Όνομα: _____ Ημερομηνία: _____ Βαθμολογία: _____

Αρχιτεκτονική και ασφάλεια Zero Trust

Συνεχής επαλήθευση, μικροτμηματοποίηση δικτύου, διαχείριση ταυτότητας και πρόσβασης, ελάχιστα δικαιώματα και έλεγχοι στάσης ασφαλείας.

ΕΠΙΣΚΟΠΗΣΗ ΜΑΘΗΣΗΣ ΑΣΦΑΛΕΙΑΣ ZERO TRUST

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 στην αρχιτεκτονική και την ασφάλεια Zero Trust. Θα εξερευνήσεις τη συνεχή επαλήθευση, τον μικροκερματισμό του δικτύου, τη διαχείριση ταυτότητας και πρόσβασης (IAM), τα ελάχιστα δικαιώματα και τον έλεγχο συνεδριών.

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/zero-trust-kybernetiki-asfaleia/

Η πορεία μάθησής σου: στρατηγική Zero Trust

- Κατανόησε τη βασική αρχή της συνεχούς επαλήθευσης.
- Εφάρμοσε μικροτμηματοποίηση δικτύου και πρόσβαση ελάχιστων προνομίων.
- Ρύθμισε ελέγχους στάσης ασφαλείας συσκευών και ενεργό έλεγχο συνεδριών.

ΟΔΗΓΙΕΣ ΓΙΑ ΤΟΝ ΟΔΗΓΟ ΑΣΦΑΛΕΙΑΣ ZERO TRUST

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 αρχιτεκτονική Zero Trust. Ολοκλήρωσε με τη δραστηριότητα μπόνους Σκέψου γρήγορα.

ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΚΑΙ ΑΣΦΑΛΕΙΑ ZERO TRUST (ΕΙΣΑΓΩΓΗ)

Η ασφάλεια Zero Trust αντικαθιστά τα παλιά μοντέλα περιμέτρου δικτύου με αυστηρή πολιτική «ποτέ μην εμπιστεύεσαι, πάντα επαλήθευε». Η εφαρμογή μικροτμηματοποίησης, διαχείρισης ταυτότητας και πρόσβασης (IAM), δικαιωμάτων ελάχιστου προνομίου και ελέγχων κατάστασης αποκλείει την πλευρική κίνηση των απειλών.

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

Σημείο ελέγχου 1: Πρόκληση πολλαπλής επιλογής

1. **1. Ποια είναι η βασική αρχή της ασφάλειας Zero Trust;**
   - A. Ποτέ μην εμπιστεύεσαι, πάντα επαλήθευε κάθε αίτημα πρόσβασης ανεξάρτητα από την πηγή
   - B. Η παραδοχή ότι όλη η κίνηση εντός του εταιρικού τείχους προστασίας είναι ασφαλής
   - C. Αποθήκευση αρχείων βάσης δεδομένων χωρίς κρυπτογράφηση για μεγαλύτερη ταχύτητα
   - D. Επιβολή ταυτοποίησης email μόνο με εγγραφές SPF

2. **2. Τι είναι η μικροτμηματοποίηση δικτύου;**
   - A. Διαίρεση των δικτύων σε μικρές, απομονωμένες ζώνες για τον περιορισμό της πλευρικής κίνησης
   - B. Κρυπτογράφηση καρτών δικτύου κατά τη μετάδοση δεδομένων
   - C. Σύνδεση όλων των τοπικών διακομιστών σε μία δημόσια διεύθυνση IP
   - D. Παρακολούθηση των πληκτρολογήσεων του χρήστη σε συνεδρίες προγράμματος περιήγησης

3. **3. Ποια είναι η αρχή των ελάχιστων προνομίων;**
   - A. Περιορισμός των δικαιωμάτων πρόσβασης του χρήστη σε όσα είναι απαραίτητα για την εργασία του
   - B. Παραχώρηση όλων των προνομίων συστήματος σε κάθε χρήστη από προεπιλογή
   - C. Επιτρέποντας ανώνυμες συνδέσεις σε εταιρικούς διακομιστές βάσεων δεδομένων
   - D. Ρύθμιση δημόσιων δρομολογητών Wi-Fi χωρίς κωδικούς πρόσβασης

4. **4. Τι είναι η Διαχείριση Ταυτότητας και Πρόσβασης (IAM);**
   - A. Πλαίσια διαχείρισης ψηφιακών ταυτοτήτων και ελέγχου των προνομίων του συστήματος
   - B. Βοηθητικά προγράμματα antivirus που σαρώνουν τοπικούς καταλόγους αρχείων
   - C. Ένα σύστημα αποθήκευσης αντιγράφων ασφαλείας με μέσα απομονωμένα από το δίκτυο (air-gapped)
   - D. Ένα πρωτόκολλο πύλης email που απορρίπτει πλαστά domain

5. **5. Τι σημαίνει συνεχής ταυτοποίηση;**
   - A. Επαναλαμβανόμενη επαλήθευση της ταυτότητας του χρήστη και της κατάστασης της συσκευής κατά τη διάρκεια μιας ενεργής συνεδρίας
   - B. Αλλαγή του κύριου κωδικού πρόσβασης κάθε 10 λεπτά
   - C. Κατακερματισμός εγγραφών βάσης δεδομένων με πολλούς αλγορίθμους
   - D. Κρυπτογράφηση πακέτων μετάδοσης δικτύου με κλειδιά TLS

Σημείο ελέγχου 2: Πρόκληση Σωστό ή Λάθος

6 Ερώτηση 6

6. Το Zero Trust υποθέτει ότι όλη η κίνηση εντός του εταιρικού τείχους προστασίας είναι ασφαλής.

○ Σωστό ○ Λάθος

7 Ερώτηση 7

7. Η μικροτμηματοποίηση (micro-segmentation) περιορίζει την ικανότητα των επιτιθέμενων να κινούνται πλευρικά ανάμεσα σε εσωτερικούς διακομιστές.

○ Σωστό ○ Λάθος

8 Ερώτηση 8

8. Τα ελάχιστα προνόμια παρέχουν από προεπιλογή πρόσβαση σε όλα τα αρχεία της βάσης δεδομένων.

○ Σωστό ○ Λάθος

9 Ερώτηση 9

9. Η συνεχής επαλήθευση ελέγχει την κατάσταση της συσκευής και τα διαπιστευτήρια σε όλη τη διάρκεια μιας συνεδρίας σύνδεσης.

○ Σωστό ○ Λάθος

10 Ερώτηση 10

10. Η εφαρμογή του Zero Trust μειώνει τον αντίκτυπο των παραβιασμένων εταιρικών συνδέσεων.

○ 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 απαίτηση διαπιστευτηρίων σε κάθε σημείο πρόσβασης είναι συνεχής _____ .

2. Ο διαχωρισμός του εταιρικού δικτύου σε μικροσκοπικές ζώνες είναι η μικρο- _____ .

3. Η διαμόρφωση ψηφιακών ταυτοτήτων και ελέγχου πρόσβασης χρησιμοποιεί ένα σύστημα _____ .

4. Ο περιορισμός των δικαιωμάτων των χρηστών βασίζεται στην αρχή «ελάχιστα _____ ».

5. Η αξιολόγηση της υγείας των συνδεδεμένων συσκευών σαρώνει τη _____ των συσκευών.

6. Η καταγραφή και η επισκόπηση των ενεργών συνεδριών αποτελεί _____ ασφαλείας.

ΤΡΑΠΕΖΑ ΛΕΞΕΩΝ

ΔΡΟΜΟΛΟΓΗΤΗΣ ΕΛΕΓΧΟΣ ΕΠΑΛΗΘΕΥΣΗ ΠΡΟΝΟΜΙΑ ΣΤΑΣΗ ΤΕΙΧΟΣ ΤΜΗΜΑΤΟΠΟΙΗΣΗ ΙΑΜ

Γράψε τις απαντήσεις σου εδώ:

1. | **2.**

3. | **4.**

5. | **6.**

Σημείο ελέγχου 4: Αντιστοίχιση εννοιών ασφάλειας

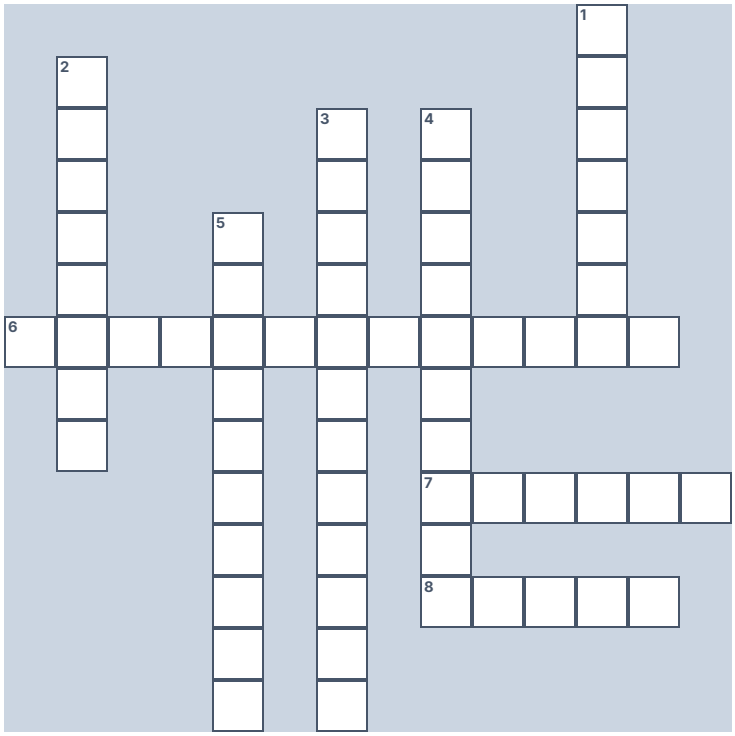
ΑΝΤΙΣΤΟΙΧΙΣΗ ΟΡΙΣΜΩΝ

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

☐	1. ΕΠΑΛΗΘΕΥΣΗ	A	Διαχείριση της πρόσβασης σε διαπιστευτήρια χρηστών.
☐	2. ΤΜΗΜΑΤΟΠΟΙΗΣΗ	B	Αρχή των ελάχιστων δικαιωμάτων πρόσβασης.
☐	3. IAM	C	Δρομολόγηση κίνησης πακέτων δικτύου.
☐	4. ΠΡΟΝΟΜΙΟ	D	Προστασία εξωτερικού φράγματος δικτύου.
☐	5. ΣΤΑΣΗ ΑΣΦΑΛΕΙΑΣ	E	Εξέταση των καταγεγραμμένων συνεδριών πρόσβασης.
☐	6. ΕΛΕΓΧΟΣ	F	Διαίρεση των εσωτερικών ζωνών δικτύου.
☐	7. ΤΕΙΧΟΣ ΠΡΟΣΤΑΣΙΑΣ	G	Έλεγχος των διαπιστευτηρίων του χρήστη σε κάθε περίπτωση.
☐	8. ΔΡΟΜΟΛΟΓΗΤΗΣ	H	Αξιολόγηση της κατάστασης υγείας της συσκευής.

Σημείο ελέγχου 5: Σταυρόλεξο

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



ΟΡΙΖΟΝΤΙΑ

6. Διαχωρισμός των εσωτερικών ζωνών του δικτύου (13)

7. Προστασία του εξωτερικού ορίου του δικτύου (τείχος προστασίας) (6)

8. Αξιολόγηση της κατάστασης υγείας των συσκευών (5)

ΚΑΘΕΤΑ

1. Επισκόπηση των καταγεγραμμένων συνεδριών πρόσβασης (7)

2. Αρχή των ελάχιστων δικαιωμάτων πρόσβασης (8)

3. Δρομολόγηση της κίνησης των πακέτων δικτύου (12)

4. Διαχείριση ταυτοτήτων και πρόσβασης των χρηστών (IAM) (10)

5. Συνεχής έλεγχος των διαπιστευτηρίων των χρηστών (10)

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

6 οριζόντια: Διαχωρισμός των εσωτερικών ζωνών του δικτύου (13 γράμματα):

7 οριζόντια: Προστασία του εξωτερικού ορίου του δικτύου (τείχος προστασίας) (6 γράμματα):

8 οριζόντια: Αξιολόγηση της κατάστασης υγείας των συσκευών (5 γράμματα):

ΚΑΘΕΤΑ

1 κάθετα: Επισκόπηση των καταγεγραμμένων συνεδριών πρόσβασης (7 γράμματα):

2 κάθετα: Αρχή των ελάχιστων δικαιωμάτων πρόσβασης (8 γράμματα):

3 κάθετα: Δρομολόγηση της κίνησης των πακέτων δικτύου (12 γράμματα):

4 κάθετα: Διαχείριση ταυτοτήτων και πρόσβασης των χρηστών (IAM) (10 γράμματα):

5 κάθετα: Συνεχής έλεγχος των διαπιστευτηρίων των χρηστών (10 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.

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

ΛΙΣΤΑ ΛΕΞΕΩΝ

ΕΠΑΛΗΘΕΥΣΗ ΤΜΗΜΑΤΟΠΟΙΗΣΗ ΤΑΥΤΟΤΗΤΕΣ ΠΡΟΝΟΜΙΑ ΣΤΑΣΗ ΕΛΕΓΧΟΣ
ΤΕΙΧΟΣ ΔΡΟΜΟΛΟΓΗΤΗΣ

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. ΕΠΑΛΗΘΕΥΣΗ
B. ΤΜΗΜΑΤΟΠΟΙΗΣΗ
C. ΤΑΥΤΟΤΗΤΕΣ
D. ΠΡΟΝΟΜΙΑ
E. ΣΤΑΣΗ
F. ΕΛΕΓΧΟΣ
G. ΤΕΙΧΟΣ
H. ΔΡΟΜΟΛΟΓΗΤΗΣ

ΟΡΙΣΜΟΙ ΚΑΙ ΠΕΔΙΑ ΑΝΤΙΣΤΟΙΧΙΣΗΣ	
	1. Προστασία του εξωτερικού ορίου του δικτύου (τείχος προστασίας).
	2. Επισκόπηση των καταγεγραμμένων συνεδριών πρόσβασης.
	3. Αρχή των ελάχιστων δικαιωμάτων πρόσβασης.
	4. Διαχωρισμός των εσωτερικών ζωνών του δικτύου.
	5. Δρομολόγηση της κίνησης των πακέτων δικτύου.
	6. Αξιολόγηση της κατάστασης υγείας των συσκευών.
	7. Διαχείριση ταυτοτήτων και πρόσβασης των χρηστών (IAM).
	8. Συνεχής έλεγχος των διαπιστευτηρίων των χρηστών.

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. ΣΕΘΗΠΕΥΗΛΑ
2. ΕΤΤΑΟΣΗΤΤΥ
3. ΑΣΗΣΤ
4. ΣΧΙΟΤΕ
5. ΟΗΜΗΠΑΗΤΙΟΤΣΜ
6. ΙΑΝΜΠΟΡΟ
7. ΕΟΧΣΛΓΕ
8. ΓΟΟΤΟΣΔΛΡΗΗΜ

Δραστηριότητα μπόνους: Σκέψου γρήγορα

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

1	Πληροφορίες που δεν πρέπει ποτέ να μοιράζεσαι			
2	Ασφαλείς συνήθειες που μπορείς να ξεκινήσεις σήμερα			
3	Πράγματα που ελέγχονται σε μια συσκευή			
4	Πράγματα που καταγράφονται σε αρχεία καταγραφής			
5	Λέξεις που σχετίζονται με την κυβερνοασφάλεια			
6	Πράγματα που ελέγχει το Zero Trust			
7	Μέρη όπου δείχνεις ταυτότητα στην καθημερινή ζωή			
8	Τρόποι να αποδείξεις ότι είσαι πράγματι εσύ			
9	Πράγματα που κάνεις μετά από μια διαρροή δεδομένων			
10	Ενδείξεις ότι ένας υπολογιστής έχει μολυνθεί			
11	Λόγοι για να ενημερώνεις το λογισμικό			
12	Επίπεδα πρόσβασης σε μια εταιρεία			
13	Εργαλεία ασφαλείας που γνωρίζεις			
14	Ζώνες στις οποίες μπορεί να χωριστεί ένα δίκτυο			
15	Ρήσεις για την εμπιστοσύνη			

Σημείο ελέγχου 8: Μελέτες περίπτωσης κυβερνοασφάλειας

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

ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ 1: ΜΕΤΑΒΑΣΗ ΣΕ ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΔΙΚΤΥΟΥ ZERO TRUST



Σενάριο: Μια μεγάλη επιχείρηση χρησιμοποιεί προς το παρόν ένα επίπεδο εσωτερικό δίκτυο όπου οποιαδήποτε συσκευή στο τοπικό δίκτυο μπορεί να έχει πρόσβαση σε όλους τους εταιρικούς διακομιστές και βάσεις δεδομένων.

Ερώτηση συζήτησης: Σχεδίασε μια στρατηγική μικροτμηματοποίησης δικτύου για τον περιορισμό της πλευρικής κίνησης.

ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ 2: ΕΦΑΡΜΟΓΗ ΕΛΕΓΧΩΝ ΠΡΟΣΒΑΣΗΣ ΕΛΑΧΙΣΤΩΝ ΔΙΚΑΙΩΜΑΤΩΝ



Σενάριο: Τα αρχεία καταγραφής ελέγχου αποκαλύπτουν ότι προσωρινοί χρήστες βάσεων δεδομένων και εργαζόμενοι χαμηλού επιπέδου διαθέτουν καθολικά δικαιώματα ανάγνωσης και εγγραφής σε κρίσιμες λογιστικές βάσεις δεδομένων.

Ερώτηση συζήτησης: Έλεγξε και περιόρισε τα προνόμια IAM της βάσης δεδομένων για να επιβληθεί η ελάχιστη προνομιακή πρόσβαση (least privilege).

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

5	16	1	11	7	8	5	20	5		16	1	13	19	1		12	5					
12	7	4	5	13	9	10	7		5	12	16	9	18	19	15	18	20	13	7			

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 το Zero Trust;

Το Zero Trust είναι ένα πλαίσιο ασφάλειας που υποθέτει ότι οι απειλές υπάρχουν τόσο έξω όσο και μέσα στα όρια του δικτύου, απαιτώντας επαλήθευση για κάθε αίτημα. [1]

Q2: Ποιος είναι ο βασικός κανόνας του Zero Trust;

Μην εμπιστεύεσαι ποτέ, επαλήθευε πάντα.

Q3: Τι είναι ο μικροκατακερματισμός δικτύου (micro-segmentation);

Διαίρεση ενός δικτύου σε μικρά, ασφαλή λογικά τμήματα για τον έλεγχο της κίνησης και τον περιορισμό των παραβιάσεων.

Q4: Τι είναι η αρχή των ελάχιστων δικαιωμάτων;

Παροχή στους χρήστες μόνο των ελάχιστων δικαιωμάτων πρόσβασης που απαιτούνται για την εκτέλεση των συγκεκριμένων εργασιών τους. [2]

Q5: Τι σημαίνει IAM;

Διαχείριση ταυτότητας και πρόσβασης.

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

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

Q6: Πώς βοηθά ο έλεγχος κατάστασης συσκευής;

Επαληθεύει ότι μια συσκευή έχει ενημερωθεί, εκτελεί ενεργό antivirus και είναι ασφαλής πριν επιτρέψει την πρόσβαση.

Q7: Τι είναι η πλευρική κίνηση (lateral movement);

Η διαδικασία με την οποία οι επιτιθέμενοι κινούνται μέσα σε ένα δίκτυο, από έναν αρχικό παραβιασμένο κόμβο προς συστήματα μεγαλύτερης αξίας.

Q8: Αντικαθιστά το Zero Trust τα τείχη προστασίας;

Όχι, τη βελτιώνει προσθέτοντας ελέγχους με επίκεντρο την ταυτότητα και εσωτερικά τείχη προστασίας τμηματοποίησης.

Q9: Τι είναι ο συνεχής έλεγχος ταυτότητας;

Συνεχής επαλήθευση της ταυτότητας του χρήστη καθ' όλη τη διάρκεια μιας ενεργής συνεδρίας σύνδεσης και όχι μόνο στην αρχική σύνδεση.

Q10: Γιατί είναι επικίνδυνο ένα επίπεδο δίκτυο (flat network);

Σε επίπεδα δίκτυα, ένας μόνο παραβιασμένος κόμβος επιτρέπει στους επιτιθέμενους να αποκτήσουν εύκολα πρόσβαση σε οποιαδήποτε βάση δεδομένων του δικτύου.

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 αντιμετωπίζει το Zero Trust το μοντέλο περιμέτρου;

Αντικαθιστά το απαρχαιωμένο μοντέλο «κάστρου και τάφρου», μεταφέροντας την άμυνα από τα δίκτυα ορίου σε συγκεκριμένες ταυτότητες και πόρους χρηστών.

Q2: Τι είναι ένα σημείο λήψης αποφάσεων πολιτικής (PDP);

Το στοιχείο του συστήματος που αξιολογεί τα αιτήματα εξουσιοδότησης με βάση κανόνες ασφαλείας για να αποφασίσει αν θα παραχωρηθεί η πρόσβαση.

Q3: Τι είναι το σημείο επιβολής πολιτικής (PEP);

Ο κόμβος του συστήματος (όπως μια πύλη ή ένας διαμεσολαβητής) που επιτρέπει ή αποκλείει φυσικά τα αιτήματα σύνδεσης με βάση την απόφαση του PDP.

Q4: Πώς υποστηρίζει ο έλεγχος πρόσβασης βάσει ρόλων (RBAC) το Zero Trust;

Το RBAC ομαδοποιεί τα δικαιώματα σε συγκεκριμένους ρόλους, βοηθώντας να αποτραπεί η απόκτηση υπερβολικών διαχειριστικών προνομίων από τους χρήστες.

Q5: Τι είναι ο έλεγχος πρόσβασης βάσει συμφραζομένων;

Αξιολόγηση των αιτημάτων σύνδεσης με δευτερεύοντα στοιχεία, όπως γεωγραφική τοποθεσία, στάση συσκευής και ώρα σύνδεσης, για την εκτίμηση του κινδύνου.

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: Σε τι διαφέρει ο μικροκατακερματισμός δικτύου από τα τυπικά VLAN;

Τα VLAN χωρίζουν τα δίκτυα σε ευρέα λογικά τμήματα στο επίπεδο 2, ενώ ο μικροκερματισμός χρησιμοποιεί πολιτική λογισμικού για να απομονώνει μεμονωμένους φόρτους εργασίας.

Q7: Τι είναι η πρόσβαση just-in-time (JIT);

Προσωρινή παροχή αυξημένων διοικητικών δικαιωμάτων και αυτόματη ανάκλησή τους μόλις ολοκληρωθεί η εργασία.

Q8: Πώς ασφαλίζεις τα API σε ένα πλαίσιο Zero Trust;

Απαιτώντας κρυπτογραφικά υπογεγραμμένα διακριτικά OAuth και ελέγχοντας τις υπογραφές των αιτημάτων σε κάθε πύλη API.

Q9: Τι είναι ένας πελάτης πρόσβασης δικτύου μηδενικής εμπιστοσύνης (ZTNA);

Ένας πράκτορας λογισμικού που δημιουργεί ασφαλείς, κρυπτογραφημένες εξερχόμενες συνδέσεις με συγκεκριμένες εφαρμογές αντί για ακατέργαστα υποδίκτυα.

Q10: Πώς βοηθά ο έλεγχος αρχείων καταγραφής το Zero Trust;

Η συνεχής καταγραφή επιτρέπει σε αυτοματοποιημένα εργαλεία αναλύσεων ασφαλείας να εντοπίζουν ανωμαλίες και να αναστέλλουν άμεσα παράνομες συνδέσεις.

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

Οι αρχιτεκτονικές Zero Trust αντικαθιστούν το παλαιό μοντέλο «κάστρου και τάφρου» με κανόνες επαλήθευσης με επίκεντρο την ταυτότητα.

2. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Η μικρο-τμηματοποίηση δικτύου μειώνει την περιοχή που μπορεί να φτάσει το κακόβουλο λογισμικό, απομονώνοντας τα φορτία εργασίας σε μικρές προστατευμένες ζώνες.

3. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Το Zero Trust εστιάζει στην προστασία πόρων, όπως περιουσιακά στοιχεία, υπηρεσίες και λογαριασμούς, και όχι τμημάτων του δικτύου. [1]

4. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Οι πολιτικές πρόσβασης ελάχιστων προνομίων μειώνουν τον κίνδυνο διαφυγής δεδομένων από εσωτερικούς παράγοντες από τις βασικές βάσεις δεδομένων.

5. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Η επικύρωση στάσης συσκευής ελέγχει σε πραγματικό χρόνο τα επίπεδα ενημερώσεων του λειτουργικού συστήματος και την κατάσταση του ενεργού antivirus.

6. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Οι μεσίτες Zero Trust Network Access (ZTNA) μπορούν να αντικαταστήσουν ή να συμπληρώσουν τα εταιρικά VPN για να περιορίσουν το εύρος πρόσβασης των χρηστών.

7. ΕΙΔΗΣΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Η ανάθεση διοικητικών προνομίων Just-In-Time (JIT) μειώνει τον κίνδυνο κλοπής διαπιστευτηρίων σε ελεγκτές τομέα.

8. ΕΙΔΗΣΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Η συνεχής επικύρωση καταγράφει και ελέγχει τη συμπεριφορά των συνεδριών, αναστέλλοντας χρήστες που εμφανίζουν ανώμαλα μοτίβα εκτέλεσης σεναρίων.

9. ΕΙΔΗΣΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Οι παραδοσιακές άμυνες περιμέτρου αδυνατούν να αποκλείσουν πλευρικές επιθέσεις μόλις διαρρεύσει ένα διαπιστευτήριο διαχειριστή.

10. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Η Ειδική Έκδοση NIST 800-207 (2020) δίνει έναν αφηρημένο ορισμό της αρχιτεκτονικής Zero Trust, με μοντέλα ανάπτυξης. [1]

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. (2020). SP 800-207: Zero Trust Architecture.
https://csrc.nist.gov/pubs/sp/800/207/final

[2] CISA. (2023). Zero Trust Maturity Model.
https://www.cisa.gov/zero-trust-maturity-model

[3] NIST. (2025). SP 800-63B-4: Digital Identity Guidelines: Authentication and Authenticator Management.
https://pages.nist.gov/800-63-4/sp800-63b.html

[4] FBI Internet Crime Complaint Center. (2026). 2025 IC3 Annual Report.
https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

[5] CISA. (2023). #StopRansomware Guide.
https://www.cisa.gov/stopransomware/ransomware-guide

Λύσεις: Σημείο ελέγχου 1 – Πολλαπλής επιλογής

1 Ερώτηση 1 — **Σωστή απάντηση: A**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Ποια είναι η βασική αρχή της ασφάλειας Zero Trust; → Ποτέ μην εμπιστεύεσαι, πάντα επαλήθευε κάθε αίτημα πρόσβασης ανεξάρτητα από την πηγή

2 Ερώτηση 2 — **Σωστή απάντηση: A**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Τι είναι η μικροτμηματοποίηση δικτύου; → Διαίρεση των δικτύων σε μικρές, απομονωμένες ζώνες για τον περιορισμό της πλευρικής κίνησης

3 Ερώτηση 3 — **Σωστή απάντηση: A**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Ποια είναι η αρχή των ελάχιστων προνομίων; → Περιορισμός των δικαιωμάτων πρόσβασης του χρήστη σε όσα είναι απαραίτητα για την εργασία του

4 Ερώτηση 4 — **Σωστή απάντηση: A**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Τι είναι η Διαχείριση Ταυτότητας και Πρόσβασης (IAM); → Πλαίσια διαχείρισης ψηφιακών ταυτοτήτων και ελέγχου των προνομίων του συστήματος

5 Ερώτηση 5 — **Σωστή απάντηση: A**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Τι σημαίνει συνεχής ταυτοποίηση; → Επαναλαμβανόμενη επαλήθευση της ταυτότητας του χρήστη και της κατάστασης της συσκευής κατά τη διάρκεια μιας ενεργής συνεδρίας

Λύσεις: Σημείο ελέγχου 2 – Σωστό ή Λάθος

6 **Ερώτηση 6** **Σωστή απάντηση: Λάθος**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Λάθος: το Zero Trust δεν παρέχει σιωπηρή εμπιστοσύνη με βάση την τοποθεσία στο δίκτυο, μέσα ή έξω.

7 **Ερώτηση 7** **Σωστή απάντηση: Σωστό**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Σωστό: μικρές απομονωμένες ζώνες περιορίζουν πόσο μακριά μπορεί να κινηθεί ένας εισβολέας ανάμεσα σε διακομιστές.

8 **Ερώτηση 8** **Σωστή απάντηση: Λάθος**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Λάθος: η ελάχιστη προνομιακή πρόσβαση (least privilege) παρέχει μόνο την ελάχιστη πρόσβαση που χρειάζεται κάθε ρόλος.

9 **Ερώτηση 9** **Σωστή απάντηση: Σωστό**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Η συνεχής επαλήθευση ελέγχει την κατάσταση της συσκευής και τα διαπιστευτήρια σε όλη τη διάρκεια μιας συνεδρίας σύνδεσης.

10 **Ερώτηση 10** **Σωστή απάντηση: Σωστό**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Η εφαρμογή του Zero Trust μειώνει τον αντίκτυπο των παραβιασμένων εταιρικών συνδέσεων.

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

G 1. ΕΠΑΛΗΘΕΥΣΗ	F 2. ΤΜΗΜΑΤΟΠΟΙΗΣΗ	A 3. IAM	B 4. ΠΡΟΝΟΜΙΟ
H 5. ΣΤΑΣΗ ΑΣΦΑΛΕΙΑΣ	E 6. ΕΛΕΓΧΟΣ	D 7. ΤΕΙΧΟΣ ΠΡΟΣΤΑΣΙΑΣ	C 8. ΔΡΟΜΟΛΟΓΗΤΗΣ

ΣΗΜΕΙΟ ΕΛΕΓΧΟΥ 3: ΛΥΣΕΙΣ – ΒΑΣΙΚΟΙ ΟΡΟΙ

1 ΕΠΑΛΗΘΕΥΣΗ	2 ΤΜΗΜΑΤΟΠΟΙΗΣΗ	3 IAM	4 ΠΡΟΝΟΜΙΑ
5 ΣΤΑΣΗ	6 ΕΛΕΓΧΟΣ		

ΣΗΜΕΙΟ ΕΛΕΓΧΟΥ 6, ΕΝΑΛΛΑΚΤΙΚΑ: ΛΥΣΕΙΣ – ΑΝΤΙΣΤΟΙΧΙΣΗ ΛΕΞΕΩΝ

1 G – ΤΕΙΧΟΣ	2 F – ΕΛΕΓΧΟΣ	3 D – ΠΡΟΝΟΜΙΑ	4 B – ΤΜΗΜΑΤΟΠΟΙΗΣΗ
5 H – ΔΡΟΜΟΛΟΓΗΤΗΣ	6 E – ΣΤΑΣΗ	7 C – ΤΑΥΤΟΤΗΤΕΣ	8 A – ΕΠΑΛΗΘΕΥΣΗ

ΣΗΜΕΙΩΣΕΙΣ ΣΥΖΗΤΗΣΗΣ ΓΙΑ ΕΚΠΑΙΔΕΥΤΙΚΟΥΣ

Βασικοί όροι:
Έλεγξε αν οι μαθητές μπορούν να εξηγήσουν με δικά τους λόγια τους όρους ΕΠΑΛΗΘΕΥΣΗ, ΤΜΗΜΑΤΟΠΟΙΗΣΗ και IAM 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.

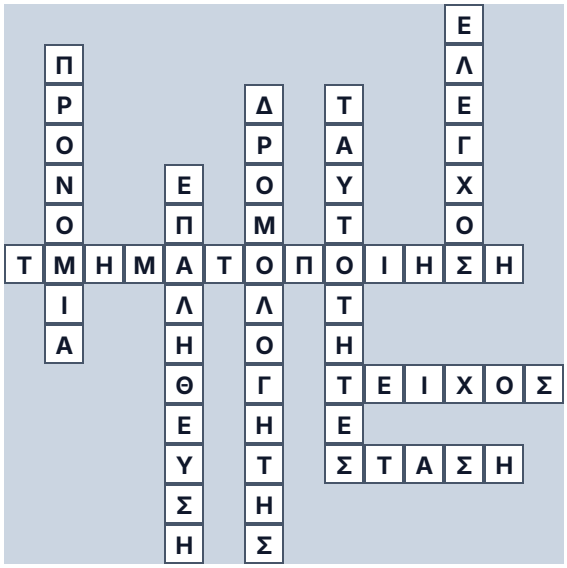
Αξιολόγηση πηγών:
Ζήτησε από τους μαθητές να επαληθεύσουν τουλάχιστον έναν ισχυρισμό στις πηγές του φύλλου και συζητήστε γιατί οι αριθμοί, οι τιμές και οι κανόνες μπορεί να αλλάζουν με τον χρόνο.

Λύσεις γρίφων και σημειώσεις για τον εκπαιδευτικό

ΛΥΣΗ ΓΡΙΦΟΥ ΛΕΞΕΩΝ

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

ΛΥΣΗ ΣΤΑΥΡΟΛΕΞΟΥ



ΟΔΗΓΟΣ ΕΚΠΑΙΔΕΥΤΙΚΟΥ ΓΙΑ ΤΙΣ ΛΥΣΕΙΣ ΤΟΥ ΣΤΑΥΡΟΛΕΞΟΥ

ΟΡΙΖΟΝΤΙΑ

6 οριζόντια: ΤΜΗΜΑΤΟΠΟΙΗΣΗ Διαχωρισμός των εσωτερικών ζωνών του δικτύου (13 γράμματα)

7 οριζόντια: ΤΕΙΧΟΣ Προστασία του εξωτερικού ορίου του δικτύου (τείχος προστασίας) (6 γράμματα)

8 οριζόντια: ΣΤΑΣΗ Αξιολόγηση της κατάστασης υγείας των συσκευών (5 γράμματα)

ΚΑΘΕΤΑ

1 κάθετα: ΕΛΕΓΧΟΣ Επισκόπηση των καταγεγραμμένων συνεδριών πρόσβασης (7 γράμματα)

2 κάθετα: ΠΡΟΝΟΜΙΑ Αρχή των ελάχιστων δικαιωμάτων πρόσβασης (8 γράμματα)

3 κάθετα: ΔΡΟΜΟΛΟΓΗΤΗΣ Δρομολόγηση της κίνησης των πακέτων δικτύου (12 γράμματα)

4 κάθετα: ΤΑΥΤΟΤΗΤΕΣ Διαχείριση ταυτοτήτων και πρόσβασης των χρηστών (IAM) (10 γράμματα)

5 κάθετα: ΕΠΑΛΗΘΕΥΣΗ Συνεχής έλεγχος των διαπιστευτηρίων των χρηστών (10 γράμματα)

Λύσεις: ανακατεμένες λέξεις και λύση κώδικα

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

ΛΥΣΕΙΣ ΑΝΑΜΕΙΞΗΣ ΛΕΞΕΩΝ

1. ΣΕΘΗΠΕΥΗΛΑ — **ΕΠΑΛΗΘΕΥΣΗ**
2. ΕΤΤΑΟΣΗΤΤΥ — **ΤΑΥΤΟΤΗΤΕΣ**
3. ΑΣΗΣΤ — **ΣΤΑΣΗ**
4. ΣΧΙΟΤΕ — **ΤΕΙΧΟΣ**
5. ΟΗΜΗΠΑΗΤΙΟΤΣΜ — **ΤΜΗΜΑΤΟΠΟΙΗΣΗ**
6. ΙΑΝΜΠΟΡΟ — **ΠΡΟΝΟΜΙΑ**
7. ΕΟΧΣΛΓΕ — **ΕΛΕΓΧΟΣ**
8. ΓΟΟΤΟΣΔΛΡΗΗΜ — **ΔΡΟΜΟΛΟΓΗΤΗΣ**

ΚΛΕΙΔΙ ΠΡΟΚΛΗΣΗΣ ΜΥΣΤΙΚΟΥ ΚΩΔΙΚΑ

"ΕΠΑΛΗΘΕΥΕ ΠΑΝΤΑ ΜΕ ΜΗΔΕΝΙΚΗ ΕΜΠΙΣΤΟΣΥΝΗ"

Λύσεις των μελετών περίπτωσης

A Μελέτη περίπτωσης 1: Μετάβαση σε αρχιτεκτονική δικτύου Zero Trust

Λύση για τον εκπαιδευτικό

ΟΔΗΓΙΕΣ ΒΑΘΜΟΛΟΓΗΣΗΣ

Οι απαντήσεις των μαθητών πρέπει να καλύπτουν τα εξής σημεία:

- Ανάλυση σεναρίου: Μια μεγάλη επιχείρηση χρησιμοποιεί σήμερα ένα επίπεδο εσωτερικό δίκτυο όπου κάθε συσκευή στο τοπικό δίκτυο μπορεί να έχει πρόσβαση σε όλους τους εταιρικούς διακομιστές και βάσεις δεδομένων.
- Προτεινόμενη στρατηγική και λύση: Τμηματοποίησε το επίπεδο δίκτυο σε απομονωμένες ζώνες τμημάτων. Εγκατάστησε εσωτερικά τείχη προστασίας για τον έλεγχο της κίνησης μεταξύ των ζωνών και επίβαλε επικύρωση διακριτικού σύνδεσης για κάθε πρόσβαση.

B Μελέτη περίπτωσης 2: Εφαρμογή ελέγχων πρόσβασης ελάχιστων δικαιωμάτων

Λύση για τον εκπαιδευτικό

ΟΔΗΓΙΕΣ ΒΑΘΜΟΛΟΓΗΣΗΣ

Οι απαντήσεις των μαθητών πρέπει να καλύπτουν τα εξής σημεία:

- Ανάλυση σεναρίου: Τα αρχεία καταγραφής ελέγχου αποκαλύπτουν ότι προσωρινοί χρήστες της βάσης δεδομένων και υπάλληλοι χαμηλού επιπέδου διαθέτουν καθολικά δικαιώματα ανάγνωσης και εγγραφής σε κρίσιμες λογιστικές βάσεις δεδομένων.
- Προτεινόμενη στρατηγική και λύση: Ανακάλεσε όλα τα καθολικά διαχειριστικά προνόμια. Εφάρμοσε έλεγχο πρόσβασης βάσει ρόλων (RBAC) που να ταιριάζει με τους ακριβείς ρόλους εργασίας και θέσπισε εβδομαδιαίους αυτοματοποιημένους ελέγχους δικαιωμάτων.