Εφαρμογή Ηλεκτρονικής Διαχείρισης Μετεγγραφών

Παραδοτέο: Αναφορά Συντήρησης και Λειτουργίας της Εφαρμογής

Συνοπτική μελέτη ασφαλείας για την Ηλεκτρονική Υπηρεσία Διαχείρισης Μετεγγραφών σε Πανεπιστήμια/Τ.Ε.Ι.

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ
επένδυση στην κοινωνία της γνώσης
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ & ΘΡΗΣΚΕΥΜΑΤΩΝ, ΠΟΛΙΤΙΣΜΟΥ & ΑΘΛΗΤΙΣΜΟΥ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ
ΕΣΠΑ 2007-2013
πρόγραμμα για την ανάπτυξη
ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΩΝΙΚΟ ΤΑΜΕΙΟ
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

1. Εισαγωγή

Το παρόν έγγραφο αποτελεί μελέτη ασφαλείας του κεντρικού πληροφοριακού συστήματος της εφαρμογής ηλεκτρονικής διαχείρισης μετεγγραφών των φοιτητών των Πανεπιστημίων και των ΤΕΙ της επικράτειας που έχει αναπτυχθεί από την ΕΔΕΤ ΑΕ. Παρουσιάζει και αναλύει τα βασικά χαρακτηριστικά ασφάλειας που θα διαθέτει η εφαρμογή σε λειτουργικό και διαχειριστικό επίπεδο, καθώς και σε επίπεδο υλικού και φυσικής ασφάλειας. Επίσης, η μελέτη περιλαμβάνει τις διαδικασίες ανάκτησης δεδομένων σε περίπτωση αποτυχίας του βασικού συστήματος και την λειτουργία εφεδρικών συστημάτων (disaster recovery). Τέλος η μελέτη καταγράφει τις απαιτήσεις για τον έλεγχο πρόσβασης στο σύστημα ηλεκτρονικής διαχείρισης μετεγγραφών και τις υποχρεώσεις των χρηστών για την διαφύλαξη των στοιχείων πρόσβασης στην εφαρμογή. Σημειώνεται ότι η λειτουργία της εφαρμογής θα υποστηρίζεται από Γραφείο Αρωγής (Help Desk), το οποίο θα είναι ενήμερο για την πολιτική ασφάλειας και θα καθοδηγεί τους χρήστες για την ορθή χρήση της εφαρμογής σε θέματα ασφάλειας και προστασίας προσωπικών δεδομένων.

2. Χαρακτηριστικά Συστήματος Ασφαλείας

Η πλατφόρμα η οποία φιλοξενεί την εφαρμογή ηλεκτρονικής διαχείρισης μετεγγραφών αποτελείται από επιμέρους τμήματα λογισμικού και υλικού και για τον λόγο αυτό τα χαρακτηριστικά του συστήματος ασφαλείας έχουν χωριστεί στα εξής τμήματα: Προστασία Λογισμικού Διακομιστή, Προστασία Δικτύου, Προστασία Βάσης Δεδομένων, Διαδικασία λήψης Αντιγράφων Ασφαλείας, Ασφαλής Επικοινωνία Διεπαφής με τον Χρήστη και Προδιαγραφές Ασφαλείας Κτιριακής Εγκατάστασης (Φυσική Ασφάλεια). Σημειώνεται ότι η εφαρμογή είναι διαδικτυακή (web based) και για το λόγο αυτό υλοποιούνται και μηχανισμοί για την ασφαλή επικοινωνία στο Διαδίκτυο (Internet).

Προστασία Λογισμικού Διακομιστή

Το πρώτο χαρακτηριστικό ασφάλειας αναφέρεται στην προστασία του λογισμικού του διακομιστή των εφαρμογών διαδικτύου. Η προστασία αυτή επιτυγχάνεται με τους παρακάτω τρόπους:

- **Εγκατάσταση και χρήση λειτουργικού Microsoft Windows Server**

Στους εξυπηρετητές της εφαρμογής (servers) προτείνεται η εγκατάσταση λειτουργικού συστήματος Microsoft Windows Server. Η επιλογή του λειτουργικού συστήματος Microsoft Windows Server έχει αποδειχτεί από την εφαρμογή του σε άλλα συστήματα ότι εξασφαλίζει υψηλή ασφάλεια και αξιοπιστία. Οι λόγοι που επιλέγεται το συγκεκριμένο λειτουργικό σύστημα είναι:

Είναι ένα σύγχρονο λειτουργικό σύστημα που ενσωματώνει τις τελευταίες τεχνολογίες σε θέματα ασφάλειας και αξιοπιστίας. Προσφέρει έτοιμες και δοκιμασμένες λύσεις που ικανοποιούν τις υψηλές απαιτήσεις ασφάλειας, αξιοπιστίας και διαθεσιμότητας που συναντώνται σε εφαρμογές μεγάλης κλίμακας.

Υποστηρίζεται από μία από τις μεγαλύτερες εταιρείες λογισμικού βεβαιώνοντας έτσι την έγκαιρη διαθεσιμότητα ενημερώσεων τόσο ασφαλείας όσο και επιδιορθώσεως προβλημάτων σε όλο το βάθος χρόνου λειτουργίας του συστήματος καθώς και την ύπαρξη υποστήριξης επιχειρησιακού επιπέδου.

Το γεγονός πως το λειτουργικό σύστημα αλλά και οι υπόλοιπες εφαρμογές που χρησιμοποιούνται (firewalls, βάση δεδομένων, web server) έχουν αναπτυχθεί και προσφέρονται από την ίδια εταιρεία βεβαιώνει και την υψηλή συμβατότητα και συνεργασία όλων των σε λειτουργία υποσυστημάτων σε όλα τα επίπεδα, ασφάλειας αλλά και επίδοσης.

Υποστηρίζεται από σχεδόν όλους τους κατασκευαστές hardware, άρα βεβαιώνονται η υψηλή συμβατότητα με το εκάστοτε hardware, οι υψηλές επιδόσεις του συστήματος, αλλά και η διαθεσιμότητα υπόστηριξης από τους κατασκευαστές σε όποια πρόβλημα και αν παρουσιαστεί.

Ακολουθούν επιπλέον λόγοι για τους οποίους λειτουργικό σύστημα Microsoft Windows Server παρουσιάζει αυξημένη προστασία και αξιοπιστία:

- Ασφάλεια μέσω σχεδιασμού
- Προστασία μνήμης διεργασιών
- Προσωπικοί λογαριασμοί χρηστών
- Προσωπικοί χώροι αποθήκευσης αρχείων
- Προσωπικές ρυθμίσεις εφαρμογών
- Άδειες πρόσβασης αρχείων

- Ασφάλεια μέσω κρυπτογραφίας
- Ευαίσθητα δεδομένα κρυπτογραφούνται
- Υποστήριξη κρυπτογραφημένων συστημάτων αρχείων
- Δωρεάν πρόσβαση σε ενημερώσεις τόσο του λειτουργικού όσο και των εφαρμογών.

- **Ελεγχόμενη πρόσβαση χρηστών και περιοδική αλλαγή του κωδικού του διαχειριστή**

Ένα σημαντικό μέτρο ασφαλείας σε ένα περιβάλλον δικτυακού εξυπηρετητή/διακομιστή είναι η ελεγχόμενη πρόσβαση των χρηστών. Η ελεγχόμενη πρόσβαση πραγματοποιείται με τη σωστή δημιουργία λογαριασμού χρηστών και της απαγόρευσης ανάγνωσης, εκτέλεσης και εγγραφής αρχείων τα οποία δεν ανήκουν σε αυτούς.

- **Ελεγχόμενη πρόσβαση σε αρχεία της διεπαφής**

Η πρόσβαση στα αρχεία της διεπαφής τα οποία χρησιμοποιούνται από τον διακομιστή για να υλοποιούν τη λειτουργικότητα της Εφαρμογής, θα πρέπει να είναι πλήρως ελεγχόμενη. Αυτό

σημαίνει πως πρόσβαση εγγραφής και ανάγνωσης έχει μόνο ο διαχειριστής του συστήματος, και πρόσβαση ανάγνωσης μόνο ο εξυπηρετητής ιστού ο οποίος παράγει το περιεχόμενο που βλέπει ο χρήστης στον περιηγητή του (browser).

- **Καταγραφή ενεργειών χρηστών**

Οι ενέργειες των χρηστών καταγράφονται με σκοπό τον έλεγχο και διόρθωση βλαβών αλλά και την παροχή ασφάλειας μέσω του εντοπισμού κακόβουλων ενεργειών. Συγκεκριμένα η καταγραφή γίνεται σε ειδικά αρχεία (log files), τα οποία περιέχουν σε κατάλληλη μορφή πληροφορίες για το πότε έγινε και από ποιόν χρήστη μια συγκεκριμένη ενέργεια.

Προστασία Δικτύου μέσω Firewall

Για την προστασία του δικτύου, την πρόληψη επιθέσεων και τη ρύθμιση της κυκλοφορίας δεδομένων προτείνεται να εγκατασταθεί ένα «τείχος προστασίας» (firewall). Το firewall θα πρέπει

να ρυθμιστεί ώστε να απορρίπτει όλες τις συνδέσεις εκτός αυτών που επιτρέπει ο διαχειριστής του δικτύου (default deny). Κατά την εγκατάσταση, παραμετροποίηση και διαχείριση του Firewall προτείνεται να ληφθούν υπόψη τα παρακάτω:

- Οι μηχανισμοί firewall θα πρέπει να διαμορφωθούν και να προκαθοριστούν με τέτοιο τρόπο που να εξασφαλίζουν την προστασία του δικτύου από κακόβουλες ενέργειες. Θα πρέπει να δέχονται μόνο τα απαιτούμενα πρωτόκολλα και IP διευθύνσεις
- Η φυσική πρόσβαση στο firewall θα πρέπει να περιορίζεται μόνο στα εξουσιοδοτημένα άτομα.
- Η λογική πρόσβαση στο firewall θα πρέπει να υπόκεινται σε αυστηρούς περιορισμούς και στην επικύρωση των χρηστών τους. Αυτοί οι έλεγχοι πρέπει να αναθεωρούνται τακτικά.
- Τα αποτελέσματα των ελέγχων του firewall θα πρέπει να αναθεωρούνται συχνά και να αποθηκεύονται σε ασφαλή σημεία.
- Θα πρέπει να καταγράφονται και να ελέγχονται όλες οι απόπειρες παραβίασης του δικτύου.
- Πετυχημένες και αποτυχημένες απόπειρες πρόσβασης στο firewall θα πρέπει να παρουσιάζονται και να ελέγχονται.
- Οι προκαθορισμένοι κωδικοί πρόσβασης θα πρέπει να απενεργοποιούνται για όλα τα firewall.
- Οι επιφυλακές ασφάλειας από τον κατασκευαστή firewall και από τα συμβουλευτικά όργανα ασφάλειας, θα πρέπει να λαμβάνονται σοβαρά υπόψη.

Όλες οι συνδέσεις και οι έλεγχοι του firewall πρέπει να αναθεωρούνται τακτικά και να εξετάζονται για θέματα ασφαλείας.

Η χρήση του Microsoft ISA Firewall δίνει τη δυνατότητα δημιουργίας ενός firewall που θα αναλαμβάνει τον φόρτο που δημιουργείται από την κρυπτογράφηση των δεδομένων

(ssl offloading), θα προσφέρει υψηλή διαθεσιμότητα προστατεύοντας από βλάβες του hardware (load balancing) αλλά θα είναι και ιδιαίτερα ασφαλές λόγω τις αποθήκευσης των ρυθμίσεων του σε διαφορετικό μη προσβάσιμο από το Internet σύστημα (configuration storage server).

- **Ενεργοποίηση προστασίας στον Διακομιστή (Local Firewall)**

Για την προστασία του διακομιστή από το εσωτερικό δίκτυο θα ενεργοποιηθεί τοπικό firewall στο λειτουργικό σύστημα του διακομιστή ώστε επιτρέπει τον περιορισμό πρόσβασης σε συγκεκριμένες θύρες μεγιστοποιώντας την ασφάλεια και την ανοχή σε διάφορες δικτυακές επιθέσεις.

- **Ενεργοποίηση προστασίας στο Δίκτυο (Network Firewall)**

Ακόμη, προτείνεται να εγκατασταθεί και ένα τείχος προστασίας firewall σε επίπεδο δικτύου το οποίο να αποκόπτει οποιαδήποτε επικοινωνία με τον διακομιστή εκτός συγκεκριμένων θυρών για την πρόσβαση στην Εφαρμογή (π.χ. θύρα 80 και θύρα 443) και την απομακρυσμένη διαχείριση του διακομιστή.

- **Προστασία από δικτυακές επιθέσεις Άρνησης Υπηρεσίας (Denial of Service)**

Για την προστασία από επιθέσεις τύπου Denial of Service στην ιστοσελίδα της Εφαρμογής ηλεκτρονικής διαχείρισης μετεγγραφών, συνίσταται η χρήση εφαρμογών Web Application Firewalls, τα οποία ελέγχουν το περιεχόμενο της εισερχόμενης δικτυακής κίνησης στους διακομιστές (Web Servers) και φιλτράρουν κατάλληλα τις σχετικές επιθέσεις.

Προστασία Βάσης Δεδομένων

Ένα σημαντικό τμήμα της υποδομής της Εφαρμογής Ηλεκτρονικής Διαχείρισης Μετεγγραφών είναι η τοπική Βάση Δεδομένων (ΒΔ) στην οποία θα καταχωρίζονται οι αιτήσεις για μετεγγραφή. Για την υλοποίηση της ΒΔ προτείνεται η αξιοποίηση του αξιόπιστου συστήματος διαχείρισης βάσεων δεδομένων Microsoft SQL Server για τους ίδιους λόγους που προαναφέρθηκαν σχετικά με την επιλογή του λειτουργικού συστήματος Microsoft Windows Server. Η προστασία της τοπικής Βάσης Δεδομένων είναι υψίστης σημασίας για την ασφάλεια και αξιοπιστία της όλης Εφαρμογής. Ένας από τους βασικούς σχετικούς κινδύνους είναι ο κίνδυνος απόκτησης μη εξουσιοδοτημένης πρόσβασης στην Βάση, ο οποίος αντιμετωπίζεται με την ελεγχόμενη πρόσβαση.

- **Ελεγχόμενη πρόσβαση στην τοπική Βάση Δεδομένων**

Η ελεγχόμενη πρόσβαση στην τοπική Βάση Δεδομένων (ΒΔ) έχει να κάνει αφενός με τη δημιουργία λογαριασμού χρηστών και τον περιορισμό εξουσιοδότησης, καθώς και τον αποκλεισμό πρόσβασης στην τοπική ΒΔ απομακρυσμένα. Το δεύτερο μέτρο αφορά τον κάθε είδος αποκλεισμό πρόσβασης στη ΒΔ απομακρυσμένα Κατά την εγκατάσταση της ΒΔ προτείνεται να γίνουν ειδικές ρυθμίσεις ώστε να γίνεται εφικτή η πρόσβαση μόνο τοπικά από τον διακομιστή καθώς και η ρύθμιση των κανόνων του firewall (βλ. παραπάνω) για την αποτροπή της απομακρυσμένης πρόσβασης και σε δικτυακό επίπεδο.

Φυσική Ασφάλεια και Διαδικασίες Λήψης Αντιγράφων Ασφαλείας

Με τη διαδικασία λήψης αντιγράφων εξασφαλίζεται σε μέγιστο βαθμό η ανάκτηση δεδομένων της εφαρμογής και των χρηστών σε περιπτώσεις απώλειας δεδομένων. Κατάσταση απώλειας δεδομένων μπορεί να προκύψει:

- Από κατάσταση σφάλματος στα μέσα αποθήκευσης του διακομιστή (Σκληροί Δίσκοι)
- Από εσφαλμένη διαγραφή αρχείων
- Από διακοπή παροχής ρεύματος που μπορεί να συνοδευτεί από σφάλμα στα μέσα αποθήκευσης
- Από φυσική καταστροφή του χώρου φιλοξενίας του υλικού (H/W) της εφαρμογής (διακομιστές, βάσεις δεδομένων, κτλ.)

Επιβάλλεται η σωστά σχεδιασμένη διαδικασία λήψης αντιγράφων και ασφαλής αποθήκευσης δεδομένων τόσο σε ειδικά διαμορφωμένες αποθηκευτικές μονάδες με προστασία από λάθη εγγραφής και αστοχίας υλικού (π.χ. συστοιχίες δίσκων με RAID 5) όσο και σε μεταφερόμενες μονάδες (μαγνητικές ταινίες), οι οποίες θα αποθηκεύονται σε ξεχωριστό ασφαλές μέρος (εντός της ΕΔΕΤ ΑΕ). Η διαδικασία λήψης αντιγράφων θα πρέπει να πραγματοποιείται αυτόματα και σε τακτά χρονικά διαστήματα ώστε να ελαχιστοποιείται η απώλεια δεδομένων στην περίπτωση σφαλμάτων και φυσικών καταστροφών (λήψη αντιγράφων ασφαλείας σε εξωτερικές μονάδες τουλάχιστον 1 φορά την ημέρα). Τα δεδομένα τα οποία θεωρούνται ως απαραίτητα για τη λήψη

αντιγράφων ασφαλείας είναι η Βάση Δεδομένων της Εφαρμογής ηλεκτρονικής διαχείρισης μετεγγραφών και η Βάση Δεδομένων των Χρηστών του Συστήματος.

Για την αποφυγή φυσικών καταστροφών στο χώρο φιλοξενίας του εξοπλισμού της Εφαρμογής (Datacenter ΕΔΕΤ ΑΕ) επιβάλλεται η ύπαρξη και χρήση κατάλληλων μηχανισμών πυρασφάλειας (αισθητήρων πυρός και ειδικού μηχανισμού κατάσβεσης για Datacenter) καθώς και εναλλακτική παροχή ενέργειας (συστοιχίες UPS με δυνατότητα ηλεκτρικής τροφοδότησης για ικανό χρονικό διάστημα ώστε να αποκατασταθεί η βλάβη ή να μεταφερθεί η Εφαρμογή αλλού).

Η φυσική ασφάλεια μπορεί να επιτευχθεί τοποθετώντας φυσικούς φραγμούς γύρω από τους χώρους των εγκαταστάσεων του συστήματος ηλεκτρονικής διαχείρισης μετεγγραφών . Κάθε τέτοιος φυσικός φραγμός αποτελεί τμήμα μίας φυσικής περιμέτρου, η οποία αυξάνει το παρεχόμενο επίπεδο ασφαλείας. Οι εγκαταστάσεις του πληροφοριακού συστήματος θα πρέπει να βρίσκονται εντός μίας τέτοιας περιμέτρου ασφαλείας.

Η περίμετρος ασφαλείας αποτελείται από σύνολο φυσικών φραγμών όπως τοίχους, εισόδους με

συσκευές ελέγχου κάρτας ή με ύπαρξη προσωπικού φύλαξης κ.τ.λ. Οι ακόλουθες οδηγίες θα πρέπει να λαμβάνονται υπ’ όψιν και να εφαρμόζονται:

- Η περίμετρος ασφαλείας θα πρέπει να είναι ορισμένη με ακρίβεια.
- Η περίμετρος κτιρίου ή χώρων που περιέχουν στοιχεία του πληροφοριακού συστήματος θα πρέπει να είναι επαρκής από φυσικής απόψεως (δηλ. δεν θα πρέπει να υπάρχουν κενά και σημεία όπου να είναι εφικτή η διείσδυση). Οι εξωτερικοί τοίχοι της εγκατάστασης θα πρέπει να είναι στιβαρής κατασκευής και όλες οι είσοδοι θα πρέπει να έχουν την κατάλληλη προστασία ενάντια σε μη εξουσιοδοτημένη πρόσβαση π.χ. με μηχανισμούς ασφαλείας, μπάρες, συναγερμούς, κλειδαριές ασφαλείας κ.τ.λ.
- Οι επισκέπτες του χώρου του συστήματος θα πρέπει να καταγράφονται και να συνοδεύονται.
- Ύπαρξη προσωπικού ελέγχου στην είσοδο ή άλλα μέτρα ελέγχου της φυσικής πρόσβασης στις εγκαταστάσεις της ΕΔΕΤ ΑΕ θα πρέπει να έχουν υλοποιηθεί. Η είσοδος στις εγκαταστάσεις θα πρέπει να επιτρέπεται μόνο σε εξουσιοδοτημένο προσωπικό.
- Το προσωπικό και οι επισκέπτες θα πρέπει να φέρουν κατάλληλα αναγνωριστικά πινακίδια.

– Οι φυσικοί φραγμοί θα πρέπει εάν είναι αναγκαίο να εκτείνονται από το πραγματικό πάτωμα έως την πραγματική οροφή ώστε να αποτραπεί μη εξουσιοδοτημένη πρόσβαση ή βλάβη από φυσικά αίτια (όπως από φωτιά ή πλημμύρα).

Η δικτυακή καλωδίωση θα πρέπει να εγκαθίσταται και να συντηρείται από ειδικευμένους μηχανικούς για να εξασφαλίζεται η ακεραιότητα τόσο της καλωδίωσης όσο και των επιτοίχιων υποδοχών. Όποιες επιτοίχιες δικτυακές υποδοχές θα πρέπει να σφραγίζονται και να γίνεται επίσημη καταγραφή της καταστάσεώς τους. Η δικτυακή καλωδίωση παραμένει ευπρόσβλητος στόχος αφού σε πολλές περιπτώσεις είναι εκτεθειμένη και απροστάτευτη. Η ασφάλεια της δικτυακής καλωδίωσης πρέπει να αναθεωρείται κατά τη διάρκεια όποιων αναβαθμίσεων ή αλλαγών σε υπολογιστικό υλικό ή εγκαταστάσεις. Η ασφάλεια της καλωδίωσης πρέπει να λαμβάνεται υπόψη και κατά την αρχική δημιουργία των εγκαταστάσεων, αλλά και ακολούθως όποτε λαμβάνουν χώρα αναβαθμίσεις υλικού. Ο εξοπλισμός θα πρέπει να συντηρείται σωστά για να εξασφαλίζεται η συνέχεια στη διαθεσιμότητα του και η ακεραιότητά του.

Σχέδιο Ανάκαμψης σε Περιπτώσεις Φυσικών Καταστροφών (Disaster Recovery)

Σε περίπτωση φυσικής καταστροφής του χώρου φιλοξενίας της Εφαρμογής ηλεκτρονικής διαχείρισης μετεγγραφών (Datacenter ΕΔΕΤ στο κτίριο του Εθνικού Ιδρύματος Ερευνών), το οποίο θα συνεπάγεται και καταστροφή του βασικού εξοπλισμού και απώλειας δεδομένων, συνίσταται η ύπαρξη κατάλληλου εναλλακτικού χώρου και υποδομών για την άμεση φιλοξενία της Εφαρμογής. Η μετάπτωση στη νέα υποδομή θα γίνεται άμεσα καθώς εκεί θα υπάρχει όμοια διάταξη

(identical configuration) που θα επιτρέπει την απρόσκοπτη λειτουργία της εφαρμογής. Το σχέδιο ανάκαμψης αφορά τα εφεδρικά αντίγραφα δεδομένων και τις εφεδρικές εγκαταστάσεις του συστήματος. Τα εφεδρικά αντίγραφα δεδομένων πρέπει να λαμβάνονται και να τηρούνται από αρμόδια στελέχη της ΕΔΕΤ ΑΕ και να μη διαβιβάζονται σε εξωτερικούς φορείς (πχ. προμηθευτές, συντηρητές). Τα εφεδρικά αντίγραφα πρέπει να απολαμβάνουν του ίδιου επιπέδου προστασίας με τα εν ενεργεία δεδομένα και να φυλάσσονται σε κατάλληλους χώρους που τα προστατεύουν από

φυσικούς και κλιματολογικούς παράγοντες. Επίσης προτείνεται να υπάρχουν εφεδρικοί χώροι εγκατάστασης που καλύπτουν τα βασικά πληροφοριακά συστήματα της εφαρμογής. Ως πρώτη επιλογή για την εγκατάσταση Disaster Recovery Site (DRS) προτείνεται άλλος χώρος της ΕΔΕΤ (Datacenter στο κτίριο Υπουργείου Παιδείας). Στον εφεδρικό χώρο θα εγκατασταθεί μόνιμα ο απαραίτητος εξοπλισμός για την παροχή των υπηρεσιών του συστήματος ηλεκτρονικής Διαχείρισης μετεγγραφών. Στο πλαίσιο αυτό θα συνταχθεί κατάλογος με τον απαραίτητο εξοπλισμό που πρέπει να διατεθεί για την εγκατάσταση και λειτουργία στο νέο χώρο. Ο εφεδρικός χώρος θα διαθέτει επαρκείς εγκαταστάσεις παροχής ηλεκτρικής ενέργειας, καθώς και γραμμές τηλεπικοινωνιών. Ο εφεδρικός χώρος θα πληροί τις προϋποθέσεις που προδιαγράφονται για τη φυσική ασφάλεια που αναφέρονται παραπάνω.

Ασφαλής Επικοινωνία Διεπαφής με το Χρήστη

Η ασφαλής επικοινωνία μεταξύ της διεπαφής της εφαρμογής και τον χρήστη περιλαμβάνει την κρυπτογράφηση δεδομένων και παραμέτρων χρήστη καθώς και την αυθεντικοποίηση χρήστη. Η αυθεντικοποίηση και κρυπτογράφηση γίνεται μέσω Secure Sockets Layer (SSL) και Ψηφιακών Πιστοποιητικών.

- **Επικοινωνία μέσω Secure Sockets Layer (SSL)**

Η επικοινωνία μέσω SSL πραγματοποιείται από την πλευρά του χρήστη μέσω του προγράμματος περιήγησης (browser) ενώ από την πλευρά του εξυπηρετητή ιστού (web server) απαιτείται κατάλληλη ρύθμιση, και δημιουργία κατάλληλου ψηφιακού πιστοποιητικού.

Το πρωτόκολλο SSL έχει σχεδιαστεί για να παρέχει απόρρητη επικοινωνία μεταξύ δύο συστημάτων, από τα οποία το ένα λειτουργεί ως client και το άλλο ως server. Η εξασφάλιση του απορρήτου γίνεται με την κρυπτογράφηση όλων των μηνυμάτων στο επίπεδο SSL Record Protocol. Παρέχει, επιπλέον, υποχρεωτική πιστοποίηση της ταυτότητας του server και προαιρετικά της ταυτότητας του client, μέσω έγκυρων πιστοποιητικών από έμπιστες Αρχές Έκδοσης Πιστοποιητικών (Certificates Authorities). Υποστηρίζει πληθώρα μηχανισμών κρυπτογράφησης και ψηφιακών υπογραφών για αντιμετώπιση όλων των διαφορετικών αναγκών. Τέλος, εξασφαλίζει την ακεραιότητα των δεδομένων, εφαρμόζοντας την τεχνική των Message Authentication Codes

(MACs), ώστε κανείς να μην μπορεί να αλλοιώσει την πληροφορία χωρίς να γίνει αντιληπτός. Όλα τα παραπάνω γίνονται με τρόπο διαφανή και απλό.

- **Εγγραφή και Πιστοποίηση Χρηστών και Ταυτοποίηση χρηστών**

Η ταυτοποίηση χρηστών αναφέρεται στον έλεγχο εισόδου στην εφαρμογή για διαπιστευμένους χρήστες μόνο, οι οποίοι μπορεί να είναι οι φοιτητές που έχουν εγγραφεί στην εφαρμογή. Ο έλεγχος εισόδου (login) θα γίνεται μέσω του αναγνωριστικού χρήστη (username) (μοναδικό για κάθε χρήστη) και του κωδικού πρόσβασης (password), τα οποία έχουν δημιουργηθεί και καταχωρισθεί στον χρήστη κατά τη διαδικασία εγγραφής και πιστοποίησης. Οι λειτουργικές λεπτομέρειες σχετικά με τη διαχείριση πρόσβασης χρηστών και με την πολιτική ασφάλειας και ορθής χρήσης των κωδικών αναλύονται στην επόμενη ενότητα της μελέτης. Ο κάθε χρήστης της εφαρμογής θα είναι υπεύθυνος για τη διαφύλαξη των στοιχείων πρόσβασης στην εφαρμογή ηλεκτρονικής διαχείρισης μετεγγραφών.

Για να εγγραφεί ο φοιτητής πρέπει να εισάγει τα στοιχεία : Όνομα, Επώνυμο, Πατρώνυμο και Μητρώνυμο (όπως ακριβώς αναγράφονται στην αστυνομική ταυτότητα) καθώς και τον Κωδικό των Πανελληνίων Εξετάσεων. Εφόσον τα στοιχεία που εισήγαγε ο χρήστης είναι σωστά, η εφαρμογή θα εντοπίζει το τμήμα στο οποίο έχει εισαχθεί ο φοιτητής και το εμφανίζει. Ο φοιτητής θα πρέπει στη συνέχεια να συμπληρώσει τα πεδία: Όνομα Χρήστη, Κωδικός Πρόσβασης, Επιβεβαίωση Κωδικού Πρόσβασης, e-mail και κινητό τηλέφωνο (απαιτείται στη συνέχεια για την πιστοποίηση του χρήστη) και να ζητήσει τη δημιουργία λογαριασμού. Στη συνέχεια θα εμφανίζεται στο φοιτητή μήνυμα ότι ο λογαριασμός του δημιουργήθηκε επιτυχώς και ότι εστάλησαν οδηγίες ενεργοποίησης του λογαριασμού στη διεύθυνση e-mail που δήλωσε. Εάν ο φοιτητής δεν λάβει το e-mail ενεργοποίησης θα πρέπει να επικοινωνήσει με το Γραφείο Αρωγής Χρηστών. Το e-mail που θα λαμβάνει ο φοιτητής θα περιέχει τον υπερ-σύνδεσμο στον οποίο θα πρέπει να πατήσει, ώστε να ενεργοποιηθεί ο λογαριασμός του. Μόλις ο φοιτητής συνδεθεί για πρώτη φορά με το λογαριασμό του στην εφαρμογή θα ενημερωθεί ότι δεν έχει πιστοποιηθεί. Για να πιστοποιηθεί θα πρέπει να

ενεργοποιήσει την διαδικασία Πιστοποίησης Λογαριασμού εισάγοντας ένα κωδικό που θα λαμβάνει με sms στο κινητό του τηλέφωνο στη φάση εγγραφής.

- **Έξοδος από την Εφαρμογή**

Μετά από επιτυχημένη ταυτοποίηση του χρήστη, θα δημιουργείται η κατάλληλη σύνοδος (με συγκεκριμένη μέγιστη χρονική διάρκεια) στην εφαρμογή (web session), η οποία θα παρέχει στον χρήστη τη δυνατότητα να χρησιμοποιήσει την εφαρμογή χωρίς περαιτέρω ταυτοποίηση. Όταν ο χρήστης εξέλθει από την εφαρμογή (logout) ή απενεργοποιηθεί (time out) μετά από κάποιο χρόνο αδράνειας θα πρέπει να επανεισάγει τους κωδικούς πρόσβασης για να μπορέσει να χρησιμοποιήσει την εφαρμογή.

Διαχείριση Κωδικών Πρόσβασης

- **Γενικοί Κανόνες**

Οι κωδικοί είναι μια σημαντική παράμετρος της ασφάλειας υπολογιστών. Είναι η πρώτη γραμμή προστασίας για τους λογαριασμούς χρηστών. Ένας ατυχώς επιλεγμένος κωδικός μπορεί να έχει ως αποτέλεσμα την έκθεση ολόκληρου του δικτύου του οργανισμού.

- **Πολιτική Ασφάλειας Κωδικών**

Σχετικά με την πολιτική ασφάλειας και ορθής χρήσης των κωδικών προτείνονται τα ακόλουθα:

– Να διασφαλίζεται ότι οι χρήστες που πρέπει να έχουν τους δικούς τους προσωπικούς κωδικούς πρόσβασης θα πρέπει να προμηθεύονται αρχικά ένα προσωρινό ασφαλή κωδικό πρόσβασης τον οποίο θα είναι υποχρεωμένοι να τον αλλάξουν αμέσως μετά. Σε περίπτωση που ένας χρήστης ξεχάσει των κωδικό πρόσβασής του και πρέπει να του δοθεί ένας τέτοιος προσωρινός κωδικός, αυτό θα πρέπει να γίνει αφού ελεγχθεί η ταυτότητα του χρήστη.
– Πρέπει να γίνεται επιβεβαίωση του κωδικού πρόσβασης όταν το τερματικό είναι ενεργό για πάρα πολύ ώρα.
– Οι προσωρινοί κωδικοί πρόσβασης θα πρέπει να δίδονται στους χρήστες με ασφαλή τρόπο.

- Οι κωδικοί πρόσβασης δεν θα πρέπει ποτέ να αποθηκεύονται σε υπολογιστικά συστήματα σε μη προστατευμένη μορφή.
- Οι κωδικοί δεν πρέπει να εισάγονται σε μηνύματα ηλεκτρονικής αλληλογραφίας ή άλλες μορφές ηλεκτρονικής επικοινωνίας.
- Όλοι οι κωδικοί επιπέδου χρήστη και επιπέδου συστήματος πρέπει να συμμορφώνονται με τις γενικές οδηγίες δημιουργίας ισχυρών κωδικών (βλέπε παρακάτω).
- Οι χρήστες πρέπει να ακολουθούν ορθές πρακτικές ασφάλειας κατά την επιλογή και χρήση κωδικών. Όλοι οι χρήστες συμβουλεύονται να:
    - διατηρούν τους κωδικούς εμπιστευτικούς
    - αποφεύγουν τη σημείωση των κωδικών σε χαρτί, εκτός και αν αυτό μπορεί να αποθηκευτεί με ασφάλεια.
    - αλλάζουν κωδικό όποτε υπάρχει οποιαδήποτε ένδειξη πιθανής έκθεσης συστήματος ή κωδικού
    - επιλέγουν ποιοτικούς κωδικούς (σύμφωνα με τις γενικές οδηγίες δημιουργίας ισχυρών κωδικών – βλέπε παρακάτω) με ελάχιστο μήκος έξι χαρακτήρες οι οποίοι είναι:
        -
        - εύκολοι στη απομνημόνευση
        - δε βασίζονται σε κάτι το οποίο μπορεί να μαντέψει ή να ανακτήσει εύκολα κάποιος άλλος χρησιμοποιώντας πληροφορία σχετική με το χρήστη, π.χ. ονόματα, αριθμούς τηλεφώνου, ημερομηνίες γεννήσεως, κτλ.
        - δεν έχουν συνεχόμενους όμοιους χαρακτήρες ή ομάδες μόνο αριθμητικών ή μόνο αλφαβητικών χαρακτήρων
    - αποφεύγουν την εισαγωγή κωδικών σε αυτοματοποιημένες διαδικασίες σύνδεσης, π.χ. αποθηκευμένους σε μακροεντολές ή πλήκτρα συντομεύσεων
    - μη μοιράζονται τους κωδικούς που χρησιμοποιούνται, συμπεριλαμβανομένων και των βοηθών ή των γραμματέων
    - Να μην αποκαλύπτεται κωδικός από το τηλέφωνο σε ΚΑΝΕΝΑΝ

- Να μην αποκαλύπτεται κωδικός σε μήνυμα ηλεκτρονικής αλληλογραφίας
- Να μη γίνεται αναφορά στον κωδικό μπροστά σε άλλους
- Να μην υποδηλώνεται η μορφή του κωδικού (π.χ. «το οικογενειακό μου όνομα»)
- Να μην αποκαλύπτεται κωδικός σε ερωτηματολόγια ή φόρμες ασφάλειας
- Να μην μοιράζεται κωδικός με μέλη της οικογένειας.
- Να μην αποκαλύπτεται κωδικός σε συνεργάτες κατά τη διάρκεια διακοπών

3. Διαχείριση Εξοπλισμού και Λογισμικού Εφαρμογής

Η Εφαρμογή Ηλεκτρονικής Διαχείρισης Μετεγγραφών έχει συγκεκριμένες απαιτήσεις τόσο σε λογισμικό (Λειτουργικό Σύστημα, Web Server, Application Server, Βάση Δεδομένων) όσο και υλικό (εξυπηρετητές, firewall, συστήματα backup, κτλ.). Η ορθή και αδιάλειπτη λειτουργία της Εφαρμογής προϋποθέτει τη δυνατότητα διαχείρισης του παραπάνω εξοπλισμού και λογισμικού από ομάδα ατόμων με κατάλληλη τεχνική κατάρτιση, των οποίων οι αρμοδιότητες θα περιλαμβάνουν:

- Τον έλεγχο για τη σωστή λήψη αντιγράφων ασφαλείας
- Τον έλεγχο για τυχόν σφάλματα υλικού στον εξοπλισμό
- Τον έλεγχο για τυχόν σφάλματα λογισμικού
- Τον έλεγχο για τη σωστή απόδοση της Εφαρμογής (π.χ. χρόνοι απόκρισης Εφαρμογής, Βάσης Δεδομένων, κτλ)
- Διαδικασίες συντήρησης λογισμικού και εξοπλισμού

Οι παραπάνω διαδικασίες θα πρέπει να γίνονται με τρόπο ασφαλή. Αυτό περιλαμβάνει:

- Την ελεγχόμενη πρόσβαση στο λειτουργικό των διακομιστών και το λογισμικό της εφαρμογής μόνο σε εξουσιοδοτημένα άτομα (SSH με χρήση κλειδιού δημόσιας κρυπτογράφησης) και πρόσβαση μόνο από εμπιστευόμενα δίκτυα (Χρήση VPN, εσωτερικού δικτύου ΕΔΕΤ)
- Την καταγραφή της πρόσβασης και των ενεργειών χρήστη σε επίπεδο λειτουργικού

- Τον αποκλεισμό πρόσβασης από ανοιχτό δίκτυο (Internet) στους διακομιστές που φιλοξενούν την Εφαρμογή

Σημαντικό ρόλο θα παίξει η αυτόματη καταγραφή περιστατικών. Η καταγραφή περιστατικών (logs) που σχετίζονται με θέματα ασφάλειας θα πρέπει να πραγματοποιείται και να κρατείται για μία συμφωνημένη περίοδο, προκειμένου να βοηθήσει σε μελλοντικές έρευνες και παρακολούθηση του ελέγχου πρόσβασης. Η καταγραφή σε επίπεδο συστήματος θα πρέπει τουλάχιστον να περιλαμβάνει:

- IDs των χρηστών.
- ημερομηνίες και ώρες σύνδεσης και αποσύνδεσης στο σύστημα.
- ταυτότητα του τερματικού ή τοποθεσία αν είναι εφικτό (διεύθυνση απομακρυσμένου υπολογιστή).
- εγγραφές επιτυχημένων και απορριπτέων προσπαθειών (αποτυχημένες προσπάθειες, καταπατήσεις της πολιτικής πρόσβασης) προειδοποιήσεις ή αποτυχίες του συστήματος
- προειδοποιήσεις από την διαχείριση του δικτύου
- προειδοποιήσεις από τον εντοπισμό εισβολής στα ιδιόκτητα συστήματα.
- λάθη και χρόνοι εκκίνησης και διακοπής της λειτουργίας του συστήματος.

Συγκεκριμένες καταγραφές ελέγχων πρέπει να απαιτηθεί να αρχειοθετηθούν, εξαιτίας της απαίτησης για συλλογή αποδεικτικών στοιχείων.

4. Σύνοψη

Στην παρούσα μελέτη παρουσιάστηκαν συνοπτικά οι βασικές πολιτικές ασφάλειας που προτείνονται για την Εφαρμογή Διαχείρισης Μετεγγραφών. Οι χρήστες και οι διαχειριστές πρέπει να εκπαιδευτούν και να ενημερώνονται, σχετικά με τις διαδικασίες ασφάλειας προκειμένου να ελαχιστοποιηθούν οι πιθανοί κίνδυνοι που απειλούν την Εφαρμογή. Επίσης ειδικότερα οι διαχειριστές πρέπει να μεριμνούν για την συνεχή ενημέρωση και αναβάθμιση των διαφόρων τμημάτων λογισμικού (λειτουργικό σύστημα, Βάση Δεδομένων, λογισμικό εφαρμογής, κτλ.) με σκοπό την άμεση αντιμετώπιση απειλών που μπορεί να προκύψουν από κενά ασφαλείας ή λειτουργικά σφάλματα. Για το λόγο αυτό προτείνεται ο ορισμός ενός στελέχους (υπεύθυνος ασφάλειας) ως υπεύθυνο να δίδει κατευθύνσεις σε χρήστες και διαχειριστές του συστήματος και να

τους επισημαίνει τις ευθύνες τους και τις διαδικασίες που θα πρέπει να τηρούν, και να ελέγχει την συνολική ασφάλεια της εφαρμογής.