ΕΘΝΙΚΗ ΣΧΟΛΗ ΔΗΜΟΣΙΑΣ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΑΥΤΟΔΙΟΙΚΗΣΗΣ

ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ ΣΤΗ ΔΗΜΟΣΙΑ ΔΙΟΙΚΗΣΗ

Τελική Εργασία

ΤΜΗΜΑ ΚΟΙΝΩΝΙΚΗΣ ΦΡΟΝΤΙΔΑΣ

ΑΔΑΜΑΝΤΙΑ ΖΗΣΟΠΟΥΛΟΥ

ΚΣΤ' ΕΚΠΑΙΔΕΥΤΙΚΗ ΣΕΙΡΑ

Αθήνα, Νοέμβριος 2019

Θέμα

Καλείστε σε ένα νεοσύστατο οργανισμό του Δημοσίου ως στελέχη της Δημόσιας Διοίκησης για παροχή συμβουλευτικού έργου σε ζητήματα κυβερνοασφάλειας.

Α. Να περιγράψετε τις προτάσεις σας προς την διοίκηση του οργανισμού σε σχέση με τις ενέργειες που θα πρέπει να προβεί ώστε να βελτιωθεί το επίπεδο ασφαλείας του.

Β. Μετά την εφαρμογή των όποιων οργανωτικών και λοιπών μέτρων από τον συγκεκριμένο οργανισμό και μετά από 2 χρόνια λειτουργίας του, ο οργανισμός δέχεται κυβερνοεπίθεση στις υποδομές του με αποτέλεσμα να μην είναι διαθέσιμη στο κοινό η κεντρική σελίδα του στο διαδίκτυο και παράλληλα διαπιστώνεται ότι σε κάποιους ηλεκτρονικούς υπολογιστές του προσωπικού έχει γίνει κρυπτογράφηση αρχείων και εμφανίζεται μήνυμα για αποστολή λύτρων σε bitcoins.

Περιγράψτε τις ενέργειες στις οποίες πρέπει να προβείτε.

Περιεχόμενα

Ερώτημα Α

1. Εισαγωγή

Το παρόν Σχέδιο Ασφάλειας διεξάγεται για λογαριασμό του Πανεπιστημίου Χ, και αφορά τις νέες εγκαταστάσεις των Γραμματειών των Τμημάτων και της Κεντρικής Γραμματείας του. Το Σχέδιο Ασφάλειας είναι σύμφωνο με το σχετικό νομικό πλαίσιο, τους κανονισμούς, τις στρατηγικές και τις προδιαγραφές. (βλέπε βιβλιογραφία)

2. Καταγραφή των παγίων

Ο φορέας στεγάζεται σε ένα κτίριο εμβαδού 2.000 τ.μ.. Στο κτίριο δεν στεγάζεται άλλη υπηρεσία. Στον φορέα εργάζονται 200 υπάλληλοι, οι οποίοι διεκπεραιώνουν τα καθήκοντά τους με την χρήση σταθερών ηλεκτρονικών υπολογιστών. Οι υπάλληλοι επιμερίζονται σε 20 τμήματα, εκ των οποίων τα 10 είναι κεντρικές γραμματείες των τμημάτων του Πανεπιστημίου και έχουν φυσικές συναλλαγές με το κοινό, και 1 τμήμα είναι η κεντρική γραμματεία.

3. Καταγραφή των κενών ασφαλείας (Gap analysis)

Ο φορέας ενδεχομένως να δεχτεί παθητική ή ενεργητική επίθεση. Η παθητική επίθεση, που μπορεί να είναι υποκλοπή μηνύματος ή παρακολούθηση της κίνησης δεδομένων, στοχεύει στη συλλογή και χρήση πληροφοριών του συστήματος χωρίς να γίνει αντιληπτή και χωρίς να επηρεάσει την ομαλή λειτουργία του. Η παθητική επίθεση οδηγεί κυρίως σε διαρροή δεδομένων. Οι ενεργητικές επιθέσεις, που περιλαμβάνουν τη μεταμφίεση, την επανεκπομπή, την τροποποίηση, την άρνηση υπηρεσίας και την εξαντλητική αναζήτηση κωδικού, έχουν στόχο να παρέμβουν και να τροποποιήσουν τον τρόπο λειτουργίας του συστήματος. Παράλληλα υπάρχουν και οι επιθέσεις Κοινωνικής Μηχανικής και Ηλεκτρονικής Εξαπάτησης.

Τα κενά ασφαλείας στο ΠΣ οδηγούν σε παραβίαση της ασφάλειας (εμπιστευτικότητα, ακεραιότητα, διαθεσιμότητα) του ψηφιακού συστήματος, με συνέπειες είτε την απώλεια των δεδομένων είτε την διαρροή δεδομένων.

Σύμφωνα με την αναλυτική καταγραφή των κενών ασφαλείας (gap analysis), τα κενά ασφαλείας είναι:

- Φυσική καταστροφή server και ηλεκτρονικών υπολογιστών, που θα οδηγήσει σε απώλεια δεδομένων
- Επίθεση με ιομορφικό ή κακόβουλο λογισμικό που μπορεί να εισέλθει στο ΠΣ μέσω αρχείων επισυναπτόμενων σε emails, αρχείων που εισέρχονται στο σύστημα από εξωτερικές θύρες ή από την απλή χρήση μολυσμένου CD ή USB.
- Κακόβουλες πράξεις των φυσικών προσώπων που έχουν πρόσβαση στο ΠΣ ή συμμετέχουν στην συντήρηση του εξοπλισμού του

4. Ανάλυσης επικινδυνότητας (Risk assessment)

Κατά την μέθοδο ανάλυσης επικινδυνότητας καθορίζονται ποιες πηγές πληροφοριών χρειάζονται προστασία και αποκρυσταλλώνονται οι πιθανοί κίνδυνοι, που μπορεί να προκύψουν από αποτυχημένη εφαρμογή του συστήματος ασφαλείας του πληροφοριακού συστήματος, και να οδηγήσουν σε απώλεια εμπιστευτικότητας, ακεραιτότητας και διαθεσιμότητας. Τα κύρια στοιχεία που θα προστατευθούν είναι το σύνολο των ψηφιακών συστημάτων, τα δεδομένα και ο εξοπλισμός.

Ο σκοπός της εκτίμησης κινδύνων είναι να δημιουργηθούν οι κατάλληλες στρατηγικές και έλεγχοι για την τήρηση των πληροφοριακών στοιχείων, από την διοίκηση.

4.1. Κατηγορίες δεδομένων που χρειάζονται προστασία

Η ταξινόμηση των πληροφοριών κρίνεται απαραίτητη για τον προσδιορισμό της σχετικής ευαισθησίας και της κρισιμότητας προστασίας τους. Για την βέλτιστη ανάπτυξη στρατηγικής για την προστασία της ιδιωτικότητας και της εμπιστευτικότητας των δεδομένων, θα δημιουργηθεί ένα Πρότυπο Ταξινόμησης και Προστασίας Δεδομένων, το οποίο θα λαμβάνει υπόψη το εθνικό και ευρωπαϊκό νομοθετικό πλαίσιο, καθώς και τους κανονισμούς και τις πανεπιστημιακές πολιτικές.

Το Πρότυπο Ταξινόμησης και Προστασίας Δεδομένων εφαρμόζεται σε όλα τα δεδομένα (π.χ. στοιχεία σπουδαστών, έρευνας, οικονομικών στοιχείων, εργαζομένων) που συλλέγονται σε ηλεκτρονική μορφή ή σε έντυπη μορφή από το Πανεπιστήμιο.

Όλα τα δεδομένα πρέπει να ταξινομηθούν σε μία από τις τρεις βαθμίδες ευαισθησίας ή ταξινομήσεις: απόρρητα, εσωτερικά / ιδιωτικά, δημόσια. Αν και όλες οι κατηγορίες ταξινόμησης απαιτούν κάποιο επίπεδο προστασίας, αυτό δεν είναι ίδιο για κάθε κατηγορία.
Όλα τα Πανεπιστημιακά δεδομένα θα πρέπει να αναθεωρούνται σε περιοδική βάση και να ταξινομούνται ανάλογα με τη χρήση, την ευαισθησία και τη σπουδαιότητά τους στο Πανεπιστήμιο και σύμφωνα με την εθνική νομοθεσία. Το απαιτούμενο επίπεδο ασφάλειας εξαρτάται εν μέρει από την επίδραση που θα είχε η μη εξουσιοδοτημένη πρόσβαση ή αποκάλυψη αυτών των δεδομένων στις πανεπιστημιακές λειτουργίες και διαδικασίες, στην αξιοπιστία και στα περιουσιακά στοιχεία του πανεπιστημίου, καθώς και στο απόρρητο των μεμονωμένων μελών της πανεπιστημιακής κοινότητας.

Απόρρητα δεδομένα

Η μη εξουσιοδοτημένη αποκάλυψη ή καταστροφή τους προκαλεί σοβαρές ζημίες στο Πανεπιστήμιο, στους σπουδαστές του ή στους υπαλλήλους του (π.χ. αριθμοί κοινωνικής ασφάλισης, ημερομηνίες γέννησης, ιατρικά αρχεία, πληροφορίες πιστωτικών καρτών ή τραπεζικών λογαριασμών). Τα απόρρητα δεδομένα προορίζονται αποκλειστικά για χρήση εντός του Πανεπιστημίου και η επεξεργασία τους διέπεται από την αρχή της ελαχιστοποίησης των δεδομένων. Η απώλεια ή η διαρροή αυτών συνεπάγεται υψηλό οικονομικό και διοικητικό κόστος, και θέτει σε υψηλό κίνδυνο την ιδιωτικότητα φυσικών προσώπων, με συνέπεια την αστική ευθύνη του φορέα.

Εσωτερικά/ Ιδιωτικά δεδομένα

Οι πληροφορίες σχετικά με την εσωτερική λειτουργία πρέπει να προστατεύονται για δεοντολογικούς και οικονομικούς λόγους, αν και δεν προστατεύονται συγκεκριμένα από το νομοθετικό πλαίσιο.
Η απώλεια ή η διαρροή αυτών προκαλεί υψηλό διοικητικό κόστος για την επανασυλλογή δεδομένων, οικονομικές απώλειες, δυσφήμιση του Πανεπιστημίου και παραβίαση δικαιωμάτων ιδιωτικού απορρήτου (π.χ. εκπαιδευτικά αρχεία φοιτητών, ιστορικό απασχόλησης και βιογραφικά στοιχεία των αποφοίτων). Τα δεδομένα αυτά προορίζονται για χρήση από τους υπαλλήλους, αλλά και από τρίτους που καλύπτονται από συμφωνία μη δημοσιοποίησης.

Δημόσια δεδομένα

Τα δημόσια δεδομένα δεν είναι αυτόματα δημοσιοποιημένα στο ευρύ κοινό, αλλά δύνανται να γίνουν προσβάσιμα. Αυτά τα δεδομένα είτε ορίζονται σαφώς ως δημόσιες πληροφορίες (π.χ. μισθολογικές κλίμακες των δημοσίων υπαλλήλων) είτε προορίζονται να είναι άμεσα διαθέσιμα σε άτομα τόσο εντός όσο και εκτός της πανεπιστημιούπολης (π.χ. διευθύνσεις ηλεκτρονικού ταχυδρομείου εργασίας του εργαζομένου ή πληροφορίες καταλόγου σπουδαστών). Η διαρροή αυτών δεν προκαλεί οικονομικές απώλειες ή διοικητικές κυρώσεις και δεν θέτει σε κίνδυνο την ασφάλεια της ιδιωτικότητας φυσικών προσώπων. Ωστόσο, η απώλειά τους έχει διοικητικό κόστος.

Καθώς οι οικονομικές, κανονιστικές και λειτουργικές συνθήκες είναι συνεχώς μεταβαλλόμενες, απαιτούνται μηχανισμοί για τον εντοπισμό και την αντιμετώπιση των ειδικών κινδύνων που συνδέονται με τον δυναμικό χαρακτήρα των ενδεχόμενων αλλαγών. Συνεπώς, η μέθοδος ανάλυσης επικινδυνότητας πρέπει συνεχώς να ανατροφοδοτείται και το Τμήμα Πληροφορικής, σε συνεργασία με άλλα τμήματα, θα διεξάγουν ετήσια εκτίμηση κινδύνου ή / και ανάλυση επιπτώσεων, προκειμένου να επιτυγχάνεται:

• Καταγραφή και προσδιορισμός της φύσης των πηγών πληροφόρησης

• Κατανόηση και τεκμηρίωση των κινδύνων σε περίπτωση αποτυχιών εφαρμογής που μπορεί να προκαλέσουν απώλεια εμπιστευτικότητας, ακεραιότητας ή διαθεσιμότητας πηγών δεδομένων

• Προσδιορισμός του απαιτούμενου επιπέδου ασφάλειας για την προστασία των δεδομένων

5. Πολιτική Ασφαλείας (Security policy)

Βασικός σκοπός της Πολιτικής Κυβερνοασφάλειας, η οποία αποτυπώνεται στο Σχέδιο Ασφαλείας του φορέα, είναι η προστασία του συστήματος δικτύου και πληροφοριών, των χρηστών του εν λόγου συστήματος και άλλων επηρεαζόμενων από κυβερνοαπειλές προσώπων. Η αρχή της αναλογικότητας και η αρχή του ελάχιστου προνομίου διέπουν το σύνολο της πολιτικής κυβερνοασφάλειας.

Η συνεχής παρακολούθηση, έλεγχος και ανατροφοδότηση της εφαρμογής της πολιτικής σε προκαθορισμένα χρονικά διαστήματα ή κατά την αντιμετώπιση μη αναμενόμενων κρίσεων ασφαλείας, κρίνεται απαραίτητη λόγω του δυναμικά εξελισσόμενου εξωτερικού περιβάλλοντος.

Η πολιτική ασφαλείας καλύπτει τις βασικές απαιτήσεις ασφαλείας, οι οποίες αποτελούν και επιμέρους στόχους, δηλαδή την εμπιστευτικότητα, την ακεραιότητα, την διαθεσιμότητα, την αυθεντικοποίηση, την εξουσιοδότηση, την μη άρνηση της ευθύνης και την ανθεκτικότητα.

Στις παρακάτω ενότητες περιγράφονται η αποτίμηση των αγαθών που χρίζουν προστασίας (risk analysis), οι διαδικασίες ασφαλείας (security procedures), τα μέτρα φυσικής ασφαλείας που αφορούν την συγκεκριμένη πολιτική, οι ρόλοι των εμπλεκομένων μερών (designate) καθώς και η εφαρμογή του Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR).

Το Σχέδιο Ασφάλειας αναθεωρείται κάθε 2 έτη και τροποποιείται στις περιπτώσεις που συμβαίνουν σημαντικές αλλαγές σε κάποιο τουλάχιστον από τα εξής: α) στην οργανωτική δομή του υπευθύνου επεξεργασίας, β) στα πληροφοριακά συστήματα, γ) στις απαιτήσεις ασφαλείας, δ) στις τεχνολογικές εξελίξεις, ε) στο είδος ή/και στην επεξεργασία των προσωπικών δεδομένων. Η Πολιτική Ασφαλείας μπορεί επίσης να μεταβάλλεται κατόπιν διενέργειας εσωτερικού ή εξωτερικού ελέγχου, ο οποίος καταδεικνύει μη επαρκή ή/και μη αποτελεσματικά μέτρα ως προς την ασφάλεια, ή κατόπιν περιστατικού παραβίασης της ασφάλειας.

6. Διαδικασίες Ασφαλείας (Security procedures)

6.1. Ελεγχόμενη Πρόσβαση στο Δίκτυο (network access control)

Η πρόσβαση των χρηστών στο δίκτυο γίνεται μέσω προσωπικών λογαριασμών. Σε όλους τους υπαλλήλους που διαθέτουν Η/Υ και έχουν άδεια να εκτελούν καθήκοντα μέσω του ΠΣ, θα δίδεται προσωπικός λογαριασμός χρήστη. Ο κάθε λογαριασμός έχει μοναδική ταυτότητα, που θα αποτελείται από το Όνομα Χρήστη και τον Κωδικό Πρόσβασης (συνθηματικά), καθώς απαγορεύεται η χρήση κοινών λογαριασμών από πολλαπλούς χρήστες.

Κάθε νέος υπάλληλος αιτείται χορήγηση προσωπικού λογαριασμού στον Υπεύθυνο Ασφαλείας, κατόπιν εγκρίσεως του αιτήματος από τον προϊστάμενο του αιτούντα. Η αίτηση περιλαμβάνει τα στοιχεία ταυτότητας του χρήστη και τις επιτρεπόμενες προσβάσεις και τα δικαιώματά του.

Με την δημιουργία νέου λογαριασμού, ο χρήστης λαμβάνει προσωρινό κωδικό, τον οποίο είναι υποχρεωμένος να τον αλλάξει σύμφωνα με τις οδηγίες που θα λάβει για την δημιουργία νέων κωδικών.

Κωδικοί προσωπικών λογαριασμών

Όλοι οι χρήστες του φορέα (συμπεριλαμβανομένων φοιτητών, διδασκόντων, προσωπικού και επισκεπτών) είναι υπεύθυνοι για την επιλογή και την εξασφάλιση των κωδικών πρόσβασής τους. Οι κανόνες δημιουργίας νέων κωδικών πρόσβασης είναι:

- Ορισμός κωδικού πρόσβασης μήκους 7 χαρακτήρων για τους χρήστες και 10 χαρακτήρων για τους διαχειριστές.
- Ο κωδικός πρέπει να περιέχει ειδικούς χαρακτήρες για την αύξηση του επιπέδου ασφάλειας
- Ο κωδικός πρέπει να περιέχει 2 ή περισσοτέρους αριθμούς αλλά πάντα θα υπάρχουν και τουλάχιστον 2 αλφαβητικοί λατινικοί χαρακτήρες.
- Δεν επιτρέπεται ο ορισμός κωδικού που ένας τρίτος θα μπορούσε εύκολα να μαντέψει.
- Η ανανέωση του κωδικού είναι υποχρεωτική κάθε 180 ημέρες. Θα υπάρχει ενημερωτικό μήνυμα για τις τελευταίες 30 ημέρες και εάν δεν αλλαχθεί ο κωδικός, τότε ο λογαριασμός θα κλειδώνει.
- Ο νέος κωδικός δεν επιτρέπεται να είναι επανάληψη κάποιου που έχει ήδη χρησιμοποιηθεί παλαιότερα από τον συγκεκριμένο χρήστη.
- Ο κωδικός είναι αυστηρά προσωπικός και πρέπει να παραμένει μυστικός από συναδέλφους.

Προβλέπεται διαδικασία ανάκτησης των κωδικών πρόσβασης, η οποία και προστατεύεται. Σε κάθε περίπτωση, ο χρήστης ενημερώνει το Τμήμα Πληροφορικής. Ειδικότερα:

- 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.
- Υποχρέωση του χρήστη, την πρώτη φορά που θα συνδεθεί στο εσωτερικό δίκτυο, πρέπει να είναι η αλλαγή του κωδικού. Σε κάθε περίπτωση ο νέος κωδικός πρέπει να ακολουθεί τους κανόνες δημιουργίας κωδικών.

Κάθε χρήστης έχει συγκεκριμένους ρόλους στο ΠΣ και του παρέχονται δικαιώματα πρόσβασης ανάλογα των αρμοδιοτήτων του. Δεν επιτρέπεται η ανταλλαγή κωδικών πρόσβασης μεταξύ των χρηστών. Οι διαδικασίες ελέγχου πρόσβασης καταγράφονται, εφαρμόζονται και ενημερώνονται σε όλο το ΠΣ, ώστε να αποτρέπεται η μη εξουσιοδοτημένη πρόσβαση. Οι διαδικασίες και τα μέτρα καλύπτουν όλα τα στάδια της πρόσβασης κάθε χρήστη, από την αρχική εγγραφή νέων χρηστών μέχρι την τελική διαγραφή τους.

Τα δικαιώματα πρόσβασης των χρηστών επανεξετάζονται σε τακτά χρονικά διαστήματα (τουλάχιστον μία φορά το χρόνο) για να εξασφαλιστεί ότι παρέχονται κατάλληλα δικαιώματα βάσει των καθηκόντων του κάθε χρήστη.

Όταν ένας εργαζόμενος αποχωρεί από το ανθρώπινο δυναμικό του Πανεπιστημίου, η πρόσβασή του στα πληροφοριακά συστήματα πρέπει να αναστέλλεται με το πέρας των εργασιών της τελευταίας εργάσιμης ημέρας του. Είναι ευθύνη του Υπεύθυνου Ανθρώπινου Δυναμικού να ζητήσει την αναστολή των δικαιωμάτων πρόσβασης μέσω του Υπεύθυνου Ασφάλειας.

Τέλος, ο κάθε λογαριασμός δεν παρέχει ενδείξεις των προνομίων του χρήστη, της ιεραρχικής του θέσης και δεν περιέχει το ονοματεπώνυμο του.

6.2. Ελεγχόμενη Λειτουργία εντός Δικτύου

Το ΠΣ υποστηρίζεται από domain server (εξυπηρετητή), όπου ορίζονται τα δικαιώματα όλων των χρηστών και οι επιτρεπόμενες ενέργειές τους μέσα στο ΠΣ.

Αντίγραφα ασφαλείας δημιουργούνται κάθε 24 ώρες, κατά την διάρκεια της νύχτας, και αποθηκεύονται σε εσωτερικό ιδιωτικό σύννεφο (internal private cloud). Κάθε 15 ημερολογιακές ημέρες γίνεται έλεγχος ορθής δημιουργίας και αποθήκευσης των αντιγράφων ασφαλείας.

Ταυτόχρονα δημιουργούνται αρχεία καταγραφής ενεργειών χρηστών και συμβάντων ασφαλείας (log files) και αποθηκεύονται στον server.

Οι χρήστες έχουν την δυνατότητα :

- Επεξεργασίας και αποθήκευσης αρχείων μόνο στον server και όχι στα δικά τους τερματικά.
- Εκτυπώσεων μέσω κεντρικών εκτυπωτών. Κάθε γραμματεία τμήματος έχει δύο εκτυπωτές σε προστατευμένο σημείο από τους επισκέπτες. Κάθε τμήμα στην κεντρική διοίκηση έχει από έναν εκτυπωτή. Σε κάθε όροφο του κτιρίου βρίσκεται ένα δωμάτιο εκτυπωτών, των τμημάτων του ορόφου. Οι εκτυπώσεις ανά χρήστη γίνονται

με εισαγωγή κωδικού για την διασφάλιση μη διαρροή στοιχείων σε χρήστες με διαφορετικές αρμοδιότητες

- Σάρωσης εγγράφων. Οι σαρώσεις πραγματοποιούνται με παρόμοιο τρόπο όπως οι εκτυπώσεις, και δημιουργούν αυτόματα αρχεία στο σύστημα μέσω του κατάλληλου εγκατεστημένου λογισμικού.

Οι χρήστες δεν έχουν την δυνατότητα εγκατάστασης ή τροποίησης εγκατεστημένου λογισμικού στο ΠΣ ή στα δικά τους τερματικά. Επίσης, δεν έχουν την δυνατότητα μεταφοράς αρχείων (εισαγωγή ή εξαγωγή) της υπηρεσίας μέσω αποσπώμενων μέσων αποθήκευσης, καθώς δεν υπάρχουν αντίστοιχες θύρες στα τερματικά τους. Σε περίπτωση που χρήστης επιθυμεί την εισαγωγή ή αντιγραφή ή απόσπαση αρχείου από το σύστημα, πρέπει να αιτηθεί, έχοντας την σύμφωνη δεσμευτική γνώμη του προϊσταμένου του, στο Τμήμα Πληροφορικής, το οποίο ελέγχει τις ειδικότερες προϋποθέσεις για την ασφαλή μεταφορά αρχείων, και διενεργεί την μεταφορά με τον πιο ασφαλή και πρόσφορο τρόπο (π.χ. αντιγραφή σε DVD).

6.3. Ελεγχόμενη Επικοινωνία εντός και εκτός Δικτύου

6.3.1. Διαδίκτυο

Όλοι οι χρήστες του ΠΣ έχουν πρόσβαση στο διαδίκτυο, αλλά εξαιρούνται από την πρόσβαση σε μη ασφαλείς ιστοσελίδες. Συν τοις άλλοις, δεν έχουν την δυνατότητα να κατεβάζουν και να αποθηκεύουν αρχεία από το διαδίκτυο ούτε στα τερματικά τους ούτε στον sever.

Για προστασία από κακόβουλο λογισμικό όλων των υπολογιστών (τόσο των Η/Υ των υπαλλήλων όσο και των διακομιστών) χρησιμοποιούνται αντιιακά προγράμματα (antivirus), καθώς και προγράμματα τειχών ασφαλείας (firewall). Το antivirus και το firewall διαθέτουν ανά πάσα στιγμή τις πλέον πρόσφατες ενημερώσεις. Επιπλέον, στο λειτουργικό σύστημα των υπολογιστών (καθώς είναι συνδεδεμένοι στο Διαδίκτυο) εγκαθίστανται ανά τακτά διαστήματα ενημερώσεις ασφαλείας.

6.3.2. Επικοινωνία με άλλα εξωτερικά δίκτυα

Παράλληλα, δεν υπάρχει η δυνατότητα σύνδεσης με άλλα εξωτερικά μη έμπιστα δίκτυα. Δυνατότητα σύνδεσης με άλλα εξωτερικά δίκτυα δημοσίων φορέων υπάρχει μόνο σε εξουσιοδοτημένους υπαλλήλους μετά από ειδική άδεια του υπευθύνου ασφαλείας και του

προϊσταμένου του υπαλλήλου. Ο τελευταίος επιβεβαιώνει την αναγκαιότητα της εν λόγω άδειας σύμφωνα με τις αρμοδιότητες του υπαλλήλου.

Η διακίνηση αλληλογραφίας με άλλους φορείς του Δημοσίου γίνεται μόνο μέσω του Κεντρικού Συστήματος Ηλεκτρονικής Διακίνησης Εγγράφων του Δημοσίου (ΣΗΔΕ). Ο φορέας πρέπει να εγκαταστήσει το ΣΗΔΕ, έτσι ώστε κάθε δικαιούχος υπάλληλος να έχει πλήρη εικόνα για το που ακριβώς βρίσκονται τα έγγραφα, από ποιον υπογράφονται και πότε διεκπεραιώνονται

6.3.3. Λογαριασμός Ηλεκτρονικού Ταχυδρομείου (email)

Κάθε τμήμα του φορέα έχει τουλάχιστον έναν λογαριασμό ηλεκτρονικού ταχυδρομείου επικοινωνίας, τον οποίο διαχειρίζεται ένας αρμόδιος υπάλληλος, έχοντας ειδικά ορισμένο αναπληρωτή σε περίπτωση απουσίας του. Λογαριασμό, δύναται να έχει και κάθε υπάλληλος, εφόσον αυτό συνάδει με τα καθήκοντά του σύμφωνα με το διάγραμμα διαδικασιών του φορέα και κατόπιν σύμφωνης γνώμης του προϊσταμένου του.

Ο λογαριασμός αποκτάται κατόπιν αίτησης του υπαλλήλου μετά από σύμφωνη γνώμη του προϊσταμένου του, και χορηγείται από τον Υπεύθυνο Ασφαλείας. Η αίτηση περιλαμβάνει τα στοιχεία ταυτότητας του χρήστη και τις επιτρεπόμενες προσβάσεις και τα δικαιώματά του.
Με την δημιουργία νέου προσωπικού λογαριασμού ηλεκτρονικού ταχυδρομείου, ο χρήστης λαμβάνει προσωρινό κωδικό, τον οποίο είναι υποχρεωμένος να αλλάξει σύμφωνα με τις οδηγίες που θα λάβει για την δημιουργία νέων κωδικών.
Για τους κωδικούς του προσωπικού λογαριασμού του ηλεκτρονικού ταχυδρομείου καθώς και για την διαδικασία ανάκτησής τους, ισχύουν όσα αναφέρθηκαν στο 5.1 σχετικά με τους κωδικούς λογαριασμού πρόσβασης στο δίκτυο.
Η διεύθυνση του κάθε προσωπικού λογαριασμού ηλεκτρονικού ταχυδρομείου δεν πρέπει να υποδηλώνει την τοποθεσία εργασίας ή προσωπικά στοιχεία του χρήστη.
Κατά την χρήση του ηλεκτρονικού ταχυδρομείου, ο υπάλληλος οφείλει:

- να ελέγχει προσεκτικά τα εισερχόμενα μηνύματα για τη σωστή διεύθυνση ηλεκτρονικού ταχυδρομείου και την ακρίβεια της ορθογραφίας του ονόματος του αποστολέα.
- Να μην κάνει κλικ σε ύποπτους συνδέσμους
- Να μην ανοίγει επισυνάψεις ή συνδέσμους που περιλαμβάνονται σε ανεπιθύμητα μηνύματα ακόμη και αν γνωρίζει τον αποστολέα.

- Να απευθυνθεί πάραυτα στο εξουσιοδοτημένο προσωπικό αν ένα μήνυμα ηλεκτρονικού ταχυδρομείου είναι αμφισβητήσιμο ή γενικά ύποπτο ακόμα και αν είναι γνωστός ο αποστολέας.

6.4. Ελεγχόμενη Πρόσβαση Ιστοτόπου (website access control)

Ο ιστότοπος του φορέα παρέχει ενημέρωση και ηλεκτρονικές υπηρεσίες προς τους πολίτες. Η διαδικασία ελεγχόμενης πρόσβασης ιστοτόπου, στοχεύει στην θωράκιση του ιστότοπου από μη εξουσιοδοτημένη πρόσβαση και βασίζεται στην ασφαλή δημιουργία νέου λογαριασμού χρήστη, καθώς και στην ταυτοποίηση και αυθεντικοποίηση του χρήστη κάθε φορά που επιθυμεί να συνδεθεί στον ιστότοπο

Για την καλύτερη εφαρμογή της διαδικασίας πρέπει να γίνει διαχωρισμός των χρηστών και οριοθέτηση των δικαιωμάτων τους. Για την πρόσβαση στον ιστότοπο, ο πολίτης εισάγει όνομα χρήστη και κωδικό, ώστε να επιβεβαιώνεται το δικαίωμα χρήσης των λειτουργιών του ιστότοπου, εκτός των βασικών που η χρήση τους είναι ελεύθερη. Η δυνατότητα δημιουργίας νέων συνθηματικών παρέχεται μέσω της ηλεκτρονικής υπηρεσίας δημιουργίας προσωπικού λογαριασμού χρήστη. Για αυτή τη δημιουργία πρέπει ο χρήστης να δηλώσει τα στοιχεία του σε μία φόρμα όπου δίνεται μέσα από τον ιστότοπο και να κάνει αποδοχή των όρων, πριν την αποστολή της αίτησης για δημιουργία λογαριασμού στο φορέα.

Μετά την δημιουργία νέου λογαριασμού, ο χρήστη ακολουθεί την διαδικασία πρόσβασης χρησιμοποιώντας τα συνθηματικά του για να συνδεθεί στον ιστότοπο, ενώ έχει πάντα την δυνατότητα αίτησης διαγραφής του λογαριασμού του. Διαγραφή δύναται να γίνεται και από τον φορέα όταν παρατηρηθεί παράνομη ή παράτυπη χρήση ενός λογαριασμού.

Η ενημέρωση του ιστοτόπου γίνεται από το τμήμα επικοινωνίας του φορέα, και η δημιουργία και η συντήρησή του από το Τμήμα Πληροφορικής.

6.5. Διαδικασία Διαχείρισης Αλλαγών (change management procedure)

Η Διαδικασία Διαχείρισης Αλλαγών στοχεύει στην εξασφάλιση 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. Η αναγκαιότητα αλλαγών, η οποία αφορά περιπτώσεις είτε βλάβης είτε αναβάθμισης, εγκρίνεται από τον Προϊστάμενο της Μονάδας Πληροφορικής,

κατόπιν ενημέρωσής του. Αν η αλλαγή αφορά εγκατάσταση νέου τύπου εξοπλισμού ή λογισμικού απαιτείται επιπλέον η έγκριση του Υπεύθυνου Ασφάλειας.

Για την ανάγκη αλλαγής εξοπλισμού ενημερώνεται η Μονάδα Πληροφορικής, από τον αρμόδιο διαχειριστή για την υλοποίηση της αλλαγής. Η Μονάδα Πληροφορικής παραλαμβάνει τον εξοπλισμό, και ελέγχει κατά πόσο καλύπτει πλήρως την ανάγκη καθώς και ότι είναι ασφαλής για την συγκεκριμένη χρήση. Κατόπιν εξετάζονται οι οδηγίες εγκατάστασης και παραμετροποίησης του εξοπλισμού. Κάθε εξοπλισμός φέρει σήμανση όπου αναγράφεται ο ειδικός κωδικός από τον οποίο γίνεται εύκολα αντιληπτό ο κατασκευαστής, το μοντέλο, τα βασικά χαρακτηριστικά και η ημερομηνία προμήθειας. Εφόσον γίνουν όλες οι απαραίτητες ενέργειες για τη λήψη αντιγράφων ασφάλειας, όπου κρίνεται απαραίτητο, ελέγχεται η καλή λειτουργία του νέου εξοπλισμού σε απομονωμένο περιβάλλον και ενημερώνεται η επιχειρησιακή μονάδα του φορέα που θα επηρεαστεί από την αλλαγή με τυχόν διακοπή λειτουργίας του συστήματος. Μετά την πραγματοποίηση της αλλαγής, ελέγχεται η ομαλή του λειτουργία και γίνεται επαναφορά των δεδομένων από το αντίγραφο ασφαλείας, όπου χρειάζεται. Τέλος δημιουργείται νέο αντίγραφο ασφαλείας και ενημερώνεται η Μονάδα Πληροφορικής για την έκβαση της διαδικασίας, η οποία και καταγράφεται στο ημερολόγιο εργασιών με τα απαραίτητα στοιχεία.

Όσον αφορά την αλλαγή λογισμικού, η Μονάδα Πληροφορικής ενημερώνεται για την αιτιολογημένη ανάγκη αλλαγής και συντάσσει τεχνική μελέτη, από την οποία προκύπτει ποιο λογισμικό καλύπτει πλήρως τις επικείμενες απαιτήσεις. Κατόπιν, δημιουργείται αντίγραφο ασφαλείας, στο μηχάνημα όπου θα εγκατασταθεί το νέο λογισμικό, για τα δεδομένα όπου δύναται να επηρεασθούν με την αλλαγή του εν λόγω λογισμικού. Μετά τον έλεγχο συμβατότητας των αρχείων με το νέο λογισμικό, γίνεται απεγκατάσταση του παλιού και εγκατάσταση του νέου. Πραγματοποιείται έλεγχος καλής λειτουργίας, επαναφορά των αρχείων του συστήματος και έλεγχος λειτουργίας τους. Τέλος, δημιουργείται νέο αντίγραφο ασφαλείας και ενημερώνεται η Μονάδα Πληροφορικής για την έκβαση της διαδικασίας, η οποία και καταγράφεται στο ημερολόγιο εργασιών με τα απαραίτητα στοιχεία.

6.6. Σχέδιο Συνέχισης Λειτουργίας (business continuity plan)

Σκοπός του Σχεδίου Συνέχισης Λειτουργίας των ψηφιακών συστημάτων είναι η λήψη κατάλληλων μέτρων σε περιπτώσεις έκτακτης ανάγκης έτσι ώστε:

- Να ελαχιστοποιούνται οι διακοπές κανονικής λειτουργίας

- Να περιορίζεται η έκταση των ζημιών και καταστροφών, καθώς και να αποφεύγεται η πιθανή κλιμάκωση αυτών
- Οι εργαζόμενοι να έχουν την κατάλληλη εκπαίδευση, εξάσκηση και εξοικείωση με τις διαδικασίες έκτακτης ανάγκης
- Να αποκαθίσταται γρήγορα η ομαλή λειτουργία
- Να ελαχιστοποιούνται οι οικονομικές επιπτώσεις

Οι πιθανοί κίνδυνοι που μπορούν να προκαλέσουν ένα έκτακτο συμβάν και να ενεργοποιήσουν την διαδικασία του ΣΣΛ είναι:

- Κίνδυνοι ολικής καταστροφής: πυρκαγιά, διαρροή/ πλημμύρα, καταιγίδα με ισχυρούς ανέμους, σεισμός, τρομοκρατικές ενέργειες και δολιοφθορά.
- Κίνδυνοι μερικής καταστροφής: διακοπή ρεύματος, αβλεψία προσωπικού.
- Κίνδυνοι καταστροφής από ιομορφικό λογισμικό: προσβολή ψηφιακού συστήματος από ιομορφικό λογισμικό.
- Κίνδυνοι μη εξουσιοδοτημένης πρόσβασης στο σύστημα: απόπειρα μη εξουσιοδοτημένης πρόσβασης στο σύστημα.

Σε περίπτωση διαπίστωσης από το προσωπικό ότι συντρέχει κάποιος από τους κινδύνους των προηγούμενων διαδικασιών ενημερώνεται τηλεφωνικά ή αυτοπροσώπως ο υπεύθυνος ασφαλείας και το τμήμα Πληροφορικής. Αρμόδιοι για την λήψη αποφάσεων σε περιπτώσεις έκτακτης ανάγκης είναι ο υπεύθυνος ασφαλείας και ο προϊστάμενος του Τμήματος Πληροφορικής.

Για την εκπαίδευση των χρηστών σε ότι αφορά την αντιμετώπιση καταστάσεων ανάγκης, οργανώνονται από τον φορέα κάθε 6 μήνες ειδικά σεμινάρια και προσομοιώσεις τις διαδικασίας.

Σε κάθε περίπτωση, η Διοίκηση ενημερώνεται με έκθεση που συντάσσει ο υπεύθυνος ασφαλείας, για τα αίτια της κατάστασης ανάγκης, τις δράσεις αντιμετώπισης και τα αποτελέσματά τους.

6.6.1. Σχέδιο Αποκατάστασης Καταστροφής (Disaster recovery plan)

Μετά την εκδήλωση του περιστατικού ασφάλειας και εφόσον αυτό είναι εφικτό, το τμήμα Πληροφορικής σε συνεννόηση με τον υπεύθυνο ασφαλείας προχωρά στην διαδικασία αποκατάστασης ομαλής λειτουργίας.

Οι αρχικές δράσεις επικεντρώνονται στην προστασία και διατήρηση των εξαρτημάτων του δικτύου. Ακολουθεί η διόρθωση των βλαβών και της δικτυακής υποδομής είτε από το τμήμα Πληροφορικής είτε από ειδικευμένο προσωπικό του κατασκευαστή – προμηθευτή. Σε περίπτωση που μέρος της δικτυακής υποδομής ή κάποιος Η/Υ χρήζει αντικατάσταση, το Τμήμα Πληροφορικής προχωρά είτε σε χρήση των αποθεμάτων που υπάρχουν γι' αυτό τον σκοπό είτε σε παραγγελία νέων εξαρτημάτων. Εφόσον δεν συντρέχει ανάγκη επισκευής των συστημάτων, το τμήμα πληροφορικής προχωρά σε δοκιμές καλής λειτουργίας με σταδιακή αποκατάσταση του συστήματος. Εφόσον διαπιστωθεί ότι έχουν καταστραφεί αρχεία, προχωρά σε ανάκτηση από τα αντίγραφα ασφαλείας εντός 12 ωρών.

Για την διασφάλιση συνεχούς παροχής ηλεκτρικού ρεύματος γίνεται χρήση συστημάτων αδιάλειπτης λειτουργίας (UPS) και ηλεκτρογεννήτριας.

Για την διασφάλιση των αρχείων χρησιμοποιούνται αντίγραφα ασφαλείας σύμφωνα με την παράγραφο 6.2.

6.7. Ελεγχόμενο φυσικό περιβάλλον

Ο φορέας στεγάζεται σε ένα κτίριο με υψηλό επίπεδο ασφαλείας. Ειδικότερα, η είσοδος στο κτίριο γίνεται με ειδική κάρτα εισόδου και οι επισκέπτες δίνουν τα στοιχεία τους στον υπάλληλο υποδοχής. Η είσοδος και οι χώροι κυκλοφορίας του κτιρίου παρακολουθούνται από κλειστό σύστημα ασφαλείας με κάμερες. Το κτίριο έχει συναγερμό διάρρηξης, ανίχνευσης πυρκαγιάς και πλημμύρας, καθώς και ενεργητικό σύστημα πυρόσβεσης. Το σύστημα συναγερμών είναι συνδεδεμένο με το τμήμα φύλαξης του κτιρίου καθώς και με την πυροσβεστική. Η θερμοκρασία, η υγρασία και η ποιότητα του αέρα στο κτίριο υποστηρίζονται με μηχανικό σύστημα κλιματισμού και ελέγχονται από Κεντρικό Σύστημα Ελέγχου Κτιρίου (BMS). Στους χώρους με ηλεκτρονικό εξοπλισμό ή/και υπολογιστές έχουν τοποθετηθεί ανιχνευτές πυρασφάλειας και πλημμύρας κατόπιν ειδικής μελέτης. Η υγρασία και η θερμοκρασία στους συγκεκριμένους χώρους, παραμένουν σταθερές σε συνθήκες ειδικά μελετημένες για την εύρυθμη λειτουργία τους.

Ο φορέας έχει ένα Πληροφοριακό Σύστημα, το οποίο υποστηρίζεται από έναν κεντρικό εξυπηρετητή (server) που βρίσκεται σε ειδικά διαμορφωμένο χώρο (computer room) στο 1ο επίπεδο υπογείου. Το computer room δεν έρχεται σε επαφή με το έδαφος, καθώς το κτίριο έχει και δεύτερο επίπεδο υπογείου με θέσεις στάθμευσης.

Κάθε πρωί πριν την έναρξη της βάρδιας των υπαλλήλων, καθώς και στην λήξη του ωραρίου, οι χώροι ελέγχονται από υπάλληλο της ομάδας φύλαξης του κτιρίου. Κατά την διάρκεια μη λειτουργίας του κτιρίου, αυτό φυλάσσεται από υπάλληλο του τμήματος φύλαξης.

Στους χώρους υποδοχής κοινού, οι χώροι φύλαξης (φωριαμοί, συρτάρια κλπ) φυσικών εγγράφων, οι ηλεκτρονικοί υπολογιστές και κάθε είδους ηλεκτρονική συσκευή είναι σε σημεία μη προσβάσιμα από το κοινό. Στους κοινόχρηστους χώρους του κτιρίου δεν υπάρχουν χώροι φύλαξης φυσικών εγγράφων ή Η/Υ ή κάθε είδους ηλεκτρονική συσκευή.

Τέλος όλοι οι υπάλληλοι οφείλουν να ακολουθούν πολιτική καθαρού γραφείου (clean desk policy) και πολιτική καθαρής επιφάνειας εργασίας Η/Υ (clean desktop policy).

7. Ρόλοι των εμπλεκομένων μερών (Designate)

Πέραν των αρμοδιοτήτων που αναφέρονται στην ενότητα 6, ισχύουν τα κάτωθι.

7.1. Διαχειριστής (Administrator)

Ο λογαριασμός Διαχειριστή δίνεται μόνο σε συγκεκριμένους υπαλλήλους καθιστώντας τους υπεύθυνους για την παραμετροποίηση και επίλυση προβλημάτων δικτύου. Τα βασικά του καθήκοντα είναι:

- Επίβλεψη και ο έλεγχος της ομαλής λειτουργίας των ψηφιακών συστημάτων
- Πρόσβαση σε όλους τους φακέλους και τα δεδομένα όλων των εξυπηρετητών και ηλεκτρονικών υπολογιστών και πλήρη έλεγχο σε όλες τις εφαρμογές
- Δυνατότητα εγκατάστασης και απεγκατάστασης προγραμμάτων λογισμικού
- Εγκατάσταση των νέων εκδόσεων του αντί-ιομορφικού λογισμικού και την ενημέρωση των λειτουργικών συστημάτων
- Επίβλεψη του ιστοτόπου διαθέτοντας πλήρη δικαιώματα πρόσβασης στο σύστημα διαχείρισης περιεχομένου και έχοντας δυνατότητα επεξεργασίας των ιστοσελίδων και των αρχείων του, καθώς και του προφίλ των χρηστών.
- Άμεση ενημέρωση του Υπεύθυνου Ασφάλειας σε περίπτωση περιστατικού ασφάλειας

7.2. Τμήμα Πληροφορικής (IT Department)

Το Τμήμα Πληροφορικής είναι λειτουργικά και διοικητικά ανεξάρτητο από τους τελικούς χρήστες των υπηρεσιών πληροφορικής, και εξουσιοδοτείται από την Διοίκηση.

Τα βασικά του καθήκοντα είναι:

- Η ομαλή λειτουργία του εσωτερικού δικτύου, την συντήρησή του και των απαιτούμενων αναβαθμίσεων
- Ο καθορισμός κανόνων πρόσβασης στο δίκτυο
- Σχεδιασμός, δημιουργία και εκχώρηση δικαιωμάτων πρόσβασης στους χρήστες
- Εποπτεία και έλεγχος των αλλαγών εξοπλισμού και λογισμικού
- Μέριμνα για την αποτροπή κάθε απειλής απώλειας δεδομένων, δυσλειτουργίας του συστήματος ή ασυμβατότητας του νέου εξοπλισμού ή λογισμικού με το υφιστάμενο σύστημα
- Τεχνική υποστήριξης στους χρήστες

7.3. Υπεύθυνος Ασφάλειας (Security Officer)

Έχει ως αποκλειστική αρμοδιότητα και αντικείμενο την ασφάλεια των ψηφιακών συστημάτων, διαθέτοντας τις απαραίτητες γνώσεις, δεξιότητες και εμπειρία. Ως βασικός υπεύθυνος για την εφαρμογή του σχεδίου ασφάλειας, είναι αρμόδιος για:

- την υλοποίηση και εφαρμογή των μέτρων ασφάλειας
- την σύνταξη αναφορών και ενημέρωση της Διοίκησης σχετικά με θέματα ασφάλειας
- την διεξαγωγή τακτικών και έκτακτων ελέγχων για την εφαρμογή του σχεδίου ασφάλειας

Το έργο του υποστηρίζεται από εξειδικευμένη ομάδα στελεχών πληροφορικής και από τους διαχειριστές των ψηφιακών συστημάτων, και ελέγχεται από την Επιτροπή Εποπτείας και Ελέγχου, στην οποία και δεν μπορεί να συμμετέχει.

Ο Υπεύθυνος Ασφάλειας ορίζεται από την Διοίκηση του φορέα και ενδέχεται να είναι ο προϊστάμενος του Τμήματος Πληροφορικής.

7.4. Επιτροπή Εποπτείας και Ελέγχου (Steering Committee)

Έχει ως αρμοδιότητα τη διεξαγωγή ελέγχων τόσο για την εφαρμογή της πολιτικής ασφάλειας, όσο και για την ορθή χρήση των ψηφιακών συστημάτων από το προσωπικό. Επίσης, οφείλει να αναφέρει τις αδυναμίες που εντοπίζει στη λειτουργία των συστημάτων και να προτείνει αλλαγές και βελτιώσεις σε τεχνικό και σε οργανωτικό επίπεδο.

7.5. Τμήμα φύλαξης του κτιρίου

Είναι υπεύθυνο για την ασφάλεια του κτιρίου και σε περίπτωση παραβίασης του κτιρίου ή διαπίστωσης ύποπτου γεγονότος οφείλει να ενημερώσει την Διοίκηση και τον Υπεύθυνο Ασφάλειας.

7.6.Χρήστες

Βλέπε σχετικές ενότητες διαδικασιών.

7.7. Πολίτες

Βλέπε ενότητα 6.4.

8. Εφαρμογή Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR) και Υπεύθυνος Προστασίας Δεδομένων (DPO)

Το Σχέδιο Ασφάλειας είναι συμβατό με τον Γενικό Κανονισμό Προστασία Δεδομένων και ορίζεται Υπεύθυνος Προστασίας Δεδομένων του φορέα σύμφωνα με την κείμενη νομοθεσία. (βλέπε βιβλιογραφία)

Ερώτημα Β

Ο υπάλληλος που διαπίστωσε πρώτος το πρόβλημα, αντιλήφθηκε αμέσως ότι πρόκειται για προσβολή του ψηφιακού συστήματος από ιομορφικό λογισμικό.

Κατόπιν ο υπάλληλος σύμφωνα με την εκπαίδευση που είχε λάβει σε αντίστοιχο σεμινάριο προσομοίωσης, που διοργάνωσε ο φορέας για το προσωπικό αλλά και με το Σχέδιο Ασφάλειας, αποσυνέδεσε τον Η/Υ από το εσωτερικό δίκτυο και ενημέρωσε άμεσα τον Υπεύθυνο Ασφαλείας, ο οποίος είναι και προϊστάμενος του Τμήματος Πληροφορικής.

Ο Υπεύθυνος Ασφάλειας και το υπόλοιπο Τμήμα Πληροφορικής προχώρησαν άμεσα στις διαδικασίες που προβλέπει το Σχέδιο Αποκατάστασης Καταστροφής. Ειδικότερα, προέβησαν στον εντοπισμό του προβλήματος και επιβεβαίωσαν την προσβολή του Η/Υ και του ιστοτόπου από ιομορφικό λογισμικό. Ο Υπεύθυνος Ασφάλειας ενημέρωσε τηλεφωνικά την διοίκηση για το πρόβλημα καθώς και για την απόφασή του να μην ανταποκριθούν στον εκβιασμό, καθώς τα μέτρα που είχαν ληφθεί για την προστασία των ψηφιακών συστημάτων ήταν ικανά να αποκαταστήσουν την ομαλή λειτουργία του συστήματος και του ιστοτόπου άμεσα. Πιο συγκεκριμένα, το Τμήμα Πληροφορικής απομάκρυνε το ιομορφικό λογισμικό από τα προσβαλλόμενα ψηφιακά συστήματα και ανέσυρε τα αντίγραφα ασφαλείας των αρχείων και του ιστοτόπου, που είχαν δημιουργηθεί το προηγούμενο βράδυ. Προχώρησε σε εξέταση και εγκατάσταση των αντιγράφων ασφάλειας, και σε δοκιμαστική λειτουργία του συστήματος. Μετά την επιτυχή εφαρμογή των παραπάνω, έθεσε σε κανονική λειτουργία τα ψηφιακά συστήματα.

Ο Υπεύθυνος Ασφαλείας και το Τμήμα Πληροφορικής, προχώρησαν στις απαιτούμενες ενέργειες για τον εντοπισμό του κενού ασφάλειας. Έπειτα από ανάλυση των log files και συζητήσεις με τους υπαλλήλους, κατέληξαν στο συμπέρασμα ότι το ιομορφικό λογισμικό είχε εισχωρήσει στο σύστημα το τελευταίο 24ωρο με φυσική επαφή σε κάποιον από τους Η/Υ, που είχαν προσβληθεί. Παρατηρώντας τα αντίγραφα των βιντεοσκοπήσεων από τις κάμερες που καταγράφουν τις κινήσεις στους κοινόχρηστους χώρους, διαπίστωσαν ότι το μόνο άτομο που ήρθε σε φυσική επαφή με κάποιον από τους εν λόγω Η/Υ, πέραν των υπαλλήλων του φορέα, ήταν ένα άτομο από το συνεργείο καθαρισμού που συνεργάζεται με

τον φορέα. Συν τοις άλλοι συμπέραναν ότι το συγκεκριμένο άτομο προώθησε το ιομορφικό λογισμικό στο σύστημα μέσω εφαπτόμενης συσκευής στον πύργο του Η/Υ.

Πράγματι, επικοινωνώντας με τον υπεύθυνο του συνεργείου καθαρισμού, ο τελευταίος τους ενημέρωσε ότι την προηγούμενη ημέρα εργάστηκε στις εγκαταστάσεις του φορέα ένας νέος υπάλληλος, του οποίου τα ίχνη μετά τον καθαρισμό του κτιρίου του φορέα χάθηκαν και τα δηλωθέντα στοιχεία του ήταν αναληθή.

Ο Υπεύθυνος Ασφάλειας διαπιστώνοντας ότι η μη επίβλεψη του συνεργείου καθαρισμού από υπάλληλο του Τμήματος Φύλαξης του κτιρίου αποτελεί σημαντικό κενό ασφαλείας για τα ψηφιακά συστήματα του φορέα, αποφάσισε και προχώρησε στην αναθεώρηση του Σχεδίου Ασφάλειας. Ειδικότερα πρόσθεσε στην παράγραφο 6.7 «Ελεγχόμενο Φυσικό Περιβάλλον» το εξής κείμενο:

«Οι εργασίες του εκάστοτε συνεργείου καθαρισμού επιβλέπονται από υπάλληλο του τμήματος φύλαξης του κτιρίου»

Τέλος ο Υπεύθυνος Ασφάλειας συνέταξε ενημερωτική έκθεση προς την Διοίκηση για τα αίτια της κατάστασης ανάγκης, τις δράσεις αντιμετώπισης και τα αποτελέσματά τους.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Νόμος 4577/2018 (ΦΕΚ Α’ 199/3-12-2018). Ενσωμάτωση στην ελληνική νομοθεσία της Οδηγίας 2016/1148/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με μέτρα για υψηλό κοινό επίπεδο ασφάλειας συστημάτων δικτύου και πληροφοριών σε ολόκληρη την Ένωση και άλλες διατάξεις.

Νόμος 4411/2016 (ΦΕΚ Α' 142/3-8-2016). Κύρωση της Σύμβασης του Συμβουλίου της Ευρώπης για το έγκλημα στον Κυβερνοχώρο και του Προσθέτου Πρωτοκόλλου της, σχετικά με την ποινικοποίηση πράξεων ρατσιστικής και ξενοφοβικής φύσης, που διαπράττονται μέσω Συστημάτων Υπολογιστών - Μεταφορά στο ελληνικό δίκαιο της Οδηγίας 2013/40/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου για τις επιθέσεις κατά συστημάτων πληροφοριών και την αντικατάσταση της απόφασης - πλαισίου 2005/222/ΔΕΥ του Συμβουλίου, ρυθμίσεις σωφρονιστικής και αντεγκληματικής πολιτικής και άλλες διατάξεις.

Κανονισμός 2016/679/ΕΕ για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων (Γενικός Κανονισμός Προστασίας Δεδομένων).

Νόμος 3979/2011 - (ΦΕΚ 138 Α/16-6-2011). "Για την ηλεκτρονική διακυβέρνηση και λοιπές διατάξεις".

Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων)

Νόμος 4624/2019 (ΦΕΚ 137 Α/29-8-2019) Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και ενσωμάτωση

στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 και άλλες διατάξεις