1^0 Εργαστήριο: Σχεδιασμός Πολιτικής ασφάλειας

Σκοπός: Σκοπός του εργαστηρίου είναι η εξοικείωση των φοιτητών με το σχεδιασμό και υλοποίηση Πολιτικών ασφάλειας Παρόχων Δικτυακών Υπηρεσιών στα πλαίσια ενός ολοκληρωμένου σχεδίου ασφάλειας. Θα γίνει εφαρμογή μέσω μελέτης περίπτωσης για το τμήμα Υποστήριξης πληροφορικής του τμήματός μας.

Μέθοδος: Οι φοιτητές αρχικά θα μελετήσουν τα βασικά χαρακτηριστικά ενός σχεδίου ασφάλειας και ιδιαίτερα αυτά της πολιτική ασφάλειας.

Ένα **σχέδιο ασφάλειας** αποτελεί ένα έγγραφο το οποίο απαρτίζεται κυρίως από την πολιτική ασφάλειας, την περιγραφή της υφιστάμενης κατάστασης της υποδομής από τη σκοπιά της ασφάλειας, τις απαιτήσεις ασφάλειας, το πλάνο υλοποίησης και την περιγραφή των διαδικασιών συνεχούς επισκόπησης και αναθεώρησης του σχεδίου ασφάλειας.
Η **πολιτική ασφάλειας** είναι ένα σύνολο κανόνων, οι οποίοι προσδιορίζουν επακριβώς το ρόλο κάθε εμπλεκόμενου μέσα σε μία εταιρία ή έναν οργανισμό, τις αρμοδιότητες, τις ευθύνες και τα καθήκοντά του.

Μια πολιτική ασφαλείας πρέπει να περιλαμβάνει τα ακόλουθα στοιχεία:

- *Αγαθά (Assets):* πρόκειται για τις οντότητες (πχ υλικό, λογισμικό, πληροφορίες, θέσεις κλειδιά του οργανισμού κλπ) του πληροφοριακού συστήματος που έχουν αξία και πρέπει να προστατευθούν
- *Ρόλους και αρμοδιότητες (Roles and Responsibilities):* πρόκειται για τους ρόλους και τις υπευθυνότητες, αρμοδιότητες, καθήκοντα, ευθύνες του κάθε ρόλου για θέματα που αφορούν το πληροφοριακό σύστημα και την ασφάλειά του
- *Στόχους (Security policy objectives*): πρόκειται για το στόχο (ή τους στόχους) ασφαλείας που καθορίζει συνοπτικά την εστίαση της πολιτικής και θέτει περιορισμούς
- *Πεδίο εφαρμογής της πολιτικής ασφαλείας (Scope of Security Policy):* πρόκειται για την εμβέλεια, την έκταση και το χώρο που αφορά η πολιτική ασφαλείας
- *Οδηγίες, κατευθυντήριες γραμμές (Guidelines):*
- *Κουλτούρα, άλλες πολιτικές, νομοθεσία (Culture, legislation, other policies):* πρόκειται για το σύνολο των πεποιθήσεων, αξιών, αρχών, πολιτικών, κωδίκων δεοντολογίας, νόμων που συνθέτουν την κουλτούρα του οργανισμού και του περιβάλλοντος αυτού και ανατροφοδοτούν τους μηχανισμούς του μέσω μιας διαδικασίας συνεχούς εκμάθησης
- *Υλοποίηση και εφαρμογή της πολιτικής ασφαλείας - Ενημέρωση και συμμόρφωση (Implementation and application of the security policy – Awareness, enforcement, breach)*: πρόκειται για το οργανωτικό πλαίσιο ρόλων, αρμοδιοτήτων, κανονισμών, επιτροπών για την υλοποίηση και εφαρμογή της πολιτικής ασφαλείας, για την ενημέρωση του προσωπικού σχετικά με την συμμόρφωση και τις ενέργειες που λαμβάνονται στην περίπτωση παραβίασής της πολιτικής ασφαλείας
- *Επισκόπηση και αναθεώρηση της πολιτικής (Review and audit)*: πρόκειται για την τακτική επισκόπηση και αναθεώρηση της πολιτικής σύμφωνα με τις εκάστοτε συνθήκες ώστε να είναι επίκαιρη και να καλύπτει το σύνολο των δομικών στοιχείων του πληροφοριακού συστήματος και των διαδικασιών διαχείρισης

Τα βασικά χαρακτηριστικά της πολιτικής ασφαλείας πρέπει να είναι τα παρακάτω:

- Απαιτεί *συμμόρφωση από το προσωπικό του οργανισμού*. Το έγγραφο της πολιτικής θα πρέπει να είναι στη διάθεση όλου του προσωπικού
- Εκφράζει *γενικότερες απόψεις ή αρχές* του οργανισμού
- Είναι *σαφής* ώστε να μην παρουσιάζονται δυσκολίες στην κατανόηση και εφαρμογή της και *εφαρμόσιμη* από άποψη κόστους
- Είναι *γενικεύσιμη* ώστε η εφαρμογή της να είναι επεκτάσιμη σε μελλοντικά συστήματα που ενδεχομένως ενταχθούν στο πληροφοριακό σύστημα του οργανισμού
- Είναι *απαλλαγμένη από μη απαραίτητους τεχνικούς όρους και εξειδικευμένες αναφορές* ώστε να μην καθίσταται δύσκολη στην εφαρμογή της και εξαρτημένη από τεχνολογικές επιλογές καθώς και να μην τροποποιείται συχνά, παρά μόνο όταν συμβαίνουν σημαντικές αλλαγές στα εξής :
  - Στην οργανωτική δομή και στην κουλτούρα του οργανισμού
  - Στις απαιτήσεις ασφαλείας
  - Στις τεχνολογικές εξελίξεις

Παράδειγμα: Ενδεικτικά παραδείγματα υλοποίησης πολιτικής ασφάλειας σε εκπαιδευτικά ιδρύματα είναι:
- Lancaster University Electronic Information Systems Security Policy http://www.lancs.ac.uk/homepage/webmenus/e-security
- Murdoch University – Office of Information Technology Services – IT Security Policy http://wwwits2.murdoch.edu.au/security/policy.html
- NIST Special Publication 800-XX INTERNET SECURITY POLICY: A TECHNICAL GUIDE http://csrc.nist.gov/publications/PubsSPs.html

Παραδοτέο:

Θεωρείστε το Πληροφοριακό σύστημα της γραμματείας, το οποίο παρέχει υπηρεσίες στους φοιτητές και το προσωπικό του τμήματος και του ιδρύματος συνολικά. Ακολουθώντας την προσέγγιση που περιγράφθηκε γράψτε μια κατάλληλη πολιτική ασφάλειας για το Πληροφοριακό σύστημα αυτό ως μέρος ενός ολοκληρωμένου σχεδίου ασφάλειας.

Θα πρέπει να λάβετε υπόψη τις γενικότερες αρχές του ιδρύματος καθώς και το πλαίσιο που επιβάλετε μέσα από τον κανονισμό περί διασφάλισης απορρήτου στις Δικτυακές επικοινωνίες και υπηρεσίες.

Η επεξεργασία των απαντήσεων μπορεί να γίνει σε ομάδες των δύο ατόμων. Η κάθε ομάδα θα παραδώσει την εργασία της ηλεκτρονικά έως την Επόμενη εβδομάδα.