ΕΘΝΙΚΗ ΣΧΟΛΗ ΔΗΜΟΣΙΑΣ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΑΥΤΟΔΙΟΙΚΗΣΗΣ

Κυβερνοασφάλεια στη Δημόσια Διοίκηση

Κυβερνοασφάλεια σε Δημόσιο Οργανισμό

ΣΟΥΛΙΩΤΗ ΠΑΡΑΣΚΕΥΗ
ΤΜΗΜΑ ΔΙΟΙΚΗΣΗΣ ΜΟΝΑΔΩΝ ΚΟΙΝΩΝΙΚΗΣ ΦΡΟΝΤΙΔΑΣ

ΚΣΤ΄ ΕΚΠΑΙΔΕΥΤΙΚΗ ΣΕΙΡΑ

Διδάσκων: ΚΟΛΑΪΤΗΣ ΧΡΗΣΤΟΣ

30/11/2019

Πίνακας περιεχομένων

ΕΙΣΑΓΩΓΗ

Η σημασία της έννοιας κυβερνοασφάλεια έχει εδραιωθεί μετά τη διευρυμένη χρήση των ψηφιακών τεχνολογιών στη πλειοψηφία των τομέων δράσης της σύγχρονης κοινωνίας και κατά συνέπεια στη καθημερινότητα των πολιτών. Συνδέεται με τις ενέργειες που απαιτούνται προκειμένου να διασφαλιστεί η προστασία των συστημάτων δικτύου και πληροφοριών, των χρηστών αυτών των συστημάτων, αλλά και οποιουδήποτε υποκειμένου ενδέχεται να υποστεί κυβερνοαπειλή (Εγχειρίδιο Μαθήματος, 2019,σ6).

Στο απαιτητικό από πλευράς απόκρουσης κυβερνοεπιθέσεων σύγχρονο περιβάλλον, ο Οργανισμός για την υποστήριξη των ανέργων (ΟΑ), επιδιώκοντας την εύρυθμη λειτουργία του, οφείλει να διαθέτει και να εφαρμόζει μια πολιτική ασφάλειας. Οι παρεχόμενες υπηρεσίες εκ μέρους του ΟΑ, συνοπτικά αφορούν:

1. Ανεύρεση εργασίας (με χρήση του ιστοτόπου του οργανισμού που θα έχει αναρτημένες τις διαθέσιμες θέσεις εργασίας, παροχή συμβουλευτικής/καθοδήγησης αυτοπρόσωπα ή διαδικτυακά)

2. Λήψη επιδομάτων κατόπιν εγγραφής ως άνεργοι στη σχετική πλατφόρμα

3. Υπηρεσίες σύζευξης ανέργων –εργοδοτών / επιχειρήσεων, με σκοπό την κάλυψη κενών θέσεων απασχόλησης).

Η εκπλήρωση του σκοπού και του έργου του ΟΑ προϋποθέτει την ύπαρξη υποδομών, υλικού, προσωπικού και δεδομένων, τα οποία θα αποτελέσουν το αντικείμενο της πολιτικής ασφάλειας του οργανισμού.

ΚΕΦΑΛΑΟ Ι: ΣΧΕΔΙΑΣΜΟΣ ΤΗΣ ΠΟΛΙΤΙΚΗΣ ΑΣΦΑΛΕΙΑΣ

Μια ολοκληρωμένη πολιτική ασφάλειας για τον ΟΑ, θα πρέπει να διαθέτει σκοπούς, στόχους, ρόλους, αρμοδιότητες, κανόνες, οδηγίες και διαδικασίες για την κατοχύρωση των αρχών και απαιτήσεων ασφάλειας των πληροφοριακών συστημάτων και δικτυακών υποδομών του οργανισμού. Ταυτόχρονα θα πρέπει να φέρει την άδεια και επικύρωση της διοίκησης του φορέα.

1. ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΥΛΙΚΩΝ

Η προστασία των υλικών του φορέα ΟΑ, ισοδυναμεί με την προστασία των μέσων που λαμβάνουν μέρος στη παροχή των υπηρεσιών του οργανισμού προς τους χρήστες του[1]. Αυτό αφορά α'ύλες (χαρτί, γραφική ύλη, αναλώσιμα εκτυπωτών και φωτοτυπικών μηχανημάτων) αλλά και αρχεία σε έγχαρτη μορφή. Αρμόδιος για την προστασία αυτών θα πρέπει να θεωρηθεί ο Υπεύθυνος Αναλωσίμων, ο οποίος σε εβδομαδιαία βάση θα πρέπει να παρακολουθεί την ανάλωση των υλικών και να προβαίνει στις αντίστοιχες ενέργειες για την ανανέωσή τους. Ο χώρος φύλαξης των συγκεκριμένων υλικών, θα πρέπει να εξασφαλίζει την συντήρηση και την αποφυγή αλλοίωσης ή καταστροφής των υλικών, ενώ προτείνεται να είναι απομακρυσμένος από σημεία παροχής/διέλευσης νερού (αποχωρητήριο, χώρος κουζίνας) καθώς και σημεία που είναι δυνατό να αναπτυχθούν υψηλές θερμοκρασίες. Ομοίως τα αρχεία του ΟΑ σε έγχαρτη μορφή θα πρέπει να φυλάσσονται σε χώρους που η πρόσβαση θα είναι δυνατή μόνο σε εξουσιοδοτημένους υπαλλήλους, οι οποίοι θα φέρουν υπό μορφή πλαστικοποιημένης κάρτας με ενσωματωμένο μηχαναγνώσιμο αριθμό, το σχετικό πιστοποιητικό εισόδου στους συγκεκριμένους χώρους. Στο εσωτερικό των συγκεκριμένων χώρων θα πρέπει να υφίστανται κατάλληλες υποδομές αποθήκευσης, όπως ειδικά ερμάρια με ενσωματωμένες θύρες. Οι προηγούμενοι χώροι επίσης δεν θα πρέπει να συνορεύουν με σημεία που προσδιορίστηκαν και στη περίπτωση των α' υλών.

Μέρος των υλικών λογίζονται και τα έπιπλα που θα διαθέτει ο ΟΑ. Η προστασία τους θα πρέπει να στοχεύει στη διατήρησή της καλής τους κατάστασης κατά την αναμονή και εξυπηρέτηση των χρηστών του ΟΑ. Υπεύθυνος για αυτή ορίζεται ο Υπεύθυνος ασφάλειας του ΟΑ, ο οποίος καθ' όλο το ωράριο λειτουργίας του οργανισμού θα επιτηρεί και θα επιβλέπει την προσήκουσα χρήση τους. Ανάλογη ευθύνη επωμίζεται σε σχέση με τη προστασία του κέντρου Η/Υ εντός του ΟΑ, διαθέσιμου στο κοινό.

[1] Ήτοι ανέργους, εργοδότες, λοιπούς φορείς που συνεργάζονται μαζί του.

2. ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΥΠΟΔΟΜΩΝ

Η χρήση των ηλεκτρονικών υπολογιστών (Η/Υ) ως κρίσιμη υποδομή του ΟΑ, διακρίνεται μεταξύ του προσωπικού και του κοινού (computer room). Κατά συνέπεια διαχωρίζονται τα μέτρα για την ασφάλεια της κάθε υποδομής.

Σημαντικό ρόλο και στις δύο περιπτώσεις επιτελεί ο Υπεύθυνος δικτύου, καθώς καλείται να επιβλέπει την ορθή σύνδεση των συσκευών στο δίκτυο, την καθημερινή τεχνική υποστήριξη, τη συντήρηση, λειτουργία και αποκατάσταση βλάβης των Πληροφοριακών Συστημάτων, ενώ επίσης πραγματοποιεί ελέγχους για την ορθή εφαρμογή της πολιτικής ασφάλειας. Η απρόσκοπτη λειτουργία του ιστοτόπου του ΟΑ, καθώς και η δυνατότητα διαχείρισης αλλαγών στα συστήματα ή τον εξοπλισμό του φορέα, πρέπει να κατοχυρώνονται.

2.1 ΤΟ ΔΙΚΤΥΟ

Για να είναι ασφαλής η πρόσβαση των Η/Υ στο εσωτερικό δίκτυο του ΟΑ από κάθε εργαζόμενο, θα πρέπει να αντιμετωπίζεται ο κίνδυνος της μη εξουσιοδοτημένης πρόσβασης. Αυτό προϋποθέτει ότι ο κάθε εργαζόμενος διαθέτει ένα προσωπικό λογαριασμό, και είναι Υπεύθυνος για τη διαφύλαξη των συνθηματικών που του χορηγήθηκαν, ώστε να μην έρθουν σε γνώση μη εξουσιοδοτημένων χρηστών του εσωτερικού δικτύου του ΟΑ.

Η διαφύλαξη αυτών των στοιχείων δεν είναι εφικτή αν δεν διακριθούν ρόλοι μεταξύ των εργαζομένων. Κυριότεροι αυτών είναι του διαχειριστή του δικτύου και του υπαλλήλου, ενώ αδιαμφισβήτητη είναι η σημασία της συμμετοχής της μονάδας πληροφορικής του ΟΑ.

Ο διαχειριστής του δικτύου και η ομάδα που τον υποστηρίζει θα ευθύνεται για την επίλυση προβλημάτων που είναι δυνατό να εμφανιστούν στο δίκτυο, το οποίο προϋποθέτει τη πρόσβασή του σε οποιοδήποτε ηλεκτρονικό πόρο, λογαριασμό, είδος δεδομένου που υπάρχει στο δίκτυο (διαθεσιμότητα, ως απαίτηση ασφάλειας). Η προηγούμενη δυνατότητα εξυπηρετείται εφόσον ο διαχειριστής είναι δυνατό να προβεί σε εγκατάσταση/ απεγκατάσταση προγραμμάτων για τη βελτίωση της υφιστάμενης λειτουργίας του δικτύου καθώς και εγκατάστασης αντι-ιομορφικού[2]

[2] Πρόκειται για κακόβουλο λογισμικό, βασισμένο σε κώδικα εντολών που επιδιώκει τη παραβίαση των συστημάτων ασφάλειας ενός οργανισμού.

λογισμικού για την προστασία του συνόλου των εφαρμογών. Επίσης οφείλει να μετονομάζει αμέσως το λογαριασμό που δημιουργείται για τον ίδιο από τη μονάδα πληροφορικής. Ομοίως οφείλει να πράξει και κάθε εξουσιοδοτημένος χρήστης του συστήματος, με τρόπο που δεν θα είναι δυνατή η αναγνώρισή του στην ιεραρχία, οι αρμοδιότητές ή το ονοματεπώνυμό του. Καλείται επίσης να ελέγξει τη σωστή λειτουργία και διαχείριση νέων και υφιστάμενων λογαριασμών χρηστών και τυχών αλλαγών[3] που θα ζητηθούν από τους τελευταίους.

Οι υπάλληλοι θα διαθέτουν προσωπικό λογαριασμό εφόσον από τα καθήκοντά τους προβλέπεται η χρήση Η/Υ. Θα προβλεφθεί η δυνατότητα να εισάγουν και να επεξεργάζονται αρχεία στο δίκτυο, όχι όμως και η εγκατάσταση/απεγκατάσταση εφαρμογών λογισμικού ή περιφερειακών συσκευών (αρχή του ελαχίστου προνομίου). Για οποιοδήποτε πρόβλημα παρουσιαστεί κατά την αλληλεπίδρασή τους με το δίκτυο, οφείλουν να ενημερώσουν την ομάδα των διαχειριστών. Η απόδοση ενός μοναδικού λογαριασμού και σχετικών συνθηματικών[4] στο κάθε υπάλληλο θα γίνεται από το αρμόδιο τμήμα της μονάδας πληροφορικής του ΟΑ (ήτοι τμήμα διαχείρισης διαδικτυακής επικοινωνίας), και για τη διαφύλαξη της μυστικότητάς τους θα ευθύνεται ατομικά ο κάθε υπάλληλος. Η τήρηση του συνθηματικού πρόσβασης θα πρέπει να ακολουθεί τον κανόνα των 8 έως 10 χαρακτήρων, με τυχαίους, σε μη λογική ακολουθία γραμματαριθμούς και συμπερίληψη ειδικών χαρακτήρων[5]. Η ανανέωση του κωδικού πρόσβασης θα είναι υποχρεωτική με την πάροδο 90 ημερών και θα πρέπει να διαφέρει ριζικά από τον προηγούμενο. Όταν δημιουργείται για πρώτη φορά ένα λογαριασμός, η ομάδα των διαχειριστών ενημερώνει τον αποδέκτη με μήνυμα στο ηλεκτρονικό του ταχυδρομείο για τις δυνατότητες χρήσης/ πρόσβασης μέσω αυτού, στο δίκτυο.

Ωστόσο η αναγνώριση ενός υπαλλήλου ως πιστοποιημένου χρήστη του δικτύου θα γίνεται με ευθύνη του προϊσταμένου του τμήματος στο οποίο ανήκει. Ο υπάλληλος συμπληρώνει μια αίτηση στην οποία αποτυπώνονται τα στοιχεία ταυτότητας του χρήστη, email, τηλέφωνο, η θέση του ιεραρχικά στον ΟΑ, τα καθήκοντα, οι αρμοδιότητες και τα δικαιώματα που πρέπει να διαθέτει σε δικτυακούς πόρους προκειμένου να τους διαχειριστεί. Η αίτηση θα σταλεί στο τμήμα διαχείρισης

[3] Σε στοιχεία ή δικαιολογητικά.
[4] Συνθηματικά: Κωδικός χρήστη(user name) και κωδικός πρόσβασης (password)
[5] Ειδικοί χαρακτήρες: &, *,@, !, $, +, #,%

διαδικτυακής επικοινωνίας του ΟΑ, ώστε να προβούν στις απαραίτητες ενέργειες (εμπιστευτικότητα, ως αρχή ασφάλειας). Το ίδιο τμήμα, εκτός της δημιουργίας λογαριασμών μετά την εξέταση δικαιωμάτων πρόσβασης, θα εξετάζει τη διαγραφή λογαριασμών που δεν βρίσκονται πλέον σε χρήση, προκειμένου να μην υπερφορτώνεται το δίκτυο και να περιορίζεται το πεδίο επίθεσης στο δίκτυο του ΟΑ.

Η επαρκής προστασία των υποδομών προϋποθέτει την εγκατάσταση στο σύνολο των Η/Υ υπό χρήση, ενός συστήματος για την απόκρουση επιθέσεων ιομορφικού λογισμικού (antivirus).

Τα καθήκοντα της μονάδας πληροφορικής σχετίζονται με τις αρμοδιότητες προηγούμενων και επόμενων ρόλων/τμημάτων που θα παρουσιαστούν. Συνεπώς παραλείπεται σε αυτό το σημείο μια διακριτή παρουσίασή της.

2.2 Ο ΙΣΤΟΤΟΠΟΣ

Η πρόσβαση στον ιστότοπο του οργανισμού – ως βάση της διάδρασης μεταξύ του ΟΑ και των χρηστών του- θα στοχεύει στη μέγιστη δυνατή αξιοποίηση ευκαιριών απασχόλησης /συνεργασίας με τον ΟΑ.

Λόγω της ιδιαίτερης φύσης των παρεχόμενων υπηρεσιών[6], ο ΟΑ θα παρέχει τη δυνατότητα γενικής (προς κάθε ενδιαφερόμενο) αλλά και εξατομικευμένης πρόσβασης σε αυτές, μέσα από τη δημιουργία ενός λογαριασμού χρήστη. Ο διαχωρισμός των χρηστών σε ομάδες με διαφορετικές δυνατότητες πρόσβασης κρίνεται απαραίτητος για την περιφρούρηση της ασφάλειάς του από μη εξουσιοδοτημένους χρήστες. Η εξατομικευμένη πρόσβαση προϋποθέτει την αίτηση δημιουργίας λογαριασμού[7] μέσω του ιστοτόπου του ΟΑ. Μέριμνα θα πρέπει να ληφθεί από τον υπεύθυνο του δικτύου και την μονάδα πληροφορικής για την προστασία απλών και ευαίσθητων δεδομένων προσωπικού χαρακτήρα κατά το πλαίσιο του Γενικού Κανονισμού Προστασίας Δεδομένων (ΓΚΠΔ, Κανονισμός 2016/679 της ΕΕ)

Μια δεύτερη δυνατότητα πρόσβασης για όσους δεν επιθυμούν να εγγραφούν θα δίνεται μέσω του συνδυασμού των μοναδικών αριθμών μητρώου κοινωνικής ασφάλισης (ΑΜΚΑ) και μητρώου ασφαλισμένου (ΑΜΑ). Η πρόσβαση του χρήστη

[6]Υπονοώντας το κοινωνικά ευαίσθητο ζήτημα της ανεργίας
[7]Με τη συμπλήρωση σχετικής φόρμας, αποδεχόμενος τους όρους που θέτει.

θα πραγματοποιείται μέσω των συνθηματικών που θα έχει παραλάβει στο email του από το διαχειριστή του ιστοτόπου[8]. Η διαγραφή ενός λογαριασμού χρήστη θα είναι δυνατή κατόπιν αιτήματος του χρήστη ή στη περίπτωση που ο διαχειριστής παρατηρήσει παράνομη χρήση του.

Ο καθορισμός των χαρακτηριστικών του λογαριασμού, οι κανόνες για τη δημιουργία/αντικατάσταση κωδικού πρόσβασης ισχύουν όπως και στη περίπτωση της πρόσβασης στο δίκτυο του ΟΑ (σ6, ευθύνη: τμήμα διαχείρισης διαδικτυακής επικοινωνίας).

Καθιερώνεται διακριτός ρόλος διαχειριστή του ιστοτόπου, προκειμένου μαζί με την ομάδα του και σε συνεργασία με τη μονάδα Πληροφορικής (όταν κρίνεται απαραίτητο), να επιτηρούν την εύρυθμη λειτουργία του ιστοτόπου του ΟΑ. Αυτό ισοδυναμεί με την απόδοση πλήρων δικαιωμάτων πρόσβασης στη διαχείριση του περιεχομένου των ιστοσελίδων, των αρχείων που περιέχουν, όπως και δυνατότητα παρέμβασης στο προφίλ των χρηστών του, από το διαχειριστή του ιστοτόπου. Επίσης θα καθορίζει το ποιές πληροφορίες θα πρέπει να μεταδοθούν χρησιμοποιώντας μεθόδους κρυπτογράφησης[9]. Σε περίπτωση που αντιληφθεί πιθανό περιστατικό παραβίασης της ασφάλειας του ιστοτόπου, θα πρέπει να απευθυνθεί στη μονάδα πληροφορικής.

Όσα αναφέρθηκαν ως δυνατότητες/αρμοδιότητες και μέτρα προστασίας στο τμήμα του ΔΙΚΤΥΟΥ για το ρόλο των υπαλλήλων του ΟΑ, ισχύουν επίσης και για τους υπαλλήλους που κάνουν χρήση του ιστοτόπου του ΟΑ.

Η ποιοτική και αποτελεσματική λειτουργία της πλατφόρμας του ιστοτόπου του ΟΑ, θα πιστοποιηθεί κατά ISO 9001, από ένα διαπιστευμένο φορέα[10]. Ανάλογη πιστοποίηση θα πρέπει να προβλεφτεί και για τη λειτουργία του εσωτερικού δικτύου του ΟΑ.

[8] Ρόλος διακριτός σε σχέση με τον υπεύθυνο δικτύου (βλ. παρακάτω).
[9] Η κρυπτογράφηση ταυτίζεται με τη διαδικασία κωδικοποίησης της πληροφορίας με τέτοιο τρόπο ώστε να εμποδίζει την ανάγνωσή της από μη εξουσιοδοτημένα μέρη. (https://encryption.eset.com/gr/what-is-encryption/)
[10] Παράδειγμα διαπιστευμένου φορέα μπορεί να αναζητηθεί στα πλαίσια του Ελληνικού Οργανισμού Τυποποίησης (ΕΛΟΤ), http://elot.gr/45_457_ell_html.aspx

2.3 Η ΔΙΑΔΙΚΑΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ ΑΛΛΑΓΩΝ

Βλάβη, απόσυρση ή αναβάθμιση μέρους του εξοπλισμού/λογισμικού, θα πρέπει να έχει καταγράφει με ακρίβεια ως προς τα χαρακτηριστικά και την ημερομηνία παραλαβής του νέου υλικού ή του αποσυρόμενου.

Υπεύθυνος για την έγκριση των ανωτέρω ενεργειών είναι ο προϊστάμενος της μονάδας πληροφορικής, ενώ όταν εγκαθίσταται νέο λογισμικό ή νέος εξοπλισμός συγκατατίθεται και διεκπεραιώνει τις εργασίες ο Υπεύθυνος δικτύου. Με την ολοκλήρωση της διαδικασίας αντικατάστασης/ απόσυρσης θα πρέπει να ενημερώνεται και ο Υπεύθυνος Παγίων, προβαίνοντας στις αντίστοιχες ενέργειες επικαιροποίησης του μητρώου παγίων.

Πριν την εγκατάσταση νέου εξοπλισμού/ λογισμικού η λήψη των απαραίτητων αντίγραφων ασφαλείας (σε περίπτωση που αντικαθιστά παλαιότερο υλικό), ο έλεγχος και η καλή λειτουργία του νέου υλικού σε απομονωμένο περιβάλλον και η ενημέρωση των τμημάτων του φορέα που αναμένεται να επηρεαστούν από τη συγκεκριμένη αλλαγή, αποτελούν αρμοδιότητα του Υπεύθυνου δικτύου. Μετά τη λήψη αρχείων ασφαλείας (back up), τηρείται ημερολόγιο εργασιών, περιλαμβάνοντας τις ενέργειες που απαιτήθηκαν για την ολοκλήρωση της διαδικασίας και τα ονόματα των υπευθύνων. Η τήρηση αρχείων δραστηριοτήτων είναι σύμφωνη με το πνεύμα του ΓΚΠΔ (άρθρο 30 ΓΚΠΔ 2016/679 ΕΕ).

3. ΠΡΟΣΩΠΙΚΟ

Έκτος από τη χρήση συνθηματικών πρόσβασης για τους χρήστες του δικτύου και του ιστοτόπου, που αποδίδονται σε κάθε εξουσιοδοτημένο χρήστη από το προσωπικό του οργανισμού, θα πρέπει να εξειδικευτούν κάποιες πτυχές αυτής της διαδικασίας.

Σε περίπτωση που λαμβάνεται ένα email από άγνωστο/επισφαλή αποστολέα, ο υπάλληλος δεν θα πρέπει να το εκτελεί ενώ θα πρέπει να ενημερώνεται η μονάδα πληροφορικής προκειμένου να ελεγχθεί ως προς το περιεχόμενό του, για τον αποκλεισμό κακόβουλων μηνυμάτων. Επίσης η διακίνηση της αλληλογραφίας θα πρέπει να ακολουθεί το σύστημα ηλεκτρονικής διαχείρισης αλληλογραφίας (ΣΗΔΕ), στο εσωτερικό του φορέα, όσο και με άλλους φορείς (government.gov.gr).

Η προστασία των εγγράφων που διακινούνται και γίνονται αντικείμενο επεξεργασίας, θα καθορίζεται από τη διαβάθμιση που τους έχει αποδοθεί, από τον συντάκτη τους βάσει του περιεχομένου τους, και αφού έχει ελεγχθεί και προσυπογραφεί από τους υπόλοιπους αρμόδιους για τη διακίνηση του (Κ.Ε.Δ.Υ., σ35). Στη συνέχεια ο Υπεύθυνος επεξεργασίας των εγγράφων φέρει την ευθύνη εφαρμογής των κατάλληλων τεχνικών και οργανωτικών μέτρων ώστε η επεξεργασία των δεδομένων να είναι σύμφωνη με τον ΓΚΠΔ (άρθρο 24,§1 ΓΚΠΔ).

Οι υπάλληλοι έχουν την ευθύνη διαφύλαξης της μυστικότητας των κωδικών πρόσβασης. Σε περίπτωση όμως που δεν δύνανται να ανακαλέσουν τα συγκεκριμένα στοιχεία θα πρέπει να απευθύνονται στο τμήμα διαχείρισης διαδικτυακής επικοινωνίας.

Οι δυνατότητες πρόσβασης των υπαλλήλων σε εκτύπωση ή σκανάρισμα αρχείων προσδιορίζονται από τον διαχειριστή του ιστοτόπου, και θα πρέπει να ακολουθούν την αρχή του ελαχίστου προνομίου. Ταυτόχρονα απαγορεύεται ρητά η μεταφορά αρχείων ή δεδομένων του φορέα από τον υπάλληλο εκτός του φορέα με οποιοδήποτε μέσο αποθήκευσης δεδομένων[11]. Εξαίρεση στο προηγούμενο κανόνα μπορεί να δικαιολογηθεί μόνο εφόσον ενημερωθεί γραπτώς η μονάδα πληροφορικής και δοθεί η αντίστοιχη έγκριση.

Η λήψη αντιγράφων ασφαλείας των εργασιών των υπαλλήλων με το πέρας του ωραρίου, θα πρέπει να συντελείται σε ημερήσια βάση. Με κριτήριο το αν μια εργασία που επιτελέσθηκε έχει καταχωρηθεί σε ηλεκτρονική όσο και έγχαρτη μορφή θα καθορίζεται ο τρόπος λήψης αντιγράφου ασφαλείας της. Σε περίπτωση που πληρούνται και οι δύο συνθήκες η αποθήκευση θα γίνεται τοπικά, σε συγκεκριμένο φάκελο του Η/Υ που χειρίζεται ο υπάλληλος, ανάλογα με το περιεχόμενό της. Αν ωστόσο έχει καταχωρηθεί μόνο σε ηλεκτρονική μορφή τότε η αποθήκευσή της έκτος του τοπικού φακέλου στον Η/Υ, θα γίνεται επίσης σε απομακρυσμένο εξυπηρετητή (server) του ΟΑ, σε συγκεκριμένο φάκελο/ κατηγορία σύμφωνα με το περιεχόμενό της. Η πρόσβαση στο συγκεκριμένο εξυπηρετητή, θα γίνεται μέσω κωδικών που θα έχει δημιουργήσει για τον κάθε υπάλληλο τμήμα διαχείρισης διαδικτυακής επικοινωνίας.

[11] Usb, memory card, memory stick, CD, DVD.

4. ΘΕΣΜΙΚΗ ΣΥΜΜΟΡΦΩΣΗ

4.1 ΣΥΜΜΟΡΦΩΣΗ ΜΕ ΤΟΝ ΓΚΠΔ

Η προσαρμογή της πολιτικής ασφάλειας του ΟΑ στο πρότυπο που υπαγορεύει ο ευρωπαϊκός γενικός κανονισμός (ΓΚΠΔ) (https://eur-lex.europa.eu) για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και της ελεύθερης κυκλοφορίας τους, διασφαλίζεται μέσω: της χρήσης του συστήματος ΣΗΔΕ, της λήψης προστασίας μέσω εγκατάστασης αντι-ιομορφικού λογισμικού, της πρόβλεψης του ρόλου Υπευθύνου προστασίας δεδομένων[12], με μέριμνα δημοσίευσης των στοιχείων επικοινωνίας του ώστε να είναι προσβάσιμος στα υποκείμενα των δεδομένων υπό επεξεργασία (αρθ.38,§4 ΓΚΠΔ).

Ο βαθμός πρόσβασης δεδομένων υπό επεξεργασία και κατά συνέπεια οι ρόλοι του Υπευθύνου και εκτελούντος την επεξεργασία[13] καθορίζονται για κάθε εργασία που γίνεται στον ΟΑ, βάσει περιγράμματος θέσης εργασίας, ενώ απονέμεται από το διαχειριστή του δικτύου και του ιστοτόπου αντίστοιχα, τηρώντας την αρχή του ελαχίστου προνομίου.

Η συμμόρφωση με τον ΓΚΠΔ αποδεικνύεται και μέσω της υιοθέτησης τεχνικών και οργανωτικών μέτρων στον ΟΑ για την τήρηση των βασικών απαιτήσεων ασφάλειας όπως της κρυπτογράφησης και της ψευδωνυμοποίησης[14] (άρθρο 32,§1, εδαφ.α,

[12] Ειδικότερα, ο ρόλος του DPO είναι απόρροια της συμμόρφωσης του υπευθύνου και του εκτελούντος την επεξεργασία, βάσει του ΓΚΠΔ (αρθ.37 ΓΚΠΔ) να ορίζουν υπεύθυνο προστασίας δεδομένων και να ενημερώνουν την εποπτική αρχή για τα στοιχεία του. Εν προκειμένω ο DPO επιλέγεται από τον Διοικητή του ΟΑ. Ο DPO αναφέρεται στον υπεύθυνο επεξεργασίας, στο Διοικητή του οργανισμού, τον υπεύθυνο επικοινωνίας και την ΑΠΔΠΧ, ως αρμόδια εποπτική αρχή. Η ευθύνη που υπέχει δεν είναι προσωπική, και ο ρόλος του είναι πρωτίστως συμβουλευτικός.

[13] Ο εκτελών την επεξεργασία είναι φυσικό ή νομικό πρόσωπο, δημόσια αρχή, άλλος φορέας ο οποίος επεξεργάζεται δεδομένα προσωπικού χαρακτήρα, για λογαριασμό του υπευθύνου της επεξεργασίας, χωρίς όμως να καθορίζει το σκοπό και τον τρόπο επεξεργασίας των δεδομένων.

[14] «Η ψευδωνυμοποίηση συνεπάγεται την επεξεργασία των δεδομένων με τέτοιο τρόπο ώστε τα δεδομένα να μην είναι δυνατό να αποδοθούν σε συγκεκριμένο υποκείμενο των δεδομένων χωρίς τη χρήση συμπληρωματικών πληροφοριών, εφόσον οι εν λόγω συμπληρωματικές πληροφορίες διατηρούνται χωριστά και υπόκεινται σε τεχνικά και οργανωτικά μέτρα προκειμένου να διασφαλιστεί ότι δεν μπορούν να αποδοθούν σε ταυτοποιημένο ή ταυτοποιήσιμο φυσικό πρόσωπο». Πηγή:https://www.lawspot.gr/nomikes-plirofories/nomothesia/kanonismos-gia-tin-prostasia-dedomenon/arthro-4-genikos-kanonismos

ΓΚΠΔ) κατά την επεξεργασία των δεδομένων, στο βαθμό που κρίνεται σκόπιμο από τον υπεύθυνο ή τον εκτελών την επεξεργασία.

4.2 ΕΘΝΙΚΟ ΘΕΣΜΙΚΟ ΠΛΑΙΣΙΟ

Η πολιτική ασφάλειας του ΟΑ καθοδηγείται από τις απαιτήσεις της εθνικής στρατηγικής κυβερνοασφάλειας, η οποία καθιερώνεται θεσμικά με την συναφή υπουργική απόφαση του 2018 (ΑΔΑ:Ψ4Ρ7465ΧΘ0-Ζ6Ω), και ευθύνη διαχείρισής της από την Εθνική Αρχή Κυβερνοασφάλεια. Υπό αυτή την έννοια προβλέπει την ύπαρξη ενός σχεδίου συνέχισης λειτουργίας (ακολούθως ΣΣΛ 4.2.2) σε περίπτωση που σημειωθεί περιστατικό κυβερνοεπίθεσης. Αναθέτει ρόλους και αρμοδιότητες στο προσωπικό του οργανισμού (ενότητες 2.1-2.3&3), προβαίνει σε μια προσπάθεια αποτίμησης πιθανών κινδύνων (ακολούθως 4.2.1).

4.2.1 RISK ASSESSMENT

Η αποτίμηση ενδεχόμενων κινδύνων από τη λειτουργία του ΟΑ, θα πρέπει να επισημάνει το είδος τους, τα υποκείμενα που αφορούν και τις συνθήκες που είναι δυνατό να εμφανιστούν (https://oiraproject.eu)(www.hse.gov.uk).

Το είδος των κινδύνων μπορεί να κατηγοριοποιηθεί σε καταστάσεις που συνδέονται με φυσικές καταστροφές (απειλή υγείας και ασφάλειας), έλλειψη σταθερής τροφοδοσίας του ηλεκτρικού δικτύου (διακοπή ρεύματος), αναπαραγωγή κακόβουλου λογισμικού και μη εξουσιοδοτημένη πρόσβαση στο σύστημα.

Αναφερόμενοι στους θιγόμενους, θα πρέπει να συμπεριληφθούν:

- Οι χρηστές της πλατφόρμας του ΟΑ, υφιστάμενοι παράνομη επεξεργασία και χρήση των προσωπικών τους δεδομένων,
- Ο ΟΑ σε περίπτωση απώλειας του ελέγχου του εσωτερικού του δικτύου, της διαδικτυακής πλατφόρμας, επιτείνοντας την απώλεια αρχείων και προγραμμάτων που συνδέονται με την καθημερινή του λειτουργιά, καταλήγοντας να χάσει την αξιοπιστία του ως φορέας που συναλλάσσεται με άλλους φορείς (δημοσίου/ ιδιωτικού τομέα).

Οι συνθήκες που ευνοούν την εμφάνιση των κινδύνων ταυτίζονται με:

- Η ελλιπής φυσική θωράκιση του κτιρίου του οργανισμού (δεν πραγματοποιούνται τα ακόλουθα: εφοδιασμός με πυροσβεστήρες, τακτικοί έλεγχοι υδραυλικών εγκαταστάσεων, πιστοποιητικό αντισεισμικής προστασίας)
- Έλλειψη εξοπλισμού για την παροχή σταθερής τάσης του ηλεκτρικού ρεύματος.
- Ελλιπή μέτρα ασφάλειας κατά την επεξεργασία των δεδομένων, και η μη συμμόρφωση με την αρχή της αναλογικότητας ως προς την αναγκαιότητα και το κόστος τήρησής τους.
- Ανεπαρκής και μη έγκαιρη επανεξέταση των μέτρων ασφάλειας των υλικών και υποδομών σε τακτά χρονικά διαστήματα για την επικαιροποίησή τους.
- Μη διακριτοί και σαφώς προσδιορισμένοι ρόλοι του προσωπικού του ΟΑ. Επιπροσθέτως, έλλειψη εξειδικευμένης μονάδας διαχείρισης κινδύνων του ΟΑ, με εστίαση στις υπηρεσίες που παρέχει.
- Επίθεση από υιό τεχνολογίας-αιχμής και απουσία κατάλληλου αντι-ιομορφικού προγράμματος.
- Ελλιπής ενημέρωση υπαλλήλου για τον τρόπο διαχείρισης μηνυμάτων που αποστέλλονται ως συνημμένα ή phising μέσω email, ο οποίος προβαίνει στην εκτέλεσή τους χωρίς να ενημερώσει τη μονάδα πληροφορικής
- Λανθασμένη ρύθμιση firewall με ευθύνη του διαχειριστή του δικτύου του ΟΑ[15].
- Διαπιστώθηκε περιστατικό παραβίασης των προσωπικών δεδομένων των χρηστών, και δεν ακολούθησε γραπτή ενημέρωση της μονάδας πληροφορικής και της ΑΠΔΠΧ[16] με αναλυτική περιγραφή όλων των συνθηκών και των εμπλεκόμενων προσώπων. Μη εκπλήρωση της ευθύνης του υπευθύνου επεξεργασίας, να καταγράφει το σύνολο περιστατικών, σε εσωτερικό υπηρεσιακό αρχείο ηλεκτρονικής μορφής, στο οποίο θα έχει επίσης πρόσβαση ο προϊστάμενος της μονάδας πληροφορικής.
- Έλλειψη ενός σχεδίου συνέχισης λειτουργίας (ΣΣΛ) και κοινοποίησής του στα εξουσιοδοτημένα υποκείμενα.

[15] Το firewall θα πρέπει να ρυθμίζεται ώστε να αποκλείει όλες τις συνδέσεις, πέραν αυτών που έχει επιτρέψει ο διαχειριστής του δικτύου (default-deny).

[16] Αρχή προστασίας δεδομένων προσωπικού χαρακτήρα.

4.2.2 ΣΥΝΕΧΙΣΗ ΤΟΥ ΣΥΣΤΗΜΑΤΟΣ ΛΕΙΤΟΥΡΓΙΑΣ (ΣΣΛ)

Η αποτύπωση ενός σχεδίου συνέχισης της λειτουργίας του ΟΑ, πρακτικά υπονοεί ένα σχέδιο για την επανόρθωση των βλαβών που έχουν συντελεστεί σε περίπτωση που εμφανιστούν οι κίνδυνοι που αναφέρθηκαν στο 4.2.1(disaster recovery system). Οι διαδικασίες που θα πρέπει να συντελεστούν στα πλαίσιά του, αποτελούν αναπόσπαστο μέρος της πολιτικής ασφάλειας του ΟΑ καθώς η έλλειψή τους θα προξενούσε σοβαρό πλήγμα στην εύρυθμη λειτουργία του οργανισμού (www.information-age.com) (www.airmic.com).

Περιεχόμενο του ΣΣΛ:

i. Προσδιορισμός του είδους της επίθεσης, γεγονός που θα καθοδηγήσει και τον τρόπο διασφάλισης του δικτύου του ΟΑ. Σε αυτό το στάδιο ενδέχεται να χρειαστεί το δίκτυο να αδρανοποιηθεί εν μέρει ή συνολικά, να τεθεί σε λειτουργία η εφεδρική ιστοσελίδα του ΟΑ, να ανασχεδιαστεί/ επαναπροσδιοριστεί η λειτουργία των firewalls, να ζητηθεί από τον πάροχο διαδικτυακών υπηρεσιών να λάβει τα απαιτούμενα μέτρα ώστε να μπλοκαριστούν οι προσπάθειες του επιτιθέμενου.
ii. Αναγνώριση καθηκόντων κάθε συμμετέχοντος στην πολιτική ασφάλειας, βάσει ιεραρχίας, αρμοδιοτήτων και των δικαιωμάτων πρόσβασης που διαθέτει στο δίκτυο/ιστότοπο. Κατά συνέπεια αναμένεται:
    a. Οι τεχνικοί της μονάδας πληροφορικής θα πρέπει να εστιάσουν στο να εντοπίσουν την αιτία της επίθεσης, ενώ προηγουμένως να έχουν απομονώσει τους Η/Υ που εμφανίζουν αδυναμία πρόσβασης στο δίκτυο ή τα δεδομένα του ΟΑ. Εκτιμώντας την ένταση της βλάβης/ κυβερνοεπίθεσης θα πρέπει να συμμετέχει στην αντιμετώπισής η ομάδα αντιμετώπισης κρίσεων.
    b. Ο προϊστάμενος της μονάδας πληροφορικής θα πρέπει να ενημερώσει την αρμόδια ομάδα απόκρισης για συμβάντα που αφορούν την ασφάλεια υπολογιστών (CSIRT[17]) και να τεθεί σε εφαρμογή η διαδικασία που έχει προβλέψει η CSIRT, βάσει των χαρακτηριστικών του περιστατικού.

[17] Computer Security Incident Response Team. Σε εθνικό επίπεδο έχει οριστεί η Διεύθυνση Κυβερνοάμυνας του Γενικού Επιτελείου Εθνικής Άμυνας (ΓΕΕΘΑ).

c. Ο Υπεύθυνος επικοινωνίας του ΟΑ, θα πρέπει να προβεί σε επίσημη ενημέρωση των χρηστών για το περιστατικό, μέσω της εφεδρικής ιστοσελίδας του ΟΑ ή με οποιοδήποτε άλλο πρόσφορο μέσο (ανακοίνωση στην κρατική τηλεόραση). Η ενημέρωση θα πρέπει να διατυπωθεί σε κατανοητή γλώσσα για το ευρύ κοινό και να είναι αδιάλειπτη μέχρι το σημείο απόλυτης επαναφοράς του συστήματος.

d. Ο DPO θα πρέπει να βρίσκεται στη διάθεση των χρηστών του ΟΑ προκειμένου να παρέχει κάθε πληροφορία που θα του ζητηθεί σε σχέση με την ασφάλεια των δεδομένων των χρηστών (αρθ.38§4 ΓΚΠΔ)

e. Προετοιμασία του νομικού τμήματος του ΟΑ για αντιμετώπιση ενδεχόμενων αιτημάτων αποζημιώσεων.

iii. Ο Υπεύθυνος επικοινωνίας του ΟΑ θα πρέπει να κοινοποιήσει το περιστατικό κυβερνοεπίθεσης στην ΑΠΔΠΧ και στους Προϊσταμένους της δίωξης ηλεκτρονικού εγκλήματος

iv. Προσδιορισμός του εύρους των ζημιών/απωλειών, που υποδεικνύει τα μέρη του ΣΣΛ που θα ενεργοποιηθούν.

v. Κατά το στάδιο της αντιμετώπισης του περιστατικού θα αξιοποιηθεί η λήψη αντιγράφων ασφαλείας, προκειμένου να είναι δυνατή η επεξεργασία των δεδομένων των χρηστών και η εκπλήρωση των παρεχόμενων υπηρεσιών του ΟΑ στο μέγιστο δυνατό βαθμό.

vi. Προσδιορισμός των μέτρων αντιμετώπισης σε περίπτωση φυσικών καταστροφών, ανάλογα με το είδος τους. Πρόβλεψη ύπαρξης συσκευής UPS[18] για την αδιάλειπτη τροφοδοσία του ΟΑ με ηλεκτρικό ρεύμα.

vii. Εφόσον ο ΟΑ έχει συμβληθεί με εξωτερικούς συνεργάτες για θέματα ασφάλειας και επαναφοράς του συστήματός του, απαιτείται ο καθορισμός του τρόπου - χρόνου επικοινωνίας και ανταπόκρισης αυτών στα πλαίσια περιστατικού κυβερνοεπίθεσης.

viii. Αξιολόγηση πεπραγμένων και αναζήτηση ευθυνών με το πέρας του περιστατικού κυβερνοεπίθεσης.

ix. Αποτύπωση του ΣΣΛ με εύληπτο τρόπο, φύλαξή του σε διαβαθμισμένο χώρο και μέριμνα για τη διαδικυακή διάχυσή του στο προσωπικό μέσω των κωδικών που έχουν δημιουργηθεί ήδη από το τμήμα διαχείρισης διαδικτυακής

[18] Uninterruptible Power Supply

επικοινωνίας για κάθε υπάλληλο για τη πρόσβασή του σε αντίγραφα ασφαλείας (σ6). Εκτίμηση του βαθμού τήρησης και επικαιροποίησης του ΣΣΛ, βάσει νεότερων τεχνολογικών εξελίξεων και απειλών.

x. Η πρόβλεψη εκπαίδευσης του προσωπικού σε συνθήκες προσομοίωσης μιας κυβερνοεπίθεσης και εξοικείωσης με συναφή νέα εργαλεία/τεχνολογίες με τη συμμετοχή του Υπευθύνου δικτύου, σε τετράμηνη βάση, και σχετική ενημέρωση της Διοίκηση του οργανισμού.

xi. Έλεγχοι δοκιμών σε τριμηνιαία βάση για τη διασφάλιση της ικανοποιητικής λειτουργίας των υποσυστημάτων και του συνολικού πληροφοριακού συστήματος του ΟΑ.

xii. Πρόβλεψη προμήθειας πέντε νέων συσκευών Η/Υ (μη εγκατεστημένοι στο δίκτυο), που θα λειτουργήσουν εφεδρικά, σε περίπτωση που καταστραφεί/ προσβληθεί από ιό ο υφιστάμενος εξοπλισμός.

ΚΕΦΑΛΑΙΟ ΙΙ: ΔΙΑΧΕΙΡΙΣΗ ΚΡΙΣΕΩΝ

Το αποτέλεσμα της κυβερνοεπίθεσης που πραγματοποιείται στον ΟΑ καθιστά αδύνατη τη πρόσβαση στη κεντρική σελίδα του στο διαδίκτυο ενώ συγχρόνως κάποιοι Η/Υ του προσωπικού έχουν υποστεί κρυπτογράφηση των αρχείων και για την ανάκτησή τους ζητείται η καταβολή λύτρων σε μορφή κρυπτονομίσματος[19] (bitcoins). Η αντιμετώπιση των συγκεκριμένων περιστατικών (crisis management), απαιτεί την υλοποίηση κάποιων ενεργειών πριν, κατά τη διάρκεια και μετά την εμφάνισή τους (https://careersincybersecurity.com)

1. ΕΝΕΡΓΕΙΕΣ ΠΡΟΕΤΟΙΜΑΣΙΑΣ

Η προετοιμασία για το περιστατικό ισοδυναμεί με διαπίστωση του βαθμού επικαιροποίησης του ΣΣΛ, ενσωμάτωση και εξοικείωση νέων εργαλείων και τεχνολογιών σε θέματα κυβερνοεπιθέσεων, επιμόρφωση του προσωπικού.

2. ΕΝΕΡΓΕΙΕΣ ΚΑΤΑ ΤΗ ΔΙΑΡΚΕΙΑ ΤΟΥ ΠΕΡΙΣΤΑΤΙΚΟΥ

Η αποκατάσταση της κεντρικής διαδικτυακής σελίδας του ΟΑ και η αδυναμία πρόσβασης σε αρχεία/δεδομένα μέσω των Η/Υ του προσωπικού, θα αντιμετωπιστεί με την επέμβαση των τεχνικών της μονάδας πληροφορικής, που όπως έχει προβλεφθεί στα πλαίσια της δημιουργίας του ΣΣΛ (ii. a, σ14), θα προβούν σε αποσύνδεση και αντικατάσταση των Η/Υ (xii,σ16) που προσβλήθηκαν, λαμβάνοντας τα απαιτούμενα μέτρα για την ασφάλειά τους (§2.3, σ9).

Μεταξύ των ενεργειών που θα πρέπει απαρέγκλιτα να πραγματοποιηθούν, είναι η αποφυγή πληρωμής των συγκεκριμένων λύτρων σε μορφή κρυπτονομίσματος[20].Η συγκεκριμένη επιλογή υποστηρίζεται από την πρόβλεψη στα πλαίσια της πολιτικής ασφάλειας, λήψης αντιγράφων ασφάλειας (v. σ15&σ9), γεγονός που θα αξιοποιηθεί στη προκειμένη περίπτωση από το προσωπικό του οργανισμού[21]. Φυσικά αυτό προϋποθέτει τα αντίγραφα ασφαλείας που διαθέτει να είναι επικαιροποιημένα (λήψη αυτών σε ημερήσια βάση), άμεσα προσβάσιμα (φύλαξη σε εξωτερικό server του ΟΑ) καθώς επίσης και το να είναι κατάλληλα εκπαιδευμένο το προσωπικό ώστε να τα

[19] Το κρυπτονόμισμα αποτελεί ένα είδος ψηφιακού ή εικονικού χρήματος , που δεν πρέπει να συγχέεται με το ηλεκτρονικό χρήμα, που εκφράζει εθνικά νομίσματα.
[20] Ως διαδικασία αφορά τη μετατροπή χρημάτων σε κρυπτονόμισμα, τα οποία στη συνέχεια θα σταλούν σε μια ανώνυμη διεύθυνση (https://tictac.gr/ti-einai-to-bitcoin/)
[21] Το μήνυμα ωστόσο που θα σταλεί παρέχοντας στο εξουσιοδοτημένο προσωπικό πρόσβαση στα αρχεία αντιγράφων ασφαλείας, θα είναι σε κρυπτογραφημένη μορφή .

ανακαλέσει και να τα εγκαταστήσει ώστε να επιτελούν τις καθιερωμένες λειτουργίες του ΟΑ. Ομοίως έχει προβλεφθεί η ύπαρξη εναλλακτικής κεντρικής σελίδας, εγκατεστημένης σε απομακρυσμένο server του ΟΑ, η οποία τίθεται σε λειτουργία μετά από περιστατικό επίθεσης, όπως αυτό που περιγράφηκε.

Ο προσδιορισμός του είδους της επίθεσης θα πρέπει να εστιάσει στη ταυτότητα και τον αριθμό των Η/Υ που έχουν προσβληθεί, στο χρόνο που θα απαιτηθεί για την αποκατάσταση της κεντρικής ιστοσελίδας του ΟΑ, το βαθμό που η εφεδρική κεντρική σελίδα του ΟΑ λειτουργεί απρόσκοπτα και αν παρατηρείται κάποια ασυνήθιστη δραστηριότητα από χρήστες (μέσω παρακολούθησης αναρτημένων σχολίων).

Επιβεβλημένο είναι επίσης το βήμα ενημέρωσης της ΑΠΔΠΧ, της Δίωξης Ηλεκτρονικού εγκλήματος, της CSIRT κατά το ΣΣΛ (iii. σ15), ενώ η ενημέρωση στην οποία θα προβεί ο Υπεύθυνος επικοινωνίας του ΟΑ θα πρέπει να αποσκοπεί στη διαβεβαίωση επανόρθωσης οποιασδήποτε βλάβης υπέστησαν στα πλαίσια παράνομης επεξεργασίας των δεδομένων τους, οι χρήστες του οργανισμού.

3. ΕΛΛΕΙΜΜΑΤΙΚΕΣ ΠΕΡΙΟΧΕΣ

Ωστόσο θα πρέπει να εξετασθεί ποιό σημείο του ΣΣΛ και της πολιτικής ασφάλειας του ΟΑ αποδείχθηκε ελλιπές, ώστε να πραγματοποιηθεί το συγκεκριμένο διπλό περιστατικό.

Το ενδεχόμενο της αγοράς ενός αντι-ιομορφικού προγράμματος (antivirus), η οποία έγινε χωρίς την επαρκή εκτίμηση των δυνατοτήτων του ως προς τις ανάγκες ασφάλειας που θα έπρεπε να καλύψει, αποτελεί μια πιθανή εξήγηση. Σε αυτή τη περίπτωση ακόμα και αν υπήρξε πιστοποιημένο κατά ISO, δεν μπορούσε να έχει μια ευνοϊκότερη εξέλιξη ως προς την αποτροπή ή αποφυγή του περιστατικού που σημειώθηκε, καθώς το βασικό πρόβλημα είναι η ελλιπής εκτίμηση των αναγκών ασφάλειας από τον σχεδιασμό (security by design). Δεν μπορεί επίσης να αποκλειστεί το ότι η συγκεκριμένη επιλογή έλαβε χώρα υπό την πίεση που ασκεί μια εκτεταμένη προσπάθεια εξοικονόμησης πόρων στο δημόσιο τομέα, με αποτέλεσμα το συγκεκριμένο λογισμικό να ήταν εγνωσμένα χαμηλότερων δυνατοτήτων (και κόστους), προκειμένου να ανταποκριθεί στις καθημερινές λειτουργίες του οργανισμού και όχι σε περιστατικά μεγαλύτερης επικινδυνότητας. Ωστόσο σε αυτή τη

περίπτωση είναι προφανές ότι παραβιάζεται η αρχή της αναλογικότητας των εκτιμούμενων μέσων ασφάλειας που θα απαιτούνταν, ως προς το κόστος που θα συνεπάγονταν.

Η κατάρρευση της κεντρικής σελίδας του ΟΑ, είναι δυνατό να συναρτάται εκτός από το περιστατικό της κρυπτογράφησης αρχείων που υπέστησαν Η/Υς του προσωπικού λόγω μη ενδεδειγμένου antivirus, σε ανθρώπινο σφάλμα προγραμματισμού, σε ένα ή περισσότερους Η/Υ ή στο κεντρικό εξυπηρετητή. Ήδη έχει αναφερθεί η σημασία της ορθής ρύθμισης του firewall από τον διαχειριστή του δικτύου (σ13)(www.thetoc.gr).

4. ΕΝΕΡΓΕΙΕΣ ΑΝΑΤΡΟΦΟΔΟΤΗΣΗΣ -ΑΝΑΣΧΕΔΙΑΣΜΟΥ

Προτείνεται η ποιοτική (και ενδεχομένως κοστολογική) αναβάθμιση του αντι-ιομορφικού λογισμικού του ΟΑ, ειδικότερα στο χώρο των κοινόχρηστων Η/Υ του computer room, που δεν βρίσκεται υπό την αποκλειστική εποπτεία και χρήση ενός συγκεκριμένου προσώπου, καθιστώντας τους ακόμα πιο ευάλωτους σε κακόβουλο λογισμικό.

Επισημάνθηκε έλλειμμα στο πεδίο του προγραμματισμού του δικτύου (εσφαλμένος χειρισμός των firewalls) το οποίο συνεπάγεται ότι καταστρατηγήθηκε πρακτικά η αρχή της ασφάλειας εξ ορισμού (security by default). Η αποφυγή επανάληψης ανάλογου περιστατικού θα ήταν δυνατή εφόσον ο διαχειριστής του δικτύου είτε επιμορφωνόταν στο συγκεκριμένο αντικείμενο είτε αντικαθίστατο από άτομο που να διαθέτει αποδεδειγμένα τη σχετική εμπειρία.

Σημαντική κρίνεται η ανάληψη δράσεων που σχετίζονται με την εκπαίδευση του κοινού (με τη μορφή διήμερων σεμιναρίων σε εξαμηνιαία βάση για τους εγγεγραμμένους χρήστες του ΟΑ) και του προσωπικού, για ζητήματα που αφορούν κυβερνοεπιθέσεις και κακόβουλο λογισμικό τελευταίας αιχμής· προτείνονται επίσης ασκήσεις ετοιμότητας σε περιστατικά κυβερνοεπιθέσεων (αφορά μόνο το προσωπικό του ΟΑ). Τα ανωτέρω ενώ προβλέπονται στα πλαίσια της εθνικής στρατηγικής ασφάλειας του κυβερνοχώρου για τα συστήματα δικτύου και πληροφοριών, εν προκειμένω, στον ΟΑ κάλυψαν μόνο το σκέλος του προσωπικού (σημείο x, σ16). Παραμένει ωστόσο κρίσιμο να εξεταστεί στα πλαίσια μιας αξιολόγησης πεπραγμένων σε σχέση με τη τηρούμενη πολιτική ασφάλειας αν πράγματι έλαβαν χώρα αυτές οι

δράσεις, το οποίο προτείνεται να καταγράφεται από τον Υπεύθυνο ασφάλειας του ΟΑ.

Η κρισιμότητα ενός περιστατικού κυβερνοεπίθεσης όπως αυτού που συντελέσθηκε, επιτάσσει την αναζήτηση/απόδοση ευθυνών μεταξύ των βασικών ρόλων του συστήματος. Η συγκεκριμένη έρευνα θα πρέπει να ξεκινήσει από το σημείο ii. που προβλέπεται στο ΣΣΛ (σ14), σε σχέση με το ρόλο που επιτέλεσε κάθε τμήμα κατά το περιστατικό.

Όπως επισημάνθηκε και στο ΣΣΛ η ανάγκη επανεξέτασης των μέτρων ασφάλειας είναι απαραίτητη και ορίζεται σε εξαμηνιαία βάση. Μεταξύ αυτών ο ΟΑ λειτουργώντας προληπτικά, θα ήταν σκόπιμο να αυστηροποιήσει τους ελέγχους εφαρμογών, που εγκαθίστανται και εκτελούνται στο σύστημά του. Η κατασκευή μιας whitelist με τις λεπτομερώς ελεγμένες εφαρμογές, θα αποτελούσε φραγμό στην εκτέλεση κακόβουλου λογισμικού (Murno, 2012)

Τέλος η συμμετοχή του ΟΑ σε ένα δίκτυο οργανωμένο από τη διεθνή επιστημονική κοινότητα, προκειμένου να συμβάλλει στην ευαισθητοποίηση, αναγνώριση και αντιμετώπιση παρόμοιων περιστατικών κυβερνοεπιθέσεων σε άλλους οργανισμούς, θα διεύρυνε σημαντικά και τη δική του επάρκεια και ετοιμότητα επί του θέματος. (Εγχειρίδιο Μαθήματος, 2019,σ109)

ΒΙΒΛΙΟΓΡΑΦΙΑ-ΔΙΑΔΙΚΤΥΑΚΟΙ ΤΟΠΟΙ

- Εγχειρίδιο Μαθήματος, 2019: ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ ΣΤΗ ΔΗΜΟΣΙΑ ΔΙΟΙΚΗΣΗ, ΕΘΝΙΚΟ ΚΕΝΤΡΟ ΔΗΜΟΣΙΑΣ ΔΙΟΙΚΗΣΗΣ & ΑΥΤΟΔΙΟΙΚΗΣΗΣ.
- Murno K. (2012). Deconstructing Flame: the limitations of traditional defenses. Elsevier, Computer Fraud & Security, Volume 2012, Issue 10, pp.8-11.
- Για το Σύστημα Ηλεκτρονικής Διαχείρισης Εγγράφων «ΙΡΙΔΑ»: Υπουργείο Εσωτερικών (2018): Σε πλήρη λειτουργία το νέο Πληροφοριακό Σύστημα Ηλεκτρονικής Διαχείρισης Εγγράφων «ΙΡΙΔΑ», διαθέσιμο στο: https://government.gov.gr/se-pliri-litourgia-to-neo-pliroforiako-sistima-ilektronikis-diachirisis-engrafon-irida-tou-ipes/ και https://government.gov.gr/ασφαλής-διακίνηση-εγγράφων-στο-δημόσ/, Πρόσβαση 30/11/2019.
- Κανονισμός Επικοινωνίας Δημοσίων Υπηρεσιών (Κ.Ε.Δ.Υ.), Υπουργείο Εσωτερικών Δημόσιας Διοίκησης και Αποκέντρωσης, Γενική Γραμματεία Δημόσιας Διοίκησης, Γενική Διεύθυνση Διοικητικής Οργάνωσης και Διαδικασιών, Διεύθυνση Απλούστευσης Διαδικασιών και Παραγωγικότητας, Αθήνα 2003. Διαθέσιμο στο: http://tdp.admin.ntua.gr/KEDY.pdf, Πρόσβαση 30/11/2019.
- Για το ΓΚΠΔ, (GDPR) Κανονισμός 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της ΕΕ: Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης, LL119, Νομοθεσία 59ο έτος, 4 Μαΐου 2016. Διαθέσιμο στο: https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=EL, Πρόσβαση 30/11/2019.
- Για το Risk Assessment: Ανάρτηση στο διαδικτυακό χώρο του Health and Safety Executive: Risk- Controlling the risks in the workplace, διαθέσιμο στο: http://www.hse.gov.uk/risk/controlling-risks.htm, Πρόσβαση 30/11/2019.
- Για το Risk Assessment: Ανάρτηση στο διαδικτυακό χώρο του Ευρωπαϊκού οργανισμού για την ασφάλεια και την υγεία στην εργασία, διαθέσιμο στο: https://oiraproject.eu/el/what-risk-assessment, Πρόσβαση 30/11/2019.
- Για το ΣΣΛ: Ανάρτηση στο διαδικτυακό χώρο airmic.com: Hewitt S., Six-step plan for dealing with a cyber security breach, διαθέσιμο στο:

https://www.airmic.com/news/six-step-plan-dealing-cyber-security-breach, Πρόσβαση 30/11/2019.

- Για το ΣΣΛ: Ανάρτηση στο διαδικτυακό χώρο Information Age: Rossi B., (2015). 6 critical steps fro responding to a cyber security. Διαθέσιμο στο: https://www.information-age.com/6-critical-steps-responding-cyber-attack-123459644/, Πρόσβαση 30/11/2019.
- Crisis Management: Ανάρτηση στο διαδικτυακό χώρο Careers in cyber security: Crisis Management: 7 Steps to contain a cyber attack, διαθέσιμο στο: https://careersincybersecurity.com/crisis-management-7-steps-contain-cyber-attack/, Πρόσβαση 30/11/2019.
- Κατάρρευση ιστότοπου: Ανάρτηση στο διαδικτυακό χώρο The TOC Times of change, 15/3/2019, διαθέσιμο στο: https://www.thetoc.gr/diethni/article/ena-anthrwpino-lathos-i-aitia-katarreusis-facebook-kai-instagram, Πρόσβαση 30/11/2019.