



ΣΥΜΠΛΗΡΩΜΑΤΙΚΟΣ ΟΔΗΓΟΣ ΕΦΑΡΜΟΓΗΣ

Πώς να εφαρμόσετε το Μοντέλο Ασφάλειας Cloud (CSI) στον οργανισμό σας

Συνοδευτικός οδηγός του έργου «**Go Cloud! Go Secure! A Cloud Security Implementation Model for SMEs**» (Erasmus+ 2024-1-AT01-KA220-VET-000245093).

Εκπαιδευτικό υλικό και διαδραστικά εργαλεία: gocloudsecure.eu

1. Σκοπός του Οδηγού

Το Μοντέλο CSI αποτελείται από πέντε φάσεις και βοηθά τις μικρομεσαίες επιχειρήσεις (ΜΜΕ) να ενισχύσουν την ασφάλεια των υπηρεσιών cloud που χρησιμοποιούν, είτε πρόκειται για λογισμικό (SaaS), πλατφόρμες (PaaS) είτε για υποδομές (IaaS).

Ο παρών οδηγός συμπληρώνει την επίσημη τεκμηρίωση του Μοντέλου CSI. Παρουσιάζει συνοπτικά κάθε φάση και περιλαμβάνει ένα πρακτικό παράδειγμα εφαρμογής, ώστε οι επιχειρήσεις να κατανοήσουν τη διαδικασία και να την προσαρμόσουν στις ανάγκες τους.

Για περισσότερες πληροφορίες, πρότυπα και αναλυτικές οδηγίες, συμβουλευτείτε τα έγγραφα των πέντε φάσεων του Μοντέλου CSI.

Χρησιμοποιήστε τον οδηγό μαζί με τα δύο βασικά εργαλεία CSI:

- **[CSI Matrix \(Πίνακας CSI\)](#)**: Διαδραστικό εργαλείο που καταγράφει τις απειλές, τις ευπάθειες και τους κινδύνους κάθε υπηρεσίας cloud και τους αξιολογεί με βάση το OWASP Top 10. Χρησιμοποιείται στις Φάσεις 1-3.
- **[CSI Self-Assessment](#) & [CSI Course \(SecureCloud SME\)](#)**: Εργαλείο αυτοαξιολόγησης και εκπαιδευτικό υλικό για τις βασικές αρχές του cloud, τις κυβερνοαπειλές, τον ασφαλή σχεδιασμό και τη διακυβέρνηση. Υποστηρίζουν την προετοιμασία και την υλοποίηση της εκπαίδευσης στις Φάσεις 3-4.

Συμβουλή: Έχετε ανοιχτό τον οδηγό και το *CSI Matrix* κατά τις Φάσεις 1-3. Ακολουθήστε τις οδηγίες του εργαλείου, ολοκληρώστε την αξιολόγηση και αξιοποιήστε τα αποτελέσματα στις επόμενες φάσεις.



2. Το Μοντέλο CSI με μια ματιά

Το Μοντέλο CSI λειτουργεί ως ένας συνεχής κύκλος πέντε φάσεων. Κάθε φάση έχει συγκεκριμένο στόχο, βασικά βήματα και αποτελέσματα που αξιοποιούνται στην επόμενη.

Φάση	Στόχος	Βασικά βήματα	Αποτελέσματα
1. Ανάλυση	Κατανόηση της χρήσης cloud, των απειλών και των απαιτήσεων συμμόρφωσης.	Καταγραφή υπηρεσιών cloud · Αξιολόγηση κινδύνων με το CSI Matrix · Έλεγχος συμμόρφωσης	Κατάλογος υπηρεσιών, αρχική αξιολόγηση CSI Matrix, σχετικές κανονιστικές απαιτήσεις.
2. Καθορισμός	Θέσπιση κανόνων ασφάλειας, ιεράρχηση κινδύνων και καθορισμός στόχων προστασίας.	Πολιτική ασφάλειας · Ιεράρχηση κινδύνων · Στόχοι προστασίας · Ρόλοι και αρμοδιότητες	Πολιτική Ασφάλειας Cloud, κατάλογος κινδύνων ανά προτεραιότητα, στόχοι και αρμοδιότητες.
3. Σχεδιασμός	Μετατροπή των κινδύνων και των στόχων σε συγκεκριμένο σχέδιο δράσης.	Μέτρα περιορισμού κινδύνων · Αντιστοίχιση μέτρων · Τεκμηρίωση · Πρόγραμμα εκπαίδευσης	Σχέδιο μέτρων, πίνακας αντιστοίχισης, πρότυπα και λίστες ελέγχου, πρόγραμμα εκπαίδευσης.
4. Εφαρμογή	Εφαρμογή μέτρων ασφάλειας και εκπαίδευση του προσωπικού.	Τεχνικές παρεμβάσεις · Εκπαίδευση και ευαισθητοποίηση	Εφαρμοσμένα μέτρα, ολοκληρωμένη εκπαίδευση, ασφαλέστερο περιβάλλον σύμφωνα με την πολιτική ασφάλειας.
5. Επαλήθευση	Έλεγχος της αποτελεσματικότητας και συνεχής βελτίωση.	Δοκιμές · Παρακολούθηση δεικτών (KPIs) · Καταγραφή περιστατικών και ανατροφοδότηση	Ελεγμένα μέτρα, πίνακας παρακολούθησης, συμπεράσματα και βελτιωμένες πολιτικές και εκπαιδεύσεις.

3. Οδηγίες βήμα προς βήμα

Ακολουθήστε τις πέντε φάσεις με τη σειρά, καθώς τα αποτελέσματα κάθε φάσης αποτελούν τη βάση για την επόμενη.

Φάση 1 - Ανάλυση

Στόχος: Να κατανοήσετε ποιες υπηρεσίες cloud χρησιμοποιεί η επιχείρησή σας, σε ποιες απειλές και ευπάθειες εκτίθεται και ποιες απαιτήσεις συμμόρφωσης πρέπει να τηρεί.

- **Καταγραφή υπηρεσιών cloud:** Καταγράψτε όλες τις υπηρεσίες που χρησιμοποιείτε (IaaS, PaaS, SaaS, αποθήκευση, βάσεις δεδομένων, δίκτυα και υπηρεσίες ασφάλειας). Σημειώστε ποιες είναι κρίσιμες για τη λειτουργία της επιχείρησής.
- **Αξιολόγηση κινδύνων:** Χρησιμοποιήστε το CSI Matrix για να εντοπίσετε τις απειλές κάθε υπηρεσίας (π.χ. διαρροή δεδομένων, επιθέσεις DDoS), τις ευπάθειες (π.χ. ανεπαρκής έλεγχος ταυτότητας) και τους πιθανούς κινδύνους (π.χ. απώλεια δεδομένων, παραβίαση λογαριασμών).

Με τη χρηματοδότηση της Ευρωπαϊκής Ένωσης. Οι απόψεις και οι γνώμες που διατυπώνονται εκφράζουν αποκλειστικά τις απόψεις των συντακτών και δεν αντιπροσωπεύουν κατ' ανάγκη τις απόψεις της Ευρωπαϊκής Ένωσης ή της OeAD-GmbH. Η Ευρωπαϊκή Ένωση και η χορηγούσα αρχή δεν μπορούν να θεωρηθούν υπεύθυνες για τις εκφραζόμενες απόψεις.

Project Number: 2024-1-AT01-KA220-VET-000245093.



- **Έλεγχος συμμόρφωσης:** Εξετάστε κατά πόσο τηρούνται οι σχετικοί ευρωπαϊκοί κανονισμοί (GDPR, DORA, NIS2) και τα πρότυπα που εφαρμόζετε ή επιδιώκετε να υιοθετήσετε (ISO/IEC 27001, ISO/IEC 27017, ISO 22301).

Αποτέλεσμα: Κατάλογος υπηρεσιών cloud, ολοκληρωμένη αξιολόγηση CSI Matrix και καταγραφή των απαιτήσεων συμμόρφωσης.

Φάση 2 - Καθορισμός

Στόχος: Να θεσπίσετε κανόνες ασφάλειας, να ιεραρχήσετε τους κινδύνους και να καθορίσετε τους στόχους προστασίας της επιχείρησής σας.

- **Πολιτική ασφάλειας:** Συντάξτε μια Πολιτική Ασφάλειας Cloud που να καλύπτει την ασφαλή χρήση υπηρεσιών, τη διαχείριση πρόσβασης και την προστασία δεδομένων.
- **Ιεράρχηση κινδύνων:** Αξιολογήστε κάθε κίνδυνο του CSI Matrix με βάση την πιθανότητα εμφάνισης και τις πιθανές επιπτώσεις του. Δώστε προτεραιότητα στους σημαντικότερους.
- **Καθορισμός στόχων προστασίας:** Για κάθε κίνδυνο υψηλής προτεραιότητας, ορίστε έναν σαφή στόχο. Για παράδειγμα, για τον κίνδυνο «ανεπαρκής έλεγχος ταυτότητας», στόχος μπορεί να είναι η «ενίσχυση της ασφάλειας των λογαριασμών».
- **Ρόλοι και αρμοδιότητες:** Ορίστε ποιος είναι υπεύθυνος για τη διαχείριση του cloud, των δεδομένων, της ασφάλειας και της κανονιστικής συμμόρφωσης. Στις μικρότερες επιχειρήσεις, ένα άτομο μπορεί να αναλαμβάνει περισσότερους από έναν ρόλους.

Αποτέλεσμα: Πολιτική Ασφάλειας Cloud, ιεραρχημένοι κίνδυνοι, καθορισμένοι στόχοι προστασίας και σαφείς αρμοδιότητες.

Φάση 3 - Σχεδιασμός

Στόχος: Να μετατρέψετε τους κινδύνους και τους στόχους προστασίας σε ένα συγκεκριμένο σχέδιο εφαρμογής, με τεχνικά μέτρα, τεκμηρίωση και εκπαίδευση.

- **Μέτρα περιορισμού κινδύνων:** Ορίστε συγκεκριμένες ενέργειες για κάθε στόχο προστασίας. Για παράδειγμα, για την «ενίσχυση της ασφάλειας των λογαριασμών», εφαρμόστε έλεγχο ταυτότητας πολλαπλών παραγόντων (MFA).
- **Αντιστοίχιση μέτρων:** Δημιουργήστε έναν πίνακα που να δείχνει ποια υπηρεσία cloud προστατεύει κάθε μέτρο.
- **Τεκμηρίωση:** Ετοιμάστε μια λίστα ελέγχου εφαρμογής, ένα πρότυπο αντιμετώπισης περιστατικών ασφάλειας και ένα έντυπο ελέγχου αρχείων καταγραφής (Audit Logs).
- **Πρόγραμμα εκπαίδευσης:** Σχεδιάστε σύντομες, πρακτικές εκπαιδευτικές ενότητες με βάση το υλικό CSI, προσαρμοσμένες στις τεχνικές γνώσεις και τις ανάγκες της ομάδας σας.

Αποτέλεσμα: Κατάλογος μέτρων περιορισμού κινδύνων, πίνακας αντιστοίχισης μέτρων, έγγραφα εφαρμογής και πρόγραμμα εκπαίδευσης.



Φάση 4 - Εφαρμογή

Στόχος: Να εφαρμόσετε τα προγραμματισμένα μέτρα σε όλες τις σχετικές υπηρεσίες cloud και να εκπαιδεύσετε το προσωπικό.

- **Τεχνικές ενέργειες:** Υλοποιήστε το σχέδιο της Φάσης 3, όπως την ενεργοποίηση MFA, την κρυπτογράφηση και την εφαρμογή πολιτικών διαχείρισης ταυτοτήτων και πρόσβασης (IAM, RBAC). Ξεκινήστε από απλές παρεμβάσεις με άμεσο όφελος, αξιοποιώντας ενσωματωμένα εργαλεία όπως το AWS Config ή το Azure Security Center.
- **Εκπαίδευση και ευαισθητοποίηση:** Υλοποιήστε το πρόγραμμα εκπαίδευσης, δίνοντας έμφαση στους κινδύνους που εντοπίστηκαν μέσω του CSI Matrix και αξιοποιώντας το εκπαιδευτικό υλικό CSI.

Αποτέλεσμα: Εφαρμοσμένα μέτρα ασφάλειας, ολοκληρωμένη εκπαίδευση προσωπικού και στοιχεία που τεκμηριώνουν την υλοποίησή τους.

Φάση 5 - Επαλήθευση

Στόχος: Να αξιολογήσετε την αποτελεσματικότητα των μέτρων ασφάλειας και να βελτιώνετε συνεχώς την προστασία της επιχείρησης.

- **Δοκιμές:** Πραγματοποιήστε προσομοιώσεις επιθέσεων, ελέγχους μέτρων ασφάλειας και αξιολογήσεις ασφαλείας.
- **Παρακολούθηση:** Παρακολουθείτε βασικούς δείκτες (KPIs), όπως αποτυχημένες προσπάθειες σύνδεσης, ειδοποιήσεις λανθασμένων ρυθμίσεων και εκκρεμείς ενημερώσεις ασφαλείας. Μπορείτε να χρησιμοποιείτε έναν απλό πίνακα παρακολούθησης.
- **Ανατροφοδότηση:** Τηρείτε αρχείο περιστατικών ασφάλειας, καταγράφοντας τι συνέβη, γιατί συνέβη, ποιες ήταν οι επιπτώσεις και πώς αντιμετωπίστηκε. Αξιοποιήστε τα συμπεράσματα για να βελτιώσετε τις Φάσεις 1 και 2.

Αποτέλεσμα: Ελεγμένα μέτρα ασφάλειας, αποτελέσματα δεικτών KPI, διορθωτικές ενέργειες και συμπεράσματα για τον επόμενο κύκλο CSI.

4. Πρακτικό παράδειγμα εφαρμογής

Υποθετική επιχείρηση: NordicCraft Handicrafts

Η NordicCraft είναι μια μικρομεσαία επιχείρηση ηλεκτρονικού εμπορίου με 25 εργαζομένους, η οποία πωλεί χειροποίητα προϊόντα μέσω διαδικτύου.

Το παράδειγμα δείχνει πώς εφαρμόζονται στην πράξη οι πέντε φάσεις του Μοντέλου CSI. Τα στοιχεία και τα αποτελέσματα είναι ενδεικτικά.



Φάση 1 - Ανάλυση: Καταγραφή υπηρεσιών cloud και αξιολόγηση κινδύνων

Υπηρεσία cloud	Μοντέλο υπηρεσίας	Χρήση στην επιχείρηση
Shopify	SaaS	Ηλεκτρονικό κατάστημα, διαχείριση παραγγελιών, προσωπικά δεδομένα πελατών και διαβίβαση πληρωμών.
Google Workspace	SaaS	Εταιρικό email, κοινόχρηστα αρχεία και ημερολόγια.
AWS S3	IaaS / Αποθήκευση	Φωτογραφίες προϊόντων και καθημερινά αντίγραφα ασφαλείας των αρχείων παραγγελιών.
Azure App Service	PaaS	Ειδική διαδικτυακή εφαρμογή διαχείρισης παραγγελιών που συνδέει το Shopify με την αποθήκη.

Αποτελέσματα CSI Matrix (απόσπασμα):

Υπηρεσία	Απειλή	Ευπάθεια	Κίνδυνος	Προτεραιότητα
Πίνακας διαχείρισης Shopify	Παραβίαση λογαριασμών / phishing	Δεν χρησιμοποιείται MFA στους λογαριασμούς διαχειριστών.	Μη εξουσιοδοτημένες αλλαγές, διαρροή δεδομένων πελατών.	Υψηλή
AWS S3	Έκθεση δεδομένων	Ο αποθηκευτικός χώρος (bucket) επιτρέπει δημόσια πρόσβαση ανάγνωσης.	Διαρροή εικόνων πελατών και αρχείων αντιγράφων ασφαλείας.	Υψηλή
Εφαρμογή παραγγελιών Azure	Επιθέσεις έγχυσης κώδικα / εκμετάλλευση γνωστής ευπάθειας (CVE)	Παρωχημένες βιβλιοθήκες τρίτων και απουσία WAF.	Παραβίαση δεδομένων παραγγελιών και πελατών, διακοπή λειτουργίας.	Μεσαία
Google Workspace	Παραβίαση εταιρικού email	Αδύναμοι ή επαναχρησιμοποιούμενοι κωδικοί και μη υποχρεωτική χρήση MFA.	Απώλεια δεδομένων, πλαστά αιτήματα πληρωμής.	Μεσαία

Έλεγχος συμμόρφωσης:

Η NordicCraft επεξεργάζεται προσωπικά δεδομένα πελατών, επομένως ο GDPR εφαρμόζεται στην περίπτωση της.

Η επιχείρηση δεν εμπίπτει άμεσα στο πεδίο εφαρμογής των DORA και NIS2, αλλά επέλεξε να υιοθετήσει οικειοθελώς καλές πρακτικές του προτύπου ISO/IEC 27001.

Φάση 2 - Καθορισμός: Πολιτική ασφάλειας, προτεραιότητες και ρόλοι

Η NordicCraft συνέταξε μια μονοσέλιδη Πολιτική Ασφάλειας Cloud, η οποία καλύπτει την πρόσβαση στους λογαριασμούς, την ταξινόμηση δεδομένων και τη δημιουργία αντιγράφων ασφαλείας.

Δόθηκε άμεση προτεραιότητα στους δύο κινδύνους υψηλής σοβαρότητας: στους λογαριασμούς διαχειριστών του Shopify και στη δημόσια πρόσβαση στον αποθηκευτικό χώρο AWS S3.

Με τη χρηματοδότηση της Ευρωπαϊκής Ένωσης. Οι απόψεις και οι γνώμες που διατυπώνονται εκφράζουν αποκλειστικά τις απόψεις των συντακτών και δεν αντιπροσωπεύουν κατ' ανάγκη τις απόψεις της Ευρωπαϊκής Ένωσης ή της OeAD-GmbH. Η Ευρωπαϊκή Ένωση και η χορηγούσα αρχή δεν μπορούν να θεωρηθούν υπεύθυνες για τις εκφραζόμενες απόψεις.
Project Number: 2024-1-AT01-KA220-VET-000245093.



Οι αρμοδιότητες κατανεμήθηκαν ως εξής:

- **Διαχειριστής Cloud:** Υπεύθυνος Πληροφορικής - ρυθμίζει και διαχειρίζεται όλες τις πλατφόρμες cloud.
- **Υπεύθυνος Δεδομένων:** Υπεύθυνος Λειτουργιών - καθορίζει την ταξινόμηση των δεδομένων πελατών και τους κανόνες πρόσβασης.
- **Υπεύθυνος Ασφάλειας:** Υπεύθυνος Πληροφορικής, με τη στήριξη εξωτερικού συνεργάτη IT - παρακολουθεί την ασφάλεια, διαχειρίζεται περιστατικά και ενημερώνει την πολιτική.
- **Υπεύθυνος Κανονιστικής Συμμόρφωσης:** Γενικός Διευθυντής - διασφαλίζει την ευθυγράμμιση με τον GDPR και το ISO/IEC 27001.

Φάση 3 - Σχεδιασμός: Μέτρα περιορισμού κινδύνων

Κίνδυνος	Στόχος προστασίας	Μέτρο αντιμετώπισης	Υπεύθυνος
Ανεπαρκής ασφάλεια λογαριασμών διαχειριστών Shopify	Ενίσχυση της ασφάλειας λογαριασμών	Υποχρεωτική ενεργοποίηση MFA σε όλους τους λογαριασμούς διαχειριστών Shopify.	Υπεύθυνος Πληροφορικής
Δημόσια πρόσβαση στον χώρο AWS S3	Περιορισμός πρόσβασης στα απολύτως απαραίτητα δικαιώματα	Μετατροπή του bucket σε ιδιωτικό, εφαρμογή πολιτικής πρόσβασης και ενεργοποίηση καταγραφής προσβάσεων.	Υπεύθυνος Πληροφορικής
Παρωχημένες βιβλιοθήκες της εφαρμογής Azure	Μείωση των σημείων που μπορούν να αξιοποιηθούν για επίθεση	Ενημέρωση βιβλιοθηκών, ενεργοποίηση Azure WAF και αυτόματων ενημερώσεων.	Εξωτερικός συνεργάτης IT
Απουσία MFA στο Google Workspace	Ενίσχυση της ασφάλειας λογαριασμών	Υποχρεωτική χρήση MFA σε όλη την επιχείρηση και ενεργοποίηση ειδοποιήσεων σύνδεσης.	Υπεύθυνος Πληροφορικής

Έγγραφα που ετοιμάστηκαν:

- Πολιτική Ασφάλειας Cloud.
- Λίστα ελέγχου εφαρμογής, με μία εγγραφή για κάθε μέτρο.
- Πρότυπο Αντιμετώπισης Περιστατικών Ασφάλειας.
- Έντυπο Ελέγχου Αρχείων Καταγραφής (Audit Logs).

Πρόγραμμα εκπαίδευσης:

Προγραμματίστηκαν δύο εκπαιδευτικές συναντήσεις διάρκειας 45 λεπτών, με βάση το υλικό CSI:

- «MFA και σωστή διαχείριση κωδικών πρόσβασης»
- «Πώς αναγνωρίζουμε το phishing και αναφέρουμε περιστατικά ασφάλειας»

Φάση 4 - Εφαρμογή: Τεχνικά μέτρα και εκπαίδευση

Η NordicCraft προχώρησε στις ακόλουθες ενέργειες:

- Ενεργοποίησε την υποχρεωτική χρήση MFA σε όλους τους λογαριασμούς διαχειριστών Shopify και Google Workspace. Το μέτρο ολοκληρώθηκε την πρώτη εβδομάδα.
- Περιορίσε την πρόσβαση στον αποθηκευτικό χώρο AWS S3, ενεργοποιώντας πολιτική πρόσβασης και καταγραφή ενεργειών.

Με τη χρηματοδότηση της Ευρωπαϊκής Ένωσης. Οι απόψεις και οι γνώμες που διατυπώνονται εκφράζουν αποκλειστικά τις απόψεις των συντακτών και δεν αντιπροσωπεύουν κατ' ανάγκη τις απόψεις της Ευρωπαϊκής Ένωσης ή της OeAD-GmbH. Η Ευρωπαϊκή Ένωση και η χορηγούσα αρχή δεν μπορούν να θεωρηθούν υπεύθυνες για τις εκφραζόμενες απόψεις.

Project Number: 2024-1-AT01-KA220-VET-000245093.



- Ενημέρωσε τις βιβλιοθήκες της εφαρμογής Azure App Service και ενεργοποίησε το Azure WAF για την προστασία της εφαρμογής παραγγελιών.
- Πραγματοποίησε και τις δύο εκπαιδευτικές συναντήσεις για τους 25 εργαζομένους. Η συμμετοχή καταγράφηκε σε κοινόχρηστο υπολογιστικό φύλλο.

Φάση 5 - Επαλήθευση: Δοκιμές, παρακολούθηση και ανατροφοδότηση

Έναν μήνα μετά την εφαρμογή των μέτρων, ο εξωτερικός συνεργάτης IT πραγματοποίησε δοκιμή προσομοίωσης phishing και βασικό έλεγχο ευπαθειών στην εφαρμογή Azure.

Παράλληλα, δημιουργήθηκε ένας απλός πίνακας παρακολούθησης δεικτών KPI σε υπολογιστικό φύλλο.

Δείκτης (KPI)	Τρόπος μέτρησης	Όριο ειδοποίησης
Αποτυχημένες προσπάθειες σύνδεσης (όλες οι πλατφόρμες)	Εβδομαδιαία εξαγωγή στοιχείων από τα εργαλεία διαχείρισης.	Πάνω από 10 προσπάθειες ανά λογαριασμό την εβδομάδα.
Ποσοστό λογαριασμών διαχειριστών με ενεργό MFA	Μηνιαίος έλεγχος ρυθμίσεων ταυτότητας.	Κάτω από 100%.
Ημέρες από την τελευταία ενημέρωση βιβλιοθηκών ή διορθώσεων ασφάλειας (εφαρμογή Azure)	Μηνιαίο αρχείο ενημερώσεων.	Πάνω από 30 ημέρες.
Εκκρεμή περιστατικά ασφάλειας	Συνεχής παρακολούθηση.	Οποιοδήποτε περιστατικό παραμένει ανοιχτό πάνω από 14 ημέρες.

Δημιουργήθηκε επίσης αρχείο περιστατικών ασφάλειας, στο οποίο καταγράφονται το συμβάν, η αιτία, οι επιπτώσεις και τα μέτρα αντιμετώπισης.

Τα αποτελέσματα των ελέγχων και τα συμπεράσματα αξιοποιούνται για την επικαιροποίηση του CSI Matrix, των πολιτικών, των μέτρων ασφάλειας και της εκπαίδευσης.

Έτσι, η επιχείρηση μπορεί να ξεκινήσει έναν νέο κύκλο CSI από τη Φάση 1, βελτιώνοντας συνεχώς την ασφάλειά της.

5. Λίστα ελέγχου πριν ξεκινήσετε

Πριν εφαρμόσετε για πρώτη φορά το Μοντέλο CSI, βεβαιωθείτε ότι έχετε:

- Ορίσει έναν υπεύθυνο για τον συνολικό συντονισμό της εφαρμογής. Σε μια μικρή επιχείρηση δεν χρειάζεται να είναι αποκλειστικά υπεύθυνος ασφάλειας.
- Προγραμματίσει χρόνο για την ολοκλήρωση της Αυτοαξιολόγησης CSI από την ομάδα, ώστε να καταγράψετε το αρχικό επίπεδο γνώσεων.
- Εξασφαλίσει πρόσβαση στο CSI Matrix για την αξιολόγηση κινδύνων της Φάσης 1.
- Δημιουργήσει έναν κοινόχρηστο φάκελο για την Πολιτική Ασφάλειας Cloud, τις λίστες ελέγχου και το αρχείο περιστατικών.
- Προγραμματίσει τακτική υπενθύμιση για επανάληψη της Φάσης 1, π.χ. κάθε 6–12 μήνες ή μετά από σημαντικές αλλαγές στις υπηρεσίες cloud.



6. Χρήσιμοι πόροι

Όλα τα εργαλεία του οδηγού είναι διαθέσιμα στο gocloudsecure.eu.

- [CSI Model](#): Πλήρης τεκμηρίωση και των πέντε φάσεων του Μοντέλου CSI.
- [CSI Matrix](#): Διαδραστικό εργαλείο εντοπισμού και αξιολόγησης απειλών και κινδύνων ασφάλειας cloud.
- [CSI Self-Assessment](#): Εργαλείο αξιολόγησης των γνώσεων της ομάδας σας σε θέματα ασφάλειας cloud.
- [CSI Course-SecureCloud SME](#): Εκπαιδευτικό υλικό για την ανάπτυξη πρακτικών γνώσεων και δεξιοτήτων στην ασφάλεια cloud.

Σημείωση για τον Οδηγό

Ο παρών οδηγός αποτελεί ανεπίσημο, συμπληρωματικό υλικό που δημιουργήθηκε για να διευκολύνει την εφαρμογή του Μοντέλου CSI.

Δεν αντικαθιστά την επίσημη έκδοση «Go Cloud! Go Secure! — A Cloud Security Implementation Model for SMEs» (Erasmus+ 2024-1-AT01-KA220-VET-000245093), η οποία διατίθεται με άδεια CC BY-NC-ND 4.0.