Example Advisory ΔΕΙΓΜΑ

Έκθεση αξιολόγησης κυβερνοασφάλειας

Kymora Logistics

Για	Kymora Logistics
Συντάχθηκε από	Example Advisory
Ημερομηνία	2 Νοεμβρίου 2026
Διαβάθμιση	Εμπιστευτικό

Περιεχόμενα

1. Σύνοψη για τη διοίκηση 3

2. Πεδίο και μέθοδος 4

3. Συμμόρφωση με τον Ν. 5160/2024 5

4. Ωριμότητα 8

5. Έκθεση στο διαδίκτυο 9

6. Εσωτερικό δίκτυο 11

7. Διακυβέρνηση 12

8. Κίνδυνος σε χρήμα 13

9. Οδικός χάρτης 14

10. Περιορισμοί 19

11. Υπογραφές 20

1. Σύνοψη για τη διοίκηση

Διαδρομές επίθεσης για άμεση διόρθωση

- **Διαδρομή κατάληψης λογαριασμού** (κρίσιμη σοβαρότητα συνολικά, από ευρήματα με υψηλή σοβαρότητα). 1 εκτεθειμένο διαπιστευτήριο στο example.com, και ένα σημείο VPN στο vpn.example.com. Ο μισθωτής Microsoft 365 δεν επιβάλλει δεύτερο παράγοντα. Η υπηρεσία είναι απομακρυσμένης πρόσβασης, οπότε ένα διαπιστευτήριο που ισχύει είναι συνεδρία στον κόμβο.

Η ανάλυση κενών ΕΑΚ βρίσκεται σε συμμόρφωση 49,4%, με εκτίμηση Υψηλός Κίνδυνος κατά τη μέθοδο της Αρχής.

Η αξιολόγηση ωριμότητας με βάση το πλαίσιο NIS2 Άρθρο 21(2) έχει μέσο όρο 2,1 στα 5, με στόχο το 3.

Ο βαθμός έκθεσης των συστημάτων που είναι προσβάσιμα από το διαδίκτυο είναι 4,1 στα 10 (Χαμηλός). Ενεργά ευρήματα: 0 κρίσιμα και 2 υψηλά.

Πολιτικές της ΚΥΑ 1689/2025 που είναι εγκεκριμένες και εντός της ημερομηνίας επανεξέτασής τους: 6 από 12.

Το ποσοτικοποιημένο μητρώο κινδύνων εκτιμά αναμενόμενη απώλεια 183.900 € ανά έτος.

Ο οδικός χάρτης περιλαμβάνει 39 ενέργειες, 12 υψηλής προτεραιότητας.

Από τα 143 κενά ΕΑΚ, ο οδικός χάρτης περιλαμβάνει τα 15 μεγαλύτερα. Τα υπόλοιπα βρίσκονται στο αρχείο της ανάλυσης κενών.

2. Πεδίο και μέθοδος

Δεν έχει καταγραφεί δήλωση πεδίου εφαρμογής του ΣΔΑΠ.

Τομείς στο πεδίο: example.com, example.net.

Μέθοδος

- Η ανάλυση κενών της ΕΑΚ, απαντημένη από τον οργανισμό μαζί με τον σύμβουλό του και βαθμολογημένη με την τεκμηριωμένη μέθοδο της Αρχής.
- Αξιολόγηση ωριμότητας με βάση το πλαίσιο NIS2 Άρθρο 21(2), με κάθε στοιχείο απαντημένο σε κλίμακα 0 έως 5.
- Αυτοματοποιημένη παρακολούθηση από το Vardion των συστημάτων που είναι προσβάσιμα από το διαδίκτυο, σε διευθύνσεις που ενέκρινε ο οργανισμός.
- Το εσωτερικό δίκτυο, από την απογραφή των υπολογιστών, τους ελέγχους διαμόρφωσης και τυχόν εσωτερική σάρωση, βαθμολογημένο στη δική του κλίμακα.
- Τα αρχεία του ΣΔΑΠ του οργανισμού: το ευρετήριο πολιτικών, ο υπεύθυνος ασφάλειας, το πρόγραμμα και το μητρώο κινδύνων.

3. Συμμόρφωση με τον Ν. 5160/2024

Ανάλυση κενών ΕΑΚ: απαντήθηκαν 169 από 169 μέτρα. Σημαντική οντότητα.

ΣΥΜΜΟΡΦΩΣΗ	ΕΠΙΠΕΔΟ ΚΙΝΔΥΝΟΥ
49,4%	**Υψηλός Κίνδυνος**

ΕΝΟΤΗΤΑ	ΣΥΜΜΟΡΦΩΣΗ	ΕΠΙΠΕΔΟ ΚΙΝΔΥΝΟΥ
1. Υποχρεώσεις & Ευθύνη των Ανωτάτων Οργάνων Διοίκησης	50,0%	Υψηλός Κίνδυνος
2. Πλαίσιο Διαχείρισης Κινδύνων	38,2%	Υψηλός Κίνδυνος
3. Πολιτικές και Διαδικασίες Ασφάλειας Πληροφοριών	60,7%	Μέτριος Κίνδυνος
4. Ρόλοι, Αρμοδιότητες και Εξουσίες	64,5%	Μέτριος Κίνδυνος
5. Ανεξάρτητος Έλεγχος Ασφάλειας Πληροφοριών	12,5%	Κρίσιμος Κίνδυνος
6. Διαδικασίες Παρακολούθησης της Συμμόρφωσης	42,9%	Υψηλός Κίνδυνος
7. Ασφάλεια Ανθρώπινου Δυναμικού	56,7%	Μέτριος Κίνδυνος
8. Διαχείριση Υλικού και Λογισμικού	56,3%	Μέτριος Κίνδυνος
9. Διαχείριση Ασφάλειας Αλυσίδας Εφοδιασμού	47,7%	Υψηλός Κίνδυνος
10. Διαχείριση Ταυτότητας, Αυθεντικοποίηση και Έλεγχος Πρόσβασης	70,5%	Μέτριος Κίνδυνος
11. Ασφαλής Παραμετροποίηση Υλικού, Λογισμικού, Υπηρεσιών και Δικτύων	60,9%	Μέτριος Κίνδυνος
12. Αρχές Ασφαλούς Ανάπτυξης Εφαρμογών	48,9%	Υψηλός Κίνδυνος
13. Διαχείριση Αλλαγών	32,4%	Υψηλός Κίνδυνος
14. Διαχείριση και Γνωστοποίηση Ευπαθειών	51,3%	Μέτριος Κίνδυνος
15. Αξιολόγηση της Αποτελεσματικότητας των Μέτρων Διαχείρισης Κινδύνων Κυβερνοασφάλειας	37,5%	Υψηλός Κίνδυνος
16. Ασφάλεια Δικτύων, Υποδομών και Υπηρεσιών Νέφους	40,8%	Υψηλός Κίνδυνος
17. Προστασία από Κακόβουλο Λογισμικό	68,8%	Μέτριος Κίνδυνος
18. Εκπαίδευση και Ευαισθητοποίηση σε Θέματα Κυβερνοασφάλειας	50,0%	Υψηλός Κίνδυνος
19. Χρήση Κρυπτογραφίας	42,4%	Υψηλός Κίνδυνος
20. Φυσική & Περιβαλλοντική Ασφάλεια	57,6%	Μέτριος Κίνδυνος
21. Διαχείριση Περιστατικών Ασφάλειας & Υποχρεώσεις Αναφοράς	39,9%	Υψηλός Κίνδυνος
22. Ασφάλεια Τεχνητής Νοημοσύνης (AI Security)	Δεν εφαρμόζεται	

ΕΝΟΤΗΤΑ	ΣΥΜΜΟΡΦΩΣΗ	ΕΠΙΠΕΔΟ ΚΙΝΔΥΝΟΥ
23. Ασφάλεια Λειτουργικής Τεχνολογίας, Διαδικτύου των Πραγμάτων και Ιατρικών Συσκευών (OT, IoT, IoMT Security)	31,3%	Υψηλός Κίνδυνος
24. Επιχειρησιακή Συνέχεια και Διαχείριση Κρίσεων	61,4%	Μέτριος Κίνδυνος

Μεγαλύτερα κενά

ΜΕΤΡΟ	ΥΛΟΠΟΙΗΣΗ	ΜΟΝΑΔΕΣ ΠΟΥ ΛΕΙΠΟΥΝ
5.3 Εφόσον από τα αποτελέσματα του ανεξάρτητου ελέγχου προκύψει ανεπαρκής υλοποίηση των απαραίτητων τεχνικών, οργανωτικών και επιχειρησιακών μέτρων κυβερνοασφάλειας, το ανώτατο όργανο διοίκησης της οντότητας εκκινεί διαδικασίες διορθωτικών ενεργειών.	Δεν έχει ξεκινήσει	5,00
5.4 Οι ανεξάρτητοι έλεγχοι διενεργούνται σε προγραμματισμένα χρονικά διαστήματα, καθώς και όταν λαμβάνουν χώρα σοβαρά περιστατικά κυβερνοασφάλειας ή σημαντικές αλλαγές στις λειτουργίες της οντότητας ή εφόσον έχει μεταβληθεί το τρέχον διεθνές περιβάλλον κυβερνοαπειλών.	Δεν έχει ξεκινήσει	5,00
15.3 Η οντότητα υλοποιεί διαδικασίες αποκατάστασης των ελλείψεων που διαπιστώνονται στους εξωτερικούς ελέγχους παρείσδυσης, καθώς και διαδικασίες επικύρωσης των διορθωτικών μέτρων, με βάση συγκεκριμένο πλάνο προτεραιοποίησης, λαμβάνοντας υπόψη την κρισιμότητα των ευρημάτων.	Δεν έχει ξεκινήσει	5,00
21.11 Η οντότητα διασφαλίζει τακτικά (προτείνεται ετησίως) ότι στην υπηρεσία SOC περιλαμβάνονται το σύνολο των συστημάτων και των υποδομών.	Δεν έχει ξεκινήσει	5,00
23.4 Η οντότητα χρησιμοποιεί τεχνολογίες παρακολούθησης για την ανίχνευση ανωμαλιών, απειλών και επιθέσεων στις εξειδικευμένες υποδομές της.	Δεν έχει ξεκινήσει	5,00
24.5 Η οντότητα έχει υλοποιήσει εναλλακτικό τοποθεσία (Disaster Recovery Site) για όλες τις κρίσιμες υποδομές, λαμβάνοντας υπόψη τα αποτελέσματα της Ανάλυσης Επιχειρηματικών Επιπτώσεων (Business Impact Analysis - BIA). Η επιλογή των συστημάτων που υποστηρίζονται στο DR Site βασίζεται σε προκαθορισμένους δείκτες: Στόχο Σημείου Ανάκαμψης (Recovery Point Objective - RPO), Χρόνο Ανάκτησης (Recovery Time Objective - RTO) και Μέγιστο Ανεκτό Διάστημα Διακοπής (Maximum Tolerable Period of Disruption - MTPD) διασφαλίζοντας τη συνέχεια κρίσιμων επιχειρησιακών λειτουργιών σε περίπτωση σοβαρής διακοπής ή καταστροφής.	Δεν έχει ξεκινήσει	5,00
8.6 Η οντότητα εφαρμόζει ετικετοποίηση (labeling) όλων των αγαθών (υλικού και πληροφοριών), σύμφωνα με το σχήμα ταξινόμησης (classification scheme, π.χ., Δημόσια, Εσωτερικά, Εμπιστευτικά) των αγαθών και των δεδομένων.	Δεν έχει ξεκινήσει	4,00

ΜΕΤΡΟ	ΥΛΟΠΟΙΗΣΗ	ΜΟΝΑΔΕΣ ΠΟΥ ΛΕΙΠΟΥΝ
13.4 Οι διαδικασίες διαχείρισης αλλαγών αξιολογούνται και επικαιροποιούνται σε περιοδική βάση (προτείνεται ετησίως), καθώς και όταν λαμβάνουν χώρα σοβαρά περιστατικά κυβερνοασφάλειας ή σημαντικές αλλαγές στις λειτουργίες της οντότητας.	Δεν έχει ξεκινήσει	4,00
16.1.10 Η οντότητα εφαρμόζει φιλτράρισμα της δικτυακής κίνησης μεταξύ των διακριτών υποδικτύων, με βάση τις απαιτήσεις ασφάλειας κάθε ζώνης.	Δεν έχει ξεκινήσει	4,00
16.1.12 Οι πολιτικές και διαδικασίες που αφορούν στην ασφάλεια δικτύων αξιολογούνται και, κατά περίπτωση, επικαιροποιούνται τακτικά σε προγραμματισμένα χρονικά διαστήματα (προτείνεται σε ετήσια βάση), καθώς και όταν λαμβάνουν χώρα σοβαρά περιστατικά κυβερνοασφάλειας ή σημαντικές αλλαγές στις λειτουργίες της οντότητας ή εφόσον έχει μεταβληθεί το τρέχον διεθνές περιβάλλον κυβερνοαπειλών.	Δεν έχει ξεκινήσει	4,00

Το Vardion υπολογίζει αυτή τη βαθμολογία από τις απαντήσεις σας με τη μέθοδο που δημοσιεύει η Αρχή. Δεν αποτελεί κρίση της Αρχής ούτε νομική συμβουλή.

Πηγή: Εθνική Αρχή Κυβερνοασφάλειας, Υπόδειγμα εργαλείου gap analysis για τη συμμόρφωση με τον ν. 5160/2024 (Οδηγία NIS2), Σεπτέμβριος 2025, cyber.gov.gr, άδεια CC BY-ND 4.0.

4. Ωριμότητα

Μέτρα NIS2: αξιολόγηση με βάση το πλαίσιο NIS2 Άρθρο 21(2), με στόχο το επίπεδο 3.

ΤΟΜΕΑΣ	ΒΑΘΜΟΣ	ΣΤΟΧΟΣ	ΑΠΑΝΤΗΘΗΚΑΝ
Άρθρο 21 παράγραφος 2	2,1	3,0	10/10

Μεγαλύτερα κενά

ΣΤΟΙΧΕΙΟ	ΕΠΙΠΕΔΟ	ΣΤΟΧΟΣ
21.2.c Επιχειρησιακή συνέχεια, όπως διαχείριση αντιγράφων ασφαλείας και αποκατάσταση έπειτα από καταστροφή, και διαχείριση των κρίσεων	1	3
21.2.g Βασικές πρακτικές κυβερνοϋγιεινής και κατάρτιση στην κυβερνοασφάλεια	1	3
21.2.a Πολιτικές για την ανάλυση κινδύνου και την ασφάλεια των πληροφοριακών συστημάτων	2	3
21.2.d Ασφάλεια της αλυσίδας εφοδιασμού, συμπεριλαμβανομένων των σχετικών με την ασφάλεια πτυχών που αφορούν τις σχέσεις μεταξύ κάθε οντότητας και των άμεσων προμηθευτών ή παρόχων υπηρεσιών της	2	3
21.2.f Πολιτικές και διαδικασίες για την αξιολόγηση της αποτελεσματικότητας των μέτρων διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας	2	3
21.2.h Πολιτικές και διαδικασίες σχετικά με τη χρήση κρυπτογραφίας και, κατά περίπτωση, κρυπτογράφησης	2	3
21.2.j Χρήση λύσεων πολυπαραγοντικής επαλήθευσης ταυτότητας ή συνεχούς επαλήθευσης ταυτότητας, ασφαλών φωνητικών επικοινωνιών, επικοινωνιών βίντεο και κειμένου και ασφαλών συστημάτων επικοινωνιών έκτακτης ανάγκης εντός της οντότητας, κατά περίπτωση	2	3

5. Έκθεση στο διαδίκτυο

Από την τελευταία πλήρη σάρωση στις 2 Νοεμβρίου 2026 και τους ελέγχους που έγιναν από τότε.

ΒΑΘΜΟΣ ΕΚΘΕΣΗΣ	ΚΡΙΣΙΜΗ	ΥΨΗΛΗ	ΜΕΤΡΙΑ
4,1 Χαμηλός	0	2	2

ΧΑΜΗΛΗ	ΠΛΗΡΟΦΟΡΙΑΚΗ
3	3

Διαδρομή κατάληψης λογαριασμού: κρίσιμη σοβαρότητα συνολικά, γιατί τα ευρήματά της δίνουν πρόσβαση μόνο όταν συνδυάζονται. Καθένα αναφέρεται παρακάτω με τη δική του σοβαρότητα.

Εικόνα ανά τομέα

ΕΚΤΕΘΕΙΜΕΝΕΣ ΥΠΗΡΕΣΙΕΣ	ΕΝΗΜΕΡΩΣΕΙΣ	ΚΡΥΠΤΟΓΡΑΦΗΣΗ	ΠΑΡΑΜΕΤΡΟΠΟΙΗΣΗ WEB
A	A	C	B

ΗΛΕΚΤΡΟΝΙΚΟ ΤΑΧΥΔΡΟΜΕΙΟ	ΤΟΜΕΙΣ ΚΑΙ DNS	ΔΙΑΠΙΣΤΕΥΤΗΡΙΑ
A	C	D

Κάθε περιοχή βαθμολογείται με βάση τον κίνδυνο των ανοικτών ευρημάτων της: A κανένα ανοικτό, B χαμηλός, C μέτριος, D υψηλός και F κρίσιμος.

Αλλαγές που μειώνουν περισσότερο τον κίνδυνο

ΕΝΕΡΓΕΙΑ	ΠΟΥ	ΣΟΒΑΡΟΤΗΤΑ	ΕΥΡΗΜΑΤΑ
Επαναφέρετε τα διαπιστευτήρια του λογαριασμού που αναφέρει το εύρημα, ανακαλέστε τις ενεργές συνεδρίες του και επιβεβαιώστε ότι επιβάλλεται πολυπαραγοντική ταυτοποίηση στο σημείο σύνδεσης που αναφέρει.	vpn.example.com (τα στοιχεία φαίνονται στην κονσόλα, στο εύρημα F-33FE27B430)	Υψηλή	1
Ενεργοποιήστε τις προεπιλογές ασφάλειας, ή δημιουργήστε πολιτική πρόσβασης υπό όρους που απαιτεί έλεγχο ταυτότητας πολλαπλών παραγόντων για όλους τους χρήστες.	Μισθωτής Microsoft 365 example.com	Υψηλή	1
Επαναφέρετε τον κωδικό του λογαριασμού που αναφέρει το εύρημα και ανακαλέστε τις ενεργές συνεδρίες του.	example.com (τα στοιχεία φαίνονται στην κονσόλα, στο εύρημα F-258E45A9D5)	Μέτρια	1
Επανεκδώστε το πιστοποιητικό ώστε να καλύπτει τα ονόματα που σερβίρονται σε αυτή τη διεύθυνση, ή σερβίρετε το αντίστοιχο πιστοποιητικό για κάθε όνομα.	203.0.113.13	Μέτρια	1

ΕΝΕΡΓΕΙΑ	ΠΟΥ	ΣΟΒΑΡΟΤΗΤΑ	ΕΥΡΗΜΑΤΑ
Αφαιρέστε την έκδοση του προϊόντος από τις κεφαλίδες Server, X-Powered-By και X-AspNet-Version.	203.0.113.10, 203.0.113.11	Χαμηλή	2
Δημοσιεύστε εγγραφή CAA με τις αρχές πιστοποίησης που επιτρέπεται να εκδίδουν για τον τομέα.	example.com	Χαμηλή	1
Προσθέστε στις αποκρίσεις αυτής της υπηρεσίας τις κεφαλίδες ασφάλειας που αναφέρει το εύρημα.	203.0.113.10, 203.0.113.11	Πληροφοριακή	2
Περιορίστε αυτό το περιβάλλον διαχείρισης στις διευθύνσεις που το χρειάζονται, ή βάλτε το πίσω από το VPN.	vpn.example.com	Πληροφοριακή	1

6. Εσωτερικό δίκτυο

Αυτό καλύπτει το εσωτερικό δίκτυο, από την εσωτερική σάρωση της 12 Οκτωβρίου 2026, καταταγμένο όπως τα ευρήματα προς το διαδίκτυο και ποτέ αθροισμένο με αυτά.

ΒΑΘΜΟΣ ΕΚΘΕΣΗΣ	ΚΡΙΣΙΜΗ	ΥΨΗΛΗ	ΜΕΤΡΙΑ
0,9 Χαμηλός	**0**	**0**	**2**

ΧΑΜΗΛΗ	ΠΛΗΡΟΦΟΡΙΑΚΗ
0	**0**

Αλλαγές που μειώνουν περισσότερο τον κίνδυνο

ΕΝΕΡΓΕΙΑ	ΠΟΥ	ΣΟΒΑΡΟΤΗΤΑ	ΕΥΡΗΜΑΤΑ
Περιορίστε το 3389/tcp στους υπολογιστές που το χρειάζονται, με κανόνα τείχους προστασίας ή ξεχωριστό τμήμα δικτύου.	192.168.10.31	Μέτρια	1
Περιορίστε το 445/tcp στους υπολογιστές που το χρειάζονται, με κανόνα τείχους προστασίας ή ξεχωριστό τμήμα δικτύου.	192.168.10.20	Μέτρια	1

7. Διακυβέρνηση

Πολιτικές της ΚΥΑ 1689/2025 που υπάρχουν στο ευρετήριο πολιτικών και είναι επίκαιρες: 6 από 12. Οι υπόλοιπες αναφέρονται παρακάτω, με την κατάσταση της καθεμίας.

ΠΟΛΙΤΙΚΗ	ΚΑΤΑΣΤΑΣΗ
Πολιτική αποδεκτής χρήσης	Καθυστερεί η επανεξέταση
Πολιτική αφαιρούμενων μέσων	Λείπει
Πολιτική ασφάλειας της εφοδιαστικής αλυσίδας	Λείπει
Πολιτική δοκιμών ασφάλειας	Λείπει
Πολιτική κρυπτογραφίας	Λείπει
Πολιτική φυσικής και περιβαλλοντικής ασφάλειας	Λείπει

Υπεύθυνος ασφάλειας: Νίκος Γεωργίου, με αναφορά σε Διευθύνουσα σύμβουλος.

Η τελευταία ανασκόπηση από τη διοίκηση έγινε στις 9 Αυγούστου 2026.

Οι παρακάτω υποχρεώσεις του προγράμματος καθυστερούν ή δεν έχουν γίνει ποτέ.

- Εκστρατεία ευαισθητοποίησης στην ασφάλεια
- Επανεξέταση προνομιακών προσβάσεων
- Επανεξέταση κρίσιμων προμηθευτών

8. Κίνδυνος σε χρήμα

ΑΝΑΜΕΝΟΜΕΝΗ ΑΠΩΛΕΙΑ ΑΝΑ ΕΤΟΣ	ΕΝΑ ΕΤΟΣ ΣΤΑ ΔΕΚΑ
183.900 €	**693.000 €**

1. Λογισμικό λύτρων σταματά τη διεκπεραίωση αποστολών 153.800 € ανά έτος
2. Κλοπή δεδομένων πελατών από την πύλη 30.100 € ανά έτος

Εκτίμηση που προσομοιώθηκε από εύρη που καταχωρίστηκαν από officer, με τελευταία αλλαγή στις 8 Σεπτεμβρίου 2026. Είναι κρίση, όχι μέτρηση.

9. Οδικός χάρτης

Μια ενέργεια κρατά την προτεραιότητα που ορίσατε. Διαφορετικά προκύπτει από την πηγή: σοβαρότητα για τεχνική αλλαγή, μονάδες που λείπουν για μέτρο ΕΑΚ, επίπεδα που λείπουν για στοιχείο ωριμότητας.

Μια ενέργεια χωρίς υπεύθυνο ανατίθεται στον υπεύθυνο ασφάλειας. Μια ενέργεια χωρίς ημερομηνία οφείλεται έως την προθεσμία των ευρημάτων που κλείνει, αλλιώς μέσα σε 30 ημέρες στην υψηλή προτεραιότητα, 90 στη μεσαία και 180 στη χαμηλή. Μια ημερομηνία που έχει περάσει εμφανίζεται ως η ημερομηνία της έκθεσης, μαζί με την ημερομηνία που όφειλε.

Από τα 143 κενά ΕΑΚ, ο οδικός χάρτης περιλαμβάνει τα 15 μεγαλύτερα. Τα υπόλοιπα βρίσκονται στο αρχείο της ανάλυσης κενών.

#	ΕΝΕΡΓΕΙΑ	ΠΗΓΗ	ΠΡΟΤΕΡΑΙΟΤΗΤΑ	ΥΠΕΥΘΥΝΟΣ	ΠΡΟΘΕΣΜΙΑ
1	Κάλυψη του κενού στο μέτρο ΕΑΚ 21.11: Η οντότητα διασφαλίζει τακτικά (προτείνεται ετησίως) ότι στην υπηρεσία SOC περιλαμβάνονται το σύνολο των συστημάτων και των υποδομών.	ΕΑΚ 21.11	Υψηλή	Υπεύθυνος ασφάλειας	1 Ιανουαρίου 2027
2	Ολοκλήρωση και δοκιμή του σχεδίου επιχειρησιακής συνέχειας και τήρηση δοκιμασμένων αντιγράφων ασφαλείας των κρίσιμων συστημάτων.	ΕΑΚ 24.5	Υψηλή	Υπεύθυνος πληροφορικής	2 Δεκεμβρίου 2026
3	Σύνταξη της διαδικασίας διαχείρισης αλλαγών και έγκρισή της.	ΕΑΚ 13.4	Υψηλή	Υπεύθυνος πληροφορικής	17 Δεκεμβρίου 2026
4	Κάλυψη του κενού στο μέτρο ΕΑΚ 21.9: Η οντότητα διασφαλίζει την αποτελεσματική λειτουργία του Κέντρου Επιχειρήσεων Ασφαλείας (SOC) μέσω της αξιοποίησης σύγχρονων Συστημάτων Διαχείρισης Πληροφοριών και Συμβάντων Ασφαλείας (SIEM), Ορχήστρωσης και Αυτοματοποιημένης Απόκρισης (SOAR) ή/και Εκτεταμένης Ανίχνευσης και Απόκρισης (XDR), με στόχο την αυτοματοποίηση διαδικασιών και την ταχεία απόκριση σε περιστατικά ασφαλείας σε πραγματικό χρόνο.	ΕΑΚ 21.9	Υψηλή	Υπεύθυνος ασφάλειας	1 Ιανουαρίου 2027
5	Προγραμματισμός εκπαίδευσης κυβερνοασφάλειας για το ανώτατο όργανο διοίκησης και ενημέρωσης για όλο το προσωπικό.	ΕΑΚ 1.6	Υψηλή	Διευθύνουσα σύμβουλος	1 Ιανουαρίου 2027
6	Σύνταξη του σχεδίου αντιμετώπισης κινδύνων και έγκρισή του από τη διευθύνουσα σύμβουλο.	ΕΑΚ 2.3	Υψηλή	Υπεύθυνος ασφάλειας	17 Δεκεμβρίου 2026

#	ΕΝΕΡΓΕΙΑ	ΠΗΓΗ	ΠΡΟΤΕΡΑΙΟΤΗΤΑ	ΥΠΕΥΘΥΝΟΣ	ΠΡΟΘΕΣΜΙΑ
7	Άνοδος στο επίπεδο 3: 21.2.c Επιχειρησιακή συνέχεια, όπως διαχείριση αντιγράφων ασφαλείας και αποκατάσταση έπειτα από καταστροφή, και διαχείριση των κρίσεων	Ωριμότητα	Υψηλή	Υπεύθυνος ασφάλειας	2 Δεκεμβρίου 2026
8	Άνοδος στο επίπεδο 3: 21.2.g Βασικές πρακτικές κυβερνοϋγιεινής και κατάρτιση στην κυβερνοασφάλεια	Ωριμότητα	Υψηλή	Υπεύθυνος ασφάλειας	2 Δεκεμβρίου 2026
9	Επαναφέρετε τα διαπιστευτήρια του λογαριασμού που αναφέρει το εύρημα, ανακαλέστε τις ενεργές συνεδρίες του και επιβεβαιώστε ότι επιβάλλεται πολυπαραγοντική ταυτοποίηση στο σημείο σύνδεσης που αναφέρει. Πού: vpn.example.com (τα στοιχεία φαίνονται στην κονσόλα, στο εύρημα F-33FE27B430)	Τεχνικό	Υψηλή	Υπεύθυνος ασφάλειας	26 Νοεμβρίου 2026
10	Ενεργοποιήστε τις προεπιλογές ασφάλειας, ή δημιουργήστε πολιτική πρόσβασης υπό όρους που απαιτεί έλεγχο ταυτότητας πολλαπλών παραγόντων για όλους τους χρήστες. Πού: Μισθωτής Microsoft 365 example.com	Τεχνικό	Υψηλή	Υπεύθυνος πληροφορικής	27 Νοεμβρίου 2026
11	Ολοκλήρωση της εκπρόθεσμης υποχρέωσης: Εκστρατεία ευαισθητοποίησης στην ασφάλεια Εκπρόθεσμη από τις 4 Οκτωβρίου 2026	Πρόγραμμα	Υψηλή	Ανθρώπινο δυναμικό	2 Νοεμβρίου 2026
12	Ολοκλήρωση της εκπρόθεσμης υποχρέωσης: Επανεξέταση προνομιακών προσβάσεων Εκπρόθεσμη από τις 24 Οκτωβρίου 2026	Πρόγραμμα	Υψηλή	Υπεύθυνος πληροφορικής	2 Νοεμβρίου 2026
13	Ανάθεση σε ανεξάρτητο ελεγκτή και ορισμός χρονοδιαγράμματος ελέγχων.	ΕΑΚ 5.3, 5.4, 5.1	Μέτρια	Διευθύνουσα σύμβουλος	31 Ιανουαρίου 2027
14	Προγραμματισμός της ετήσιας δοκιμής ασφάλειας και της ετήσιας αυτοαξιολόγησης.	ΕΑΚ 15.3	Μέτρια	Υπεύθυνος ασφάλειας	1 Ιανουαρίου 2027
15	Καταγραφή των σαρωτών και των καμερών της αποθήκης, μεταφορά τους σε δικό τους δίκτυο και παρακολούθησή του.	ΕΑΚ 23.4	Μέτρια	Υπεύθυνος πληροφορικής	2 Μαρτίου 2027
16	Σήμανση των στοιχείων του μητρώου και παρακολούθηση της χωρητικότητας των κρίσιμων συστημάτων.	ΕΑΚ 8.6	Μέτρια	Υπεύθυνος πληροφορικής	2 Μαρτίου 2027

#	ΕΝΕΡΓΕΙΑ	ΠΗΓΗ	ΠΡΟΤΕΡΑΙΟΤΗΤΑ	ΥΠΕΥΘΥΝΟΣ	ΠΡΟΘΕΣΜΙΑ
17	Κάλυψη του κενού στο μέτρο ΕΑΚ 16.1.10: Η οντότητα εφαρμόζει φιλτράρισμα της δικτυακής κίνησης μεταξύ των διακριτών υποδικτύων, με βάση τις απαιτήσεις ασφάλειας κάθε ζώνης.	ΕΑΚ 16.1.10	Μέτρια	Υπεύθυνος πληροφορικής	31 Ιανουαρίου 2027
18	Κάλυψη του κενού στο μέτρο ΕΑΚ 16.1.12: Οι πολιτικές και διαδικασίες που αφορούν στην ασφάλεια δικτύων αξιολογούνται και, κατά περίπτωση, επικαιροποιούνται τακτικά σε προγραμματισμένα χρονικά διαστήματα (προτείνεται σε ετήσια βάση), καθώς και όταν λαμβάνουν χώρα σοβαρά περιστατικά κυβερνοασφάλειας ή σημαντικές αλλαγές στις λειτουργίες της οντότητας ή εφόσον έχει μεταβληθεί το τρέχον διεθνές περιβάλλον κυβερνοαπειλών.	ΕΑΚ 16.1.12	Μέτρια	Υπεύθυνος πληροφορικής	31 Ιανουαρίου 2027
19	Κρυπτογράφηση των κρίσιμων δεδομένων και επανεξέταση της διαδικασίας κρυπτογραφίας.	ΕΑΚ 19.5	Μέτρια	Υπεύθυνος πληροφορικής	2 Μαρτίου 2027
20	Άνοδος στο επίπεδο 3: 21.2.a Πολιτικές για την ανάλυση κινδύνου και την ασφάλεια των πληροφοριακών συστημάτων	Ωριμότητα	Μέτρια	Υπεύθυνος ασφάλειας	31 Ιανουαρίου 2027
21	Άνοδος στο επίπεδο 3: 21.2.d Ασφάλεια της αλυσίδας εφοδιασμού, συμπεριλαμβανομένων των σχετικών με την ασφάλεια πτυχών που αφορούν τις σχέσεις μεταξύ κάθε οντότητας και των άμεσων προμηθευτών ή παρόχων υπηρεσιών της	Ωριμότητα	Μέτρια	Υπεύθυνος ασφάλειας	31 Ιανουαρίου 2027
22	Άνοδος στο επίπεδο 3: 21.2.f Πολιτικές και διαδικασίες για την αξιολόγηση της αποτελεσματικότητας των μέτρων διαχείρισης κινδύνων στον τομέα της κυβερνοασφάλειας	Ωριμότητα	Μέτρια	Υπεύθυνος ασφάλειας	31 Ιανουαρίου 2027
23	Άνοδος στο επίπεδο 3: 21.2.h Πολιτικές και διαδικασίες σχετικά με τη χρήση κρυπτογραφίας και, κατά περίπτωση, κρυπτογράφησης	Ωριμότητα	Μέτρια	Υπεύθυνος ασφάλειας	31 Ιανουαρίου 2027
24	Άνοδος στο επίπεδο 3: 21.2.j Χρήση λύσεων πολυπαραγοντικής επαλήθευσης ταυτότητας ή συνεχούς επαλήθευσης ταυτότητας, ασφαλών φωνητικών επικοινωνιών, επικοινωνιών βίντεο και κειμένου και ασφαλών συστημάτων επικοινωνιών έκτακτης ανάγκης εντός της οντότητας, κατά περίπτωση	Ωριμότητα	Μέτρια	Υπεύθυνος ασφάλειας	31 Ιανουαρίου 2027

#	ΕΝΕΡΓΕΙΑ	ΠΗΓΗ	ΠΡΟΤΕΡΑΙΟΤΗΤΑ	ΥΠΕΥΘΥΝΟΣ	ΠΡΟΘΕΣΜΙΑ
25	Επαναφέρετε τον κωδικό του λογαριασμού που αναφέρει το εύρημα και ανακαλέστε τις ενεργές συνεδρίες του. Πού: example.com (τα στοιχεία φαίνονται στην κονσόλα, στο εύρημα F-258E45A9D5)	Τεχνικό	Μέτρια	Υπεύθυνος ασφάλειας	28 Δεκεμβρίου 2026
26	Επανεκδώστε το πιστοποιητικό ώστε να καλύπτει τα ονόματα που σερβίρονται σε αυτή τη διεύθυνση, ή σερβίρετε το αντίστοιχο πιστοποιητικό για κάθε όνομα. Πού: 203.0.113.13	Τεχνικό	Μέτρια	Υπεύθυνος πληροφορικής	3 Ιανουαρίου 2027
27	Περιορίστε το 3389/tcp στους υπολογιστές που το χρειάζονται, με κανόνα τείχους προστασίας ή ξεχωριστό τμήμα δικτύου. Πού: 192.168.10.31	Εσωτερικό δίκτυο	Μέτρια	Υπεύθυνος ασφάλειας	10 Ιανουαρίου 2027
28	Περιορίστε το 445/tcp στους υπολογιστές που το χρειάζονται, με κανόνα τείχους προστασίας ή ξεχωριστό τμήμα δικτύου. Πού: 192.168.10.20	Εσωτερικό δίκτυο	Μέτρια	Υπεύθυνος ασφάλειας	10 Ιανουαρίου 2027
29	Επανεξέταση και νέα έγκριση: Πολιτική αποδεκτής χρήσης	Πολιτική	Μέτρια	Υπεύθυνος ασφάλειας	31 Ιανουαρίου 2027
30	Υιοθέτηση και έγκριση: Πολιτική αφαιρούμενων μέσων	Πολιτική	Μέτρια	Υπεύθυνος ασφάλειας	31 Ιανουαρίου 2027
31	Υιοθέτηση και έγκριση: Πολιτική ασφάλειας της εφοδιαστικής αλυσίδας	Πολιτική	Μέτρια	Υπεύθυνος ασφάλειας	31 Ιανουαρίου 2027
32	Υιοθέτηση και έγκριση: Πολιτική δοκιμών ασφάλειας	Πολιτική	Μέτρια	Υπεύθυνος ασφάλειας	31 Ιανουαρίου 2027
33	Υιοθέτηση και έγκριση: Πολιτική κρυπτογραφίας	Πολιτική	Μέτρια	Υπεύθυνος ασφάλειας	31 Ιανουαρίου 2027
34	Υιοθέτηση και έγκριση: Πολιτική φυσικής και περιβαλλοντικής ασφάλειας	Πολιτική	Μέτρια	Υπεύθυνος ασφάλειας	31 Ιανουαρίου 2027
35	Πρώτη εκτέλεση: Επανεξέταση κρίσιμων προμηθευτών	Πρόγραμμα	Μέτρια	Υπεύθυνος ασφάλειας	31 Ιανουαρίου 2027
36	Αφαιρέστε την έκδοση του προϊόντος από τις κεφαλίδες Server, X-Powered-By και X-AspNet-Version. Πού: 203.0.113.10, 203.0.113.11	Τεχνικό	Χαμηλή	Ανάδοχος ιστοτόπου	13 Φεβρουαρίου 2027
37	Δημοσιεύστε εγγραφή CAA με τις αρχές πιστοποίησης που επιτρέπεται να εκδίδουν για τον τομέα. Πού: example.com	Τεχνικό	Χαμηλή	Υπεύθυνος ασφάλειας	31 Ιανουαρίου 2027

#	ΕΝΕΡΓΕΙΑ	ΠΗΓΗ	ΠΡΟΤΕΡΑΙΟΤΗΤΑ	ΥΠΕΥΘΥΝΟΣ	ΠΡΟΘΕΣΜΙΑ
38	Προσθέστε στις αποκρίσεις αυτής της υπηρεσίας τις κεφαλίδες ασφάλειας που αναφέρει το εύρημα. Πού: 203.0.113.10, 203.0.113.11	Τεχνικό	Χαμηλή	Ανάδοχος ιστοτόπου	1 Μαΐου 2027
39	Περιορίστε αυτό το περιβάλλον διαχείρισης στις διευθύνσεις που το χρειάζονται, ή βάλτε το πίσω από το VPN. Πού: vpn.example.com	Τεχνικό	Χαμηλή	Υπεύθυνος πληροφορικής	1 Μαΐου 2027

10. Περιορισμοί

- Οι απαντήσεις ΕΑΚ και ωριμότητας είναι του ίδιου του οργανισμού, καταγεγραμμένες με τον σύμβουλό του. Δεν έχουν επαληθευτεί ανεξάρτητα.
- Η έκθεση αυτή είναι αξιολόγηση. Δεν είναι πιστοποίηση ούτε γνώμη ελέγχου.

11. Υπογραφές

Υπογράφεται από όσους συνέταξαν, έλεγξαν και αποδέχθηκαν την έκθεση.

ΡΟΛΟΣ	ΟΝΟΜΑ	ΥΠΟΓΡΑΦΗ	ΗΜΕΡΟΜΗΝΙΑ
Συντάχθηκε από			
Ελέγχθηκε από			
Έγινε αποδεκτή από			