ΕΘΝΙΚΟ
ΚΕΝΤΡΟ
ΔΗΜΟΣΙΑΣ
ΔΙΟΙΚΗΣΗΣ &
ΑΥΤΟΔΙΟΙΚΗΣΗΣ

ΕΘΝΙΚΗ ΣΧΟΛΗ ΔΗΜΟΣΙΑΣ ΔΙΟΙΚΗΣΗΣ & ΑΥΤΟΔΙΟΙΚΗΣΗΣ

ΚΣΤ ΣΕΙΡΑ

ΤΜΗΜΑ ΔΙΟΙΚΗΣΗΣ ΥΠΗΡΕΣΙΩΝ ΥΓΕΙΑΣ

Κυβερνοασφάλεια στη Δημόσια Διοίκηση

Θέμα:

Κυβερνοασφάλεια σε Δημόσιο Οργανισμό

Σπουδαστής:
Πακιρτζόγλου Ιωάννης

Διδάσκων:
Κολαΐτης Χρήστος

ΑΘΗΝΑ-2019

Πολιτική Ασφαλείας

1. Παρουσίαση Οργανισμού

Η παρούσα μελέτη αφορά τον οργανισμό «Κέντρο Πολιτισμού Ίδρυμα Σταύρος Νιάρχος Α.Ε.» (εφεξής ο οργανισμός) είναι μια ανώνυμη εταιρεία μη κερδοσκοπικού σκοπού με τριπλή υπόσταση.

Πιο συγκεκριμένα, ο οργανισμός ιδρύεται για να λειτουργεί ως πάροχος υπηρεσιών προς την Εθνική Βιβλιοθήκη της Ελλάδος (ΕΒΕ) και την Εθνική Λυρική Σκηνή (ΕΛΣ). Σε δεύτερο επίπεδο, ο οργανισμός αναλαμβάνει την οργάνωση και λειτουργία του Πάρκου Σταύρος Νιάρχος (εφεξής το Πάρκο), ως βασικού πυλώνα του τρισδιάστατου Κέντρου Πολιτισμού ΙΣΝ.

Τέλος, ο οργανισμός λειτουργεί ως το όχημα που επιδιώκει την ενοποίηση των λειτουργιών και των δραστηριοτήτων της ΕΒΕ, της ΕΛΣ και του Πάρκου σε ένα ενιαίο πόλο έλξης συμβάλλοντας στην ανάδειξη του Κέντρου Πολιτισμού ΙΣΝ σε έναν ενιαίο εκπαιδευτικό και πολιτιστικό προορισμό.

2. Οργάνωση και Δομή Οργανισμού

Το Κέντρο Πολιτισμού ΙΣΝ στεγάζεται σε δικό του κτίριο και έχει λειτουργική οργανωτική δομή: Τη διοίκηση του οργανισμού ασκεί το διοικητικό συμβούλιο, ενώ ο γενικός διευθυντής έχει το συνολικό έλεγχο των τεσσάρων διευθύνσεων του οργανισμού. Οι τέσσερις διευθύνσεις είναι οι ακόλουθες: α) Διεύθυνση Ασφαλείας η οποία είναι αρμόδια για την ασφάλεια του Κέντρου Πολιτισμού ΙΣΝ. β) Διεύθυνση Συντήρησης και Τεχνικής Υποστήριξης Εγκαταστάσεων η οποία είναι υπεύθυνη για τη συντήρηση πρασίνου, εγκαταστάσεων, εξοπλισμού και για τα συστήματα μηχανοργάνωσης του οργανισμού. Η Διεύθυνση περιλαμβάνει τρία τμήματα: Συντήρησης Πρασίνου, Συντήρησης Εγκαταστάσεων και Μηχανοργάνωσης. γ) Διεύθυνση Προγραμμάτων και Εκδηλώσεων η οποία είναι υπεύθυνη για τον σχεδιασμό και υλοποίηση εκπαιδευτικών και ψυχαγωγικών προγραμμάτων, τις δημόσιες σχέσεις, τη διοργάνωση εκδηλώσεων, την ανάπτυξη και προβολή του οργανισμού και την εξεύρεση πόρων. Η Διεύθυνση αναλόγως των αρμοδιοτήτων της περιλαμβάνει 5 αντίστοιχα τμήματα. δ) Διεύθυνση Διοικητικών Υπηρεσιών που περιλαμβάνει

το λογιστήριο, τα τμήματα νομικών υποθέσεων και διαχείρισης ανθρώπινου δυναμικού και τις υπηρεσίες επισκεπτών (τηλεφωνικό κέντρο, ιατρικό κέντρο και τμήμα μεταφορών).[1]

3. Περιουσιακά Στοιχεία Οργανισμού (Assets)

Εξαιρετική σημασία για την λειτουργία του οργανισμού έχουν το κτίριο όπου στεγάζονται η ΕΒΕ και η ΕΛΣ καθώς και το Πάρκο. Συνεπώς, οι κτιριακές εγκαταστάσεις με τον υλικοτεχνικό εξοπλισμό τους και το Πάρκο πρέπει να προστατευτούν.

Πιο συγκεκριμένα, πρέπει να προστατευτούν το δίκτυο, ο Server και ο back up του, τα βιβλία, οι χώροι και ο εξοπλισμός ψηφιοποίησης, το πληροφοριακό σύστημα της βιβλιοθήκης, οι υπολογιστές, ο ιστότοπος, οι χώροι αποθήκευσης, τα οχήματα μεταφοράς προσωπικού και επισκεπτών, το σύστημα αντλιών για το πότισμα του Πάρκου, ο υλικοτεχνικός εξοπλισμός της ΕΛΣ και της ΕΒΕ, οι εγκαταστάσεις παροχής ηλεκτρικού ρεύματος και νερού του οργανισμού και φυσικά τα δεδομένα και ιδίως τα προσωπικά δεδομένα των επισκεπτών που συλλέγονται από τον οργανισμό.

Ο οργανισμός λαμβάνει αυστηρά υλικά, ηλεκτρονικά και διοικητικά μέτρα για την προστασία του. Ειδικότερα, ο οργανισμός χρησιμοποιεί εύλογα μέτρα για την προστασία από ιούς και άλλα επιβλαβή στοιχεία. Επιπλέον, ο οργανισμός εξασφαλίζει την κρυπτογραφημένη μετάδοση των δεδομένων και λαμβάνει κάθε πρόσφορο μέσο για την ασφαλή μετάδοση και αποθήκευσή τους. Ακόμα για την ασφάλεια του οργανισμού χρησιμοποιούνται τόσο μόνιμο προσωπικό όσο και εξωτερικοί συνεργάτες.

4. Gap Analysis

Εξαιτίας της πρόσφατης έναρξης λειτουργίας του οργανισμού έχουν ληφθεί όλα τα απαραίτητα μέτρα για την προστασία του από φυσικές καταστροφές, παθητικές και ενεργητικές επιθέσεις και κακόβουλα λογισμικά. Ωστόσο, πρέπει να προβλεφθεί ένα πρόγραμμα ενημέρωσης του προσωπικού για θέματα που αφορούν στη μείωση των κινδύνων όπως αθέλητες λανθασμένες ενέργειες ανθρώπων καθώς παρατηρείται ένα έλλειμμα γνώσης και κουλτούρας ασφαλείας στο προσωπικό του οργανισμού. Ακόμα, πρέπει να αυστηροποιηθεί η επίβλεψη των επισκεπτών στους χώρους του οργανισμού για την αποφυγή σκόπιμων κακόβουλων ενεργειών ανθρώπων και

[1] ίΣΝ/SNf. *Κέντρο Πολιτισμού Ίδρυμα Σταύρος Νιάρχος Α.Ε.: Βασικές Αρχές Στελέχωσης και Λειτουργίας του Οργανισμού.* Αθήνα: 2008, σελ. 4.

ειδικότερα στο χώρο της Βιβλιοθήκης όπου φυλάσσονται σπάνιες εκδόσεις καθώς έχει παρατηρηθεί συχνή προσπάθεια παραβίασης των κανονισμών της Βιβλιοθήκης.

5. Αξιολόγηση Κινδύνου (Risk Assessment)

Τα βασικά αγαθά του οργανισμού που πρέπει να προστατευτούν διότι είναι κρίσιμα για την λειτουργία του είναι ο Server, το δίκτυο, η ιστοσελίδα, το ηλεκτρονικό ταχυδρομείο, το υλικό (hardware) και το λογισμικό (software), συστήματα επεξεργασίας και αποθήκευσης, τα δεδομένα και οι ηλεκτρολογικές εγκαταστάσεις. Οι απειλές που αντιμετωπίζουν τα συγκεκριμένα αγαθά είναι αρκετές όπως φυσικές καταστροφές, κακόβουλες ενέργειες παραδείγματος χάριν εισαγωγή ιομορφικού λογισμικού, επιθέσεις εκ των έσω (insider attacks), μεθόδων κοινωνικής μηχανικής και διαδικτυακών επιθέσεων, δυσλειτουργία συστήματος και ακούσιες λανθασμένες ενέργειες του προσωπικού. Οι συνέπειες μιας ενδεχόμενης παραβίασης τους κρίνεται ότι ενέχουν υψηλό ρίσκο καθώς θέτουν εν αμφιβόλω τους ακόλουθους τρεις σκοπούς ασφαλείας: ακεραιότητα, διαθεσιμότητα και εμπιστευτικότητα και μπορεί να δημιουργήσουν αδυναμία πρόσβασης σε σημαντικά και κρίσιμα δεδομένα, μεγάλο πλήγμα στη φήμη του οργανισμού, ανάγκες για περισσότερο προσωπικό καθώς και μεγαλύτερες ανάγκες εκπαίδευσης αλλά και ενδεχομένως πρόστιμα και αποζημιώσεις στην περίπτωση παραβίασης προσωπικών δεδομένων. Στόχος της προτεινόμενης πολιτικής ασφαλείας είναι να περιορίσει αυτούς τους κινδύνους.

6. Πολιτική Ασφαλείας (Security Policy)

6.1 Οργανωτική Ασφάλεια

Η οργανωτική ασφάλεια έχει ως σκοπό να διαχειριστεί την ασφάλεια πληροφοριών και υλικοτεχνικού εξοπλισμού μέσα στον οργανισμό. Προαπαιτείται να συσταθεί ένα διοικητικό δίκτυο, το οποίο θα εκπονήσει και θα ελέγχει τις πολιτικές ασφαλείας μέσα στον οργανισμό. Η διοίκηση θα πρέπει να εγκρίνει την πολιτική ασφαλείας και να αναθέσει ρόλους ασφαλείας στο προσωπικό.

Εν προκειμένω, οι εμπλεκόμενοι οι οποίοι θα προσδιορίσουν τις απαιτήσεις ασφαλείας είναι:

- Ο διευθυντής ασφαλείας, ο οποίος είναι αρμόδιος για την ασφάλεια του οργανισμού.

- Ο υπεύθυνος προστασίας δεδομένων του οργανισμού (DPO), ο οποίος παρέχει συμβουλευτική ενημέρωση στον οργανισμό και στο προσωπικό του σχετικά με τις υποχρεώσεις τους που απορρέουν από τον Κανονισμό Προστασίας Προσωπικών Δεδομένων – GDPR (ν. 4624/2019) και άλλες διατάξεις περί προστασίας δεδομένων. Επιπλέον, φροντίζει για την εσωτερική συμμόρφωση προς τις επιταγές της νομοθεσίας περί προστασίας δεδομένων (π.χ. εκπαίδευση προσωπικού, διενέργεια ελέγχων).
- Το τμήμα Μηχανοργάνωσης, το οποίο διαχειρίζεται την τεχνολογική υποδομή του οργανισμού. Επιπλέον, είναι αρμόδιο για τον καθορισμό των κανόνων πρόσβασης, καθώς και τον σχεδιασμό και την δημιουργία των δικαιωμάτων πρόσβασης που αντιστοιχούν στις υπηρεσιακές ανάγκες των θέσεων σε συνεργασία με τις επιχειρησιακές μονάδες του οργανισμού.
- Οι υπεύθυνοι των τμημάτων που θα κληθούν να εφαρμόσουν την Πολιτική ασφαλείας.

6.2 Φυσική Ασφάλεια

Α) Ασφάλεια Χώρων

Πρέπει να ορισθεί σαφής περίμετρος του οργανισμού και να περιφραχθεί. Οι είσοδοι του οργανισμού είναι πλήρως ελεγχόμενες και τηρείται αρχείο καταγραφής με την ώρα και την ημερομηνία της εισόδου και της αποχώρησης επισκεπτών, η παρουσία των οποίων δύναται να επιβλέπεται από το προσωπικό ασφαλείας του οργανισμού όταν εισέρχονται σε ελεγχόμενο χώρο.

Η πρόσβαση σε περιοχές όπου φυλάσσονται ή επεξεργάζονται ευαίσθητα αγαθά (πχ τμήμα χειρογράφων και χώροι ψηφιοποίησης της ΕΒΕ) πρέπει να ελέγχεται και να είναι περιορισμένη σε εξουσιοδοτημένα άτομα μόνο και να υπάρχουν έλεγχοι εξουσιοδότησης. Οι επισκέπτες θα προσέρχονται μόνο μετά από ραντεβού και πάντα υπό επιτήρηση. Φωτογραφικός, video ή άλλος εξοπλισμός καταγραφής, όπως κάμερες σε κινητές συσκευές δεν επιτρέπεται.

Οι είσοδοι των γραφείων του οργανισμού ελέγχονται μέσω κλειστού κυκλώματος παρακολούθησης, το οποίο διατηρεί αρχείο για τουλάχιστον 15 μέρες.

Κατά την αποχώρηση από τα γραφεία το προσωπικό, φροντίζει ώστε οι ντουλάπες και τα συρτάρια να είναι κλειδωμένα και τα κλειδιά αυτών να είναι ασφαλισμένα. Μετά τη λήξη της εργασίας τους οι εργαζόμενοι οφείλουν να ασφαλίζουν τους χώρους τους.

Ιδιαίτερη έμφαση δίνεται στο server room όπου η πρόσβαση είναι εκτός από ελεγχόμενη και καταγραφόμενη μέσω καμερών κλειστού κυκλώματος. Η είσοδος γίνεται μόνο με χρήση κλειδιών, τα οποία κατέχουν συγκεκριμένα άτομα του οργανισμού.

Για την αντιμετώπιση ζημιών λόγω πυρκαγιάς έχουν εγκατασταθεί συσκευές πυρανίχνευσης και πυροσβεστικός εξοπλισμός σε όλους τους χώρους του οργανισμού. Τα εύφλεκτα υλικά (πχ χαρτικά) αποθηκεύονται σε ξεχωριστό χώρο σε ασφαλή απόσταση από κρίσιμες εγκαταστάσεις.

Οι χώροι ελέγχου του δικτύου ηλεκτρικού ρεύματος, κλιματισμού και πυρασφάλειας είναι ελεγχόμενοι και ασφαλισμένοι.

Το εισερχόμενο υλικό επιθεωρείται για πιθανές απειλές πριν μεταφερθεί στο εσωτερικό του οργανισμού, καθώς και να καταχωρηθεί σύμφωνα με τις διαδικασίες διαχείρισης αγαθών.

Β) Ασφάλεια Εξοπλισμού

Οι γραμμές ηλεκτροδότησης και τηλεπικοινωνιών πρέπει να είναι υπόγειες ώστε να προστατεύονται από δολιοφθορές και υποκλοπές. Ακόμα η χρήση κοινών καλωδίων μέσα από κοινόχρηστους χώρους πρέπει να αποφεύγεται στη δικτυακή καλωδίωση. Φθαρμένα καλώδια πρέπει να αντικαθίστανται άμεσα για την αποφυγή καταστροφής δεδομένων.

Ο εξοπλισμός πρέπει να είναι τοποθετημένος και προστατευμένος ώστε να μειώνεται ο κίνδυνος από φυσικές και περιβαλλοντικές καταστροφές.

Ο εξοπλισμός πρέπει να απενεργοποιείται στο τέλος της μέρας.

Απαγορεύεται η κατανάλωση φαγητού, ποτού και το κάπνισμα μέσα στους χώρους εργασίας.

Οι υπολογιστές του προσωπικού εγκαθίστανται σε θέσεις όπου κοινό δεν έχει οπτική πρόσβαση στην οθόνη και το πληκτρολόγιο ώστε να μην έχει τη δυνατότητα θέασης στοιχείων ή κωδικών πρόσβασης.

Όλοι οι υπολογιστές πρέπει να είναι συνδεδεμένοι με σταθεροποιητές ρεύματος (UPS).

Οι υπολογιστές κλειδώνουν αυτόματα μετά την παρέλευση 10 λεπτών αδράνειας.

Ο ευαίσθητος εξοπλισμός πχ συντήρηση και ψηφιοποίηση βρίσκεται σε χώρους με ελεγχόμενη πρόσβαση.

Οι χώροι λειτουργίας των εξυπηρετητών (server room) τροφοδοτούνται από ιδιαίτερη ηλεκτρική γραμμή και διαθέτουν αυτόνομο σύστημα κλιματισμού. Επιπλέον, ελέγχεται η θερμοκρασία και η υγρασία μέσω ειδικού εργαλείου επίβλεψης περιβαλλοντικών συνθηκών.

Όλος ο εξοπλισμός συντηρείται τακτικά από το τμήμα μηχανοργάνωσης σε περίπτωση ανάγκης μεταφοράς του εκτός οργανισμού τα δεδομένα ανάλογα με την σημαντικότητά τους μεταφέρονται, κρυπτογραφούνται ή διαγράφονται.

Απαγορεύεται η απομάκρυνση εξοπλισμού από την θέση του χωρίς γραπτή άδεια του διευθυντή ασφαλείας. Ο εξοπλισμός πρέπει να καταγράφεται όταν απομακρύνεται από τον οργανισμό και να καταγράφεται ξανά όταν επιστρέφει.

6.3 Τεχνικά μέτρα Ασφαλείας

Α) Έλεγχος Πρόσβασης στο Δίκτυο

Ο έλεγχος πρόσβασης είναι βασικό εργαλείο εφαρμογής της πολιτικής ασφαλείας και απαιτεί τον καθορισμό ρόλων. Θα οριστούν δυο βασικά επίπεδα χρηστών: α) Διαχειριστής και β) Απλός Χρήστης. Κάθε επίπεδο χρήστη θα έχει ανάλογες δυνατότητες, υποχρεώσεις και δικαιώματα. Τα δικαιώματα και οι προσβάσεις των χρηστών δίνονται με βάση τις αρχές: Ανάγκη γνώσης και ανάγκη χρήσης. Με άλλα λόγια, αυτά σχετίζονται άμεσα με την εργασία και την θέση του στον οργανισμό.

Διαχειριστής (Τμήμα Μηχανοργάνωσης): Ο λογαριασμός διαχειριστή δίδεται σε συγκεκριμένους υπαλλήλους. Οι διαχειριστές είναι υπεύθυνοι για τη διαχείριση του συστήματος, μπορούν να αλλάξουν τις ρυθμίσεις ασφάλειας, να εγκαταστήσουν υλικό και λογισμικό, να αποκτήσουν πρόσβαση σε όλα τα αρχεία και είναι υπεύθυνοι για την εγκατάσταση anti-virus και την ενημέρωση των λειτουργικών συστημάτων. Τέλος έχει πλήρη έλεγχο σε όλες τις εφαρμογές.

Απλός Χρήστης: Όλοι οι υπάλληλοι που διαθέτουν ηλεκτρονικό υπολογιστή είναι απλοί χρήστες. Τα δικαιώματά τους είναι περιορισμένα όσον αφορά την εισαγωγή και επεξεργασία αρχείων. Έχουν πλήρη έλεγχο των τοπικών αρχείων, αλλά δεν έχουν δεν έχουν δυνατότητα

εγκατάστασης εφαρμογών λογισμικού ή περιφερειακών συσκευών. Για τυχόν πρόβλημα ή δυσλειτουργία απευθύνονται στους διαχειριστές για την επίλυσή του.

Κάθε χρήστης των συστημάτων του οργανισμού έχει μοναδική ταυτότητα που του αποδίδεται κατά την πρόσληψή του και απενεργοποιείται κατά την λήξη της εργασίας του και αποτελείται από το όνομα χρήστη (username) και τον κωδικό πρόσβασης (password), το οποίο ο χρήστης δεσμεύεται να διατηρεί μυστικό.

Όλα οι κωδικοί πρόσβασης πρέπει να διατηρούνται στη μνήμη των χρηστών και σε καμία περίπτωση να καταγράφονται σε έγγραφα ή ηλεκτρονικές συσκευές και να αποκαλύπτονται σε συναδέρφους. Επιπλέον, υπάρχει όριο αποτυχημένων προσπαθειών σύνδεσης (τρεις) μετά κλειδώνεται ο λογαριασμός για 15 λεπτά.

Απαγορεύεται η χρήση της επιλογής «Remember Password» των εφαρμογών.

Σε καμία περίπτωση δεν θα υπάρχουν μηχανήματα και πληροφοριακά συστήματα χωρίς κωδικό πρόσβασης και δεν θα χρησιμοποιείται ο ίδιος κωδικός σε πάνω από ένα μηχάνημα.

Τα passwords πρέπει να έχουν μήκος τουλάχιστον 8 χαρακτήρων, να περιέχουν πεζά και κεφαλαία γράμματα, αριθμούς και σύμβολα.

Όλοι οι κωδικοί πρόσβασης πρέπει να αλλάζουν υποχρεωτικά τουλάχιστον κάθε 6 μήνες.

Σε περίπτωση που υπάρχει υποψία παραβίασης κωδικού πρόσβασης τότε ενημερώνεται ο διευθυντής ασφαλείας και το τμήμα μηχανοργάνωσης και η αλλαγή γίνεται άμεσα.

Σε περίπτωση που κάποιος χρήστης ξεχάσει την ταυτότητά του η διαδικασία που πρέπει να ακολουθηθεί είναι: Εάν ξεχάσει το όνομα χρήστη, ο διαχειριστής το αναζητά μέσα από τη βάση χρηστών και ενημερώνει τον χρήστη. Εάν έχει ξεχάσει τον κωδικό πρόσβασης ο διαχειριστής διαγράφει τον παλιό και ορίζει έναν καινούργιο τον οποίο ο χρήστης υποχρεούται να αλλάξει κατά την πρώτη σύνδεσή του στο εσωτερικό δίκτυο.

Β) Διαχείριση Ασφάλειας Δικτύου

Υπάρχει προστασία από κακόβουλο λογισμικό τόσο των υπολογιστών όσο και των Servers μέσω antivirus καθώς και με την χρήση firewall, τα οποία μάλιστα ενημερώνονται συχνά και αυτομάτως.

Στην περίπτωση που απαιτούνται εισερχόμενες συνδέσεις προς το δίκτυο του οργανισμού αυτές θα υλοποιούνται μέσω VPN και θα καταγράφονται.

Η πρόσβαση στο Web επιτρέπεται μόνο στα πλαίσια των υποχρεώσεων του οργανισμού. Απαγορεύεται η χρήση για προσωπικούς λόγους.

Για την ασφάλεια στο διαδίκτυο να χρησιμοποιείτε ασφαλείς συνδέσεις στο Web, το οποίο τεκμηριώνεται από το εικονίδιο του κλειδωμένου λουκέτου, ενώ η διεύθυνση που συνδέεστε πρέπει να αρχίζει από https://. Επιπλέον, να είστε βέβαιοι ότι οι ρυθμίσεις ασφαλείας του προγράμματος πλοήγησης στο Web είναι αρκούντως υψηλές.

Δεν πρέπει να επιτρέπεται η χρήση αφαιρούμενων μέσων αποθήκευσης πληροφορίας (CD, USB stick). Εάν είναι απαραίτητη η χρήση τους πρέπει να απενεργοποιείται η αυτόματη εκκίνηση και να ελέγχονται για ύπαρξη κακόβουλου λογισμικού.

Μην κατεβάζετε αρχεία από άγνωστες ή ύποπτες πηγές.

Γ) Αντίγραφα Ασφαλείας

Οι χρήστες δεν πρέπει να αποθηκεύουν σημαντικά δεδομένα τους στους τοπικούς υπολογιστές, αλλά στο Server.

Η διαδικασία λήψης αντιγράφων ασφαλείας (back up) είναι εξέχουσας σημασίας για τη διασφάλιση της ακεραιότητας και διαθεσιμότητας της πληροφορίας και το σχέδιο ανάκαμψης από καταστροφές.

Τα αντίγραφα ασφαλείας εκτελούνται κατά τις βραδινές ώρες καθώς η πλειοψηφία του προσωπικού απουσιάζει.

Τα ημερήσια back up αποθηκεύονται σε σκληρό δίσκο εντός του computer room. Το εβδομαδιαίο back up αποθηκεύεται σε πυρίμαχο χρηματοκιβώτιο.

Καθημερινά ο προϊστάμενος του τμήματος μηχανοργάνωσης ενημερώνεται με email για την λήψη αντιγράφων ασφαλείας

Η διαθεσιμότητα των δεδομένων που βρίσκονται σε αποθηκευτικά μέσα πρέπει να ελέγχεται τακτικά.

Δ) Ασφάλεια Επικοινωνιών

Απαγορεύεται η χρήση του email για ανταλλαγή πληροφοριών που δεν σχετίζονται με τη λειτουργία του οργανισμού.

Ύποπτα emails πρέπει να σβήνονται και να μην προωθούνται. Επιπλέον, δεν ανοίγονται αρχεία που έρχονται συνημμένα σε emails από αγνώστους ή ύποπτους αποστολείς. Τέτοια emails πρέπει να σβήνονται αμέσως και να διαγράφονται και από τον κάδο ανακύκλωσης του υπολογιστή.

Προβλέπεται η ύπαρξη δεύτερου εναλλακτικού παρόχου του ηλεκτρονικού ταχυδρομείου.

Η χρήση των Social Media (πχ facebook) επιτρέπεται μόνο στα πλαίσια των υποχρεώσεων του προσωπικού προς τον οργανισμό. Απαγορεύεται η χρήση για προσωπικούς λόγους.

Τα Fax, οι εκτυπωτές και τα φωτοτυπικά μηχανήματα θα πρέπει να βρίσκονται σε ελεγχόμενους χώρους.

Τα εκτυπωμένα έγγραφα θα πρέπει να απομακρύνονται άμεσα.

Για την διακίνηση ψηφιακών εγγράφων ή μηνυμάτων απαιτείται η ψηφιακή υπογραφή (π.δ. 150/2001) ώστε να διασφαλίζεται η αυθεντικότητα και ακεραιότητά τους και η αδυναμία αποποίησης της ευθύνης του αποστολέα.

6.4 Ελεγχόμενη Πρόσβαση Ιστοτόπου

Θα ακολουθείται διαδικασία ελεγχόμενης πρόσβασης στον ιστότοπο τόσο για την δημιουργία νέου λογαριασμού χρήστη όσο και για την ταυτοποίηση και αυθεντικοποίησή του κάθε φορά που επιθυμεί να εισέλθει σ’ αυτόν.

Η πρόσβαση στον ιστότοπο απαιτεί όνομα χρήστη και κωδικό, ώστε να επιβεβαιώνεται το δικαίωμα χρήσης των λειτουργιών του, εκτός των βασικών που η χρήση τους είναι ελεύθερη.

Το περιεχόμενο του ιστοτόπου προστατεύεται με την ρύθμιση δικαιωμάτων πρόσβασης των χρηστών και των διαχειριστών. Ο διαχειριστής έχει αυξημένα δικαιώματα πρόσβασης (δυνατότητα επεξεργασίας ιστοσελίδων, αρχείων και προφίλ χρηστών και ελέγχου), ενώ ο χρήστης μπορεί να πλοηγηθεί στον ιστότοπο και να χρησιμοποιήσει τις παρεχόμενες ηλεκτρονικές υπηρεσίες του οργανισμού.

Το περιεχόμενο του ιστοτόπου τοποθετείται σε διαφορετικό δίσκο από το λειτουργικό σύστημα.

Ελέγχεται η ακεραιότητά του, ότι οι σύνδεσμοί του είναι έγκυροι και λειτουργικοί και ότι δεν έχουν εισαχθεί τρωτότητες από σενάρια ή «κρυφά» πεδία φόρμας.[2]

Προβλέπεται η ύπαρξη δεύτερου εναλλακτικού παρόχου του ιστοτόπου.

Λογαριασμός χρήστη μπορεί να δημιουργηθεί από την αρχική σελίδα του όπου υπάρχει επιλογή δημιουργίας νέου λογαριασμού όπου ο χρήστης καταχωρεί τα στοιχεία του σε ειδική φόρμα και λαμβάνει username και password. Ο χρήστης όποτε επιθυμεί μπορεί να αιτηθεί διαγραφή του λογαριασμού και του προφίλ του.

6.5 Διαχείριση Αλλαγών

Υπεύθυνο για την διαχείριση αλλαγών είναι το τμήμα μηχανοργάνωσης. Το τμήμα είναι συνεχώς ενήμερο για θέματα αλλαγής εξοπλισμού και λογισμικού, αναλαμβάνοντας την εποπτεία και τον έλεγχο της διαδικασίας. Ακόμα μεριμνά για την αποτροπή κάθε απειλής απώλειας δεδομένων, δυσλειτουργίας του συστήματος ή ασυμβατότητας του νέου εξοπλισμού ή λογισμικού με το υπάρχον σύστημα.

Όλος ο εξοπλισμός θα φέρει ένδειξη με κωδικό καταγραφής και τα βασικά χαρακτηριστικά του.

Αλλαγές γίνονται αποκλειστικά σε περιπτώσεις βλάβης ή αναβάθμισης.

7. Διαδικασία Ασφαλείας (Security Procedure)

7.1 Οργανωτική Ασφάλεια

Οργάνωση σεμιναρίων, προγραμμάτων εκπαίδευσης και ημερίδων για την αποτελεσματική εκπαίδευση των υπαλλήλων του οργανισμού σε θέματα ασφάλειας. Η ενημέρωση και ευαισθητοποίηση των υπαλλήλων για θέματα ασφάλειας πληροφορίων πρέπει να αποτελεί συνεχή διαδικασία του οργανισμού.

---

[2] Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων. *Γενικά Μέτρα Προστασίας Συστημάτων από Ηλεκτρονικές Επιθέσεις.* Αθήνα: Φεβρουάριος 2012, σελ.7.

Ο οργανισμός πρέπει να προβαίνει ανά εξάμηνο σε άσκηση περιστατικού κυβερνοασφάλειας, ώστε να ανιχνεύεται η ετοιμότητα του προσωπικού.

Για την αντιμετώπιση σοβαρών περιστατικών παραβίασης συγκροτείται Ομάδα αντιμετώπισής τους, η οποία αποτελείται από τον DPO, τον διευθυντή ασφάλειας, τον προϊστάμενο του τμήματος μηχανοργάνωσης, μέλος από τη νομική υπηρεσία και τις δημόσιες σχέσεις του οργανισμού. Αρμοδιότητές της: η αποσαφήνιση και αντιμετώπιση του συμβάντος, ο περιορισμός των επιπτώσεων, η επικοινωνιακή διαχείρισή του, ο εντοπισμός των κενών ασφαλείας και η κάλυψη τους με ταυτόχρονη ενημέρωση της πολιτικής ασφαλείας.

7.2 Φυσική Ασφάλεια

Για την φυσική ασφάλεια του οργανισμού υπεύθυνοι είναι το μόνιμο προσωπικό αλλά και εξωτερικοί συνεργάτες (εταιρεία security), οι οποίοι καλούνται να εφαρμόσουν τους κανόνες της ενότητας 6.2.

7.3 Τεχνικά μέτρα Ασφαλείας

Σε περίπτωση παραβίασης ή απώλειας κωδικού πρόσβασης βλέπε διαδικασία που προβλέπεται στο 6.3 Α.

Σε περίπτωση που μηχανήματα έχουν προσβληθεί από ιούς θα πρέπει να ενημερώνεται το τμήμα μηχανοργάνωσης και να αποσυνδέονται από το δίκτυο του οργανισμού μέχρι να βεβαιωθούμε ότι δεν είναι πια μολυσμένα. Το τμήμα μηχανοργάνωσης καθαρίζει το μηχάνημα και το επαναφέρει στην προηγούμενη κατάσταση μέσω των αντιγράφων ασφαλείας.

Σε περίπτωση ύποπτου αρχείου συνημμένου σε email καλούμε το τμήμα μηχανοργάνωσης και ακολουθούμε τη διαδικασία που προβλέπεται στο 6.3 Δ.

Πάντα πρέπει να ελέγχονται για ιούς τα αφαιρούμενα μέσα αποθήκευσης πριν χρησιμοποιηθούν.

Σε περίπτωση διαρροής προσωπικών δεδομένων καλείται η ομάδα αντιμετώπισης περιστατικών παραβίασης οφείλουν: Να μετριάσουν την ζημία που υπέστησαν τα υποκείμενα των δεδομένων. Να ενημερώσουν τα υποκείμενα των δεδομένων. Να ενημερώσουν την Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα εντός 72 ωρών (άρθρα 33-34 GDPR 2016/679). Εφόσον συμβεί το περιστατικό παραβίασης δεδομένων προσωπικού χαρακτήρα, οφείλουμε να

διδαχθούμε από την εμπειρία αυτή, αξιοποιώντας την τουλάχιστον για τη βελτίωση των πολιτικών ασφαλείας.

7.4 Ελεγχόμενη Πρόσβαση στον Ιστότοπο

Για την δημιουργία λογαριασμού χρήστη ακολουθούμε την διαδικασία που προβλέπεται στο 6.4.

Σε περίπτωση κυβερνοεπίθεσης στον ιστότοπο του οργανισμού καλείται η ομάδα αντιμετώπισης περιστατικών παραβίασης και κατεβαίνει προσωρινά ο ιστότοπος μέχρι να αντιμετωπιστεί το περιστατικό. Ταυτόχρονα αναλαμβάνει την επικοινωνιακή διαχείριση της κατάστασης. Μετά την αντιμετώπιση του περιστατικού εντοπίζει τα κενά ασφαλείας και ενημερώνει την πολιτική ασφαλείας.

7.5 Διαχείριση Αλλαγών

Η διαδικασία αλλαγής εξοπλισμού περιγράφεται ως: Ανάγκη για την αλλαγή εξοπλισμού. Ενημέρωση του τμήματος μηχανοργάνωσης. Παραλαβή νέου εξοπλισμού συμβατού με τις ανάγκες χρήσης. Εφόσον υπάρχουν χρήσιμα δεδομένα ανακτώνται από το υλικό προς αντικατάσταση. Εγκατάσταση νέου εξοπλισμού. Έλεγχος καλής λειτουργίας. Πραγματοποιείται η αλλαγή. Έλεγχος ομαλής λειτουργίας του συστήματος. Επαναφορά δεδομένων από αντίγραφα ασφαλείας. Παράδοση προς χρήση.

Η διαδικασία αλλαγής λογισμικού περιγράφεται ως: Ανάγκη για την αλλαγή λογισμικού. Ενημέρωση του τμήματος μηχανοργάνωσης. Σύνταξη τεχνικής μελέτης για την είσοδο του νέου λογισμικού. Παραλαβή νέου λογισμικού συμβατού με τις ανάγκες χρήσης. Δημιουργούνται αντίγραφα ασφαλείας ώστε να αποφευχθεί απώλεια δεδομένων. Απεγκατάσταση παλαιού λογισμικού. Εγκατάσταση νέου λογισμικού. Έλεγχος καλής λειτουργίας. Επαναφορά αρχείων συστήματος. Παράδοση προς χρήση.

8. Σχέδιο Ανάκαμψης από Καταστροφές (Disaster-Recovery)

Η επιχειρησιακή συνέχεια αποτελεί βασικό στόχο του οργανισμού και η επίτευξή της απαιτεί μεταξύ άλλων και τη διαχείριση των περιστατικών ασφαλείας που ενδέχεται να διακόψουν ή να παρακωλύσουν την ομαλή του λειτουργία.

Η απρόσκοπτη λειτουργία και η αποτελεσματική υποστήριξη κάθε συστήματος προϋποθέτουν την ύπαρξη πολιτικών, προτύπων και διαδικασιών του οργανισμού από όλα τα εμπλεκόμενα τμήματα, αλλά και τους παρόχους υπηρεσιών πληροφορικής.

Το Σχέδιο Ανάκαμψης από Καταστροφές προβλέπει τα μέτρα, τα οποία εφαρμόζονται σε περιπτώσεις έκτακτης ανάγκης. Κύριος υπεύθυνος για την άρτια διεκπεραίωση του σχεδίου είναι το τμήμα μηχανοργάνωσης.

Πιο συγκεκριμένα, για την έγκαιρη αντιμετώπιση ζημιών λόγω πυρκαγιάς έχουν εγκατασταθεί συσκευές πυρανίχνευσης και πυροσβεστικός εξοπλισμός σε όλους τους χώρους του οργανισμού. Σε περίπτωση βλάβης των αντλιών στις γεωτρήσεις για την άρδευση του Πάρκου έχει προβλεφθεί η ύπαρξη μονάδας αφαλάτωσης, η χρήση ανακυκλωμένου ύδατος και η παροχή νερού από τον Δήμο Καλλιθέας. Σε περίπτωση προβλήματος στην ηλεκτροδότηση του οργανισμού πλέον των UPS έχει προβλεφθεί η ύπαρξη γεννητριών στα υπόγεια του οργανισμού για την συνέχιση της λειτουργίας του.

Όσον αφορά τις εισβολές στα πληροφοριακά συστήματα του οργανισμού, για την ανίχνευση και αντιμετώπισή τους μπορούν να χρησιμοποιηθούν ειδικά συστήματα λογισμικού, τα επονομαζόμενα συστήματα ανίχνευσης εισβολών, τα οποία κάνουν χρήση αισθητήρων και δίνουν τακτικές αναφορές στα κέντρα ελέγχου.

Πλέον της ύπαρξης back up Server σε περίπτωση βλάβης ή παραβίασης του κεντρικού Server για την απρόσκοπτη λειτουργία του προβλέπεται ιδιαίτερη ηλεκτρική γραμμή και διαθέτει αυτόνομο σύστημα κλιματισμού. Επιπλέον, τηρούνται αντίγραφα ασφαλείας για την ανά πάσα στιγμή επαναφορά του συστήματος στη πρότερη κατάσταση ή ανάκτηση δεδομένων του λογισμικού ώστε να επιτυγχάνεται διαθεσιμότητα και ακεραιότητα των δεδομένων.

Ακόμα για τον ιστότοπο και το ηλεκτρονικό ταχυδρομείο του οργανισμού προβλέπονται εναλλακτικοί πάροχοι ώστε αν δεχτούν επίθεση να εξασφαλίζεται η συνέχεια του οργανισμού.

Τέλος, η εκπαίδευση του προσωπικού μέσα από την σχεδίαση συχνών ασκήσεων πάνω στην αντιμετώπιση περιστατικών παραβίασης προσδίδει στο προσωπικό την απαραίτητη ετοιμότητα για την ταχεία ανάκτηση της επιχειρησιακής ικανότητας του οργανισμού σε περίπτωση που καταστεί ανάγκη.

9. Συμμόρφωση

Η πολιτική ασφαλείας του οργανισμού εκπονήθηκε λαμβάνοντας πλήρως υπόψιν τις διατάξεις του GDPR (2016/679ΕΕ όπως ενσωματώθηκε με ν. 4624/2019) για την προστασία των προσωπικών δεδομένων και συμμορφώνεται πλήρως με αυτές. Επιπλέον, σχεδιάστηκε έχοντας υπόψιν τις διατάξεις του ν. 4577/2018 και τις ΥΑ 1027/2019 για την σχεδίαση μιας σύγχρονης πολιτικής ασφαλείας όπως αυτή ορίζεται από τις επιταγές της ΕΕ.

10. Διαδικασίες Ελέγχου και Αξιολόγησης της Πολιτικής Ασφαλείας

Για την ορθή εφαρμογή και βελτίωση της πολιτικής ασφαλείας είναι απαραίτητη η διεξαγωγή ελέγχων, καθώς και ο προγραμματισμός περιοδικών ασκήσεων διείσδυσης στα συστήματα του οργανισμού ώστε να διαπιστωθεί η αντοχή τους και να εντοπιστούν τυχόν κενά ασφαλείας. Η αξιολόγηση της αποτελεσματικότητας της πολιτικής ασφαλείας και των αντίμετρων συνεισφέρει στην ανατροφοδότηση και αναθεώρησή της.

11. Αντιμετώπιση

Καταρχάς λόγω της σοβαρότητας του περιστατικού ασφαλείας θα κληθεί η ομάδα αντιμετώπισης περιστατικών παραβίασης. Το υπεύθυνο τμήμα μηχανοργάνωσης θα κατεβάσει άμεσα η κεντρική σελίδα του οργανισμού και θα ενεργοποιήσει το σχέδιο ανάκαμψης από καταστροφές ώστε να ανέβει όσο το δυνατό γρηγορότερα η κεντρική σελίδα του οργανισμού από εναλλακτικό πάροχο και επανέλθει σε λειτουργία μέσα από τα αντίγραφα ασφαλείας που διατηρεί ο οργανισμός.

Η υπεύθυνος επικοινωνίας της ομάδας αντιμετώπισης θα κληθεί να διαχειριστεί την διαμορφωθείσα κατάσταση και να διασκεδάσει την αλγεινή εικόνα της πτώσης της κεντρικής σελίδας υποβαθμίζοντας το γεγονός ώστε να μην πληγή ανεπανόρθωτα η φήμη του οργανισμού.

Όσον αφορά τους ηλεκτρονικούς υπολογιστές το αρμόδιο τμήμα μηχανοργάνωσης θα τους αποσυνδέσει από το δίκτυο, θα γίνει προσπάθεια καθαρισμού τους (format) και να επανέλθουν στην πρότερη κατάσταση με την χρήση των αντιγράφων ασφαλείας. Αν αυτό δεν είναι εφικτό θα ξεκινήσει διαδικασία αντικατάστασής τους. Σε καμία περίπτωση ο οργανισμός δεν διαπραγματεύεται με τρομοκράτες, ούτε είναι διατεθειμένος να πληρώσει το ποσό που ζητείται ως λύτρα.

Μετά την αντιμετώπιση του περιστατικού η ομάδα αντιμετώπισης θα διερευνήσει τα αίτια πρόκλησης του συμβάντος ώστε να διαπιστωθεί το κενό ασφαλείας στον οργανισμό και να καλυφθεί. Αφού καταγραφούν οι διαδικασίες αντιμετώπισης του περιστατικού μαζί με την κάλυψη των ευπαθειών η ομάδα αντιμετώπισης περιστατικών παραβίασης προχώρα σε αναθεώρηση της πολιτικής στα σημεία όπου παρατηρήθηκαν αδυναμίες. Το νέο σχέδιο αποστέλλεται προς έγκριση στην διοίκηση του οργανισμού.

Βιβλιογραφία

Εγχειρίδιο «Κυβερνοασφάλεια στη Δημόσια Ασφάλεια». Αθήνα: ΕΚΔΔΑ. 2019.

Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων. *Γενικά Μέτρα Προστασίας Συστημάτων από Ηλεκτρονικές Επιθέσεις.* Αθήνα: Φεβρουάριος 2012.

ίΣΝ/SNf. *Κέντρο Πολιτισμού Ίδρυμα Σταύρος Νιάρχος Α.Ε.: Βασικές Αρχές Στελέχωσης και Λειτουργίας του Οργανισμού.* Αθήνα: 2008.

Κανονισμός 2016/679ΕΕ

ν. 4577/2018 ΦΕΚ 199 Α΄

ν. 4624/2019 ΦΕΚ 137 Α΄

υπουργική απόφαση 1027/2019 ΦΕΚ 3739 Β΄