ΕΠΙΤΡΟΠΟΣ ΕΠΙΚΟΙΝΩΝΙΩΝ
Αρχή Ψηφιακής Ασφάλειας

NCC
ΕΘΝΙΚΟ ΚΕΝΤΡΟ ΣΥΝΤΟΝΙΣΜΟΥ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ
ΚΥΠΡΟΥ

ΠΛΑΙΣΙΟ ΚΥΒΕΡΝΟ-ΥΓΙΕΙΝΗΣ ΓΙΑ ΜΙΚΡΟΜΕΣΑΙΕΣ ΕΠΙΧΕΙΡΗΣΕΙΣ

ΑΡΧΗ ΨΗΦΙΑΚΗΣ ΑΣΦΑΛΕΙΑΣ (ΑΨΑ)
ΕΘΝΙΚΟ ΚΕΝΤΡΟ ΣΥΝΤΟΝΙΣΜΟΥ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ (NCC-CY)

ΟΚΤΩΒΡΙΟΣ 2023

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΙΝΑΚΕΣ

ΓΡΑΦΗΜΑΤΑ

ΧΑΙΡΕΤΙΣΜΟΣ ΕΠΙΤΡΟΠΟΥ

Στην περίοδο του ψηφιακού μετασχηματισμού στην οποία βρισκόμαστε, η Κύπρος έχει διεισδύσει βαθιά στην ψηφιακή μεταρρύθμιση με κύριο μέλημα την αναβάθμιση της ψηφιακής ωριμότητας της κοινωνίας σε όλους τους τομείς. Μία αναβάθμιση από την οποία δεν θα μπορούσε να λείπει η ραχοκοκαλιά της οικονομίας μας, οι μικρομεσαίες επιχειρήσεις (ΜμΕ), οι οποίες στηρίζουν και επιταχύνουν την ανάπτυξη και την καινοτομία της οικονομίας. Ωστόσο, ο θησαυρός τους είναι τα δεδομένα τους. Έτσι, προστατεύοντας τα δεδομένα μιας επιχείρησης διασφαλίζεται η λειτουργικότητα ενώ παράλληλα διευρύνεται η ευρηματικότητα.

Η Αρχή Ψηφιακής Ασφάλειας (ΑΨΑ) ως το Εθνικό Κέντρο Συντονισμού Κυβερνοασφάλειας (NCC-CY) λειτουργεί συντονισμένα, σε συνεργασία με τον δημόσιο και τον ιδιωτικό τομέα, τους ερευνητικούς και τεχνολογικούς φορείς, την ακαδημαϊκή και επιστημονική κοινότητα για την βελτίωση του επιπέδου κυβερνοασφάλειας κυρίως στις ΜμΕ. Το NCC-CY παροτρύνει την εφαρμογή του Πλαισίου Κυβερνο-υγιεινής για τις ΜμΕ, ώστε να μπορέσουν να ανταποκριθούν αποτελεσματικά στις σύγχρονες προκλήσεις της ψηφιακής εποχής.

Με την υλοποίηση του Πλαισίου Κυβερνο-υγιεινής, οι ΜμΕ θα ενισχύσουν το ανταγωνιστικό τους πλεονέκτημα, την προστασία των υποδομών και των πληροφοριών τους και θα δοθεί η δυνατότητα να ξεχωρίσουν στην αγορά. Επιπλέον, η εφαρμογή αυτών των σημείων ελέγχου θα διασφαλίσει την εμπιστοσύνη, την ακεραιότητα και τη διαθεσιμότητα των πληροφοριών τους, προστατεύοντας έτσι την επιχειρηματική τους δραστηριότητα. Επιπλέον, οι ΜμΕ θα αποκτήσουν αξιοπιστία στη λειτουργία της υποδομής τους, καθώς θα είναι ευέλικτες και θα έχουν ψηλότερο επίπεδο ελέγχου επί των θεμάτων της κυβερνοασφάλειας.

Η κυβερνοασφάλεια είναι ομαδική δραστηριότητα και χρειάζεται τη συνεισφορά όλων μας. Το NCC-CY προωθεί ένα πνεύμα συνεργασίας και επιδιώκει να σφραγίσει την ασφάλεια της κάθε επιχείρησης στον κυβερνοχώρο, μέσω του Πλαισίου Κυβερνο-υγιεινής. Το όραμά μας είναι να παρέχουμε στις ΜμΕ ένα υγιές περιβάλλον για να αναπτύξουν τις δυνατότητες τους περιορίζοντας στο ελάχιστο, τους κινδύνους που ελλοχεύουν.

Μιχαηλίδης Γιώργος

Επίτροπος Επικοινωνιών

ΕΠΙΤΡΟΠΟΣ ΕΠΙΚΟΙΝΩΝΙΩΝ | Αρχή Ψηφιακής Ασφάλειας
NCC
ΙΔΡΥΜΑ ΕΡΕΥΝΑΣ ΚΑΙ ΚΑΙΝΟΤΟΜΙΑΣ

ΠΛΑΙΣΙΟ ΚΥΒΕΡΝΟ-ΥΓΙΕΙΝΗΣ ΓΙΑ ΜΙΚΡΟΜΕΣΑΙΕΣ ΕΠΙΧΕΙΡΗΣΕΙΣ (ΜΜΕ)

ΠΡΟΛΟΓΟΣ

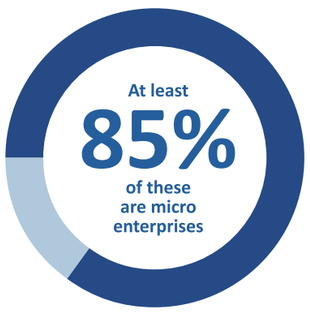
Με Απόφαση του Υπουργικού Συμβουλίου την 21η Δεκεμβρίου 2021 η Αρχή Ψηφιακής Ασφάλειας (ΑΨΑ) ορίστηκε ως το Εθνικό Κέντρο Συντονισμού Κυβερνοασφάλειας (NCC-CY-National Coordination Centre) στην Κυπριακή Δημοκρατία.

Το NCC-CY έχει ως αποστολή τη διατήρηση και την ενίσχυση του επιπέδου Κυβερνοασφάλειας στην Κυπριακή Δημοκρατία και να ενισχύσει τις αντίστοιχες προσπάθειες αλλά και να συμβάλει αντίστοιχα σε επίπεδο Ευρωπαϊκής Ένωσης. Μια από τις δράσεις του NCC-CY είναι η στήριξη της κοινότητας στην παραγωγή καινοτομίας, αλλά και η ενίσχυση και η ανάπτυξη της Κυβερνοασφάλειας κυρίως στις μικρομεσαίες επιχειρήσεις (ΜμΕ), με απώτερο σκοπό να καταστεί η Κυπριακή Δημοκρατία πρωτοπόρος στον τομέα της Κυβερνοασφάλειας, διασφαλίζοντας έναν αξιόπιστο και προστατευμένο κυβερνοχώρο για όλους τους πολίτες και τις επιχειρήσεις.

Το NCC-CY, στα πλαίσια των αρμοδιοτήτων του, και με σκοπό την ενίσχυση και την ανάπτυξη της ανθεκτικότητας της κυβερνοασφάλειας, ειδικότερα στην οικοδόμηση μέτρων κυβερνοασφάλειας στις μικρομεσαίες επιχειρήσεις (ΜμΕ), επισημαίνει και αναλύει τα βασικά σημεία ελέγχου ασφάλειας στον κυβερνοχώρο ως προηγμένες βέλτιστες πρακτικές και συμβουλές. Το παρόν έγγραφο δίνει τη δυνατότητα στις ΜμΕ να αξιολογήσουν το τρέχον επίπεδο ωριμότητάς τους, να προσδιορίσουν τα τρωτά σημεία τους και να μετριάσουν τον κίνδυνο, ενισχύοντας παράλληλα τις πρακτικές κυβερνοασφάλειας που εφαρμόζουν ώστε να επενδύσουν σωστά στην προστασία των πληροφοριών και των δεδομένων τους.

ΕΙΣΑΓΩΓΗ

ΜΙΚΡΟΜΕΣΑΙΕΣ ΕΠΙΧΕΙΡΗΣΕΙΣ



Average cost of a data breach by country or region
Source: Cost of a Data Breach Report 2022, IBM
3R8N1DZJ (ibm.com)

Σύμφωνα με τη Σύσταση της Επιτροπής των Ευρωπαϊκών Κοινοτήτων με ημερομηνία 06/05/2003 και αρ. 2003/361/ΕΚ ο ορισμός των «Μικρομεσαίων Επιχειρήσεων» (ΜμΕ) ορίζεται με βάση:

- τον αριθμό των υπαλλήλων
  Απασχολούν <250 άτομα
- τον κύκλο εργασιών ή το σύνολο του ισολογισμού
  Έχουν ≤ € 50 εκατ. ετήσιου κύκλου εργασιών ή ≤ € 43 εκατ. Ετήσιου συνολικού ισολογισμού.

Όπως αναγράφεται και στην σχετική ιστοσελίδα της Ευρωπαϊκής Επιτροπής:

«Οι μικρές και μεσαίες επιχειρήσεις (ΜμΕ) αποτελούν τη ραχοκοκαλιά της ευρωπαϊκής οικονομίας. Αντιπροσωπεύουν το 99 % του συνόλου των επιχειρήσεων στην ΕΕ. Απασχολούν περίπου 100 εκατομμύρια άτομα, αντιπροσωπεύουν περισσότερο από το ήμισυ του Ακαθάριστου Εγχώριου Προϊόντος της Ευρώπης και διαδραματίζουν καίριο ρόλο στην προστιθέμενη αξία σε κάθε τομέα της οικονομίας. Οι ΜμΕ φέρνουν καινοτόμες λύσεις σε προκλήσεις όπως η κλιματική αλλαγή, η αποδοτική χρήση των πόρων και η κοινωνική συνοχή και συμβάλλουν στη διάδοση αυτής της καινοτομίας σε όλες τις περιφέρειες της Ευρώπης. Ως εκ τούτου, είναι καίριας σημασίας για τη διττή μετάβαση της ΕΕ σε μια βιώσιμη και ψηφιακή οικονομία. Είναι ουσιαστικής σημασίας για την ανταγωνιστικότητα και την ευημερία της Ευρώπης, τα βιομηχανικά οικοσυστήματα, την οικονομική και τεχνολογική κυριαρχία και την ανθεκτικότητα σε εξωτερικούς κλυδωνισμούς.»[1]

[1] https://single-market-economy.ec.europa.eu/smes_el?etrans=el

ΕΠΙΤΡΟΠΟΣ ΕΠΙΚΟΙΝΩΝΙΩΝ | Αρχή Ψηφιακής Ασφάλειας
NCC | ΙΔΡΥΜΑ ΕΡΕΥΝΑΣ ΚΑΙ ΚΑΙΝΟΤΟΜΙΑΣ

ΜΜΕ ΣΤΗΝ ΚΥΠΡΟ

Σύμφωνα με τα στοιχεία της Στατιστικής Υπηρεσίας Κύπρου και τα στοιχεία του CYSTAT-DB[2], οι επιχειρήσεις στην Κύπρο που απασχολούν μέχρι 249 άτομα ανεξάρτητα από την οικονομική δραστηριότητα υπερβαίνουν (στοιχεία ενημερωμένα 21/12/2021) τις 100.000.

Η κατανομή των δυνητικά μικρομεσαίων επιχειρήσεων[3] (σύμφωνα με το πλήθος απασχολούμενου προσωπικού) αποτυπώνεται στον Πίνακα 1.

Πίνακας 1: Κατανομή των δυνητικά μικρομεσαίων επιχειρήσεων

2018			2019			2020		
Αριθμός Επιχειρήσεων			Αριθμός Επιχειρήσεων			Αριθμός Επιχειρήσεων		
0-9	10-49	50-249	0-9	10-49	50-249	0-9	10-49	50-249
95,879	4,443	710	101,550	4,655	731	103,836	4,550	714

Στον Πίνακα 1 φαίνεται επίσης, ότι το πλήθος των επιχειρήσεων αυτής της κατηγορίας, αυξάνεται κάθε χρόνο.

ΜΜΕ ΚΑΙ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ

Το 2021, ο ENISA (European Union Agency for Cybersecurity), διενήργησε ανάλυση σχετικά με την ικανότητα των Ευρωπαϊκών ΜμΕ να ανταπεξέλθουν στις προκλήσεις σχετικά με την κυβερνοασφάλεια, που προέκυψαν από την πρόσφατη πανδημία COVID19[4].

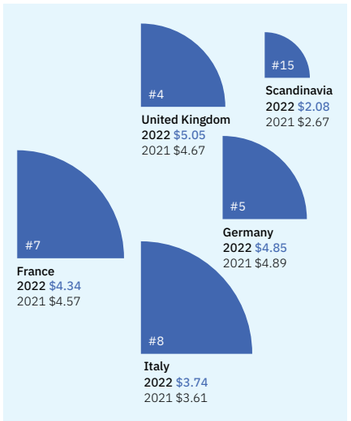
Κάποια από τα συμπεράσματα στα οποία κατέληξε η ανάλυση είναι τα ακόλουθα:

- Οι Ευρωπαϊκές ΜμΕ εμφανίζονται να κατανοούν ότι η κυβερνοασφάλεια είναι ένα σημαντικό ζήτημα, καθώς και ότι έχουν μεγάλη εξάρτηση από την υποδομή πληροφορικής και επικοινωνιών (ICT infrastructure).
- Περισσότερες από το 80% των Ευρωπαϊκών ΜμΕ που συμμετείχαν στην έρευνα που διενεργήθηκε, αναφέρουν ότι πιθανά περιστατικά κυβερνοασφάλειας θα είχαν πολύ σημαντικές αρνητικές επιπτώσεις για την επιχείρησή τους ακόμα και από την πρώτη εβδομάδα μετά την έλευση του περιστατικού.
- Το 36% των Ευρωπαϊκών ΜμΕ που συμμετείχαν στην έρευνα απάντησε ότι είχε κάποιο περιστατικό ασφαλείας τα τελευταία 5 χρόνια.
- Οι Ευρωπαϊκές ΜμΕ φαίνονται να υλοποιούν κάποια από τα βασικά μέτρα, μόνο ως μέρος της συνολικής υλοποίησης πληροφορικής. Παρόλα αυτά, φαίνεται ότι, εκτός αν τα μέτρα αυτά είναι μέρος κάποιας λύσης πληροφορικής, πολλές ΜμΕ δεν κατανοούν τους κινδύνους τους οποίους διατρέχουν σε επίπεδο κυβερνοασφάλειας.

[2] https://cystatdb.cystat.gov.cy/ με σημεία ελέγχου: Οικονομική δραστηριότητα: ΣΥΝΟΛΟ, Έτη 2018, 2019, 2020 και μέγεθος επιχείρησης 0-9 άτομα, 10-49 άτομα και 50-249 άτομα.
[3] Δυνητικά διότι υπάρχει και το δεύτερο σημεία ελέγχου σχετικά με τον κύκλο εργασιών ή τον ετήσιο συνολικό ισολογισμό για τα οποία δεν παρέχονται στοιχεία στην συγκεκριμένη πηγή.
[4] Cybersecurity for SMEs, Challenges and Recommendations, June 2021, https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes

Κόστος περιστατικών ασφάλειας

Από την άλλη πλευρά, αξίζει να σημειωθεί ότι «Οι επιθέσεις στον κυβερνοχώρο συνέχισαν να αυξάνονται κατά το δεύτερο εξάμηνο του 2021 και του 2022, όχι μόνο ως προς τα είδη επιθέσεων και τους αριθμούς αλλά και ως προς την επίδρασή τους»[5], ενώ το κόστος κατά μέσο όρο των περιστατικών αυξάνεται συνεχώς.



Πηγή: European Commission - Annual Report on European SMEs 2021/2022 (SME AR 2021_22_Final Report)

Όπως αναφέρεται στην έκθεση της IBM[6]:

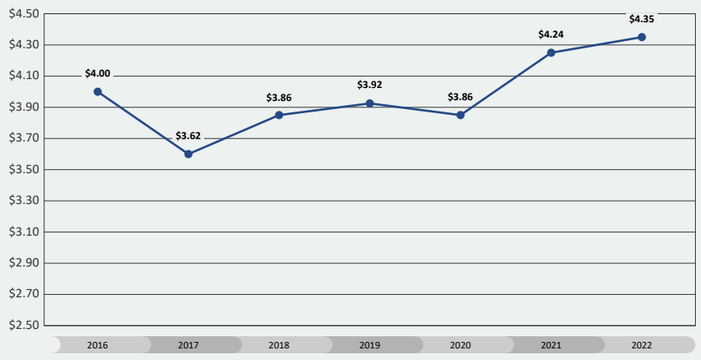
- Το μέσο κόστος μιας παραβίασης δεδομένων έφτασε σε υψηλό επίπεδο το 2022.
- Το κόστος ανά ρεκόρ μιας παραβίασης δεδομένων έφτασε στο υψηλότερο επίπεδο των τελευταίων επτά ετών

Επιπλέον, σύμφωνα με τα στοιχεία των παγκύπριων ερευνών που διεξήγαγε η Αρχή Ψηφιακής Ασφάλειας εντός του 2022[7], προέκυψε ότι:

- Σχεδόν οι μισές επιχειρήσεις (46%) δέχθηκαν κάποια επίθεση/ παραβίαση τους τελευταίους 12 μήνες με μέσο όρο 3-4 επιθέσεις τον μήνα.

Από τις επιχειρήσεις που δέχθηκαν επίθεση για τις μισές σχεδόν (48%) υπήρξε οικονομικό κόστος που ανέρχεται σε σχεδόν 23 χιλιάδες ευρώ κατά μέσο όρο.

Γράφημα 1: Μέση τιμή κόστους για κάθε παραβίαση δεδομένων



Υπολογίστηκε σε US$

[5] ENISA Threat Landscape Report 2022, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022/@@download/fullReport
[6] Cost of a Data Breach Report 2022, IBM, https://www.ibm.com/downloads/cas/3R8N1DZJ
[7] https://dsa.cy/category/press-releases/consumers-survey

ΕΠΙΤΡΟΠΟΣ ΕΠΙΚΟΙΝΩΝΙΩΝ | Αρχή Ψηφιακής Ασφάλειας
NCC | ΙΔΡΥΜΑ ΕΡΕΥΝΑΣ ΚΑΙ ΚΑΙΝΟΤΟΜΙΑΣ

ΣΚΟΠΟΣ ΤΟΥ ΠΑΡΟΝΤΟΣ ΕΓΓΡΑΦΟΥ

Η Αρχή Ψηφιακής Ασφάλειας (ΑΨΑ) ως το Εθνικό Κέντρο Συντονισμού Κυβερνοασφάλειας (NCC-CY) έχοντας αναγνωρίσει ότι,

- οι ΜμΕ για την Κύπρο αντιπροσωπεύουν το μεγαλύτερο ποσοστό της οικονομίας και επαγγελματικής δραστηριότητας και η συμβολή τους στην σταθερή και ανοδική πορεία ανάπτυξης της Κυπριακής Οικονομίας είναι πολύ σημαντική και
- οι επιπτώσεις περιστατικών κυβερνοασφάλειας μπορεί να έχουν δυσμενείς επιπτώσεις και να διαταράξουν την ορθή λειτουργία και τη συνέχεια της λειτουργίας των ΜμΕ

αποφάσισε να συντάξει το παρόν έγγραφο μέτρων με σκοπό:

- την ανάπτυξη της κουλτούρας της κυβερνοασφάλειας στις ΜμΕ. Το παρόν έγγραφο παρέχει ένα ολοκληρωμένο σύνολο κανόνων, σημείων ελέγχου και διαδικασιών για ένα βασικό επίπεδο ασφάλειας στον κυβερνοχώρο που θα πρέπει να έχουν οι επιχειρήσεις για να προστατευθούν από απειλές στον κυβερνοχώρο ώστε να δημιουργήσουν ή να αναπτύξουν ένα επαρκές επίπεδο κυβερνοασφάλειας,
- την παροχή καθοδήγησης στο αντικείμενο της κυβερνοασφάλειας με τη μορφή συγκεκριμένων πρακτικών μέτρων,
- την αύξηση της επίγνωσης των ΜμΕ σε θέματα και τρόπους προστασίας από κυβερνοαπειλές,
- την παρακίνηση των ΜμΕ να προωθήσουν την υλοποίηση βασικών μέτρων κυβερνοασφάλειας, μέσω δομημένης προσέγγισης,
- τη δημιουργία ενός ενιαίου, ελάχιστου επιπέδου κυβερνοασφάλειας σε όλες τις επιχειρήσεις της Κύπρου,
- την απλοποίηση και προσαρμογή των υπαρχόντων προτύπων για συστήματα διαχείρισης ασφάλειας πληροφοριών (όπως είναι τα ISO/IEC 27001:2022[8], NIST SP 800-53 (revision 5)[9], NIST SP 800-171 (revision 2)[10] και άλλα) στις ανάγκες των ΜμΕ.

[8] https://www.iso.org/standard/27001
[9] https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
[10] https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final

ΣΗΜΕΙΑ ΕΛΕΓΧΟΥ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΜΜΕ

Η ΑΨΑ ως το Εθνικό Κέντρο Συντονισμού Κυβερνοασφάλειας NCC-CY, διεξήγαγε μελέτη για την αναγνώριση και ανάλυση προτύπων, οδηγιών και άλλων δημοσιεύσεων που περιγράφουν τα σημεία ελέγχου κυβερνοασφάλειας σε διεθνές και εθνικό επίπεδο. Τα έγγραφα που εξετάστηκαν αφορούσαν πρακτικές που προτάθηκαν προς εφαρμογή γενικά από οργανισμούς και ειδικά από ΜμΕ.

Η ΑΨΑ ως το NCC-CY, έλαβε υπόψη τα αποτελέσματα της παραπάνω ανάλυσης και δημιούργησε το παρόν έγγραφο σημείων ελέγχου.

Τα σημεία ελέγχου κυβερνοασφάλειας για τις ΜμΕ, χωρίζονται και αναλύονται στις ακόλουθες ενότητες του εγγράφου:

1. Πολιτική Ασφάλειας

2. Ενημέρωση και Εκπαίδευση

3. Ενημέρωση Λογισμικού

4. Προστασία από κακόβουλο λογισμικό

5. Ασφάλεια Δικτύου

6. Αντίγραφα Ασφαλείας

7. Έλεγχος Πρόσβασης

8. Περιστατικά Ασφαλείας

9. Μέτρα Φυσικής Ασφάλειας

10. Προστασία Δεδομένων

11. Ανάλυση Επιχειρησιακών Επιπτώσεων

Η σειρά με την οποία παρουσιάζονται τα κριτήρια κυβερνοασφάλειας ΜμΕ δεν υποδηλώνουν και τη σειρά/προτεραιότητα υλοποίησής τους.

"Icons designed by Freepik"

1. ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΕΙΑΣ

ΣΚΟΠΟΣ

Μέσα από την πολιτική κυβερνοασφάλειας, ο οργανισμός ενημερώνει τα εσωτερικά και εξωτερικά ενδιαφερόμενα μέρη σχετικά με τη δέσμευση και τους στόχους του οργανισμού σε σχέση με την κυβερνοασφάλεια.

ΣΗΜΕΙΟ ΕΛΕΓΧΟΥ 1.1

Η ανώτατη διοίκηση του οργανισμού έχει δημιουργήσει, εγκρίνει και επικοινωνήσει εσωτερικά και εξωτερικά την πολιτική κυβερνοασφάλειας του. Η πολιτική κυβερνοασφάλειας ανασκοπείται κατ' ελάχιστο μια φορά το χρόνο και επικαιροποιείται όπως απαιτείται.

ΠΕΡΙΓΡΑΦΗ

Η πολιτική κυβερνοασφάλειας είναι το ανώτερο ιεραρχικά έγγραφο ενός οργανισμού σε σχέση με την ασφάλεια. Η πολιτική κυβερνοασφάλειας, περιέχει κατ' ελάχιστο:

- Μία δήλωση σχετικά με τη δέσμευση του οργανισμού για την συμμόρφωση προς τις σχετικές με την κυβερνοασφάλεια νομικές, κανονιστικές και συμβατικές απαιτήσεις.
- Μια δήλωση σχετικά με τη δέσμευση του οργανισμού για τη συμμόρφωση με τα σημεία ελέγχου του παρόντος εγγράφου και τυχόν τροποποιήσεων και κατευθυντήριων οδηγιών, που εκδίδονται από την Αρχή Ψηφιακής Ασφάλειας.
- Μια υψηλού επιπέδου περιγραφή των μέτρων που υλοποιεί ο οργανισμός σε σχέση με την κυβερνοασφάλεια.
- Παραπομπή ή περίληψη σε κατάλληλο παράρτημα των λοιπών πολιτικών που έχει δημιουργήσει ο οργανισμός που άπτονται στο θέμα της κυβερνοασφάλειας.
- Τον ορισμό ενός ατόμου της ανώτατης διοίκησης που θα λειτουργεί ως σημείο επαφής ανάμεσα στα ενδιαφερόμενα μέρη και τον οργανισμό σε θέματα κυβερνοασφάλειας.
- Μια δήλωση σχετικά με τη δέσμευση του οργανισμού για την έγκαιρη αντιμετώπιση περιστατικών ασφαλείας και τη σχετική ενημέρωση των ενδιαφερόμενων μερών.
- Μία δήλωση σχετικά με τη δέσμευση του οργανισμού για την εφαρμογή κατάλληλων διορθωτικών ή προληπτικών ενεργειών σε περίπτωση που αυτές τεκμηριωμένα απαιτηθούν από εξουσιοδοτημένα ενδιαφερόμενα μέρη (π.χ. οργανισμός ελέγχου κλπ).

Η πολιτική Κυβερνοασφάλειας θα επικοινωνείται με πρόσφορο τρόπο και θα επαληθεύεται η αποτελεσματικότητα της επικοινωνίας, με το προσωπικό του οργανισμού, στα πλαίσια του σημείου ελέγχου 2.1. Η πολιτική κυβερνοασφάλειας είναι διαθέσιμη, διατηρώντας την αρχή της «ανάγκης γνώσης» (need to know) και σε εξωτερικά ενδιαφερόμενα μέρη.

Η ανώτατη διοίκηση έχει την ευθύνη να αναγνωρίζει αλλαγές στο εξωτερικό ή /και εσωτερικό περιβάλλον του οργανισμού και να επικαιροποιεί την πολιτική και τα λοιπά μέτρα του οργανισμού όπως απαιτείται.

2. ΕΝΗΜΕΡΩΣΗ ΚΑΙ ΕΚΠΑΙΔΕΥΣΗ

ΣΚΟΠΟΣ

Το προσωπικό είναι ενήμερο σχετικά με θέματα προστασίας από κυβερνοαπειλές και λειτουργεί με αυτοπεποίθηση τις σχετικές λειτουργίες στα πλαίσια του ρόλου του.

ΣΗΜΕΙΟ ΕΛΕΓΧΟΥ 2.1

Το προσωπικό που απασχολείται στον οργανισμό και οι χρήστες που έχουν πρόσβαση στις πληροφορίες του (ανεξάρτητα από τη σχέση εργασίας), πρέπει να είναι ενήμεροι (να έχουν επίγνωση), σχετικά με την ασφάλεια πληροφοριών και ειδικότερα με τον τρόπο με τον οποίο συνεισφέρουν σε αυτή μέσα από τον ρόλο τους. Κατάλληλες δράσεις ευαισθητοποίησης για την κυβερνοασφάλεια διενεργούνται σε τακτική βάση και τουλάχιστον μια φορά ανά έτος.

ΠΕΡΙΓΡΑΦΗ

Οι δράσεις ευαισθητοποίησης για την κυβερνοασφάλεια έχουν ως στόχο στην ενημέρωση του προσωπικού για τις ευθύνες του ως προς την κυβερνοασφάλεια του οργανισμού και τα μέσα με τα οποία τις υλοποιεί.

Οι δράσεις ευαισθητοποίησης για την κυβερνοασφάλεια θα πρέπει να σχεδιάζονται λαμβάνοντας υπόψη τους ρόλους του προσωπικού στον οργανισμό, συμπεριλαμβανομένου του εσωτερικού και του εξωτερικού προσωπικού (π.χ. εξωτερικοί σύμβουλοι, προσωπικό προμηθευτών). Οι δράσεις ευαισθητοποίησης για την κυβερνοασφάλεια θα πρέπει να προγραμματίζονται τουλάχιστον ετησίως, έτσι ώστε οι δραστηριότητες να επαναλαμβάνονται και να καλύπτουν επιπλέον και τους νέους εργοδοτούμενους.

Οι δράσεις ευαισθητοποίησης για την κυβερνοασφάλεια μπορεί να υλοποιούνται από εσωτερικό ή και εξωτερικό προσωπικό, να ακολουθούν επίσημα περιγράμματα και θεματολογία ή να ακολουθούν θεματολογία σχεδιασμένη από τον ίδιο τον οργανισμό.

ΣΗΜΕΙΟ ΕΛΕΓΧΟΥ 2.2

Το προσωπικό που απασχολείται από τον οργανισμό και οι χρήστες που έχουν πρόσβαση στις πληροφορίες του (ανεξάρτητα από την σχέση εργασίας), λαμβάνουν εκπαίδευση, κατάρτιση και ενημέρωση σχετικά με τις πολιτικές, τις διαδικασίες, τα μέτρα ασφάλειας που εφαρμόζει ο οργανισμός καθώς και σχετικά τεχνολογικά ή οργανωτικά ζητήματα. Οι παρεχόμενες εκπαιδευτικές δράσεις είναι κατάλληλες και προσαρμοσμένες στις απαιτήσεις ασφαλείας των διαφόρων ρόλων εντός του οργανισμού.

ΠΕΡΙΓΡΑΦΗ

Ο Οργανισμός θα πρέπει να αναγνωρίσει και να καταγράψει ανά ρόλο εργασίας, τις βασικές υπευθυνότητες και αρμοδιότητες σε σχέση με την κυβερνοασφάλεια.

Κατ’ ελάχιστο όλοι οι ρόλοι εργασίας, θα περιλαμβάνουν και την υπευθυνότητα τήρησης των πολιτικών, διαδικασιών και μέτρων ασφαλείας που υλοποιεί ο οργανισμός και σχετίζονται με το ρόλο τους.

ΕΠΙΤΡΟΠΟΣ ΕΠΙΚΟΙΝΩΝΙΩΝ | Αρχή Ψηφιακής Ασφάλειας
NCC | ΙΔΡΥΜΑ ΕΡΕΥΝΑΣ ΚΑΙ ΚΑΙΝΟΤΟΜΙΑΣ

Για τις περιπτώσεις που αναγνωριστούν επιπλέον αρμοδιότητες και υπευθυνότητες ασφάλειας, θα πρέπει να καταγραφούν οι ελάχιστες γνώσεις, δεξιότητες και ικανότητες που απαιτούνται για την ορθή και αποτελεσματική υλοποίησή τους.

Ο οργανισμός θα πρέπει να προσδιορίσει, να προετοιμάσει και να εφαρμόσει ένα κατάλληλο σχέδιο εκπαίδευσης για την κάλυψη των αναγνωρισμένων γνώσεων, δεξιοτήτων και ικανοτήτων, σε περίπτωση που αυτές 1) δεν υπάρχουν ήδη στο προσωπικό και 2) απαιτούν επικαιροποίηση.

Το πρόγραμμα εκπαίδευσης και κατάρτισης θα πρέπει να λαμβάνει διαφορετικές μορφές (π.χ. διαλέξεις ή αυτοδιδασκαλία, να καθοδηγείται από εξειδικευμένο προσωπικό ή συμβούλους (εκπαίδευση στην εργασία), και τα μέλη του προσωπικού που να ακολουθούν διαφορετικές δραστηριότητες). Αντίστοιχα οι μέθοδοι εκπαίδευσης μπορεί να γίνονται σε τάξη, από απόσταση, ή και μέσω συγκεκριμένων εφαρμογών κ.α.

Οι δράσεις εκπαίδευσης και ενημέρωσης αξιολογούνται ως προς την αποτελεσματικότητά τους. Τα αρχεία διατηρούνται τόσο για την παροχή της εκπαίδευσης και ενημέρωσης όσο και για την αποτελεσματικότητά τους.

3. ΕΝΗΜΕΡΩΣΗ ΛΟΓΙΣΜΙΚΟΥ

ΣΚΟΠΟΣ

Τα συστήματα πληροφορικής και επικοινωνιών του οργανισμού έχουν λιγότερες ευπάθειες (vulnerabilities) και άρα είναι λιγότερο εκτεθειμένα στους σχετικούς κινδύνους.

ΣΗΜΕΙΟ ΕΛΕΓΧΟΥ 3.1

Τα συστήματα πληροφορικής και επικοινωνιών του οργανισμού πρέπει να έχουν εγκατεστημένες τις τελευταίες, σταθερές ενημερώσεις ασφαλείας από αξιόπιστες πηγές μόνο (π.χ. κατασκευαστή).

ΠΕΡΙΓΡΑΦΗ

Όλα τα συστήματα έχουν ευπάθειες (vulnerabilities), τις οποίες μπορεί κάποιος κακόβουλος παράγοντας να εκμεταλλευτεί και να προκαλέσει κάποια ζημιά στον οργανισμό.

Ο οργανισμός πρέπει να αναγνωρίσει τα συστήματα πληροφορικής και επικοινωνιών που σχετίζονται με τις πληροφορίες του αλλά και που υποστηρίζουν σημαντικές δραστηριότητές του.

Θα πρέπει να σημειωθεί ότι τα συστήματα αυτά μπορεί να είναι υπολογιστές, φορητοί υπολογιστές, φορητές συσκευές (π.χ. tablet, mobile phones κ.α.), συστήματα τηλεπικοινωνιών (π.χ. τηλεφωνικά κέντρα VoIP), εξυπηρετητές (servers), συσκευές με δυνατότητα διασύνδεσης στο διαδίκτυο και στο δίκτυο του οργανισμού (π.χ. τηλεοράσεις ή άλλες IoT συσκευές).

Στο βαθμό που το επιτρέπουν τα παραπάνω συστήματα, θα πρέπει να είναι ενεργοποιημένες οι αυτόματες ενημερώσεις. Σε περίπτωση που δεν υπάρχει η επιλογή αυτόματων ενημερώσεων, θα πρέπει να υλοποιείται χειροκίνητος έλεγχος για ενημερώσεις από κατάλληλα καταρτισμένο προσωπικό, τουλάχιστον μια φορά το μήνα.

Ειδικότερα για τους εξυπηρετητές, θα πρέπει να εγκαθίστανται οι ενημερώσεις ασφαλείας που έχουν υψηλή και μέση κρισιμότητα εντός τριών μηνών από την ανακοίνωση της αδυναμίας και μετά από σχετική δοκιμή είτε σε άλλο μη κρίσιμο σύστημα, ή μετά από επιβεβαίωση από τον κατασκευαστή ή άλλα μέρη (π.χ. εταιρίες παροχής υπηρεσιών πληροφορικής) ότι, δεν θα δημιουργήσει σημαντικά προβλήματα.

ΣΗΜΕΙΟ ΕΛΕΓΧΟΥ 3.2

Αυτοματοποιημένες ανιχνεύσεις ευπαθειών και δοκιμές παρείσδυσης υλοποιούνται μια φορά ανά έτος.

ΠΕΡΙΓΡΑΦΗ

Για την εξασφάλιση ότι δεν υπάρχουν σημαντικές ευπάθειες στα συστήματα πληροφορικής και επικοινωνιών του οργανισμού, απαιτείται η διενέργεια αυτοματοποιημένης ανάλυσης / ανίχνευσης ευπαθειών τουλάχιστον μια φορά το χρόνο. Η συγκεκριμένη δραστηριότητα μπορεί να γίνεται από τον ίδιο τον οργανισμό ή από άλλο πρόσωπο με την προϋπόθεση της ύπαρξης του κατάλληλου εξοπλισμού / λογισμικών και ορθά καταρτισμένου προσωπικού. Τα αποτελέσματα της ανίχνευσης ευπαθειών καταγράφονται σε σχετική έκθεση, η οποία παραδίδεται στην διοίκηση του οργανισμού και περιλαμβάνει (μεταξύ άλλων) τις ευπάθειες που έχουν ανιχνευθεί ανά σύστημα του οργανισμού, ταξινομημένες βάσει του βαθμού επικινδυνότητάς τους. Ο οργανισμός θα πρέπει να λάβει άμεσα μέτρα ώστε να αντιμετωπίσει τις επιβεβαιωμένες[11] ευπάθειες που βρίσκονται στην υψηλή κατηγορία (CVSS 7-10[12]), καθώς και να δημιουργήσει ένα πλάνο για την διαχείριση των επιβεβαιωμένων τρωτοτήτων που βρίσκονται στην μέση κατηγορία (CVSS 4-6).

Οι δοκιμές παρείσδυσης (penetration tests) διενεργούνται με σκοπό την ουσιαστική και πρακτική αξιολόγηση του επιπέδου ασφαλείας του οργανισμού έναντι σχετικών απειλών. Μια φορά το χρόνο, ο οργανισμός θα πρέπει να διενεργεί εξωτερική δοκιμή παρείσδυσης (external penetration test) από οντότητα με κατάλληλες γνώσεις, εμπειρία και εξοπλισμό. Τα αποτελέσματα της εκάστοτε δοκιμής παρείσδυσης καταγράφονται σε σχετική έκθεση, η οποία παραδίδεται στην διοίκηση του οργανισμού και περιλαμβάνει (μεταξύ άλλων) αναφορές σε τυχόν επιτυχημένη πρόσβαση στα συστήματα, τα σενάρια και βήματα που ακολουθήθηκαν κατά τις δοκιμές (επιτυχείς και ανεπιτυχείς), και τις προτάσεις σχετικά με τον τρόπο διόρθωσης των ανοιχτών σημείων. Ο οργανισμός θα πρέπει να λάβει άμεσα μέτρα ώστε να αντιμετωπίσει τα αναγραφόμενα ως σημαντικά στην σχετική αναφορά (σημεία επιτυχούς παρείσδυσης).

ΣΗΜΕΙΟ ΕΛΕΓΧΟΥ 3.3

Συστήματα πληροφορικής και επικοινωνιών που δεν υποστηρίζονται πλέον από τους κατασκευαστές τους με ενημερώσεις (κατ' ελάχιστον) ασφαλείας (end of life), δεν πρέπει να χρησιμοποιούνται από τον οργανισμό.

ΠΕΡΙΓΡΑΦΗ

Συστήματα πληροφορικής και επικοινωνιών που δεν υποστηρίζονται πλέον από τους κατασκευαστές τους με ενημερώσεις (κατ' ελάχιστον) ασφαλείας (end of life), αποτελούν μια σημαντική αδυναμία για την κυβερνοασφάλεια ενός οργανισμού. Αυτό οφείλεται στο γεγονός ότι μπορεί να έχουν προκύψει ευπάθειες (στο διάστημα από το end of life μέχρι σήμερα), οι οποίες να παρουσιάζουν μεγάλο ρίσκο εκμετάλλευσης τους από κακόβουλους χρήστες, και για τις οποίες να μην υπάρχει κάποιος τρόπος αντιμετώπισης ή επίλυσης.

Ο οργανισμός θα πρέπει να παρακολουθεί τις ημερομηνίες πέραν των οποίων δεν θα υπάρχει σχετική υποστήριξη για τα συστήματα πληροφορικής και επικοινωνιών και να προβαίνει στις κατάλληλες προληπτικές ενέργειες αντικατάστασης, αλλαγής ή αναβάθμισης τους.

Σε περίπτωση που υπάρχει κάποιο σύστημα πληροφορικής και επικοινωνιών που βρίσκεται στο τέλος της χρήσιμης ζωής του (End of Life), και το οποίο δεν μπορεί να αντικατασταθεί ή να αναβαθμιστεί ή να αλλαχθεί (legacy), θα πρέπει με την σύμφωνη γνώμη της διοίκησης του οργανισμού, να λαμβάνονται επιπλέον μέτρα ασφαλείας (π.χ. διαχωρισμός από το υπόλοιπο δίκτυο, περιορισμός πρόσβασης, συγκεκριμένο ωράριο λειτουργίας, αφαίρεση δικαιωμάτων κ.α.).

[11] Με τον όρο επιβεβαιωμένες ευπάθειες εννοείται ότι έχει προηγηθεί διαδικασία επιβεβαίωσης της ύπαρξης της ευπάθειας στα συστήματα του οργανισμού. Η επιβεβαίωση είναι σημαντική δεδομένου ότι μπορεί να εμφανιστεί εσφαλμένα θετικό αποτέλεσμα (false positive).
[12] https://www.first.org/cvss/

4. ΠΡΟΣΤΑΣΙΑ ΑΠΟ ΚΑΚΟΒΟΥΛΟ ΛΟΓΙΣΜΙΚΟ

ΣΚΟΠΟΣ

Τα συστήματα πληροφορικής και επικοινωνιών του οργανισμού είναι προστατευμένα έναντι κακόβουλων λογισμικών.

ΣΗΜΕΙΟ ΕΛΕΓΧΟΥ 4.1

Προγράμματα και λειτουργίες προστασίας έναντι κακόβουλου λογισμικού είναι εγκατεστημένα στο σύνολο των συστημάτων πληροφορικής και επικοινωνιών του οργανισμού. Ενημερώσεις γίνονται σε τακτική βάση.

ΠΕΡΙΓΡΑΦΗ

Με τον όρο κακόβουλο λογισμικό, νοείται οποιοδήποτε λογισμικό που έχει σκόπιμα σχεδιαστεί για να προκαλέσει διαταραχή σε ένα σύστημα πληροφορικής ή επικοινωνιών ή σε ένα σύνολο τους (π.χ. δίκτυο), να διαρρεύσει πληροφορίες, να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε πληροφορίες και συστήματα, να στερήσει την πρόσβαση στον χρήστη σε πληροφορίες ή να αλλοιώσει τα αποθηκευμένα ή μεταδιδόμενα δεδομένα.

Παραδείγματα τύπων κακόβουλου λογισμικού είναι (μεταξύ άλλων) οι ιοί (viruses), τα σκουλήκια (worms), οι δούρειοι ίπποι (Trojan viruses), λογισμικό κατασκοπείας (spyware), διαφημιστικό λογισμικό (adware), και λυτρισμικό (ransomware).

Σε κάθε σύστημα πληροφορικής και επικοινωνιών (όπου αυτό είναι εφικτό και υπάρχει σχετική λύση) θα πρέπει να εγκαθίσταται ή ενεργοποιείται υπηρεσία ή λειτουργία προστασίας έναντι κακόβουλου λογισμικού. Η εγκατάσταση / ενεργοποίηση της σχετικής προστασίας θα πρέπει να εφαρμόζεται σε όλα τα συστήματα ανεξάρτητα από τον κατασκευαστή, το λειτουργικό σύστημα ή το είδος τους.

Θα πρέπει να είναι ενεργοποιημένη η αυτόματη λήψη και εγκατάσταση ενημερώσεων των προγραμμάτων / λειτουργιών και να γίνεται ο σχετικός έλεγχος για ενημερώσεις (των προγραμμάτων αλλά και των σχετικών υπογραφών και άλλων αρχείων ενημέρωσης) τουλάχιστον μια φορά την ημέρα.

Τα προγράμματα και οι λειτουργίες προστασίας από κακόβουλο λογισμικό θα πρέπει να διενεργούν αυτόματη σάρωση (scan) σε αρχεία και προγράμματα (π.χ. όταν κατεβαίνουν και ανοίγουν αρχεία από το διαδίκτυο, όταν ανοίγουν αρχεία από μέσα αποθήκευσης ή από δικτυακές πηγές κ.α.) καθώς και σε ιστοσελίδες κατά την πρόσβαση.

Μια φορά την εβδομάδα, θα πρέπει να διενεργείται αυτόματα μια πλήρης σάρωση και σε περίπτωση εύρεσης κάποιας απειλής, θα πρέπει να υλοποιούνται οι κατάλληλες ενέργειες άμεσα.

Τα προγράμματα και οι λειτουργίες προστασίας από κακόβουλο λογισμικό θα πρέπει να έχουν ενεργοποιημένη την λειτουργία tamper protection ώστε να μην μπορεί η προστασία να απενεργοποιηθεί κατά λάθος ή κακόβουλα.

5. ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΟΥ

ΣΚΟΠΟΣ

Τα συστήματα πληροφορικής και επικοινωνιών του οργανισμού είναι προστατευμένα έναντι απειλών που προέρχονται από το δημόσιο εξωτερικό δίκτυο.

ΣΗΜΕΙΟ ΕΛΕΓΧΟΥ 5.1

Ο οργανισμός έχει εγκαταστήσει και παραμετροποιήσει firewall σε κατάλληλα σημεία του δικτύου του, με σκοπό την αποτελεσματική προστασία των συστημάτων και των πληροφοριών του από τις σχετικές απειλές.

ΠΕΡΙΓΡΑΦΗ

Ο οργανισμός θα πρέπει να εξετάσει την αρχιτεκτονική δικτύου που έχει υλοποιήσει και να εισάγει firewall κατ' ελάχιστο ανάμεσα στο εξωτερικό δίκτυο και το δημόσιο εξωτερικό δίκτυο (internet) και στην συνέχεια σε όποιο άλλο σημείο κρίνεται ότι χρειάζεται για την αύξηση της προστασίας.

Το(α) firewall μπορεί να είναι είτε hardware είτε software και να παραμετροποιηθεί υιοθετώντας την θετική πολιτική (δηλαδή: όλες οι δυνατότητες, πόρτες, πρωτόκολλα απαγορεύονται και στην συνέχεια ενεργοποιείται μόνο ότι είναι αυστηρά απαραίτητο – deny all by default).

Το(α) firewall θα έχει(ουν) ενεργοποιημένους μηχανισμούς παρακολούθησης και καταγραφής των ενεργειών που πραγματοποιούνται ώστε να μπορούν να ανιχνευτούν ενέργειες που μπορεί να επηρεάσουν την ασφάλεια των πληροφοριών ή/και των συστημάτων. Οι καταγραφές (logs) θα πρέπει να τηρούνται για τουλάχιστον 6 μήνες.

Στο(α) firewall πρέπει να υπάρχει(ουν) ενεργοποιημένη δυνατότητα για την προστασία από κακόβουλο λογισμικό (π.χ. ιούς).

Σε περίπτωση που ο οργανισμός κρίνει ότι απαιτείται, μπορεί να εισάγει σύστημα για την ανίχνευση ή και την αυτοματοποιημένη προστασία από εισβολές (IDS/IPS).

Απομακρυσμένη πρόσβαση σε εξουσιοδοτημένα άτομα του οργανισμού, διενεργείται μόνο μέσω ασφαλών καναλιών όπως είναι το VPN (virtual private network). Το(α) firewall θα πρέπει να είναι κατάλληλα παραμετροποιημένα ώστε να επιτρέπουν σύνδεση μόνο μετά από τον κατάλληλο έλεγχο και αυθεντικοποίηση σε επίπεδο χρήστη και σε επίπεδο συσκευής. Μόνο συγκεκριμένες και εξουσιοδοτημένες συσκευές του οργανισμού έχουν δικαίωμα πρόσβασης μέσω VPN στο δίκτυο του οργανισμού.

Οι απαιτήσεις του σημείου ελέγχου 3.1 εφαρμόζονται όπως προβλέπεται και στην περίπτωση των firewall. Τα αποτελέσματα της εφαρμογής του σημείου ελέγχου 3.2 λαμβάνονται υπόψη στην αποτελεσματική παραμετροποίησή του.

Τα δεδομένα της παραμετροποίησης του (των) firewall του οργανισμού διατηρούνται σε αρχείο που εντάσσεται στην πολιτική αντιγράφων ασφαλείας όπως προβλέπεται από το σημείο ελέγχου 6.1.

Αλλαγές στην παραμετροποίηση του (των) firewall επιτρέπονται μόνο για συγκεκριμένους, καταγεγραμμένους λόγους. Οι αλλαγές διενεργούνται μόνο από σχετικά εξουσιοδοτημένο προσωπικό.

ΣΗΜΕΙΟ ΕΛΕΓΧΟΥ 5.2

Σε περίπτωση που ο οργανισμός παρέχει την δυνατότητα ασύρματης πρόσβασης στο δίκτυο του οργανισμού, αυτό θα πρέπει να γίνεται με κατάλληλη δρομολόγηση και προστασία μέσω του(των) εγκατεστημένων firewall.

ΠΕΡΙΓΡΑΦΗ

Χρήστες που δεν ανήκουν στον οργανισμό, δεν θα πρέπει να έχουν τη δυνατότητα να συνδεθούν στο ασύρματο δίκτυο που χρησιμοποιείται ως επέκταση (σε σύνδεση με) του εσωτερικού δικτύου.

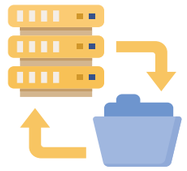
Σε περίπτωση που ο οργανισμός το επιθυμεί, για τους επισκέπτες του οργανισμού μπορεί να παρέχεται ασύρματη πρόσβαση στο δημόσιο εξωτερικό δίκτυο (internet) με τρόπο που θα είναι πλήρως απομονωμένο από το υπόλοιπο εσωτερικό δίκτυο. Αυτό μπορεί να επιτευχθεί είτε μέσω δεύτερης εντελώς χωριστής σύνδεσης στο δημόσιο εξωτερικό δίκτυο (internet) είτε μέσω του firewall με κατάλληλη παραμετροποίηση ώστε η συγκεκριμένη πρόσβαση να είναι εντελώς διαχωρισμένη από αυτήν προς το εσωτερικό δίκτυο (θα δίνεται δυνατότητα μόνο πρόσβασης στο δημόσιο εξωτερικό δίκτυο (internet)).

Το ασύρματο δίκτυο (είτε εσωτερικό είτε για τους επισκέπτες) πρέπει να είναι προστατευμένο με κρυπτογράφηση WPA2 και πάνω (π.χ. WPA3).

Η πρόσβαση στο διαχειριστικό περιβάλλον του εμπλεκόμενου (στο ασύρματο δίκτυο) εξοπλισμού θα είναι αυστηρά περιορισμένη σε ειδικά εξουσιοδοτημένο και κατάλληλο προσωπικό.

Οι απαιτήσεις του σημείου ελέγχου 3.1 εφαρμόζονται όπως προβλέπεται και στην περίπτωση του εξοπλισμού του ασύρματου δικτύου. Τα αποτελέσματα της εφαρμογής του σημείου ελέγχου 3.2 λαμβάνονται υπόψη στην αποτελεσματική παραμετροποίησή του.

6. ΑΝΤΙΓΡΑΦΑ ΑΣΦΑΛΕΙΑΣ



ΣΚΟΠΟΣ

Τα αντίγραφα ασφαλείας της κρίσιμης πληροφορίας του οργανισμού εξασφαλίζουν την διαθεσιμότητα, ακεραιότητα και εμπιστευτικότητα της έναντι των σχετικών απειλών.

ΣΗΜΕΙΟ ΕΛΕΓΧΟΥ 6.1

Ο οργανισμός αναγνωρίζει την κρίσιμη πληροφορία του και λαμβάνει αντίγραφα ασφαλείας της σε τακτά χρονικά διαστήματα σύμφωνα με την σχετική πολιτική αντιγράφων ασφαλείας.

ΠΕΡΙΓΡΑΦΗ

Οι πληροφορίες ενός οργανισμού είναι ένα σημαντικό αγαθό – περιουσιακό στοιχείο. Συγκεκριμένες πληροφορίες μπορεί να είναι τόσο κρίσιμες για τον οργανισμό, ώστε η απώλειά τους ή, η μερική ή ολική αποκάλυψή τους σε μη εξουσιοδοτημένα μέρη ή η αλλοίωσή τους μπορεί να έχει σημαντικές δυσμενείς επιπτώσεις για τον οργανισμό.

Για την προστασία των πληροφοριών αυτών, απαιτείται οι οργανισμοί να αναγνωρίσουν τις κρίσιμες πληροφορίες τους (σύμφωνα με τον παραπάνω ορισμό) και στη συνέχεια να λαμβάνουν σε τακτική βάση αντίγραφα ασφαλείας είτε των πληροφοριών είτε των συστημάτων που τις φιλοξενούν σύμφωνα με την σχετική καταγεγραμμένη πολιτική αντιγράφων ασφαλείας.

Δεδομένου ότι κάθε οργανισμός έχει διαφορετικές απαιτήσεις λειτουργίας, διαφορετικούς νόμους και κανονισμούς στους οποίους υπόκειται και διαφορετικούς στόχους και στρατηγικές, ο χρόνος λήψης των αντιγράφων ασφαλείας, η συχνότητα, το χρονικό διάστημα διατήρησης, το μέσο και το σημείο αποθήκευσης καθορίζονται σύμφωνα και με τα αποτελέσματα της σχετικής ανάλυσης επιχειρησιακών επιπτώσεων (Business Impact Analysis) – σημείο ελέγχου 11.1.

Κατ΄ ελάχιστο, ο οργανισμός θα πρέπει να υλοποιεί στρατηγική 3-2-1 σχετικά με τα αντίγραφα ασφαλείας των κρίσιμων πληροφοριών:

- Θα διατηρούνται τουλάχιστον τρία (3) αντίγραφα των κρίσιμων πληροφοριών. Ως πρώτο αντίγραφο υπολογίζεται το παραγωγικό (το σύστημα το οποίο ο οργανισμός χρησιμοποιεί για την καθημερινή του λειτουργία).
- Το δεύτερο αντίγραφο ασφαλείας μπορεί να βρίσκεται στον χώρο του οργανισμού, με την προϋπόθεση ότι δεν είναι συνδεδεμένο στο παραγωγικό σύστημα. Η λήψη του αντιγράφου ασφαλείας θα πρέπει να γίνεται τουλάχιστον μια φορά την ημέρα σε κατάλληλη ώρα ώστε να μπορεί να ολοκληρωθεί χωρίς να δημιουργεί σημαντικά προβλήματα στην λειτουργία του οργανισμού και στην ολοκλήρωση της διαδικασίας.
- Το τρίτο αντίγραφο θα πρέπει να βρίσκεται σε διαφορετικό χώρο από τα προηγούμενα δύο (2) και σε ικανή απόσταση ώστε να μην μπορεί εύκολα να επηρεαστεί από ένα περιστατικό που λαμβάνει χώρα στους χώρους του οργανισμού. Η λήψη του αντιγράφου ασφαλείας θα πρέπει να γίνεται τουλάχιστον μια φορά την εβδομάδα σε κατάλληλη ώρα ώστε να μπορεί να ολοκληρωθεί χωρίς να δημιουργεί σημαντικά προβλήματα στην λειτουργία του οργανισμού και στην ολοκλήρωση της διαδικασίας. Το μέσο ή η διαδικασία αποθήκευσης θα πρέπει να

είναι προστατευμένο από μη εξουσιοδοτημένη πρόσβαση μέσω της εφαρμογής κατάλληλης κρυπτογράφησης. Το συγκεκριμένο αντίγραφο μπορεί να βρίσκεται και σε υπηρεσία υπολογιστικού νέφους (cloud computing) η οποία παρέχει το επιθυμητό επίπεδο προστασίας.

Κατάλληλο προσωπικό θα είναι επιφορτισμένο με την παρακολούθηση της ορθής ολοκλήρωσης της λήψης των αντιγράφων ασφαλείας και θα διενεργεί σχετικές δοκιμές ανάκτησης (για την επιβεβαίωση της αποτελεσματικής λειτουργίας) τουλάχιστον μια φορά την εβδομάδα.

Σε περίπτωση που οργανισμός χρησιμοποιεί υπηρεσίες υπολογιστικού νέφους και δεν διαθέτει εκτεταμένη εσωτερική δομή, τότε η παραπάνω 3-2-1 πολιτική διατηρείται με τις ακόλουθες τροποποιήσεις:

- Θα διατηρούνται τουλάχιστον 3 αντίγραφα των κρίσιμων πληροφοριών. Ως πρώτο αντίγραφο υπολογίζεται το παραγωγικό το οποίο στην προκειμένη περίπτωση βρίσκεται στο cloud.
- Το δεύτερο αντίγραφο ασφαλείας μπορεί να βρίσκεται σε κατάλληλο εξοπλισμό αποθήκευσης στον χώρο του οργανισμού. Η λήψη του αντιγράφου ασφαλείας θα πρέπει να γίνεται τουλάχιστον μια φορά την ημέρα σε κατάλληλη ώρα ώστε να μπορεί να ολοκληρωθεί χωρίς να δημιουργεί σημαντικά προβλήματα στην λειτουργία του οργανισμού και στην ολοκλήρωση της διαδικασίας.
- Το τρίτο αντίγραφο θα πρέπει να βρίσκεται σε διαφορετικό χώρο από τα προηγούμενα 2 ή σε διαφορετικό cloud provider από το παραγωγικό. Η λήψη του αντιγράφου ασφαλείας θα πρέπει να γίνεται τουλάχιστον μια φορά την εβδομάδα σε κατάλληλη ώρα ώστε να μπορεί να ολοκληρωθεί χωρίς να δημιουργεί σημαντικά προβλήματα στην λειτουργία του οργανισμού και στην ολοκλήρωση της διαδικασίας. Το μέσο ή η διαδικασία αποθήκευσης ή τα δεδομένα θα πρέπει να είναι προστατευμένο από μη εξουσιοδοτημένη πρόσβαση μέσω της εφαρμογής κατάλληλης κρυπτογράφησης.

7. ΕΛΕΓΧΟΣ ΠΡΟΣΒΑΣΗΣ

ΣΚΟΠΟΣ

Η πληροφορία του οργανισμού είναι οργανωμένη και διαθέσιμη μόνο σε σχετικά εξουσιοδοτημένα μέρη, με αποτέλεσμα την καλύτερη διαχείρισή της και την μείωση της πιθανότητας μη εξουσιοδοτημένης πρόσβασης.

ΣΗΜΕΙΟ ΕΛΕΓΧΟΥ 7.1

Ο οργανισμός αναγνωρίζει τα σημεία στα οποία βρίσκεται σημαντική πληροφορία για αυτόν. Για την πληροφορία και με βάση το είδος, τη χρήση και την κρισιμότητά της, ο οργανισμός έχει δημιουργήσει μια δομή σε κατάλληλο αποθηκευτικό χώρο, η οποία του επιτρέπει να παρέχει δικαιώματα πρόσβασης σε εξουσιοδοτημένους και αυθεντικοποιημένους χρήστες ακολουθώντας την αρχή του Need-to-know (ανάγκη γνώσης).

ΠΕΡΙΓΡΑΦΗ

Η αρχή Need-to-know (ανάγκη γνώσης) προνοεί ότι ο χρήστης θα έχει πρόσβαση μόνο στην πληροφορία που χρειάζεται προκειμένου να μπορεί να εκτελέσει το ρόλο του αποτελεσματικά.

Ο οργανισμός θα πρέπει να αναγνωρίσει για κάθε πληροφορία, ποιος ρόλος έχει ανάγκη πρόσβασης σε αυτή και σε ποιο επίπεδο. Ο οργανισμός θα τηρεί λίστα με τα δικαιώματα πρόσβασης (ρόλος και επίπεδο πρόσβασης) ανά κατηγορία ή ομάδα πληροφορίας, τρόπος με τον οποίο δίνεται η πρόσβαση (π.χ. συγκεκριμένο μέσο αποθήκευσης, εφαρμογές, συστήματα κ.α.).

Τα επίπεδα πρόσβασης που θα έχουν αναγνωριστεί θα είναι κατ΄ελάχιστο:

- Πλήρη πρόσβαση: Δεν υπάρχει κανένας περιορισμός στις ενέργειες που μπορεί να διενεργήσει ο χρήστης επί των πληροφοριών ή την εφαρμογή.
- Δικαίωμα αλλαγής: Ο χρήστης μπορεί να διενεργήσει ενέργειες αλλαγές επί των πληροφοριών, περιλαμβανομένης σε κάποιες περιπτώσεις και της διαγραφής.
- Δικαίωμα μόνο ανάγνωσης: Ο χρήστης μπορεί να αποκτήσει πρόσβαση στην πληροφορία και να την δει αλλά δεν μπορεί να διενεργήσει επιπλέον ενέργειες.

Οι αλλαγές στα δικαιώματα πρόσβασης θα είναι ελεγχόμενες και κατάλληλα εξουσιοδοτημένες. Σε περίπτωση αλλαγής, θα ενημερώνεται η λίστα με τα δικαιώματα πρόσβασης που αναφέρεται παραπάνω.

Πρόσβαση σε μη αυθεντικοποιημένους χρήστες δεν θα πρέπει να επιτρέπεται. Η αυθεντικοποίηση θα πρέπει να γίνεται μέσω κατάλληλων μηχανισμών που δίνουν το επιθυμητό επίπεδο ασφαλείας, κατ΄ελάχιστο μέσω της χρήσης συνδυασμού ονόματος χρήστη και κωδικού πρόσβασης σύμφωνα με το σημείο ελέγχου 7.2.

Οι λογαριασμοί πρόσβασης των χρηστών είναι μοναδικά ανατεθειμένοι σε μοναδικά άτομα και δεν επιτρέπεται ο διαμοιρασμός λογαριασμών. Για ειδικές περιπτώσεις συστημάτων που δεν επιτρέπουν την ύπαρξη πολλαπλών λογαριασμών, θα πρέπει να εισάγονται επιπλέον μέτρα ώστε να μπορεί να γίνει ιχνηλάτηση και αντιστοίχιση σε φυσικό πρόσωπο.

Σε περίπτωση αποχώρησης ή αλλαγής εργασίας, οι αλλαγές στα δικαιώματα πρόσβασης πρέπει να γίνονται άμεσα.

ΣΗΜΕΙΟ ΕΛΕΓΧΟΥ 7.2

Ο οργανισμός έχει δημιουργήσει, εφαρμόσει σε όλα τα συστήματά του και τηρεί κατάλληλη πολιτική κωδικών πρόσβασης.

ΠΕΡΙΓΡΑΦΗ

Ο οργανισμός θα πρέπει να δημιουργήσει μια πολιτική κωδικών πρόσβασης η οποία θα περιέχει τους ελάχιστους κανόνες σχετικά με τους κωδικούς πρόσβασης ή τα άλλα μέσα αυθεντικοποίησης.

Κατ' ελάχιστο η πολιτική αυτή θα περιλαμβάνει:

- Το πλήθος των χαρακτήρων των κωδικών πρόσβασης. Το πλήθος χαρακτήρων δεν μπορεί να είναι μικρότερο του 8.
- Το είδος των χαρακτήρων των κωδικών πρόσβασης. Κατ' ελάχιστο οι κωδικοί πρόσβασης θα πρέπει να αποτελούνται τουλάχιστον από 3 κατηγορίες (ενδεικτικές κατηγορίες: κεφαλαία γράμματα, πεζά γράμματα, αριθμοί, ειδικοί χαρακτήρες).
- Η υποχρέωση για κρυπτογράφηση των κωδικών πρόσβασης.
- Η υποχρέωση της αλλαγής των κωδικών πρόσβασης τουλάχιστον ανά 42 ημέρες. Σε περίπτωση που αυτό δεν επιτρέπεται από το αντίστοιχο σύστημα, θα πρέπει να μεταβάλλονται (αυξάνονται) ανάλογα τα λοιπά χαρακτηριστικά όπως αναφέρονται παραπάνω για να εξασφαλίζουν αποδεκτό επίπεδο ασφάλειας.
- Η υποχρέωση της τήρησης ιστορικού των κωδικών πρόσβασης ώστε να μην μπορεί να χρησιμοποιηθούν τουλάχιστον οι 6 προηγούμενοι κωδικοί πρόσβασης.
  Ειδικά για την περίπτωση της από απόσταση πρόσβασης και της πρόσβασης με πλήρη / διαχειριστικά δικαιώματα συνιστάται η χρήση πολυπαραγοντικής αυθεντικοποίησης (multi factor authentication).

ΣΗΜΕΙΟ ΕΛΕΓΧΟΥ 7.3

Διαχειριστικά δικαιώματα ή προνομιακά δικαιώματα (admin/privileged rights) δίνονται στο ελάχιστο απαραίτητο εξουσιοδοτημένο προσωπικό.

ΠΕΡΙΓΡΑΦΗ

Τα άτομα και οι ρόλοι που έχουν διαχειριστικά ή προνομιακά δικαιώματα καταγράφονται στην λίστα με τα δικαιώματα πρόσβασης που αναφέρεται στο σημείο ελέγχου 7.1. Η ανάθεση τέτοιων δικαιωμάτων είναι αυστηρά ελεγχόμενη και δίνεται μόνο σε περίπτωση που απαιτείται για την διενέργεια των σχετικών καθηκόντων.

Λογαριασμοί με διαχειριστικά ή προνομιακά δικαιώματα δεν χρησιμοποιούνται σε καθημερινές εργασίες που δεν απαιτούν δικαιώματα τέτοιου επιπέδου.

Εγκαταστάσεις νέων λογισμικών και δυνατοτήτων διενεργούνται μόνο από λογαριασμούς με διαχειριστικά ή προνομιακά δικαιώματα, μετά από σχετικό έλεγχο από το κατάλληλο προσωπικό.

Οι ενέργειες των λογαριασμών (περιλαμβανομένων αυτών με διαχειριστικά ή προνομιακά δικαιώματα) καταγράφονται σε σχετικά αρχεία καταγραφής (logs) και διατηρούνται για τουλάχιστον 6 μήνες.

8. ΠΕΡΙΣΤΑΤΙΚΑ ΑΣΦΑΛΕΙΑΣ

ΣΚΟΠΟΣ

Ο οργανισμός είναι περισσότερο προετοιμασμένος έναντι ενός περιστατικού ασφαλείας. Η ύπαρξη των κατάλληλων προβλέψεων επιτρέπουν τη γρήγορη, αποτελεσματική και συντεταγμένη ανταπόκριση στα περιστατικά ασφαλείας.

ΣΗΜΕΙΟ ΕΛΕΓΧΟΥ 8.1

Ο οργανισμός έχει δημιουργήσει μια δομή και διαδικασία ανταπόκρισης σε περιστατικά ασφαλείας. Το προσωπικό που θα συμμετέχει στις αντίστοιχες διαδικασίες είναι κατάλληλα εκπαιδευμένο.

ΠΕΡΙΓΡΑΦΗ

Τα μέτρα που εφαρμόζει ένας οργανισμός δεν μπορούν να του εγγυηθούν ολική προστασία των δεδομένων και των συστημάτων. Ακόμα και στις περιπτώσεις που ο οργανισμός υλοποιεί αυστηρά μέτρα ασφαλείας, θα υπάρχει κάποιος εναπομείναντας κίνδυνος, κάποια αδυναμία ή κάποιος τρόπος επίθεσης που δεν θα έχει αντιμετωπιστεί. Ένα περιστατικό ασφαλείας είναι ένα ή μια σειρά από ανεπιθύμητα ή μη αναμενόμενα συμβάντα ασφαλείας, τα οποία έχουν μια σημαντική πιθανότητα να επηρεάσουν τις επιχειρησιακές διεργασίες και απειλούν την ασφάλεια των πληροφοριών του οργανισμού.

Όπως συνάγεται από τα παραπάνω, η προετοιμασία για την αντιμετώπιση περιστατικών είναι πολύ σημαντική για τον οργανισμό, και αυτό επιτυγχάνεται με προκαθορισμένες διαδικασίες (οι οποίες έχουν δοκιμαστεί για την αποτελεσματικότητά τους) και με την εκπαίδευση του προσωπικού για την αντιμετώπιση συμβάντων.

Ο οργανισμός θα πρέπει να δημιουργήσει μια διαδικασία για την αντιμετώπιση περιστατικών ασφαλείας η οποία θα περιλαμβάνει κατ' ελάχιστο:

- Τον ορισμό ενός προσώπου από την ανώτατη διοίκηση υπεύθυνο για τη διαχείριση των περιστατικών. Το συγκεκριμένο άτομο θα πρέπει να έχει ή να αποκτήσει κατάλληλες γνώσεις ώστε να μπορεί να διενεργεί το ρόλο με αποτελεσματικότητα.
- Τον ορισμό της ομάδας για την ανταπόκριση σε περιστατικά ασφαλείας με επιμέρους ρόλους όπως απαιτείται. Μέλη της ομάδας μπορεί να είναι και εξωτερικά προς τον οργανισμό μέρη, με την προϋπόθεση σύναψης κατάλληλης καταγεγραμμένης συμφωνίας.
- Τον ορισμό των συστημάτων που παρακολουθούνται και τους τρόπους με τους οποίους μπορεί να ληφθεί ενημέρωση / ειδοποίηση για πιθανό συμβάν ή περιστατικό ασφαλείας.
- Την περιγραφή των βημάτων που πρέπει να γίνουν καλύπτοντας το σύνολο του κύκλου ζωής ενός περιστατικού (προετοιμασία, αναγνώριση και καταγραφή, αξιολόγηση και απόφαση, ανταπόκριση, ολοκλήρωση και εξαγωγή διδαγμάτων).
- Τον καθορισμό των τρόπων και των μέσων με τα οποία θα πραγματοποιείται η ενημέρωση των εμπλεκόμενων μερών καθ' όλη της διάρκεια του κύκλου ζωής.
- Τα σημεία ελέγχου ενεργοποίησης του μηχανισμού ανταπόκρισης περιστατικών.
- Τον τρόπο καταγραφής, τα ενδιαφερόμενα μέρη που χρειάζεται να ενημερωθούν ή να κληθούν για συνδρομή, ένα σχετικό χρονοδιάγραμμα με εκκίνηση την στιγμή αναγνώρισης ότι

υπάρχει περιστατικό ασφαλείας και την ελάχιστη πληροφορία που θα πρέπει να περιέχεται ανά περίπτωση στην κάθε ενημέρωση.

Τα περιστατικά που σχετίζονται με δεδομένα προσωπικού χαρακτήρα θα προβλέπονται και περιλαμβάνονται ευκρινώς μέσα στην διαδικασία ανταπόκρισης σε περιστατικά ασφαλείας. Σημειώνεται ότι: αν συμβεί παραβίαση δεδομένων που θέτει σε κίνδυνο τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων, ο οργανισμός οφείλει να ειδοποιήσει το Γραφείο Επιτρόπου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα (https://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/home_en/home_en?opendocument) εντός 72 ωρών αφότου γίνει αντιληπτή η παραβίαση.

9. ΜΕΤΡΑ ΦΥΣΙΚΗΣ ΑΣΦΑΛΕΙΑΣ

ΣΚΟΠΟΣ

Ο οργανισμός είναι περισσότερο προστατευμένος από απειλές που προέρχονται από το φυσικό περιβάλλον, είτε πρόκειται για μη εξουσιοδοτημένη φυσική πρόσβαση είτε πρόκειται για επιπτώσεις ως αποτέλεσμα περιβαλλοντικού γεγονότος ή καταστροφής.

ΣΗΜΕΙΟ ΕΛΕΓΧΟΥ 9.1

Ο οργανισμός έχει υιοθετήσει μέτρα φυσικής ασφάλειας για την προστασία των συστημάτων και των εγκαταστάσεων από φυσικές και περιβαλλοντικές απειλές.

ΠΕΡΙΓΡΑΦΗ

Τα σημεία που βρίσκεται εγκατεστημένος εξοπλισμός συστημάτων πληροφορικής και επικοινωνιών, καθώς και τα σημεία στα οποία φιλοξενείται η πληροφορία του οργανισμού (σε οποιοδήποτε μέσο) θα πρέπει να προστατεύεται από φυσική μη εξουσιοδοτημένη πρόσβαση και περιβαλλοντικές συνθήκες και καταστροφές.

Τα ελάχιστα μέτρα ασφαλείας που θα πρέπει να υλοποιούνται από τον οργανισμό είναι:

- Κλειδαριές σε παράθυρα και πόρτες.
- Συναγερμοί που τοποθετούνται σε κατάλληλα σημεία και ενεργοποιούνται εκτός ωραρίου εργασίας (ο συναγερμός θα έχει ατομικούς κωδικούς ενεργοποίησης / απενεργοποίησης γνωστούς μόνο στον εξουσιοδοτημένο χρήστη – η απόδοση των κωδικών πρόσβασης ή των καρτών πρόσβασης ακολουθεί το σημείο ελέγχου 7.1. Η αρχή του need to have θα εφαρμόζεται και σε αυτή την περίπτωση).
- Ελεγχόμενη πρόσβαση σε σημείο που αποθηκεύουν ή επεξεργάζονται κρίσιμες πληροφορίες ή στεγάζουν κρίσιμο εξοπλισμό (π.χ. access control με ατομικούς κωδικούς γνωστούς μόνο στον εξουσιοδοτημένο χρήστη – η απόδοση των κωδικών πρόσβασης ή των καρτών πρόσβασης ακολουθεί το σημείο ελέγχου 7.1).
- Προστασία από φωτιά, σύμφωνα με την σχετική μελέτη (λαμβάνοντας υπόψη τις συγκεκριμένες συνθήκες και τρόπο χρήσης των χώρων, τη τρέχουσα χρονική στιγμή).
- Πρόβλεψη για συνεχή συνοδεία επισκεπτών από το αρμόδιο άτομο του προσωπικού.
- Τα καλώδια ισχύος πρέπει να διαχωρίζονται από τα καλώδια δικτύου για την αποφυγή παρεμβολών. Τα καλώδια δικτύου πρέπει να προστατεύονται από αγωγούς και, όπου είναι δυνατόν, να αποφεύγονται οι διαδρομές μέσω δημόσιων χώρων.
- Μέτρηση θερμοκρασίας και υγρασίας και όπου είναι εφικτό αυτόματη ενημέρωση σε περίπτωση που βρίσκονται εκτός ορίων.
- Προστασία από ζημιές, βανδαλισμούς και κλοπή ανάλογα με την τοποθεσία και τις δυνατότητες πρόσβασης του χώρου.
- Προστασία από διακοπές ή άλλες διαταραχές της παροχής ενέργειας με τέτοιο τρόπο ώστε να εξασφαλίζεται κατ' ελάχιστο ο ασφαλής τερματισμός των κρίσιμων συστημάτων πληροφορικής και επικοινωνιών (graceful shutdown). Οι ανάγκες για παροχή ενέργειας και σε αυτές τις περιπτώσεις θα είναι συμβατές με τα στοιχεία που έχουν αναγνωριστεί σύμφωνα με το σημείο ελέγχου 11.1.

Οι παραπάνω απαιτήσεις θα πρέπει να ισχύουν και να εξασφαλίζονται ακόμα κα αν ο εξοπλισμός του οργανισμού (σύνολο ή μέρος) βρίσκεται σε datacenter τρίτου ή στο cloud.

Τα εργαλεία ταυτοποίησης και πρόσβασης (π.χ. ψηφιακές κάρτες εισόδου, κλειδιά, κωδικοί εισόδου κ.λπ.) πρέπει να βρίσκονται στην κατοχή μόνο των προσώπων που έχουν δικαίωμα πρόσβασης προς εν λόγω χώρους και δεν πρέπει να δανείζονται σε κανέναν άλλον.

Έγγραφα τα οποία βρίσκονται σε γραφεία θα πρέπει να προστατεύονται κατάλληλα με μέτρα προς:

- Κατάλληλα ντουλάπια αρχειοθέτησης που είναι κλειδωμένα με τα κλειδιά αποθηκευμένα μακριά από το ντουλάπι ή
- κλειδωμένα χρηματοκιβώτια.

10. ΠΡΟΣΤΑΣΙΑ ΔΕΔΟΜΕΝΩΝ

ΣΚΟΠΟΣ

Ο οργανισμός υλοποιεί πολιτική και αυτοαξιολόγηση για την προστασία δεδομένων προσωπικού χαρακτήρα με στόχο την καλύτερη συμμόρφωση προς τις σχετικές νομικές και κανονιστικές απαιτήσεις και την μεγαλύτερη προστασία των υποκειμένων των δεδομένων και του οργανισμού.

ΣΗΜΕΙΟ ΕΛΕΓΧΟΥ 10.1

Ο οργανισμός σχεδιάζει, υλοποιεί, εγκρίνει και δημοσιοποιεί Πολιτική Προστασίας Δεδομένων Προσωπικού Χαρακτήρα.

ΠΕΡΙΓΡΑΦΗ

Ο οργανισμός διενεργεί αυτό-αξιολόγηση σχετικά με τα δεδομένα προσωπικού χαρακτήρα και τη συμμόρφωσή του προς τις σχετικές διατάξεις της νομοθεσίας. Η αυτο-αξιολόγηση μπορεί να γίνεται με τη χρήση κατάλληλης μεθοδολογίας που έχει αναπτυχθεί από τον οργανισμό ή από κατάλληλη αξιόπιστη εξωτερική πηγή.
Ενδεικτικά αναφέρονται οι ακόλουθες πηγές:

https://www.dataprotection.gov.cy/dataprotection

https://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/page3a_gr/page3a_gr?opendocument

European Union Agency for Cybersecurity (ENISA):
https://www.enisa.europa.eu/risk-level-tool/risk

Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων – Οδηγός για την προστασία δεδομένων προσωπικού χαρακτήρα για μικρές επιχειρήσεις:
https://edpb.europa.eu/sme-data-protection-guide/home_en

Η διαδικασία της αυτό-αξιολόγησης θα επαναλαμβάνεται ετησίως. Ο οργανισμός θα διατηρεί τα αποτελέσματα της αυτό-αξιολόγησης και θα υλοποιήσει όποια μέτρα προκύπτει ότι είναι απαραίτητα για την εξασφάλιση της συμμόρφωσης προς τις σχετικές απαιτήσεις.
Ο οργανισμός θα δημιουργήσει μια πολιτική προστασίας δεδομένων προσωπικού χαρακτήρα η οποία θα είναι σύμφωνη με τις απαιτήσεις της σχετικής νομοθεσίας, κανονισμών και οδηγιών του Γραφείου Επιτρόπου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, με βάση τα αποτελέσματα της αυτό-αξιολόγησης (όπως αυτή περιγράφεται παραπάνω) και θα περιέχει τα ακόλουθα στοιχεία:

- Μια σύντομη περιγραφή των δραστηριοτήτων του οργανισμού
- Τα πλήρη στοιχεία επικοινωνίας του οργανισμού
- Τα στοιχεία επικοινωνίας του υπεύθυνου προστασίας δεδομένων
- Τα δεδομένα (κατηγορίες) προσωπικού χαρακτήρα που επεξεργάζεται
- Την πηγή από την οποία προέρχονται τα δεδομένα προσωπικού
- χαρακτήρα (στις περιπτώσεις όπου δεν συλλέγονται απ' ευθείας από τα υποκείμενα των δεδομένων)
- Τους σκοπούς και τις νομικές βάσεις της επεξεργασίας
- Τα έννομα συμφέροντα που επιδιώκονται από τον υπεύθυνο επεξεργασίας ή από τρίτο (στις περιπτώσεις όπου η επεξεργασία βασίζεται σε έννομο συμφέρον)
- Τους αποδέκτες (ή κατηγορίες αποδεκτών) των δεδομένων προσωπικού χαρακτήρα

- Το χρονικό διάστημα διατήρησης των δεδομένων προσωπικού χαρακτήρα ή εάν δεν είναι δυνατό, τα σημεία ελέγχου που χρησιμοποιούνται για τον καθορισμό αυτής της περιόδου
- Αναφορά κατά πόσο γίνεται διαβίβαση δεδομένων προσωπικού χαρακτήρα σε τρίτη χώρα ή διεθνή οργανισμό
- Πληροφορίες σχετικά με τα δικαιώματα των υποκειμένων (π.χ. δικαίωμα πρόσβασης, διόρθωσης, διαγραφής κ.α.)
- Την ύπαρξη του δικαιώματος ανάκλησης της συγκατάθεσής (στις περιπτώσεις όπου η επεξεργασία βασίζεται στη συγκατάθεση του υποκειμένου των δεδομένων)
- Πληροφορίες σχετικά με τον τρόπο με τον οποίο τα υποκείμενα των δεδομένων μπορούν να υποβάλουν παράπονα είτε στον οργανισμό είτε απευθείας στην εποπτική αρχή.
- Κατά πόσο το υποκείμενο των δεδομένων υποχρεούται να παρέχει τα δεδομένα προσωπικού χαρακτήρα και ποιες ενδεχόμενες συνέπειες θα είχε η μη παροχή των δεδομένων αυτών
- Την ύπαρξη αυτοματοποιημένης λήψης αποφάσεων, συμπεριλαμβανομένης της κατάρτισης προφίλ και, τουλάχιστον στις περιπτώσεις αυτές, σημαντικές πληροφορίες σχετικά με τη λογική που ακολουθείται, καθώς και τη σημασία και τις προβλεπόμενες συνέπειες της εν λόγω επεξεργασίας για το υποκείμενο των δεδομένων.

Μπορείτε να λάβετε περισσότερες πληροφορίες σχετικά με την πολιτική προστασίας δεδομένων/πολιτική απορρήτου/ενημέρωση υποκειμένων των δεδομένων στην ιστοσελίδα του Γραφείου της Επιτρόπου Προστασίας Δεδομένων Προσωπικού Χαρακτήρα στο μέρος «Πληροφορίες για πολίτες» - «Τα δικαιώματα σου» - «Διαφάνεια – Δικαίωμα ενημέρωσης»: https://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/All/39B375E9A0126F47C22582F9002BFE2B

Η πολιτική προστασίας δεδομένων προσωπικού χαρακτήρα θα είναι διαθέσιμη κατ' ελάχιστο μέσω της ιστοσελίδας του οργανισμού και θα ανασκοπείται για την καταλληλότητά της τουλάχιστον μια φορά το έτος.

11. ΑΝΑΛΥΣΗ ΕΠΙΧΕΙΡΗΣΙΑΚΩΝ ΕΠΙΠΤΩΣΕΩΝ

ΣΚΟΠΟΣ

Ο οργανισμός διενεργεί ανάλυση επιχειρησιακών επιπτώσεων, με στόχο να αναγνωρίσει οργανωμένα τις προτεραιότητες, τα επίπεδα και τις εξαρτήσεις των υπηρεσιών και διεργασιών του. Μέσα από την συγκεκριμένη ανάλυση, ο οργανισμός έχει την δυνατότητα να προσαρμόσει τα διάφορα μέτρα στις επιχειρησιακές του απαιτήσεις.

ΣΗΜΕΙΟ ΕΛΕΓΧΟΥ 11.1

Ο οργανισμός έχει σχεδιάσει και υλοποιήσει κατάλληλη μεθοδολογία για την ανάλυση επιχειρησιακών επιπτώσεων. Τα αποτελέσματα και τα βασικά μεγέθη που προκύπτουν από την εφαρμογή της μεθοδολογίας καταγράφονται, διατηρούνται και τροφοδοτούν τον σχεδιασμό σχετικών μέτρων και υλοποιήσεων.

ΠΕΡΙΓΡΑΦΗ

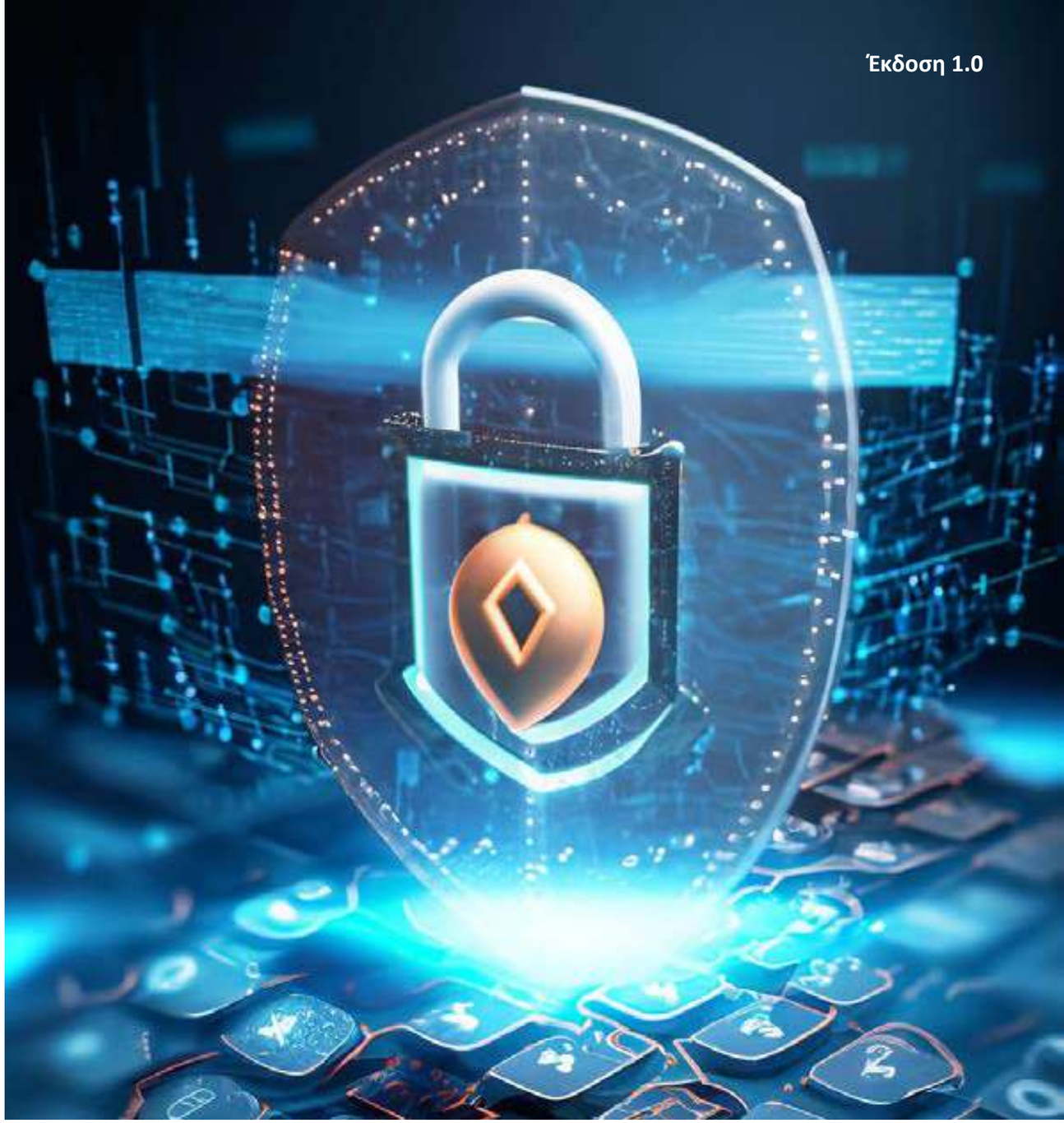
Η ανάλυση επιχειρησιακών επιπτώσεων βοηθά τον οργανισμό να εντοπίσει και να τεκμηριώσει τις κρίσιμες επιχειρησιακές διεργασίες και τα υποστηρικτικά τους στοιχεία. Αυτό βοηθά τον οργανισμό στην κατανόηση του περιβάλλοντος του και στο τι είναι πιο σημαντικό για αυτόν πριν λάβει μέτρα για την προστασία του. Η ανάλυση επιχειρησιακών επιπτώσεων αναδεικνύει τον τρόπο με τον οποίο αυτές οι βασικές διεργασίες και υπηρεσίες θα επηρεάζονταν σε περίπτωση που η κανονική επιχειρησιακή λειτουργία παρεμποδίζονταν, διακόπτονταν ή εξαλείφονταν.

Υλοποιώντας τη μεθοδολογία για την ανάλυση επιχειρησιακών επιπτώσεων ο οργανισμός επιτυγχάνει:

- να προσδιορίσει τις βασικές επιχειρησιακές διεργασίες και λειτουργίες
- να προτεραιοποιήσει τις βασικές επιχειρησιακές διεργασίες και λειτουργίες
- να καταρτήσει λεπτομερή κατάλογο με τις απαιτήσεις για την ανάκαμψη
- να προσδιορίσει τον αντίκτυπο που θα έχει μία διακοπή στις καθημερινές λειτουργίες για διαφορετικές περιόδους διάρκειας της διακοπής
- να προσδιορίσει το μέγιστο χρόνο που μπορεί να αντέξει να μην λειτουργεί μια διεργασία ή υπηρεσία (Maximum Acceptable Outage – MAO)
- να προσδιορίσει τον επιθυμητό χρόνο ανάκαμψης σε περίπτωση διαταραχής (Recovery time objective – RTO)
- να προσδιορίσει την ελάχιστη παλαιότητα δεδομένων για την εξασφάλιση της αποτελεσματικής ανάκαμψης (RPO – Recovery point objective)
- να καθορίσει τον οικονομικό, λειτουργικό και νομικό αντίκτυπο που θα έχει ο οργανισμός από μία διαταραχή που επηρεάζει τις υπηρεσίες.

Τα αποτελέσματα σχετικά με τα RTO (recovery time objective), RPO (Recovery Point objective) και MAO (Maximum acceptable Outage) θα χρησιμοποιούνται για τη λήψη αποφάσεων και σχεδιασμό σχετικών πολιτικών και μέτρων (π.χ. σημείο ελέγχου 5.1.). Επιπλέον, ο οργανισμός δημιουργεί και αποτυπώνει στα πλαίσια του BIA τους τρόπους με τους οποίους θα επιτύχει τα παραπάνω μεγέθη σε περίπτωση διαταραχής.

Οι σχετικές εκτιμήσεις επιχειρησιακών επιπτώσεων θα επανεξετάζονται ετησίως και σε περίπτωση σημαντικών αλλαγών στον οργανισμό, όπως μετακινήσεις γραφείων, συγχωνεύσεις και εξαγορές ή εισαγωγή νέων υπηρεσιών ή αλλαγή υπηρεσιών.



Έκδοση 1.0

Δήλωση Αποποίησης Ευθύνης

Το παρόν έγγραφο αποσκοπεί στην υποστήριξη των ΜμΕ για την επίτευξη ενός ελάχιστου επιπέδου κυβερνοασφάλειας. Οι πληροφορίες που παρέχονται είναι καθοδηγητικής φύσεως και δεν εξατομικεύονται σε συγκεκριμένη κατάσταση οποιουδήποτε φυσικού ή νομικού προσώπου. Το παρόν πλαίσιο κυβερνο-υγιεινής δεν αποτελεί νομική δέσμευση. Παρόλο που η εφαρμογή του προτεινόμενου πλαισίου κυβερνο-υγιεινής ενισχύει το επίπεδο κυβερνοασφάλειας, δεν μπορεί να διασφαλίσει πως η επιχείρηση μέσω της εφαρμογής θα αποτρέψει εξολοκλήρου οποιαδήποτε κυβερνοεπίθεση. Η οποιαδήποτε χρήση, αναπαραγωγή, κοινοποίηση, αντιγραφή, παραποίηση, αναπροσαρμογή και οποιασδήποτε άλλης μορφής χρήση του παρόντος απαγορεύεται χωρίς την πρότερη γραπτή συγκατάθεση της Αρχής Ψηφιακής Ασφάλειας προς το σκοπό αυτό.

Με τη συγχρηματοδότηση της Ευρωπαϊκής Ένωσης

Με τη συγχρηματοδότηση από το πρόγραμμα "Ψηφιακή Ευρώπη" της Ευρωπαϊκής Ένωσης στο πλαίσιο της συμφωνίας επιχορήγησης αριθ. 101101331.

Με τη συγχρηματοδότηση της Αρχής Ψηφιακής Ασφάλειας (ΑΨΑ)