4 – Διαδικασίες Ασφάλειας

Εθνική Σχολή Δημόσιας Διοίκησης & Αυτοδιοίκησης
Απρίλιος 2021

Ενότητες

- Ελεγχόμενη Πρόσβαση των Χρηστών στο Δίκτυο (Network Access Control)
- Ελεγχόμενη Πρόσβαση Ιστότοπου (Website Access Control)
- Διαδικασία Διαχείρισης Αλλαγών (Change Management Procedure)
- Σχέδιο Συνέχισης Λειτουργίας (Business Continuity Plan)

Διαδικασίες Ασφάλειας

- Αναλυτική περιγραφή επιλεγμένων προτεινόμενων διαδικασιών ασφάλειας στο πλαίσιο εφαρμογής του σχεδίου ασφάλειας ενός υποθετικού οργανισμού της Δημόσιας Διοίκησης με την ονομασία «**Φορέας**»

Διαδικασίες Ασφάλειας

- Αναλυτικότερα, θα παρουσιαστούν 4 διαδικασίες:
- **Ελεγχόμενη Πρόσβαση στο Εσωτερικό Δίκτυο** (network access control)
- **Ελεγχόμενη Πρόσβαση στον Ιστότοπο** (website access control)
- **Διαδικασία Διαχείρισης Αλλαγών** (change management procedure)
- **Σχέδιο Συνέχισης Λειτουργίας** (business continuity plan)

Ελεγχόμενη Πρόσβαση στο Δίκτυο

- Αποτελεί βασική διαδικασία ασφάλειας για κάθε φορέα του δημοσίου
- Οι περισσότεροι εργαζόμενοι διαθέτουν ηλεκτρονικό υπολογιστή για τη διεκπεραίωση των υπηρεσιακών τους καθηκόντων και τα περισσότερα δεδομένα και οι πληροφορίες βρίσκονται σε **ψηφιακή μορφή**
- Τα αποθηκευμένα δεδομένα στους εξυπηρετητές και στους προσωπικούς υπολογιστές των χρηστών πρέπει να προστατεύονται από τον **κίνδυνο μη εξουσιοδοτημένης πρόσβασης**

Ελεγχόμενη Πρόσβαση στο Δίκτυο

- Η πρόσβαση των χρηστών στο δίκτυο γίνεται μέσω **προσωπικών λογαριασμών**
- Η χορήγηση των συνθηματικών έγκειται στους **γενικούς κανόνες χορήγησης κωδικών** όπως αυτές έχουν αποτυπωθεί στη Μελέτη Ασφάλειας
- Οι χρήστες είναι υποχρεωμένοι να διαφυλάττουν τους **κωδικούς πρόσβασης** των συνθηματικών τους ώστε να αποφευχθούν οι πιθανότητες να αποκαλυφθούν σε μη εξουσιοδοτημένα πρόσωπα

Ελεγχόμενη Πρόσβαση στο Δίκτυο

- Στα περισσότερα ψηφιακά συστήματα οι κωδικοί πρόσβασης αποτελούν την πρώτη δικλείδα ασφαλείας και κατά συνέπεια, είναι σημαντικό η χρήση τους να γίνεται **συνειδητά** και **υπεύθυνα**
- Οι χρήστες δεν πρέπει να μοιράζονται τους λογαριασμούς και τους κωδικούς τους με συναδέλφους, φίλους, γνωστούς ή συγγενείς, ούτε να τους αποκαλύπτουν μέσω τηλεφώνου ή ηλεκτρονικού ταχυδρομείου

Ελεγχόμενη Πρόσβαση στο Δίκτυο

- Οι κωδικοί πρόσβασης θα πρέπει να αλλάζουν σε **τακτικά διαστήματα**, ενώ οι χρήστες των οποίων οι λογαριασμοί ανήκουν σε ομάδες με αυξημένα δικαιώματα, π.χ. διαχειριστές συστημάτων ή εφαρμογών, θα πρέπει να έχουν **ξεχωριστούς κωδικούς** για όλους τους υπόλοιπους λογαριασμούς τους
- Οι χρήστες δεν θα πρέπει να καταγράφουν τους κωδικούς τους σε χαρτί και να το αφήνουν έκθετο στο γραφείο τους

Διαχειριστής

- Ο λογαριασμός **Διαχειριστή** δίνεται σε υπαλλήλους που είναι υπεύθυνοι για την παραμετροποίηση και επίλυση προβλημάτων δικτύου
- Ο λογαριασμός αυτός έχει **πρόσβαση** σε όλους τους φακέλους και σε όλους τους εξυπηρετητές και ηλεκτρονικούς υπολογιστές

Διαχειριστής

- Έχει τη δυνατότητα εγκατάστασης και απεγκατάστασης προγραμμάτων που είναι χρήσιμα για την καλύτερη λειτουργία του δικτύου
- Είναι υπεύθυνος για την εγκατάσταση των νέων εκδόσεων του αντί-ιομορφικού λογισμικού και την ενημέρωση των λειτουργικών συστημάτων
- Ο Διαχειριστής έχει επίσης πλήρη έλεγχο σε όλες τις εφαρμογές

Υπάλληλος

- Ο λογαριασμός δίδεται σε όλους τους **υπαλλήλους** που θα διαθέτουν ηλεκτρονικό υπολογιστή
- Τα **δικαιώματα** του είναι περιορισμένα όσον αφορά την εισαγωγή και επεξεργασία αρχείων
- Ο **έλεγχος** στα τοπικά αρχεία του υπολογιστή του είναι πλήρης αλλά δεν θα υπάρχει δυνατότητα εγκατάστασης εφαρμογών λογισμικού ή περιφερειακών συσκευών

Συνθηματικά

- Κάθε λογαριασμός έχει μοναδική ταυτότητα και αποτελείται από το Όνομα Χρήστη και τον Κωδικό Πρόσβασης (**συνθηματικά**)
- Αποδίδεται στον κάθε χρήστη ξεχωριστά και αυτός θα είναι υπεύθυνος για την διαφύλαξη του

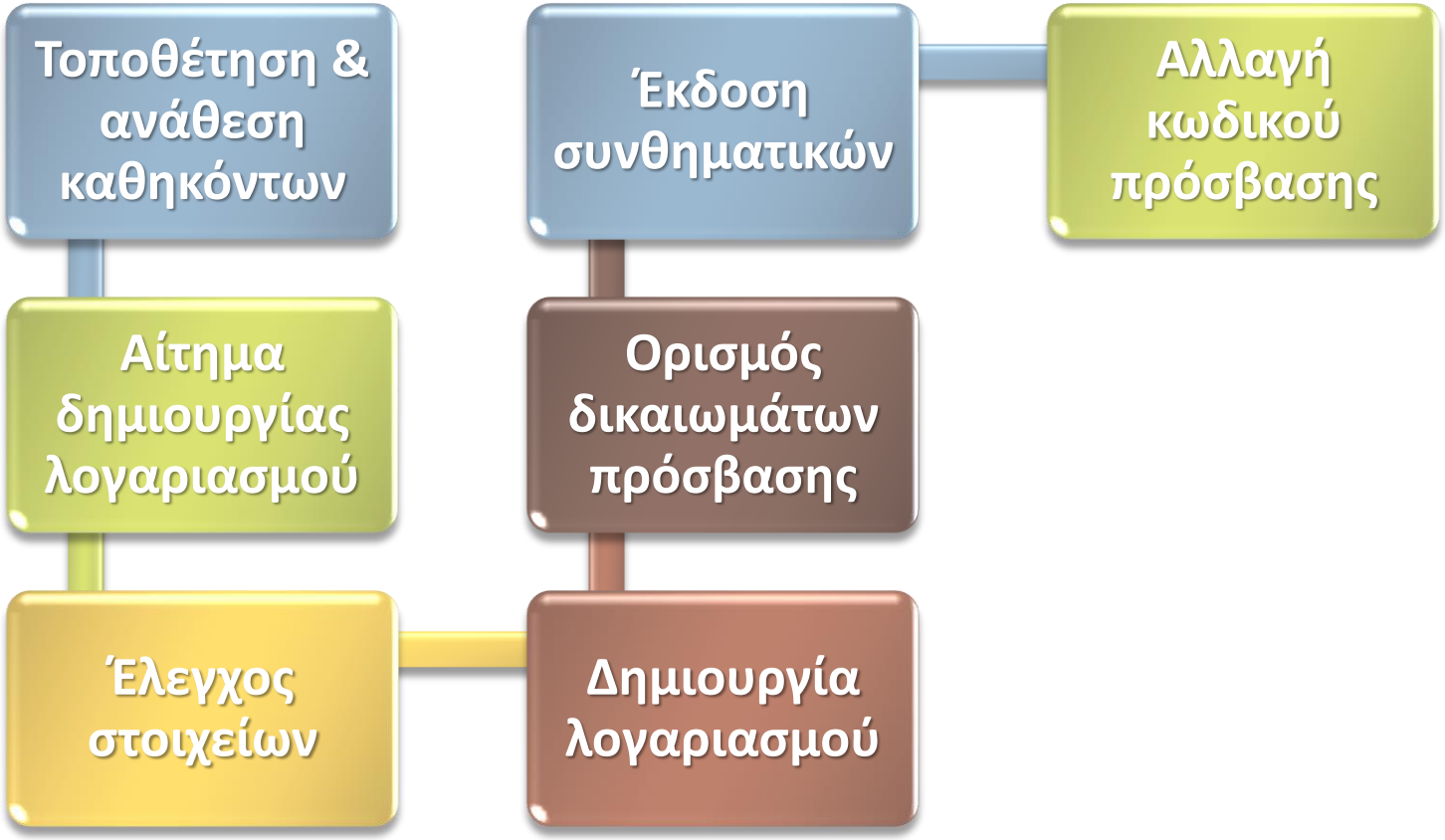
Συνθηματικά

- Η απόδοση του κάθε λογαριασμού στον αντίστοιχο χρήστη βοηθά στην ανεύρεση του χωρίς την εμφάνιση του αληθινού του ονόματος και της ιεραρχικής του θέσης
- Ο κάθε λογαριασμός πρέπει να μην παρέχει ενδείξεις των προνομίων του χρήστη, να μην παρέχει ενδείξεις της ιεραρχικής του θέσης και να μην περιέχει το Ονοματεπώνυμο του

Διαδικασία Ανάκτησης Συνθηματικών

- Εάν έχει ξεχάσει το **Όνομα Χρήστη**, ο Διαχειριστής το αναζητά μέσα από τη βάση χρηστών του συστήματος και ενημερώνει τον χρήστη
- Εάν έχει ξεχάσει τον **Κωδικό Πρόσβασης**, ο Διαχειριστής προχωρά στην αρχικοποίηση του κωδικού πρόσβασης του χρήστη, διαγράφοντας τον παλιό κωδικό (που ούτε ο ίδιος δεν τον γνωρίζει) και ορίζοντας έναν καινούργιο
- Στη συνέχεια ενημερώνει το χρήστη για τον νέο κωδικό

Περιγραφή Διαδικασίας Ελεγχόμενης Πρόσβασης στο Δίκτυο



Ελεγχόμενη Πρόσβαση Ιστότοπου

- Η **Διαδικασία Ελεγχόμενης Πρόσβασης στον Ιστότοπο** του Φορέα (**Website Access Control**) στοχεύει στη διασφάλιση εξουσιοδοτημένης πρόσβασης στο πολυμεσικό περιεχόμενο του οργανισμού
- Ο ιστότοπος του φορέα, εκτός του ενημερωτικού χαρακτήρα, θα παρέχει και ηλεκτρονικές υπηρεσίες προς τους πολίτες

Ελεγχόμενη Πρόσβαση Ιστότοπου

- Η διαδικασία ακολουθείται για την
  - δημιουργία νέου λογαριασμού χρήστη
  - ταυτοποίηση και αυθεντικοποίηση του χρήστη κάθε φορά που επιθυμεί να συνδεθεί στον ιστότοπο

Ρόλοι

- Με τη διαδικασία ελεγχόμενης πρόσβασης στον ιστότοπο ταυτοποιούνται και αυθεντικοποιούνται οι πολίτες που επιθυμούν να αξιοποιήσουν τις ηλεκτρονικές υπηρεσίες του φορέα
- Διαχωρισμός των χρηστών και οριοθέτηση των δικαιωμάτων τους

Ρόλοι

- Δύο επίπεδα πρόσβασης
  - Πολίτες
  - Διαχειριστές του συστήματος

- Ανάλογα με τα δικαιώματα που έχει κάθε χρήστης, έχει και τις ανάλογες δυνατότητες πρόσβασης στο σύστημα

Διαχειριστής

- Ο χρήστης **Διαχειριστής** διαθέτει πλήρη δικαιώματα πρόσβασης στο σύστημα διαχείρισης περιεχομένου, με δυνατότητα επεξεργασίας των ιστοσελίδων και των αρχείων του ιστότοπου, καθώς και του προφίλ των χρηστών
- Παρακολουθεί και ελέγχει την ομαλή λειτουργία του συστήματος και επικοινωνεί άμεσα με τον **Υπεύθυνο Ασφάλειας** του φορέα σε περίπτωση περιστατικού ασφάλειας

Πολίτης

- Ο χρήστης με τα δικαιώματα του **πολίτη** μπορεί να πλοηγηθεί στον ιστότοπο και να χρησιμοποιήσει τις παρεχόμενες ηλεκτρονικές υπηρεσίες του φορέα
- Κάθε χρήστης που έχει δημιουργήσει λογαριασμό και του έχει παραχωρηθεί όνομα χρήστη και αντίστοιχος κωδικός, είναι έτοιμος να κάνει χρήση των δικαιωμάτων του προσωπικού του προφίλ

Περιγραφή Διαδικασίας Ελεγχόμενης Πρόσβασης στον Ιστότοπο

Διαδικασία Διαχείρισης Αλλαγών

- Στόχος της **Διαδικασίας Διαχείρισης Αλλαγών (Change Management Procedure)** είναι να εξασφαλιστεί η ύπαρξη τυποποιημένης μεθόδου για τον αποτελεσματικό και αποδοτικό χειρισμό όλων των αλλαγών εξοπλισμού και λογισμικού, προκειμένου να ελαχιστοποιηθούν τυχόν επιπτώσεις στην ποιότητα των παρεχόμενων ηλεκτρονικών υπηρεσιών

Ρόλοι

- Η **Μονάδα Πληροφορικής** θα πρέπει να είναι συνεχώς ενήμερη για όλες τις εξελίξεις σχετικά με τα θέματα αλλαγών εξοπλισμού και λογισμικού, αναλαμβάνοντας την εποπτεία και τον έλεγχο της διαδικασίας
- Οι κρίσιμες αλλαγές εξοπλισμού και λογισμικού απαιτούν επιπλέον την έγκριση του **Υπεύθυνου Ασφάλειας** του φορέα

Ρόλοι

- Με την ολοκλήρωση της αλλαγής θα πρέπει να ενημερωθεί ο **κατάλογος παγίων** του φορέα για την καλύτερη τεκμηρίωση της υλικοτεχνικής υποδομής
- Ο **Υπεύθυνος Παγίων** είναι υπεύθυνος για την καταγραφή και παρακολούθηση των παγίων

Περιγραφή Διαδικασίας

- Οι αλλαγές εξοπλισμού ή λογισμικού του φορέα υλοποιούνται υπό την εποπτεία της **Μονάδας Πληροφορικής**, ανεξαρτήτως μεγέθους ή αξίας της αλλαγής
- Ορίζεται ο **υπεύθυνος διαχειριστής του συστήματος**, ο οποίος οφείλει να επιτηρεί την διαδικασία και να ελέγχει την ομαλή λειτουργία του συστήματος, ενημερώνοντας σχετικά τον **Υπεύθυνο Ασφάλειας**

Διαδικασία Αλλαγής Εξοπλισμού

Διαδικασία Αλλαγής Λογισμικού

Σχέδιο Συνέχισης Λειτουργίας

- Το **Σχέδιο Συνέχισης Λειτουργίας (Business Continuity Plan)** θα πρέπει να λαμβάνει υπόψη τις πλέον πρόσφατες εξελίξεις στην πληροφορική στον βαθμό που επηρεάζουν τη λειτουργία του οργανισμού, συμβάλλοντας σημαντικά στην αποτελεσματική διαχείριση του λειτουργικού κινδύνου που σχετίζεται με κάθε ψηφιακό σύστημα

Σχέδιο Συνέχισης Λειτουργίας

- Το **Σχέδιο Συνέχισης Λειτουργίας (ΣΣΛ)** είναι το έγγραφο που αναφέρεται στα μέτρα, τα οποία εφαρμόζονται σε περιπτώσεις έκτακτης ανάγκης, όπως της καταστροφής ενός υπολογιστικού κέντρου ή την κατάρρευση ενός επιχειρησιακού δικτύου

- Το **Σχέδιο Συνέχισης Λειτουργίας** συμπληρώνει το **Σχέδιο Ασφαλείας**

Σχέδιο Συνέχισης Λειτουργίας

- Περιλαμβάνει μέτρα που στοχεύουν σε:
  - ελαχιστοποίηση διακοπών της κανονικής λειτουργίας
  - περιορισμό της έκτασης των ζημιών και καταστροφών και αποφυγή πιθανής κλιμάκωσης αυτών
  - εκπαίδευση, εξάσκηση και εξοικείωση των εργαζομένων με τις διαδικασίες έκτακτης ανάγκης
  - δυνατότητα γρήγορης αποκατάστασης της ομαλής λειτουργίας
  - ελαχιστοποίηση των οικονομικών επιπτώσεων

Σχέδιο Συνέχισης Λειτουργίας

- Το **Σχέδιο Συνέχισης Λειτουργίας** πρέπει να προσδιορίζει τους πιθανούς κινδύνους και γενικότερα τα κριτήρια που καθορίζουν την κατάσταση ως έκτακτη και επιβάλλουν την ενεργοποίηση του σχεδίου
- Πρέπει να υπάρχουν **σαφείς** και **γραπτές** διαδικασίες που να θέτουν τον φορέα σε κατάσταση έκτακτης ανάγκης και να επιτρέπουν εφαρμογή του σχεδίου

Σχέδιο Συνέχισης Λειτουργίας

- Το **Σχέδιο Συνέχισης Λειτουργίας** πρέπει να περιέχει:
  - κατάσταση με τα μέλη του προσωπικού που θα κληθούν στην περίπτωση καταστροφής
  - τα τηλέφωνα των προμηθευτών υλικού και λογισμικού
  - τα τηλέφωνα των σημαντικών συνεργατών ή αρμόδιων φορέων που μπορούν να συνδράμουν στη συνέχιση της λειτουργίας του

Σχέδιο Συνέχισης Λειτουργίας

- Το **Σχέδιο Συνέχισης Λειτουργίας** θα πρέπει να περιέχει **διαδικασίες** για τον υπολογισμό της ζημιάς από την καταστροφή που συντελέστηκε, ενώ θα πρέπει να περιέχει έναν ρεαλιστικό **χρονοπρογραμματισμό** με σαφή ανάθεση καθηκόντων για την αποκατάσταση της λειτουργίας της Υπηρεσίας

Ρόλοι

- Ο φορέας θα πρέπει να διαθέτει αρμόδια **Μονάδα Πληροφορικής**, λειτουργικά και διοικητικά ανεξάρτητη από τους τελικούς χρήστες των υπηρεσιών πληροφορικής
- Θα πρέπει να διαθέτει **οργανόγραμμα** στο οποίο να απεικονίζονται οι επιχειρησιακές και οργανωτικές ανάγκες της Μονάδας Πληροφορικής και να περιγράφονται με σαφήνεια οι **αρμοδιότητες** των επί μέρους Τομέων που την αποτελούν

Ρόλοι

- Η **Μονάδα Πληροφορικής** θα πρέπει να διαθέτει καταγεγραμμένες και επίσημα εγκεκριμένες **περιγραφές θέσεων εργασίας** στις οποίες θα περιλαμβάνονται οι αρμοδιότητες, οι υπευθυνότητες και οι δεξιότητες που απαιτούνται για κάθε θέση

Ρόλοι

- Ο **Υπεύθυνος Ασφάλειας** θα πρέπει να υποστηρίζεται στο έργο του από εξειδικευμένη ομάδα έμπειρων στελεχών πληροφορικής, οι οποίοι να έχουν ολοκληρωμένη εικόνα για το επίπεδο ασφάλειας του συστήματος και τους κινδύνους που απορρέουν από την ανάπτυξη, ενσωμάτωση και λειτουργία του

Περιγραφή Διαδικασίας

- Ο φορέας θα πρέπει να διαθέτει εγκεκριμένο από τη Διοίκηση **Σχέδιο Συνέχειας Λειτουργίας (ΣΣΛ)** για τα ψηφιακά συστήματα, έτσι ώστε να εξασφαλίζεται η συνέχεια των κρισιμότερων λειτουργιών τους

Περιγραφή Διαδικασίας

- Αρχικά θα πρέπει να εξασφαλιστεί η συνέχεια των εργασιών για τις οποίες υπάρχει διαδικασία λήψης και διαχείρισης αντιγράφων ασφαλείας του λογισμικού, των παραμέτρων λειτουργίας και των δεδομένων, καθώς και η ύπαρξη του αναγκαίου εφεδρικού εξοπλισμού, συσκευών παροχής αδιάλειπτης τάσης, ηλεκτρογεννητριών κ.λπ., στους χώρους λειτουργίας των συστημάτων.

Περιγραφή Διαδικασίας

- Με στόχο την αποτελεσματική και γρήγορη ανάκτηση των δεδομένων και του λογισμικού εφαρμογών, θα πρέπει τα αντίγραφα ασφαλείας να δημιουργούνται με συγκεκριμένες διαδικασίες και με συχνότητα, η οποία να υπαγορεύεται από την κρισιμότητα των πληροφοριών

Περιεχόμενο Σχεδίου Συνέχισης Λειτουργίας

- Κατάταξη των συστημάτων βάση λειτουργικής ανάγκης
- Οργανωτική δομή και αρμοδιότητες στελεχών
- Διαδικασίες εκτίμησης του εύρους της καταστροφής
- Διαδικασίες ενεργοποίησης του ΣΣΛ και κινητοποίησης των ομάδων έκτακτης ανάγκης
- Ενέργειες που εκτελούνται σε επείγουσες καταστάσεις
- Κατάλογος προμηθευτών με τους οποίους υπάρχουν συμβάσεις
- Διαδικασίες που εξασφαλίζουν ότι το ΣΣΛ ενημερώνεται τακτικά
- Διαδικασίες εκπαίδευσης και ενημέρωσης του προσωπικού
- Διαδικασίες εκτέλεσης δοκιμών

Περιγραφή Διαδικασίας

- Οι αναπόφευκτες αλλαγές που συμβαίνουν στα ψηφιακά συστήματα με τη πάροδο του χρόνου απαιτούν τη **περιοδική αναθεώρηση** του ΣΣΛ
- Όπου είναι εφικτό, πρέπει να συνάπτονται **συμφωνίες με τους προμηθευτές** που να περιγράφονται οι διαδικασίες επείγοντος εφοδιασμού με τον απαραίτητο εξοπλισμό

Case Studies

1. Σχεδιάστε μία Διαδικασία Αντιμετώπισης Περιστατικών Παραβίασης Ασφάλειας (Security Incident Management Procedure).

2. Σχεδιάστε μία Διαδικασία Ελεγχόμενης Πρόσβασης στο Ολοκληρωμένο Πληροφοριακό Σύστημα (ΟΠΣ) ενός φορέα της Δημόσιας Διοίκησης.

3. Σχεδιάστε τον κανονισμό ορθής πλοήγησης στο Διαδίκτυο.

4. Σχεδιάστε τον κανονισμό ορθής χρήσης του Ηλεκτρονικού Ταχυδρομείου.

5. Σχεδιάστε τη διαδικασία Καθαρής Επιφάνειας Εργασίας (Clean Desk Policy).

Ευχαριστώ για την προσοχή σας

Ερωτήσεις