Erasmus+ Project No: 2024-1-AT01-KA220-VET-000245093

ΜΟΝΤΕΛΟ ΕΦΑΡΜΟΓΗΣ CSI

GO CLOUD GO SECURE

Φάση 1: ΑΝΑΛΥΣΗ

- Βήμα 1: Καταγραφή υπηρεσιών cloud
- Βήμα 2: Χαρτογράφηση κινδύνων
- Βήμα 3: Συμμόρφωση

Φάση 2: ΚΑΘΟΡΙΣΜΟΣ

- Βήμα 4: Ρόλοι και αρμοδιότητες
- Βήμα 3: Καθορισμός στόχων ελέγχου
- Βήμα 2: Ιεράρχηση κινδύνων
- Βήμα 1: Ανάπτυξη πολιτικής

Φάση 3: ΣΧΕΔΙΑΣΜΟΣ

- Βήμα 1: Μέτρα αντιμετώπισης
- Βήμα 2: Αντιστοίχιση ελέγχων
- Βήμα 3: Τεκμηρίωση
- Βήμα 4: Πρόγραμμα κατάρτισης

Φάση 4: ΕΦΑΡΜΟΓΗ

- Βήμα 2: Κατάρτιση και ευαισθητοποίηση
- Βήμα 1: Τεχνικά μέτρα

Φάση 5: ΕΠΑΛΗΘΕΥΣΗ

- Βήμα 1: Δοκιμές
- Βήμα 2: Παρακολούθηση
- Βήμα 3: Ανατροφοδότηση

Με τη συγχρηματοδότηση της Ευρωπαϊκής Ένωσης

Erasmus+ Project No: 2024-1-AT01-KA220-VET-000245093

ΜΟΝΤΕΛΟ ΕΦΑΡΜΟΓΗΣ CSI

GO CLOUD GO SECURE

Φάση 1: ΑΝΑΛΥΣΗ

Βήμα 1: Καταγραφή υπηρεσιών cloud

Καταγράψτε όλες τις υπηρεσίες cloud που χρησιμοποιεί ο οργανισμός σας. Πριν από την αξιολόγηση, είναι σημαντικό να γνωρίζετε τι χρησιμοποιείτε και ποιες υπηρεσίες είναι κρίσιμες.

Βήμα 2: Χαρτογράφηση κινδύνων

Ο Πίνακας CSI εντοπίζει απειλές, ευπάθειες και κινδύνους για κάθε υπηρεσία cloud, δίνοντας σαφή εικόνα των βασικών αδυναμιών του οργανισμού.

Βήμα 3: Συμμόρφωση

Ελέγξτε τη συμμόρφωση του οργανισμού με τους κανονισμούς της ΕΕ και τα διεθνή πρότυπα, ώστε να αποφύγετε πρόστιμα, απώλεια δεδομένων και βλάβη στη φήμη. Ορισμένα απαιτούν συγκεκριμένα μέτρα, όπως καταγραφή πρόσβασης, κρυπτογράφηση και αναφορά περιστατικών.

Φάση 2: ΚΑΘΟΡΙΣΜΟΣ

Βήμα 1: Ανάπτυξη πολιτικής

Συντάξτε Πολιτική Ασφάλειας Cloud που να ορίζει κανόνες για ασφαλή χρήση, έλεγχο πρόσβασης και προστασία δεδομένων, αποτελώντας τη βάση του πλαισίου ασφάλειας.

Βήμα 2: Ιεράρχηση κινδύνων

Χρησιμοποιήστε τον Πίνακα CSI για να αξιολογήσετε τους κινδύνους βάσει πιθανότητας και επίπτωσης, δίνοντας προτεραιότητα στους πιο επείγοντες.

Βήμα 3: Καθορισμός στόχων ελέγχου

Ορίστε σαφείς στόχους αντιμετώπισης για κάθε κίνδυνο υψηλής προτεραιότητας του Πίνακα CSI, ώστε η αναγνώριση του κινδύνου να μετατραπεί σε στοχευμένο σχέδιο δράσης.

Βήμα 4: Ρόλοι και αρμοδιότητες

Καθορίστε σαφείς ρόλους: ο Διαχειριστής Cloud διαχειρίζεται τις πλατφόρμες, ο Ιδιοκτήτης Δεδομένων την πρόσβαση στα δεδομένα, ο Υπεύθυνος Ασφάλειας την παρακολούθηση και τα περιστατικά και ο Υπεύθυνος Συμμόρφωσης την τήρηση των κανονιστικών απαιτήσεων.

Φάση 3: ΣΧΕΔΙΑΣΜΟΣ

Βήμα 1: Μέτρα αντιμετώπισης

Για κάθε κίνδυνο υψηλής προτεραιότητας του Πίνακα CSI, ορίστε συγκεκριμένα και εφαρμόσιμα μέτρα, ώστε η υλοποίηση να είναι γρήγορη και συνεπής, ιδιαίτερα σε ΜΜΕ χωρίς μόνιμο προσωπικό ασφάλειας.

Βήμα 2: Αντιστοίχιση ελέγχων

Δημιουργήστε πίνακα που συνδέει τα μέτρα αντιμετώπισης με συγκεκριμένες υπηρεσίες cloud, διευκρινίζοντας τι προστατεύεται και πώς εφαρμόζονται οι έλεγχοι.

Βήμα 3: Τεκμηρίωση

Ετοιμάστε πρότυπα και λίστες ελέγχου, όπως λίστες εφαρμογής, πρότυπα απόκρισης σε περιστατικά και φόρμες ελέγχου αρχείων καταγραφής, για την εφαρμογή πολιτικών, τους ελέγχους και τη συνεχή βελτίωση.

Βήμα 4: Πρόγραμμα κατάρτισης

Σχεδιάστε πρακτικό Πρόγραμμα Κατάρτισης CSI για τις βασικές αρχές του cloud, τις κύριες ευπάθειες και τις λανθασμένες ρυθμίσεις, ώστε να εκπαιδευτεί αποτελεσματικά το προσωπικό και να αποτραπεί το 80% των αστοχιών ασφάλειας cloud.

Με τη συγχρηματοδότηση της Ευρωπαϊκής Ένωσης

Erasmus+ Project No: 2024-1-AT01-KA220-VET-000245093

CSI IMPLEMENTATION MODEL

GO CLOUD GO SECURE

Φάση 4: ΕΦΑΡΜΟΓΗ

Εφαρμόστε τα τεχνικά μέτρα του σχεδίου της Φάσης 3, όπως MFA, κρυπτογράφηση, πολιτικές IAM και RBAC, με ενσωματωμένα εργαλεία όπως AWS Config και Azure Security Center. Ξεκινήστε με άμεσες βελτιώσεις, όπως η ενεργοποίηση MFA και RBAC.

Βήμα 1: Τεχνικά μέτρα

Εφαρμόστε το σχέδιο κατάρτισης της Φάσης 3, με επίκεντρο τον Πίνακα CSI και το εκπαιδευτικό υλικό, μέσω σύντομων πρακτικών ενοτήτων προσαρμοσμένων στην τεχνική πραγματικότητα και το προφίλ κινδύνου του οργανισμού.

Βήμα 2: Κατάρτιση και ευαισθητοποίηση

Φάση 5: ΕΠΑΛΗΘΕΥΣΗ

Βήμα 1: Δοκιμές

Πραγματοποιήστε δοκιμές ανθεκτικότητας με ασκήσεις, προσομοιωμένες επιθέσεις, ελέγχους μέτρων και αξιολογήσεις ασφάλειας, ώστε να επιβεβαιώσετε ότι τα μέτρα έχουν εφαρμοστεί σωστά, είναι αποτελεσματικά και επικαιροποιημένα και ότι ο οργανισμός είναι έτοιμος για πραγματικές απειλές.

Βήμα 2: Παρακολούθηση

Καθορίστε δείκτες απόδοσης για την παρακολούθηση της ασφάλειας cloud, την προληπτική διαχείριση και την αποτύπωση της προόδου. Βασικοί δείκτες είναι οι αποτυχημένες συνδέσεις, οι ειδοποιήσεις λανθασμένης ρύθμισης και οι παρωχημένες ενημερώσεις, σε ένα απλό dashboard μετρήσεων.

Βήμα 3: Ανατροφοδότηση

Δημιουργήστε μητρώο περιστατικών με τα στοιχεία, τα αίτια, τις επιπτώσεις και τα μέτρα αντιμετώπισης κάθε συμβάντος, ώστε να επικαιροποιείτε τις αξιολογήσεις κινδύνου, να βελτιώνετε τις πολιτικές και να προσαρμόζετε την κατάρτιση, διατηρώντας το πλαίσιο ασφάλειας δυναμικό και εξελισσόμενο.

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 του Ευρωπαϊκού Εκτελεστικού Οργανισμού Εκπαίδευσης και Πολιτισμού (EACEA). Η Ευρωπαϊκή Ένωση και ο EACEA δεν μπορούν να θεωρηθούν υπεύθυνοι για τις εκφραζόμενες απόψεις.

Με τη συγχρηματοδότηση της Ευρωπαϊκής Ένωσης