ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ

ΕΘΝΙΚΗ ΑΡΧΗ ΚΥΒΕΡΝΟ ΑΣΦΑΛΕΙΑΣ



ΕΓΧΕΙΡΙΔΙΟ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΓΙΑ ΜΙΚΡΟΜΕΣΑΙΕΣ ΕΠΙΧΕΙΡΗΣΕΙΣ

ΝΟΕΜΒΡΙΟΣ 2026

ΕΚΠΟΝΗΣΗ

Το «Εγχειρίδιο Κυβερνοασφάλειας για Μικρομεσαίες Επιχειρήσεις» έχει εκπονηθεί από το Τμήμα Απαιτήσεων και Αρχιτεκτονικής Ασφάλειας | Διεύθυνση Στρατηγικού Σχεδιασμού Κυβερνοασφάλειας | Γενική Διεύθυνση Επιτελικού Σχεδιασμού της Εθνικής Αρχής Κυβερνοασφάλειας.

ΑΠΟΠΟΙΗΣΗ ΕΥΘΥΝΗΣ

Το «Εγχειρίδιο Κυβερνοασφάλειας για Μικρομεσαίες Επιχειρήσεις» έχει ενημερωτικό και καθοδηγητικό χαρακτήρα και δεν αποτελεί νομικά δεσμευτικό κείμενο. Περιλαμβάνει γενικές οδηγίες και προτεινόμενες πρακτικές για την ενίσχυση της ασφάλειας των πληροφοριακών συστημάτων και τη μείωση των κινδύνων κυβερνοασφάλειας.

Η τήρηση των προτεινόμενων οδηγιών δεν εγγυάται την απόλυτη προστασία έναντι του συνεχώς εξελισσόμενου πεδίου κυβερνοαπειλών ούτε συνιστά, από μόνη της, εκπλήρωση των νομοθετικών και κανονιστικών υποχρεώσεων που ενδέχεται να ισχύουν για κάθε επιχείρηση, η οποία παραμένει υπεύθυνη για την αξιολόγηση των ιδιαίτερων κινδύνων που αντιμετωπίζει, την εφαρμογή κατάλληλων μέτρων ασφάλειας και τη συμμόρφωσή της με το εκάστοτε εφαρμοστέο θεσμικό πλαίσιο.

ΑΔΕΙΑ ΧΡΗΣΗΣ

Εθνική Αρχή Κυβερνοασφάλειας, Νοέμβριος 2026

Εκτός εάν αναφέρεται διαφορετικά, η επαναχρησιμοποίηση αυτού του οδηγού επιτρέπεται βάσει της άδειας Creative Commons Attribution 4.0 International (CC BY 4.0) (https://creativecommons.org/licenses/by/4.0/). Αυτό σημαίνει ότι επιτρέπεται η επαναχρησιμοποίηση, εφόσον αναφέρεται η κατάλληλη πηγή και υποδεικνύονται τυχόν αλλαγές. Για οποιαδήποτε χρήση ή αναπαραγωγή στοιχείων που δεν ανήκουν στην Εθνική Αρχή Κυβερνοασφάλειας, ενδέχεται να χρειαστεί να ζητηθεί άδεια απευθείας από τους αντίστοιχους κατόχους δικαιωμάτων.

Περιεχόμενα

Χαιρετισμός Διοικητή Εθνικής Αρχής Κυβερνοασφάλειας 4

Εισαγωγή 5

Περιεχόμενο και δομή του Εγχειριδίου 6

1. Διακυβέρνηση κυβερνοασφάλειας 8

2. Καταγραφή και διαχείριση πληροφοριακών αγαθών 12

3. Ασφαλής παραμετροποίηση υλικού και λογισμικού 17

4. Διαχείριση ευπαθειών 20

5. Διαχείριση ταυτότητας και έλεγχος πρόσβασης 23

6. Ασφάλεια δικτύων 27

7. Προστασία από κακόβουλο λογισμικό 30

8. Εκπαίδευση και ευαισθητοποίηση σε θέματα κυβερνοασφάλειας 34

9. Ασφάλεια εφοδιαστικής αλυσίδας 36

10. Διαχείριση υπηρεσιών νεφοϋπολογιστικής 39

11. Κρυπτογραφία 42

12. Λήψη αντιγράφων ασφαλείας 44

13. Καταγραφή και παρακολούθηση συμβάντων 47

14. Διαχείριση περιστατικών κυβερνοασφάλειας 49

15. Έλεγχοι παρείσδυσης (penetration tests) 52

16. Φυσική ασφάλεια πληροφοριακών αγαθών 55

17. Ασφαλής χρήση Τεχνητής Νοημοσύνης 58

Χαιρετισμός Διοικητή Εθνικής Αρχής Κυβερνοασφάλειας

Ο ψηφιακός μετασχηματισμός των ελληνικών επιχειρήσεων αποτελεί κεντρικό μοχλό ανάπτυξης για τη χώρα, ταυτόχρονα όμως φέρνει νέες προκλήσεις στον τομέα της κυβερνοασφάλειας. Οι κυβερνοεπιθέσεις δεν αφορούν πλέον αποκλειστικά μεγάλους οργανισμούς ή φορείς κρίσιμων υποδομών. Οι μικρομεσαίες επιχειρήσεις (ΜμΕ), που συγκροτούν τη ραχοκοκαλιά της ελληνικής οικονομίας, αποτελούν εξίσου στόχο, και μάλιστα με αυξανόμενο ρυθμό. Η εμπειρία της Εθνικής Αρχής Κυβερνοασφάλειας δείχνει ότι η συντριπτική πλειονότητα των επιθέσεων σε ΜμΕ θα μπορούσε να είχε αποτραπεί ή ο αντίκτυπός τους να είχε περιοριστεί σημαντικά, αν είχαν υιοθετηθεί βασικά μέτρα κυβερνοϋγιεινής, συχνά χαμηλού κόστους και πολυπλοκότητας, τα οποία εφαρμοζόμενα με συνέπεια, μειώνουν δραστικά την έκθεση σε κυβερνοαπειλές.

Η ενσωμάτωση της Οδηγίας (ΕΕ) 2022/2555 (NIS2) στην ελληνική έννομη τάξη με τον ν. 5160/2024 και η κοινή υπουργική απόφαση 1689/2025 (ΦΕΚ Β' 2186) θέσπισαν για πρώτη φορά ολοκληρωμένο Εθνικό Πλαίσιο Απαιτήσεων Κυβερνοασφάλειας για τις βασικές και σημαντικές οντότητες. Οι κίνδυνοι όμως δεν περιορίζονται σε όσες οντότητες εμπίπτουν στο εν λόγω πεδίο εφαρμογής: το σύνολο των ελληνικών ΜμΕ εκτίθεται σε κυβερνοαπειλές που μπορούν να πλήξουν τη λειτουργία, τη φήμη και την βιωσιμότητά τους.

Για τον λόγο αυτό, η Εθνική Αρχή Κυβερνοασφάλειας εκπόνησε το παρόν Εγχειρίδιο Κυβερνοασφάλειας, στο πνεύμα του ν. 5160/2024, απευθυνόμενο στο σύνολο των ελληνικών ΜμΕ, ανεξαρτήτως κλάδου, μεγέθους ή τυχόν υπαγωγής σε ειδικό κανονιστικό πλαίσιο. Το παρόν συνιστά έναν λειτουργικό οδηγό που μεταφράζει τις απαιτήσεις και τις διεθνείς βέλτιστες πρακτικές σε συγκεκριμένα, εφαρμόσιμα βήματα.

Η υιοθέτηση μέτρων κυβερνοϋγιεινής είναι, πρωτίστως, ζήτημα κουλτούρας και διακυβέρνησης: η ενεργή εμπλοκή της διοίκησης, η ευαισθητοποίηση του προσωπικού και η ετοιμότητα αντίδρασης σε περιστατικά συνιστούν τους ακρογωνιαίους λίθους ενός ανθεκτικού επιχειρηματικού περιβάλλοντος. Η Εθνική Αρχή Κυβερνοασφάλειας στέκεται στο πλευρό κάθε ελληνικής επιχείρησης, παρέχοντας καθοδήγηση, τεχνικές οδηγίες αλλά και τις υπηρεσίες του Εθνικού CSIRT, όποτε αυτό απαιτηθεί.

Καλώ θερμά όλες τις ελληνικές μικρομεσαίες επιχειρήσεις, ανεξάρτητα από το αν εμπίπτουν στο πεδίο εφαρμογής της κείμενης νομοθεσίας για την κυβερνοασφάλεια, να μελετήσουν το παρόν Εγχειρίδιο, να αξιολογήσουν το επίπεδο ωριμότητάς τους και να σχεδιάσουν την υλοποίηση των απαιτήσεων με σταδιακό και αναλογικό προς τους κινδύνους τρόπο. Η συλλογική ενίσχυση της κυβερνοανθεκτικότητας της χώρας ξεκινά από την κάθε επιχείρηση χωριστά.

Μιχάλης Μπλέτσας

Διοικητής Εθνικής Αρχής Κυβερνοασφάλειας

Εισαγωγή

Η χρήση τεχνολογιών πληροφορικής και επικοινωνιών αποτελεί πλέον αναπόσπαστο μέρος της καθημερινότητας κάθε επιχείρησης, ανεξαρτήτως μεγέθους και τομέα δραστηριότητας. Διεργασίες όπως η ηλεκτρονική τιμολόγηση, η εξυπηρέτηση πελατών μέσω διαδικτύου, η χρήση υπηρεσιών νεφοϋπολογιστικής, η απομακρυσμένη εργασία, η αξιοποίηση εφαρμογών τεχνητής νοημοσύνης έχουν μεταμορφώσει ριζικά τον τρόπο που οι επιχειρήσεις παράγουν αξία, καθιστώντας ταυτόχρονα την κυβερνοασφάλεια κρίσιμο παράγοντα για τη βιωσιμότητα και την ανταγωνιστικότητά τους.

Παρά την παραδοσιακή αντίληψη ότι οι κυβερνοεγκληματίες στοχεύουν αποκλειστικά μεγάλους οργανισμούς, οι μικρομεσαίες επιχειρήσεις (ΜμΕ), που αποτελούν τη ραχοκοκαλιά της ελληνικής οικονομίας, δέχονται καθημερινά ποικίλες κυβερνοεπιθέσεις, όπως λυτρισμικού (ransomware), ηλεκτρονικού «ψαρέματος» (phishing) και επιθέσεις άρνησης παροχής υπηρεσιών (denial of service). Οι συνέπειες των κυβερνοεπιθέσεων μπορούν να αποδειχθούν καταστροφικές: διακοπή λειτουργίας, απώλεια δεδομένων πελατών, οικονομική ζημιά, πλήγμα στη φήμη έως και οριστικό κλείσιμο της επιχείρησης.

Σε ευρωπαϊκό επίπεδο, η Οδηγία (ΕΕ) 2022/2555 (NIS2) αποσκοπεί σε ένα ενιαίο, υψηλό επίπεδο κυβερνοασφάλειας σε ολόκληρη την Ένωση. Η Οδηγία ενσωματώθηκε στην ελληνική έννομη τάξη με τον ν. 5160/2024, ενώ με την υπ' αρ. 1689/2025 κοινή υπουργική απόφαση (ΦΕΚ Β' 2186/6.5.2025) θεσπίστηκε το Εθνικό Πλαίσιο Απαιτήσεων Κυβερνοασφάλειας Βασικών και Σημαντικών Οντοτήτων, το οποίο εξειδικεύει τα τεχνικά, οργανωτικά και επιχειρησιακά μέτρα διαχείρισης των κινδύνων κυβερνοασφάλειας. Στο πεδίο εφαρμογής της εν λόγω ΚΥΑ εμπίπτει και σημαντικός αριθμός μεσαίων επιχειρήσεων, ιδίως όσες δραστηριοποιούνται σε κρίσιμους τομείς (ενέργεια, υγεία, μεταφορές, ψηφιακές υποδομές, διαχείριση υπηρεσιών ΤΠΕ κ.ά.) και πληρούν τα κριτήρια μεγέθους του νόμου.

Πέραν αυτών**,** η Εθνική Αρχή Κυβερνοασφάλειας θεωρεί ότι ένα αναλογικό ελάχιστο επίπεδο κυβερνοϋγιεινής πρέπει να υιοθετείται σταδιακά από το σύνολο των ΜμΕ, ως αναγκαία προϋπόθεση τόσο για τη βιωσιμότητά τους όσο και για τη συνολική ανθεκτικότητα του εθνικού ψηφιακού οικοσυστήματος. Ο όρος «κυβερνοϋγιεινή» (cyber hygiene) αναφέρεται στο σύνολο των βασικών, καθημερινών πρακτικών και μέτρων που, εφαρμοζόμενα με συνέπεια, προστατεύουν τα πληροφοριακά αγαθά από κυβερνοεπιθέσεις, προσφέροντας ένα ισχυρό πρώτο επίπεδο προστασίας με μέτρα που μπορεί να εφαρμόσει κάθε επιχείρηση, ανεξάρτητα από τους τεχνικούς της πόρους.

Για το λόγο αυτό, η Εθνική Αρχή Κυβερνοασφάλειας εκδίδει το παρόν Εγχειρίδιο, το οποίο απευθύνεται στο σύνολο των ελληνικών ΜμΕ, ανεξαρτήτως κλάδου και μεγέθους και αποτελεί έναν πρακτικό οδηγό ενίσχυσης του επιπέδου κυβερνοασφάλειάς τους, ανεξαρτήτως της τυχόν υπαγωγής τους στο πεδίο εφαρμογής του ν. 5160/2024. Επισημαίνεται ότι το Εγχειρίδιο περιέχει νομικά μη δεσμευτικές οδηγίες προς τις επιχειρήσεις, οι οποίες όμως αφορούν σε απαιτήσεις που περιλαμβάνονται σε όλα τα διεθνή πρότυπα και πλαίσια κυβερνοασφάλειας και αναγνωρίζονται ως βέλτιστες πρακτικές για την αντιμετώπιση μεγάλου εύρους κυβερνοεπιθέσεων. Ως εκ τούτου, οι επιχειρήσεις ενθαρρύνονται στο να εφαρμόσουν τα μέτρα που περιγράφονται σε αυτό. Η συνεπής υιοθέτηση των πρακτικών που περιγράφονται στο παρόν Εγχειρίδιο συνιστά πρωτίστως επένδυση στη βιωσιμότητα, την αξιοπιστία και την εμπιστοσύνη που εμπνέει κάθε επιχείρηση στους πελάτες, τους συνεργάτες της και το κοινωνικό σύνολο.

Περιεχόμενο και δομή του Εγχειριδίου

Το Εγχειρίδιο διαρθρώνεται σε 17 κεφάλαια, τα οποία αποτελούν βασικές θεματικές περιοχές κυβερνοασφάλειας που συνδέονται άμεσα με την καθημερινή λειτουργία των επιχειρήσεων. Κάθε θεματική ενότητα περιλαμβάνει επιμέρους απαιτήσεις, οι οποίες διατυπώνονται με τρόπο που επιτρέπει στις επιχειρήσεις να κατανοήσουν τί πρέπει να υλοποιήσουν, γιατί είναι σημαντικό και με ποιον τρόπο μπορεί να αξιολογηθεί η εφαρμογή του. Για τον σκοπό αυτό, κάθε απαίτηση συνοδεύεται από τρία διακριτά μέρη: την περιγραφή, τις οδηγίες υλοποίησης και τις διαδικασίες αξιολόγησης.

Η **περιγραφή** εξηγεί το αντικείμενο και τη σημασία της απαίτησης, καθώς και τους κινδύνους που επιχειρεί να περιορίσει.

Οι **οδηγίες υλοποίησης** παρέχουν πρακτικές κατευθύνσεις για την εφαρμογή κατάλληλων τεχνικών, οργανωτικών και επιχειρησιακών μέτρων. Πρόκειται, ουσιαστικά, για τον πυρήνα του Εγχειριδίου, καθώς αφορούν σε εστιασμένες ενέργειες υλοποίησης της κάθε απαίτησης, οι οποίες είναι σύμφωνες με διεθνή πρότυπα, πλαίσια και βέλτιστες πρακτικές κυβερνοασφάλειας, όπως ενδεικτικά:

1. NIST Cybersecurity Framework 2.0
2. ISO / IEC 27002:2022
3. NIST SP 800-53 rev. 5
4. CIS Critical Security Controls v8.1
5. ENISA, Technical Implementation Guidance on Commission Implementing Regulation (EU) 2024/2690
6. US Joint Ransomware Task Force (CISA, NSA, FBI, MS-ISAC), StopRansomware Guide

Οι **διαδικασίες αξιολόγησης** προσδιορίζουν, για κάθε απαίτηση, έως τρεις διαφορετικές μεθόδους ελέγχου και τεκμηρίωσης της υλοποίησής της. Στο παρόν Εγχειρίδιο, υιοθετείται η οδηγία του NIST SP 800-53A rev. 5 “Assessing Security and Privacy Controls in Information Systems and Organizations”, σύμφωνα με την οποία οι μέθοδοι αξιολόγησης είναι οι εξής:

α. εξέταση (examine): είναι η διαδικασία επισκόπησης, μελέτης, παρατήρησης, αναθεώρησης ή ανάλυσης ενός ή περισσοτέρων αντικειμένων αξιολόγησης (π.χ. η μελέτη πολιτικών ασφάλειας και διαδικασιών, η επισκόπηση διαγραμμάτων δικτύου, η παρατήρηση εγκατάστασης συγκεκριμένου υλικού ή λογισμικού κ.α.),

β. συνέντευξη (interview): είναι η διαδικασία διενέργειας συζητήσεων με άτομα ή ομάδες ατόμων εντός της επιχείρησης, με σκοπό τη λήψη διευκρινήσεων και τεκμηριωτικών στοιχείων για ένα ή περισσότερα αντικείμενα αξιολόγησης,

γ. δοκιμή (test): είναι η διαδικασία δοκιμής ενός ή περισσοτέρων αντικειμένων αξιολόγησης κάτω από συγκεκριμένες συνθήκες, με σκοπό τη σύγκριση μεταξύ πραγματικής και αναμενόμενης συμπεριφοράς (π.χ. η δοκιμή των μηχανισμών ελέγχου πρόσβασης και αυθεντικοποίησης, των μηχανισμών λήψης αντιγράφων ασφαλείας ή η δοκιμή του πλάνου αντιμετώπισης περιστατικών).

Οι μικρομεσαίες επιχειρήσεις διαφέρουν σημαντικά ως προς το μέγεθος, τον κλάδο δραστηριότητας, τον βαθμό ψηφιακής εξάρτησης, την πολυπλοκότητα των πληροφοριακών τους συστημάτων και τους διαθέσιμους πόρους. Ως εκ τούτου, οι απαιτήσεις του Εγχειριδίου πρέπει να εφαρμόζονται με τρόπο ανάλογο προς την έκθεση κάθε επιχείρησης σε κινδύνους κυβερνοασφάλειας, την κρισιμότητα των συστημάτων και των δεδομένων της, το κόστος των μέτρων, καθώς και τις επιχειρησιακές και κανονιστικές της υποχρεώσεις.

Παράλληλα, το Εγχειρίδιο δεν υποκαθιστά τυχόν ειδικές υποχρεώσεις που απορρέουν από την εθνική ή ενωσιακή νομοθεσία, τομεακές ρυθμίσεις, συμβατικές δεσμεύσεις ή από διεθνή πρότυπα ασφάλειας πληροφοριών. Αντιθέτως, λειτουργεί συμπληρωματικά προς αυτά, παρέχοντας στις μικρομεσαίες επιχειρήσεις ένα πρακτικό σημείο εκκίνησης για τη βελτίωση του επιπέδου κυβερνοασφάλειάς τους και για τη σταδιακή μετάβαση σε πιο ώριμες πρακτικές διαχείρισης κινδύνων στον κυβερνοχώρο.

Η εφαρμογή του Εγχειριδίου πρέπει να νοείται ως συνεχής διαδικασία και όχι ως εφάπαξ ενέργεια. Η “κυβερνοϋγιεινή” προϋποθέτει περιοδική ανασκόπηση, επικαιροποίηση και βελτίωση των μέτρων ασφάλειας, ιδίως όταν μεταβάλλονται οι επιχειρησιακές λειτουργίες, οι χρησιμοποιούμενες τεχνολογίες, οι εξωτερικοί συνεργάτες, το κανονιστικό περιβάλλον ή το επίπεδο των κυβερνοαπειλών.

1. Διακυβέρνηση κυβερνοασφάλειας

ΑΠΑΙΤΗΣΗ 1.1

Αναπτύξτε κατάλληλους μηχανισμούς και διαδικασίες διαχείρισης στο ανώτατο επίπεδο ηγεσίας, με σκοπό την αποτελεσματική διακυβέρνηση των θεμάτων κυβερνοασφάλειας της επιχείρησης.

ΠΕΡΙΓΡΑΦΗ

- Λόγω της συνεχούς εξέλιξης του ψηφιακού μετασχηματισμού, η κυβερνοασφάλεια, πλέον, επηρεάζει κάθε πτυχή σε μία επιχείρηση. Η αποτελεσματική υλοποίηση μέτρων προστασίας, ανίχνευσης, απόκρισης και ανάκαμψης από κυβερνοεπιθέσεις προϋποθέτει τη διαχείριση των θεμάτων κυβερνοασφάλειας από το ανώτατο επίπεδο ηγεσίας. Η ανώτατη διοίκηση των επιχειρήσεων πρέπει να υλοποιήσει δομές διακυβέρνησης για την ασφάλεια των πληροφοριακών συστημάτων με σαφώς καθορισμένες γραμμές λήψης αποφάσεων, ευθύνης και λογοδοσίας.
- Η ανώτατη διοίκηση των επιχειρήσεων πρέπει να αναπτύξει στρατηγική για την κυβερνοασφάλεια, η οποία να ευθυγραμμίζεται με τη συνολική επιχειρηματική της στρατηγική και να ενσωματώνει διαδικασίες κυβερνοασφάλειας στο σύνολο των επιχειρηματικών της λειτουργιών, στην οργανωσιακή διαχείριση κινδύνου και στη λήψη αποφάσεων.
- Το εύρος των δομών διακυβέρνησης κυβερνοασφάλειας εξαρτάται από το μέγεθος και την πολυπλοκότητα των λειτουργιών της επιχείρησης και πρέπει να είναι το κατάλληλο με βάση την αρχή της αναλογικότητας.

ΟΔΗΓΙΕΣ ΥΛΟΠΟΙΗΣΗΣ

- Διασφαλίστε ότι τα στρατηγικά θέματα κυβερνοασφάλειας της επιχείρησής σας συζητούνται τακτικά στο ανώτατο επίπεδο ηγεσίας. Οι εν λόγω συζητήσεις βασίζονται σε έγκαιρες και ακριβείς πληροφορίες που προέρχονται από πηγές με επαρκή τεχνογνωσία. Στο πλαίσιο των εν λόγω συζητήσεων, η κυβερνοασφάλεια αναγνωρίζεται ως ουσιαστικός παράγοντας για την ανθεκτικότητα των επιχειρηματικών σας λειτουργιών.
- Αναθέστε σε ένα άτομο τη συνολική ευθύνη και λογοδοσία για την ασφάλεια των πληροφοριακών συστημάτων της επιχείρησής σας. Για τη στρατηγική διαχείριση των εν λόγω θεμάτων, το άτομο αυτό απευθύνεται απευθείας στο ανώτατο επίπεδο ηγεσίας. Για μικρές επιχειρήσεις, ο ρόλος του υπευθύνου κυβερνοασφάλειας μπορεί να ανατεθεί στον ιδιοκτήτη / διαχειριστή των πληροφοριακών αγαθών ή σε εξωτερικό συνεργάτη πληροφορικής, με σαφή όμως ευθύνη παρακολούθησης, κλιμάκωσης και λήψης αποφάσεων.
- Καθορίστε ρόλους και αρμοδιότητες όσον αφορά στην κυβερνοασφάλεια, σύμφωνα με τις επιχειρηματικές σας ανάγκες. Διασφαλίστε ότι το προσωπικό που αναλαμβάνει τέτοιους ρόλους διαθέτει τις κατάλληλες ικανότητες και τεχνογνωσία, καθώς και τους απαραίτητους πόρους για την εκτέλεση των καθηκόντων του.
- Αναθέστε, ως ανώτατη διοίκηση, την εξουσία λήψης αποφάσεων που σχετίζονται με τους κινδύνους κυβερνοασφάλειας στο προσωπικό με τις κατάλληλες αρμοδιότητες, ικανότητες και τεχνογνωσία. Στο πλαίσιο αυτό, αναπτύξτε κανάλια επικοινωνίας που διευκολύνουν τη ροή της

πληροφορίας εντός της επιχείρησής σας, καθώς και μετρήσιμους δείκτες που επιτρέπουν την κλιμάκωση της εξουσίας λήψης αποφάσεων όποτε τούτο κριθεί αναγκαίο.

- Τηρήστε απλό μητρώο κινδύνων κυβερνοασφάλειας, στο οποίο καταγράφονται τα κυριότερα σενάρια κινδύνου, η πιθανή επίπτωση, τα υφιστάμενα μέτρα, οι πρόσθετες απαιτούμενες ενέργειες, ο υπεύθυνος υλοποίησης και η καθορισμένη ημερομηνία επανεξέτασης. Το μητρώο επικαιροποιείται τουλάχιστον ετησίως ή κατόπιν σημαντικού περιστατικού, σημαντικής αλλαγής υποδομής ή νέας απειλής που εντοπίζεται από αξιόπιστες πηγές.
- Εξασφαλίστε ότι τα μέλη της ανώτατης διοίκησης παρακολουθούν, σε τακτική βάση, στοχευμένη εκπαίδευση σε θέματα κυβερνοασφάλειας, ώστε να αναγνωρίζουν τους κινδύνους που σχετίζονται με την επιχείρηση και να λαμβάνουν τεκμηριωμένες αποφάσεις. Η εκπαίδευση μπορεί να έχει τη μορφή σύντομων ενημερωτικών συναντήσεων, εξωτερικών σεμιναρίων ή προσομοιώσεων αντιμετώπισης περιστατικού σε επίπεδο διοίκησης (executive tabletop).
- Εντάξτε την κυβερνοασφάλεια στον ετήσιο προϋπολογισμό της επιχείρησής σας, με σαφή κατανομή πόρων για άδειες λογισμικού, εκπαίδευση προσωπικού, υπηρεσίες εξωτερικών συνεργατών και αντιμετώπιση περιστατικών.

ΔΙΑΔΙΚΑΣΙΕΣ ΑΞΙΟΛΟΓΗΣΗΣ

- Εξέταση / επισκόπηση:
  - πρακτικών διοικητικού συμβουλίου, στα οποία αποτυπώνονται τακτικές συζητήσεις για θέματα διαχείρισης κινδύνων κυβερνοασφάλειας,
  - γραπτών πολιτικών ασφάλειας πληροφοριακών συστημάτων, έγγραφων ή σε ψηφιακή μορφή, εγκεκριμένων από την ανώτατη διοίκηση του οργανισμού,
  - ετήσιου προϋπολογισμού κυβερνοασφάλειας και τεκμηριωτικών στοιχείων απορρόφησής του,
  - προγραμμάτων εκπαίδευσης για θέματα κυβερνοασφάλειας, υλικού εκπαίδευσης και αντίστοιχων βεβαιώσεων παρακολούθησης από μέλη της ανώτατης διοίκησης.
- Διενέργεια συνέντευξης / συζήτησης με τον υπεύθυνο κυβερνοασφάλειας, καθώς και με μέλη της ανώτατης διοίκησης της επιχείρησης.

ΑΠΑΙΤΗΣΗ 1.2

Εκπονήστε πολιτικές ασφάλειας πληροφοριακών συστημάτων, με σκοπό την ανάπτυξη μίας δομημένης, συνεπούς και νομικά επαρκούς προσέγγισης της προστασίας των πληροφοριακών σας αγαθών.

ΠΕΡΙΓΡΑΦΗ

- Οι πολιτικές ασφάλειας πληροφοριακών συστημάτων αποτελούν το κύριο σύνολο εγγράφων στο πλαίσιο της διακυβέρνησης της κυβερνοασφάλειας και αποτυπώνουν την προσέγγιση της διοίκησης για τη συνολική διαχείριση του προγράμματος κυβερνοασφάλειας μίας επιχείρησης. Οι πολιτικές ασφάλειας αποτελούν κείμενα που σε υψηλό επίπεδο ορίζουν το “τι” πρέπει να κάνει η επιχείρηση (μέτρα προστασίας, αρχές, υποχρεώσεις) και “ποιος” έχει την αρμοδιότητα και ευθύνη υλοποίησής τους. Στο πεδίο αυτό, διακρίνονται από τις διαδικασίες (procedures), οι οποίες

αποτελούν κείμενα που σε χαμηλό επίπεδο περιγράφουν το “πώς”, δηλαδή βήμα-προς-βήμα οδηγίες για την υλοποίηση των μέτρων και των υποχρεώσεων που καθορίζονται στις πολιτικές.

ΟΔΗΓΙΕΣ ΥΛΟΠΟΙΗΣΗΣ

- Εκπονήστε πολιτικές ασφάλειας πληροφοριακών συστημάτων. Το μέγεθος των πολιτικών εξαρτάται από το εύρος και την πολυπλοκότητα των επιχειρηματικών σας λειτουργιών. Ως ελάχιστο πακέτο πολιτικών για τις μικρομεσαίες επιχειρήσεις θα πρέπει να υπάρχουν σύντομα, πρακτικά και κατανοητά κείμενα για κοινές θεματικές περιοχές ασφάλειας πληροφοριακών συστημάτων, όπως, ενδεικτικά, είναι ο έλεγχος πρόσβασης, ο έλεγχος ταυτότητας πολλαπλών παραγόντων (MFA), η ορθή χρήση συστημάτων, οι ενημερώσεις ασφάλειας, η ασφάλεια του δικτύου, η χρήση cloud υπηρεσιών, η προστασία από κακόβουλο λογισμικό, η λήψη αντιγράφων ασφαλείας και η διαχείριση περιστατικών.
- Διασφαλίστε ότι οι πολιτικές ασφάλειας πληροφοριακών συστημάτων εγκρίνονται από την ανώτατη διοίκηση της επιχείρησης.
- Διασφαλίστε ότι οι πολιτικές ασφάλειας πληροφοριακών συστημάτων περιγράφουν, σε αφαιρετικό επίπεδο, απαιτήσεις που αφορούν σε μέτρα ασφάλειας και κανόνες για την προστασία των συστημάτων δικτύου και πληροφοριών από απειλές.
- Διασφαλίστε ότι οι πολιτικές ασφάλειας πληροφοριακών συστημάτων περιγράφουν με σαφήνεια το πεδίο εφαρμογής (scope) όσον αφορά στα συστήματα, δεδομένα, εφαρμογές, εξοπλισμό και οργανικές μονάδες ή / και χρήστες.
- Διασφαλίστε ότι οι πολιτικές ασφάλειας πληροφοριακών συστημάτων περιλαμβάνουν ανάθεση ρόλων, αρμοδιοτήτων και ευθυνών για χρήστες ή / και οργανικές μονάδες, με σκοπό τη σωστή εφαρμογή, την τήρηση και την επιβολή των απαιτήσεων κάθε πολιτικής, καθώς και για την επίτευξη λογοδοσίας.
- Διασφαλίστε ότι οι πολιτικές ασφάλειας πληροφοριακών συστημάτων κοινοποιούνται, ανάλογα με το περιεχόμενό τους, στους σχετικούς αποδέκτες, όπως είναι το προσωπικό και οι οργανικές μονάδες, οι προμηθευτές και πάροχοι υπηρεσιών ή / και άλλες εξωτερικές ομάδες ή αρχές. Όσον αφορά στο προσωπικό, διασφαλίστε ότι κάθε εργαζόμενος λαμβάνει γνώση των σχετικών πολιτικών κατά την έναρξη της εργασιακής σχέσης και σε κάθε ουσιώδη αναθεώρηση, τηρώντας απλό αρχείο ενυπόγραφης ή ηλεκτρονικής αποδοχής.
- Διατυπώστε τις πολιτικές σε απλή, σαφή και κατανοητή γλώσσα, αποφεύγοντας υπερβολικούς νομικούς ή τεχνικούς όρους όπου δεν είναι αναγκαίο, ώστε κάθε εργαζόμενος να μπορεί να κατανοήσει και να εφαρμόσει τις υποχρεώσεις που τον αφορούν.
- Τηρήστε έκδοση (versioning) και ημερομηνία ισχύος σε κάθε πολιτική, ώστε σε κάθε χρονική στιγμή να είναι σαφές ποια έκδοση ισχύει, ποιος την ενέκρινε και πότε.

ΔΙΑΔΙΚΑΣΙΕΣ ΑΞΙΟΛΟΓΗΣΗΣ

- Εξέταση / επισκόπιση γραπτών πολιτικών ασφάλειας πληροφοριακών συστημάτων, έγγραφων ή σε ψηφιακή μορφή, εγκεκριμένων από την ανώτατη διοίκηση της επιχείρησης.
- Διενέργεια συνέντευξης / συζήτησης με τον υπεύθυνο κυβερνοασφάλειας, καθώς και με μέλη της ανώτατης διοίκησης της επιχείρησης.

ΑΠΑΙΤΗΣΗ 1.3

Διενεργήστε ανασκόπηση και επικαιροποίηση των πολιτικών ασφάλειας πληροφοριακών συστημάτων σε περιοδικά διαστήματα, καθώς και όταν λαμβάνουν χώρα σοβαρά περιστατικά κυβερνοασφάλειας ή σημαντικές αλλαγές στις λειτουργίες της επιχείρησης.

ΠΕΡΙΓΡΑΦΗ

- Η ανασκόπηση και επικαιροποίηση των πολιτικών ασφάλειας πληροφοριακών συστημάτων πρέπει να διενεργείται σε περιοδικά διαστήματα, κατά προτίμηση σε ετήσια βάση, αξιολογώντας αλλαγές που έχουν συμβεί στο περιβάλλον της επιχείρησης, με σκοπό τη βελτίωση του επιπέδου κυβερνοασφάλειάς της και την προσαρμογή της στο μεταβαλλόμενο περιβάλλον κυβερνοαπειλών.

ΟΔΗΓΙΕΣ ΥΛΟΠΟΙΗΣΗΣ

- Διενεργήστε ανασκόπηση και επικαιροποίηση των πολιτικών ασφάλειας πληροφοριακών συστημάτων σε περιοδικά διαστήματα, λαμβάνοντας υπόψη διάφορες παραμέτρους, όπως ενδεικτικά:
  - προμήθειες νέων τεχνολογιών πληροφορικής και επικοινωνιών που μεταβάλλουν σημαντικά την ψηφιακή επιφάνεια επίθεσης (π.χ. τεχνολογίες που βασίζονται στην Τεχνητή Νοημοσύνη),
  - αλλαγές στο νομοθετικό και κανονιστικό πλαίσιο που επιβάλλουν νέες απαιτήσεις στις επιχειρήσεις,
  - μεταβολές στο νομικό ή επιχειρηματικό καθεστώς της επιχείρησης (εξαγορές, συγχωνεύσεις κ.α.),
  - ευρήματα σημαντικών κενών ασφάλειας από ελέγχους ευπαθειών ή δοκιμών παρείσδυσης, που επιβάλλουν ενίσχυση των μέτρων κυβερνοασφάλειας,
  - σοβαρά περιστατικά κυβερνοασφάλειας, που επιβάλλουν την αναθεώρηση πολιτικών και διαδικασιών, καθώς και τη λήψη κατάλληλων τεχνικών, οργανωτικών και επιχειρησιακών μέτρων περιορισμού των κινδύνων σε αποδεκτό όριο.
  - Σε κάθε αναθεώρηση πολιτικής, επικοινωνήστε συνοπτικά τις αλλαγές στους εργαζομένους και τους εξωτερικούς συνεργάτες και ζητήστε εκ νέου ενημερωμένη αποδοχή, όπου αυτό απαιτείται.

ΔΙΑΔΙΚΑΣΙΕΣ ΑΞΙΟΛΟΓΗΣΗΣ

- Εξέταση / επισκόπηση:
  - εγγράφων, αρχείων ή αναφορών που αφορούν σε διαδικασίες ανασκόπησης ή αναθεώρησης πολιτικών ασφάλειας πληροφοριακών συστημάτων,
  - αναθεωρημένων ή επικαιροποιημένων πολιτικών ασφάλειας πληροφοριακών συστημάτων, εγκεκριμένων από την ανώτατη διοίκηση του οργανισμού.
- Διενέργεια συνέντευξης / συζήτησης με τον υπεύθυνο κυβερνοασφάλειας, καθώς και με μέλη της ανώτατης διοίκησης της επιχείρησης.

2. Καταγραφή και διαχείριση πληροφοριακών αγαθών

ΑΠΑΙΤΗΣΗ 2.1

Αναπτύξτε αναλυτικό μητρώο των πληροφοριακών αγαθών που φιλοξενούνται στην υποδομή σας, καθώς και σε περιβάλλοντα νεφοϋπολογιστικής, με σκοπό την πλήρη κατανόηση του εύρους των αγαθών και των αναγκαίων μέτρων προστασίας και συντήρησής τους.

ΠΕΡΙΓΡΑΦΗ

- Ο φυσικός τεχνολογικός εξοπλισμός των επιχειρήσεων περιλαμβάνει υπολογιστές χρηστών (σταθερούς και φορητούς), διακομιστές, δικτυακές συσκευές (δρομολογητές, switches), καθώς και φορητά μέσα αποθήκευσης ή και συσκευές IoT (Internet-of-Things). Το λογισμικό περιλαμβάνει λειτουργικά συστήματα, καθώς και κάθε είδους εφαρμογές και υπηρεσίες που προσφέρουν επιχειρηματική αξία. Στις εν λόγω εφαρμογές συμπεριλαμβάνεται και το λογισμικό τεχνητής νοημοσύνης, ιδίως πράκτορες τεχνητής νοημοσύνης (AI agents) που αποκτούν πρόσβαση σε εταιρικά δεδομένα.
- Ο εντοπισμός και η καταγραφή των πληροφοριακών αγαθών (information asset inventory), τόσο εντός της υποδομής όσο και σε περιβάλλοντα νεφοϋπολογιστικής (cloud), παρέχει στις επιχειρήσεις πλήρη εικόνα των τεχνολογιών πληροφορικής και επικοινωνιών που διαθέτουν και αποτελεί βασική πληροφορία για την υλοποίηση των κατάλληλων μέτρων κυβερνοασφάλειας.

ΟΔΗΓΙΕΣ ΥΛΟΠΟΙΗΣΗΣ

- Αναπτύξτε αναλυτικό μητρώο των πληροφοριακών αγαθών που φιλοξενούνται στην υποδομή σας, καθώς και σε περιβάλλοντα νεφοϋπολογιστικής. Η ανάπτυξη του εν λόγω μητρώου δε συνεπάγεται, κατ' ανάγκη, την τήρηση ενός και μοναδικού καταλόγου, αλλά μπορεί να ιδωθεί ως ένα δυναμικό σύνολο διακριτών καταγραφών υλικού, λογισμικού, εικονικών μηχανών κ.λπ. Κατά περίπτωση, η ανάπτυξη του μητρώου δύναται να υποστηριχθεί και από ειδικές προς τούτο εφαρμογές ιχνηλάτησης / διαχείρισης πληροφοριακών αγαθών (asset discovery / asset management tools).
- Διασφαλίστε ότι το μητρώο πληροφοριακών αγαθών περιέχει επαρκή στοιχεία περιγραφής, όπως ενδεικτικά machine name, IP διεύθυνση (εφόσον είναι static), mac address, όνομα ιδιοκτήτη, έκδοση, αριθμός αδειών, περιγραφή λειτουργίας, τοποθεσία κ.λπ. Το βάθος λεπτομέρειας του μητρώου ανταποκρίνεται στις ανάγκες της επιχείρησης.
- Ορίστε έναν ιδιοκτήτη (asset owner) για κάθε αγαθό που έχει εντοπισθεί. Ο ιδιοκτήτης (άτομο, ομάδα ή υπηρεσιακή δομή) είναι υπεύθυνος για την ορθή διαχείριση του αγαθού καθ' όλη τη διάρκεια του κύκλου ζωής του.
- Διασφαλίστε ότι το μητρώο πληροφοριακών αγαθών επικαιροποιείται τακτικά με κάθε αλλαγή, προσθήκη ή αφαίρεση αγαθών.
- Εντοπίστε τα «σκιώδη» πληροφοριακά αγαθά (shadow IT) της επιχείρησής σας. Πρόκειται για τεχνολογίες πληροφορικής που έχουν αποκτηθεί εκτός των επίσημων διαδικασιών προμηθειών, χωρίς την έγκριση ή και τη γνώση του τμήματος πληροφορικής. Η έλλειψη ορατότητας και ελέγχου για τα εν λόγω αγαθά οδηγεί σε σοβαρούς κινδύνους ασφάλειας, όπως η εξαίρεσή τους από τις

τακτικές ενημερώσεις λογισμικού, η παράκαμψη των εγκεκριμένων μηχανισμών ελέγχου πρόσβασης και η επιβολή κυρώσεων.

- Παρακολουθήστε τις άδειες χρήσης λογισμικού (software licenses) και τις ημερομηνίες λήξης τους, για αποφυγή τόσο ελλιπούς υποστήριξης από τον προμηθευτή όσο και ζητημάτων συμβατικής συμμόρφωσης.
- Διαμορφώστε κανόνες για την ασφαλή διαχείριση των φορητών μέσων αποθήκευσης (USB, εξωτερικοί σκληροί δίσκοι κ.α.), όπως ενδεικτικά:
  - Χρησιμοποιήστε μόνο εγκεκριμένα φορητά μέσα.
  - Απενεργοποιήστε τη λειτουργία AutoRun / AutoPlay στα φορητά μέσα.
  - Διασφαλίστε ότι το antivirus / antimalware software διενεργεί σάρωση των φορητών μέσων κατά τη σύνδεσή τους με το υπολογιστικό σύστημα.
  - Διασφαλίστε ότι τα εμπιστευτικά και ευαίσθητα δεδομένα τηρούνται κρυπτογραφημένα στα φορητά μέσα.
  - Μη συνδέετε άγνωστα φορητά μέσα σε εταιρικούς υπολογιστές. Φορητά μέσα που ευρίσκονται τυχαία στους χώρους της επιχείρησης, καθώς και αυτά που προέρχονται από πελάτες, προμηθευτές, επισκέπτες κ.λπ. πρέπει να αντιμετωπίζονται ως μη έμπιστα.

ΔΙΑΔΙΚΑΣΙΕΣ ΑΞΙΟΛΟΓΗΣΗΣ

- Εξέταση / επισκόπηση / παρατήρηση:
  - μητρώου πληροφοριακών αγαθών (π.χ. αρχεία excel ή λογισμικό asset discovery / asset management).
  - δειγματοληπτικού εύρους πληροφοριακών αγαθών και επιβεβαίωση εγγραφής τους στο μητρώο.
- Διενέργεια συνέντευξης / συζήτησης με τον υπεύθυνο κυβερνοασφάλειας, καθώς και με μέλη του προσωπικού με αρμοδιότητα τη διαχείριση των πληροφοριακών αγαθών.

ΑΠΑΙΤΗΣΗ 2.2

Εκπονήστε πολιτική και κανόνες για την ορθή χρήση των πληροφοριακών αγαθών, καθώς και των δεδομένων, που θα καλύπτει την πλήρη διάρκεια του κύκλου ζωής τους.

ΠΕΡΙΓΡΑΦΗ

- Το προσωπικό και οι εξωτερικοί χρήστες που χρησιμοποιούν ή έχουν αποκτήσει πρόσβαση σε πληροφοριακά αγαθά και δεδομένα μίας επιχείρησης πρέπει να ενημερώνονται για τις απαιτήσεις ασφάλειας που αφορούν στην προστασία και στο χειρισμό τους. Η πολιτική ορθής χρήσης περιέχει σαφείς κανόνες και υποχρεώσεις για την αποδεκτή και ορθή χρήση των συσκευών, εφαρμογών και δεδομένων μίας επιχείρησης και οι αποδέκτες της είναι υπεύθυνοι για την ορθή εφαρμογή της. Οι εν λόγω κανόνες καλύπτουν τον πλήρη κύκλο ζωής των αγαθών και δεδομένων και λαμβάνουν υπόψη τα διακριτά επίπεδα κρισιμότητάς τους και τους καθορισμένους κινδύνους.

ΟΔΗΓΙΕΣ ΥΛΟΠΟΙΗΣΗΣ

- Εκπονήστε πολιτική ορθής χρήσης των πληροφοριακών αγαθών και δεδομένων, που να καλύπτει τον πλήρη κύκλο ζωής τους (απόκτηση, χρήση, αποθήκευση, μεταφορά, τελική απόρριψη). Η εν λόγω πολιτική αφορά στην εφαρμογή απαιτήσεων ασφάλειας με βάση τον κίνδυνο που σχετίζεται με τη χρήση κάθε αγαθού. Οι κανόνες ορθής χρήσης των αγαθών και των δεδομένων πρέπει να είναι ανάλογες με τα επίπεδα κατηγοριοποίησης τους.
- Διασφαλίστε ότι η πολιτική ορθής χρήσης καλύπτει τουλάχιστον τα παρακάτω:
  - Τις αναμενόμενες και μη αποδεκτές συμπεριφορές χρηστών υπό το πρίσμα της ασφάλειας πληροφοριών.
  - Τους επιτρεπόμενους και απαγορευμένους τρόπους χρήσης των πληροφοριακών αγαθών και των δεδομένων της επιχείρησης.
  - Τις δραστηριότητες παρακολούθησης (monitoring activities) που διενεργούνται από την επιχείρηση.
  - Την ορθή χρήση των τεχνολογιών τεχνητής νοημοσύνης.
  - Τις διαδικασίες που αφορούν στην αποχώρηση προσωπικού ή χρηστών (επιστροφή εταιρικού εξοπλισμού, απενεργοποίηση λογαριασμών, ασφαλής διαγραφή δεδομένων κ.α.).
- Διασφαλίστε ότι η πολιτική ορθής χρήσης καλύπτει το σύνολο των αγαθών και δεδομένων του πεδίου εφαρμογής, όπως ενδεικτικά:
  - σταθερές και κινητές συσκευές, καθώς και φορητά μέσα αποθήκευσης (USB),
  - πόρους στην υποδομή του οργανισμού, καθώς και πόρους νεφοϋπολογιστικής (cloud),
  - διαχείριση προσωπικών συσκευών στο χώρο εργασίας (Bring Your Own Device - BYOD).
- Διασφαλίστε ότι η πολιτική ορθής χρήσης κοινοποιείται στο προσωπικό, στους προμηθευτές και παρόχους υπηρεσιών, καθώς και σε οποιονδήποτε εξωτερικό χρήστη χρησιμοποιεί ή έχει πρόσβαση σε πληροφοριακά αγαθά και δεδομένα της επιχείρησής σας.

ΔΙΑΔΙΚΑΣΙΕΣ ΑΞΙΟΛΟΓΗΣΗΣ

- Εξέταση / επισκόπηση:
  - γραπτής πολιτικής ορθής χρήσης πληροφοριακών αγαθών, έγγραφης ή σε ψηφιακή μορφή, εγκεκριμένης από την ανώτατη διοίκηση του οργανισμού,
  - βεβαιώσεων, έγγραφων ή σε ψηφιακή μορφή, ότι το προσωπικό και οι σχετικοί εξωτερικοί παράγοντες (προμηθευτές και πάροχοι υπηρεσιών ή / και άλλοι χρήστες / ομάδες) έχουν λάβει γνώση της πολιτικής ορθής χρήσης πληροφοριακών αγαθών.
- Διενέργεια συνέντευξης / συζήτησης με τον υπεύθυνο κυβερνοασφάλειας, καθώς και με μέλη του προσωπικού με αρμοδιότητα τη διαχείριση των πληροφοριακών αγαθών.

ΑΠΑΙΤΗΣΗ 2.3

Καθορίστε διακριτά επίπεδα κατηγοριοποίησης των δεδομένων που επεξεργάζεστε, ανάλογα με την κρισιμότητά τους.

ΠΕΡΙΓΡΑΦΗ

- Οι πληροφορίες / δεδομένα πρέπει να ταξινομούνται / κατηγοριοποιούνται σε διακριτά επίπεδα, ανάλογα με τις επιχειρησιακές απαιτήσεις προστασίας της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητάς τους. Τα διαφορετικά επίπεδα υποδεικνύουν και τα απαιτούμενα μέτρα προστασίας των δεδομένων ανάλογα με την ευαισθησία και την επιχειρηματική τους αξία. Το επίπεδο ταξινόμησης / κατηγοριοποίησης (classification level) μπορεί να καθορισθεί από το επίπεδο των επιπτώσεων που μία παραβίαση δεδομένων θα είχε στην επιχείρηση.

ΟΔΗΓΙΕΣ ΥΛΟΠΟΙΗΣΗΣ

- Καθορίστε διακριτά επίπεδα ταξινόμησης / κατηγοριοποίησης των δεδομένων που επεξεργάζεστε ανάλογα με την κρισιμότητά τους. Προς διευκόλυνση, κάθε επίπεδο ταξινόμησης μπορεί να λάβει μία ονομασία που θα έχει νόημα εντός του πλαισίου της επιχείρησης. Καθορίστε και επικοινωνήστε ονομασίες που σχετίζονται με το βαθμό ευαισθησίας των δεδομένων, π.χ. δημόσιας χρήσης, εσωτερικής χρήσης, εμπιστευτικό κ.α. Μπορείτε να χρησιμοποιήσετε σχήματα ταξινόμησης που απορρέουν από την εθνική νομοθεσία ή διεθνώς αναγνωρισμένα πρότυπα διαμοιρασμού πληροφορίας, όπως π.χ. το traffic light protocol (TLP).
- Διασφαλίστε ότι τα πληροφοριακά αγαθά της επιχείρησης (συστήματα, εξοπλισμός και λογισμικό) κατηγοριοποιούνται ανάλογα με το επίπεδο ταξινόμησης / κατηγοριοποίησης των δεδομένων που αποθηκεύουν και επεξεργάζονται.
- Λάβετε ιδιαίτερη μέριμνα για τις ειδικές κατηγορίες προσωπικών δεδομένων του άρθρου 9 του Γενικού Κανονισμού Προστασίας Δεδομένων (GDPR), όπως είναι δεδομένα υγείας, βιομετρικά κ.λπ., τα οποία απαιτούν εγγενώς αυστηρότερα μέτρα προστασίας, ανεξαρτήτως του εσωτερικού επιπέδου ταξινόμησης.

ΔΙΑΔΙΚΑΣΙΕΣ ΑΞΙΟΛΟΓΗΣΗΣ

- Εξέταση / επισκόπηση:
  - Καταγεγραμμένων, σε έγγραφη ή ψηφιακή μορφή, επιπέδων κατηγοριοποίησης / ταξινόμησης των δεδομένων / πληροφοριών και των πληροφοριακών αγαθών, καθώς και των κανόνων διαμοιρασμού πληροφορίας,
  - Επικαιροποιημένου μητρώου πληροφοριακών αγαθών, μαζί με τα επίπεδα κατηγοριοποίησης / ταξινόμησης ανά αγαθό.
- Διενέργεια συνέντευξης / συζήτησης με τον υπεύθυνο κυβερνοασφάλειας, καθώς και με μέλη του προσωπικού με αρμοδιότητα τη διαχείριση των πληροφοριακών αγαθών.

ΑΠΑΙΤΗΣΗ 2.4

Καθορίστε κανόνες ασφάλειας για τη διαχείριση των προσωπικών συσκευών που οι εργαζόμενοι χρησιμοποιούν για εργασιακές δραστηριότητες.

ΠΕΡΙΓΡΑΦΗ

- Η χρήση προσωπικών συσκευών των εργαζομένων για εργασιακούς σκοπούς (bring your own device – BYOD), ενώ προσφέρει ευελιξία και ευκολία, εν τούτοις μπορεί να προκαλέσει απώλεια δεδομένων της επιχείρησης, καθώς και παραβίαση της ιδιωτικότητας. Όταν η επιχείρηση επιτρέπει τη χρήση τέτοιων συσκευών (laptops, tablets, smartphones) για την επεξεργασία δεδομένων της, τότε θα πρέπει να υλοποιείται ένα μοντέλο με βάση ανάλυση κινδύνου (risk-based) και με πυρήνα την αρχή των ελάχιστων προνομίων (least privilege).

ΟΔΗΓΙΕΣ ΥΛΟΠΟΙΗΣΗΣ

- Διαμορφώστε σαφείς κανόνες για την επιτρεπόμενη χρήση BYOD συσκευών στην επιχείρησή σας. Κατ' ελάχιστο, η BYOD συσκευή πρέπει, απαραίτητα:
  - να τρέχει λειτουργικό σύστημα που να υποστηρίζεται ενεργά,
  - να λαμβάνει τακτικές ενημερώσεις ασφάλειας από τον κατασκευαστή, κατά προτίμηση αυτοματοποιημένες,
  - να χρησιμοποιεί μόνο υποστηριζόμενα προγράμματα περιήγησης στο διαδίκτυο (browsers) και υποστηριζόμενες client εφαρμογές κατά την πρόσβαση σε εταιρικά δεδομένα,
  - να υποστηρίζει την κρυπτογράφηση συσκευής (device encryption),
  - να εφαρμόζει έλεγχο ταυτότητας πολλαπλών παραγόντων (MFA) για την πρόσβαση σε εταιρικά δεδομένα (εταιρικό email, cloud εφαρμογές, απομακρυσμένη σύνδεση, διαχειριστικοί λογαριασμοί).

  Ως γενική οδηγία, οι BYOD συσκευές αποκτούν πρόσβαση μόνο στους εταιρικούς πόρους που απαιτείται, μόνο όταν υλοποιούν μία ελάχιστη βάση μέτρων ασφάλειας και μόνο μέσω διαδικασιών ισχυρής αυθεντικοποίησης.
- Εξετάστε τη χρήση εργαλείων ή υπηρεσιών MDM (Mobile Device Management) ή UEM (Unified Endpoint Management), ώστε να μπορείτε να εφαρμόσετε πολιτικές όπως εντοπισμός συσκευής, απομακρυσμένη διαγραφή εταιρικών δεδομένων και επιβολή μέτρων ασφάλειας.

ΔΙΑΔΙΚΑΣΙΕΣ ΑΞΙΟΛΟΓΗΣΗΣ

- Εξέταση / επισκόπηση / παρατήρηση:
  - πολιτικών και διαδικασιών που αφορούν σε διαχείριση BOYD συσκευών,
  - επιβαλλόμενων μέτρων ασφάλειας σε επιλεγμένο δείγμα BYOD συσκευών.
- Διενέργεια συνέντευξης / συζήτησης με τον υπεύθυνο κυβερνοασφάλειας, καθώς και με μέλη του προσωπικού με αρμοδιότητα τη διαχείριση των πληροφοριακών αγαθών.

3. Ασφαλής παραμετροποίηση υλικού και λογισμικού

ΑΠΑΙΤΗΣΗ 3.1

Υλοποιήστε ασφαλείς παραμετροποιήσεις (secure configurations) σε υλικό και λογισμικό, ανάλογες με την κρισιμότητα των επιχειρηματικών σας λειτουργιών.

ΠΕΡΙΓΡΑΦΗ

- Οι προεπιλεγμένες (default) παραμετροποιήσεις στα αγαθά και στο λογισμικό μίας επιχείρησης συχνά προσανατολίζονται στην ευκολία εγκατάστασης και χρήσης και λιγότερο στην ασφάλεια. Ενδεικτικά, ανοικτές θύρες και υπηρεσίες, προεπιλεγμένα συνθηματικά, προεγκατάσταση περιττού λογισμικού κ.α., αποτελούν ευπάθειες που εν δυνάμει συνιστούν αντικείμενο εκμετάλλευσης εάν αφεθούν στις αρχικές τους ρυθμίσεις.
- Οι παραμετροποιήσεις που σχετίζονται με την ασφάλεια μπορούν να υλοποιηθούν σε διακομιστές, υπολογιστές χρηστών, συσκευές εισόδου – εξόδου (π.χ. εκτυπωτές, σαρωτές, κ.α.), δικτυακές συσκευές (π.χ. δρομολογητές, firewalls, ασύρματα σημεία πρόσβασης, κ.α.), IoT συσκευές, λειτουργικά συστήματα και εφαρμογές.
- Οι παραμετροποιήσεις ασφάλειας περιλαμβάνουν ρυθμίσεις στη registry, ρυθμίσεις δικαιωμάτων και προνομίων πρόσβασης σε λογαριασμούς, αρχεία ή καταλόγους (directories), καθώς και ρυθμίσεις για λειτουργίες, δικτυακές θύρες, πρωτόκολλα και απομακρυσμένες συνδέσεις.

ΟΔΗΓΙΕΣ ΥΛΟΠΟΙΗΣΗΣ

- Υλοποιήστε ασφαλείς παραμετροποιήσεις (secure configurations) σε συστήματα, εφαρμογές, υπηρεσίες και δίκτυα, ανάλογες με την κρισιμότητα των επιχειρηματικών σας λειτουργιών. Για την υλοποίηση ασφαλών παραμετροποιήσεων σε συγκεκριμένες τεχνολογικές πλατφόρμες και προϊόντα, εξετάστε την εφαρμογή αντίστοιχων οδηγιών ή σημείων αναφοράς (benchmarks) από αναγνωρισμένους οργανισμούς, όπως ενδεικτικά κατασκευαστές προϊόντων και λογισμικού, ερευνητικά / ακαδημαϊκά ιδρύματα ή δημόσιες αρχές.
- Υλοποιήστε την αρχή της ελάχιστης λειτουργικότητας (least functionality), ρυθμίζοντας τα συστήματά σας να παρέχουν μόνο τις λειτουργίες που είναι απαραίτητες για τις επιχειρηματικές σας ανάγκες. Για το σκοπό αυτό, απενεργοποιήστε ή αφαιρέστε λειτουργίες, δικτυακές θύρες, πρωτόκολλα, συνδέσεις και υπηρεσίες που είναι περιττές ή ανασφαλείς. Ειδικότερα:
  - Μη χρησιμοποιείτε ανασφαλή πρωτόκολλα, όπως π.χ. το Telnet, το HTTP, FTP ή SMBv1.
  - Απενεργοποιήστε δικτυακές θύρες (network ports) που δεν χρησιμοποιούνται.
- Εφαρμόστε ασφαλείς παραμετροποιήσεις στο πρωτόκολλο RDP (Remote Desktop Protocol). Οι επιτιθέμενοι συχνά αποκτούν αρχική πρόσβαση σε ένα δίκτυο μέσω εκτεθειμένων και μη σωστά παραμετροποιημένων απομακρυσμένων υπηρεσιών και κατόπιν μετακινούνται στο δίκτυο. Εάν το RDP είναι απαραίτητο, εφαρμόστε βέλτιστες πρακτικές. Ελέγξτε το δίκτυό σας για συστήματα που χρησιμοποιούν το RDP, κλείστε τις θύρες RDP που δεν χρησιμοποιούνται, επιβάλλετε κλείδωμα λογαριασμών (account lockouts) μετά από προκαθορισμένο αριθμό προσπαθειών εισόδου, υλοποιείστε MFA (multi factor authentication) και καταγράψτε (logging) τις προσπάθειες εισόδου μέσω του RDP.

- Εφαρμόστε ασφαλείς παραμετροποιήσεις στο πρωτόκολλο SMB (Server Message Block), ειδικότερα:
    - Διακόψτε, στο firewall της εξωτερικής περιμέτρου του δικτύου, την εισερχόμενη από και εξερχόμενη προς το Internet επικοινωνία στις παρακάτω θύρες: TCP 445 (SMB), UDP 137 (NetBIOS Name Resolution), UDP 138 (NetBIOS Datagram Service) και TCP 139 (NetBIOS Session Service).
    - Διακόψτε ή περιορίστε την εσωτερική SMB κίνηση, έτσι ώστε οι επικοινωνίες να λαμβάνουν χώρα μόνο μεταξύ των συστημάτων που απαιτείται. Για παράδειγμα, οι Windows συσκευές χρειάζονται τις SMB επικοινωνίες με τους domain controllers για να λαμβάνουν την group policy, αλλά οι περισσότεροι σταθμοί εργασίας με Windows δεν χρειάζεται να έχουν πρόσβαση σε άλλους σταθμούς εργασίας με Windows.
    - Απενεργοποιήστε την έκδοση SMBv1 στο εσωτερικό δίκτυο και αναβαθμίστε στην έκδοση v3 ή στην πλέον πρόσφατη, μετά την επίλυση υφιστάμενων εξαρτήσεων (dependencies) σε υπάρχοντα συστήματα ή εφαρμογές.
- Απεγκαταστήστε ή απενεργοποιήστε λογισμικό και υπηρεσίες που δεν χρησιμοποιούνται.
- Υλοποιείστε ασφαλείς παραμετροποιήσεις για την εγκατάσταση λογισμικού από χρήστες, όπως ενδεικτικά:
    - Επιτρέψτε την εγκατάσταση νέου λογισμικού μόνο σε χρήστες με λογαριασμούς αυξημένων προνομίων.
    - Επιτρέψτε την εγκατάσταση ενημερώσεων και ενημερώσεων ασφάλειας για υπάρχον λογισμικό σε χρήστες με μη προνομιακούς λογαριασμούς.
    - Επιτρέψτε την εγκατάσταση νέου λογισμικού από αποθετήρια που ελέγχονται από τον οργανισμό σε χρήστες με μη προνομιακούς λογαριασμούς.
    - Απαγορέψτε την εγκατάσταση λογισμικού με άγνωστη ή ύποπτη προέλευση που θεωρείται δυνητικά κακόβουλο.
- Εφαρμόστε διαδικασία ελέγχου αλλαγών (change management) για κάθε ουσιώδη μεταβολή των ασφαλών παραμετροποιήσεων: αιτιολόγηση, υπεύθυνος έγκρισης, ημερομηνία υλοποίησης. Στις μικρές επιχειρήσεις, αρκεί ένα απλό αρχείο καταγραφής αλλαγών.

ΔΙΑΔΙΚΑΣΙΕΣ ΑΞΙΟΛΟΓΗΣΗΣ

- Εξέταση / επισκόπηση:
    - πολιτικών ή διαδικασιών που αφορούν σε παραμετροποιήσεις ασφάλειας συστημάτων,
    - δειγματοληπτικού εύρους συστημάτων για την επιβεβαίωση συμμόρφωσης των παραμετροποιήσεών τους με γνωστά πρότυπα ή σημεία αναφοράς.
- Διενέργεια συνέντευξης / συζήτησης με τον υπεύθυνο κυβερνοασφάλειας, καθώς και με μέλη του προσωπικού με αρμοδιότητα την παραμετροποίηση συστημάτων, εφαρμογών, υπηρεσιών και δικτύων.

ΑΠΑΙΤΗΣΗ 3.2

Διασφαλίστε ότι οι προεπιλεγμένοι λογαριασμοί (default accounts) σε συσκευές με δημόσια πρόσβαση στο διαδίκτυο απενεργοποιούνται ή τροποποιούνται αμέσως μετά την εγκατάσταση των συσκευών.

ΠΕΡΙΓΡΑΦΗ

- Παρατηρείται συχνά, σε συσκευές που είναι συνδεδεμένες στο διαδίκτυο (routers, access points, εκτυπωτές, κάμερες, αλλά και σε συσκευές επιχειρησιακής τεχνολογίας κρίσιμων υποδομών όπως είναι τα PLCs) η ύπαρξη προεπιλεγμένων από τον κατασκευαστή λογαριασμών για τους οποίους δεν έχει αλλαχθεί ο αρχικός (default) κωδικός, που συνήθως είναι της μορφής “1234”, “default”, “admin”, “password”, κ.α. Το γεγονός αυτό αποτελεί κρίσιμη ευπάθεια που εκμεταλλεύονται συνεχώς οι επιτιθέμενοι, καθώς μέσω αυτής αποκτούν εύκολα μη εξουσιοδοτημένη πρόσβαση σε συστήματα.

ΟΔΗΓΙΕΣ ΥΛΟΠΟΙΗΣΗΣ

- Διασφαλίστε ότι οι προεπιλεγμένοι λογαριασμοί (default accounts) απενεργοποιούνται ή τροποποιούνται κατά την εγκατάσταση κάθε νέου προϊόντος, συστήματος ή εφαρμογής και εφαρμόστε διαδικασία ρύθμισης μοναδικών και ισχυρών κωδικών πρόσβασης (unique and strong passwords) για κάθε διακριτή συσκευή, ιδίως γι’ αυτές που είναι προσβάσιμες από το διαδίκτυο.
- Αποθηκεύστε τα νέα ισχυρά διαπιστευτήρια σε εγκεκριμένο διαχειριστή κωδικών (password manager) ή σε ασφαλή μηχανισμό διαχείρισης μυστικών, και ορίστε υπεύθυνο για την τακτική ανανέωσή τους σε κρίσιμες συσκευές.

ΔΙΑΔΙΚΑΣΙΕΣ ΑΞΙΟΛΟΓΗΣΗΣ

- Εξέταση / επισκόπηση:
  - πολιτικών ή διαδικασιών που αφορούν σε παραμετροποιήσεις ασφάλειας συστημάτων.
  - δειγματοληπτικού εύρους συσκευών (routers, access points, κ.α.) για τον έλεγχο ύπαρξης λογαριασμών με προεπιλεγμένους κωδικούς πρόσβασης.
- Διενέργεια συνέντευξης / συζήτησης με τον υπεύθυνο κυβερνοασφάλειας, καθώς και με μέλη του προσωπικού με αρμοδιότητα την παραμετροποίηση συστημάτων, εφαρμογών, υπηρεσιών και δικτύων.

4. Διαχείριση ευπαθειών

ΑΠΑΙΤΗΣΗ 4.1

Υλοποιήστε διαδικασίες εντοπισμού, αξιολόγησης και αντιμετώπισης των τεχνικών ευπαθειών στα πληροφοριακά συστήματα της επιχείρησης.

ΠΕΡΙΓΡΑΦΗ

- Οι επιτιθέμενοι συνεχώς αναζητούν ευπάθειες (vulnerabilities) σε πληροφοριακά αγαθά με σκοπό την εκμετάλλευσή τους και την επακόλουθη απόκτηση με εξουσιοδοτημένης πρόσβασης. Από την άλλη πλευρά, οι αμυνόμενοι πρέπει να λαμβάνουν έγκαιρη πληροφόρηση για νέες κυβερνοαπειλές, να έχουν πρόσβαση σε ενημερώσεις λογισμικού και ενημερώσεις ασφάλειας, καθώς και να εντοπίζουν ευπάθειες με τη χρήση κατάλληλων εργαλείων. Επιπλέον, η χρήση τεχνητής νοημοσύνης έχει επιταχύνει θεαματικά το χρόνο ανίχνευσης ευπαθειών, τόσο για τους επιτιθέμενους όσο και για τους αμυνόμενους. Για τις επιχειρήσεις, η διαχείριση ευπαθειών είναι μία συνεχής δραστηριότητα που απαιτεί οργάνωση, χρόνο, δέουσα προσοχή και πόρους.

ΟΔΗΓΙΕΣ ΥΛΟΠΟΙΗΣΗΣ

- Εντοπίστε αξιόπιστες και αναγνωρισμένες πηγές πληροφόρησης σχετικές με ευπάθειες τεχνολογιών πληροφορικής και επικοινωνιών, όπως είναι κατασκευαστές και προμηθευτές λογισμικού, ομάδες απόκρισης για περιστατικά κυβερνοασφάλειας (CSIRTs) ή αρμόδιες κρατικές Αρχές.
- Υλοποιήστε έγκαιρα τις ενημερώσεις λογισμικού (software updates) και τις ενημερώσεις ασφάλειας (security patches) σε λειτουργικά συστήματα και εφαρμογές. Για την προτεραιοποίηση της εγκατάστασης των ενημερώσεων ασφάλειας, λάβετε υπόψη σας παράγοντες κινδύνου, όπως:
  - Το ευπαθές σύστημα είναι εκτεθειμένο στο διαδίκτυο.
  - Έχει επιβεβαιωθεί από δημόσιες πηγές ότι η ευπάθεια αποτελεί αντικείμενο ενεργούς εκμετάλλευσης, π.χ. είναι εγγεγραμμένη στον δημοφιλή κατάλογο KEV (Known Exploited Vulnerabilities Catalog https://www.cisa.gov/known-exploited-vulnerabilities-catalog).
- Υλοποιήστε λήψη των ενημερώσεων λογισμικού και των ενημερώσεων ασφάλειας με αυτοματοποιημένο τρόπο, όπου αυτό είναι εφικτό (π.χ. σε λειτουργικά συστήματα Windows στους σταθμούς εργασίας χρηστών ή σε λογισμικό εφαρμογών).
- Εξετάστε, εφόσον είναι εφικτό, τη δυνατότητα πραγματοποίησης δοκιμών των ενημερώσεων και επιδιορθώσεων ασφάλειας σε απομονωμένο περιβάλλον, προτού αυτές υλοποιηθούν στο παραγωγικό περιβάλλον, όπου απαιτείται.
- Υλοποιήστε κατάλληλα αντισταθμιστικά μέτρα στις περιπτώσεις όπου η εφαρμογή των ενημερώσεων λογισμικού ή των ενημερώσεων ασφάλειας δεν είναι εφικτή, όπως ενδεικτικά απενεργοποίηση λειτουργιών ή υπηρεσιών, διαμερισματοποίηση δικτύου, καθώς και αυστηρά μέτρα ελέγχου πρόσβασης ή / και παρακολούθησης (monitoring).
- Διενεργήστε σαρώσεις ευπαθειών (vulnerability scans) στα συστήματά σας σε τακτική βάση, με τη χρήση αυτοματοποιημένων εργαλείων. Τα εν λόγω εργαλεία εμφανίζουν αποτελέσματα για: (i) μη ενημερωμένα (unpatched) συστήματα, (ii) λειτουργίες, θύρες, πρωτόκολλα ή υπηρεσίες που

δεν θα έπρεπε να είναι προσβάσιμα σε χρήστες ή συσκευές και (iii) λανθασμένες παραμετροποιήσεις (misconfigurations). Η συχνότητα των σαρώσεων πρέπει να είναι ανάλογη της κρισιμότητας των συστημάτων και του επιπέδου κινδύνου. Εξετάστε τη δυνατότητα διενέργειας σαρώσεων ευπαθειών σε μηνιαία βάση ή και νωρίτερα, ανάλογα με τις δυνατότητες της επιχείρησης. Δώστε απόλυτη προτεραιότητα στους διακομιστές και στις δικτυακές συσκευές που είναι προσβάσιμες από το διαδίκτυο. Για μικρές επιχειρήσεις, αρκούν προσιτές εμπορικές ή ανοικτού κώδικα λύσεις λογισμικού σαρώσεων.

- Αναπτύξτε πλάνο αποκατάστασης των ευπαθειών που ανακαλύπτονται κατά τη διαδικασία των σαρώσεων, ορίζοντας σαφείς ρόλους, αρμοδιότητες και ευθύνες και λαμβάνοντας υπόψη παραμέτρους όπως είναι η κρισιμότητα των ευπαθών συστημάτων και το γενικότερο περιβάλλον κινδύνου. Ενέργειες αντιμετώπισης της ευπάθειας δύνανται να είναι:
  - η πλήρης αποκατάσταση / επιδιόρθωσή της (remediation), όπως ενδεικτικά η εφαρμογή ενημέρωσης ασφάλειας (software patch) με βάση τις οδηγίες του κατασκευαστή ή η αφαίρεση / απόσυρση του ευπαθούς συστήματος.
  - ο μετριασμός των επιπτώσεών της (impact mitigation) στις περιπτώσεις όπου η αποκατάσταση δεν είναι εφικτή ή άμεση, με ενέργειες όπως ενδεικτικά την αφαίρεση προεπιλεγμένων συνθηματικών (default credentials), τη διαμερισματοποίηση του δικτύου, την αλλαγή των κανόνων του firewall, την υλοποίηση ελέγχου ταυτότητας πολλαπλών παραγόντων (MFA), την καταγραφή και παρακολούθηση συμβάντων κ.α.

ΔΙΑΔΙΚΑΣΙΕΣ ΑΞΙΟΛΟΓΗΣΗΣ

- Εξέταση / επισκόπηση:
  - διαδικασιών διαχείρισης ευπαθειών,
  - καταγραφών ή / και ιστορικού υλοποίησης ενημερώσεων λογισμικού και ενημερώσεων ασφάλειας,
  - ιστορικού υλοποίησης σαρώσεων ευπαθειών.
- Διενέργεια συνέντευξης / συζήτησης με τον υπεύθυνο κυβερνοασφάλειας, καθώς και με μέλη του προσωπικού με αρμοδιότητα τη διαχείριση των τεχνικών ευπαθειών τεχνολογιών πληροφορικής και επικοινωνιών.
- Διενέργεια δοκιμών σε μηχανισμούς ή εργαλεία υλοποίησης - εφαρμογής ενημερώσεων λογισμικού και επιδιορθώσεων ασφάλειας.

ΑΠΑΙΤΗΣΗ 4.2

Προβείτε σε απόσυρση ή αντικατάσταση των τεχνολογιών πληροφορικής και επικοινωνιών για τις οποίες έχει λήξει η υποστήριξη από τον προμηθευτή ή τον κατασκευαστή.

ΠΕΡΙΓΡΑΦΗ

- Η διακοπή υποστήριξης (“end of support”) των τεχνολογιών πληροφορικής και επικοινωνιών από τον προμηθευτή ή τον κατασκευαστή σημαίνει τη λήξη παροχής τεχνικής υποστήριξης,

ενημερώσεων λογισμικού και επιδιορθώσεων ασφάλειας. Η συνέχιση χρήσης τέτοιων προϊόντων καθιστά την επιχείρηση ιδιαίτερα ευάλωτη σε κυβερνοαπειλές.

ΟΔΗΓΙΕΣ ΥΛΟΠΟΙΗΣΗΣ

- Υλοποιήστε πλάνο σταδιακής απόσυρσης ή αντικατάστασης των μη υποστηριζόμενων λειτουργικών συστημάτων, εφαρμογών, δικτυακών συσκευών και εξοπλισμού πληροφορικής. Στις περιπτώσεις όπου η άμεση απόσυρση ή αντικατάσταση των μη υποστηριζόμενων τεχνολογιών πληροφορικής και επικοινωνιών δεν είναι εφικτή, προβείτε σε δικτυακή απομόνωσή τους με διακοπή κάθε κίνησης από και προς το διαδίκτυο.
- Σε κάθε περίπτωση συνέχισης χρήσης μη υποστηριζόμενης τεχνολογίας, τεκμηριώστε ρητή αποδοχή κινδύνου από την ανώτατη διοίκηση, με συγκεκριμένα αντισταθμιστικά μέτρα και ημερομηνία λήξης της εξαίρεσης.
- Καταγράψτε στο μητρώο πληροφοριακών αγαθών την ημερομηνία λήξης υποστήριξης κάθε κρίσιμου λειτουργικού συστήματος, εφαρμογής ή συσκευής και εντάξτε την αντικατάσταση στον ετήσιο προϋπολογισμό πληροφορικής.

ΔΙΑΔΙΚΑΣΙΕΣ ΑΞΙΟΛΟΓΗΣΗΣ

- Εξέταση / επισκόπηση:
  - ύπαρξης μη υποστηριζόμενων τεχνολογιών πληροφορικής και επικοινωνιών,
  - τεκμηριωμένων στοιχείων απόσυρσης ή αντικατάστασής τους,
  - τεκμηριωμένων αποφάσεων της ανώτατης διοίκησης για περιπτώσεις παρατεταμένης χρήσης μη υποστηριζόμενων τεχνολογιών, με περιγραφή αντισταθμιστικών μέτρων.
- Διενέργεια συνέντευξης / συζήτησης με τον υπεύθυνο κυβερνοασφάλειας, καθώς και με μέλη του προσωπικού με αρμοδιότητα τη διαχείριση των πληροφοριακών αγαθών.

5. Διαχείριση ταυτότητας και έλεγχος πρόσβασης

ΑΠΑΙΤΗΣΗ 5.1

Διαχειριστείτε με ασφάλεια τον πλήρη κύκλο ζωής των λογαριασμών χρηστών στα πληροφοριακά σας συστήματα.

ΠΕΡΙΓΡΑΦΗ

- Οι ψηφιακές ταυτότητες χρηστών κατηγοριοποιούνται σε ανθρώπινες ταυτότητες (human identities) και μη-ανθρώπινες ταυτότητες (non-human identities). Στην πρώτη κατηγορία ανήκουν οι λογαριασμοί προσώπων που αλληλεπιδρούν με τα συστήματα μίας επιχείρησης (εργαζόμενοι, προμηθευτές και πάροχοι υπηρεσιών, άλλοι συνεργάτες). Στη δεύτερη κατηγορία ανήκουν οι λογαριασμοί που χορηγούνται σε συσκευές, εφαρμογές λογισμικού, υπηρεσίες (service accounts), καθώς και σε πράκτορες τεχνητής νοημοσύνης (AI agents).

ΟΔΗΓΙΕΣ ΥΛΟΠΟΙΗΣΗΣ

- Χορηγήστε μοναδική ταυτότητα σε κάθε χρήστη που αποκτά λογαριασμό στην επιχείρηση, με σκοπό τη διασφάλιση λογοδοσίας για ενέργειες που εκτελούνται με τη συγκεκριμένη ταυτότητα. Οι ταυτότητες που χορηγούνται σε πολλαπλά πρόσωπα (shared identities) επιτρέπονται μόνο όταν είναι απαραίτητες για τις επιχειρηματικές σας ανάγκες και πρέπει να υπόκεινται σε ειδική έγκριση και τεκμηρίωση.
- Δημιουργήστε και τηρείτε μητρώο με το σύνολο των λογαριασμών χρηστών που διαχειρίζεται η επιχείρηση. Κατ' ελάχιστο, το μητρώο θα πρέπει να περιλαμβάνει το ονοματεπώνυμο, το όνομα χρήστη (username), τις ημερομηνίες έναρξης / λήξης και την οργανική μονάδα. Περιοδικά, επιβεβαιώστε ότι όλοι οι ενεργοί λογαριασμοί είναι εξουσιοδοτημένοι (authorized).
- Επιβάλλετε μοναδικούς και ισχυρούς κωδικούς πρόσβασης για το σύνολο των λογαριασμών χρηστών.
- Διαγράψτε ή απενεργοποιήστε λογαριασμούς χρηστών που παραμένουν αδρανείς για μία προκαθορισμένη χρονική περίοδο, π.χ. 2 μήνες.
- Ορίστε υποχρεωτική ημερομηνία αυτόματης λήξης (account expiration) για τους λογαριασμούς εξωτερικών συνεργατών, προμηθευτών και εποχικού προσωπικού. Παρατάσεις δίνονται μόνο κατόπιν ρητής έγκρισης από τον επιχειρησιακό υπεύθυνο.
- Διενεργήστε περιοδική πιστοποίηση ενεργών λογαριασμών (access certification): τουλάχιστον δύο φορές ετησίως ο επικεφαλής κάθε τμήματος ή ο ιδιοκτήτης κάθε εφαρμογής επιβεβαιώνει εγγράφως ότι οι ενεργοί λογαριασμοί παραμένουν αναγκαίοι.
- Εφαρμόστε τη δέουσα προσοχή στη διαχείριση και εποπτεία των μη-ανθρώπινων ταυτοτήτων, όσον αφορά στο εύρος των λειτουργιών και των προνομίων τους.

ΔΙΑΔΙΚΑΣΙΕΣ ΑΞΙΟΛΟΓΗΣΗΣ

- Εξέταση / επισκόπηση: α) πολιτικών και διαδικασιών που αφορούν στη διαχείριση λογαριασμών χρηστών, β) μητρώου λογαριασμών χρηστών.

- Διενέργεια συνέντευξης / συζήτησης με τον υπεύθυνο κυβερνοασφάλειας, καθώς και με μέλη του προσωπικού με αρμοδιότητα τη διαχείριση των λογαριασμών χρηστών.
- Διενέργεια δοκιμών σε μηχανισμούς ή εφαρμογές λογισμικού που εκτελούν και επιβάλλουν διαδικασίες διαχείρισης λογαριασμών χρηστών και ελέγχου πρόσβασης.

ΑΠΑΙΤΗΣΗ 5.2

Υλοποιήστε κανόνες για τον έλεγχο της πρόσβασης στα πληροφοριακά σας συστήματα, με βάση τις επιχειρηματικές σας ανάγκες και τις απαιτήσεις ασφάλειας πληροφοριών.

ΠΕΡΙΓΡΑΦΗ

- Οι διαδικασίες ελέγχου πρόσβασης είναι ιδιαίτερα κρίσιμες για τις επιχειρήσεις. Αβλεψίες και λανθασμένες παραμετροποιήσεις στο πεδίο αυτό αποτελούν πολύ συχνή αιτία περιστατικών. Η πρόσβαση πρέπει να χορηγείται μόνο όταν υπάρχει επιχειρησιακή ανάγκη, να αναθεωρείται περιοδικά και να αφαιρείται άμεσα όταν αλλάζει ο ρόλος ή λήγει η συνεργασία του χρήστη.
- Οι λογαριασμοί με αυξημένα προνόμια πρέπει να αντιμετωπίζονται ως αγαθά υψηλού κινδύνου και να προστατεύονται με ισχυρότερη αυθεντικοποίηση, ξεχωριστή χρήση και αυξημένη παρακολούθηση.

ΟΔΗΓΙΕΣ ΥΛΟΠΟΙΗΣΗΣ

- Εφαρμόστε την αρχή της ανάγκης γνώσης (need to know): σε έναν χρήστη χορηγείται πρόσβαση μόνο στις πληροφορίες που ο χρήστης χρειάζεται για την εκτέλεση των καθηκόντων του.
- Εφαρμόστε την αρχή των ελάχιστων προνομίων (least privilege): περιορίστε τα προνομιακά δικαιώματα πρόσβασης (π.χ. διαχειριστικά δικαιώματα) αποκλειστικά στους χρήστες που είναι απαραίτητο λόγω των καθηκόντων τους.
- Διασφαλίστε ότι στους χρήστες που εκτελούν αποκλειστικά δραστηριότητες που δεν απαιτούν διαχειριστικό ρόλο και αφορούν καθημερινές εργασίες γενικής φύσης (π.χ. χρήση προγραμμάτων γραφείου, ανάγνωση και αποστολή email, περιήγηση στο διαδίκτυο κ.α.) χορηγείται αποκλειστικά μη προνομιακός λογαριασμός (non-privileged account).
- Διασφαλίστε ότι οι προνομιακοί λογαριασμοί (π.χ. διαχειριστικοί λογαριασμοί) χρησιμοποιούνται αποκλειστικά για καθήκοντα που απαιτούν προνομιακή πρόσβαση. Για τους χρήστες που, λόγω καθηκόντων, διαθέτουν προνομιακούς λογαριασμούς, χορηγήστε δεύτερο μη προνομιακό λογαριασμό για την εκτέλεση καθημερινών εργασιών γενικής φύσης (π.χ. χρήση προγραμμάτων γραφείου, ανάγνωση και αποστολή email, περιήγηση στο διαδίκτυο κ.α.).
- Επιβάλλετε κλείδωμα λογαριασμών χρηστών μετά από συγκεκριμένο αριθμό ανεπιτυχών προσπαθειών εισόδου και για προκαθορισμένο χρονικό διάστημα. Το μέτρο αφορά ιδίως στην αντιμετώπιση των διαφόρων τύπων επιθέσεων brute-force, όπως είναι το credential stuffing, η λεξικογραφική επίθεση (dictionary attack), το password spraying και η επίθεση rainbow table.
- Επιβάλλετε αυτόματο κλείδωμα οθόνης μετά από σύντομη περίοδο αδράνειας (π.χ. 15 λεπτά) και απαιτείστε ισχυρό κωδικό για ξεκλείδωμα.

- Επιβάλλετε αυτόματο τερματισμό συνεδρίας (session timeout) μετά από εύλογο διάστημα αδράνειας, ιδίως σε εφαρμογές νεφοϋπολογιστικής και σε διαχειριστικές διεπαφές (administrative interfaces).
- Όπου είναι διαθέσιμη, εφαρμόστε πολιτική πρόσβασης υπό όρους (conditional access): απαγόρευση συνδέσεων από μη αναμενόμενες γεωγραφικές περιοχές, υψηλού κινδύνου δίκτυα ή μη συμβατές συσκευές. Στις πιο διαδεδομένες σουίτες παραγωγικότητας οι σχετικές δυνατότητες είναι ενσωματωμένες.
- Επιβάλλετε ελάχιστο μήκος κωδικών πρόσβασης (passwords) τουλάχιστον 14 χαρακτήρων για τους λογαριασμούς που δεν υλοποιούν MFA. Εφαρμόστε ισχυρά συνθηματικά, διασφαλίζοντας ότι οι κωδικοί πρόσβασης δεν αποτελούνται από λέξεις που υπάρχουν σε λεξικά ή συνδυασμούς τους, καθώς και ήδη παραβιασμένους κωδικούς. Εξετάστε την περίπτωση χρήσης passphrases και password managers, έτσι ώστε να είναι ευκολότερο για τους χρήστες να τηρούν ισχυρά συνθηματικά.

ΔΙΑΔΙΚΑΣΙΕΣ ΑΞΙΟΛΟΓΗΣΗΣ

- Εξέταση / επισκόπηση:
  - πολιτικών και διαδικασιών που αφορούν στη διαχείριση λογαριασμών χρηστών και στον έλεγχο πρόσβασης,
  - δειγματοληπτικού εύρους λογαριασμών χρηστών με καθήκοντα γενικής φύσης για επιβεβαίωση ότι δεν διαθέτουν διαχειριστικά δικαιώματα στις τερματικές συσκευές τους.
- Διενέργεια συνέντευξης / συζήτησης με τον υπεύθυνο κυβερνοασφάλειας, καθώς και με μέλη του προσωπικού με αρμοδιότητα τη διαχείριση των λογαριασμών χρηστών και τον έλεγχο πρόσβασης.
- Διενέργεια δοκιμών σε μηχανισμούς ή εφαρμογές λογισμικού που υλοποιούν λειτουργίες αυθεντικοποίησης, καθώς και χορήγησης δικαιωμάτων πρόσβασης.

ΑΠΑΙΤΗΣΗ 5.3

Υλοποιήστε έλεγχο ταυτότητας πολλαπλών παραγόντων (multi-factor authentication-MFA), όπου απαιτείται με βάση την κρισιμότητα των συστημάτων και των δεδομένων σας.

ΠΕΡΙΓΡΑΦΗ

- Η αυθεντικοποίηση πολλαπλών παραγόντων (multi-factor authentication – MFA), ή έλεγχος ταυτότητας πολλαπλών παραγόντων, απαιτεί τη χρήση δύο ή περισσότερων διαφορετικών παραγόντων για την επίτευξη της αυθεντικοποίησης. Οι εν λόγω παράγοντες είναι:
  - κάτι που ο χρήστης γνωρίζει (π.χ. ένα password ή ένα PIN),
  - κάτι που ο χρήστης έχει (π.χ. ένα smartphone ή μία έξυπνη κάρτα) και
  - κάτι που ο χρήστης «είναι» (βιομετρικά χαρακτηριστικά, όπως π.χ. το δακτυλικό αποτύπωμα ή η αναγνώριση προσώπου).
- Τα είδη του MFA κατά σειρά ισχύος, από το πιο αδύναμο έως το πιο ισχυρό, έχουν ως εξής:

- SMS-based: αποστέλλεται ένας κωδικός στο τηλέφωνο ή στο email του χρήστη. Η εν λόγω διαδικασία, αν και υπερτερεί έναντι της απλής εισαγωγής κωδικού πρόσβασης, εμφανίζει αυξανόμενες αδυναμίες λόγω των επιθέσεων ανταλλαγής κάρτας SIM (SIM swap) και υποκλοπών μηνυμάτων.
- App-based: αποστέλλεται ένας κωδικός (one-time password) ή και ειδοποιήσεις (push notifications) σε εφαρμογή αυθεντικοποίησης στο smartphone του χρήστη.
- Phishing-resistant MFA: υλοποιούνται κρυπτογραφικά πρωτόκολλα (FIDO/WebAuthn, PKI) που ταυτοποιούν την ίδια τη συσκευή του χρήστη σε ένα domain.

ΟΔΗΓΙΕΣ ΥΛΟΠΟΙΗΣΗΣ

- Εφαρμόστε MFA σε όλους τους λογαριασμούς χρηστών που είναι προσβάσιμοι από το διαδίκτυο (email, VPN, RDP, υπηρεσίες cloud, web portals).
- Εφαρμόστε MFA σε όλους τους διαχειριστικούς λογαριασμούς.
- Εφαρμόστε MFA για την απομακρυσμένη δικτυακή πρόσβαση (remote network access).
- Εντοπίστε εφαρμογές παλαιού τύπου που δεν υποστηρίζουν MFA και εφαρμόστε αντισταθμιστικά μέτρα: τοποθέτηση πίσω από VPN με υποχρεωτικό MFA, περιορισμός πρόσβασης μέσω λίστας επιτρεπόμενων IP διευθύνσεων, αυξημένη παρακολούθηση συνδέσεων και ανάπτυξη πλάνου αντικατάστασης της εφαρμογής.
- Για διαχειριστικούς λογαριασμούς και κρίσιμες cloud υπηρεσίες, προτιμήστε phishing-resistant MFA, όπου είναι διαθέσιμο, ιδίως με χρήση FIDO2/WebAuthn security keys ή ισοδύναμων μηχανισμών.

ΔΙΑΔΙΚΑΣΙΕΣ ΑΞΙΟΛΟΓΗΣΗΣ

- Εξέταση / επισκόπηση:
  - πολιτικών, διαδικασιών και παραμετροποιήσεων (configurations) που αφορούν στην υλοποίηση ελέγχου ταυτότητας πολλαπλών παραγόντων,
  - διαχειριστικών λογαριασμών και λογαριασμών με πρόσβαση από το διαδίκτυο για επιβεβαίωση της ενεργοποίησης MFA,
  - δειγματοληπτικού εύρους εφαρμογών παλαιού τύπου χωρίς MFA για επιβεβαίωση εφαρμογής τεκμηριωμένων αντισταθμιστικών μέτρων.
- Διενέργεια συνέντευξης / συζήτησης με τον υπεύθυνο κυβερνοασφάλειας, καθώς και με μέλη του προσωπικού με αρμοδιότητα τη διαχείριση των λογαριασμών χρηστών και τον έλεγχο πρόσβασης.
- Διενέργεια δοκιμών σε μηχανισμούς ή εφαρμογές λογισμικού που υλοποιούν λειτουργίες ελέγχου ταυτότητας πολλαπλών παραγόντων.

6. Ασφάλεια δικτύων

ΑΠΑΙΤΗΣΗ 6.1

Υλοποιήστε διαδικασίες και τεχνολογίες προστασίας των δικτύων σας από μη εξουσιοδοτημένη πρόσβαση.

ΠΕΡΙΓΡΑΦΗ

- Η ασφαλής αρχιτεκτονική των δικτυακών συσκευών (firewalls, routers, switches, gateways, wireless access points) είναι κρίσιμης σημασίας για την άμυνα εναντίον των κυβερνοαπειλών και την προστασία των πόρων εντός του δικτύου της επιχείρησης. Όλα τα σύγχρονα δίκτυα διατρέχουν τον κίνδυνο παραβίασης, ιδίως εάν οι συσκευές δεν διαθέτουν σωστές παραμετροποιήσεις και δεν συντηρούνται κατάλληλα. Οι πολιτικές ασφάλειας δικτύων συνεχώς εξελίσσονται, καθώς οι επιτιθέμενοι εκμεταλλεύονται νέες ευπάθειες, ενώ παράλληλα νέες μέθοδοι προστασίας των συσκευών αναπτύσσονται. Επιπλέον, μία βασική παράμετρος της ασφάλειας είναι και η υλοποίηση τεχνολογιών συνεχούς παρακολούθησης (continuous monitoring) των δικτύων, που επιτρέπουν την ανίχνευση ύποπτων συμβάντων και την αποστολή ειδοποιήσεων (alerts) στους διαχειριστές, με σκοπό την έγκαιρη απόκριση σε περιστατικά κυβερνοασφάλειας.

ΟΔΗΓΙΕΣ ΥΛΟΠΟΙΗΣΗΣ

- Αναπτύξτε αναλυτικά διαγράμματα που περιγράφουν την τοπολογία του δικτύου σας. Τα διαγράμματα θα περιλαμβάνουν την περιγραφή συστημάτων και ροών δεδομένων εντός των δικτύων σας, το σχήμα διευθυνσιοδότησης (IP addressing scheme), τις δικτυακές συνδέσεις, τις αλληλεξαρτήσεις, καθώς και τις προσβάσεις που παρέχονται σε τρίτα μέρη, σε παρόχους διαχειριζόμενων υπηρεσιών (MSPs) και σε cloud συνδέσεις από εξωτερικά και εσωτερικά τερματικά.
- Υλοποιείστε τείχος προστασίας (firewall) στην εξωτερική περίμετρο μεταξύ του δικτύου σας και του διαδικτύου (Internet). Για την παραμετροποίησή του, εφαρμόστε την προσέγγιση “deny-by-default, permit-by-exception”, υλοποιώντας κανόνες που επιτρέπουν ρητά μόνο τις συνδέσεις που απαιτούνται για την υποστήριξη της αποστολής της επιχείρησής σας.
- Αλλάξτε τους προεπιλεγμένους διαχειριστικούς κωδικούς πρόσβασης (default administrative passwords) κατά την αρχική εγκατάσταση του firewall. Οι νέοι κωδικοί πρέπει να είναι ισχυροί και μοναδικοί για κάθε συσκευή.
- Αποτρέψτε την πρόσβαση από το διαδίκτυο στο διαχειριστικό περιβάλλον του firewall. Εφόσον υπάρχει τεκμηριωμένη επιχειρηματική ανάγκη για το αντίθετο, διασφαλίστε την εφαρμογή MFA, τον περιορισμό της πρόσβασης από συγκεκριμένες IP διευθύνσεις και την υλοποίηση ισχυρών κωδικών πρόσβασης.
- Υλοποιείστε διαμερισματοποίηση του δικτύου σας (network segmentation) σε διακριτά υποδίκτυα με βάση τα επίπεδα κρισιμότητας των συστημάτων σας. Υλοποιήστε το διαχωρισμό είτε μέσω VLANs (virtual local area networks) είτε μέσω φυσικού διαχωρισμού με χρήση firewalls ή filtering routers. Διασφαλίστε ότι συστήματα με παρόμοια κατηγοριοποίηση ασφάλειας είναι τοποθετημένα στο ίδιο υποδίκτυο. Ιδιαίτερη προσοχή θα πρέπει να δοθεί στις διεπαφές

διαχείρισης των δικτυακών συσκευών της επιχείρησης, όπου προτείνεται να πραγματοποιείται μέσω διακριτού δικτύου διαχείρισης (management VLAN).

- Υλοποιείστε φιλτράρισμα της δικτυακής κίνησης (traffic filtering) μεταξύ των υποδικτύων, με σκοπό να περιορίσετε τη ροή της πληροφορίας στην απολύτως απαραίτητη για τις ανάγκες της επιχείρησης.
- Διασφαλίστε ότι εφόσον διαθέτετε συστήματα που είναι προσβάσιμα από το διαδίκτυο (π.χ. υπηρεσίες όπως web, mail, VPN, κ.α.), τότε αυτά βρίσκονται σε υποδίκτυα που είναι με φυσικό ή λογικό τρόπο διαχωρισμένα από το εσωτερικό σας δίκτυο. Η εν λόγω αρχιτεκτονική ονομάζεται "αποστρατικοποιημένη ζώνη" (demilitarized zone – DMZ).
- Υλοποιείστε τείχος προστασίας σε μορφή λογισμικού (software firewall) σε διακομιστές και υπολογιστές χρηστών, για τον έλεγχο των εισερχόμενων και εξερχόμενων δικτυακών συνδέσεων σε επίπεδο τελικής συσκευής.
- Υλοποιείστε σύστημα ανίχνευσης εισβολών σε επίπεδο δικτύου (network intrusion detection system – IDS). Το IDS αποτελεί τεχνολογία κυβερνοασφάλειας που παρακολουθεί συνεχώς τη δικτυακή κίνηση και αποστέλλει ειδοποιήσεις (alerts) όταν ανιχνεύσει ύποπτες δραστηριότητες. Αξιοποιήστε εμπορικά προϊόντα ή λύσεις λογισμικού ανοικτού κώδικα, ανάλογα με τις δυνατότητές σας και τη διαχείριση κινδύνου, λαμβάνοντας υπόψη και τις απαιτήσεις σε πόρους που συνεπάγεται η εγκατάσταση, παραμετροποίηση και συντήρησή τους. Για μικρές επιχειρήσεις, εξετάστε, εναλλακτικά, τη σύναψη υπηρεσίας Managed Detection and Response (MDR) με αξιόπιστο πάροχο υπηρεσιών ασφάλειας για το σκοπό αυτό.
- Διαμορφώστε ξεχωριστό ασύρματο δίκτυο επισκεπτών (guest Wi-Fi) απομονωμένο από το εσωτερικό ασύρματο & ενσύρματο δίκτυο της επιχείρησης, ώστε επισκέπτες, πελάτες ή προσωπικές συσκευές εργαζομένων να μην έχουν πρόσβαση στους πόρους και τα δεδομένα της επιχείρησης. Όσον αφορά στον κωδικό του ασύρματου δικτύου, προτείνεται η περιοδική αλλαγή αυτού, αλλά και μετά από σημαντική εκδήλωση ή φιλοξενία τρίτων, ώστε να μην παραμένει σε γνώση προσώπων που δεν βρίσκονται πλέον στις εγκαταστάσεις της επιχείρησης.
- Ασφαλίστε το ασύρματο δίκτυο της επιχείρησης με ισχυρή σύγχρονη κρυπτογράφηση (WPA2-Enterprise ή WPA3), αλλάξτε τα προεπιλεγμένα διαπιστευτήρια του δρομολογητή και κρύψτε ή αλλάξτε το προεπιλεγμένο SSID που αποκαλύπτει τον κατασκευαστή της συσκευής.
- Επιβάλλετε στους εργαζόμενους τη χρήση εικονικού ιδιωτικού δικτύου (VPN) όταν συνδέονται σε εταιρικούς πόρους από μη έμπιστα δίκτυα (π.χ. δημόσια Wi-Fi σε αεροδρόμια, ξενοδοχεία κ.λπ.). Αποφύγετε τη χρήση δημόσιων δικτύων Wi-Fi για δραστηριότητες διαχείρισης συστημάτων ή για πρόσβαση σε ευαίσθητα δεδομένα.
- Εφαρμόστε προστατευτική υπηρεσία DNS (protective / sinkhole DNS) σε επίπεδο επιχείρησης. Το protective DNS αναλύει τα DNS queries και εμποδίζει τους χρήστες να συνδεθούν σε γνωστά κακόβουλα domains (command-and-control, phishing κ.α.). Το sinkhole DNS είναι μία τεχνική που ανακατευθύνει αιτήματα για γνωστά κακόβουλα domains σε ελεγχόμενες από την επιχείρηση IP διευθύνσεις. Λύσεις του τύπου αυτού προσφέρονται από δημόσιους και εμπορικούς παρόχους και αποτελούν ένα από τα πλέον αποδοτικά μέτρα χαμηλού κόστους.
- Δημιουργήστε ξεχωριστό υποδίκτυο (VLAN) για συσκευές IoT και επιχειρησιακής τεχνολογίας (κάμερες, εκτυπωτές, smart TVs, θερμοστάτες, αισθητήρες), απομονωμένο από το δίκτυο των σταθμών εργασίας και των διακομιστών. Οι περισσότερες IoT συσκευές δεν λαμβάνουν τακτικές ενημερώσεις ασφάλειας και αποτελούν συχνό σημείο εισόδου σε εταιρικά δίκτυα.

ΔΙΑΔΙΚΑΣΙΕΣ ΑΞΙΟΛΟΓΗΣΗΣ

- Εξέταση / επισκόπηση / παρατήρηση:
  - εγκατάστασης τεχνολογιών firewalls (σε υλικό και λογισμικό),
  - πολιτικών, διαδικασιών και παραμετροποιήσεων (configurations) που αφορούν στη διαχείριση δικτύων,
  - διαγραμμάτων δικτύου,
  - καταγραφών (logs) από δικτυακές συσκευές.
- Διενέργεια συνέντευξης / συζήτησης με τον υπεύθυνο κυβερνοασφάλειας, καθώς και με διαχειριστές δικτύων και συστημάτων.
- Διενέργεια δοκιμών σε μηχανισμούς και τεχνολογίες που υλοποιούν λειτουργίες και παραμετροποιήσεις δικτυακών συσκευών.

7. Προστασία από κακόβουλο λογισμικό

ΑΠΑΙΤΗΣΗ 7.1

Εγκαταστήστε λογισμικό ανίχνευσης και προστασίας από κακόβουλο λογισμικό (anti-malware software).

ΠΕΡΙΓΡΑΦΗ

- Το κακόβουλο λογισμικό έχει τη μορφή είτε ολοκληρωμένου εκτελέσιμου αρχείου είτε συνόλου εντολών και έχει σκοπό την πρόκληση κακόβουλων ενεργειών σε συστήματα. Πιθανές πηγές του περιλαμβάνουν: το άνοιγμα κακόβουλων συνημμένων αρχείων μέσω ηλεκτρονικού ταχυδρομείου, η λήψη (download) μολυσμένων αρχείων και εφαρμογών από το διαδίκτυο, καθώς και τα μολυσμένα φορητά μέσα αποθήκευσης (USB).
- Το λογισμικό προστασίας από κακόβουλο λογισμικό (anti-malware ή πιο γνωστό ως antivirus) ανιχνεύει, θέτει σε καραντίνα ή / και απομακρύνει κακόβουλο λογισμικό χρησιμοποιώντας ένα συνδυασμό ανίχνευσης με βάση υπογραφές (signatures), ανάλυσης συμπεριφοράς (behavioral analysis) και παρακολούθησης σε πραγματικό χρόνο (real-time monitoring).

ΟΔΗΓΙΕΣ ΥΛΟΠΟΙΗΣΗΣ

- Διασφαλίστε ότι το λογισμικό antivirus εγκαθίσταται σε όλους τους διακομιστές (web, mail, proxy, κ.α.) και σε όλους τους υπολογιστές χρηστών (desktops και laptops).
- Διασφαλίστε ότι το λογισμικό antivirus λειτουργεί μέσω κεντρικής διαχείρισης.
- Παραμετροποιήστε το λογισμικό antivirus ώστε η ενημέρωση των νέων υπογραφών (detection signatures) να διενεργείται αυτοματοποιημένα σε καθημερινή βάση.
- Παραμετροποιήστε το λογισμικό antivirus να διενεργεί περιοδικές σαρώσεις (scans) του συστήματος, καθώς και σαρώσεις σε πραγματικό χρόνο αρχείων που προέρχονται από εξωτερικές πηγές κατά τη λήψη, άνοιγμα ή εκτέλεσή τους.
- Εξετάστε τη δυνατότητα αναβάθμισης από κλασικό antivirus σε λύση EDR (Endpoint Detection and Response) ή MDR (Managed Detection and Response), με σκοπό τη βελτίωση της ασφάλειας των πληροφοριακών συστημάτων της επιχείρησης. Οι λύσεις αυτές παρέχουν ανίχνευση βάσει συμπεριφοράς, καταγραφή τηλεμετρίας τερματικών, αυτόματο περιορισμό συμβάντων και, ειδικά στην περίπτωση του MDR, υποστήριξη από εξωτερική ομάδα ανάλυσης σε 24ωρη βάση, καλύπτοντας κυβερνοαπειλές που παρακάμπτουν τα παραδοσιακά antivirus (όπως ενδεικτικά fileless malware, living-off-the-land techniques).

ΔΙΑΔΙΚΑΣΙΕΣ ΑΞΙΟΛΟΓΗΣΗΣ

- Εξέταση / επισκόπηση / παρατήρηση:
  - εγκατάστασης τεχνολογιών προστασίας από κακόβουλο λογισμικό και επιβεβαίωση ότι όλες οι ενεργές κατηγορίες τερματικών συσκευών (όπως Windows, macOS, Linux, εικονικές μηχανές σε περιβάλλοντα νεφοϋπολογιστικής) καλύπτονται από λύση antivirus ή EDR.

- πολιτικών, διαδικασιών και παραμετροποιήσεων (configurations) που αφορούν στις τεχνολογίες προστασίας από κακόβουλο λογισμικό.

- Διενέργεια συνέντευξης / συζήτησης με διαχειριστές δικτύων και συστημάτων.
- Διενέργεια δοκιμών σε μηχανισμούς και τεχνολογίες που υλοποιούν λειτουργίες και παραμετροποιήσεις τεχνολογιών προστασίας από κακόβουλο λογισμικό.

ΑΠΑΙΤΗΣΗ 7.2

Υλοποιήστε μηχανισμούς ελέγχου εκτέλεσης εφαρμογών (application control).

ΠΕΡΙΓΡΑΦΗ

- Ο έλεγχος εκτέλεσης εφαρμογών (application control) είναι μία ιδιαίτερα αποτελεσματική μέθοδος όχι μόνο για την αποτροπή εκτέλεσης κακόβουλου λογισμικού σε διακομιστές και υπολογιστές χρηστών, αλλά και για τη διασφάλιση της εκτέλεσης μόνο εγκεκριμένων εφαρμογών στο περιβάλλον μίας επιχείρησης.
- Ο έλεγχος εκτέλεσης εφαρμογών εφαρμόζεται με δύο τρόπους:
  - Application blocklist: δημιουργείται ένας κατάλογος με όλες τις δυνατές μη εξουσιοδοτημένες εφαρμογές, η εκτέλεση των οποίων αποτρέπεται.
  - Application allowlist: αποτελεσματικότερη μέθοδος, κατά την οποία δημιουργείται ένας κατάλογος με τους εξουσιοδοτημένους τύπους λογισμικού και αποτρέπεται η εκτέλεση όλων των υπολοίπων.

ΟΔΗΓΙΕΣ ΥΛΟΠΟΙΗΣΗΣ

- Υλοποιήστε έλεγχο εκτέλεσης εφαρμογών σε όλους τους διακομιστές (web, mail, proxy, κ.α.) και σε όλους τους υπολογιστές χρηστών (desktops και laptops). Στο πλαίσιο αυτό, καθορίστε, με βάση τις επιχειρηματικές σας απαιτήσεις, τα είδη των εφαρμογών, όπως π.χ. εκτελέσιμα αρχεία (π.χ. .exe και .com), βιβλιοθήκες λογισμικού (π.χ. .dll αρχεία), scripts (π.χ. .ps1, .bat και .cmd), οδηγούς συσκευών (drivers) κ.α., που επιτρέπετε να εκτελούνται στα συστήματά σας.
- Για επιχειρήσεις χωρίς εξειδικευμένη ομάδα ασφάλειας, αξιοποιήστε ενσωματωμένα εργαλεία ελέγχου εκτέλεσης: Windows Defender Application Control (WDAC) ή AppLocker σε Windows, Smart App Control σε νεότερες εκδόσεις Windows 11, Gatekeeper και Notarization σε macOS. Πρόκειται για λύσεις χωρίς πρόσθετο κόστος.
- Διασφαλίστε ότι οι χρήστες με μη προνομιακά δικαιώματα δεν μπορούν να απενεργοποιήσουν ή να παρακάμψουν τους μηχανισμούς ελέγχου εκτέλεσης εφαρμογών.

ΔΙΑΔΙΚΑΣΙΕΣ ΑΞΙΟΛΟΓΗΣΗΣ

- Εξέταση / επισκόπηση πολιτικών, διαδικασιών και παραμετροποιήσεων (configurations) που αφορούν στον έλεγχο εκτέλεσης εφαρμογών.
- Διενέργεια συνέντευξης / συζήτησης με διαχειριστές δικτύων και συστημάτων.
- Διενέργεια δοκιμών σε τεχνολογίες και μηχανισμούς που παραμετροποιούν και περιορίζουν την εκτέλεση λογισμικού.

ΑΠΑΙΤΗΣΗ 7.3

Υλοποιήστε μηχανισμούς και τεχνολογίες προστασίας του ηλεκτρονικού ταχυδρομείου και των εφαρμογών περιήγησης στο διαδίκτυο.

ΠΕΡΙΓΡΑΦΗ

- Το email και το web αποτελούν τα δύο βασικά μέσα με τα οποία οι χρήστες μίας επιχείρησης αλληλεπιδρούν με εξωτερικούς χρήστες και περιβάλλοντα. Για το λόγο αυτό, αποτελούν κύριους στόχους για επιθέσεις τόσο μέσω κακόβουλου λογισμικού όσο και μέσω κοινωνικής μηχανικής.

ΟΔΗΓΙΕΣ ΥΛΟΠΟΙΗΣΗΣ

- Εφαρμόστε φίλτρα που ανιχνεύουν emails με γνωστούς κακόβουλους δείκτες, όπως γνωστές λέξεις-κλειδιά που συναντώνται σε phishing emails (known malicious subject lines) και μπλοκάρετε στο firewall τις ύποπτες IP διευθύνσεις.
- Εφαρμόστε φίλτρα που ελέγχουν τα επισυναπτόμενα αρχεία των emails, με σκοπό τον περιορισμό τύπων αρχείων που συνήθως περιέχουν κακόβουλο λογισμικό.
- Εφαρμόστε τις παρακάτω παραμετροποιήσεις στην email υποδομή σας:
  - Ενεργοποιήστε το STARTTLS.
  - Ενεργοποιήστε τα Sender Policy Framework (SPF) και Domain Keys Identified Mail (DKIM).
  - Ενεργοποιήστε την πολιτική Domain-based Message Authentication, Reporting and Conformance (DMARC) και ρυθμίστε τη στην επιλογή “reject”.
- Διασφαλίστε ότι στην υποδομή σας χρησιμοποιούνται μόνο οι πλέον πρόσφατες και υποστηριζόμενες εκδόσεις προγραμμάτων περιήγησης στο διαδίκτυο (web browsers) και εφαρμογών ηλεκτρονικού ταχυδρομείου (email clients).
- Περιορίστε τα πρόσθετα (add-ons), τις επεκτάσεις (extensions) και τα plug-ins στα προγράμματα περιήγησης στο διαδίκτυο με βάση τις επιχειρηματικές σας ανάγκες.
- Υλοποιήστε μηχανισμούς και τεχνολογίες φιλτραρίσματος ιστοσελίδων (web filtering), με σκοπό τον περιορισμό πρόσβασης των χρηστών σας σε μη εξουσιοδοτημένο ή κακόβουλο περιεχόμενο. Το εν λόγω μέτρο μπορεί να εφαρμοστεί με διάφορους τρόπους, όπως:
  - DNS filtering: εμποδίζεται η πρόσβαση σε συγκριμένα domain names, με βάση γνωστές block lists ή την πολιτική της επιχείρησης,
  - URL filtering: εμποδίζεται η πρόσβαση σε συγκεκριμένες ιστοσελίδες,
  - Content filtering: εμποδίζεται η πρόσβαση με βάση την κατηγορία του περιεχομένου.
- Ενεργοποιήστε ορατή σήμανση εξωτερικών μηνυμάτων ηλεκτρονικού ταχυδρομείου (“external email banner”), ώστε οι χρήστες να αναγνωρίζουν ευκολότερα μηνύματα που προέρχονται εκτός της επιχείρησης.
- Εξετάστε τη δυνατότητα μετάπτωσης των λογαριασμών ηλεκτρονικού ταχυδρομείου σε αξιόπιστες υπηρεσίες υπολογιστικού νέφους, ειδικά στην περίπτωση αδυναμίας συντήρησης και υποστήριξης με τακτικές ενημερώσεις ασφάλειας, λόγω έλλειψης πόρων .

- Εξετάστε την υλοποίηση εργαλείου αναφοράς ύποπτων μηνυμάτων («Report Phishing» button) στο εταιρικό email, ώστε οι χρήστες να μπορούν να αναφέρουν phishing μηνύματα με ένα κλικ. Αναφορές που υποβάλλονται από χρήστες αποτελούν, διεθνώς, μία από τις πιο γρήγορες πηγές ανίχνευσης στοχευμένων εκστρατειών κοινωνικής μηχανικής.

ΔΙΑΔΙΚΑΣΙΕΣ ΑΞΙΟΛΟΓΗΣΗΣ

- Εξέταση / επισκόπηση:
  - πολιτικών, διαδικασιών και παραμετροποιήσεων (configurations) μηχανισμών προστασίας και φιλτραρίσματος για το ηλεκτρονικό ταχυδρομείο και την περιήγηση στο διαδίκτυο,
  - καταγραφών (logs) από τεχνολογίες φιλτραρίσματος email και web.
- Διενέργεια συνέντευξης / συζήτησης με διαχειριστές δικτύων και συστημάτων.
- Διενέργεια δοκιμών σε τεχνολογίες και μηχανισμούς προστασίας και φιλτραρίσματος για το ηλεκτρονικό ταχυδρομείο και την περιήγηση στο διαδίκτυο.

8. Εκπαίδευση και ευαισθητοποίηση σε θέματα κυβερνοασφάλειας

ΑΠΑΙΤΗΣΗ 8.1

Διενεργήστε, σε περιοδική βάση, προγράμματα εκπαίδευσης και ευαισθητοποίησης σε θέματα κυβερνοασφάλειας για το σύνολο του προσωπικού σας, καθώς και για μέλη της διοίκησης.

ΠΕΡΙΓΡΑΦΗ

- Ο ανθρώπινος παράγοντας αποτελεί τον πλέον αδύναμο κρίκο στην κυβερνοασφάλεια και οι ενέργειες των χρηστών, είτε σκόπιμες είτε ακούσιες, μπορούν να προκαλέσουν σοβαρά περιστατικά παραβίασης συστημάτων και δεδομένων. Παραδείγματα αποτελούν το άνοιγμα ενός κακόβουλου συνδέσμου σε ένα phishing email, η αποστολή ευαίσθητης πληροφορίας σε λάθος παραλήπτη ή η χρήση αδύναμων κωδικών πρόσβασης.
- Η αποτελεσματική εκπαίδευση δεν είναι μία εφάπαξ ενέργεια αλλά μια συνεχής διαδικασία που συνδυάζει αρχική εκπαίδευση κατά την έναρξη της εργασιακής σχέσης, ετήσια επανεκπαίδευση, στοχευμένη εκπαίδευση ανά ρόλο για όσους έχουν αυξημένη έκθεση σε κινδύνους, καθώς και διαρκή ευαισθητοποίηση μέσω τακτικών μηνυμάτων και προσομοιώσεων.

ΟΔΗΓΙΕΣ ΥΛΟΠΟΙΗΣΗΣ

- Υλοποιήστε, σε περιοδική βάση, προγράμματα εκπαίδευσης και ευαισθητοποίησης σε βασικά θέματα κυβερνοϋγιεινής που θα απευθύνονται στο σύνολο του προσωπικού και σε μέλη της Διοίκησης. Τα εν λόγω προγράμματα θα πρέπει να καλύπτουν, κατ' ελάχιστο, τα ακόλουθα:
  - τους τρόπους αναγνώρισης δυνητικών συμβάντων κυβερνοασφάλειας και αναφοράς τους στο αρμόδιο προσωπικό,
  - την ασφαλή χρήση του ηλεκτρονικού ταχυδρομείου και τους τρόπους αναγνώρισης των emails εξαπάτησης (phishing και business email compromise),
  - τους τρόπους αναγνώρισης μηνυμάτων εξαπάτησης, παραπληροφόρησης και κοινωνικής μηχανικής, συμπεριλαμβανομένων των deepfakes,
  - την ασφαλή χρήση των εφαρμογών τεχνητής νοημοσύνης,
  - τους τρόπους δημιουργίας και διαχείρισης ισχυρών κωδικών πρόσβασης,
  - τη χρήση μεθόδων αυθεντικοποίησης πολλαπλών παραγόντων (multi-factor authentication),
  - τους τρόπους ασφαλούς πλοήγησης στο διαδίκτυο,
  - τους τρόπους λήψης αντιγράφων ασφαλείας (backup),
  - τους τρόπους ασφαλούς χρήσης κινητών συσκευών,
  - τη σημασία των τακτικών ενημερώσεων ασφάλειας (security updates),
  - τις βασικές ρυθμίσεις ασφάλειας στο οικιακό δίκτυο του χρήστη.
- Υλοποιήστε, σε περιοδική βάση, προγράμματα εκπαίδευσης σε θέματα κυβερνοασφάλειας που θα απευθύνονται σε μέλη του προσωπικού με τεχνικά εξειδικευμένο ρόλο και καθήκοντα.

Ανάλογα με τους ρόλους, την τεχνογνωσία και τις αρμοδιότητες, η ύλη των εν λόγω προγραμμάτων μπορεί να περιλαμβάνει:

- λεπτομερείς οδηγίες για την ασφαλή παραμετροποίηση συσκευών, συστημάτων, εφαρμογών, υπηρεσιών και δικτύων,
- τεχνική ανάλυση γνωστών απειλών και κινδύνων κυβερνοασφάλειας,
- εκπαίδευση στη διαχείριση και αποτελεσματική απόκριση σε περιστατικά κυβερνοασφάλειας,
- εκπαίδευση στη διαχείριση κρίσεων και σε διαδικασίες διασφάλισης της επιχειρησιακής συνέχειας (business continuity),
- θέματα κυβερνοασφάλειας διαδικτυακών εφαρμογών (π.χ. OWASP Top-10) και εφαρμογών τεχνητής νοημοσύνης (LLM, agentic AI).

- Εξετάστε την περιοδική διενέργεια ελεγχόμενων προσομοιώσεων phishing τουλάχιστον δύο φορές ετησίως, με σταδιακά αυξανόμενο βαθμό δυσκολίας.
- Μετρήστε την αποτελεσματικότητα της εκπαίδευσης με απλούς δείκτες, όπως ποσοστό συμμετοχής, χρόνος αναφοράς ύποπτου μηνύματος, αριθμός αναφορών phishing και αποτελέσματα προσομοιώσεων κοινωνικής μηχανικής, όπου αυτές εφαρμόζονται.

ΔΙΑΔΙΚΑΣΙΕΣ ΑΞΙΟΛΟΓΗΣΗΣ

- Εξέταση / επισκόπηση:
  - πολιτικών και διαδικασιών που αφορούν στην περιοδική εκπαίδευση και ευαισθητοποίηση σε θέματα κυβερνοασφάλειας,
  - σχετικού υλικού εκπαίδευσης,
  - καταστάσεων / βεβαιώσεων παρακολούθησης προγραμμάτων εκπαίδευσης για το προσωπικό, τα μέλη της Διοίκησης, καθώς και για προσωπικό με τεχνικά εξειδικευμένο ρόλο και καθήκοντα.
- Διενέργεια συνέντευξης / συζήτησης με μέλη της Διοίκησης, τον υπεύθυνο κυβερνοασφάλειας ή / και μέλη του προσωπικού με αρμοδιότητα τη διενέργεια προγραμμάτων εκπαίδευσης και ευαισθητοποίησης για θέματα κυβερνοασφάλειας.

9. Ασφάλεια εφοδιαστικής αλυσίδας

ΑΠΑΙΤΗΣΗ 9.1

Υλοποιήστε διαδικασίες αξιολόγησης των προμηθευτών και παρόχων υπηρεσιών πληροφορικής, με σκοπό τη διαχείριση των κινδύνων κυβερνοασφάλειας που σχετίζονται με τη χρήση προϊόντων και υπηρεσιών τους.

ΠΕΡΙΓΡΑΦΗ

- Στο σημερινό πλήρως διασυνδεδεμένο κόσμο αρκετές επιχειρήσεις στηρίζονται σε εξωτερικούς προμηθευτές και παρόχους υπηρεσιών Τ.Π.Ε. (τεχνολογίες πληροφορικής και επικοινωνιών) για την προμήθεια προϊόντων, καθώς και για τη διαχείριση και υποστήριξη των υποδομών, συστημάτων και δικτύων τους. Αυτό έχει ως αποτέλεσμα, σε περίπτωση παραβίασης των πληροφοριακών συστημάτων των παρόχων από κυβερνοεγκληματίες, να επηρεαστούν αντίστοιχα και οι υποδομές των συμβαλλόμενων επιχειρήσεων. Για παράδειγμα, στην περίπτωση κυβερνοεπίθεσης με λυτρισμικό (ransomware) οι λειτουργίες της επιχείρησης θα επηρεαστούν έμμεσα, καθώς η διαθεσιμότητα των συστημάτων του παρόχου θα διαταραχθεί. Ακόμα χειρότερα, εάν υπάρχει απευθείας διασύνδεση των συστημάτων της επιχείρησης και του παρόχου, μία επίθεση με λυτρισμικό θα μπορούσε να κρυπτογραφήσει και τα δεδομένα της ίδιας της επιχείρησης. Για το λόγο αυτό, είναι επιτακτικό οι πολιτικές κυβερνοασφάλειας των επιχειρήσεων να επεκτείνονται και στους προμηθευτές και παρόχους υπηρεσιών τους.
- Η κυβερνοασφάλεια στην εφοδιαστική αλυσίδα δεν περιορίζεται στους άμεσους προμηθευτές: σύγχρονα περιστατικά έδειξαν ότι ευπάθειες σε υπεργολάβους των προμηθευτών (fourth-party risk) μπορούν να επηρεάσουν εξίσου τη λειτουργία της επιχείρησης. Επιπλέον, η υπερβολική εξάρτηση από έναν μόνο πάροχο (concentration risk) μπορεί να προκαλέσει διακοπή λειτουργίας ακόμη και χωρίς κυβερνοεπίθεση, εφόσον ο εν λόγω πάροχος αντιμετωπίσει σοβαρό περιστατικό.

ΟΔΗΓΙΕΣ ΥΛΟΠΟΙΗΣΗΣ

- Αναπτύξτε ενημερωμένο μητρώο με τους άμεσους προμηθευτές και παρόχους υπηρεσιών Τ.Π.Ε. και, εφόσον είναι εφικτό, κατηγοριοποιήστε τους σε διαφορετικά επίπεδα κρισιμότητας. Διασφαλίστε ότι το μητρώο περιλαμβάνει κατ' ελάχιστον τα σημεία επαφής, τα προϊόντα και υπηρεσίες Τ.Π.Ε. που κάθε προμηθευτής παρέχει, καθώς και την έδρα τους. Επιπλέον, συνιστάται η συμπερίληψη της ημερομηνίας έναρξης και λήξης των αντίστοιχων συμβάσεων.
- Επιλέξτε προϊόντα και υπηρεσίες πληροφορικής από αξιόπιστες πηγές. Η αξιοπιστία υλικού και λογισμικού είναι ζήτημα ποιοτικού ελέγχου. Ενώ, γενικά, δεν είναι εφικτό για μία μικρομεσαία επιχείρηση να επιθεωρήσει τα συστήματα ποιοτικού ελέγχου των προμηθευτών της, μπορεί να κάνει αξιόπιστες κρίσεις με βάση τη φήμη του προμηθευτή ή κατασκευαστή.
- Επιλέξτε προμηθευτές και παρόχους υπηρεσιών Τ.Π.Ε. που επιδεικνύουν τη δέουσα προσήλωση στην κυβερνοασφάλεια των συστημάτων και υποδομών τους. Διερευνήστε τις πρακτικές και τα μέτρα κυβερνοασφάλειας που εφαρμόζουν οι προμηθευτές και πάροχοι υπηρεσιών στην υποδομή τους, καθώς και κατά την άσκηση των υπηρεσιών τους. Εξετάστε στοιχεία, όπως ενδεικτικά η ύπαρξη πιστοποίησης σύμφωνα με κάποιο διεθνώς αναγνωρισμένο πρότυπο κυβερνοασφάλειας, το ιστορικό κυβερνοεπιθέσεων και παραβιάσεων, η ύπαρξη πολιτικών ασφάλειας και πλάνου αντιμετώπισης περιστατικών, η δέσμευση για παράδοση υψηλής ποιότητας

ασφαλών προϊόντων και εφαρμογής αρχών όπως π.χ. ασφάλειας από το σχεδιασμό και συγγραφής ασφαλούς κώδικα, η παροχή συνεχούς τεχνικής υποστήριξης, καθώς και η τακτική και έγκαιρη έκδοση ενημερώσεων λογισμικού και ενημερώσεων ασφάλειας (software patches).

- Διαμορφώστε και επικοινωνήστε ένα σύνολο ελάχιστων απαιτήσεων κυβερνοασφάλειας για τους προμηθευτές και παρόχους υπηρεσιών σας, το οποίο να αντανακλά τη διαχείριση κινδύνων που έχετε διενεργήσει. Οι εν λόγω απαιτήσεις θα πρέπει να είναι δικαιολογημένες, αναλογικές και εφικτές και να καταγράφονται ρητά στις συμβάσεις ή σε ανάλογα συμφωνητικά συνεννόησης (memorandum of understandings). Λάβετε υπόψη σας διεθνώς αποδεκτά πρότυπα και βέλτιστες πρακτικές και διαμορφώστε απαιτήσεις που σχετίζονται με κοινές θεματικές κυβερνοασφάλειας, όπως ενδεικτικά έλεγχος πρόσβασης, ασφάλεια δικτύων, προστασία από κακόβουλο λογισμικό, χρήση κρυπτογραφίας, διασφάλιση επιχειρησιακής συνέχειας κ.α.
- Διασφαλίστε τη συμπερίληψη απαιτήσεων κυβερνοασφάλειας στις συμβάσεις με προμηθευτές και παρόχους υπηρεσιών Τ.Π.Ε., όπως:
  - Περιγραφή των συστημάτων και δεδομένων που ο ανάδοχος τυχόν αποκτά πρόσβαση κατά τη διάρκεια της σύμβασης, καθώς και τις αντίστοιχες μεθόδους πρόσβασης.
  - Περιγραφή των απαιτήσεων κυβερνοασφάλειας που αφορούν στην υποδομή του αναδόχου, όπως π.χ. η ύπαρξη πιστοποίησης σύμφωνα με κάποιο διεθνώς αναγνωρισμένο πρότυπο κυβερνοασφάλειας.
  - Περιγραφή των ελάχιστων απαιτήσεων κυβερνοασφάλειας που αφορούν στον έλεγχο πρόσβασης του αναδόχου στα συστήματα της επιχείρησής σας και τις μεθόδους προστασίας των δεδομένων σας που τυχόν τηρούνται στην υποδομή του αναδόχου. Παραδείγματα αποτελούν η υλοποίηση MFA στους λογαριασμούς του αναδόχου, η καταγραφή και παρακολούθηση (logging and monitoring) των ενεργειών του, η διαμερισματοποίηση του δικτύου, η κρυπτογράφηση, η τήρηση αντιγράφων ασφαλείας κ.α.
  - Περιγραφή των απαιτήσεων και διαδικασιών που αφορούν στη διαχείριση περιστατικών κυβερνοασφάλειας (όπως η έγκαιρη κοινοποίηση και η συνεργασία).
  - Το δικαίωμα της διενέργειας ελέγχου εκ μέρους της επιχείρησης.
  - Τη ρύθμιση θεμάτων που αφορούν στη λήξη της σύμβασης, όπως είναι η απενεργοποίηση λογαριασμών των αναδόχων (user accounts), η επιστροφή αγαθών, η ασφαλής διαγραφή δεδομένων και οι απαιτήσεις εμπιστευτικότητας.
- Για κρίσιμους παρόχους, ζητήστε ρητή δέσμευση έγκαιρης ενημέρωσης σε περίπτωση περιστατικού που μπορεί να επηρεάσει τα δεδομένα ή τη λειτουργία της επιχείρησής σας, καθώς και σαφή στοιχεία επικοινωνίας για κλιμάκωση περιστατικών.
- Περιορίστε την πρόσβαση εξωτερικών συνεργατών στα απολύτως αναγκαία συστήματα, με ατομικούς λογαριασμούς, εφαρμογή MFA, χρονικό περιορισμό πρόσβασης και περιοδική ανασκόπηση ενεργών δικαιωμάτων.
- Για κρίσιμο λογισμικό και υπηρεσίες, ζητήστε από τους προμηθευτές τεκμηρίωση συστατικών λογισμικού (Software Bill of Materials – SBOM) και διαδικασία ενημέρωσής σας σε περίπτωση ευπαθειών σε βιβλιοθήκες τρίτων που αξιοποιεί το προϊόν τους.
- Αξιολογήστε τον κίνδυνο συγκέντρωσης (concentration risk): για κρίσιμες λειτουργίες, εξετάστε εναλλακτικούς παρόχους ή στρατηγική πολλαπλής υλοποίησης (multi-vendor), ώστε σοβαρό περιστατικό σε έναν πάροχο να μην παραλύσει ολόκληρη την επιχειρηματική λειτουργία.

- Όταν ο προμηθευτής επεξεργάζεται προσωπικά δεδομένα για λογαριασμό σας, συνάψτε σύμβαση επεξεργασίας δεδομένων (Data Processing Agreement — DPA) σύμφωνα με το άρθρο 28 του GDPR και τηρήστε επικαιροποιημένο κατάλογο υποπαρόχων (subprocessors) που εγκρίνετε.

ΔΙΑΔΙΚΑΣΙΕΣ ΑΞΙΟΛΟΓΗΣΗΣ

- Εξέταση / επισκόπηση:
  - πολιτικών και διαδικασιών που αφορούν στις σχέσεις της επιχείρησης με προμηθευτές και παρόχους υπηρεσιών Τ.Π.Ε. και τη διαχείριση της εφοδιαστικής αλυσίδας,
  - συμβάσεων προμήθειας πληροφοριακών αγαθών ή ανάθεσης υπηρεσιών διαχείρισης και υποστήριξης συστημάτων, εφαρμογών και δικτύων.
- Διενέργεια συνέντευξης / συζήτησης με μέλη της Διοίκησης, τον υπεύθυνο κυβερνοασφάλειας ή / και μέλη του προσωπικού με αρμοδιότητα τη διαχείριση ζητημάτων που αφορούν στην εφοδιαστική αλυσίδα.

10. Διαχείριση υπηρεσιών νεφοϋπολογιστικής

ΑΠΑΙΤΗΣΗ 10.1

Εφαρμόστε αρχές κυβερνοασφάλειας κατά την επιλογή και χρήση υπηρεσιών νεφοϋπολογιστικής (cloud).

ΠΕΡΙΓΡΑΦΗ

- Οι υπηρεσίες νεφοϋπολογιστικής (cloud computing) μπορούν να προσφέρουν αρκετά πλεονεκτήματα σε μία μικρομεσαία επιχείρηση: λειτουργίες και δεδομένα της μεταφέρονται στο cloud, με αποτέλεσμα την αποφυγή υψηλού κόστους προμηθειών σε υλικό, λογισμικό, καθώς και σε υπηρεσίες συντήρησης και υποστήριξης, ενώ παράλληλα η επιχείρηση έχει πρόσβαση σε εφαρμογές τελευταίας τεχνολογίας. Επίσης, οι αξιόπιστοι πάροχοι cloud μπορούν να προσφέρουν υπηρεσίες κυβερνοασφάλειας ανώτερου επιπέδου σε σχέση με τις αντίστοιχες οικονομικές δυνατότητες μίας μικρομεσαίας επιχείρησης. Ωστόσο, η μεταφορά δεδομένων, εφαρμογών και λειτουργιών σε cloud πλατφόρμες εισάγει κινδύνους ασφάλειας που πρέπει να αντιμετωπίζονται καθ' όλη τη διάρκεια του κύκλου ζωής μίας υπηρεσίας cloud, από την αρχική επιλογή, τις παραμετροποιήσεις, την καθημερινή λειτουργία, έως την ανανέωση και τον τερματισμό.
- Η βασική αρχή είναι ότι η ανάθεση εφαρμογών και λειτουργιών σε τρίτους παρόχους δεν συνεπάγεται και την αντίστοιχη ανάθεση της λογοδοσίας για την κυβερνοασφάλεια. Ένας πάροχος cloud υπηρεσιών μπορεί να υλοποιεί στην υποδομή του κατάλληλα μέτρα κυβερνοασφάλειας, όμως ο πελάτης (η επιχείρηση) παραμένει υπεύθυνος για διάφορες πτυχές που άπτονται της προστασίας των δεδομένων του, του ελέγχου πρόσβασης, της ορθής παραμετροποίησης υπηρεσιών, της συμμόρφωσης με το νομοθετικό πλαίσιο και της διασφάλισης επιχειρησιακής συνέχειας.

ΟΔΗΓΙΕΣ ΥΛΟΠΟΙΗΣΗΣ

- Εφαρμόστε κριτήρια αξιολόγησης κατά την επιλογή παρόχων υπηρεσιών νεφοϋπολογιστικής, όπως ενδεικτικά:
  - η ύπαρξη πιστοποίησης σύμφωνα με διεθνώς αναγνωρισμένα πρότυπα κυβερνοασφάλειας (π.χ. ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, SOC 2 κ.α.),
  - η γεωγραφική τοποθεσία των κέντρων δεδομένων και, ειδικότερα, σε ποιες χώρες τα δεδομένα αποθηκεύονται, προσπελάζονται, υποβάλλονται σε επεξεργασία και δημιουργούνται αντίγραφα ασφαλείας,
  - Η φήμη και η εμπειρία του παρόχου στην αγορά.
- Εξετάστε προσεκτικά τους όρους της σύμβασης παροχής υπηρεσιών (Service Level Agreement – SLA), διασφαλίζοντας ότι αυτή περιλαμβάνει σαφείς αναφορές σε ζητήματα κυβερνοασφάλειας, όπως ενδεικτικά:
  - Καθορισμός του μοντέλου κοινής ευθύνης (shared responsibility model): ποιος συμβαλλόμενος έχει την ευθύνη για ποιο θεματικό πεδίο κυβερνοασφάλειας, π.χ. ενημερώσεις ασφάλειας λειτουργικών συστημάτων και εφαρμογών, διαχείριση χρηστών και

έλεγχος πρόσβασης, ασφάλεια εφαρμογών, παραμετροποιήσεις ασφάλειας, αντίγραφα ασφαλείας, απόκριση σε περιστατικά, ανάκτηση δεδομένων κ.α.

- Καθορισμός διαδικασιών διαχείρισης περιστατικών κυβερνοασφάλειας, συμπεριλαμβανομένης της έγκαιρης ενημέρωσης της επιχείρησης σε περίπτωση παραβίασης.
- Καθορισμός ζητημάτων συμμόρφωσης με τη σχετική νομοθεσία περί προστασίας προσωπικών δεδομένων.
- Καθορισμός θεμάτων διαφάνειας όσον αφορά στην ανάθεση μέρους των υπηρεσιών του παρόχου σε άλλους υπεργολάβους.

- Διασφαλίστε ότι ο πάροχος cloud υπηρεσιών εφαρμόζει κατάλληλα μέτρα προστασίας των δεδομένων της επιχείρησης, όπως ενδεικτικά:
  - Κρυπτογράφηση των δεδομένων κατά τη μεταφορά (in transit) και κατά την αποθήκευση (at rest).
  - Ασφαλής διαχείριση κρυπτογραφικών κλειδιών.
  - Έλεγχος της τοποθεσίας των κύριων δεδομένων, των αντιγράφων ασφαλείας και των καταγραφών συμβάντων.
  - Διαχωρισμός των δεδομένων της επιχείρησης από τα δεδομένα άλλων πελατών.
  - Διαδικασίες ασφαλούς διαγραφής των δεδομένων κατά τη λήξη της σύμβασης.
- Διασφαλίστε ότι ο πάροχος παρέχει στην επιχείρησή σας τη δυνατότητα διαχείρισης της πρόσβασης των χρηστών στις υπηρεσίες cloud με ασφαλή τρόπο, μέσω μηχανισμών όπως:
  - Η υλοποίηση ισχυρών κωδικών πρόσβασης.
  - Η ενεργοποίηση ελέγχου ταυτότητας πολλαπλών παραγόντων (MFA) για το σύνολο των χρηστών και, ιδίως, για την πρόσβαση των διαχειριστών, την απομακρυσμένη πρόσβαση και την πρόσβαση σε κρίσιμες εφαρμογές. Εξετάστε την υλοποίηση phishing resistant MFA.
  - Η εφαρμογή της αρχής των ελάχιστων προνομίων (least privilege) και της πρόσβασης βάσει ρόλων (role-based access).
  - Η καταγραφή των ενεργειών των χρηστών (audit logging) για σκοπούς ελέγχου.
  - Η υλοποίηση μηχανισμών κεντρικής διαχείρισης λογαριασμών (centralised account management).

  Συνιστάται η χρήση εταιρικά εγκεκριμένων υπολογιστών για τη συνολική διαχείριση της cloud υπηρεσίας.
- Καθορίστε ρητά στη σύμβαση τις διαδικασίες και απαιτήσεις που αφορούν στη μεταφορά και επιστροφή των δεδομένων σας, καθώς και στις δυνατότητες μετάβασης σε άλλον πάροχο (data portability), προκειμένου να αποφεύγονται φαινόμενα εξάρτησης από συγκεκριμένο πάροχο (vendor lock-in) και να διασφαλίζεται η επιχειρησιακή συνέχεια.
- Ελέγχετε περιοδικά τις ρυθμίσεις κοινής χρήσης αρχείων, τους εξωτερικούς χρήστες, τις συνδέσεις τρίτων εφαρμογών και τα διαχειριστικά δικαιώματα σε SaaS υπηρεσίες, διότι αποτελούν συχνή πηγή διαρροής δεδομένων στις επιχειρήσεις.

- Εξετάστε την τήρηση ανεξάρτητου αντίγραφου ασφαλείας των δεδομένων που φιλοξενούνται σε SaaS εφαρμογές (software as a service), όπου απαιτείται.
- Απαγορεύστε ρητά τη χρήση προσωπικών λογαριασμών νεφοϋπολογιστικής για επιχειρηματικά δεδομένα. Η εταιρική κυριότητα δεδομένων και η δυνατότητα ανάκτησης μετά από αποχώρηση εργαζομένου διασφαλίζεται μόνο μέσω επίσημων εταιρικών λογαριασμών.

ΔΙΑΔΙΚΑΣΙΕΣ ΑΞΙΟΛΟΓΗΣΗΣ

- Εξέταση / επισκόπηση:
  - πολιτικών και διαδικασιών που αφορούν στην επιλογή, αξιολόγηση και διαχείριση παρόχων υπηρεσιών νεφοϋπολογιστικής,
  - συμβάσεων (SLAs) με τους παρόχους cloud υπηρεσιών,
  - πιστοποιήσεων και αναφορών ελέγχου (audit reports) που έχει προσκομίσει ο πάροχος.
- Διενέργεια συνέντευξης / συζήτησης με μέλη της Διοίκησης, τον υπεύθυνο κυβερνοασφάλειας ή / και μέλη του προσωπικού με αρμοδιότητα τη διαχείριση των υπηρεσιών νεφοϋπολογιστικής.

11. Κρυπτογραφία

ΑΠΑΙΤΗΣΗ 11.1

Εφαρμόστε διαδικασίες και τεχνολογίες κρυπτογράφησης, με σκοπό την προστασία των κρίσιμων δεδομένων της επιχείρησης.

ΠΕΡΙΓΡΑΦΗ

- Τα δεδομένα αποτελούν ένα από τα πλέον κρίσιμα αγαθά για κάθε σύγχρονη επιχείρηση. Πληροφορίες πελατών, οικονομικά στοιχεία, εμπορικά μυστικά, τεχνογνωσία και προσωπικά δεδομένα εργαζομένων αποτελούν στόχο για κυβερνοεγκληματίες, καθώς η παραβίαση, αλλοίωση ή απώλειά τους μπορεί να προκαλέσει σοβαρή οικονομική ζημιά, νομικές συνέπειες και απώλεια της εμπιστοσύνης πελατών και συνεργατών.
- Η χρήση της κρυπτογραφίας αποτελεί ένα από τα πλέον αποτελεσματικά μέτρα προστασίας της εμπιστευτικότητας, ακεραιότητας και αυθεντικότητας των δεδομένων, καθώς διασφαλίζει ότι ακόμα και αν τα δεδομένα περιέλθουν σε μη εξουσιοδοτημένα πρόσωπα, αυτά δεν θα είναι σε θέση να τα διαβάσουν ή να τα αλλοιώσουν. Παράλληλα, η συστηματική κατηγοριοποίηση των δεδομένων και η εφαρμογή κατάλληλων μέτρων προστασίας ανάλογα με το επίπεδο ευαισθησίας τους, αποτελεί βασική προϋπόθεση για την ορθή διαχείρισή τους και τη συμμόρφωση με τη σχετική νομοθεσία περί προστασίας προσωπικών δεδομένων (GDPR).

ΟΔΗΓΙΕΣ ΥΛΟΠΟΙΗΣΗΣ

- Διασφαλίστε ότι τα ευαίσθητα δεδομένα της επιχείρησής σας (όπως προσωπικά δεδομένα πελατών και εργαζομένων, οικονομικά στοιχεία, εμπορικά μυστικά, διαπιστευτήρια πρόσβασης) κρυπτογραφούνται κατά την αποθήκευσή τους (data at rest) σε εξυπηρετητές, σταθμούς εργασίας, φορητές συσκευές και φορητά μέσα αποθήκευσης (π.χ. USB sticks, εξωτερικοί σκληροί δίσκοι), με χρήση ισχυρών αλγορίθμων κρυπτογράφησης που αντιστοιχούν σε διεθνώς αναγνωρισμένα πρότυπα.
- Εξασφαλίστε ότι τα δεδομένα κρυπτογραφούνται κατά τη μεταφορά τους μέσω δικτύων (data in transit), εφαρμόζοντας πρωτόκολλα ασφαλούς επικοινωνίας (π.χ. TLS 1.2 ή, κατά προτίμηση, 1.3, HTTPS, SFTP, VPN), τόσο για τις εσωτερικές επικοινωνίες όσο και για την ανταλλαγή δεδομένων με εξωτερικούς συνεργάτες, πελάτες και παρόχους υπηρεσιών.
- Για ευαίσθητες ηλεκτρονικές επικοινωνίες (νομικά έγγραφα, οικονομικές πληροφορίες, ιατρικά δεδομένα κ.α.), αξιοποιήστε λύσεις end-to-end κρυπτογραφημένης ανταλλαγής αρχείων ή μηνυμάτων, αντί κοινού ηλεκτρονικού ταχυδρομείου χωρίς πρόσθετη προστασία.
- Ενεργοποιήστε την κρυπτογράφηση πλήρους δίσκου (full-disk encryption) σε όλες τις συσκευές χρηστών που χρησιμοποιούνται για επαγγελματικούς σκοπούς, αξιοποιώντας ενσωματωμένες λύσεις όπως το BitLocker (Windows), το FileVault (macOS) ή το dm-crypt (Linux). Με τον τρόπο αυτό, σε περίπτωση απώλειας ή κλοπής της συσκευής, τα δεδομένα παραμένουν μη αναγνώσιμα.
- Υλοποιείστε διαδικασίες ασφαλούς διαχείρισης των κρυπτογραφικών κλειδιών, υλοποιώντας κατάλληλα μέτρα για την ασφαλή παραγωγή, αποθήκευση, διανομή, χρήση, ανανέωση και καταστροφή τους. Τα κρυπτογραφικά κλειδιά πρέπει να προστατεύονται με ισχυρά μέτρα ελέγχου πρόσβασης, για την αποφυγή σκόπιμης αλλοίωσης ή απώλειας.

ΔΙΑΔΙΚΑΣΙΕΣ ΑΞΙΟΛΟΓΗΣΗΣ

- Εξέταση / επισκόπηση:
  - πολιτικών και διαδικασιών χρήσης κρυπτογραφίας,
  - τεχνικών παραμετροποιήσεων κρυπτογράφησης σε συστήματα, εφαρμογές, δίκτυα και τερματικές συσκευές,
  - διαδικασιών διαχείρισης κρυπτογραφικών κλειδιών.
- Διενέργεια συνέντευξης / συζήτησης με τον υπεύθυνο κυβερνοασφάλειας ή / και μέλη του προσωπικού με αρμοδιότητα τη διαχείριση δεδομένων.

12. Λήψη αντιγράφων ασφαλείας

ΑΠΑΙΤΗΣΗ 12.1

Διατηρήστε ασφαλή και επικαιροποιημένα αντίγραφα ασφαλείας των κρίσιμων δεδομένων και πληροφοριακών συστημάτων της επιχείρησης και ελέγχετε τακτικά τη δυνατότητα ανάκτησής τους.

ΠΕΡΙΓΡΑΦΗ

- Τα αντίγραφα ασφαλείας (backups) αποτελούν τη σημαντικότερη γραμμή άμυνας μιας επιχείρησης απέναντι σε περιστατικά απώλειας δεδομένων, είτε αυτά οφείλονται σε κυβερνοεπίθεση, όπως είναι το λυτρισμικό (ransomware), είτε σε βλάβη υλικού, ανθρώπινο λάθος, φυσική καταστροφή ή κλοπή εξοπλισμού. Σε περίπτωση επιτυχούς επίθεσης, η ύπαρξη πρόσφατων και ακέραιων αντιγράφων ασφαλείας είναι συχνά ο μόνος τρόπος επαναφοράς της επιχειρησιακής λειτουργίας χωρίς την καταβολή λύτρων ή την οριστική απώλεια κρίσιμων πληροφοριών. Ωστόσο, η απλή δημιουργία αντιγράφων δεν αρκεί. Τα αντίγραφα ασφαλείας πρέπει να σχεδιάζονται με βάση τις πραγματικές ανάγκες της επιχείρησης, να φυλάσσονται με τρόπο που τα προστατεύει από τις ίδιες απειλές που ενδέχεται να πλήξουν και τα πρωτότυπα δεδομένα και, κυρίως, να ελέγχονται περιοδικά ώστε να διασφαλίζεται ότι μπορούν πράγματι να χρησιμοποιηθούν για επαναφορά όταν αυτό απαιτηθεί.

ΟΔΗΓΙΕΣ ΥΛΟΠΟΙΗΣΗΣ

- Εντοπίστε τα κρίσιμα δεδομένα και συστήματα της επιχείρησης που πρέπει να συμπεριληφθούν στη διαδικασία λήψης αντιγράφων ασφαλείας. Σε αυτά περιλαμβάνονται, ενδεικτικά, οικονομικά και λογιστικά αρχεία, βάσεις δεδομένων πελατών και προμηθευτών, συμβάσεις και νομικά έγγραφα, αρχεία ανθρώπινου δυναμικού, παραμετροποιήσεις πληροφοριακών συστημάτων, καθώς και κάθε δεδομένο του οποίου η απώλεια θα διατάρασσε σημαντικά τη λειτουργία της επιχείρησης.
- Καταγράψτε τις διαδικασίες λήψης και ανάκτησης αντιγράφων ασφαλείας σε γραπτή πολιτική, η οποία θα περιλαμβάνει τους ρόλους και τις αρμοδιότητες των εμπλεκόμενων, τη συχνότητα και τον τύπο των αντιγράφων (full, incremental, differential), τους χρόνους διατήρησης, τις τοποθεσίες αποθήκευσης και τη διαδικασία περιοδικής δοκιμής επαναφοράς.
- Καθορίστε τη συχνότητα λήψης των αντιγράφων ασφαλείας με βάση τη συχνότητα μεταβολής των δεδομένων και τη μέγιστη ανεκτή απώλεια δεδομένων για την επιχείρηση. Για δεδομένα υψηλής κρισιμότητας και συχνά μεταβαλλόμενα, συνιστάται ημερήσια συχνότητα λήψης, ενώ για λιγότερο κρίσιμα δεδομένα ενδέχεται να αρκεί εβδομαδιαία ή μηνιαία λήψη.
- Εφαρμόστε τον κανόνα «3-2-1-1-0» για τη διαχείριση των αντιγράφων ασφαλείας:
  - **3**: τηρείτε τρία αντίγραφα των δεδομένων σας. Το ένα αφορά στο πρωτότυπο (παραγωγικά δεδομένα) συν δύο επιπλέον αντίγραφα ασφαλείας.
  - **2**: αποθηκεύστε τα δύο αντίγραφα σε διαφορετικούς τύπους αποθηκευτικών μέσων, έτσι ώστε η αστοχία ενός τύπου να μην επηρεάζει ταυτόχρονα όλα τα αντίγραφα.

- **1**: διασφαλίστε ότι ένα αντίγραφο φυλάσσεται σε διαφορετική γεωγραφική τοποθεσία (offsite) ή σε αξιόπιστη υπηρεσία νεφοϋπολογιστικής, για προστασία από φυσικές καταστροφές ή κλοπή στις εγκαταστάσεις.
- **1**: αποθηκεύστε ένα αντίγραφο εκτός δικτυακής σύνδεσης (offline / air-gapped) ή ως αμετάβλητο (immutable), μη προσπελάσιμο από το παραγωγικό δίκτυο, ώστε να μην είναι δυνατή η κρυπτογράφηση ή διαγραφή του σε περίπτωση κυβερνοεπίθεσης με λυτρισμικό. Στην έννοια "εκτός σύνδεσης" περιλαμβάνεται και η αποφυγή μόνιμης σύνδεσης USB drives σε υπολογιστικά συστήματα.
- **0**: διασφαλίστε ότι παρατηρούνται μηδέν σφάλματα κατά τον έλεγχο ακεραιότητας των αντιγράφων ασφαλείας και κατά τις δοκιμές επαναφοράς (restoration tests).

- Υλοποιείστε ισχυρά μέτρα προστασίας της υποδομής αντιγράφων ασφαλείας, όπως ενδεικτικά:
  - Διαχωρίστε τους backup διαχειριστικούς λογαριασμούς από τους domain διαχειριστικούς λογαριασμούς. Ο εν λόγω διαχωρισμός είναι ιδιαίτερα σημαντικός, καθώς σε περίπτωση παραβίασης του ενός επιπέδου, το άλλο επίπεδο δεν είναι αυτόματα εκτεθειμένο.
  - Επιβάλλετε την υλοποίηση ισχυρών συνθηματικών και ελέγχου ταυτότητας πολλαπλών παραγόντων (MFA) σε όλους τους διαχειριστικούς λογαριασμούς backup.
  - Εφαρμόστε την αρχή των ελάχιστων προνομίων (least privilege) και τον έλεγχο πρόσβασης βάσει ρόλων (role-based access control).
  - Ενεργοποιείστε την καταγραφή και την παρακολούθηση συμβάντων (logging and monitoring) που σχετίζονται με πρόσβαση στην backup υποδομή, με αλλαγές παραμετροποιήσεων (configuration changes), απόπειρες διαγραφής και απόπειρες κρυπτογράφησης.
  - Υλοποιείστε διαμερισματοποίηση δικτύου (network segmentation) μεταξύ των παραγωγικών συστημάτων και της backup υποδομής.
  - Υλοποιείστε κρυπτογράφηση των αντιγράφων ασφαλείας, ιδίως όταν αυτά μεταφέρονται εκτός των εγκαταστάσεων της επιχείρησης ή φυλάσσονται σε υπηρεσίες τρίτων.
- Υλοποιείστε περιοδικά διαδικασίες ανάκτησης (restore) από τα αντίγραφα ασφαλείας σε ένα ελεγχόμενο περιβάλλον. Ένα αντίγραφο ασφαλείας που δεν έχει δοκιμαστεί δεν παρέχει εγγύηση ότι θα λειτουργήσει όταν χρειαστεί. Καταγράψτε τον απαιτούμενο χρόνο ανάκτησης (Recovery Time Objective – RTO) και επιβεβαιώστε ότι ικανοποιεί τις επιχειρηματικές σας απαιτήσεις.
- Για κάθε κρίσιμη εφαρμογή καθορίστε τους δείκτες RPO (Recovery Point Objective) και RTO (Recovery Time Objective) σε απλή επιχειρησιακή γλώσσα: πόσα δεδομένα αντέχει να χάσει η επιχείρηση και σε πόσο χρόνο πρέπει να επανέλθει η λειτουργία. Οι τιμές αυτές πρέπει να επιβεβαιώνονται με πραγματικές δοκιμές ανάκτησης.
- Επεκτείνετε τη λογική των αντιγράφων ασφαλείας σε ένα σύντομο σχέδιο Επιχειρησιακής Συνέχειας και Ανάκαμψης από Καταστροφές (Business Continuity / Disaster Recovery Plan – BCP/DRP). Το σχέδιο θα πρέπει να καλύπτει: εναλλακτικούς τρόπους εργασίας σε περίπτωση μη διαθεσιμότητας συστημάτων (π.χ. εργασία από το σπίτι, εφεδρικά laptops, χειρόγραφες διαδικασίες), εναλλακτικά κανάλια επικοινωνίας με πελάτες και προμηθευτές, σειρά προτεραιοποίησης αποκατάστασης κρίσιμων υπηρεσιών και χρηματοοικονομικά αποθέματα για ακραίες περιπτώσεις.
- Διενεργείτε τουλάχιστον μία ολοκληρωμένη ετήσια δοκιμή ανάκαμψης (full-scale disaster recovery test) που να προσομοιώνει εκτεταμένη απώλεια διαθεσιμότητας και να αξιολογεί όχι

μόνο την τεχνική ανάκτηση αλλά και τις διαδικασίες επικοινωνίας, την κλιμάκωση και την ικανότητα του προσωπικού να ακολουθήσει διαδικασίες ανάκαμψης υπό πίεση.

ΔΙΑΔΙΚΑΣΙΕΣ ΑΞΙΟΛΟΓΗΣΗΣ

- Εξέταση / επισκόπηση:
  - πολιτικών και διαδικασιών λήψης και διατήρησης αντιγράφων ασφαλείας,
  - αποτελεσμάτων περιοδικών δοκιμών επαναφοράς από αντίγραφα ασφαλείας.
- Διενέργεια συνέντευξης / συζήτησης με τον υπεύθυνο κυβερνοασφάλειας ή / και μέλη του προσωπικού με αρμοδιότητα τη διαχείριση των αντιγράφων ασφαλείας και την επαναφορά δεδομένων.

13. Καταγραφή και παρακολούθηση συμβάντων

ΑΠΑΙΤΗΣΗ 13.1

Εφαρμόστε διαδικασίες καταγραφής και παρακολούθησης συμβάντων στα πληροφοριακά συστήματα της επιχείρησης, με στόχο την έγκαιρη ανίχνευση και αντιμετώπιση περιστατικών κυβερνοασφάλειας.

ΠΕΡΙΓΡΑΦΗ

- Η καταγραφή και παρακολούθηση συμβάντων (logging and monitoring) αποτελεί θεμελιώδη πρακτική κυβερνοασφάλειας, καθώς επιτρέπει στην επιχείρηση να αντιληφθεί έγκαιρα ασυνήθιστη ή ύποπτη συμπεριφορά στα πληροφοριακά της συστήματα και να αντιδράσει πριν ένα συμβάν εξελιχθεί σε σοβαρό περιστατικό. Χωρίς επαρκή αρχεία καταγραφής, μια κυβερνοεπίθεση ενδέχεται να παραμείνει απαρατήρητη για εβδομάδες ή μήνες, ενώ ακόμη και μετά τον εντοπισμό της, η απουσία ιχνών καθιστά εξαιρετικά δύσκολη τη διερεύνηση του τρόπου παραβίασης, την έκταση των επιπτώσεων και τη λήψη μέτρων αποκατάστασης. Επιπλέον, πέραν της ενεργοποίησης της καταγραφής συμβάντων, η τακτική παρακολούθησή τους αποτελεί την ουσιαστική δραστηριότητα με την οποία εντοπίζονται κακόβουλες ενέργειες και προλαμβάνονται κυβερνοεπιθέσεις. Για το λόγο αυτό, οι επιχειρήσεις θα πρέπει, εκτός από τις τεχνικές παραμετροποιήσεις συστημάτων, να εφαρμόζουν και διαδικασίες τακτικής παρακολούθησης και ανάλυσης των καταγραφών συμβάντων.

ΟΔΗΓΙΕΣ ΥΛΟΠΟΙΗΣΗΣ

- Ενεργοποιήστε τα αρχεία καταγραφής συμβάντων (event logs) στα πληροφοριακά συστήματα της επιχείρησής σας, συμπεριλαμβανομένων των εξυπηρετητών (servers), των σταθμών εργασίας, του δικτυακού εξοπλισμού (firewalls, routers, switches), των εφαρμογών διαχείρισης και των υπηρεσιών cloud. Διασφαλίστε ότι καταγράφονται, κατ' ελάχιστον, συμβάντα όπως επιτυχημένες και αποτυχημένες προσπάθειες σύνδεσης, μεταβολές δικαιωμάτων πρόσβασης, κινήσεις προνομιακών και διαχειριστικών λογαριασμών, εγκατάσταση ή αφαίρεση λογισμικού, αιτήματα DNS (DNS query logs), σημαντικές αλλαγές παραμετροποίησης, καθώς και ειδοποιήσεις από τα συστήματα ασφάλειας (antivirus, EDR, intrusion detection systems).
- Καταγράψτε σε γραπτή διαδικασία τους ρόλους και τις αρμοδιότητες για την παρακολούθηση των συμβάντων, τη συχνότητα επισκόπησης των αρχείων καταγραφής, τα κριτήρια χαρακτηρισμού ενός συμβάντος ως ύποπτου, καθώς και τον τρόπο κλιμάκωσης προς τους υπευθύνους ή προς εξωτερικούς συνεργάτες όταν εντοπίζονται ενδείξεις πιθανού περιστατικού κυβερνοασφάλειας.
- Διασφαλίστε ότι τα ρολόγια όλων των υπολογιστικών συστημάτων που χρησιμοποιούνται στην επιχείρηση είναι συγχρονισμένα με αποδεκτές πηγές χρόνου. Με τον τρόπο αυτό επιτυγχάνεται η ακρίβεια των καταγραφών συμβάντων και είναι δυνατή η συσχέτιση και ανάλυση συμβάντων που σχετίζονται με την ασφάλεια και η υποστήριξη ερευνών που αφορούν σε περιστατικά κυβερνοασφάλειας. Μη ακριβείς καταγραφές συμβάντων μπορούν να δυσκολέψουν τις νομικές έρευνες και να βλάψουν την αξιοπιστία των τεκμηρίων. Παραδείγματα μεθόδων υλοποίησης του συγχρονισμού των ρολογιών είναι η χρήση των πρωτοκόλλων NTP (Network Time Protocol) και PTP (Precision Time Protocol), καθώς και η χρήση του GPS (Global Positioning System).

- Καθορίστε χρόνους διατήρησης των αρχείων καταγραφής, λαμβάνοντας υπόψη τις λειτουργικές ανάγκες της επιχείρησης, καθώς και τυχόν κανονιστικές, συμβατικές ή νομικές υποχρεώσεις. Οι ακριβείς χρόνοι προσαρμόζονται στις νομικές και επιχειρησιακές απαιτήσεις κατά περίπτωση.
- Υλοποιείστε τη συλλογή και διαχείριση των καταγραφών συμβάντων σε κεντρικό διακομιστή (centralized logging). Ένα σύστημα διαχείρισης καταγραφών συμβάντων (log management system) συλλέγει και αποθηκεύει logs από μία ποικιλία πηγών (σταθμούς εργασίας, διακομιστές, δικτυακές συσκευές κ.α.) σε ένα κεντρικό σημείο. Με τον τρόπο αυτό επιτυγχάνεται ευχέρεια στην ορατότητα, πρόσβαση και αναζήτηση των καταγραφών, καθώς και στον περαιτέρω έλεγχο για εντοπισμό προβλημάτων. Διασφαλίστε ότι οι καταγραφές που τηρούνται στην εν λόγω κεντρική υποδομή προστατεύονται από μη εξουσιοδοτημένη πρόσβαση, αλλοίωση ή διαγραφή.
- Καθιερώστε διαδικασία περιοδικής επισκόπησης των αρχείων καταγραφής για τον εντοπισμό ασυνήθιστης δραστηριότητας, όπως επανειλημμένες αποτυχημένες συνδέσεις, σαρώσεις δικτύου, συνδέσεις από ασυνήθιστες γεωγραφικές τοποθεσίες ή σε ασυνήθιστες ώρες, μαζικές μεταφορές δεδομένων ή ενεργοποίηση ειδοποιήσεων από εργαλεία ασφάλειας. Όπου είναι εφικτό, αξιοποιήστε αυτοματοποιημένες ειδοποιήσεις (alerts) για την έγκαιρη ανίχνευση κρίσιμων γεγονότων.
- Εξετάστε, εφόσον είναι εφικτό, την υλοποίηση συστήματος SIEM (Security Information and Event Management), είτε στην υποδομή σας, είτε ως υπηρεσία από αξιόπιστο πάροχο. Το SIEM εκτελεί τις παρακάτω λειτουργίες:
  - συλλέγει καταγραφές συμβάντων από διάφορες πηγές και τις αποθηκεύει σε ένα κεντρικό σημείο,
  - αναλύει και συσχετίζει (correlates) συμβάντα από διάφορες πηγές με τη χρήση προκαθορισμένων κανόνων και φίλτρων,
  - ανιχνεύει (detects) πιθανές κυβερνοαπειλές και δημιουργεί ειδοποιήσεις (alerts) με σκοπό την περαιτέρω διερεύνηση του συμβάντος.

  Οι σύγχρονες λύσεις SIEM προσφέρουν τη δυνατότητα συνεχούς παρακολούθησης, προηγμένων μορφών ανάλυσης, καθώς και τη χρήση τεχνολογιών μηχανικής μάθησης.
- Εξετάστε την υλοποίηση συνδρομής σε αξιόπιστους παρόχους υπηρεσιών κυβερνοασφάλειας για υπηρεσίες ανίχνευσης ή / και αντιμετώπισης περιστατικών (managed detection and response). Εναλλακτικά, διερευνήστε τις επιλογές δωρεάν πηγών τηλεμετρίας που παρέχουν πάροχοι cloud υπηρεσιών. Η ύπαρξη οποιασδήποτε στοιχειώδους ανίχνευσης είναι σημαντικά αποτελεσματικότερη από την παντελή απουσία της.

ΔΙΑΔΙΚΑΣΙΕΣ ΑΞΙΟΛΟΓΗΣΗΣ

- Εξέταση / επισκόπηση:
  - πολιτικών και διαδικασιών καταγραφής και παρακολούθησης συμβάντων,
  - δείγματος αρχείων καταγραφής από κρίσιμα συστήματα,
- Διενέργεια συνέντευξης / συζήτησης με τον υπεύθυνο κυβερνοασφάλειας ή / και μέλη του προσωπικού με αρμοδιότητα την παρακολούθηση και διαχείριση των αρχείων καταγραφής συμβάντων.

14. Διαχείριση περιστατικών κυβερνοασφάλειας

ΑΠΑΙΤΗΣΗ 14.1

Αναπτύξτε διαδικασίες διαχείρισης περιστατικών κυβερνοασφάλειας, με σκοπό την έγκαιρη και αποτελεσματική απόκριση σε κυβερνοεπιθέσεις.

ΠΕΡΙΓΡΑΦΗ

- Παρά την εφαρμογή προληπτικών μέτρων κυβερνοασφάλειας, καμία επιχείρηση δεν είναι απρόσβλητη από κυβερνοεπιθέσεις. Όταν εκδηλωθεί σημαντικό περιστατικό, η ταχύτητα και η αποτελεσματικότητα της αντίδρασης είναι κρίσιμες για τον περιορισμό των επιπτώσεων και την ταχεία επαναφορά των επιχειρηματικών λειτουργιών. Η έγκαιρη ανίχνευση, η οργανωμένη απόκριση, η επικοινωνία με τα ενδιαφερόμενα μέρη και η άντληση γνώσης από τη μελέτη των αιτιών του περιστατικού συμβάλλουν τόσο στη μείωση των ζημιών όσο και στην ενίσχυση των ικανοτήτων αντιμετώπισης μελλοντικών απειλών. Η διαχείριση περιστατικών πρέπει να είναι ένας αποτελεσματικός συνδυασμός ανθρώπινου δυναμικού, διαδικασιών και τεχνικών μέτρων και να αποτελεί μέρος του ευρύτερου πλαισίου διαχείρισης κινδύνων της επιχείρησης.

ΟΔΗΓΙΕΣ ΥΛΟΠΟΙΗΣΗΣ

- Αναπτύξτε γραπτό πλάνο απόκρισης σε περιστατικά κυβερνοασφάλειας (incident response plan). Το πλάνο θα πρέπει να περιλαμβάνει:
  - τον καθορισμό ρόλων, αρμοδιοτήτων και ευθυνών για τη διαχείριση των περιστατικών.
  - Πληροφορίες επικοινωνίας για πρόσωπα με ορισθέντα ρόλο στη διαχείριση περιστατικών (π.χ. υπεύθυνος κυβερνοασφάλειας, εξωτερικοί πάροχοι υπηρεσιών, νομικό τμήμα, γραφείο τύπου κ.α.).
  - Πληροφορίες επικοινωνίας αρμόδιων αρχών (κρατικές υπηρεσίες, CSIRTS κ.α.).
  - Περιγραφή βασικών ειδών κυβερνοεπιθέσεων (π.χ. ransomware, business email compromise, διαρροή δεδομένων, μη εξουσιοδοτημένη πρόσβαση κ.α.).
  - Οδηγίες και διαδικασίες για την ανίχνευση περιστατικών, τις ενέργειες απόκρισης, καθώς και τις ενέργειες αποκατάστασης των συστημάτων.
- Ορίστε ομάδα ή υπεύθυνο αντιμετώπισης περιστατικών (incident response team) με σαφή εξουσιοδότηση για τη λήψη αποφάσεων κατά τη διάρκεια ενός περιστατικού. Στις μικρότερες επιχειρήσεις, ο ρόλος αυτός μπορεί να ανατεθεί στον υπεύθυνο για την κυβερνοασφάλεια της επιχείρησης, σε συνεργασία με εξωτερικούς συμβούλους, εφόσον απαιτείται.
- Εξετάστε την εκ των προτέρων σύναψη συμβολαίου εξωτερικής υπηρεσίας απόκρισης σε περιστατικά (incident response retainer service) με αξιόπιστο πάροχο υπηρεσιών κυβερνοασφάλειας. Οι εν λόγω συμβάσεις προσφέρουν πλεονεκτήματα, όπως προσυμφωνημένους όρους παροχής υπηρεσιών, συνεχής διαθεσιμότητα (24/7) και εξατομικευμένες υπηρεσίες με βάση το προφίλ της επιχείρησης.
- Διαμορφώστε κατάλογο με στοιχεία επικοινωνίας για την αναφορά περιστατικών σε μέρη που πρέπει να ενημερωθούν. Ο κατάλογος μπορεί να περιλαμβάνει μέλη του προσωπικού, πελάτες,

παρόχους υπηρεσιών, αρμόδιες κρατικές αρχές, υπηρεσίες επιβολής του νόμου, CSIRTS κ.α. Ανάλογα με την περίπτωση και τους παραλήπτες, χρησιμοποιήστε κατάλληλα μέσα και κανάλια επικοινωνίας (π.χ. τηλέφωνο, email, εφαρμογές κρυπτογραφημένης ανταλλαγής μηνυμάτων κ.α.).

- Διενεργήστε έγκαιρη απόκριση σε περιστατικά κυβερνοασφάλειας, ακολουθώντας τις καταγεγραμμένες διαδικασίες. Οι διαδικασίες απόκρισης περιλαμβάνουν τις εξής δραστηριότητες:
  - Περιορισμός (containment): ενέργειες που εμποδίζουν την επέκταση του περιστατικού σε άλλα συστήματα (π.χ. απομόνωση μολυσμένων υπολογιστών από το υπόλοιπο δίκτυο, απενεργοποίηση λογαριασμών κ.α.).
  - Εξάλειψη (eradication): αφαίρεση της αιτίας του περιστατικού και κάθε ίχνους του επιτιθέμενου (π.χ. διαγραφή κακόβουλου λογισμικού, εφαρμογή ενημερώσεων ασφάλειας κ.α.).
  - Ανάκαμψη (recovery): επαναφορά των συστημάτων στην κανονική λειτουργία, εφόσον απαιτείται (π.χ. επαναφορά δεδομένων από backups, επανασύνδεση συστημάτων στο δίκτυο κ.α.).
- Εξετάστε τη δημιουργία διακριτών τεχνικών οδηγιών (playbooks) που θα συνοδεύουν το βασικό πλάνο απόκρισης σε περιστατικά. Τα incident response playbooks αποτελούν δομημένα σύνολα οδηγιών που παρέχουν βήμα-προς-βήμα τεχνικές ενέργειες για την αντιμετώπιση συγκεκριμένων κυβερνοαπειλών (π.χ. playbook για ransomware, playbook για παραβιασμένο λογαριασμό, playbook για διαρροή δεδομένων κ.α.).
- Διασφαλίστε ότι μετά το πέρας σημαντικού περιστατικού θα διενεργηθεί ανάλυση όλων των τεχνικών παραμέτρων και αιτιών της επίθεσης, που θα καταλήξει σε καταγεγραμμένη άντληση γνώσης (lessons learned), με σκοπό τη μείωση της πιθανότητας εμφάνισης παρόμοιων περιστατικών στο μέλλον.
- Διασφαλίστε ότι κατά τη διαδικασία απόκρισης σε σημαντικό περιστατικό τηρείτε λεπτομερές αρχείο καταγραφής, που θα περιλαμβάνει χρονική ακολουθία γεγονότων, ενέργειες που εκτελέστηκαν, στοιχεία που συλλέχθηκαν και αποτελέσματα ανάλυσης. Το αρχείο αυτό αποτελεί κρίσιμο στοιχείο για ενδεχόμενες δικαστικές διαδικασίες, αξιολογήσεις από τις αρχές και βελτίωση της οργανωτικής ετοιμότητας. Η εν λόγω συλλογή και καταγραφή πραγματοποιείται από κατάλληλα εξουσιοδοτημένο και εξειδικευμένο προσωπικό.
- Διασφαλίστε την έγκαιρη κοινοποίηση σημαντικών περιστατικών στις αρμόδιες εθνικές αρχές, εφόσον έχετε τη νομική υποχρέωση. Για τις μικρομεσαίες επιχειρήσεις που εμπίπτουν στο πεδίο εφαρμογής του ν. 5160/2024, η αρχική κοινοποίηση πρέπει να γίνει εντός 24 ωρών, αναλυτική αναφορά εντός 72 ωρών και τελική έκθεση εντός ενός μηνός από το περιστατικό. Για τις επιχειρήσεις που δεν εμπίπτουν στο πεδίο εφαρμογής του ν. 5160/2024, οι χρόνοι αυτοί μπορούν να χρησιμοποιούνται ως πρότυπο εσωτερικής ετοιμότητας και όχι ως αυτοτελής κανονιστική υποχρέωση.
- Διενεργείτε περιοδικά ασκήσεις προσομοίωσης (tabletop exercises) με τη συμμετοχή της διοίκησης, του τεχνικού προσωπικού και των βασικών εμπλεκόμενων φορέων, ώστε να δοκιμάζεται η εφαρμογή του πλάνου απόκρισης σε ρεαλιστικά σενάρια (ransomware, διαρροή δεδομένων, παραβίαση εταιρικού email, απώλεια διαθεσιμότητας υπηρεσίας κ.α.). Καταγράφετε τα ευρήματα και ενσωματώνετε τις βελτιώσεις στο επικαιροποιημένο σχέδιο.

ΔΙΑΔΙΚΑΣΙΕΣ ΑΞΙΟΛΟΓΗΣΗΣ

- Εξέταση / επισκόπηση:
  - πολιτικών, διαδικασιών και πλάνου απόκρισης περιστατικών κυβερνοασφάλειας,
  - αρχείων καταγραφής περιστατικών των τελευταίων ετών.
- Διενέργεια συνέντευξης / συζήτησης με μέλη της Διοίκησης, τον υπεύθυνο κυβερνοασφάλειας, καθώς και μέλη της ομάδας αντιμετώπισης περιστατικών.

15. Έλεγχοι παρείσδυσης (penetration tests)

ΑΠΑΙΤΗΣΗ 15.1

Διενεργήστε ελέγχους παρείσδυσης στα κρίσιμα πληροφοριακά συστήματα και δίκτυα της επιχείρησης, σε τακτική βάση και κατόπιν σημαντικών αλλαγών, με σκοπό τον εντοπισμό ευπαθειών και τους τρόπους εκμετάλλευσής τους από κυβερνοεγκληματίες.

ΠΕΡΙΓΡΑΦΗ

- Οι έλεγχοι παρείσδυσης (penetration tests) αποτελούν προσομοίωση ελεγχόμενων κυβερνοεπιθέσεων από εξειδικευμένο προσωπικό ή εξωτερικούς συνεργάτες, με σκοπό τον εντοπισμό ευπαθειών και τους τρόπους εκμετάλλευσής τους στα συστήματα, δίκτυα και εφαρμογές μιας επιχείρησης. Σε αντίθεση με τις απλές σαρώσεις ευπαθειών (vulnerability scanning), οι έλεγχοι παρείσδυσης προχωρούν στην ενεργή αξιοποίηση των αδυναμιών, αναπαριστώντας ρεαλιστικά τις τεχνικές, τακτικές και διαδικασίες που χρησιμοποιούν οι κυβερνοεγκληματίες. Με τον τρόπο αυτό, η επιχείρηση αποκτά συγκεκριμένη και τεκμηριωμένη εικόνα του επιπέδου της κυβερνοανθεκτικότητάς της (cyber resilience), εντοπίζει κενά ασφάλειας που δεν είναι εμφανή σε άλλους ελέγχους και αξιολογεί την αποτελεσματικότητα των μέτρων προστασίας που έχει υλοποιήσει. Οι έλεγχοι παρείσδυσης συμβάλλουν επίσης στην ικανοποίηση ρυθμιστικών απαιτήσεων και στην ενίσχυση της εμπιστοσύνης πελατών και συνεργατών.

ΟΔΗΓΙΕΣ ΥΛΟΠΟΙΗΣΗΣ

- Καθορίστε το πεδίο εφαρμογής (scope) του ελέγχου παρείσδυσης, προσδιορίζοντας τα συστήματα, δίκτυα, εφαρμογές και υπηρεσίες που θα αποτελέσουν αντικείμενο εξέτασης. Δώστε προτεραιότητα σε κρίσιμα συστήματα που υποστηρίζουν τις βασικές επιχειρηματικές σας λειτουργίες, σε συστήματα που είναι εκτεθειμένα στο διαδίκτυο, σε εφαρμογές που επεξεργάζονται ευαίσθητα ή προσωπικά δεδομένα, καθώς και σε υποδομές που έχουν υποστεί πρόσφατες σημαντικές αλλαγές. Στην περίπτωση που χρησιμοποιείτε εφαρμογές που ενσωματώνουν τεχνητή νοημοσύνη, συμπεριλάβετε στο πεδίο εφαρμογής του ελέγχου παρείσδυσης δοκιμές που εξετάζουν βασικούς κινδύνους για την ασφάλεια των δεδομένων και των επιχειρηματικών διεργασιών σας.
- Επιλέξτε αξιόπιστους και πιστοποιημένους εξωτερικούς συνεργάτες για τη διενέργεια των ελέγχων, εφόσον η επιχείρησή σας δεν διαθέτει την απαιτούμενη εξειδίκευση εσωτερικά. Αξιολογήστε υποψήφιους αναδόχους με βάση τις πιστοποιήσεις των μελών της ομάδας, την προηγούμενη εμπειρία τους σε αντίστοιχα έργα, τη μεθοδολογία που ακολουθούν και τις πρακτικές που εφαρμόζουν για την προστασία των δεδομένων που τους εκχωρούνται κατά τη διάρκεια του ελέγχου.
- Συνάψτε γραπτή σύμβαση με τον ανάδοχο, η οποία να περιγράφει με σαφήνεια το πεδίο εφαρμογής, τη μεθοδολογία, τους κανόνες εμπλοκής (rules of engagement), το χρονοδιάγραμμα, τα παραδοτέα, τις υποχρεώσεις εμπιστευτικότητας και τις διαδικασίες αναφοράς. Ορίστε ρητά τα όρια του ελέγχου, τις ώρες διενέργειας και τα σημεία επαφής σε περίπτωση εντοπισμού κρίσιμης ευπάθειας ή πρόκλησης διαταραχής στη λειτουργία των συστημάτων.

- Διενεργείτε ελέγχους παρείσδυσης σε τακτική βάση και τουλάχιστον ετησίως για τα κρίσιμα συστήματα, καθώς και εκτάκτως μετά από σημαντικές αλλαγές στις υποδομές ή στις εφαρμογές της επιχείρησης (π.χ. αναβαθμίσεις, αλλαγές αρχιτεκτονικής, μεταφορά υπηρεσιών στο cloud, έναρξη παροχής νέας υπηρεσίας), καθώς και μετά από σημαντικό περιστατικό κυβερνοασφάλειας. Συνδυάστε διαφορετικούς τύπους ελέγχων, όπως εξωτερικούς ελέγχους από το διαδίκτυο, εσωτερικούς ελέγχους από το δίκτυο της επιχείρησης, ελέγχους εφαρμογών ιστού και κινητών συσκευών, καθώς και ελέγχους κοινωνικής μηχανικής (social engineering).
- Για μικρές επιχειρήσεις χωρίς κρίσιμες διαδικτυακές εφαρμογές, ο πλήρης ετήσιος έλεγχος παρείσδυσης μπορεί να αντικαθίσταται από αναλογικό σχήμα τεχνικού ελέγχου, όπως εξωτερική σάρωση ευπαθειών, έλεγχος ασφαλούς παραμετροποίησης και επισκόπηση cloud / email ρυθμίσεων. Πλήρης έλεγχος παρείσδυσης προτείνεται όταν υπάρχουν δημόσια προσβάσιμες εφαρμογές, επεξεργασία ευαίσθητων δεδομένων, σημαντική αλλαγή αρχιτεκτονικής ή αυξημένο προφίλ κινδύνου.
- Λάβετε από τον ανάδοχο αναλυτική έκθεση αποτελεσμάτων, η οποία να περιλαμβάνει εκτενή περιγραφή κάθε εντοπισμένης ευπάθειας, την κατηγοριοποίησή της με βάση τη σοβαρότητα, τις μεθόδους αξιοποίησης που χρησιμοποιήθηκαν, την πιθανή επίπτωση στην επιχείρηση, καθώς και συγκεκριμένες και τεκμηριωμένες προτάσεις αποκατάστασης.
- Καταρτίστε σχέδιο αποκατάστασης (remediation plan) με χρονοδιάγραμμα και ρητή ανάθεση αρμοδιοτήτων για κάθε εντοπισμένη ευπάθεια, με προτεραιότητα στις κρίσιμες και υψηλής σοβαρότητας. Παρακολουθήστε συστηματικά την πρόοδο υλοποίησης και διενεργήστε επαναληπτικό έλεγχο (retest) μετά την εφαρμογή των διορθωτικών μέτρων, ώστε να επιβεβαιωθεί η ορθή αποκατάσταση των ευπαθειών χωρίς την εισαγωγή νέων.
- Διαχειριστείτε με ασφάλεια τα δεδομένα και τα ευρήματα του ελέγχου παρείσδυσης. Οι σχετικές εκθέσεις περιέχουν εξαιρετικά ευαίσθητες πληροφορίες που μπορούν να αξιοποιηθούν από κυβερνοεγκληματίες, επομένως θα πρέπει να αποθηκεύονται με κρυπτογράφηση, να διανέμονται μόνο σε εξουσιοδοτημένα στελέχη με βάση την αρχή της ανάγκης γνώσης (need-to-know) και να διαγράφονται με ασφάλεια μετά την πάροδο του απαιτούμενου χρόνου διατήρησης.
- Διασφαλίστε ότι πριν τη διενέργεια του ελέγχου έχετε λάβει ρητή έγκριση των παρόχων υπηρεσιών νεφοϋπολογιστικής για όσα συστήματά σας φιλοξενούνται σε υποδομές τους και ανήκουν στο πεδίο εφαρμογής του ελέγχου. Αρκετοί πάροχοι απαιτούν προειδοποίηση ή τήρηση συγκεκριμένων κανόνων διενέργειας ελέγχων στις υποδομές τους, και η μη συμμόρφωση μπορεί να οδηγήσει σε αναστολή της υπηρεσίας.
- Εξετάστε τη δυνατότητα χρήσης εργαλείων συνεχούς διαχείρισης εξωτερικής επιφάνειας επίθεσης (External Attack Surface Management — EASM) ως συμπληρωματικό μέτρο μεταξύ ετήσιων ελέγχων παρείσδυσης. Πρόκειται για αυτοματοποιημένα εργαλεία που συνεχώς ανακαλύπτουν, παρακολουθούν και αναλύουν πληροφοριακά αγαθά που είναι εκτεθειμένα στο διαδίκτυο από τη σκοπιά του επιτιθέμενου, με δυνατότητα προσιτού κόστους υπηρεσιών για μικρομεσαίες επιχειρήσεις.

ΔΙΑΔΙΚΑΣΙΕΣ ΑΞΙΟΛΟΓΗΣΗΣ

- Εξέταση / επισκόπηση:
  - πολιτικών και διαδικασιών διενέργειας ελέγχων παρείσδυσης και διαχείρισης ευπαθειών,
  - συμβάσεων με αναδόχους που αφορούν σε διενέργεια ελέγχων παρείσδυσης,

- εκθέσεων αποτελεσμάτων πρόσφατων ελέγχων παρείσδυσης,
- σχεδίων αποκατάστασης ευπαθειών και τεκμηρίωσης διενέργειας επαναληπτικών ελέγχων.

- Διενέργεια συνέντευξης / συζήτησης με τον υπεύθυνο κυβερνοασφάλειας, καθώς και με στελέχη που έχουν την αρμοδιότητα διαχείρισης των ελέγχων παρείσδυσης και της παρακολούθησης της αποκατάστασης των ευπαθειών.

16. Φυσική ασφάλεια πληροφοριακών αγαθών

ΑΠΑΙΤΗΣΗ 16.1

Εφαρμόστε μέτρα φυσικής ασφάλειας για τον έλεγχο της πρόσβασης σε πληροφοριακά αγαθά, καθώς και στους χώρους που φιλοξενούν κρίσιμα πληροφοριακά συστήματα της επιχείρησης.

ΠΕΡΙΓΡΑΦΗ

Η κυβερνοασφάλεια δεν εξαντλείται στις ψηφιακές απειλές: η φυσική πρόσβαση σε εγκαταστάσεις και εξοπλισμό αποτελεί εξίσου κρίσιμη παράμετρο. Οι επιχειρήσεις οφείλουν να υλοποιούν μέτρα προστασίας και παρακολούθησης των πληροφοριακών τους αγαθών και, ιδίως, των χώρων που φιλοξενούν διακομιστές και ευαίσθητα δεδομένα, για την αποτροπή εισόδου μη εξουσιοδοτημένων ατόμων και την πρόληψη κακόβουλων ενεργειών, όπως, ενδεικτικά, την κλοπή συσκευών, τη μόλυνση συστημάτων με ειδικά διαμορφωμένο USB ή και το φυσικό βανδαλισμό κρίσιμου υλικού.

ΟΔΗΓΙΕΣ ΥΛΟΠΟΙΗΣΗΣ

- Ελέγξτε τη φυσική πρόσβαση στους χώρους όπου φιλοξενούνται τα κρίσιμα συστήματά σας (server rooms, racks δικτύου κ.α.) και ενισχύστε τη φυσική τους ασφάλεια. Για το σκοπό αυτό, υλοποιήστε μέτρα όπως:
  - χρήση έξυπνων καρτών (smartcards) για την είσοδο στους χώρους και άδεια εισόδου μόνο για το εξουσιοδοτημένο προσωπικό.
  - Χρήση κλειδαριών και συστημάτων συναγερμού.
  - Χρήση καμερών CCTV.
  - Ύπαρξη προσωπικού ασφαλείας.
  - Τήρηση ψηφιακού ή έγχαρτου αρχείου καταγραφής εισόδων για λόγους ιχνηλασιμότητας.
  - Περιοδική αξιολόγηση και αναθεώρηση των δικαιωμάτων φυσικής πρόσβασης σε κρίσιμες ζώνες για το προσωπικό της επιχείρησής σας, καθώς και για το προσωπικό προμηθευτών και παρόχων υπηρεσιών.
- Εφαρμόστε πολιτική «καθαρού γραφείου και καθαρής οθόνης» (clear desk / clear screen policy) για την αποφυγή μη εξουσιοδοτημένης πρόσβασης, απώλειας ή καταστροφής δεδομένων σε γραφεία και οθόνες εργαζομένων:
  - Οι εργαζόμενοι κλειδώνουν σε κατάλληλο σημείο έγγραφα ή φορητά μέσα (USB ή εξωτερικούς σκληρούς δίσκους) που περιέχουν ευαίσθητα επιχειρηματικά δεδομένα, όταν αυτά δεν απαιτούνται άμεσα και, ιδίως, κατά τη λήξη της εργάσιμης ημέρας.
  - Οι εργαζόμενοι κλειδώνουν την οθόνη του υπολογιστή τους όταν απομακρύνονται προσωρινά από τη θέση εργασίας (π.χ. με την εντολή Windows Key + L).

ΔΙΑΔΙΚΑΣΙΕΣ ΑΞΙΟΛΟΓΗΣΗΣ

- Εξέταση / επισκόπηση / παρατήρηση:
  - πολιτικών και διαδικασιών που αφορούν στη φυσική ασφάλεια εξοπλισμού και εγκαταστάσεων,
  - μηχανισμών ελέγχου πρόσβασης στο server room.
- Διενέργεια συνέντευξης / συζήτησης με τον υπεύθυνο κυβερνοασφάλειας, καθώς και με μέλη του προσωπικού με αρμοδιότητα τη φυσική ασφάλεια εξοπλισμού και εγκαταστάσεων.

ΑΠΑΙΤΗΣΗ 16.2

Εφαρμόστε μέτρα που διασφαλίζουν τη συνεχή και αδιάλειπτη λειτουργία των κρίσιμων πληροφοριακών συστημάτων της επιχείρησης, καθώς και μέτρα προστασίας τους από φυσικές και περιβαλλοντικές απειλές.

ΠΕΡΙΓΡΑΦΗ

- Τα υποστηρικτικά μέσα που διασφαλίζουν τη συνεχή και αδιάλειπτη λειτουργία των πληροφοριακών συστημάτων περιλαμβάνουν την παροχή ηλεκτρικού ρεύματος, την παροχή νερού για την ψύξη των διακομιστών, το φυσικό αέριο για την παροχή θερμότητας ή ως backup γεννήτρια ηλεκτρικού ρεύματος, τα συστήματα HVAC (Heating, Ventilation and Air Conditioning), καθώς και τα συστήματα τηλεπικοινωνιών (διαδίκτυο και συνδεσιμότητα δικτύου). Οι φυσικές και περιβαλλοντικές απειλές περιλαμβάνουν τις πυρκαγιές, τις πλημμύρες, φυσικά φαινόμενα όπως είναι οι σεισμοί, τη μη εξουσιοδοτημένη πρόσβαση, κλοπή και φυσική βία, τα επικίνδυνα υλικά, καθώς και μακροπρόθεσμες περιβαλλοντικές μεταβολές όπως είναι η κλιματική αλλαγή ή η μόλυνση του αέρα.

ΟΔΗΓΙΕΣ ΥΛΟΠΟΙΗΣΗΣ

- Υλοποιείστε μέτρα διασφάλισης της συνεχούς και αδιάλειπτης λειτουργίας των πληροφοριακών σας συστημάτων, όπως ενδεικτικά:
  - συστήματα UPS (uninterruptible power supply),
  - γεννήτριες παροχής ρεύματος,
  - ενεργητική / παθητική ψύξη,
  - πλεονασμό (redundancy) σε εξοπλισμό συστημάτων και δικτύωσης.
- Υλοποιήστε μέτρα για την προστασία των κρίσιμων πληροφοριακών σας συστημάτων έναντι φυσικών και περιβαλλοντικών απειλών, όπως ενδεικτικά:
  - συστήματα πυρανίχνευσης και πυρόσβεσης,
  - συστήματα ελέγχου θερμοκρασίας, υγρασίας και πίεσης,
  - Συστήματα ανίχνευσης διαρροής νερού,
  - μέριμνα για αύξηση του προσωπικού ασφαλείας σε περιπτώσεις απειλών βίας.

ΔΙΑΔΙΚΑΣΙΕΣ ΑΞΙΟΛΟΓΗΣΗΣ

- Εξέταση / επισκόπηση / παρατήρηση:
  - πολιτικών και διαδικασιών που αφορούν στη φυσική ασφάλεια εξοπλισμού και εγκαταστάσεων,
  - μηχανισμών διασφάλισης της συνεχούς και αδιάλειπτης λειτουργίας των πληροφοριακών συστημάτων,
  - μέτρων προστασίας των κρίσιμων πληροφοριακών συστημάτων έναντι φυσικών και περιβαλλοντικών απειλών.
- Διενέργεια συνέντευξης / συζήτησης με τον υπεύθυνο κυβερνοασφάλειας, καθώς και με μέλη του προσωπικού με αρμοδιότητα τη φυσική ασφάλεια εξοπλισμού και εγκαταστάσεων.

17. Ασφαλής χρήση Τεχνητής Νοημοσύνης

ΑΠΑΙΤΗΣΗ 17.1

Καθορίστε σαφές πλαίσιο χρήσης εργαλείων τεχνητής νοημοσύνης εντός της επιχείρησης, ώστε να αξιοποιούνται τα οφέλη τους με ελεγχόμενο τρόπο και να περιορίζονται οι κίνδυνοι που προέρχονται από λανθασμένες ή και κακόβουλες ενέργειες.

ΠΕΡΙΓΡΑΦΗ

- Η ραγδαία υιοθέτηση εργαλείων Τεχνητής Νοημοσύνης (AI) από τους εργαζόμενους, ενώ βελτιώνει την παραγωγικότητα, εισάγει νέους κινδύνους για τις μικρομεσαίες επιχειρήσεις: ακούσια διαρροή εμπιστευτικών και ευαίσθητων δεδομένων (στοιχεία πελατών, βιομηχανικά μυστικά, passwords κ.α.) μέσω prompts σε ανοικτές υπηρεσίες ΤΝ, χρήση μη εγκεκριμένων εφαρμογών (shadow AI) που δεν επιβλέπονται από το τμήμα πληροφορικής, καθώς και κίνδυνοι εξαγωγής αναξιόπιστων αποτελεσμάτων (“hallucinations”) που ενδέχεται να ενσωματωθούν σε επίσημα έγγραφα ή σε παραδοτέα προς πελάτες. Επιπλέον, η ανάδυση “πρακτόρων τεχνητής νοημοσύνης” (agentic AI) πολλαπλασιάζει τους κινδύνους, καθώς οι εν λόγω τεχνολογίες έχουν τη δυνατότητα εκτέλεσης αυτόνομων ενεργειών στα υπολογιστικά συστήματα των επιχειρήσεων χωρίς ανθρώπινη παρέμβαση και έλεγχο.
- Οι εφαρμογές τεχνητής νοημοσύνης εκτίθενται, πλέον, σε σύγχρονες τεχνικές κυβερνοεπιθέσεων, όπως ενδεικτικά: prompt injection, όπου εισάγεται περιεχόμενο σε ένα μοντέλο που τροποποιεί τη συμπεριφορά του με τρόπους που δεν είχαν αρχικά προβλεφθεί, καθώς και εκμετάλλευση αδύναμων ρυθμίσεων στα δικαιώματα των AI agents, με αποτέλεσμα αυτά να παρακάμπτουν μέτρα ασφάλειας και να αποκτούν πρόσβαση σε εμπιστευτικά και ευαίσθητα εταιρικά αρχεία. Για τους παραπάνω λόγους, οι επιχειρήσεις πρέπει να εφαρμόζουν κατάλληλες πολιτικές που θα ελέγχουν τι δεδομένα μπορεί να “δει” η τεχνητή νοημοσύνη, σε τι συστήματα μπορεί να συνδέεται και, κυρίως, τι ενέργειες μπορεί να εκτελεί.

ΟΔΗΓΙΕΣ ΥΛΟΠΟΙΗΣΗΣ

- Εκπονήστε σύντομη πολιτική αποδεκτής χρήσης τεχνητής νοημοσύνης που να καθορίζει, μεταξύ άλλων: ποια εργαλεία AI είναι εγκεκριμένα, ποιες κατηγορίες δεδομένων απαγορεύεται να εισαχθούν σε δημόσια μοντέλα (π.χ. προσωπικά δεδομένα, οικονομικά στοιχεία, εμπορικά μυστικά, διαπιστευτήρια, πηγαίος κώδικας κ.α.), ποιοι είναι οι κανόνες για τη σύνδεση εργαλείων AI με εταιρικά συστήματα, καθώς και ποιες είναι οι απαιτήσεις για τον ανθρώπινο έλεγχο και την τεκμηρίωση του περιεχομένου που παράγεται από AI και οδηγεί σε επίσημες αποφάσεις της επιχείρησης.
- Καταγράψτε στο μητρώο πληροφοριακών αγαθών τις εφαρμογές AI που χρησιμοποιεί επίσημα η επιχείρησή σας (όπως μοντέλα, πράκτορες, σύνολα δεδομένων, MCP διακομιστές κ.α.), ποιος είναι ο ιδιοκτήτης τους (owner) και με ποια εταιρικά σας συστήματα αλληλεπιδρούν (περιβάλλοντα ανάπτυξης εφαρμογών, παραγωγικά συστήματα, cloud, υπολογιστές χρηστών κ.α.).

- Ταξινομήστε τα συστήματα AI που χρησιμοποιείτε στην επιχείρησή σας ανάλογα με τον κίνδυνο (risk). Για το σκοπό αυτό συμβουλευτείτε την κατηγοριοποίηση του Ευρωπαϊκού Κανονισμού 2024/1689 (AI Act) και εξετάστε τις υποχρεώσεις σας που προκύπτουν από την εφαρμογή του.
- Στην περίπτωση που παρέχετε εργαλεία AI ως υπηρεσία σε πελάτες (π.χ. chatbots), διασφαλίστε ότι παρέχεται σαφής ενημέρωση ότι αλληλεπιδρούν με σύστημα AI, σύμφωνα με τις απαιτήσεις διαφάνειας του Ευρωπαϊκού Κανονισμού 2024/1689 (AI Act).
- Υλοποιείστε μέτρα περιορισμού των κινδύνων από τη χρήση εργαλείων παραγωγικής τεχνητής νοημοσύνης (generative AI):
    - Εκπαιδεύστε το προσωπικό σας να μην εισάγει προσωπικά δεδομένα, οικονομικά στοιχεία, εμπορικά μυστικά, διαπιστευτήρια, ιδιόκτητο πηγαίο κώδικα κ.α. σε δημόσια δωρεάν μοντέλα AI.
    - Εξετάστε τη σύναψη συνδρομών (enterprise subscriptions) σε εργαλεία AI που προσφέρουν υπηρεσίες διαχείρισης ταυτότητας, καταγραφής ενεργειών, προστασία δεδομένων από απώλεια, καθώς και εταιρικές εγγυήσεις ότι τα δεδομένα σας δεν θα χρησιμοποιηθούν για την εκπαίδευση δημόσιων μοντέλων AI.
    - Επιβάλλετε την επαλήθευση από ανθρώπους της ορθότητας του περιεχομένου που παράγεται από εργαλεία AI και που θα χρησιμοποιηθεί επίσημα από την επιχείρησή σας (human-in-the-loop policy). Περιεχόμενο, όπως εταιρικά συμβόλαια, έγγραφα, πηγαίος κώδικας κ.λπ. πρέπει να εξετάζονται προσεκτικά ως την ορθότητά τους πριν ενσωματωθούν σε επίσημες αποφάσεις ή σε παραδοτέα προς πελάτες.
- Υλοποιείστε μέτρα περιορισμού των κινδύνων από τη χρήση πρακτόρων τεχνητής νοημοσύνης (agentic AI):
    - Εφαρμόστε την αρχή των ελάχιστων προνομίων (least privilege): οι πράκτορες τεχνητής νοημοσύνης πρέπει να έχουν τα ελάχιστα δικαιώματα πρόσβασης και προνόμια που απαιτούνται για την εκτέλεση των συγκεκριμένων εργασιών.
    - Επιβάλλετε την παρέμβαση του ανθρώπινου παράγοντα (human-in-the-loop) για την επικύρωση εκτέλεσης κρίσιμων ενεργειών, π.χ. πραγματοποίηση οικονομικών συναλλαγών, διαγραφή αρχείων, τροποποίηση συμβολαίων πελατών κ.α.
    - Παρακολουθείστε το κόστος χρήσης των πρακτόρων τεχνητής νοημοσύνης ως δείκτη κανονικής λειτουργίας: περιπτώσεις ξαφνικής και ανεξήγητης αύξησης του κόστους ενδέχεται να υποδηλώνουν κατάχρηση κλειδιών API ή ανεξέλεγκτες αυτοματοποιημένες ενέργειες.
- Διενεργήστε εκπαίδευση των χρηστών σας στην ασφαλή χρήση των εργαλείων τεχνητής νοημοσύνης: τρόποι δημιουργίας ορθών κειμένων εισόδου (prompt engineering), τρόποι επαλήθευσης παραγόμενου περιεχομένου, καθώς και κατανόηση των σημαντικότερων κινδύνων κυβερνοασφάλειας για τα εργαλεία AI (όπως prompt injection, εκτέλεση κακόβουλου κώδικα, deep fakes κ.α.).

ΔΙΑΔΙΚΑΣΙΕΣ ΑΞΙΟΛΟΓΗΣΗΣ

- Εξέταση / επισκόπηση πολιτικών και διαδικασιών χρήσης τεχνητής νοημοσύνης.
- Διενέργεια συνέντευξης / συζήτησης με μέλη της Διοίκησης, τον υπεύθυνο κυβερνοασφάλειας και χρήστες που αξιοποιούν εργαλεία ΤΝ στην καθημερινή τους εργασία.


ΕΘΝΙΚΗ ΑΡΧΗ
ΚΥΒΕΡΝΟ
ΑΣΦΑΛΕΙΑΣ