Όνομα: _____ Ημερομηνία: _____ Βαθμολογία: _____

VPN για επιχειρήσεις

Υλοποίηση πρόσβασης δικτύου Zero Trust, αποκλειστικών κόμβων πύλης και κεντρικών εταιρικών ελέγχων διαχειριστή.

ΕΠΙΣΚΟΠΗΣΗ ΜΑΘΗΣΗΣ: ΕΠΙΧΕΙΡΗΣΙΑΚΑ ΔΙΚΤΥΑ VPN

ΜΑΘΗΤΗΣ
ΙΔΙΟΤΗΤΑ ΦΟΙΤΗΤΗ
Διαδρομή Network Defender

ΑΣΦΑΛΕΣ
ΚΑΤΑΣΤΑΣΗ ΣΥΝΔΕΣΗΣ
Θωράκιση πακέτων δεδομένων

ΕΝΕΡΓΟ
ΠΡΟΣΤΑΣΙΑ ΔΙΑΡΡΟΩΝ
Προστασία από διαρροές DNS και IPv6

Καλώς ήρθες! Αυτό το φυλλάδιο δραστηριοτήτων σε καθοδηγεί στα επιχειρησιακά δίκτυα VPN. Θα εξερευνήσεις αρχιτεκτονικές Zero Trust, πύλες αποκλειστικών στατικών IP, κονσόλες διαχειριστή, παροχή πρόσβασης και σήραγγες IPsec από τοποθεσία σε τοποθεσία.

ΣΗΜΕΙΑ ΕΛΕΓΧΟΥ ΤΟΥ ΦΥΛΛΟΥ ΕΡΓΑΣΙΑΣ

- [ ] **Μέρη 1-4: Κατάκτησε τις διαμορφώσεις VPN και ασφάλειας δικτύου.**
- [ ] **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 τα καλύτερα VPN

URL: https://www.vpn.com/el/vpn/kalytero-vpn-gia-epicheiriseis-epicheirisi/

Η πορεία μάθησής σου: εταιρικό δίκτυο VPN

- Εφάρμοσε πλαίσια Zero Trust Network Access (ZTNA).
- Ρύθμισε αποκλειστικές διευθύνσεις IP πύλης διακομιστή για φίλτρα λίστας επιτρεπόμενων.
- Διαχείριση κεντρικών εταιρικών πάνελ διαχείρισης και λιστών θέσεων χρηστών.
- Έλεγξε τα αρχεία καταγραφής πρόσβασης δικτύου και το ιστορικό συνδέσεων των χρηστών.
- Ρύθμισε κανόνες Single Sign-On (SSO) και πολυπαραγοντικής ταυτοποίησης.
- Ρύθμισε τούνελ IPsec site-to-site μεταξύ υποκαταστημάτων.

ΟΔΗΓΙΕΣ ΓΙΑ ΕΠΙΧΕΙΡΗΣΙΑΚΑ ΔΙΚΤΥΑ VPN

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 στο Zero Trust και στο IPsec από σημείο σε σημείο (site-to-site). Ολοκλήρωσε με τη δραστηριότητα μπόνους Σκέψου γρήγορα.

ΑΡΧΙΤΕΚΤΟΝΙΚΕΣ ZERO TRUST ΚΑΙ ΑΠΟΚΛΕΙΣΤΙΚΕΣ ΠΥΛΕΣ (ΕΙΣΑΓΩΓΗ)

Τα VPN για επιχειρήσεις προστατεύουν τα εταιρικά περιουσιακά στοιχεία μεταβαίνοντας σε πλαίσια Zero Trust Network Access (ZTNA) και δημιουργώντας λευκή λίστα αποκλειστικών στατικών πυλών IP. Οι διαχειριστές πληροφορικής χρησιμοποιούν κεντρικές κονσόλες διαχείρισης για να ενορχηστρώνουν τούνελ IPsec site-to-site και συνδέσμους single sign-on (SSO).

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

Σημείο ελέγχου 1: Πρόκληση πολλαπλής επιλογής

1. **Ποιο μοντέλο ασφάλειας αντικαθιστά τα παλαιότερα εταιρικά VPN;**
   - A) Zero Trust
   - B) Multi-hop
   - C) Ομότιμη σύνδεση (peer-to-peer)
   - D) Μία πύλη

2. **Ποιο χαρακτηριστικό απαιτείται για να περιοριστεί η πρόσβαση στη βάση δεδομένων μόνο στους διακομιστές της εταιρείας;**
   - A) Αποκλειστική IP
   - B) Δυναμική δρομολόγηση
   - C) Διαχωρισμένο τούνελ
   - D) Διαμεσολαβητής DNS

3. **Ποιο πρωτόκολλο είναι το πρότυπο για εταιρικές σήραγγες από τοποθεσία σε τοποθεσία (site-to-site);**
   - A) IPsec
   - B) PPTP
   - C) SOCKS5
   - D) SSL v3

4. **Ποιο κεντρικό εργαλείο επιτρέπει στους διαχειριστές να διαχειρίζονται τις θέσεις των εργαζομένων;**
   - A) Κονσόλα διαχειριστή
   - B) Κλειδί μητρώου
   - C) Υλικολογισμικό δρομολογητή
   - D) Αρχείο καταγραφής συστήματος

5. **Ποιο πρότυπο ταυτοποίησης επιτρέπει τη σύνδεση μέσω Okta ή Microsoft Entra ID;**
   - A) Single Sign-On
   - B) Κοινό μυστικό
   - C) Ταυτοποίηση EPP
   - D) Κλειδί WEP

Σημείο ελέγχου 2: Πρόκληση Σωστό ή Λάθος

6 Ερώτηση 6

6. Το Zero Trust Network Access παρέχει πρόσβαση στο δίκτυο μόνο μετά από επαλήθευση της συνεχούς αξιοπιστίας της συσκευής.

- ◯ Σωστό
- ◯ Λάθος

7 Ερώτηση 7

7. Οι πύλες αποκλειστικής IP δρομολογούν την κίνηση των εργαζομένων μαζί με τυχαίους δημόσιους καταναλωτές.

- ◯ Σωστό
- ◯ Λάθος

8 Ερώτηση 8

8. Οι κεντρικές κονσόλες διαχείρισης επιτρέπουν στους διαχειριστές IT να ανακαλούν άμεσα τις θέσεις μεμονωμένων εργαζομένων.

- ◯ Σωστό
- ◯ Λάθος

9 Ερώτηση 9

9. Το IPsec είναι ένα ελαφρύ πρωτόκολλο που δεν υποστηρίζει σήραγγες δικτύου μεταξύ τοποθεσιών (site-to-site).

- ◯ Σωστό
- ◯ Λάθος

10 Ερώτηση 10

10. Το Single Sign-On επιτρέπει την ασφαλή ταυτοποίηση υπαλλήλων μέσω εταιρικών παρόχων ταυτότητας.

- ◯ 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. Οι σύγχρονες αρχιτεκτονικές ασφάλειας αντικαθιστούν τις παλιές σήραγγες με πρόσβαση _____ .

2. Για να περιορίσουν την πρόσβαση στη βάση δεδομένων, οι εταιρείες ρυθμίζουν μια πύλη με _____ .

3. Τα υποκαταστήματα συνδέονται με ασφάλεια μέσω σηράγγων site-to-site τύπου _____ .

4. Οι διαχειριστές IT κατανέμουν άδειες χρήσης στους υπαλλήλους μέσα από την κεντρική _____ .

5. Η ενσωμάτωση με το Okta επιτρέπει στους υπαλλήλους να πιστοποιούνται με την εταιρική _____ .

6. Για την προστασία των συνδέσεων, οι εταιρικές πύλες επιβάλλουν ταυτοποίηση στην οποία απαιτούνται πολλαπλοί _____ .

ΤΡΑΠΕΖΑ ΛΕΞΕΩΝ

ΕΝΙΑΙΑ ΣΥΝΔΕΣΗ ΚΟΝΣΟΛΑ ΠΑΡΑΓΟΝΤΕΣ ΠΥΛΗ ΣΗΡΑΓΓΑ
ΣΤΑΘΕΡΗ ΔΙΕΥΘΥΝΣΗ IP IPSEC ZERO TRUST

Γράψε τις απαντήσεις σου εδώ:

1. **2.**

3. **4.**

5. **6.**

Σημείο ελέγχου 4: Αντιστοίχιση βασικών εννοιών

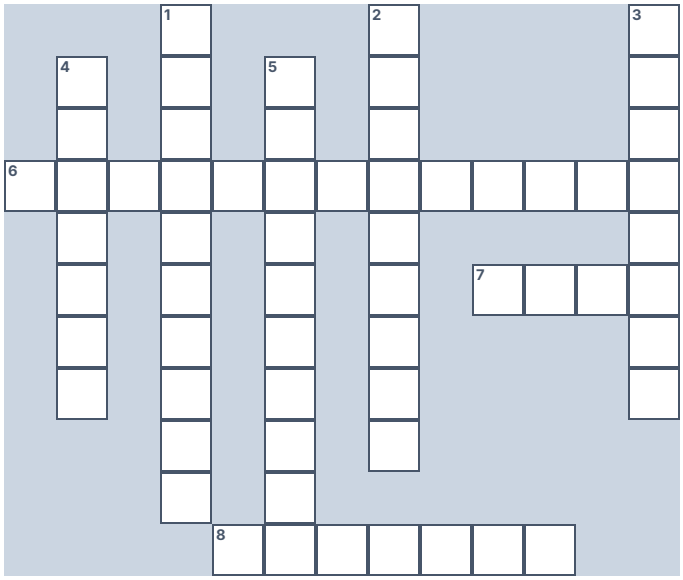
ΑΝΤΙΣΤΟΙΧΙΣΗ ΟΡΙΣΜΩΝ

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

☐	1. ΜΗΔΕΝΙΚΗ ΕΜΠΙΣΤΟΣΥΝΗ	A	Κατανομή αδειών πρόσβασης VPN στους υπαλλήλους.
☐	2. ΕΞΑΤΟΜΙΚΕΥΜΕΝΗ IP	B	Σύνδεσμος ταυτότητας Okta και Entra ID.
☐	3. IPSEC	C	Ασφάλεια σύνδεσης που απαιτεί επιπλέον διακριτικά.
☐	4. ΚΟΝΣΟΛΑ ΔΙΑΧΕΙΡΙΣΤΗ	D	Στατική διεύθυνση πύλης λίστας επιτρεπόμενων.
☐	5. ΕΝΙΑΙΑ ΣΥΝΔΕΣΗ	E	Πρότυπο τούνελ site-to-site.
☐	6. ΠΟΛΛΑΠΛΩΝ ΠΑΡΑΓΟΝΤΩΝ	F	Κόμβος δρομολόγησης εισόδου δικτύου.
☐	7. ΠΥΛΗ	G	Πύλη θέσεων του κεντρικού διαχειριστή IT.
☐	8. ΠΑΡΟΧΗ	H	Πλαίσιο συνεχούς επαλήθευσης εμπιστοσύνης.

Σημείο ελέγχου 5: Σταυρόλεξο

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



ΟΡΙΖΟΝΤΙΑ

6. Σύνδεση ταυτότητας με Okta και Entra ID (13)

7. Κόμβος δρομολόγησης στην είσοδο του δικτύου (4)

8. Ασφαλής διαδρομή που συνδέει τα δίκτυα δύο τοποθεσιών της εταιρείας (7)

ΚΑΘΕΤΑ

1. Ασφάλεια σύνδεσης που απαιτεί επιπλέον διακριτικά (10)

2. Στατική διεύθυνση πύλης για λίστα επιτρεπόμενων (9)

3. Παροχή αδειών πρόσβασης VPN στους υπαλλήλους (8)

4. Κεντρική πύλη για τους διαχειριστές IT (7)

5. Συνεχής έλεγχος ταυτότητας χρήστη και συσκευής πριν δοθεί κάθε πρόσβαση (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: Σύνδεση ταυτότητας με Okta και Entra ID (13 γράμματα):

7 οριζόντια: Κόμβος δρομολόγησης στην είσοδο του δικτύου (4 γράμματα):

8 οριζόντια: Ασφαλής διαδρομή που συνδέει τα δίκτυα δύο τοποθεσιών της εταιρείας (7 γράμματα):

ΚΑΘΕΤΑ

1 κάθετα: Ασφάλεια σύνδεσης που απαιτεί επιπλέον διακριτικά (10 γράμματα):

2 κάθετα: Στατική διεύθυνση πύλης για λίστα επιτρεπόμενων (9 γράμματα):

3 κάθετα: Παροχή αδειών πρόσβασης VPN στους υπαλλήλους (8 γράμματα):

4 κάθετα: Κεντρική πύλη για τους διαχειριστές IT (7 γράμματα):

5 κάθετα: Συνεχής έλεγχος ταυτότητας χρήστη και συσκευής πριν δοθεί κάθε πρόσβαση (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 Η Ρ Α Γ Γ Α Π Γ Σ Ο Ξ Θ Ρ Β

Φ Η Δ Σ Ω Υ Γ Α Ω Φ Δ Ζ Κ Η Ω

Η Σ Δ Ν Δ Π Χ Ρ Ο Γ Ι Τ Β Α Ω

Σ Η Ν Δ Λ Α Δ Α Ξ Δ Ε Ε Η Θ Α

Υ Γ Δ Ρ Π Μ Ε Γ Θ Ρ Υ Ω Σ Λ Ε

Ε Η Π Υ Ε Α Α Ο Π Ξ Θ Ν Ο Ο Τ

Θ Ρ Χ Π Κ Ρ Τ Ν Ρ Γ Υ Σ Ν Ψ Β

Η Ο Ζ Ρ Χ Φ Ι Τ Α Ρ Ν Ω Ψ Ψ Λ

Λ Χ Ζ Θ Μ Π Κ Ε Μ Ο Σ Μ Σ Ξ Η

Α Ο Π Η Ω Α Ξ Σ Κ Υ Η Ζ Υ Β Ψ

Π Ε Ν Ι Α Ι Α Σ Υ Ν Δ Ε Σ Η Ρ

Ε Ψ Β Π Η Μ Ω Η Κ Ξ Ο Ν Χ Γ Μ

Ω Ψ Υ Ζ Ψ Ξ Φ Υ Λ Υ Ο Β Ν Φ Τ

Μ Λ Η Υ Γ Ψ Υ Κ Ρ Α Χ Ω Ψ Μ Ρ

Η Π Χ Θ Ξ Δ Α Γ Κ Π Φ Χ Χ Λ Ι

ΛΙΣΤΑ ΛΕΞΕΩΝ

ΕΠΑΛΗΘΕΥΣΗ ΔΙΕΥΘΥΝΣΗ ΣΗΡΑΓΓΑ ΚΟΝΣΟΛΑ ΕΝΙΑΙΑΣΥΝΔΕΣΗ
ΠΑΡΑΓΟΝΤΕΣ ΠΥΛΗ ΧΟΡΗΓΗΣΗ

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. ΔΙΕΥΘΥΝΣΗ**
- **C. ΣΗΡΑΓΓΑ**
- **D. ΚΟΝΣΟΛΑ**
- **E. ΕΝΙΑΙΑΣΥΝΔΕΣΗ**
- **F. ΠΑΡΑΓΟΝΤΕΣ**
- **G. ΠΥΛΗ**
- **H. ΧΟΡΗΓΗΣΗ**

ΟΡΙΣΜΟΙ ΚΑΙ ΠΕΔΙΑ ΑΝΤΙΣΤΟΙΧΙΣΗΣ

_____ 1. Στατική διεύθυνση πύλης για λίστα επιτρεπόμενων.

_____ 2. Κόμβος δρομολόγησης στην είσοδο του δικτύου.

_____ 3. Παροχή αδειών πρόσβασης VPN στους υπαλλήλους.

_____ 4. Ασφάλεια σύνδεσης που απαιτεί επιπλέον διακριτικά.

_____ 5. Ασφαλής διαδρομή που συνδέει τα δίκτυα δύο τοποθεσιών της εταιρείας.

_____ 6. Συνεχής έλεγχος ταυτότητας χρήστη και συσκευής πριν δοθεί κάθε πρόσβαση.

_____ 7. Σύνδεση ταυτότητας με Okta και Entra ID.

_____ 8. Κεντρική πύλη για τους διαχειριστές IT.

Σημείο ελέγχου 7: Πρόκληση ανακατεμένων λέξεων

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

1. ΣΕΘΗΠΕΥΗΛΑ
2. ΣΡΑΓΓΑΗ
3. ΝΕΥΔΝΣΗΙΣΙΑ ΕΑ
4. ΗΛΠΥ
5. ΝΘΙΗΥΥΔΣΕ
6. ΛΝΟΚΣΑΟ
7. ΑΑΠΝΟΤΕΣΓΡ
8. ΗΟΓΗΧΣΗΡ

Δραστηριότητα μπόνους: Σκέψου γρήγορα

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

1	Εργαλεία που χρησιμοποιεί μια εταιρεία καθημερινά			
2	Πράγματα που ένα VPN μπορεί να κρύψει			
3	Ρόλοι σε ένα τμήμα πληροφορικής			
4	Λέξεις που περιγράφουν το Zero Trust			
5	Τρόποι να συνδέεσαι με ασφάλεια			
6	Λόγοι για να δώσεις VPN στους εργαζομένους			
7	Πράγματα που κάνεις μετά από μια παραβίαση ασφαλείας			
8	Λόγοι για να χρησιμοποιείς VPN όταν ταξιδεύεις			
9	Κανόνες για ασφαλή τηλεργασία			
10	Δεδομένα που πρέπει να προστατεύει μια εταιρεία			
11	Πράγματα που μπορούν να διαταράξουν μια βιντεοσύσκεψη			
12	Συσκευές που μπορούν να χρησιμοποιήσουν VPN			
13	Προγράμματα γραφείου που γνωρίζεις			
14	Μέρη από όπου εργάζονται οι εργαζόμενοι			
15	Συσκευές που μπορεί να έχει ένας εργαζόμενος			

Σημείο ελέγχου 8: Μελέτες περίπτωσης VPN και δικτύου

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

ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ 1: ΜΕΤΑΒΑΣΗ ΣΕ ZERO TRUST



Σενάριο: Μια επιχείρηση θέλει να ασφαλίσει τους τοπικούς διακομιστές της επαληθεύοντας συνεχώς τα πιστοποιητικά συμμόρφωσης των συσκευών, την κατάσταση του τείχους προστασίας και την τοποθεσία του χρήστη, αντί να εμπιστεύεται οποιονδήποτε βρίσκεται μέσα στο δίκτυο.

Ερώτηση συζήτησης: Ποιο πλαίσιο πρέπει να εφαρμόσει ο διευθυντής ασφάλειας πληροφορικής για να το πετύχει αυτό;

ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ 2: ΠΕΡΙΟΡΙΣΜΟΣ ΠΥΛΗΣ



Σενάριο: Μια εταιρεία φιλοξενεί ιδιωτικές χρηματοοικονομικές βάσεις δεδομένων στο cloud. Θέλει να μπλοκάρει κάθε δημόσια πρόσβαση στο internet στα πάνελ διαχείρισης, επιτρέποντας συνδέσεις μόνο από επαληθευμένα τερματικά της εταιρείας.

Ερώτηση συζήτησης: Ποια διαμόρφωση δικτύου πρέπει να ορίσει ο διαχειριστής βάσεων δεδομένων στο τείχος προστασίας του cloud;

Σημείο ελέγχου 9: Αποκρυπτογράφησε τον κώδικα

Ένας μηχανικός δικτύων ασφαλίζει τα κανάλια δρομολόγησης και τις σήραγγες πελατών. 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

7		12	7	4	5	13	9	10	7									
5	12	16	9	18	19	15	18	20	13	7		5	11	5	3	22	5	9
				10	1	8	5		18	20	18	10	5	20	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 τα VPN – βασικό επίπεδο (Μέρος Α)

Εξέτασε τις πιο συχνές ερωτήσεις και απαντήσεις για τα εικονικά ιδιωτικά δίκτυα (VPN) και τη σηραγγοποίηση.

Q1: Τι είναι ένα εταιρικό VPN (enterprise);

Μια ασφαλής σήραγγα δικτύου σχεδιασμένη για επιχειρήσεις, που επιτρέπει σε απομακρυσμένους εργαζομένους να έχουν πρόσβαση σε εταιρικά δίκτυα με κεντρική διαχείριση.

Q2: Σε τι διαφέρει το Zero Trust από τα παραδοσιακά VPN;

Τα παραδοσιακά VPN εμπιστεύονται όποιον βρίσκεται μέσα στη σήραγγα, ενώ το Zero Trust επαληθεύει συνεχώς κάθε συσκευή και σύνδεση χρήστη.

Q3: Τι είναι η Dedicated IP στα επιχειρηματικά VPN;

Μια στατική διεύθυνση IP που προορίζεται αποκλειστικά για την επιχείρησή σου, επιτρέποντάς σου να την εισαγάγεις σε λίστα επιτρεπόμενων για ασφαλή πρόσβαση σε βάσεις δεδομένων cloud.

Q4: Γιατί είναι σημαντικό το SSO για τα επιχειρηματικά VPN;

Το Single Sign-On επιτρέπει στους υπαλλήλους να χρησιμοποιούν τα εταιρικά διαπιστευτήριά τους (όπως Okta ή Microsoft Entra ID) για ασφαλή σύνδεση.

Q5: Τι είναι ένα VPN site-to-site;

Μια σήραγγα που συνδέει δύο φυσικά γραφεία (όπως ένα υποκατάστημα και τα κεντρικά) μέσω του δημόσιου διαδικτύου με χρήση IPsec.

Σημείο ελέγχου 10: Συχνές ερωτήσεις για τα VPN – βασικό επίπεδο (Μέρος Β)

Εξέτασε τις πιο συχνές ερωτήσεις και απαντήσεις για τα εικονικά ιδιωτικά δίκτυα (VPN) και τη σηραγγοποίηση.

Q6: Ποια είναι η λειτουργία μιας κονσόλας διαχείρισης;

Ένας πίνακας ελέγχου για διαχειριστές IT ώστε να προσθέτουν ή να αφαιρούν θέσεις υπαλλήλων, να εκχωρούν πύλες και να παρακολουθούν τις ενεργές συνδέσεις.

Q7: Πώς ασφαλίζει το MFA τα επιχειρηματικά VPN;

Απαιτώντας δευτερεύοντα κωδικό (όπως διακριτικό εφαρμογής πιστοποίησης ταυτότητας) για να αποτρέπεται η μη εξουσιοδοτημένη είσοδος από παραβιασμένους κωδικούς πρόσβασης.

Q8: Μπορώ να ελέγξω το ιστορικό συνδέσεων των εργαζομένων;

Ναι, τα εταιρικά VPN καταγράφουν χρονικές σημάνσεις σύνδεσης, διάρκεια και αντιστοιχισμένες IP για έλεγχο συμμόρφωσης.

Q9: Τι είναι το ZTNA;

Το Zero Trust Network Access, ένα μοντέλο ασφάλειας που παρέχει πρόσβαση μόνο σε συγκεκριμένες εφαρμογές και όχι σε ολόκληρο το δίκτυο.

Q10: Ποιος είναι ο ρόλος των κόμβων πύλης;

Λειτουργούν ως ασφαλή σημεία εισόδου για απομακρυσμένη κίνηση, δρομολογώντας τα δεδομένα απευθείας σε ιδιωτικούς εταιρικούς διακομιστές.

Σημείο ελέγχου 10: Συχνές ερωτήσεις για τα VPN – προχωρημένο επίπεδο (Μέρος C)

Εξερεύνησε προηγμένες τεχνικές πτυχές των πρωτοκόλλων τούνελ VPN, της ενσωμάτωσης προγραμμάτων πελάτη σε κινητά και της επιχειρησιακής ανάπτυξης.

Q1: Πώς προστατεύει το IPsec τις εταιρικές επικοινωνίες μεταξύ ιστότοπων;

Το IPsec κρυπτογραφεί την κίνηση στο επίπεδο δικτύου χρησιμοποιώντας το Encapsulating Security Payload (ESP) για να διασφαλίσει την εμπιστευτικότητα και την ακεραιότητα των δεδομένων.

Q2: Γιατί η παραδοσιακή ασφάλεια περιμέτρου αποτυγχάνει για εργαζομένους εξ αποστάσεως;

Επειδή οι εργαζόμενοι έχουν πρόσβαση στα δεδομένα από πολλαπλές τοποθεσίες και συσκευές, καθιστώντας παρωχημένη την περίμετρο ενός ενιαίου τείχους προστασίας δικτύου.

Q3: Πώς υλοποιούν οι διαχειριστές IT την αυτοματοποιημένη παροχή πρόσβασης;

Αντιστοιχίζοντας πρωτόκολλα SCIM μεταξύ παρόχων ταυτότητας (Okta) και της κονσόλας διαχείρισης VPN για τον συγχρονισμό των καταλόγων χρηστών.

Q4: Ποιο είναι το όφελος του split tunneling σε εταιρικά περιβάλλοντα;

Δρομολογεί την τοπική κίνηση SaaS (όπως το Microsoft 365) εκτός της σήραγγας VPN, διατηρώντας το εύρος ζώνης της εταιρικής πύλης για ιδιωτικές βάσεις δεδομένων.

Q5: Πώς επικυρώνουν οι έλεγχοι κατάστασης συσκευής (device posture checks) την ασφάλεια των τερματικών;

Ο πελάτης VPN σαρώνει τη συσκευή πριν από τη σύνδεση για να επαληθεύσει ότι το τείχος προστασίας είναι ενεργό, το antivirus εκτελείται και οι ενημερώσεις κώδικα του λειτουργικού συστήματος είναι τρέχουσες.

Σημείο ελέγχου 10: Συχνές ερωτήσεις για τα VPN – προχωρημένο επίπεδο (Μέρος D)

Εξερεύνησε προηγμένες τεχνικές πτυχές των πρωτοκόλλων τούνελ VPN, της ενσωμάτωσης προγραμμάτων πελάτη σε κινητά και της επιχειρησιακής ανάπτυξης.

Q6: Ποιος είναι ο ρόλος της διέλευσης NAT (NAT traversal) στις ρυθμίσεις επιχειρηματικών VPN;

Το NAT-T ενθυλακώνει πακέτα IPsec σε UDP ώστε να περνούν μέσα από οικιακούς δρομολογητές και τείχη προστασίας χωρίς πτώσεις σύνδεσης.

Q7: Πώς αποτρέπουν οι επιχειρήσεις την πνιγμονή του εύρους ζώνης της πύλης;

Αναπτύσσοντας πολλαπλούς περιφερειακούς κόμβους πύλης και κατανέμοντας την εισερχόμενη κίνηση των χρηστών μεταξύ τους με load balancers.

Q8: Γιατί προτιμώνται οι λίστες επιτρεπόμενων στατικών IP από τις δυναμικές;

Οι στατικές λίστες επιτρεπόμενων εμποδίζουν τις μη εξουσιοδοτημένες εξωτερικές IP να επιχειρούν χειραψίες σύνδεσης, μειώνοντας δραστικά την επιφάνεια επίθεσης.

Q9: Ποιος είναι ο ρόλος της ταυτοποίησης με πιστοποιητικά στα επιχειρηματικά VPN;

Επικυρώνει μοναδικά ψηφιακά πιστοποιητικά εγκατεστημένα σε συσκευές που διαχειρίζεται η εταιρεία, αποκλείοντας μη διαχειριζόμενους προσωπικούς υπολογιστές.

Q10: Πώς μειώνει το ZTNA τον κίνδυνο πλευρικής κίνησης;

Απομονώνοντας τις συνεδρίες των χρηστών σε συγκεκριμένους εξουσιοδοτημένους πόρους, εμποδίζοντας τους χάκερ να διασχίσουν το δίκτυο αν παραβιαστεί ένας κόμβος.

Μέρος 11: 10 πραγματικά στοιχεία και διαπιστώσεις για τα VPN

Εξέτασε πραγματικά στοιχεία για τις ταχύτητες κρυπτογράφησης VPN, τους ελέγχους πρωτοκόλλων, την κινητή συνδεσιμότητα και την απομακρυσμένη εργασία σε επιχειρήσεις.

1. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΑ VPN

Οι αρχιτεκτονικές Zero Trust επαληθεύουν συνεχώς την κατάσταση ασφάλειας κάθε συσκευής που επιχειρεί σύνδεση στο δίκτυο.

2. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΑ VPN

Οι πύλες αποκλειστικής IP επιτρέπουν στις επιχειρήσεις να θωρακίζουν βάσεις δεδομένων στο cloud με λευκή λίστα στατικών διευθύνσεων.

3. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΑ VPN

Το IPsec είναι το πρότυπο πρωτόκολλο του κλάδου για τη ρύθμιση ασφαλών σηράγγων δικτύου site-to-site μεταξύ γραφείων.

4. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΑ VPN

Οι κονσόλες διαχειριστή επιτρέπουν στα τμήματα IT να παρέχουν, να διαχειρίζονται και να ελέγχουν τις θέσεις πρόσβασης VPN των υπαλλήλων.

5. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΑ VPN

Το Single Sign-On ενσωματώνει την πρόσβαση VPN με εταιρικούς παρόχους ταυτότητας όπως το Okta και το Entra ID.

6. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΑ VPN

Ο έλεγχος ταυτότητας πολλαπλών παραγόντων αποκλείει μη εξουσιοδοτημένες απόπειρες σύνδεσης που προέρχονται από κλεμμένα κλειδιά κωδικών πρόσβασης.

7. ΕΙΔΗΣΗ ΓΙΑ ΤΑ VPN

Το split tunneling βελτιστοποιεί το εύρος ζώνης της εταιρείας αποκλείοντας τη δημόσια κίνηση SaaS από το κρυπτογραφημένο τούνελ.

8. ΕΙΔΗΣΗ ΓΙΑ ΤΑ VPN

Οι έλεγχοι στάσης συσκευής επαληθεύουν τις τοπικές ρυθμίσεις ασφάλειας πριν παραχωρηθεί πρόσβαση σε εταιρικούς διακομιστές.

9. ΕΙΔΗΣΗ ΓΙΑ ΤΑ VPN

Ο συγχρονισμός καταλόγου SCIM αυτοματοποιεί τους ελέγχους πρόσβασης κατά την ένταξη και την αποχώρηση των υπαλλήλων.

10. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΑ VPN

Το Zero Trust Network Access περιορίζει την πρόσβαση των χρηστών σε συγκεκριμένες εξουσιοδοτημένες εφαρμογές, αποτρέποντας την πλευρική κίνηση στο δίκτυο.

Τεχνικές αναφορές και πηγές

Ο οδηγός μελέτης και τα διαδραστικά παζλ έχουν συνταχθεί από παγκόσμια τεχνικά πρότυπα, προδιαγραφές και ρυθμιστικά πλαίσια.

ΑΚΑΔΗΜΑΪΚΕΣ ΚΑΙ ΒΙΟΜΗΧΑΝΙΚΕΣ ΑΝΑΦΟΡΕΣ

[1] VPN.com. (2026). Best VPN for Business: Tested & Ranked By Our Experts.

https://www.vpn.com/vpn/best-vpn-for-business/

[2] NIST. (2020). SP 800-207: Zero Trust Architecture.

https://csrc.nist.gov/pubs/sp/800/207/final

[3] NIST. (2016). SP 800-46 Rev. 2: Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security.

https://csrc.nist.gov/pubs/sp/800/46/r2/final

[4] NordLayer. (n.d.). Secure your network & stay compliant with one toggle-ready platform.

https://nordlayer.com/

Λύσεις: Σημείο ελέγχου 1 – Πολλαπλής επιλογής

1 **Zero Trust** ΜΟΝΤΕΛΟ ΖΤΝΑ **Σωστή απάντηση: A**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Τα μοντέλα Zero Trust επαληθεύουν συνεχώς τη συμμόρφωση της συσκευής πριν από την είσοδο στο δίκτυο. Παραπομπή: NIST Zero Trust.

2 **Αποκλειστική IP** ΣΤΑΤΙΚΗ IP **Σωστή απάντηση: A**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Οι αποκλειστικές διευθύνσεις IP επιτρέπουν τη δημιουργία λευκής λίστας σε πύλες ώστε να αποκλείεται η δημόσια κίνηση. Παραπομπή: Dedicated IP Guide.

3 **Πρότυπο IPsec** ΣΗΡΑΓΓΑ IPSEC **Σωστή απάντηση: A**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Το IPsec είναι το πρότυπο πρωτόκολλο που χρησιμοποιείται για σήραγγες site-to-site υποκαταστημάτων. Παραπομπή: IPsec Tunneling.

4 **Κατανομή IT** ΚΟΝΣΟΛΑ ΔΙΑΧΕΙΡΙΣΤΗ **Σωστή απάντηση: A**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Οι κεντρικοί πίνακες ελέγχου διαχειριστή επιτρέπουν στους διαχειριστές IT να κατανέμουν άδειες θέσεων. Παραπομπή: Οδηγίες CISA.

5 **Ερώτηση 5** **Σωστή απάντηση: A**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Ποιο πρότυπο ταυτοποίησης επιτρέπει τη σύνδεση μέσω Okta ή Microsoft Entra ID; → Single Sign-On

Λύσεις: Σημείο ελέγχου 2 – Σωστό ή Λάθος

6 **Zero Trust** ΕΛΕΓΧΟΙ ΖΤΝΑ **Σωστή απάντηση: Σωστό**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Τα μοντέλα Zero Trust επαληθεύουν συνεχώς τη συμμόρφωση της συσκευής πριν από την είσοδο στο δίκτυο. Παραπομπή: NIST Zero Trust.

7 **Ερώτηση 7** **Σωστή απάντηση: Λάθος**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Οι αποκλειστικές IP δεσμεύονται για μία επιχείρηση, οπότε η κίνησή της δεν αναμειγνύεται με άλλους χρήστες.

8 **Κατανομή IT** ΘΕΣΗ ΔΙΑΧΕΙΡΙΣΤΗ ΠΛΗΡΟΦΟΡΙΚΗΣ **Σωστή απάντηση: Σωστό**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Οι κεντρικοί πίνακες ελέγχου διαχειριστή επιτρέπουν στους διαχειριστές IT να κατανέμουν άδειες θέσεων. Παραπομπή: Οδηγίες CISA.

9 **Πρότυπο IPsec** ΑΠΟ ΤΟΠΟ ΣΕ ΤΟΠΟ **Σωστή απάντηση: Λάθος**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Το IPsec είναι το πρότυπο πρωτόκολλο που χρησιμοποιείται για σήραγγες site-to-site υποκαταστημάτων. Παραπομπή: IPsec Tunneling.

10 **Σύνδεσμος Okta SSO** ΣΥΝΔΕΣΗ SSO **Σωστή απάντηση: Σωστό**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Το Single Sign-On ενσωματώνει τις συνδέσεις VPN με εταιρικούς καταλόγους όπως το Okta. Παραπομπή: Okta SSO.

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

H 1. ΜΗΔΕΝΙΚΗ ΕΜΠΙΣΤΟΣΥΝΗ	D 2. ΕΞΑΤΟΜΙΚΕΥΜΕΝΗ IP	E 3. IPSEC	G 4. ΚΟΝΣΟΛΑ ΔΙΑΧΕΙΡΙΣΤΗ
B 5. ΕΝΙΑΙΑ ΣΥΝΔΕΣΗ	C 6. ΠΟΛΛΑΠΛΩΝ ΠΑΡΑΓΟΝΤΩΝ	F 7. ΠΥΛΗ	A 8. ΠΑΡΟΧΗ

ΣΗΜΕΙΟ ΕΛΕΓΧΟΥ 3: ΛΥΣΕΙΣ – ΒΑΣΙΚΟΙ ΟΡΟΙ

1 ZERO TRUST	2 ΣΤΑΘΕΡΗ ΔΙΕΥΘΥΝΣΗ IP	3 IPSEC	4 ΚΟΝΣΟΛΑ
5 ΕΝΙΑΙΑ ΣΥΝΔΕΣΗ	6 ΠΑΡΑΓΟΝΤΕΣ		

ΣΗΜΕΙΟ ΕΛΕΓΧΟΥ 6, ΕΝΑΛΛΑΚΤΙΚΑ: ΛΥΣΕΙΣ – ΑΝΤΙΣΤΟΙΧΙΣΗ ΛΕΞΕΩΝ

1 B – ΔΙΕΥΘΥΝΣΗ	2 G – ΠΥΛΗ	3 H – ΧΟΡΗΓΗΣΗ	4 F – ΠΑΡΑΓΟΝΤΕΣ
5 C – ΣΗΡΑΓΓΑ	6 A – ΕΠΑΛΗΘΕΥΣΗ	7 E – ΕΝΙΑΙΑΣΥΝΔΕΣΗ	8 D – ΚΟΝΣΟΛΑ

ΣΗΜΕΙΩΣΕΙΣ ΣΥΖΗΤΗΣΗΣ ΓΙΑ ΕΚΠΑΙΔΕΥΤΙΚΟΥΣ

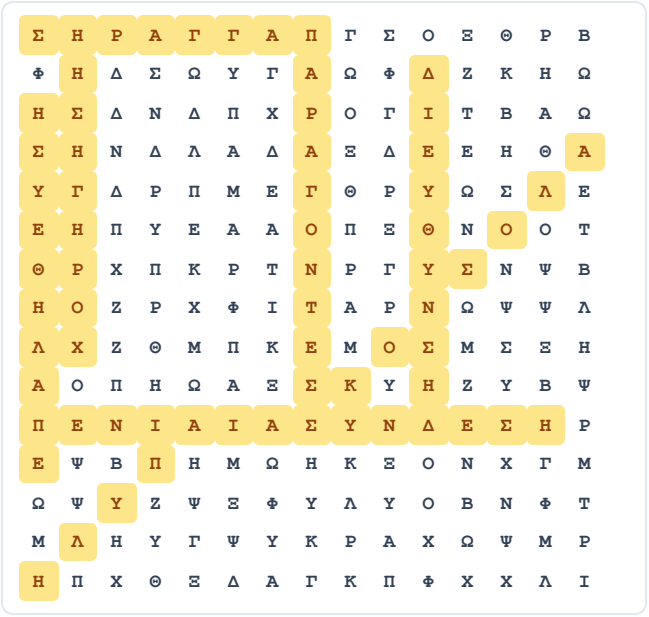
Βασικοί όροι:
Έλεγξε αν οι μαθητές μπορούν να εξηγήσουν με δικά τους λόγια τους όρους ΜΗΔΕΝΙΚΗ ΕΜΠΙΣΤΟΣΥΝΗ, ΕΞΑΤΟΜΙΚΕΥΜΕΝΗ IP και IPSEC και να δώσουν ένα παράδειγμα για τον καθένα.

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

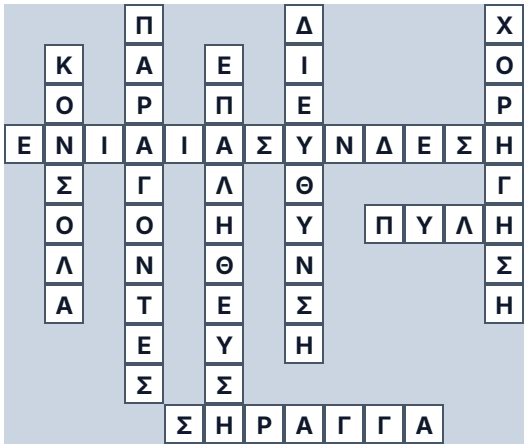
Αξιολόγηση πηγών:
Ζήτησε από τους μαθητές να επαληθεύσουν τουλάχιστον έναν ισχυρισμό στις πηγές του φύλλου και συζητήστε γιατί οι αριθμοί, οι τιμές και οι κανόνες μπορεί να αλλάζουν με τον χρόνο.

Λύσεις γρίφων και σημειώσεις για τον εκπαιδευτικό

ΛΥΣΗ ΓΡΙΦΟΥ ΛΕΞΕΩΝ



ΛΥΣΗ ΣΤΑΥΡΟΛΕΞΟΥ



ΟΔΗΓΟΣ ΕΚΠΑΙΔΕΥΤΙΚΟΥ ΓΙΑ ΤΙΣ ΛΥΣΕΙΣ ΤΟΥ ΣΤΑΥΡΟΛΕΞΟΥ

ΟΡΙΖΟΝΤΙΑ

6 οριζόντια: ΕΝΙΑΙΑΣΥΝΔΕΣΗ Σύνδεση ταυτότητας με Okta και Entra ID (13 γράμματα)

7 οριζόντια: ΠΥΛΗ Κόμβος δρομολόγησης στην είσοδο του δικτύου (4 γράμματα)

8 οριζόντια: ΣΗΡΑΓΓΑ Ασφαλής διαδρομή που συνδέει τα δίκτυα δύο τοποθεσιών της εταιρείας (7 γράμματα)

ΚΑΘΕΤΑ

1 κάθετα: ΠΑΡΑΓΟΝΤΕΣ Ασφάλεια σύνδεσης που απαιτεί επιπλέον διακριτικά (10 γράμματα)

2 κάθετα: ΔΙΕΥΘΥΝΣΗ Στατική διεύθυνση πύλης για λίστα επιτρεπόμενων (9 γράμματα)

3 κάθετα: ΧΟΡΗΓΗΣΗ Παροχή αδειών πρόσβασης VPN στους υπαλλήλους (8 γράμματα)

4 κάθετα: ΚΟΝΣΟΛΑ Κεντρική πύλη για τους διαχειριστές IT (7 γράμματα)

5 κάθετα: ΕΠΑΛΗΘΕΥΣΗ Συνεχής έλεγχος ταυτότητας χρήστη και συσκευής πριν δοθεί κάθε πρόσβαση (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. ΣΡΑΓΓΑΗ — **ΣΗΡΑΓΓΑ**
3. ΝΕΥΔΝΣΗΙΣΙΑΕΑ — **ΕΝΙΑΙΑΣΥΝΔΕΣΗ**
4. ΗΛΠΥ — **ΠΥΛΗ**
5. ΝΘΙΗΥΥΔΣΕ — **ΔΙΕΥΘΥΝΣΗ**
6. ΛΝΟΚΣΑΟ — **ΚΟΝΣΟΛΑ**
7. ΑΑΠΝΟΤΕΣΓΡ — **ΠΑΡΑΓΟΝΤΕΣ**
8. ΗΟΓΗΧΣΗΡ — **ΧΟΡΗΓΗΣΗ**

ΚΛΕΙΔΙ ΠΡΟΚΛΗΣΗΣ ΜΥΣΤΙΚΟΥ ΚΩΔΙΚΑ

"Η ΜΗΔΕΝΙΚΗ ΕΜΠΙΣΤΟΣΥΝΗ ΕΛΕΓΧΕΙ ΚΑΘΕ ΣΥΣΚΕΥΗ"

Λύσεις των μελετών περίπτωσης

A Μελέτη περίπτωσης 1: Μετάβαση σε Zero Trust

Λύση για τον εκπαιδευτικό

ΟΔΗΓΙΕΣ ΒΑΘΜΟΛΟΓΗΣΗΣ

Οι απαντήσεις των μαθητών πρέπει να καλύπτουν τα εξής σημεία:

- Ανάλυση σεναρίου: Μια επιχείρηση θέλει να θωρακίσει τους τοπικούς διακομιστές της επαληθεύοντας συνεχώς τα πιστοποιητικά συμμόρφωσης των συσκευών, την κατάσταση του τείχους προστασίας και την τοποθεσία του χρήστη, αντί να εμπιστεύεται οποιονδήποτε βρίσκεται μέσα στο δίκτυο.
- Προτεινόμενη στρατηγική και λύση: Ο διευθυντής πρέπει να μεταβεί σε μοντέλο Zero Trust Network Access (ZTNA), που επιβάλλει συνεχείς ελέγχους ασφαλείας βάσει περιβάλλοντος.

B Μελέτη περίπτωσης 2: Περιορισμός πύλης

Λύση για τον εκπαιδευτικό

ΟΔΗΓΙΕΣ ΒΑΘΜΟΛΟΓΗΣΗΣ

Οι απαντήσεις των μαθητών πρέπει να καλύπτουν τα εξής σημεία:

- Ανάλυση σεναρίου: Μια εταιρεία φιλοξενεί ιδιωτικές οικονομικές βάσεις δεδομένων στο cloud. Θέλει να αποκλείσει κάθε δημόσια πρόσβαση στο διαδίκτυο στους πίνακες διαχείρισης, επιτρέποντας συνδέσεις μόνο από επαληθευμένα εταιρικά τερματικά.
- Προτεινόμενη στρατηγική και λύση: Ο διαχειριστής πρέπει να ρυθμίσει μια πύλη Dedicated IP στο εταιρικό VPN και να εισαγάγει αυτή τη στατική διεύθυνση στη λίστα επιτρεπόμενων του τείχους προστασίας της βάσης δεδομένων στο cloud.