Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο

ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ
επένδυση στην κοινωνία της γνώσης
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ ΚΑΙ ΘΡΗΣΚΕΥΜΑΤΩΝ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ

ΕΣΠΑ 2007-2013
πρόγραμμα για την ανάπτυξη
ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΩΝΙΚΟ ΤΑΜΕΙΟ

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ

ΑΝΩΤΑΤΗ **Σ**ΧΟΛΗ
ΠΑΙΔΑΓΩΓΙΚΗΣ ΚΑΙ
ΤΕΧΝΟΛΟΓΙΚΗΣ
ΕΚΠΑΙΔΕΥΣΗΣ

____ Α.Σ.ΠΑΙ.Τ.Ε. _____

ΕΔΡΑ: ΑΜΑΡΟΥΣΙΟ (ΣΤΑΘΜΟΣ «ΕΙΡΗΝΗ» ΗΣΑΠ)
ΤΑΧ.Δ/ΝΣΗ: ΗΡΑΚΛΕΙΟ ΑΤΤΙΚΗΣ Τ.Κ. 141 21

«ΔΟΜΗ ΑΠΑΣΧΟΛΗΣΗΣ & ΣΤΑΔΙΟΔΡΟΜΙΑΣ ΑΝΩΤΑΤΗΣ ΣΧΟΛΗΣ ΠΑΙΔΑΓΩΓΙΚΗΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΚΗΣ ΕΚΠΑΙΔΕΥΣΗΣ (Α.Σ.ΠΑΙ.Τ.Ε.)»

ΔΡΑΣΗ 5: ΑΣΦΑΛΕΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΔΑΣΤΑ – ΑΝΑΠΤΥΞΗ ΚΩΔΙΚΑ ΔΕΟΝΤΟΛΟΓΙΑΣ ΤΩΝ ΔΟΜΩΝ

ΥΠΟΔΡΑΣΗ 5.1: ΑΣΦΑΛΕΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΔΑΣΤΑ

στο πλαίσιο του υποέργου

«ΔΟΜΗ ΑΠΑΣΧΟΛΗΣΗΣ & ΣΤΑΔΙΟΔΡΟΜΙΑΣ ΑΝΩΤΑΤΗΣ ΣΧΟΛΗΣ ΠΑΙΔΑΓΩΓΙΚΗΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΚΗΣ ΕΚΠΑΙΔΕΥΣΗΣ (Α.Σ.ΠΑΙ.Τ.Ε.)»

που υλοποιείται στο πλαίσιο του Επιχειρησιακού Προγράμματος «Εκπαίδευση και Δια Βίου Μάθηση» και συγχρηματοδοτείται από την Ευρωπαϊκή Ένωση (Ευρωπαϊκό Κοινωνικό Ταμείο) και από Εθνικούς Πόρους

ΝΟΕΜΒΡΙΟΣ 2013

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

«ΔΟΜΗ ΑΠΑΣΧΟΛΗΣΗΣ & ΣΤΑΔΙΟΔΡΟΜΙΑΣ ΑΝΩΤΑΤΗΣ ΣΧΟΛΗΣ ΠΑΙΔΑΓΩΓΙΚΗΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΚΗΣ ΕΚΠΑΙΔΕΥΣΗΣ (Α.Σ.ΠΑΙ.Τ.Ε.)»

Επιχειρησιακό Πρόγραμμα: «Εκπαίδευση και Διά Βίου Μάθηση»

Δράση 5: «Ασφάλεια προσωπικών δεδομένων ΔΑΣΤΑ – Ανάπτυξη κώδικα δεοντολογίας των δομών»

Υποδράση 5.1 «Ασφάλεια προσωπικών δεδομένων ΔΑΣΤΑ»

Μελέτη Ασφάλειας Πληροφοριών

ΙΩΑΝΝΑ ΚΑΝΤΖΑΒΕΛΟΥ, PH.D, M.SC

ΚΑΘ. ΕΦΑΡΜΟΓΩΝ ΤΕΙ ΑΘΗΝΑΣ

Νοέμβριος 2013

Περιεχόμενα

Εισαγωγή

Η μελέτη αυτή εκπονήθηκε στα πλαίσια της Υποδράσης 5.1 «Ασφάλεια προσωπικών δεδομένων ΔΑΣΤΑ» της Δράσης 5: «Ασφάλεια προσωπικών δεδομένων ΔΑΣΤΑ – Ανάπτυξη κώδικα δεοντολογίας των δομών».

Στόχος της μελέτης είναι η ολοκληρωμένη κάλυψη της Ασφάλειας Προσωπικών Δεδομένων ΔΑΣΤΑ όπως περιγράφεται κατά ISO 27000 από τις εξής φάσεις:

- **Δράση 1.** Καθορισμός Πολιτικής Ασφάλειας Πληροφοριών.
- **Δράση 2.** Καθορισμός των στόχων του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών.
- **Δράση 3.** Διενέργεια Ανάλυσης Κινδύνου για το προτεινόμενο Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών.
- **Δράση 4.** Καθορισμός του τρόπου αντιμετώπισης των Κινδύνων που εντοπίστηκαν.
- **Δράση 5.** Επιλογή των απαραίτητων ελέγχων και βελτιώσεων.

Η δομή της μελέτης περιλαμβάνει 5 κεφάλαια, ένα για καθεμιά από τις παραπάνω δράσεις, όπως περιγράφονται στη συνέχεια.

1. Καθορισμός Πολιτικής Ασφάλειας Πληροφοριών

Στόχος της πολιτικής ασφάλειας πληροφοριών κατά ISO/IEC 17799 είναι η παροχή κατεύθυνσης και υποστήριξης της διαχείρισης για την ασφάλεια πληροφοριών, σύμφωνα με τις απαιτήσεις του φορέα και των σχετικών νόμων και κανονισμών [1].

Επειδή το πληροφοριακό σύστημα της Δομής Απασχόλησης και Σταδιοδρομίας (ΔΑΣΤΑ) αποτελείται από έναν application server και ένα database server, ο καθορισμός της πολιτικής ασφάλειας πληροφοριών για το σύστημα αυτό περιγράφεται στη συνέχεια χωρισμένη σε δύο αντίστοιχα μέρη, την Πολιτική Ασφάλειας Βάσης Δεδομένων και την Πολιτική Ασφάλειας Εφαρμογών.

Η πολιτική ασφάλειας πληροφοριών που περιγράφεται στο κεφάλαιο αυτό θα πρέπει να εγκριθεί από τη διοίκηση και να δημοσιευθεί και να κοινοποιηθεί σε όλους τους υπαλλήλους και τα σχετιζόμενα εξωτερικά μέρη.

1.1 Καθορισμός Πολιτικής Ασφάλειας Βάσης Δεδομένων

Η Πολιτικής Ασφάλειας που θα πρέπει να εφαρμοστεί στη Βάση Δεδομένων καθορίζεται μέσα από πέντε άξονες [2,3]:

***1ος**: Πρόσβαση Χρήστη στη Βάση Δεδομένων*

Η Βάση Δεδομένων θα πρέπει να χρησιμοποιείται με ελεγχόμενη πρόσβαση. Για το λόγο αυτό, κάθε χρήστης πρέπει να κατέχει ένα αυθεντικοποιημένο ζεύγος στοιχείων (username, password) μέσω των οποίων θα συνδέεται στη βάση. Για τη διαχείριση της ελεγχόμενης αυτής πρόαβασης στη βάση θα πρέπει να καθοριστούν τα εξής:

- Εάν όλοι οι χρήστες θα μοιράζονται το ίδιο username ή όχι. Εφόσον το πλήθος των χρηστών είναι εξαιρετικά μικρό (2-3 άτομα) και δεν ενδιαφέρει το πρόσωπο που διαχειρίζεται σε δεδομένη χρονική στιγμή τη βάση, τότε θα μπορούσε να υπάρχει ένα username για όλους.

- Ο τρόπος αυθεντικοποίησης των χρηστών στη βάση. Προτείνεται ο πλέον τυπικός τρόπος αυθεντικοποίησης που υλοποιείται με το μηχανισμό των συνθηματικών (passwords).

- Τα συνθηματικά θα πρέπει να λήγουν. Ο χρόνος λήξης θα πρέπει να προσδιοριστεί από το διαχειριστή της βάσης. Προτεινόμενος χρόνος λήξης ενός συνθηματικού για τη συγκεκριμένη εφαρμογή είναι οι 6 μήνες. Μετά την πάροδο των 6 μηνών, το συνθηματικό θα μπαίνει σε μία περίοδο «χάριτος» (grace period) μέσα στην οποία ο χρήστης οφείλει να αλλάξει το συνθηματικό του. Η περίοδος χάριτος θα μπορούσε να είναι διάρκειας 7 ημερών.

- Είναι ιδιαίτερα σημαντικό να μη χρησιμοποιηθεί στην αλλαγή συνθηματικού παλαιότερο συνθηματικό ως νέο. Για το λόγο αυτό, ο μηχανισμός αυθεντικοποίησης θα πρέπει να διατηρεί ιστορικό παρελθόντων συνθηματικών μεγάλου μάλιστα εύρους (π.χ. 20 συνθηματικά). Ο χρήστης έτσι θα αποτρέπεται από τη χρήση συνθηματικών που προτιμά και τα οποία χρησιμοποιεί συνεχώς. Αυτό έχει σαν αποτέλεσμα τη μείωση της πιθανότητας εντοπισμού ενός συνθηματικού μέσω εξαντλητικής επίθεσης στα εφεδρικά αρχεία του συστήματος (backup) όπου θα φυλάσσονται κρυπτογραφημένα τα συνθηματικά.

- Κατά τον ορισμό συνθηματικού από το χρήστη, ο μηχανισμός αυθεντικοποίησης θα πρέπει να τον προτρέπει να επιλέξει κατάλληλο συνθηματικό, περιορίζοντάς τον στα εξής:

    - Το συνθηματικό να μην αποτελεί λέξη από λεξικό για να μη μπορεί να εντοπιστεί με μία επίθεση τύπου λεξικού (dictionary attack).

    - Να έχει μήκος τουλάχιστον 8 χαρακτήρες στους οποίους θα πρέπει υποχρεωτικά να συμπεριλαμβάνονται κεφαλαία, μικρά, αριθμοί και ειδικοί χαρακτήρες (π.χ.!@# κλπ.). Μικρά συνθηματικά εντοπίζονται εύκολα και γρήγορα με επιθέσεις τύπου εξαντλητικής αναζήτησης (brute force attack). Όσο μεγαλύτερο είναι ένα συνθηματικό και ταυτόχρονα όσο μεγαλύτερο είναι το πεδίο ορισμού του, τόσο περισσότεροι είναι οι διαφορετικοί συνδυασμοί που απαιτείται να εξεταστούν σε μια εξαντλητική αναζήτηση για τον εντοπισμό του, που φτάνει να είναι ανέφικτος ο χρόνος προσδιορισμού του (μέρες ή μήνες) ή να ξεπερνά το χρόνο λήξης του (προτεινόμενος 6 μήνες).

    - Να μην επιτρέπεται στο χρήστη κατά την αλλαγή να επιλέξει ως νέο συνθηματικό οποιοδήποτε συνθηματικό τηρείται στο ιστορικό. Οι χρήστες έχουν την τάση να επαναχρησιμοποιούν τα συνθηματικά τους και αντιστέκονται στις όποιες αλλαγές. Για το λόγο αυτό θα πρέπει το ιστορικό να είναι επαρκώς μεγάλο με προτεινόμενο πλήθος συνθηματικών το 20.

- Κατά την ανάπτυξη της εφαρμογής διαχείρισης της βάσης θα πρέπει να εξεταστούν τα παρακάτω ζητήματα:

    - Αν υπάρχει περιορισμός στο πλήθος των ταυτόχρονων sessions που λειτουργεί ένας συγκεκριμένος χρήστης σε δεδομένη χρονική στιγμή.

- Αν θα μπορούν μερικοί ή όλοι οι χρήστες να δημιουργούν τα δικά τους αντικείμενα.

- Αν η πρόσβαση στο λογαριασμό του Διαχειριστή Βάσης Δεδομένων (Data Base Administrator - DBA) ή σε οποιοδήποτε άλλο λογαριασμό με ιδιαίτερα προνόμια θα πρέπει να είναι περιορισμένη ή όχι.

- Ότι η βάση θα είναι προσβάσιμη απομεμακρυσμένα.

- Αν θα γίνει χρήση προχωρημένων τεχνικών ασφάλειας, όπως κρυπτογράφηση σε επίπεδο session, αυθεντικοποίηση μέσω πιστοποιητικών, αυθεντικοποίηση σε επίπεδο λειτουργικού συστήματος, firewalls, κλπ.

- Αν η βάση θα χρησιμοποιηθεί για κατανεμημένα ερωτήματα.

- Αν η χρήση partitions θα πρέπει να περιορίσει την πρόσβαση ορισμένων χρηστών σε μερικά από τα partitions.

2ος: Ευαισθησία Ανάγνωσης των Δεδομένων

- Κάθε χρήστης έχει δικαίωμα ανάγνωσης των δεδομένων που βρίσκονται σε έναν πίνακα που του ανήκει ή αντίστοιχα σε σχήμα ή υποσχήμα της βάσης που ορίζεται μέσα από ένα ερώτημα και στο οποίο αντίστοιχα του επιτρέπεται η ανάγνωση των δεδομένων.

- Ομοίως, χρήστες που κατέχουν το δικαίωμα του συστήματος “SELECT ANY TABLE” έχουν δικαίωμα ανάγνωσης των δεδομένων ολόκληρης της βάσης.

- Υπάρχει αναγκαιότητα για τον προσδιορισμό του είδους της πρόσβασης κάθε χρήστη και σε ποια δεδομένα. Συγκεκριμένα,

    - Αν υπάρχουν κάποια δεδομένα τα οποία πρέπει να είναι προσπελάσιμα από όλους τους νόμιμους χρήστες της βάσης.

    - Αν θα πρέπει να παραχωρηθούν διαφορετικά επίπεδα πρόσβασης σε διαφορετικούς χρήστες.

    - Αν θα πρέπει να χρησιμοποιηθούν επιπρόσθετοι έλεγχοι πρόσβασης, όπως μηχανισμός για την παροχή δυνατοτήτων πολλαπλών επιπέδων ασφάλειας (multi-level security capabilities), κρυπτογράφηση, firewalls, κλπ.

3ος: Ευαισθησία Εγγραφής των Δεδομένων

- Απαιτείται προσδιορισμός του ποιοι χρήστες προσθέτουν, ποιοι τροποποιούν και ποιοι διαγράφουν δεδομένα από τη βάση.

- Κάθε χρήστης έχει δικαίωμα τροποποίησης των δεδομένων που βρίσκονται σε έναν πίνακα που του ανήκει ή αντίστοιχα σε σχήμα ή υποσχήμα της βάσης που ορίζεται μέσα από ένα ερώτημα και στο οποίο αντίστοιχα του επιτρέπεται η τροποποίηση των δεδομένων.

- Ομοίως, χρήστες που κατέχουν τα δικαιώματα “INSERT ANY TABLE”, “UPDATE ANY TABLE” ή “DELETE ANY TABLE” έχουν δικαίωμα τροποποίησης των δεδομένων ολόκληρης της βάσης.

- Κατά την ανάπτυξη της εφαρμογής διαχείρισης της βάσης θα πρέπει να εξεταστούν τα παρακάτω ζητήματα:

    - Αν κάποιοι από τους πίνακες θα έχουν δυνατότητα ενημέρωσης, ή απλά προσθήκης νέων εγγραφών (όπως είναι τα logs), ή θα είναι μόνο για ανάγνωση και οποιαδήποτε τροποποίηση απαγορεύεται.

    - Αν θα απαιτούνται μηχανισμοί ελέγχου των τροποποιήσεων (audit-trails) σε κάποια δεδομένα. Σε αυτά τα δεδομένα, οι συγκεκριμένες γραμμές των πινάκων δε θα πρέπει ποτέ να διαγράφονται ή να ενημερώνονται, αλλά μόνο να σημειώνονται (marked) ως λογικά διαγραμμένες ή αντικαταστημένες, με μία χρονοσήμανση (timestamp).

    - Να προσδιοριστούν τα σημεία που θα επιτρέπεται στους χρήστες να αποθηκεύουν δεδομένα, δηλαδή σε ποια tablespaces και σε ποια σχήματα.

    - Να προσδιοριστεί το μέγεθος του χώρου του δίσκου που θα επιτρέπεται σε ένα χρήστη να χρησιμοποιεί ανά tablespace.

4ος: Πολιτική Ελέγχου

- Είναι ανάγκη να προσδιοριστεί η έκταση της παρακολούθησης για έλεγχο (auditing) που απαιτείται. Η παρακολούθηση θα επιτρέψει τον καθορισμό του ποιος είχε πρόσβαση, σε ποια δεδομένα, πότε και με ποιον τρόπο (ανάγνωση, προσθήκη, ενημέρωση, διαγραφή).

- Ο Διαχειριστής Βάσης Δεδομένων (DBA) θα πρέπει για κάθε σύνολο δεδομένων να εξετάσει τα παρακάτω ζητήματα:

- Αν θα πρέπει να γνωρίζουμε ποιος έχει επιλέξει δεδομένα από πίνακα ή ποιος έχει εισάγει δεδομένα σε πίνακα ή ποιος έχει ενημερώσει ή ποιος έχει διαγράψει δεδομένα από πίνακα.

- Αν θα πρέπει να γνωρίζουμε τον ακριβή χρόνο κάθε πρόσβασης ή αν η γνώση απλά του χρόνου του session κάθε πρόσβασης είναι αρκετή.

- Αν θα πρέπει να γνωρίζουμε τη συγκεκριμένη γραμμή και τη συγκεκριμένη στήλη που έχει γίνει πρόσβαση ή απλά τον πίνακα.

5ος: Γενικά

- Θα πρέπει να καθοριστούν τα δικαιώματα αν θα εκχωρούνται ανά χρήστη ή ανά σύνολο χρηστών που μοιράζονται τον ίδιο ρόλο.

- Θα πρέπει να καθοριστεί αν θα πρέπει να λήγει ένα session μετά από ανενεργό χρόνο (time out). Αν ναι, τότε προτείνεται ο χρόνος αυτός να είναι τα 20 λεπτά. Επιπλέον, να προσδιοριστεί αν υπάρχει περιορισμός χρόνου στο session του χρήστη.

- Θα πρέπει να καθοριστεί αν θα πρέπει τα sessions να έχουν όριο στο ποσό των I/O που παρέχουν και αν αυτό το όριο αφορά στο session ή στο SQL statement ή και στα δύο.

- Να προσδιοριστούν τα αρχεία (εκτός αυτών της βάσης) στα οποία οι χρήστες θα έχουν πρόσβαση π.χ. με χρήση PL/SQL.

- Να προσδιοριστεί το ποσό μνήμης (RAM) που μπορεί ένας χρήστης να χρησιμοποιεί ανά session.

1.2 Καθορισμός Πολιτικής Ασφάλειας Εφαρμογών

- Όλες οι εφαρμογές που χρησιμοποιούνται για λήψη, αποθήκευση, αναφορά, χειρισμό, ή μετάδοση πληροφοριών που ανήκουν στο πληροφοριακό σύστημα ΔΑΣΤΑ θα πρέπει να είναι καταγεγραμμένες και να έχουν αναπτυχθεί σύμφωνα με τις αντίστοιχες απαιτήσεις ασφάλειας.

- Όλοι οι χρήστες που τους δίνεται πρόσβαση στο πληροφοριακό σύστημα ΔΑΣΤΑ θα πρέπει να συμφωνούν ότι συμμορφώνονται με την πολιτική ασφάλειας πληροφοριών της ΔΑΣΤΑ.

- Οι εφαρμογές του πληροφοριακού συστήματος ΔΑΣΤΑ παρέχονται για την υποστήριξη συγκεκριμένων υπηρεσιών και λειτουργιών. Οποιαδήποτε χρήση αυτών των εφαρμογών που παρεμβαίνει σε αυτές τις λειτουργίες ή εμποδίζει τις εν λόγω υπηρεσίες θεωρείται ανάρμοστη. Αυτό περιλαμβάνει τη χρήση των εφαρμογών για ιδιωτική δουλειά ή τη χρήση με τρόπο τέτοιο ώστε να υποβαθμίζει ή να εξαλείφει άλλους στόχους.

- Έλεγχοι για την ασφάλεια εφαρμογών θα πρέπει να εφαρμοστούν με τρόπο τέτοιο ώστε να αντανακλάται η αξία της κάθε εφαρμογής προς τη ΔΑΣΤΑ.

- Όλο το λογισμικό θα πρέπει να είναι προστατευμένο με πρόσφατα εφαρμόσιμα patches σχετικά με την ασφάλεια και αντιιϊκό λογισμικό.

- Τα συνθηματικά είναι ο πρωταρχικός μηχανισμός για την ασφαλή πρόσβαση στις εφαρμογές. Οι χρήστες θα πρέπει να ακολουθούν τις οδηγίες επιλογής κατάλληλου συνθηματικού.

- Οι χρήστες θα πρέπει να ενεργοποιούν ένα συνθηματικό ως μέθοδο προστασίας για την ασφάλιση του υπολογιστικού συστήματος που χρησιμοποιούν.

- Οι παρεχόμενες υπηρεσίες διατηρούν το δικαίωμα να αποκρύπτουν την πρόσβαση για να διατηρήσουν την ακεραιότητα των συστημάτων τους. Αυτό περιλαμβάνει τον περιορισμό ή την ανάκληση των δικαιωμάτων ενός χρήστη ή οποιωνδήποτε άλλων βημάτων θεωρούνται απαραίτητα για τη διαχείριση και την προστασία του πληροφοριακού συστήματος ΔΑΣΤΑ και των δεδομένων του.

2. Καθορισμός των στόχων του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών

Το Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών (Information Security Management Systems - ISMS) του πληροφοριακού συστήματος ΔΑΣΤΑ θα πρέπει να είναι σχεδιασμένο έτσι ώστε να εξασφαλίζει την επιλογή κατάλληλων και ανάλογων ελέγχων ασφάλειας, οι οποίοι προστατεύουν τις πληροφορίες και παρέχουν εμπιστευτικότητα στα ενδιαφερόμενα μέρη [5].

Το ISMS της ΔΑΣΤΑ θα υλοποιηθεί ως μέρος του συνολικού συστήματος διαχείρισης, με προσέγγιση στους κινδύνους του πληροφοριακού συστήματος ΔΑΣΤΑ και στοχεύοντας όπως ορίζεται κατά ISO ([5]) στα εξής:

- την καθιέρωση ενός πλαισίου που θα παρέχει ασφάλεια πληροφοριών στο πληροφοριακό σύστημα ΔΑΣΤΑ.
- την υλοποίηση των απαραίτητων μηχανισμών ασφάλειας για το πλαίσιο αυτό.
- την ορθή λειτουργία του πλαισίου για την ασφάλεια πληροφοριών.
- την παρακολούθηση της αποτελεσματικής εφαρμογής των μηχανισμών.
- την αναθεώρηση, τον εκσυγχρονισμό και την προσαρμογή των μηχανισμών ασφάλειας σε νέες απαιτήσεις του πληροφοριακού συστήματος ΔΑΣΤΑ.
- τη συντήρηση του πλαισίου ασφάλειας πληροφοριών έτσι ώστε να πληροί τους στόχους του.

- τη βελτίωση της ασφάλειας πληροφοριών με σκοπό την αποδοτικότερη λειτουργία του πληροφοριακού συστήματος ΔΑΣΤΑ.

Ο σχεδιασμός και η ανάπτυξη του ISMS του πληροφοριακού συστήματος ΔΑΣΤΑ επηρεάζεται από τις ανάγκες και τους στόχους της ΔΑΣΤΑ, τις απαιτήσεις ασφάλειας και τις διαδικασίες που υλοποιούνται μέσα από το πληροφοριακό της σύστημα.

Η εφαρμογή διαφόρων διεργασιών, που θα αποτελούν το πλαίσιο ασφάλειας πληροφοριών και το οποίο θα υλοποιείται και θα συντηρείται από το ISMS του πληροφοριακού συστήματος ΔΑΣΤΑ, ενθαρύνουν τους χρήστες να εστιάσουν στη σπουδαιότητα και αναγκαιότητα των παρακάτω:

- Να κατανοήσουν τις απαιτήσεις ασφάλειας του πληροφοριακού συστήματος ΔΑΣΤΑ και της ανάγκης για εγκατάσταση πολιτικής και στόχων που θα παρέχουν ασφάλεια πληροφοριών.

- Να εγκατασταθούν και να λειτουργούν έλεγχοι για τη διαχείριση των κινδύνων του πληροφοριακού συστήματος ΔΑΣΤΑ, ως μέρος του γενικότερου πλαισίου των κινδύνων που αντιμετωπίζει ο φορέας της ΔΑΣΤΑ.

- Να παρακολουθούνται και να επιθεωρούνται η επίδοση και η αποτελεσματικότητα του ISMS ΔΑΣΤΑ.

- Η συνεχής βελτίωση του ISMS ΔΑΣΤΑ με βάση αντικειμενικές μετρήσεις.

Το ISO υιοθετεί μία προσέγγιση για να δομήσει όλες τις διεργασίες που υποστηρίζει ένα Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών, το “Plan-Do-Check-Act” (PCDA) μοντέλο [5]. Συνοπτικά, τα βήματα του μοντέλου PCDA για το ISMS ΔΑΣΤΑ περιλαμβάνουν τα εξής:

Plan (Σχεδιασμός για την ανάπτυξη ISMS): Για την καθιέρωση του ISMS ΔΑΣΤΑ θα πρέπει να δημιουργηθούν μία πολιτική, οι στόχοι, οι διεργασίες και οι διαδικασίες που σχετίζονται με τη διαχείριση κινδύνων και τη βελτίωση της ασφάλειας πληροφοριών, ώστε να επιφέρουν αποτελέσματα, σε συμφωνία πάντα με το γενικότερο πλαίσιο των στόχων και των πολιτικών της ΔΑΣΤΑ.

Do (Υλοποίηση και Λειτουργία του ISMS): Ανάπτυξη και λειτουργία της πολιτικής, των ελέγχων, των διεργασιών και των διαδικασιών του ISMS ΔΑΣΤΑ.

Check (Παρακολούθηση και Επιθεώρηση του ISMS): Πρόσβαση και όπου επιτρέπεται μέτρηση της επίδοσης μιας διεργασίας έναντι της πολιτικής του ISMS ΔΑΣΤΑ, των στόχων και της εμπειρίας και αναφορά των αποτελεσμάτων στη διοίκηση για επιθεώρηση.

Act (Συντήρηση και Βελτίωση του ISMS): Λήψη διορθωτικών και προληπτικών ενεργειών, με βάση τα αποτελέσματα του εσωτερικού ελέγχου του ISMS ΔΑΣΤΑ και της επιθεώρησης της διοίκησης ή άλλων σχετικών πληροφοριών, για την επίτευξη συνεχούς βελτίωσης του ISMS ΔΑΣΤΑ.

Συνοψίζοντας, το ISMS ΔΑΣΤΑ θα πρέπει να έχει ως κύριο στόχο τη διατήρηση των τριών θεμελιωδών αρχών της ασφάλειας πληροφοριών, της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας της πληροφορίας, όπως προσδιορίζεται στις απαιτήσεις ασφάλειας.

3. Διενέργεια Ανάλυσης Κινδύνου για το προτεινόμενο Σύστημα Διαχείρισης Ασφάλειας Πληροφοριών

Η υλοποίηση και καθιέρωση του ISMS ΔΑΣΤΑ που περιγράφηκε στο προηγούμενο κεφάλαιο ξεκινά με την Ανάλυση Επικινδυνότητας (Risk Analysis). Πρόκειται για μια διαδικασία με την οποία θα καθοριστούν όλα τα έκθετα σημεία του πληροφοριακού συστήματος ΔΑΣΤΑ και του πιθανού κακού που μπορεί να συμβεί σε καθένα από αυτά. Η Ανάλυση Επικινδυνότητας περιλαμβάνει τρία κύρια στάδια:

- Την καταγραφή σε λίστα όλων των σημείων έκθεσης του πληροφοριακού συστήματος ΔΑΣΤΑ.

- Για κάθε σημείο έκθεσης, καταγράφονται οι πιθανοί έλεγχοι (controls) και το κόστος του καθενός.

- Διενεργείται Ανάλυση Κόστους-Οφέλους (Cost-Benefit Analysis).

Υπάρχουν συγκεκριμένοι λόγοι για τους οποίους διενεργείται μία ανάλυση επικινδυνότητας και οι οποίοι συνοψίζονται στους ακόλουθους:

- Βελτίωση της αφύπνισης.

- Αναγνώριση των στοιχείων (assets), των αδυναμιών (vulnerabilities) και των ελέγχων (controls).

- Βελτίωση της βάσης αποφάσεων.

- Αιτιολόγηση των εξόδων για ασφάλεια πληροφοριών.

Για να πραγματοποιηθεί η ανάλυση επικινδυνότητας με συστηματικό τρόπο, ακολουθούνται τα παρακάτω βήματα [6]:

1. Αναγνώριση των περιουσιακών στοιχείων (assets).
2. Καθορισμός αδυναμιών.
3. Εκτίμηση πιθανότητας εκμετάλλευσης.
4. Υπολογισμός αναμενόμενης ετήσιας απώλειας (ζημιάς).
5. Διερεύνηση εφαρμόσιμων ελέγχων και του κόστους τους.
6. Ετήσια εξοικονόμηση προγράμματος του ελέγχου.

Στις παραγράφους που ακολουθούν αναλύονται τα βήματα που ακολουθούνται για τη διεξαγωγή της ανάλυσης επικινδυνότητας και τα οποία επαναλαμβάνονται αφού τεθεί σε ισχύ το ISMS ΔΑΣΤΑ όποτε επιθεωρείται και απαιτείται συντήρηση.

3.1 Αναγνώριση των περιουσιακών στοιχείων (assets)

Το πληροφοριακό σύστημα ΔΑΣΤΑ διαθέτει στο ενεργητικό του τα ακόλουθα στοιχεία:

› Υλικό (*Hardware*): Ένας application server, ένας database server, με επεξεργαστές, πληκτρολόγια, οθόνες, τερματικά, controllers, κλπ.

› Λογισμικό (*Software*): source programs, object programs, utilities, λειτουργικά συστήματα, compilers, κλπ.

› Δεδομένα (*Data*): δεδομένα που χρησιμοποιούνται σε βάση δεδομένων, που αποθηκεύονται, που τυπώνονται, logs, audit records, κλπ.

› Ανθρώπους (*People*): όσοι χρειάζονται για να τρέξουν το υπολογιστικό σύστημα ή συγκεκριμένα προγράμματα και χρήστες.

› Τεκμηρίωση (*Documentation*): για προγράμματα, υλικό, συστήματα, διαδικασίες διαχείρισης και για ολόκληρο το σύστημα.

› Αναλώσιμα (*Supplies*): χαρτί, φόρμες, laser cartridges, μαγνητικά μέσα και μελάνι εκτυπωτή.

3.2 Καθορισμός αδυναμιών (vulnerabilities)

Για τον καθορισμό των αδυναμιών κάθε τμήματος των περιουσιακών στοιχείων (ενεργητικού) του πληροφοριακού συστήματος ΔΑΣΤΑ δημιουργείται ένα πίνακας (Πίνακας 1), στον οποίο σε κάθε γραμμή αναγράφεται ένα στοιχείο του ενεργητικού και δημιουργούνται τρεις στήλες, μία για κάθε θεμελιώδη αρχή της ασφάλειας πληροφοριών, την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα. Σε κάθε κελί του πίνακα καθορισμού των αδυναμιών συμπληρώνεται ως αδυναμία το ενδεχόμενο κακόβουλο γεγονός που αντίστοιχα θα προσβάλει τη θεμελιώδη αρχή που αντιστοιχεί στη στήλη αυτή.

Για παράδειγμα, παραβίαση που συνδυάζεται με τροποποίηση υλικού προκαλεί έλλειψη ακεραιότητας, καταστροφή ή κλοπή υλικού προκαλεί έλλειψη διαθεσιμότητας, προσθήκη

Trojan horse σε λογισμικό προκαλεί έλλειψη ακεραιότητας, τοποθέτηση σε λάθος θέση λογισμικού προκαλεί έλλειψη διαθεσιμότητας, κλπ.

Ενεργητικό	Εμπιστευτικότητα	Ακεραιότητα	Διαθεσιμότητα
Υλικό		Overloaded Καταστροφή Παραβιασμένο	Αποτυχία Κλοπή Καταστροφή Μη διαθέσιμο
Λογισμικό	Κλοπή Αντιγραφή Πειρατεία	Trojan horse Τροποποίηση Παραβιασμένο	Διαγραφή Λάθος θέση Λήξη χρήσης
Δεδομένα	Έκθεση Πρόσβαση από εξωτερικό Συμπερασματικά	Ζημιά ♦ λάθος λογισμικού ♦ λάθος υλικού ♦ λάθος χρήστη	Διαγραφή Λάθος θέση Καταστροφή
Άνθρωποι			Έξοδος Σύνταξη Λήξη Διακοπές
Τεκμηρίωση			Απώλεια Κλοπή Καταστροφή
Αναλώσιμα			Απώλεια Κλοπή Ζημιά

Πίνακας 1: Πίνακας καθορισμού αδυναμιών στο πληροφοριακό σύστημα ΔΑΣΤΑ

Για να διευκολυνθεί η συμπλήρωση του παραπάνω πίνακα, αλλά και η ενημέρωση και συντήρηση του ISMS ΔΑΣΤΑ στο μέλλον, θα πρέπει να τεθούν μία σειρά ερωτήσεων, όπως οι παρακάτω:

- Ποιες οι επιπτώσεις από τα λάθη που γίνονται χωρίς πρόθεση.
- Ποιες οι επιπτώσεις από εσωτερικούς επιτιθέμενους με πρόθεση να προξενήσουν βλάβη.
- Ποιες οι επιπτώσεις από εξωτερικούς επιτιθέμενους.
- Ποιες οι επιπτώσεις από φυσικές καταστροφές

3.3 Εκτίμηση πιθανότητας εκμετάλλευσης

Για να γίνει εκτίμηση της πιθανότητας να συμβεί ένα από τα γεγονότα που καθορίζουν τις αδυναμίες του πληροφοριακού συστήματος ΔΑΣΤΑ, μπορούν να χρησιμοποιηθούν πολλοί διαφορετικοί τρόποι, όπως:

- Εκτίμηση πιθανότητας από δεδομένα παρατήρησης του γενικού πληθυσμού.
- Εκτίμηση πιθανότητας από δεδομένα παρατήρησης για ένα συγκεκριμένο σύστημα.
- Εκτίμηση του αριθμού εμφάνισης σε δεδομένη χρονική περίοδο.
- Εκτίμηση της πιθανότητας από ένα πίνακα.
- Η προσέγγιση Delphi.

Στη συγκεκριμένη μελέτη επιλέχθηκε ως πιο πρακτικός τρόπος η χρήση πίνακα. Ο Πίνακας 2 που παρατίθεται στη συνέχεια παρουσιάζει σε μία κλίμακα από 1 έως 10 την βαθμιαία αύξηση εμφάνισης ενός γεγονότος από 0 για λιγότερο από μια φορά στα τρία χρόνια μέχρι 10 για περισσότερο από μια φορά την ημέρα.

Συχνότητα	**Κλίμακα**
Περισσότερο από μία φορά την ημέρα	10
Μία φορά την ημέρα	9
Μία φορά στις τρεις ημέρες	8
Μία φορά την εβδομάδα	7
Μία φορά στις δύο εβδομάδες	6
Μία φορά το μήνα	5
Μία φορά στους τέσσερις μήνες	4
Μία φορά το χρόνο	3
Μία φορά στα τρία χρόνια	2
Λιγότερο από μία φορά στα τρία χρόνια	1

Πίνακας 2: Πίνακας κλιμάκωσης εμφάνισης γεγονότων στο πληροφοριακό σύστημα ΔΑΣΤΑ

Μετά την εγκατάσταση και λειτουργία του πληροφοριακού συστήματος ΔΑΣΤΑ σε πραγματικές συνθήκες, επιτρέπεται η αναπροσαρμογή των συχνοτήτων αυτών ακόμη και η χρήση άλλου τρόπου εκτίμησης της συχνότητας εμφάνισης των ευπαθειών, όπως από τα δεδομένα παρατήρησης στο σύστημα ή από μετρήσεις σε δεδομένη χρονική στιγμή.

Το αποτέλεσμα στο βήμα αυτό της ανάλυσης επικινδυνότητας παρουσιάζεται στον Πίνακα 3 και έχει προκύψει με χρήση του Πίνακα 2.

Ενεργητικό	Εμπιστευτικότητα	Ακεραιότητα	Διαθεσιμότητα
Υλικό		Overloaded 2 Καταστροφή 1 Παραβιασμένο 2	Αποτυχία 5 Κλοπή 1 Καταστροφή 1 Μη διαθέσιμο 4
Λογισμικό	Κλοπή 2 Αντιγραφή 7 Πειρατεία 4	Trojan horse 6 Τροποποίηση 6 Παραβιασμένο 5	Διαγραφή 3 Λάθος θέση 6 Λήξη χρήσης 3
Δεδομένα	Έκθεση 8 Πρόσβαση από εξωτερικό 3 Από απόρροια 5	Ζημιά ♦ λάθος λογισμικού 2 ♦ λάθος υλικού 1 ♦ λάθος χρήστη 7	Διαγραφή 5 Λάθος θέση 6 Καταστροφή 6
Άνθρωποι			Έξοδος 1 Σύνταξη 1 Λήξη 4 Διακοπές 3
Τεκμηρίωση			Απώλεια 3 Κλοπή 1 Καταστροφή 1
Αναλώσιμα			Απώλεια 4 Κλοπή 6 Ζημιά 3

Πίνακας 3: Πίνακας αδυναμιών και συχνότητας εμφάνισης αυτών στο σύστημα ΔΑΣΤΑ

3.4 Υπολογισμός αναμενόμενης ετήσιας απώλειας (ζημιάς)

Για να διευκολυνθεί ο προσδιορισμός της πηγής ενός πραγματικού ή μη κόστους, αλλά και η ενημέρωση και συντήρηση του ISMS ΔΑΣΤΑ στο μέλλον, μπορούν να τεθούν ερωτήσεις, όπως οι παρακάτω:

- Ποιες νομικές υποχρεώσεις υπάρχουν για την τήρηση της ακεραιότητας και εμπιστευτικότητας των δεδομένων;
- Μπορεί η απώλεια αυτών των δεδομένων να προκαλέσει κακό σε ένα άτομο ή σε έναν οργανισμό;
- Ποια η αξία πρόσβασης σε δεδομένα ή προγράμματα;
- Ποια η αξία για κάποιον άλλο της πρόσβασης σε δεδομένα ή προγράμματα;
- Τι προβλήματα προκύπτουν από την απώλεια δεδομένων;

Θεωρώντας ότι κάθε αδυναμία που προσδιορίστηκε στον Πίνακα 1 στοιχίζει κόστος C_i για $i=1,2,\ldots,n$ και ότι το ετήσιο κόστος απώλειας λόγω της αδυναμίας αυτής προσδιορίζεται από τη συχνότητα εμφάνισης του γεγονότος f_i, ως το γινόμενο C_i επί το χρονικό διάστημα t_i που αντιστοιχεί στη συχνότητα (1 για ένα έτος, 3 για τρεις φορές το χρόνο, 0.2 για μία φορά στα πέντε χρόνια, κλπ.), η αναμενόμενη ετήσια απώλεια υπολογίζεται από τον ακόλουθο τύπο για όλα τα στοιχεία του ενεργητικού και όλες τις n αδυναμίες τους:

$$\sum_{i=1}^{n} C_i \times t_i \qquad i = 1,2,\ldots,n$$

3.5 Διερεύνηση εφαρμόσιμων ελέγχων και του κόστους τους.

Ένας τρόπος για τον καθορισμό επιπλέον εφαρμόσιμων ελέγχων είναι αυτός που βασίζεται σε κάθε αδυναμία, ενώ ένας άλλος τρόπος είναι η αναζήτηση μέσα από λίστα γνωστών ελέγχων, όπως η παρακάτω:

- έλεγχοι κρυπτογραφίας
- ασφαλή πρωτόκολλα
- έλεγχοι ανάπτυξης προγραμμάτων
- έλεγχοι περιβάλλοντος εκτέλεσης προγραμμάτων
- χαρακτηριστικά προστασίας λειτουργικού συστήματος
- Ταυτότητας
- Αυθεντικοποίησης
- σχεδιασμού και υλοποίησης ασφαλών λειτουργικών συστημάτων
- έλεγχοι πρόσβασης σε βάση δεδομένων
- έλεγχοι αξιοπιστίας σε βάση δεδομένων
- έλεγχοι απόρροιας δεδομένων (i*nference*) από βάση δεδομένων

- έλεγχοι ασφάλειας πολλαπλών επιπέδων για δεδομένα, βάσεις δεδομένων, και λειτουργικά συστήματα
- έλεγχοι προσωπικών υπολογιστών: διαδικαστικοί, φυσικοί, υλικού, και λογισμικού
- έλεγχοι πρόσβασης στο δίκτυο
- έλεγχοι ακεραιότητας δικτύου
- φυσικοί έλεγχοι

3.6 Ετήσια εξοικονόμηση προγράμματος του ελέγχου.

Το effective cost είναι το κόστος ενός ελέγχου μείον οποιαδήποτε μείωση της αναμενόμενης ετήσιας απώλειας από τη χρήση αυτού του ελέγχου.

Γι' αυτό το πραγματικό κόστος μπορεί να είναι αρνητικό αν η μείωση του κινδύνου είναι μεγαλύτερη από το κόστος του ελέγχου.

Αν θεωρήσουμε ότι το effective cost είναι το $\boldsymbol{EC_i}$ και η μείωση της αναμενόμενης ετήσιας απώλειας από τη χρήση του συγκεκριμένου ελέγχου για τον $\boldsymbol{i}$ κίνδυνο είναι $\boldsymbol{R_i}$ τότε το effective cost κόστος ορίζεται ως:

$$EC_i = C_i - R_i$$

4. Καθορισμός του τρόπου αντιμετώπισης των Κινδύνων που εντοπίστηκαν

Για να αντιμετωπιστούν οι κίνδυνοι που αναγνωρίστηκαν στο προηγούμενο κεφάλαιο θα πρέπει να αντιστοιχηθούν οι έλεγχοι που διερευνήθηκαν στα στοιχεία του ενεργητικού και να καθοριστεί το σύνολο των ελέγχων από τους οποίους πρόκειται να γίνει η επιλογή. Στον Πίνακα 4 που ακολουθεί παραθέτονται τα στοιχεία που καθορίζουν τον τρόπο αντιμετώπισης κάθε κινδύνου ανά στοιχείο ενεργητικού του πληροφοριακού συστήματος ΔΑΣΤΑ.

Ενεργητικό	Αδυναμία	Έλεγχοι
Υλικό	Overloaded 2 Καταστροφή 1 Παραβιασμένο 2 Αποτυχία 5 Κλοπή 1 Μη διαθέσιμο 4	ασφαλή πρωτόκολλα, έλεγχοι περιβάλλοντος εκτέλεσης προγραμμάτων, έλεγχοι πρόσβασης στο δίκτυο, έλεγχοι ακεραιότητας δικτύου, έλεγχοι προσωπικών υπολογιστών: διαδικαστικοί, φυσικοί, υλικού, και λογισμικού, φυσικοί έλεγχοι
Λογισμικό	Κλοπή 2 Αντιγραφή 7 Πειρατεία 4 Trojan horse 6 Τροποποίηση 6 Παραβιασμένο 5 Διαγραφή 3 Λάθος θέση 6 Λήξη χρήσης 3	έλεγχοι ανάπτυξης προγραμμάτων έλεγχοι περιβάλλοντος εκτέλεσης προγραμμάτων χαρακτηριστικά προστασίας λειτουργικού συστήματος Ταυτότητας Αυθεντικοποίησης σχεδιασμού και υλοποίησης ασφαλών λειτουργικών συστημάτων έλεγχοι ασφάλειας πολλαπλών επιπέδων για δεδομένα, βάσεις δεδομένων, και λειτουργικά

		συστήματα έλεγχοι προσωπικών υπολογιστών: διαδικαστικοί, φυσικοί, υλικού, και λογισμικού έλεγχοι πρόσβασης στο δίκτυο έλεγχοι ακεραιότητας δικτύου φυσικοί έλεγχοι
Δεδομένα	Έκθεση 8 Πρόσβαση από εξωτερικό 3 Από απόρροια 5 Ζημιά ♦ λάθος λογισμικού 2 ♦ λάθος υλικού 1 ♦ λάθος χρήστη 7 Διαγραφή 5 Λάθος θέση 6 Καταστροφή 6	έλεγχοι κρυπτογραφίας ασφαλή πρωτόκολλα έλεγχοι ανάπτυξης προγραμμάτων έλεγχοι περιβάλλοντος εκτέλεσης προγραμμάτων χαρακτηριστικά προστασίας λειτουργικού συστήματος Ταυτότητας Αυθεντικοποίησης σχεδιασμού και υλοποίησης ασφαλών λειτουργικών συστημάτων έλεγχοι πρόσβασης σε βάση δεδομένων έλεγχοι αξιοπιστίας σε βάση δεδομένων έλεγχοι απόρροιας δεδομένων (*inference*) από βάση δεδομένων έλεγχοι ασφάλειας πολλαπλών επιπέδων για δεδομένα, βάσεις δεδομένων, και λειτουργικά συστήματα φυσικοί έλεγχοι
Άνθρωποι	Έξοδος 1 Σύνταξη 1 Λήξη 4 Διακοπές 3	Παρακολούθηση συμβάσεων, αδειών, κλπ. προσωπικού

Τεκμηρίωση	Απώλεια Κλοπή Καταστροφή	3 1 1	φυσικοί έλεγχοι
Αναλώσιμα	Απώλεια Κλοπή Ζημιά	4 6 3	Παρακολούθηση αποθήκης για την επάρκεια κατάλληλων αναλώσιμων, φυσικοί έλεγχοι

Πίνακας 4: Καθορισμός του τρόπου αντιμετώπισης κάθε κινδύνου ανά στοιχείο ενεργητικού του πληροφοριακού συστήματος ΔΑΣΤΑ

5. Επιλογή των απαραίτητων ελέγχων και βελτιώσεων

Για την επιλογή των απαραίτητων ελέγχων θα πρέπει να μετρηθεί το κόστος κάθε ελέγχου, το effective cost κάθε ελέγχου καθώς και ο συνδυασμός χρήσης πολλαπλών ελέγχων, ώστε να αποφευχθεί το επιπλέον κόστος από την επικάλυψη αυτών. Απαραίτητοι είναι οι έλεγχοι που στοχεύουν στην αντιμετώπιση κινδύνων και στην κάλυψη αντίστοιχα αδυναμιών που αφορούν κρίσιμα στοιχεία του πληροφοριακού συστήματος ΔΑΣΤΑ και για τα οποία το κόστος επαναφοράς είναι υψηλό ή/και η έλλειψη διαθεσιμότητάς τους υπολογίζεται ως καθοριστικά σημαντική για την ομαλή λειτουργία του συστήματος και κατ' επέκταση ολόκληρης της ΔΑΣΤΑ.

Στο μέλλον, θα μπορούν να επαναλαμβάνονται βήματα της ανάλυσης επικινδυνότητας έτσι ώστε να εντοπίζονται βελτιωμένοι έλεγχοι, να καλύπτονται πρόσθετες αδυναμίες και να αντιμετωπίζονται νέοι κίνδυνοι που προκύπτουν είτε λόγω της εξέλιξης και του τρόπου επιθέσεων, είτε λόγω τροποποιήσεων, αλλαγών, βελτιώσεων και διαδικασιών συντήρησης του πληροφοριακού συστήματος ΔΑΣΤΑ.

Αναφορές

[1] ISO/IEC 17799, Information technology – Security techniques – Code of practice for information security management, second edition 2005-06-15.

[2] Kreines David and Laskey Brian, Oracle Database Administration: The Essential Reference, O'Reilly & Associates, 1999, pp. 98-99.

[3] Wayne Pollock, Determining a Data Base Security Policy, last updated 12/01/2013, http://content.hccfl.edu/pollock/Oracle/SecurityPolicy.htm, accessed 20/10/2013.

[5] ISO/IEC FDIS 27001, Information technology – Security techniques –Information Security management systems - Requirements, 2005-08-30.

[6] Charles Pfleeger, Security In Computing, Prentice HallPTR, 2000.