Όνομα: _____ Ημερομηνία: _____ Βαθμολογία: _____

Προστασία δεδομένων και εταιρική αποθήκευση Οδηγός ασφαλείας

Απόκρυψη δεδομένων, δημιουργία διακριτικών (tokenization), κρυπτογράφηση σε ηρεμία και σε διαμετακόμιση, αντίγραφα ασφαλείας εκτός σύνδεσης

ΕΠΙΣΚΟΠΗΣΗ ΜΑΘΗΣΗΣ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΔΕΔΟΜΕΝΩΝ

ΑΣΦΑΛΙΣΜΕΝΟ
ΚΡΥΠΤΟΓΡΑΦΗΣΗ ΔΕΔΟΜΕΝΩΝ
Πρότυπο AES 256 bit

ΣΥΜΦΩΝΟ
ΠΑΓΚΟΣΜΙΑ ΠΡΟΤΥΠΑ
Πλαίσια GDPR και CCPA

ZERO-TRUST
ΠΟΛΙΤΙΚΗ ΠΡΟΣΒΑΣΗΣ
Έλεγχος ταυτότητας πολλαπλών παραγόντων

Καλώς ήρθες! Αυτό το φυλλάδιο δραστηριοτήτων σε καθοδηγεί στα πρότυπα και τους ελέγχους προστασίας δεδομένων. Θα εξερευνήσεις την κρυπτογράφηση ολόκληρου του δίσκου, τους ασφαλείς ελέγχους πρόσβασης, τα αντίγραφα ασφαλείας υλικού, τη στάση ασφάλειας cloud και τις τεχνικές απόκρυψης δεδομένων.

ΣΗΜΕΙΑ ΕΛΕΓΧΟΥ ΤΟΥ ΦΥΛΛΟΥ ΕΡΓΑΣΙΑΣ

- ☐ **Μέρη 1-4: Κατάκτησε την κυβερνοασφάλεια και την πρόληψη απειλών.**
- ☐ **Μέρη 5-7: Λύσε γρίφους σταυρολέξου και αναζήτησης λέξεων.**
- ☐ **Μέρη 8-9: Λύσε μελέτες περίπτωσης και πρόκληση κρυπτογραφημένου μηνύματος.**
- ☐ **Μέρος 10: Εξέτασε τις σελίδες συχνών ερωτήσεων βασικού και προχωρημένου επιπέδου.**
- ☐ **Μέρος 11: Εξερεύνησε 10 ενδιαφέροντα πραγματικά στοιχεία.**
- ☐ **Μπόνους: η πρόκληση Σκέψου γρήγορα.**

Άνοιξε τον Οδηγό του VPN.com για την κυβερνοασφάλεια

URL: https://www.vpn.com/el/kiberasfaleia/prostasia-dedomenon/

Η πορεία μάθησής σου: στρατηγική προστασίας δεδομένων

- Διαχώρισε τις τεχνικές απόκρυψης δεδομένων και δημιουργίας διακριτικών.
- Εφάρμοσε κρυπτογράφηση σε κατάσταση ηρεμίας για τους δίσκους αποθήκευσης και κρυπτογράφηση κατά τη μεταφορά με TLS.
- Σχεδίασε συστήματα αντιγράφων ασφαλείας εκτός σύνδεσης και απομονωμένα από το δίκτυο για προστασία από ransomware.

ΟΔΗΓΙΕΣ ΟΔΗΓΟΥ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

Απάντησε στις ερωτήσεις πολλαπλής επιλογής και σωστού/λάθους, συμπλήρωσε τα κενά των προτάσεων με την τράπεζα λέξεων, αντιστοίχισε ορισμούς και λύσε το σταυρόλεξο και τον γρίφο αναζήτησης λέξεων. Εφάρμοσε τις γνώσεις σου στην προστασία δεδομένων. Ολοκλήρωσε με τη δραστηριότητα μπόνους Σκέψου γρήγορα.

ΠΡΟΣΤΑΣΙΑ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΑΣΦΑΛΕΙΑ ΑΠΟΘΗΚΕΥΣΗΣ ΕΠΙΧΕΙΡΗΣΕΩΝ (ΕΙΣΑΓΩΓΗ)

Η προστασία δεδομένων διασφαλίζει τα εταιρικά περιουσιακά στοιχεία δεδομένων μέσω απόκρυψης, δημιουργίας διακριτικών, κρυπτογράφησης βάσεων δεδομένων σε ηρεμία και ασφαλών πρωτοκόλλων διαμετακόμισης. Ο σχεδιασμός αντιγράφων ασφαλείας απομονωμένων από το δίκτυο βοηθά να διασφαλιστεί ότι οι βασικές βάσεις δεδομένων μπορούν να αποκατασταθούν σε περίπτωση ενεργής εισβολής.

ΔΙΑΒΑΣΕ ΠΡΟΣΕΚΤΙΚΑ ΚΑΘΕ ΣΗΜΕΙΟ ΕΛΕΓΧΟΥ ΚΑΙ ΕΠΙΛΕΞΕ Η ΓΡΑΨΕ ΤΗ ΣΩΣΤΗ ΑΠΑΝΤΗΣΗ.

Σημείο ελέγχου 1: Πρόκληση πολλαπλής επιλογής

1. **Ποιος είναι ο κύριος σκοπός της συγκάλυψης δεδομένων (data masking);**
   - A. Αντικατάσταση ευαίσθητων αναγνωριστικών με φανταστικούς αλλά ρεαλιστικούς χαρακτήρες για την προστασία της ιδιωτικότητας
   - B. Συμπίεση μεγάλων αρχείων βάσεων δεδομένων για εξοικονόμηση φυσικού χώρου αποθήκευσης στον διακομιστή
   - C. Διαγραφή παλιών email επικοινωνίας πελατών από αρχειακά συστήματα αντιγράφων ασφαλείας
   - D. Απόκρυψη της δημόσιας IP του διακομιστή βάσης δεδομένων από σαρώσεις στο διαδίκτυο

2. **Ποιος μηχανισμός κρυπτογραφεί τα αρχεία που είναι αποθηκευμένα στον σκληρό δίσκο ενός διακομιστή βάσης δεδομένων;**
   - A. Κρυπτογράφηση ολόκληρου του δίσκου σε κατάσταση ηρεμίας
   - B. Πρωτόκολλα χειραψίας συνεδρίας TLS κατά τη μετάδοση
   - C. Κανόνες προώθησης διακομιστών ονομάτων δυναμικού DNS
   - D. Πολυπαραγοντική ταυτοποίηση με κλειδιά υλικού

3. **Τι αντιπροσωπεύει τα δεδομένα σε μετάδοση;**
   - A. Πακέτα δεδομένων που κινούνται μέσω δρομολογητών και διακοπτών δικτύου
   - B. Αποθηκευμένα αρχεία καταγραφής συναλλαγών βάσης δεδομένων σε ψυχρό δίσκο αντιγράφων ασφαλείας
   - C. Αρχειοθετημένα αρχεία χρηστών αποθηκευμένα σε απομονωμένο θησαυροφυλάκιο cloud
   - D. Στατικά αρχεία ρύθμισης συστήματος σε τοπικό αποθηκευτικό χώρο επιτραπέζιου υπολογιστή

4. **Γιατί είναι κρίσιμο ένα τακτικό αντίγραφο ασφαλείας εκτός σύνδεσης για την προστασία από ransomware;**
   - A. Παρέχει ένα καθαρό αντίγραφο εκτός σύνδεσης για την επαναφορά αρχείων χωρίς πληρωμή λύτρων
   - B. Εμποδίζει τους χάκερ να σαρώνουν τις ρυθμίσεις ανοιχτών θυρών
   - C. Αυξάνει τις ταχύτητες μετάδοσης του εύρους ζώνης του τοπικού δικτύου
   - D. Αυτοματοποιεί τα αρχεία καταγραφής αποδοχής συγκατάθεσης cookies στα προγράμματα περιήγησης

5. **Τι κάνει η διακριτικοποίηση δεδομένων (tokenization);**
   - A. Αντικαθιστά ευαίσθητους αριθμούς καρτών με μη ευαίσθητα τυχαία διακριτικά (tokens)
   - B. Δρομολογεί την κίνηση ιστού μέσω πολλαπλών ασφαλών κόμβων onion
   - C. Σαρώνει καταλόγους συστήματος για κακόβουλο λογισμικό βάσει υπογραφών
   - D. Ελέγχει τους χρόνους συνεδριών σύνδεσης των διαχειριστών της βάσης δεδομένων

Σημείο ελέγχου 2: Πρόκληση Σωστό ή Λάθος

6 Ερώτηση 6

6. Η απόκρυψη δεδομένων αλλάζει μόνιμα τις εγγραφές της βάσης δεδομένων σε περιβάλλοντα παραγωγής.

○ Σωστό ○ Λάθος

7 Ερώτηση 7

7. Τα αντίγραφα ασφαλείας εκτός χώρου πρέπει να απομονώνονται από το κύριο εταιρικό δίκτυο ώστε να αποφεύγεται η εξάπλωση ransomware.

○ Σωστό ○ Λάθος

8 Ερώτηση 8

8. Τα πιστοποιητικά SSL/TLS ασφαλίζουν τις βάσεις δεδομένων κρυπτογραφώντας τα δεδομένα που αποθηκεύονται σε κατάσταση ηρεμίας σε φυσικά μέσα.

○ Σωστό ○ Λάθος

9 Ερώτηση 9

9. Το zero-trust network access (ZTNA) επαληθεύει την ταυτότητα κάθε χρήστη πριν παραχωρήσει πρόσβαση σε βάση δεδομένων.

○ Σωστό ○ Λάθος

10 Ερώτηση 10

10. Η tokenization με θησαυροφυλάκιο αποθηκεύει τις αρχικές τιμές της κάρτας σε ένα ασφαλές κεντρικό θησαυροφυλάκιο διακριτικών.

○ Σωστό ○ Λάθος

Σημείο ελέγχου 3: Συμπλήρωση βασικών όρων

Διάβασε κάθε πρόταση παρακάτω και συμπλήρωσε το κενό με τον σωστό όρο από την Τράπεζα Λέξεων.

1. Η αντικατάσταση προσωπικών ονομάτων με ρεαλιστικά ψευδώνυμα ονομάζεται _____ δεδομένων.

2. Η κρυπτογράφηση φυσικών μπλοκ αποθήκευσης προστατεύει τα περιουσιακά στοιχεία της βάσης δεδομένων όταν βρίσκονται: _____ .

3. Τα πρωτόκολλα TLS κρυπτογραφούν ενεργά πακέτα δεδομένων καθώς βρίσκονται: _____ .

4. Τα δικαιώματα βάσει ρόλου περιορίζουν ποιοι χρήστες αποκτούν _____ στη βάση δεδομένων.

5. Η επαναφορά καθαρών εταιρικών αρχείων μετά από παραβίαση απαιτεί ένα ασφαλές εκτός σύνδεσης _____ .

6. Ο έλεγχος των ρυθμίσεων cloud αξιολογεί την ασφαλή _____ ενός οργανισμού.

ΤΡΑΠΕΖΑ ΛΕΞΕΩΝ

ΑΝΤΙΓΡΑΦΟ ΑΠΟΚΡΥΨΗ ΕΛΑΧΙΣΤΟΠΟΙΗΣΗ ΚΑΤΑΣΤΑΣΗ ΠΑΡΑΒΙΑΣΗ
ΠΡΟΣΒΑΣΗ ΣΕ ΑΔΡΑΝΕΙΑ ΣΕ ΜΕΤΑΔΟΣΗ

Γράψε τις απαντήσεις σου εδώ:

1. **2.**

3. **4.**

5. **6.**

Σημείο ελέγχου 4: Αντιστοίχιση εννοιών ασφάλειας

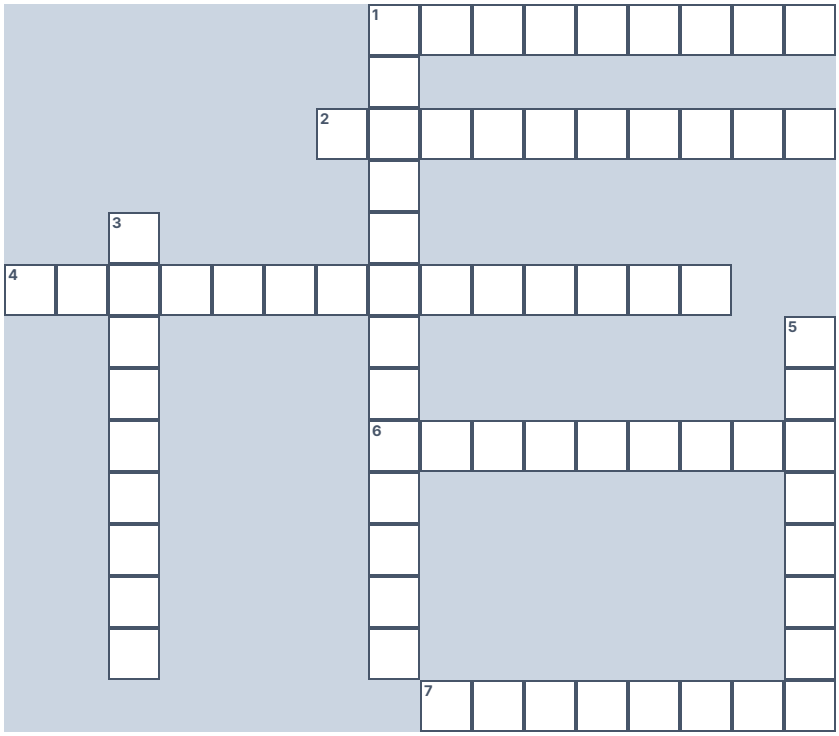
ΑΝΤΙΣΤΟΙΧΙΣΗ ΟΡΙΣΜΩΝ

Αντιστοίχισε κάθε όρο λεξιλογίου στα αριστερά με τον σωστό ορισμό του στα δεξιά, γράφοντας το αντίστοιχο γράμμα (A-H) στο πλαίσιο εισαγωγής.

☐	1. ΚΡΥΠΤΟΓΡΑΦΗΣΗ	A	Δημιουργία ασφαλών αντιγράφων δεδομένων εκτός χώρου για επαναφορά σε περίπτωση βλαβών του συστήματος.
☐	2. ΑΝΤΙΓΡΑΦΟ ΑΣΦΑΛΕΙΑΣ	B	Μετατροπή του απλού κειμένου σε μη αναγνώσιμο κρυπτογραφημένο κείμενο ώστε τα δεδομένα που υποκλέπτονται να παραμένουν ιδιωτικά.
☐	3. ΕΛΑΧΙΣΤΟΠΟΙΗΣΗ	C	Η συνολική κατάσταση ασφάλειας και ετοιμότητας άμυνας του cloud ενός οργανισμού.
☐	4. ΠΡΟΣΒΑΣΗ	D	Συμμόρφωση με ρυθμιστικά πρότυπα όπως ο GDPR ή ο CCPA για τη διαχείριση ιδιωτικών πληροφοριών χρηστών.
☐	5. ΣΤΑΣΗ ΑΣΦΑΛΕΙΑΣ	E	Περιστατικό ασφαλείας όπου προστατευμένα δεδομένα προσπελάζονται ή γνωστοποιούνται χωρίς εξουσιοδότηση.
☐	6. ΔΙΑΡΡΗΞΗ	F	Περιορισμός των δικαιωμάτων ανάγνωσης και εγγραφής της βάσης δεδομένων σε πιστοποιημένους ρόλους χρηστών.
☐	7. ΣΥΜΜΟΡΦΩΣΗ	G	Αντικατάσταση ευαίσθητων χαρακτήρων σε πεδία βάσης δεδομένων για την προστασία προσωπικών ταυτοτήτων.
☐	8. ΑΠΟΚΡΥΨΗ	H	Περιορισμός της συλλογής προσωπικών δεδομένων στο απολύτως απαραίτητο ελάχιστο για τις λειτουργίες.

Σημείο ελέγχου 5: Σταυρόλεξο

Λύσε το σταυρόλεξο πληκτρολογώντας γράμματα στα ενεργά λευκά κουτιά. Οι αριθμοί αντιστοιχούν στις οδηγίες παρακάτω.



ΟΡΙΖΟΝΤΙΑ

1. Η συνολική κατάσταση ασφαλείας και η ετοιμότητα άμυνας του cloud ενός οργανισμού (9)

2. Τήρηση κανονιστικών προτύπων, όπως ο GDPR ή ο CCPA, για τη διαχείριση ιδιωτικών πληροφοριών χρηστών (10)

4. Περιορισμός της συλλογής προσωπικών δεδομένων στο απόλυτο ελάχιστο που απαιτείται για τις λειτουργίες (14)

6. Δημιουργία ασφαλών αντιγράφων δεδομένων εκτός χώρου για επαναφορά σε περίπτωση αστοχιών του συστήματος (9)

7. Αντικατάσταση ευαίσθητων χαρακτήρων σε πεδία βάσεων δεδομένων για την προστασία προσωπικών ταυτοτήτων (8)

ΚΑΘΕΤΑ

1. Μετατροπή απλού κειμένου σε μη αναγνώσιμο κρυπτογραφημένο κείμενο, ώστε τα δεδομένα που υποκλέπτονται να παραμένουν ιδιωτικά (13)

3. Περιστατικό ασφαλείας όπου προστατευμένα δεδομένα προσπελάζονται ή αποκαλύπτονται χωρίς εξουσιοδότηση (9)

5. Περιορισμός των δικαιωμάτων ανάγνωσης και εγγραφής στη βάση δεδομένων σε πιστοποιημένους ρόλους χρηστών (8)

Σημείο ελέγχου 5, εναλλακτικά: Προσβάσιμες ενδείξεις σταυρολέξου

Οι χρήστες αναγνώστη οθόνης και πληκτρολογίου μπορούν να πληκτρολογήσουν τις απαντήσεις του σταυρολέξου απευθείας στα πεδία κειμένου παρακάτω.

ΟΡΙΖΟΝΤΙΑ

1 οριζόντια: Η συνολική κατάσταση ασφαλείας και η ετοιμότητα άμυνας του cloud ενός οργανισμού (9 γράμματα):

2 οριζόντια: Τήρηση κανονιστικών προτύπων, όπως ο GDPR ή ο CCPA, για τη διαχείριση ιδιωτικών πληροφοριών χρηστών (10 γράμματα):

4 οριζόντια: Περιορισμός της συλλογής προσωπικών δεδομένων στο απόλυτο ελάχιστο που απαιτείται για τις λειτουργίες (14 γράμματα):

6 οριζόντια: Δημιουργία ασφαλών αντιγράφων δεδομένων εκτός χώρου για επαναφορά σε περίπτωση αστοχιών του συστήματος (9 γράμματα):

7 οριζόντια: Αντικατάσταση ευαίσθητων χαρακτήρων σε πεδία βάσεων δεδομένων για την προστασία προσωπικών ταυτοτήτων (8 γράμματα):

ΚΑΘΕΤΑ

1 κάθετα: Μετατροπή απλού κειμένου σε μη αναγνώσιμο κρυπτογραφημένο κείμενο, ώστε τα δεδομένα που υποκλέπτονται να παραμένουν ιδιωτικά (13 γράμματα):

3 κάθετα: Περιστατικό ασφαλείας όπου προστατευμένα δεδομένα προσπελάζονται ή αποκαλύπτονται χωρίς εξουσιοδότηση (9 γράμματα):

5 κάθετα: Περιορισμός των δικαιωμάτων ανάγνωσης και εγγραφής στη βάση δεδομένων σε πιστοποιημένους ρόλους χρηστών (8 γράμματα):

Σημείο ελέγχου 6: Αναζήτηση κρυμμένων λέξεων

Βρες τους 8 βασικούς όρους λεξιλογίου που κρύβονται στο παρακάτω πλέγμα. Οι λέξεις μπορεί να είναι οριζόντιες, κάθετες ή διαγώνιες.

Η Ο Η Θ Η Ν Θ Π Ζ Λ Σ Λ Ρ Χ Η

Σ Φ Θ Β Τ Σ Ζ Ψ Ξ Ψ Χ Σ Η Ψ Π

Η Α Τ Χ Α Ο Ω Υ Ν Ν Ω Ξ Υ Ρ Θ

Φ Ρ Ο Σ Θ Ο Υ Φ Τ Ξ Υ Ρ Ο Τ Κ

Α Γ Α Ε Ξ Μ Λ Α Ρ Ν Κ Σ Υ Ζ Η

Ρ Ι Ο Π Χ Ψ Ι Κ Υ Ο Β Ι Ω Φ Ψ

Γ Τ Ο Κ Θ Ω Ι Ι Π Α Μ Ν Α Ε Θ

Ο Ν Α Σ Α Ι Ε Α Σ Φ Ε Μ Κ Ω Κ

Τ Α Ε Κ Π Ν Ι Η Α Ζ Ξ Κ Υ Ν Γ

Π Ν Γ Η Σ Α Ι Β Α Ρ Α Π Δ Σ Η

Υ Ε Λ Α Χ Ι Σ Τ Ο Π Ο Ι Η Σ Η

Ρ Θ Β Α Ξ Ρ Λ Ο Φ Τ Θ Ψ Ζ Ω Ρ

Κ Η Κ Α Τ Α Σ Τ Α Σ Η Χ Φ Θ Ε

Π Τ Ν Τ Κ Ρ Δ Τ Σ Λ Ο Λ Μ Σ Θ

Κ Ο Θ Ψ Ξ Λ Χ Υ Ν Ψ Π Π Β Α Λ

ΛΙΣΤΑ ΛΕΞΕΩΝ

ΚΡΥΠΤΟΓΡΑΦΗΣΗ · ΑΝΤΙΓΡΑΦΟ · ΕΛΑΧΙΣΤΟΠΟΙΗΣΗ · ΠΡΟΣΒΑΣΗ · ΚΑΤΑΣΤΑΣΗ · ΠΑΡΑΒΙΑΣΗ · ΣΥΜΜΟΡΦΩΣΗ · ΑΠΟΚΡΥΨΗ

Σημείο ελέγχου 6, εναλλακτικά: Προσβάσιμη αντιστοίχιση λεξιλογίου

Αντιστοίχισε καθέναν από τους 8 όρους λεξιλογίου του Word Search με τον σωστό ορισμό του, γράφοντας το γράμμα (A-H) στο κενό.

ΟΡΟΙ ΛΕΞΙΛΟΓΙΟΥ

A. ΚΡΥΠΤΟΓΡΑΦΗΣΗ

B. ΑΝΤΙΓΡΑΦΟ

C. ΕΛΑΧΙΣΤΟΠΟΙΗΣΗ

D. ΠΡΟΣΒΑΣΗ

E. ΚΑΤΑΣΤΑΣΗ

F. ΠΑΡΑΒΙΑΣΗ

G. ΣΥΜΜΟΡΦΩΣΗ

H. ΑΠΟΚΡΥΨΗ

ΟΡΙΣΜΟΙ ΚΑΙ ΠΕΔΙΑ ΑΝΤΙΣΤΟΙΧΙΣΗΣ

_____ 1. Περιστατικό ασφαλείας όπου προστατευμένα δεδομένα προσπελάζονται ή αποκαλύπτονται χωρίς εξουσιοδότηση.

_____ 2. Αντικατάσταση ευαίσθητων χαρακτήρων σε πεδία βάσεων δεδομένων για την προστασία προσωπικών ταυτοτήτων.

_____ 3. Περιορισμός των δικαιωμάτων ανάγνωσης και εγγραφής στη βάση δεδομένων σε πιστοποιημένους ρόλους χρηστών.

_____ 4. Η συνολική κατάσταση ασφαλείας και η ετοιμότητα άμυνας του cloud ενός οργανισμού.

_____ 5. Τήρηση κανονιστικών προτύπων, όπως ο GDPR ή ο CCPA, για τη διαχείριση ιδιωτικών πληροφοριών χρηστών.

_____ 6. Περιορισμός της συλλογής προσωπικών δεδομένων στο απόλυτο ελάχιστο που απαιτείται για τις λειτουργίες.

_____ 7. Μετατροπή απλού κειμένου σε μη αναγνώσιμο κρυπτογραφημένο κείμενο, ώστε τα δεδομένα που υποκλέπτονται να παραμένουν ιδιωτικά.

_____ 8. Δημιουργία ασφαλών αντιγράφων δεδομένων εκτός χώρου για επαναφορά σε περίπτωση αστοχιών του συστήματος.

Σημείο ελέγχου 7: Πρόκληση ανακατεμένων λέξεων

Αποκωδικοποίησε τα γράμματα παρακάτω για να αποκαλύψεις βασικές έννοιες και όρους της κυβερνοασφάλειας. Γράψε τις απαντήσεις σου στα διαθέσιμα πλαίσια εισαγωγής.

1. **ΓΥΑΣΟΡΡΦΚΗΗΤΠ**
2. **ΙΛΣΑΤΣΕΗΟΗΟΙΠΧ**
3. **ΚΤΣΑΑΗΑΣΤ**
4. **ΡΣΟΗΜΩΦΣΥΜ**
5. **ΑΓΝΟΡΙΑΦΤ**
6. **ΣΗΣΑΠΒΡΟ**
7. **ΙΠΣΗΑΑΑΒΡ**
8. **ΚΠΡΗΑΨΥΟ**

Δραστηριότητα μπόνους: Σκέψου γρήγορα

3 ΑΠΑΝΤΗΣΕΙΣ ΓΙΑ ΚΑΘΕ ΚΑΤΗΓΟΡΙΑ. ΚΕΡΔΙΖΕΙ ΟΠΟΙΟΣ ΣΥΜΠΛΗΡΩΣΕΙ ΠΡΩΤΟΣ ΤΗ ΛΙΣΤΑ.

1	Πράγματα που παίρνεις αντίγραφο ασφαλείας			
2	Λέξεις που σχετίζονται με την κυβερνοασφάλεια			
3	Άνθρωποι που επιτρέπεται να βλέπουν ευαίσθητα δεδομένα			
4	Τρόποι να διαγράφεις δεδομένα με ασφάλεια			
5	Μέρη όπου αποθηκεύονται δεδομένα			
6	Πράγματα που πρέπει να κρυπτογραφούνται			
7	Δεδομένα που πρέπει να προστατεύει ένα νοσοκομείο			
8	Τύποι αντιγράφων ασφαλείας			
9	Πληροφορίες που δεν πρέπει ποτέ να μοιράζεσαι			
10	Προειδοποιητικά σημάδια σε ένα email			
11	Ασφαλείς συνήθειες που μπορείς να ξεκινήσεις σήμερα			
12	Άνθρωποι που μπορείς να ρωτήσεις για βοήθεια στην πληροφορική			
13	Συσκευές που μπορούν να παραβιαστούν			
14	Τρόποι να προστατεύσεις δεδομένα			
15	Πράγματα που μπορούν να καταστρέψουν δεδομένα			

Σημείο ελέγχου 8: Μελέτες περίπτωσης κυβερνοασφάλειας

Εφάρμοσε τις έννοιες που έμαθες για να λύσεις τα παρακάτω σενάρια πραγματικού κόσμου.

ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ 1: ΑΝΑΒΑΘΜΙΣΗ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ ΑΠΟΘΗΚΕΥΜΕΝΩΝ ΔΕΔΟΜΕΝΩΝ ΒΑΣΗΣ ΔΕΔΟΜΕΝΩΝ ΕΠΙΧΕΙΡΗΣΗΣ

👷

Σενάριο: Ένα διαδικτυακό κατάστημα λιανικής αποθηκεύει βάσεις δεδομένων συναλλαγών σε αποθήκευση cloud χωρίς πλήρη κρυπτογράφηση δίσκου. Ένας πρόσφατος έλεγχος συμμόρφωσης το επισήμανε ως σοβαρό κίνδυνο ασφάλειας δεδομένων βάσει του CCPA. Σχεδίασε μια αρχιτεκτονική ανάκτησης.

Ερώτηση συζήτησης: Ανάλυσε τους κινδύνους συμμόρφωσης με το CCPA και πρότεινε μια στρατηγική κρυπτογράφησης δεδομένων σε αδράνεια.

ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ 2: ΠΕΡΙΟΡΙΣΜΟΣ RANSOMWARE ΚΑΙ ΑΠΟΚΑΤΑΣΤΑΣΗ ΔΕΔΟΜΕΝΩΝ

👷

Σενάριο: Μια ενεργή επίθεση ransomware κρυπτογραφεί μονάδες δικτύου σε ένα εταιρικό τοπικό δίκτυο. Ο διαχειριστής έχει εντοπίσει νωρίς τη μόλυνση. Σχεδίασε τα βήματα περιορισμού και ανάκτησης.

Ερώτηση συζήτησης: Περίγραψε αναλυτικά τις άμεσες ενέργειες περιορισμού και σχεδίασε μια ασφαλή διαδικασία επαναφοράς.

Σημείο ελέγχου 9: Αποκρυπτογράφησε τον κώδικα

Ένας επαγγελματίας κυβερνοασφάλειας προστατεύει τα περιουσιακά στοιχεία του δικτύου από διαδικτυακούς φορείς απειλών. Χρησιμοποίησε το παρακάτω κλειδί Γράμμα-Αριθμός για να αποκρυπτογραφήσεις το μήνυμα γράφοντας τα αντίστοιχα γράμματα στα κενά.

ΚΛΕΙΔΙ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ ΓΡΑΜΜΑΤΟΣ ΣΕ ΑΡΙΘΜΟ

Α=1 Β=2 Γ=3 Δ=4 Ε=5 Ζ=6 Η=7 Θ=8

Ι=9 Κ=10 Λ=11 Μ=12 Ν=13 Ξ=14 Ο=15 Π=16

Ρ=17 Σ=18 Τ=19 Υ=20 Φ=21 Χ=22 Ψ=23 Ω=24

16	17	15	18	19	1	19	5	20	18	5		19	1

9	4	9	24	19	9	10	1		4	5	4	15	12	5	13	1	18	15	20

Αποκρυπτογραφημένο μήνυμα:

ΣΥΜΒΟΥΛΗ: ΚΑΘΕ ΑΡΙΘΜΟΣ ΕΚΠΡΟΣΩΠΕΙ ΤΗ ΘΕΣΗ ΤΟΥ ΓΡΑΜΜΑΤΟΣ ΣΤΟ ΑΛΦΑΒΗΤΟ (Π.Χ. 1 = Α, 2 = Β, 24 = Ω).

Σημείο ελέγχου 10: Συχνές ερωτήσεις για την κυβερνοασφάλεια – βασικό επίπεδο (Μέρος Α)

Εξέτασε συχνές ερωτήσεις και απαντήσεις για τον μετριασμό των διαδικτυακών απειλών.

Q1: Τι είναι η προστασία δεδομένων;

Είναι η διαδικασία προστασίας προσωπικών και επιχειρηματικών δεδομένων από μη εξουσιοδοτημένη πρόσβαση, απώλεια ή αλλοίωση μέσω τεχνικών ελέγχων.

Q2: Γιατί είναι σημαντική η κρυπτογράφηση ολόκληρου του δίσκου;

Ασφαλίζει τα αποθηκευμένα μπλοκ δεδομένων σε φυσικούς δίσκους, εμποδίζοντας οποιονδήποτε να διαβάσει τα δεδομένα αν κλέψει φυσικά τον σκληρό δίσκο.

Q3: Ποια είναι η διαφορά μεταξύ κρυπτογράφησης σε αδράνεια και κρυπτογράφησης κατά τη μεταφορά;

Η κρυπτογράφηση σε ηρεμία προστατεύει τα αποθηκευμένα αρχεία σε δίσκους, ενώ η κρυπτογράφηση σε διαμετακόμιση προστατεύει τα ενεργά πακέτα δικτύου που κινούνται μέσω δρομολογητών.

Q4: Τι είναι η απόκρυψη δεδομένων (data masking);

Αντικαθιστά ευαίσθητα στοιχεία (όπως αριθμούς πιστωτικών καρτών) με πλασματικά αλλά ρεαλιστικά δεδομένα για δοκιμές χωρίς έκθεση πραγματικών εγγραφών.

Q5: Γιατί είναι σημαντικό το εκτός σύνδεσης αντίγραφο ασφαλείας;

Κρατά ένα καθαρό αντίγραφο των αρχείων σου απομονωμένο από το δίκτυο, κάτι που βοηθά στην προστασία των αντιγράφων ασφαλείας σου από κρυπτογράφηση από ransomware.

Σημείο ελέγχου 10: Συχνές ερωτήσεις για την κυβερνοασφάλεια – βασικό επίπεδο (Μέρος Β)

Εξέτασε συχνές ερωτήσεις και απαντήσεις για τον μετριασμό των διαδικτυακών απειλών.

Q6: Τι είναι ένα θησαυροφυλάκιο διακριτικοποίησης δεδομένων (data tokenization vault);

Μια ασφαλής, απομονωμένη βάση δεδομένων που αντιστοιχίζει τυχαία διακριτικά (tokens) στις αρχικές ευαίσθητες τιμές τους (όπως οι κύριοι αριθμοί πιστωτικών καρτών).

Q7: Τι σημαίνει πρόσβαση βάσης δεδομένων zero-trust;

Σημαίνει επαλήθευση της ταυτότητας και της κατάστασης της συσκευής κάθε χρήστη σε κάθε σύνδεση, αντί να εμπιστεύεσαι οποιονδήποτε βρίσκεται μέσα στο δίκτυο.

Q8: Πώς προστατεύει το TLS τα δεδομένα κατά τη μεταφορά;

Το TLS κρυπτογραφεί το φορτίο της συνεδρίας TCP, εμποδίζοντας κακόβουλους παράγοντες σε δημόσια δίκτυα να υποκλέπτουν ή να τροποποιούν τα πακέτα κατά τη μεταφορά.

Q9: Τι είναι ο έλεγχος (auditing) πρόσβασης σε βάσεις δεδομένων;

Η συνεχής καταγραφή ερωτημάτων βάσης δεδομένων και συνδέσεων για τον εντοπισμό μοτίβων μη εξουσιοδοτημένης πρόσβασης ή ανωμαλιών ασφαλείας.

Q10: Τι είναι ο έλεγχος στάσης ασφαλείας σύννεφου;

Μια διαδικασία που αναλύει διαμορφώσεις cloud για τον εντοπισμό ανοιχτών θυρών, εσφαλμένα ρυθμισμένων κανόνων πρόσβασης και κενών συμμόρφωσης ασφαλείας.

Σημείο ελέγχου 10: Συχνές ερωτήσεις για την ασφάλεια – προχωρημένο επίπεδο (Μέρος C)

Εξερεύνησε προηγμένες τεχνικές πτυχές των πλαισίων ασφάλειας, της ανάλυσης κακόβουλου λογισμικού και της συμμόρφωσης δεδομένων.

Q1: Πώς λειτουργεί η κρυπτογράφηση με φάκελο (envelope encryption);

Κρυπτογραφεί τα δεδομένα με ένα κλειδί δεδομένων και στη συνέχεια κρυπτογραφεί αυτό το κλειδί δεδομένων με ένα κύριο κλειδί, απλοποιώντας την αποθήκευση και την εναλλαγή κλειδιών.

Q2: Τι είναι η ομομορφική κρυπτογράφηση;

Μια προηγμένη μέθοδος κρυπτογράφησης που επιτρέπει την εκτέλεση πράξεων απευθείας σε κρυπτογραφημένα δεδομένα χωρίς πρώτα να αποκρυπτογραφηθούν.

Q3: Γιατί χρησιμοποιείται κρυπτογράφηση σε επίπεδο στήλης στις βάσεις δεδομένων;

Κρυπτογραφεί συγκεκριμένες ευαίσθητες στήλες (όπως ΑΦΜ/SSN) μία προς μία, προστατεύοντάς τες ακόμη και αν οι διαχειριστές αποκτήσουν γενική πρόσβαση ανάγνωσης στον πίνακα.

Q4: Τι είναι η αποτροπή απώλειας δεδομένων (DLP);

Λογισμικό που παρακολουθεί τα σημεία εξόδου του δικτύου για να εντοπίζει και να μπλοκάρει μη εξουσιοδοτημένες εξερχόμενες μεταφορές ευαίσθητων αρχείων.

Q5: Πώς προστατεύουν από το ransomware τα αντίγραφα ασφαλείας write-once-read-many (WORM);

Τα αντίγραφα ασφαλείας WORM εμποδίζουν τη διαγραφή ή την τροποποίηση των αρχείων για καθορισμένο χρονικό διάστημα, αποτρέποντας το ransomware από το να κρυπτογραφήσει υπάρχοντα αντίγραφα ασφαλείας.

Σημείο ελέγχου 10: Συχνές ερωτήσεις για την ασφάλεια – προχωρημένο επίπεδο (Μέρος D)

Εξερεύνησε προηγμένες τεχνικές πτυχές των πλαισίων ασφάλειας, της ανάλυσης κακόβουλου λογισμικού και της συμμόρφωσης δεδομένων.

Q6: Ποιος είναι ο κίνδυνος της επαναχρησιμοποίησης κλειδιών;

Η επαναχρησιμοποίηση του ίδιου κρυπτογραφικού κλειδιού σε διαφορετικές βάσεις δεδομένων σημαίνει ότι η παραβίαση ενός κλειδιού εκθέτει όλες τις βάσεις δεδομένων.

Q7: Πώς βελτιώνει η διακριτικοποίηση (tokenization) βάσεων δεδομένων τη συμμόρφωση με τον CCPA;

Τα διακριτικά (tokens) ψευδωνυμοποιούν εγγραφές σε συστήματα εκτός παραγωγής και περιορίζουν την έκθεση σε παραβιάσεις, αλλά τα δεδομένα με διακριτικά μπορεί και πάλι να αποτελούν προσωπικές πληροφορίες.

Q8: Γιατί είναι κρίσιμη η ταξινόμηση δεδομένων;

Κατηγοριοποιεί τα αρχεία ανά επίπεδο ευαισθησίας, βοηθώντας τους οργανισμούς να εφαρμόζουν την ισχυρότερη κρυπτογράφηση και τους ελέγχους πρόσβασης στα δεδομένα υψηλού κινδύνου.

Q9: Ποιος είναι ο ρόλος της περιστροφής κλειδιών;

Η τακτική ενημέρωση των κλειδιών κρυπτογράφησης περιορίζει την ποσότητα ιστορικών δεδομένων που εκτίθενται αν σπάσει τελικά ένα μεμονωμένο κλειδί.

Q10: Πώς προστατεύουν τα ασφαλή enclaves τα ερωτήματα βάσεων δεδομένων στη μνήμη;

Οι ασφαλείς περιοχές (secure enclaves) απομονώνουν τις λειτουργίες ερωτημάτων σε μπλοκ μνήμης προστατευμένα από την CPU, εμποδίζοντας τους διαχειριστές του διακομιστή να βλέπουν καθαρό κείμενο στη RAM.

Μέρος 11: 10 πραγματικά στοιχεία και διαπιστώσεις για την κυβερνοασφάλεια

Εξέτασε πραγματικά στοιχεία για τις παραβιάσεις ασφαλείας, τους μηχανισμούς άμυνας και τα πρότυπα συμμόρφωσης.

1. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Ο κανονισμός GDPR τέθηκε σε ισχύ τον Μάιο του 2018, αλλάζοντας τον τρόπο με τον οποίο οι παγκόσμιοι ιστότοποι διαχειρίζονται τις συναινέσεις για cookies και τα μητρώα προσωπικών δεδομένων.

2. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Ένα πρόστιμο για παράβαση του GDPR μπορεί να φτάσει τα 20 εκατομμύρια ευρώ ή το 4% του παγκόσμιου κύκλου εργασιών, γεγονός που συνεπάγεται σημαντική νομική έκθεση. [4]

3. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Ο CCPA τέθηκε σε ισχύ τον Ιανουάριο του 2020, καθιερώνοντας πρωτοποριακά δικαιώματα ψηφιακής ιδιωτικότητας για τους καταναλωτές στις Ηνωμένες Πολιτείες.

4. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Η ελαχιστοποίηση δεδομένων μειώνει το αποτύπωμα αποθήκευσης της βάσης δεδομένων, περιορίζοντας το κόστος λειτουργίας των διακομιστών και μειώνοντας την έκταση μιας παραβίασης.

5. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Ο κρυπτογραφικός τεμαχισμός (shredding) λύνει την πρόκληση της διαγραφής αντιγράφων ασφαλείας διαγράφοντας τα κλειδιά αντί να επεξεργάζεται ιστορικά αρχεία ταινιών αντιγράφων.

6. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Οι περισσότερες χώρες παγκοσμίως έχουν πλέον θεσπίσει νόμους προστασίας προσωπικών δεδομένων για την προστασία των δικαιωμάτων απορρήτου των καταναλωτών.

7. ΕΙΔΗΣΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Οι φόρμες συγκατάθεσης opt-in με προεπιλεγμένα τσεκαρισμένα πλαίσια απαγορεύονται ρητά σύμφωνα με τους ευρωπαϊκούς κανονιστικούς ορισμούς για την ιδιωτικότητα δεδομένων.

8. ΕΙΔΗΣΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Ο GDPR απαιτεί την αναφορά παραβιάσεων προσωπικών δεδομένων στην εποπτική αρχή εντός 72 ωρών από τη στιγμή που λαμβάνεται γνώση, όπου αυτό είναι εφικτό. [3]

9. ΕΙΔΗΣΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Η κατακερματοποίηση (hashing) κωδικών πρόσβασης με αργούς αλγορίθμους όπως οι bcrypt ή Argon2 κάνει πολύ δυσκολότερη τη σπάσιμο εκτός σύνδεσης κλεμμένων κατακερματισμών. [6]

10. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Τα δεδομένα σε ηρεμία είναι τα αποθηκευμένα αρχεία βάσεων δεδομένων, ενώ τα δεδομένα σε διαμετακόμιση αφορούν πακέτα που κινούνται ενεργά μέσω δρομολογητών δικτύου.

Τεχνικές αναφορές και πηγές

Ο οδηγός μελέτης και τα διαδραστικά παζλ έχουν συνταχθεί από παγκόσμια πρότυπα NIST, OWASP και συμμόρφωσης με την ιδιωτικότητα των δεδομένων.

ΑΚΑΔΗΜΑΪΚΕΣ ΚΑΙ ΒΙΟΜΗΧΑΝΙΚΕΣ ΑΝΑΦΟΡΕΣ

[1] NIST. (2025). SP 800-88 Rev. 2, Guidelines for Media Sanitization.

https://csrc.nist.gov/pubs/sp/800/88/r2/final

[2] CISA. (2023). #StopRansomware Guide.

https://www.cisa.gov/stopransomware/ransomware-guide

[3] Intersoft Consulting. (n.d.). Art. 33 GDPR – Notification of a personal data breach to the supervisory authority.

https://gdpr-info.eu/art-33-gdpr/

[4] Intersoft Consulting. (n.d.). Art. 83 GDPR – General conditions for imposing administrative fines.

https://gdpr-info.eu/art-83-gdpr/

[5] California Privacy Protection Agency. (n.d.). Frequently Asked Questions (FAQs).

https://cppa.ca.gov/faq.html

[6] OWASP. (n.d.). Password Storage Cheat Sheet.

https://cheatsheetseries.owasp.org/cheatsheets/Password_Storage_Cheat_Sheet.html

Λύσεις: Σημείο ελέγχου 1 – Πολλαπλής επιλογής

1 Ερώτηση 1

Σωστή απάντηση: A

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Ποιος είναι ο κύριος σκοπός της συγκάλυψης δεδομένων (data masking); → Αντικατάσταση ευαίσθητων αναγνωριστικών με φανταστικούς αλλά ρεαλιστικούς χαρακτήρες για την προστασία της ιδιωτικότητας

2 Ερώτηση 2

Σωστή απάντηση: A

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Ποιος μηχανισμός κρυπτογραφεί τα αρχεία που είναι αποθηκευμένα στον σκληρό δίσκο ενός διακομιστή βάσης δεδομένων; → Κρυπτογράφηση ολόκληρου του δίσκου σε κατάσταση ηρεμίας

3 Ερώτηση 3

Σωστή απάντηση: A

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Τι αντιπροσωπεύει τα δεδομένα σε μετάδοση; → Πακέτα δεδομένων που κινούνται μέσω δρομολογητών και διακοπτών δικτύου

4 Ερώτηση 4

Σωστή απάντηση: A

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Γιατί είναι κρίσιμο ένα τακτικό αντίγραφο ασφαλείας εκτός σύνδεσης για την προστασία από ransomware; → Παρέχει ένα καθαρό αντίγραφο εκτός σύνδεσης για την επαναφορά αρχείων χωρίς πληρωμή λύτρων

5 Ερώτηση 5

Σωστή απάντηση: A

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Τι κάνει η διακριτικοποίηση δεδομένων (tokenization); → Αντικαθιστά ευαίσθητους αριθμούς καρτών με μη ευαίσθητα τυχαία διακριτικά (tokens)

Λύσεις: Σημείο ελέγχου 2 – Σωστό ή Λάθος

6 Ερώτηση 6

Σωστή απάντηση: Λάθος

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Η απόκρυψη (masking) αλλοιώνει αντίγραφα δοκιμών ή κρύβει τιμές κατά την ερώτηση· οι εγγραφές παραγωγής παραμένουν αμετάβλητες.

7 Ερώτηση 7

Σωστή απάντηση: Σωστό

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Τα αντίγραφα ασφαλείας εκτός χώρου πρέπει να απομονώνονται από το κύριο εταιρικό δίκτυο ώστε να αποφεύγεται η εξάπλωση ransomware.

8 Ερώτηση 8

Σωστή απάντηση: Λάθος

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Τα πιστοποιητικά TLS προστατεύουν τα δεδομένα κατά τη μεταφορά· τα δεδομένα σε αδράνεια χρειάζονται κρυπτογράφηση δίσκου, αρχείων ή βάσης δεδομένων.

9 Ερώτηση 9

Σωστή απάντηση: Σωστό

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Το zero-trust network access (ZTNA) επαληθεύει την ταυτότητα κάθε χρήστη πριν παραχωρήσει πρόσβαση σε βάση δεδομένων.

10 Ερώτηση 10

Σωστή απάντηση: Σωστό

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Η tokenization με θησαυροφυλάκιο κρατά τις αρχικές τιμές σε ασφαλές θησαυροφυλάκιο διακριτικών που αντιστοιχίζει κάθε διακριτικό στα δεδομένα του.

Λύσεις λεξιλογίου και κριτήρια βαθμολόγησης

Κριτήρια βαθμολόγησης για τον εκπαιδευτικό: Δώσε 1 μονάδα για κάθε σωστή αντιστοίχιση (σύνολο 8 μονάδες) και για κάθε όρο περιεχομένου (σύνολο 6 μονάδες).

ΣΗΜΕΙΟ ΕΛΕΓΧΟΥ 4: ΛΥΣΕΙΣ – ΑΝΤΙΣΤΟΙΧΙΣΗ ΕΝΝΟΙΩΝ

B 1. ΚΡΥΠΤΟΓΡΑΦΗΣΗ	A 2. ΑΝΤΙΓΡΑΦΟ ΑΣΦΑΛΕΙΑΣ	H 3. ΕΛΑΧΙΣΤΟΠΟΙΗΣΗ	F 4. ΠΡΟΣΒΑΣΗ
C 5. ΣΤΑΣΗ ΑΣΦΑΛΕΙΑΣ	E 6. ΔΙΑΡΡΗΞΗ	D 7. ΣΥΜΜΟΡΦΩΣΗ	G 8. ΑΠΟΚΡΥΨΗ

ΣΗΜΕΙΟ ΕΛΕΓΧΟΥ 3: ΛΥΣΕΙΣ – ΒΑΣΙΚΟΙ ΟΡΟΙ

1 ΑΠΟΚΡΥΨΗ	2 ΣΕ ΑΔΡΑΝΕΙΑ	3 ΣΕ ΜΕΤΑΔΟΣΗ	4 ΠΡΟΣΒΑΣΗ
5 ΑΝΤΙΓΡΑΦΟ	6 ΚΑΤΑΣΤΑΣΗ		

ΣΗΜΕΙΟ ΕΛΕΓΧΟΥ 6, ΕΝΑΛΛΑΚΤΙΚΑ: ΛΥΣΕΙΣ – ΑΝΤΙΣΤΟΙΧΙΣΗ ΛΕΞΕΩΝ

1 F – ΠΑΡΑΒΙΑΣΗ	2 H – ΑΠΟΚΡΥΨΗ	3 D – ΠΡΟΣΒΑΣΗ	4 E – ΚΑΤΑΣΤΑΣΗ
5 G – ΣΥΜΜΟΡΦΩΣΗ	6 C – ΕΛΑΧΙΣΤΟΠΟΙΗΣΗ	7 A – ΚΡΥΠΤΟΓΡΑΦΗΣΗ	8 B – ΑΝΤΙΓΡΑΦΟ

ΣΗΜΕΙΩΣΕΙΣ ΣΥΖΗΤΗΣΗΣ ΓΙΑ ΕΚΠΑΙΔΕΥΤΙΚΟΥΣ

Βασικοί όροι:
Έλεγξε αν οι μαθητές μπορούν να εξηγήσουν με δικά τους λόγια τους όρους ΚΡΥΠΤΟΓΡΑΦΗΣΗ, ΑΝΤΙΓΡΑΦΟ ΑΣΦΑΛΕΙΑΣ και ΕΛΑΧΙΣΤΟΠΟΙΗΣΗ και να δώσουν ένα παράδειγμα για τον καθένα.

Μελέτες περίπτωσης:
Ζήτησε από τους μαθητές να στηρίζουν τις προτάσεις τους σε στοιχεία του φύλλου εργασίας και όχι σε υποθέσεις.

Αξιολόγηση πηγών:
Ζήτησε από τους μαθητές να επαληθεύσουν τουλάχιστον έναν ισχυρισμό στις πηγές του φύλλου και συζητήστε γιατί οι αριθμοί, οι τιμές και οι κανόνες μπορεί να αλλάζουν με τον χρόνο.

Λύσεις γρίφων και σημειώσεις για τον εκπαιδευτικό

ΛΥΣΗ ΓΡΙΦΟΥ ΛΕΞΕΩΝ

Η	Ο	Η	Θ	Η	Ν	Θ	Π	Ζ	Λ	Σ	Λ	Ρ	Χ	Η
Σ	Φ	Θ	Β	Τ	Σ	Ζ	Ψ	Ξ	Ψ	Χ	Σ	Η	Ψ	Π
Η	Α	Τ	Χ	Α	Ο	Ω	Υ	Ν	Ν	Ω	Ξ	Υ	Ρ	Θ
Φ	Ρ	Ο	Σ	Θ	Ο	Υ	Φ	Τ	Ξ	Υ	Ρ	Ο	Τ	Κ
Α	Γ	Α	Ε	Ξ	Μ	Λ	Α	Ρ	Ν	Κ	Σ	Υ	Ζ	Η
Ρ	Ι	Ο	Π	Χ	Ψ	Ι	Κ	Υ	Ο	Β	Ι	Ω	Φ	Ψ
Γ	Τ	Ο	Κ	Θ	Ω	Ι	Ι	Π	Α	Μ	Ν	Α	Ε	Θ
Ο	Ν	Α	Σ	Α	Ι	Ε	Α	Σ	Φ	Ε	Μ	Κ	Ω	Κ
Τ	Α	Ε	Κ	Π	Ν	Ι	Η	Α	Ζ	Ξ	Κ	Υ	Ν	Γ
Π	Ν	Γ	Η	Σ	Α	Ι	Β	Α	Ρ	Α	Π	Δ	Σ	Η
Υ	Ε	Λ	Α	Χ	Ι	Σ	Τ	Ο	Π	Ο	Ι	Η	Σ	Η
Ρ	Θ	Β	Α	Ξ	Ρ	Λ	Ο	Φ	Τ	Θ	Ψ	Ζ	Ω	Ρ
Κ	Η	Κ	Α	Τ	Α	Σ	Τ	Α	Σ	Η	Χ	Φ	Θ	Ε
Π	Τ	Ν	Τ	Κ	Ρ	Δ	Τ	Σ	Λ	Ο	Λ	Μ	Σ	Θ
Κ	Ο	Θ	Ψ	Ξ	Λ	Χ	Υ	Ν	Ψ	Π	Π	Β	Α	Λ

ΛΥΣΗ ΣΤΑΥΡΟΛΕΞΟΥ

						K	A	T	A	Σ	T	A	Σ	H
						P								
					Σ	Y	M	M	O	P	Φ	Ω	Σ	H
						Π								
		Π				T								
E	Λ	A	X	I	Σ	T	O	Π	O	I	H	Σ	H	
		P				Γ								Π
		A				P								P
		B				A	N	T	I	Γ	P	A	Φ	O
		I				Φ								Σ
		A				H								B
		Σ				Σ								A
		H				H								Σ
							A	Π	O	K	P	Y	Ψ	H

ΟΔΗΓΟΣ ΕΚΠΑΙΔΕΥΤΙΚΟΥ ΓΙΑ ΤΙΣ ΛΥΣΕΙΣ ΤΟΥ ΣΤΑΥΡΟΛΕΞΟΥ

ΟΡΙΖΟΝΤΙΑ

1 οριζόντια: ΚΑΤΑΣΤΑΣΗ Η συνολική κατάσταση ασφαλείας και η ετοιμότητα άμυνας του cloud ενός οργανισμού (9 γράμματα)

2 οριζόντια: ΣΥΜΜΟΡΦΩΣΗ Τήρηση κανονιστικών προτύπων, όπως ο GDPR ή ο CCPA, για τη διαχείριση ιδιωτικών πληροφοριών χρηστών (10 γράμματα)

4 οριζόντια: ΕΛΑΧΙΣΤΟΠΟΙΗΣΗ Περιορισμός της συλλογής προσωπικών δεδομένων στο απόλυτο ελάχιστο που απαιτείται για τις λειτουργίες (14 γράμματα)

6 οριζόντια: ΑΝΤΙΓΡΑΦΟ Δημιουργία ασφαλών αντιγράφων δεδομένων εκτός χώρου για επαναφορά σε περίπτωση αστοχιών του συστήματος (9 γράμματα)

7 οριζόντια: ΑΠΟΚΡΥΨΗ Αντικατάσταση ευαίσθητων χαρακτήρων σε πεδία βάσεων δεδομένων για την προστασία προσωπικών ταυτοτήτων (8 γράμματα)

ΚΑΘΕΤΑ

1 κάθετα: ΚΡΥΠΤΟΓΡΑΦΗΣΗ Μετατροπή απλού κειμένου σε μη αναγνώσιμο κρυπτογραφημένο κείμενο, ώστε τα δεδομένα που υποκλέπτονται να παραμένουν ιδιωτικά (13 γράμματα)

3 κάθετα: ΠΑΡΑΒΙΑΣΗ Περιστατικό ασφαλείας όπου προστατευμένα δεδομένα προσπελάζονται ή αποκαλύπτονται χωρίς εξουσιοδότηση (9 γράμματα)

5 κάθετα: ΠΡΟΣΒΑΣΗ Περιορισμός των δικαιωμάτων ανάγνωσης και εγγραφής στη βάση δεδομένων σε πιστοποιημένους ρόλους χρηστών (8 γράμματα)

Λύσεις: ανακατεμένες λέξεις και λύση κώδικα

Κλειδί βαθμολόγησης για τη δραστηριότητα αποκωδικοποίησης λέξεων λεξιλογίου και την πρόκληση Secret Cipher.

ΛΥΣΕΙΣ ΑΝΑΜΕΙΞΗΣ ΛΕΞΕΩΝ

1. ΓΥΑΣΟΡΡΦΚΗΗΤΠ — **ΚΡΥΠΤΟΓΡΑΦΗΣΗ**
2. ΙΛΣΑΤΣΕΗΟΗΟΙΠΧ — **ΕΛΑΧΙΣΤΟΠΟΙΗΣΗ**
3. ΚΤΣΑΑΗΑΣΤ — **ΚΑΤΑΣΤΑΣΗ**
4. ΡΣΟΗΜΩΦΣΥΜ — **ΣΥΜΜΟΡΦΩΣΗ**
5. ΑΓΝΟΡΙΑΦΤ — **ΑΝΤΙΓΡΑΦΟ**
6. ΣΗΣΑΠΒΡΟ — **ΠΡΟΣΒΑΣΗ**
7. ΙΠΣΗΑΑΑΒΡ — **ΠΑΡΑΒΙΑΣΗ**
8. ΚΠΡΗΑΨΥΟ — **ΑΠΟΚΡΥΨΗ**

ΚΛΕΙΔΙ ΠΡΟΚΛΗΣΗΣ ΜΥΣΤΙΚΟΥ ΚΩΔΙΚΑ

"ΠΡΟΣΤΑΤΕΥΣΕ ΤΑ ΙΔΙΩΤΙΚΑ ΔΕΔΟΜΕΝΑ ΣΟΥ"

Λύσεις των μελετών περίπτωσης

A Μελέτη περίπτωσης 1: Αναβάθμιση κρυπτογράφησης αποθηκευμένων δεδομένων βάσης δεδομένων επιχείρησης

Λύση για τον εκπαιδευτικό

ΟΔΗΓΙΕΣ ΒΑΘΜΟΛΟΓΗΣΗΣ

Οι απαντήσεις των μαθητών πρέπει να καλύπτουν τα εξής σημεία:

- Ανάλυση σεναρίου: Ένα ηλεκτρονικό κατάστημα αποθηκεύει βάσεις δεδομένων συναλλαγών σε αποθηκευτικό χώρο cloud χωρίς κρυπτογράφηση ολόκληρου του δίσκου. Ένας πρόσφατος έλεγχος συμμόρφωσης το επισήμανε ως σοβαρό κίνδυνο ασφάλειας δεδομένων βάσει του CCPA. Σχεδίασε μια αρχιτεκτονική ανάκτησης.
- Προτεινόμενη στρατηγική και λύση: Εφάρμοσε κρυπτογράφηση ολόκληρου του δίσκου AES-256 σε κατάσταση ηρεμίας σε όλα τα συστήματα αρχείων. Χρησιμοποίησε μια κεντρική υπηρεσία διαχείρισης κλειδιών (KMS) με αυτόματη εναλλαγή και επίβαλε αυστηρές πολιτικές IAM για τον έλεγχο της πρόσβασης αποκρυπτογράφησης.

B Μελέτη περίπτωσης 2: Περιορισμός ransomware και αποκατάσταση δεδομένων

Λύση για τον εκπαιδευτικό

ΟΔΗΓΙΕΣ ΒΑΘΜΟΛΟΓΗΣΗΣ

Οι απαντήσεις των μαθητών πρέπει να καλύπτουν τα εξής σημεία:

- Ανάλυση σεναρίου: Μια ενεργή επίθεση ransomware κρυπτογραφεί δίσκους δικτύου σε εταιρικό τοπικό δίκτυο. Ο διαχειριστής έχει εντοπίσει νωρίς τη μόλυνση. Σχεδίασε τα βήματα περιορισμού και ανάκτησης.
- Προτεινόμενη στρατηγική και λύση: Απομόνωσε αμέσως το παραβιασμένο τμήμα. Διαμόρφωσε εκ νέου τα επηρεασμένα τερματικά και επανάφερε από το πιο πρόσφατο αντίγραφο ασφαλείας εκτός σύνδεσης, τύπου εγγραφής-μία-φορά-ανάγνωσης-πολλές (WORM). Επαλήθευσε την ακεραιότητα του αντιγράφου πριν επανασυνδέσεις τα συστήματα.