ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ
ΤΜΗΜΑ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ
ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΩΝ ΚΑΙ ΣΥΣΤΗΜΑΤΩΝ

ΕΡΓΑΣΙΑ #4

ΘΕΜΑ: Ανάλυση και διαχείριση επικινδυνότητας πληροφοριακών συστημάτων

Α. Περιγραφή του υπό μελέτη συστήματος

Τα συστήματα πληροφορικής και επικοινωνιών της εταιρείας παροχής υπηρεσιών και προϊόντων ΤΠΕ «ACME», βασίζονται κατά κύριο λόγο στην υιοθέτηση νέων προτύπων και τεχνολογιών του Διαδικτύου και περιλαμβάνουν: 96 προσωπικούς υπολογιστές (clients) με λειτουργικό σύστημα Microsoft Windows 10, 19 εκτυπωτές προσωπικής χρήσης, 9 εκτυπωτές δικτύου, που είναι τοποθετημένοι σε διάφορα γραφεία, καθώς και 8 εξυπηρετητές (servers) με λειτουργικό σύστημα Microsoft Windows Server 2016, που είναι τοποθετημένοι σε ειδικό χώρο (computer room) με πυροπροστασία, κλιματισμό, ειδικές κλειδαριές, κλπ.

Συγκεκριμένα, υπάρχουν 2 εξυπηρετητές εφαρμογών και βάσεων δεδομένων για εσωτερική χρήση μόνο, 1 εξυπηρετητής εφαρμογών και βάσεων δεδομένων για εξωτερική χρήση μόνο, 1 εξυπηρετητής WWW, 1 εξυπηρετητής Email, 2 εξυπηρετητές αρχειοθέτησης (file servers) και 1 εξυπηρετητής για παραγωγή αντιγράφων ασφαλείας (backup). Οι εφαρμογές Qastro06, DeepBl και Oasis10 έχουν αναπτυχθεί από εξωτερικούς προμηθευτές και αφορούν την παροχή υπηρεσιών: Web-mail, ERP και CAD, αντίστοιχα. Οι ειδικές εφαρμογές Onotes, Ocalc5, Opays έχουν αναπτυχθεί από το ερευνητικό τμήμα της εταιρείας και αφορούν την παροχή υπηρεσιών: σημειώσεων, υπολογισμών και ισοτιμιών, αντίστοιχα. Οι εξυπηρετητές και ο κεντρικός δικτυακός εξοπλισμός βρίσκονται σε κατάλληλα διαμορφωμένο χώρο με προστασία από κλοπή, υγρασία, διακοπή ρεύματος κλπ.

Η δικτύωση των συστημάτων περιλαμβάνει ένα τοπικό δίκτυο (LAN) στα κεντρικά γραφεία της «ACME», όπου ο κορμός είναι υλοποιημένος με οπτικές ίνες. Υπάρχει σύνδεση με το Internet για υπηρεσίες WWW και Email. Επιπλέον, λειτουργεί ένα εσωτερικό δίκτυο επικοινωνίας (intranet) που μέσω υπηρεσιών VPN, οι οποίες παρέχονται από την εταιρεία τηλεπικοινωνιών STIX, διασυνδέεται με τα τοπικά δίκτυα των περιφερειακών γραφείων της «ACME» σε 3 διαφορετικά σημεία της χώρας. Για την προστασία του εσωτερικού δικτύου χρησιμοποιούνται διατάξεις firewall και intrusion detection, ενώ χρησιμοποιείται λογισμικό

προστασίας από κακόβουλο λογισμικό (antivirus) του οποίου η αναβάθμιση γίνεται χειροκίνητα από τον υπεύθυνο ασφαλείας κάθε βδομάδα.

Οι υπάλληλοι (29 επιστημονικό προσωπικό και 11 διοικητικό προσωπικό) και οι εξωτερικοί συνεργάτες μπορούν να συνδέονται από απόσταση (όντας εκτός των εγκαταστάσεων της εταιρείας) με τις εφαρμογές για εξωτερική χρήση μόνο. Για την αυθεντικοποίηση των χρηστών χρησιμοποιούνται ζεύγη αναγνωριστικών - συνθηματικών (username – passwords) που καθορίζονται από το διαχειριστή συστήματος και διανέμονται από το βοηθό του. Οι κωδικοί των passwords αλλάζουν για κάθε χρήστη ανά χρόνο και η αποστολή των νέων γίνεται μέσω ηλεκτρονικού ταχυδρομείου. Για την εξουσιοδότηση των χρηστών χρησιμοποιείται η προσέγγιση RBAC, όπως τη διαχειρίζεται ο υπεύθυνος ασφάλειας συστήματος, αλλά δεν έχουν καταγραφεί συγκεκριμένες πολιτικές ασφάλειας και ελέγχου πρόσβασης, ειδικότερα. Επιπλέον, εκπαίδευση γίνεται ανά 2 χρόνια μόνο στο διοικητικό προσωπικό της επιχείρησης σε θέματα ασφάλειας ΠΣ, ενώ περιοδικοί έλεγχοι (audits) για την ασφάλεια και λειτουργικότητα του υπό μελέτη συστήματος γίνονται ανά 3 χρόνια μόνο από εξωτερικό ελεγκτή. Τέλος, δεν υπάρχει επίσημη διαδικασία διοίκησης επικινδυνότητας ενώ αξιολόγηση και ανάλυση επικινδυνότητας γίνεται εφόσον προκληθεί ζημιά που προέρχεται από τη χρήση του πληροφοριακού συστήματος.

Β. Ζητούμενα

ΕΡΩΤΗΜΑ 1 – Διαχείριση κινδύνων [40]

Κατεβάστε και εγκαταστήστε στον Η/Υ σας το εργαλείο Microsoft Security Assessment Tool (MSAT 4.0) που έχει αναπτυχθεί από την Microsoft (http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=12273) με σκοπό την αξιολόγηση επικινδυνότητας πληροφοριακών συστημάτων. Χρησιμοποιώντας το MSAT καλείστε να αξιολογήσετε την ασφάλεια του υπό μελέτη πληροφοριακού συστήματος. Είναι προφανές ότι οι απαντήσεις (για ένα μεγάλο μέρος των ερωτήσεων της έρευνας) δεν προκύπτουν πάντα από την παραπάνω περιγραφή του συστήματος, οπότε θα πρέπει να προβείτε σε δικές σας παραδοχές που είτε εξειδικεύουν, είτε συμπληρώνουν την παραπάνω περιγραφή του υπό μελέτη συστήματος.

Για την απάντησή σας στο ερώτημα καλείστε να:

i. αποστείλετε το XML αρχείο που παράγεται από την αποθήκευση της αξιολόγησης (σύνδεσμος: Save Your Project) εφόσον έχετε ολοκληρώσει την

καταχώρηση των απαντήσεών σας σε όλες τις ερωτήσεις.

ii. σχολιάσετε συνοπτικά την αναφορά (report) που παράγεται από το εργαλείο MSAT, στη βάση των εννοιών της διαχείρισης κινδύνων, προσπαθώντας να εντοπίσετε ομοιότητες και διαφορές μεταξύ της διαδικασίας αξιολόγησης που υποστηρίζεται από το συγκεκριμένο εργαλείο και της διαχείρισης κινδύνων.

ΕΡΩΤΗΜΑ 2 – Προσδιορισμός απαιτήσεων ασφάλειας [20]

Ως αποτέλεσμα της μελέτης της αναφοράς (report) που παράγει το εργαλείο MSAT και με βάση τις συστάσεις (recommendations) που παρέχει για κάθε απάντηση που δώσατε, καλείστε να προχωρήσετε σε εντοπισμό των προτεινόμενων μέτρων προστασίας που αφορούν ζητήματα αυθεντικοποίησης χρηστών με χρήση συνθηματικών (password). Στη βάση αυτών, θα πρέπει να προσδιορίσετε τουλάχιστον 10 απαιτήσεις ασφάλειας για αυθεντικοποίηση χρηστών με χρήση συνθηματικών, ενώ μπορείτε να εμπλουτίσετε τις απαιτήσεις ασφάλειας στη βάση νέων παραδοχών σας.

ΕΡΩΤΗΜΑ 3 – Διαμόρφωση πολιτικής ασφάλειας [20]

Με βάση τις παραπάνω απαιτήσεις ασφάλειας αυθεντικοποίησης, καλείστε να συντάξετε την πολιτική ασφάλειας αυθεντικοποίησης. Ως οδηγό, μπορείτε να χρησιμοποιήσετε, μεταξύ άλλων, π.χ. το πρότυπο (template) Password Protection Policy του οργανισμού SANS (http://www.sans.org/resources/policies/Password_Policy.pdf).

ΕΡΩΤΗΜΑ 4 – Υλοποίηση πολιτικής ασφάλειας [20]

Για την υλοποίηση της πολιτικής ασφάλειας στο λειτουργικό σύστημα Windows 7 καλείστε να αξιοποιήσετε τους σχετικούς μηχανισμούς διαχείρισης που παρέχονται από το λειτουργικό σύστημα με συνδυασμό [προτύπων ασφαλείας][security templates][1] και [ρύθμισης παραμέτρων ασφάλειας][security configuration].

ΟΔΗΓΙΕΣ: Ανοίξτε μια νέα κονσόλα διαχείρισης ([Start → Run → MMC] [Έναρξη → Εκτέλεση → MMC]) και εγκαταστήστε τα εξής [snap-ins][συμπληρωματικά προγράμματα] (καρτέλα [Standalone → Add][Μεμονωμένο → Προσθήκη]): [Security Configuration and Analysis][Ρύθμιση παραμέτρων και ανάλυση ασφάλειας] και [Security Templates][Πρότυπα ασφάλειας] ([File → Add/Remove Snap-in] [Αρχείο → Προσθαφαίρεση συμπληρωματικών προγραμμάτων]). Κατόπιν, δημιουργείστε ένα άδειο security template (με δεξί κλικ στο Security Templates επιλέγετε νέο μονοπάτι ή/και με δεξί κλικ σε ένα υπάρχον μονοπάτι επιλέγετε “New template”) με όνομα DEIGMA1 (επέκταση .inf) και διαμορφώστε κατάλληλα

[1] στο εξής χρησιμοποιείται ο συμβολισμός [ελληνικά][english] για την παράθεση των ελληνικών και των αντίστοιχων αγγλικών εκφράσεων/όρων.

τις τιμές των κλειδιών πολιτικής (π.χ. password policy, αλλά πιθανώς όχι μόνον). Κάντε δεξί κλικ στο snap-in Security Configuration and Analysis και επιλέξτε “Open database”. Στο παράθυρο διαλόγου που θα ανοίξει, δώστε ως όνομα (της νέας database): DEIGMA (επέκταση .sdb) και στο επόμενο παράθυρο παράθυρο που θα εμφανιστεί (Import template) επιλέξτε DEIGMA1 (επέκταση .inf). Κάντε πάλι δεξί κλικ στο snap-in Security Configuration and Analysis και επιλέξτε “Analyze computer now…” για να δείτε τις διαφορές μεταξύ των τρεχουσών ρυθμίσεων του υπολογιστή σας και των ρυθμίσεων ασφάλειας που έχετε εισάγει πριν.

Στην απάντησή σας θα χρησιμοποιήσετε κείμενο, καθώς και εικόνες κατάστασης της οθόνης του υπολογιστή σας, όποτε χρειάζεται.

Καλή επιτυχία!

ΟΔΗΓΙΕΣ ΥΠΟΒΟΛΗΣ:

1. Δημιουργία αρχείου συμπίεσης με όνομα ‘ISS20_P4_***AM***.ZIP’, όπου ***AM*** είναι ο αριθμός μητρώου του φοιτητή, στο οποίο θα συμπεριληφθούν:
   Α) το κείμενο της εργασίας σε μορφή Rich Text Format και με όνομα ‘ISS20_P4_***AM***.rtf’, όπου θα συμπεριλάβετε τα στοιχεία σας και τις απαντήσεις στα ερωτήματα της εργασίας.
   Β) το αρχείο XML που παράγεται από το εργαλείο MSAT
2. Το αρχείο θα αναρτηθεί στον ιστότοπο του μαθήματος και συγκεκριμένα στο σύνδεσμο «Εργασίες Φοιτητών» με Τίτλο Εργασίας το παραπάνω όνομα (π.χ. ‘ISS20_P4_2199’).