης πρέπει να αλλάζουν τουλάχιστον μία φορά κάθε σαράντα μέρες.

Οι λεπτομέρειες για τους κωδικούς πρόσβασης καταγράφονται από τους υπεύθυνους του πληροφοριακού συστήματος και διατηρούνται σε ασφαλές μέρος.

Οι αναφορές που περιέχουν ευαίσθητες πληροφορίες και οι οποίες απαιτείται να διατεθούν πρέπει μετά τη χρήση να τοποθετούνται σε ειδικούς κάδους για κατατεμαχισμό.

Τα αντίγραφα ασφαλείας και τα αντίγραφα των δεδομένων πρέπει να αποθηκεύονται με ασφάλεια εκτός του χώρου του κεντρικού «server».

Όλα τα μέσα αποθήκευσης, συμπεριλαμβανομένων των αντιγράφων ασφαλείας πρέπει να έχουν ιδιαίτερη σήμανση για να αποφευχθεί οποιαδήποτε σύγχυση ως προς το περιεχόμενό τους.

3.2.6 Έλεγχος Λογισμικού

Όλο το λογισμικό πρέπει να αγοραστεί μέσω του τμήματος «IT» και δεν πρέπει να εγκατασταθεί κανένα λογισμικό συμπεριλαμβανομένου λογισμικού χωρίς άδεια από το τμήμα «IT».

Πρέπει να διατηρείται μητρώο (register) των λογισμικών από τους υπεύθυνους «IT».

Το λογισμικό δεν επιτρέπεται να αντιγράφεται, δεδομένου ότι αυτό συνιστά παραβίαση των δικαιωμάτων πνευματικής ιδιοκτησίας και ως εκ τούτου είναι παράνομο – εκτός αν έχει ρητά επιτραπεί από την άδεια χρήσης, η οποία περιλαμβάνει την εγκα-

τάσταση του λογισμικού από ένα σετ δίσκων(CDs) επάνω σε κάποιο αριθμό υπολογιστών.

Όλοι οι δίσκοι που περιλαμβάνουν το λογισμικό του συστήματος πρέπει να φυλάσσονται με ασφάλεια στο «IT» «server room». Αυτά είναι τα μόνα αποδεικτικά στοιχεία για τη νόμιμη άδεια χρήσης του λογισμικού, και μπορεί να απαιτηθεί να παρουσιαστούν ως αποδεικτικά στοιχεία στην Αρχή Προστασίας Πνευματικών Δικαιωμάτων.

3.3 Προστασία Προσωπικών Δεδομένων

Ο οργανισμός έχει την υποχρέωση να τηρεί τις διατάξεις του νόμου 2472/1997, για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα.

Το ανθρώπινο δυναμικό έχει το δικαίωμα σεβασμού της ιδιωτικής του ζωής και συνεπώς προσδοκά ότι οι πληροφορίες που το αφορούν πρέπει να αντιμετωπίζονται ως εμπιστευτικές.

Όλοι οι εργαζόμενοι και εξωτερικοί συνεργάτες του οργανισμού έχουν έννομο καθήκον μέριμνας για την προστασία των προσωπικών πληροφοριών.

Όλα τα τμήματα/μονάδες του οργανισμού, πρέπει να έχουν μια ενεργό πολιτική για την ενημέρωση των υποκειμένων σχετικά με το είδος των δεδομένων και των σκοπών για τους οποίους αυτές οι πληροφορίες, συλλέγονται.

Διαδικασίες (αυτοματοποιημένες ή μη) για την αποθήκευση, διάθεση και χειρισμό των πληροφοριών, πρέπει να προστατεύουν την εμπιστευτικότητα. Πρέπει να ληφθεί μέριμνα για την αποφυγή της ακούσιας παραβίασης της εμπιστοσύνης.

Η παραβίαση της εμπιστευτικότητας είναι ένα σοβαρό ζήτημα που μπορεί να οδηγήσει σε πειθαρχικές κυρώσεις.

Όλες οι αιτήσεις για λήψη δεδομένων πρέπει να διαβιβάζονται στον υπεύθυνο του πληροφοριακού συστήματος ή τον υπεύθυνο για την προστασία των δεδομένων.

3.4 Προστασία από Απομακρυσμένη Πρόσβαση

3.4.1 Ασύρματη πρόσβαση

Όπου υπάρχει απομακρυσμένη πρόσβαση του δικτύου μέσω ασύρματων συνδέσεων το δίκτυο πρέπει να ρυθμιστεί ώστε να μη διαφημίζει την ύπαρξη του, η ισχύ του σημείου πρόσβασης πρέπει να οριστεί στη χαμηλότερη τιμή, που διασφαλίζεται η λειτουργία του, να χρησιμοποιείται το «WPA2» ως πρότυπο ασφάλειας της σύνδεσης.

3.4.2 Ασφαλής πρόσβαση μέσω VPN

Η πρόσβαση του δικτύου από απομακρυσμένους χρήστες πρέπει να γίνεται μόνο μέσω «IPSec VPN» ή «SSL VPN» συνδέσεις. Αυτό κρίνεται απαραίτητο για την ασφαλή σύνδεση της απομακρυσμένης συσκευής με το δίκτυο.

3.4.3 Πρόληψη από την απώλεια δεδομένων

Όλοι οι φορητοί υπολογιστές πρέπει να έχουν τις ακόλουθες ρυθμίσεις ασφάλειας για την αποφυγή της κλοπής δεδομένων.

- Όλα τα δεδομένα του οργανισμού στο φορητό υπολογιστή πρέπει να είναι κρυπτογραφημένα χρησιμοποιώντας το κατάλληλο λογισμικό κρυπτογράφησης.
- Θα επιτρέπεται απομακρυσμένη πρόσβαση σε εμπιστευτικά έγγραφα του οργανισμού, όχι όμως η λήψη αυτών.

3.4.4 Προστασία απομακρυσμένων συσκευών

Για την αποφυγή κινδύνων του δικτύου του οργανισμού πρέπει να εγκατασταθεί λογισμικό ασφαλείας στις συσκευές.

- Λογισμικό «firewall» πρέπει να εγκατασταθεί στις συσκευές για αποφυγή κινδύνων «trojans» και «back door».
- Το λογισμικό «antivirus» πρέπει να ρυθμιστεί έτσι ώστε να πραγματοποιείται αυτόματη λήψη ενημερώσεων.

3.4.5 Αυθενπκοποίηση

Η αυθεντικοποίηση των απομακρυσμένων συσκευών που συνδέονται στο δίκτυο, πρέπει να γίνει με τη χρήση ψηφιακών πιστοποιητικών.

3.5 Σχέδιο Συνέχισης Λειτουργίας

Η πολιτική ασφάλειας πρέπει να περιλαμβάνει οδηγίες που αφορούν τις απαιτούμενες ενέργειες μετά την πραγματοποίηση ενός σημαντικού περιστατικού παραβίασης της ασφάλειας, ώστε οι λειτουργίες του οργανισμού να εξακολουθήσουν να πραγματοποιούνται με κάποιους εναλλακτικούς τρόπους, έως ότου αντιμετωπιστεί το πρόβλημα ασφάλειας του πληροφοριακού συστήματος. Για παράδειγμα πρέπει να υπάρχει εφεδρικός «Web Server».

3.6 Διαδικασίες Διαχείρισης της Πολιτική Ασφάλειας

Ένα σημαντικό κομμάτι της πολιτικής ασφάλειας περιγράφει και προσδιορίζει τις λοιπές δραστηριότητες που πρέπει να συνοδεύουν την εφαρμογή της, ώστε να είναι

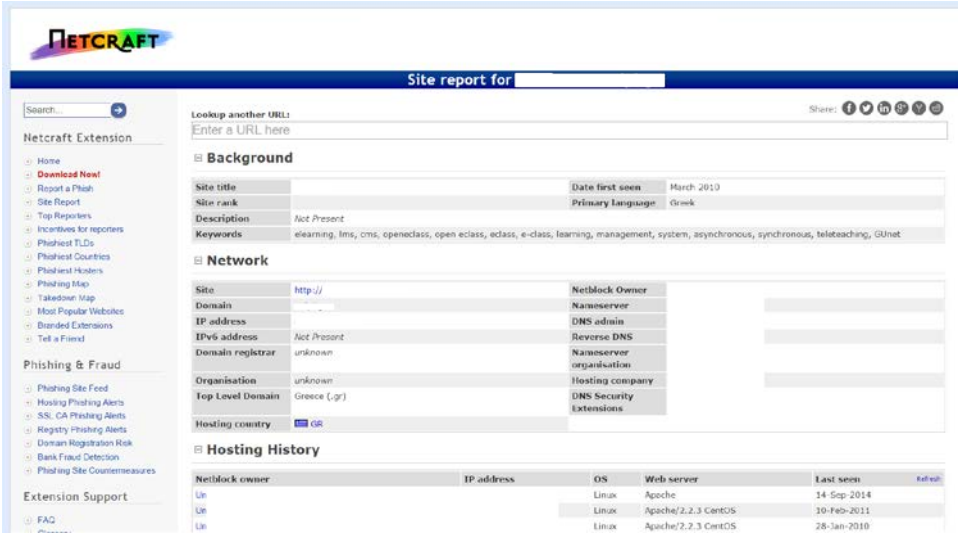
αποτελεσματική η διαχείριση της ασφάλειας του πληροφοριακού συστήματος. Αυτές οι διαδικασίες περιλαμβάνουν:

- *Την αξιολόγηση και αναθεώρηση της πολιτικής*. Η πολιτική ασφάλεια πρέπει να αξιολογείται και να αναθεωρείται, τόσο ως προς το περιεχόμενο όσο και ως προς τις διαδικασίες εφαρμογής της.
- *Τον έλεγχο και τη συμμόρφωση με την πολιτική ασφάλειας*. Στην πολιτική ασφάλειας πρέπει να καθορίζονται οι διαδικασίες με τις οποίες ελέγχεται (auditing) η εφαρμογή της πολιτικής από τους χρήστες του πληροφοριακού συστήματος, καθώς και οι διαδικασίες για το χειρισμό των περιστατικών μη συμμόρφωσης με αυτή.

4. Ανίχνευση Ευπαθειών στο Πληροφοριακό Σύστημα «Open eClass»

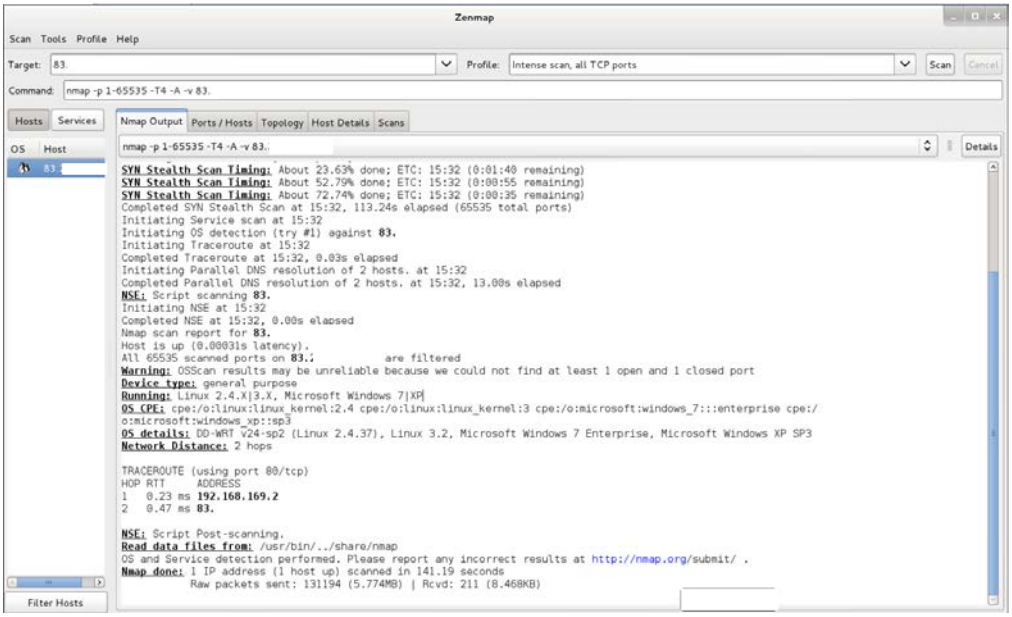
Η ανίχνευση ευπαθειών σε ένα πληροφοριακό σύστημα αποτελεί ένα ισχυρό και αποτελεσματικό εργαλείο εναντίον όλων όσων θέλουν να το βλάψουν.

Για την ανίχνευση ευπαθειών στο πληροφοριακό σύστημα «Open eClass» που φιλοξενείται από το εκάστοτε εκπαιδευτικό ίδρυμα, στην αρχή ο «pentester» συλλέγει όσες δημόσια διαθέσιμες πληροφορίες είναι δυνατόν να εντοπιστούν σχετικά με το στόχο, μέσω της ιστοσελίδας «netcraft.com». Στην εικόνα 1 παρουσιάζονται τα αποτελέσματα αναζήτησης πληροφοριών από το «netcraft.com» για το στόχο.



Εικόνα 1. *«netcraft»*

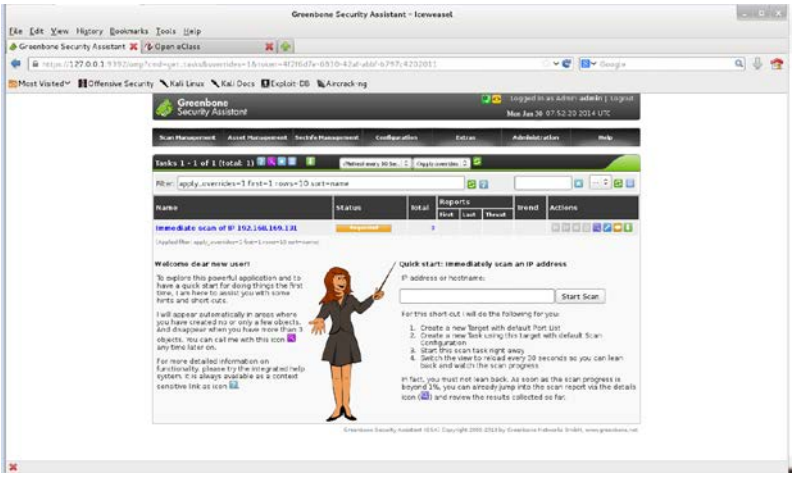
Στην συνέχεια, ο «pentester» για να βρει περισσότερες πληροφορίες για το λειτουργικό σύστημα χρησιμοποιεί την εφαρμογή «Zenmap» (εικόνα 2).



Εικόνα 2. *«Zenmap»*

Κατόπιν, για λόγους εκπαιδευτικούς και ασφαλείας η ανίχνευση ευπαθειών συνεχίζεται σε εικονικό περιβάλλον. Ο «pentester» εγκαθιστά τα λειτουργικά συστήματα «Kali Linux» και «CentOS 6.5» στο προηγμένο λογισμικό εικονικής μηχανής «VMware Workstation», σε περιβάλλον Windows. Επίσης, εγκαθιστά την εφαρμογή «OpenVAS» στο λειτουργικό σύστημα «Kali Linux» καθώς και τα λογισμικά MySQL 5.5.x, Apache HTTP Server 2.2.x, PHP 5.5.x και phpMyAdmin 4.2.x στο λειτουργικό σύστημα «CentOS 6.5». Τέλος, εγκαθιστά το λογισμικό «Open eClass 2.10», στο λειτουργικό σύστημα «CentOS 6.5».

Αμέσως μετά, ο «pentester» σαρώνει το στόχο (Open eClass) με την εφαρμογή «OpenVAS» (εικόνα 3).



Εικόνα 3. *Σάρωση του Λογισμικού «Open eClass» με την Εφαρμογή «OpenVAS»*

Μετά την σάρωση, εντοπίζονται ευπάθειες υψηλής, μέσης και χαμηλής επικινδυνότητας. Οι ευπάθειες, μέσης και χαμηλής επικινδυνότητας δεν παρουσιάζουν ιδιαίτερο ενδιαφέρον. Σαν υψηλού κινδύνου τρωτότητα το «OpenVAS» αναφέρει την πιθανότητα ευπάθειας σε επιθέσεις «*http TRACE XSS attack*». Πιο συγκεκριμένα το «OpenVAS» αναφέρει ότι, ο απομακρυσμένος «server» υποστηρίζει τις μεθόδους «TRACE» ή/και «TRACK».

Οι «servers» που υποστηρίζουν αυτές τις μεθόδους, υφίστανται «cross-site-scripting» (XSS) επιθέσεις όταν συνδυάζονται και με άλλες αδυναμίες των φυλλομετρητών. Οι επιθέσεις αυτές ονομάζονται «cross-site-tracing» (XST) επιθέσεις. Στις «XST» επιθέσεις, ο εισβολέας εκμεταλλεύεται το γεγονός ότι ο απομακρυσμένος «server» υποστηρίζει τις μεθόδους «TRACE» ή/και «TRACK», έτσι ώστε να ξεγελάσει τους νόμιμους χρήστες, με σκοπό αυτοί να του δώσουν τα διαπιστευτήριά τους.

Η λύση που προτείνεται είναι να απενεργοποιηθούν οι παραπάνω μέθοδοι με την προσθήκη των ακόλουθων γραμμών σε κάθε «virtual host» στο αρχείο διαμόρφωσης:

```
RewriteEngine on
RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
RewriteRule .* - [F]
```

5. Συμπεράσματα

Η συνεισφορά του άρθρου έγκειται στο να αναδείξει την σπουδαιότητα της πολιτικής ασφάλειας καθώς και την έγκαιρη ανίχνευση ευπαθειών σε ένα πληροφοριακό σύστημα.

Η πολιτική ασφάλειας σε ένα πληροφοριακό σύστημα αποτελεί το βασικό εργαλείο για τη διαχείριση της ασφάλειας του. Στην πολιτική ασφάλειας καθορίζονται οι στόχοι της ασφάλειας καθώς και ο τρόπος με τον οποίο οι στόχοι αυτοί θα υλοποιηθούν. Βασικό συστατικό στοιχείο κάθε πολιτικής ασφάλειας πληροφοριακού συστήματος είναι η περιγραφή των κανόνων και των διαδικασιών που πρέπει να ακολουθούνται για την προστασία των πληροφοριακών συστημάτων, καθώς και ο καθορισμός των συγκεκριμένων ρόλων και αρμοδιοτήτων που απαιτούνται για την υλοποίηση της πολιτικής ασφάλειας. Η εφαρμογή μιας πολιτικής ασφάλειας σε έναν οργανισμό έχει δεσμευτικό χαρακτήρα για όλα τα μέλη του οργανισμού.

Επίσης, η ανίχνευση ευπαθειών σε ένα πληροφοριακό σύστημα αποτελεί ένα ισχυρό και αποτελεσματικό εργαλείο εναντίον όλων όσων θέλουν να το βλάψουν. Η προστασία του υπό εξέταση πληροφοριακού συστήματος και η διασφάλιση των βασικών αρχών ασφάλειας του εκάστοτε οργανισμού, ο οποίος κατέχει το εν λόγω σύστημα προκύπτει με την μέθοδο «Penetration Testing».

Αναφορές

Καρύδα, Μ. (2004). Πολιτικές Ασφάλειας Πληροφοριακών Συστημάτων. Στο Σ. Κάτσικα, Δ. Γκρίτζαλη & Σ. Γκρίτζαλη (Επιμ.), *Ασφάλεια Πληροφοριακών Συστημάτων* (σελ. 377-406). Αθήνα: Εκδόσεις Νέων Τεχνολογιών.

Ρετάλης, Σ. (2011). *Πλατφόρμες ηλεκτρονικής μάθησης – Συστήματα Διαχείρισης Μάθησης*. Ανακτήθηκε 26 Απριλίου 2011, από http://reviews.in.gr/greece/elearning/article/?aid=1231105224

Abstract

This article describes the security policy to be followed by every educational institution that hosts the Integrated Course Management System "Open eClass". Furthermore, in this article, the types of the security attacks, in which the information system "Open eClass" is vulnerable, are presented and ways to encounter such attacks are also suggested.

Keywords: security policy, Open eClass, security attacks, ways to encounter security attacks.