Όνομα: _____ Ημερομηνία: _____ Βαθμολογία: _____

Βασικά στοιχεία κυβερνοασφάλειας και online απειλές Πρόληψη

Απειλές κυβερνοασφάλειας, τείχη προστασίας δικτύου, πολυπαραγοντική ταυτοποίηση, πλαίσια ασφαλείας

ΕΠΙΣΚΟΠΗΣΗ ΜΑΘΗΣΗΣ ΓΙΑ ΤΑ ΒΑΣΙΚΑ ΣΤΟΙΧΕΙΑ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

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 στις βασικές αρχές της κυβερνοασφάλειας και της πρόληψης διαδικτυακών απειλών. Θα εξερευνήσεις απειλές κακόβουλου λογισμικού, ταυτοποίηση πολλαπλών παραγόντων, τείχη προστασίας δικτύου και πλαίσια αντιμετώπισης περιστατικών.

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/

Η πορεία μάθησής σου: βασικά της κυβερνοασφάλειας

- Αναγνώρισε τους συνήθεις φορείς κακόβουλου λογισμικού, ηλεκτρονικού ψαρέματος και εισβολής σε εταιρικά δίκτυα.
- Εφάρμοσε τυπικούς ελέγχους κυβερνοασφάλειας, συμπεριλαμβανομένων των MFA, των τειχών προστασίας και της άμυνας τελικών σημείων.
- Αξιολόγησε τις διαδικασίες αντιμετώπισης συμβάντων για τον μετριασμό των επιπτώσεων μιας παραβίασης δεδομένων.
- Ανάλυσε τους οργανωσιακούς παράγοντες κινδύνου και την ευθυγράμμιση ασφαλείας βάσει των κατευθυντήριων γραμμών του NIST.
- Ρύθμισε πρακτικές ασφαλούς υγιεινής για να περιορίσεις το αυτοματοποιημένο credential stuffing.

ΟΔΗΓΙΕΣ ΟΔΗΓΟΥ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ

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 πρόληψη απειλών. Ολοκλήρωσε με τη δραστηριότητα μπόνους Σκέψου γρήγορα.

ΒΑΣΙΚΑ ΣΤΟΙΧΕΙΑ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑΣ ΚΑΙ ΠΡΟΛΗΨΗ ΑΠΕΙΛΩΝ (ΕΙΣΑΓΩΓΗ)

Η κυβερνοασφάλεια προστατεύει δίκτυα, συστήματα και δεδομένα από μη εξουσιοδοτημένες ψηφιακές επιθέσεις. Η ανάπτυξη ισχυρών συνηθειών ασφαλείας, η ρύθμιση τειχών προστασίας, η απαίτηση πολυπαραγοντικής ταυτοποίησης και η εκπαίδευση του προσωπικού στην αναγνώριση απειλών είναι βασικά στοιχεία της άμυνας του εταιρικού δικτύου.

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

Σημείο ελέγχου 1: Πρόκληση πολλαπλής επιλογής

1. **Ποιος είναι ο κύριος στόχος μιας επίθεσης ηλεκτρονικού ψαρέματος;**
   - A. Κλοπή διαπιστευτηρίων και ευαίσθητων δεδομένων χρηστών
   - B. Βελτίωση της ορατότητας του ιστότοπου στις μηχανές αναζήτησης
   - C. Αύξηση της χωρητικότητας εύρους ζώνης του δικτύου
   - D. Διαχείριση αντιγραφής δεδομένων του εφεδρικού κέντρου δεδομένων

2. **Ποιος μηχανισμός παρέχει την ισχυρότερη προστασία λογαριασμού;**
   - A. Έλεγχος ταυτότητας πολλαπλών παραγόντων με κλειδιά υλικού
   - B. Σύνθετοι κωδικοί πρόσβασης που ενημερώνονται κάθε τριάντα ημέρες
   - C. Περιορισμός της σύνδεσης στον λογαριασμό στις ώρες εργασίας
   - D. Απόκρυψη του ονόματος χρήστη του λογαριασμού από δημόσιους καταλόγους

3. **Τι ορίζει το ωφέλιμο φορτίο μιας μόλυνσης από ransomware;**
   - A. Κρυπτογράφηση αρχείων συστήματος και απαίτηση πληρωμής
   - B. Αθόρυβη καταγραφή πληκτρολογήσεων σε απομακρυσμένους διακομιστές
   - C. Έγχυση μη εξουσιοδοτημένων διαφημίσεων στα προγράμματα περιήγησης
   - D. Χρήση των τοπικών πόρων CPU για εξόρυξη κρυπτονομισμάτων

4. **Πώς επηρεάζει μια ευπάθεια μηδενικής ημέρας (zero-day) τις αμυντικές δικλίδες ασφαλείας;**
   - A. Στοχεύει σε ανεπίδεκτες επιδιόρθωσης, άγνωστες ευπάθειες
   - B. Απενεργοποιεί αυτόματα το εταιρικό τείχος προστασίας
   - C. Αναγκάζει το σύστημα να κάνει πλήρη επανεκκίνηση
   - D. Δεν απαιτεί κανένα κονδύλι για την αποκατάσταση

5. **Ποιο πλαίσιο διέπει τους εταιρικούς ελέγχους ασφάλειας;**
   - A. Κατευθυντήριες γραμμές του πλαισίου κυβερνοασφάλειας NIST
   - B. Προδιαγραφές σχήματος εγγράφων W3C HTML5
   - C. Εγχειρίδια εγκατάστασης προγραμμάτων οδήγησης εκτυπωτή
   - D. Ορισμοί πρωτοκόλλων δρομολόγησης του IETF

Σημείο ελέγχου 2: Πρόκληση Σωστό ή Λάθος

6 Ερώτηση Σωστό/Λάθος 6

6. Οι επιθέσεις ηλεκτρονικού ψαρέματος στοχεύουν μόνο προσωπικούς λογαριασμούς email.

- ◯ Σωστό
- ◯ Λάθος

7 Ερώτηση Σωστό/Λάθος 7

7. Η ταυτοποίηση πολλαπλών παραγόντων βοηθά στον αποκλεισμό επιθέσεων credential stuffing.

- ◯ Σωστό
- ◯ Λάθος

8 Ερώτηση Σωστό/Λάθος 8

8. Τα τείχη προστασίας ελέγχουν την κίνηση του δικτύου για να αποκλείουν τη μη εξουσιοδοτημένη πρόσβαση σε θύρες.

- ◯ Σωστό
- ◯ Λάθος

9 Ερώτηση Σωστό/Λάθος 9

9. Η αντιμετώπιση των εκμεταλλεύσεων zero-day απαιτεί τυπικές ενημερώσεις ορισμών antivirus.

- ◯ Σωστό
- ◯ Λάθος

10 Ερώτηση Σωστό/Λάθος 10

10. Ένα honeypot είναι ένας διακομιστής-δόλωμα που χρησιμοποιείται για να παρασύρει κυβερνοεγκληματίες.

- ◯ 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 διαχειριστές δικτύου εγκαθιστούν ένα _____ για να φιλτράρουν την εισερχόμενη κίνηση.

2. Ένας επιτιθέμενος χρησιμοποιεί μια zero-day _____ για να παρακάμψει τις ενημερώσεις ασφαλείας του συστήματος.

3. Οι επιτιθέμενοι στέλνουν πλαστά email εναντίον υπαλλήλων· οι εκστρατείες αυτές ονομάζονται _____ .

4. Το λυτρολογισμικό είναι ένα καταστροφικό _____ που κλειδώνει τα δεδομένα των χρηστών.

5. Η ισχυρή _____ κωδικών πρόσβασης μειώνει τον κίνδυνο κλοπής διαπιστευτηρίων.

6. Για την προστασία ευαίσθητων επικοινωνιών, οι χρήστες εφαρμόζουν την _____ των δεδομένων.

ΤΡΑΠΕΖΑ ΛΕΞΕΩΝ

ΕΚΜΕΤΑΛΛΕΥΣΗ ΗΛΕΚΤΡΟΝΙΚΟ ΨΑΡΕΜΑ ΚΑΚΟΒΟΥΛΟ ΛΟΓΙΣΜΙΚΟ ΚΡΥΠΤΟΓΡΑΦΗΣΗ
ΠΑΡΑΓΟΝΤΕΣ ΠΛΑΙΣΙΟ ΤΕΙΧΟΣ ΠΡΟΣΤΑΣΙΑΣ ΥΓΙΕΙΝΗ

Γράψε τις απαντήσεις σου εδώ:

1. **2.**

3. **4.**

5. **6.**

Σημείο ελέγχου 4: Αντιστοίχιση εννοιών ασφάλειας

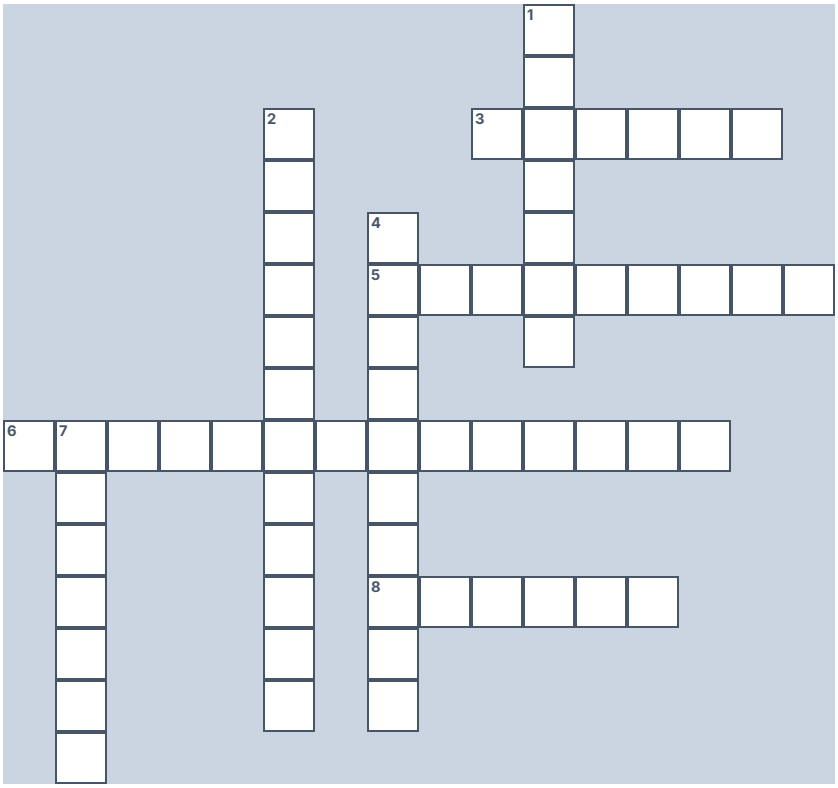
ΑΝΤΙΣΤΟΙΧΙΣΗ ΟΡΙΣΜΩΝ

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

☐	**1. Απειλή ransomware**	**A**	Δομημένες κατευθυντήριες γραμμές, όπως του NIST, που χρησιμοποιούνται για τη διαχείριση των κινδύνων στον κυβερνοχώρο.
☐	**2. Πολυπαραγοντική ταυτοποίηση**	**B**	Δομημένο σχέδιο για τον χειρισμό και τον μετριασμό παραβιάσεων ασφαλείας.
☐	**3. Εκμετάλλευση zero-day**	**C**	Φραγμός δικτύου που φιλτράρει την κίνηση βάσει κανόνων ασφαλείας.
☐	**4. Παγίδα-δόλωμα (honeypot)**	**D**	Κακόβουλο λογισμικό που κρυπτογραφεί δεδομένα και απαιτεί χρηματική πληρωμή για την αποκρυπτογράφηση.
☐	**5. Τείχος προστασίας ανίχνευσης εισβολών**	**E**	Εκμετάλλευση ευπάθειας που στοχεύεται πριν κυκλοφορήσει η διόρθωση του κατασκευαστή.
☐	**6. Αντιμετώπιση περιστατικών**	**F**	Βέλτιστες πρακτικές για τη διαχείριση διαπιστευτηρίων και κλειδιών πιστοποίησης ταυτότητας.
☐	**7. Υγιεινή κωδικών πρόσβασης**	**G**	Επαλήθευση ασφαλείας που απαιτεί δύο ή περισσότερους παράγοντες ταυτοποίησης.
☐	**8. Πλαίσιο ασφάλειας**	**H**	Σύστημα-δόλωμα που στήνεται για να προσελκύει και να αναλύει κακόβουλους παράγοντες.

Σημείο ελέγχου 5: Σταυρόλεξο

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



ΟΡΙΖΟΝΤΙΑ

3. Σύστημα-δόλωμα που στήνεται για να προσελκύσει και να αναλύσει κακόβουλους παράγοντες (6)

5. Δομημένο σχέδιο για τον χειρισμό και τον περιορισμό των παραβιάσεων ασφαλείας (9)

6. Κακόβουλο λογισμικό που κρυπτογραφεί δεδομένα και απαιτεί οικονομική πληρωμή για την αποκρυπτογράφησή τους (14)

8. Φραγμός δικτύου που φιλτράρει την κίνηση βάσει κανόνων ασφαλείας (6)

ΚΑΘΕΤΑ

1. Δομημένες κατευθυντήριες γραμμές, όπως το NIST, για τη διαχείριση των κινδύνων στον κυβερνοχώρο (7)

2. Εκμετάλλευση ευπάθειας που στοχεύεται πριν κυκλοφορήσει διόρθωση από τον κατασκευαστή (12)

4. Επαλήθευση ασφαλείας που απαιτεί δύο ή περισσότερους παράγοντες ταυτοποίησης (10)

7. Βέλτιστες πρακτικές για τη διαχείριση διαπιστευτηρίων και κλειδιών ταυτοποίησης (7)

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

3 οριζόντια: Σύστημα-δόλωμα που στήνεται για να προσελκύσει και να αναλύσει κακόβουλους παράγοντες (6 γράμματα):

5 οριζόντια: Δομημένο σχέδιο για τον χειρισμό και τον περιορισμό των παραβιάσεων ασφαλείας (9 γράμματα):

6 οριζόντια: Κακόβουλο λογισμικό που κρυπτογραφεί δεδομένα και απαιτεί οικονομική πληρωμή για την αποκρυπτογράφησή τους (14 γράμματα):

8 οριζόντια: Φραγμός δικτύου που φιλτράρει την κίνηση βάσει κανόνων ασφαλείας (6 γράμματα):

ΚΑΘΕΤΑ

1 κάθετα: Δομημένες κατευθυντήριες γραμμές, όπως το NIST, για τη διαχείριση των κινδύνων στον κυβερνοχώρο (7 γράμματα):

2 κάθετα: Εκμετάλλευση ευπάθειας που στοχεύεται πριν κυκλοφορήσει διόρθωση από τον κατασκευαστή (12 γράμματα):

4 κάθετα: Επαλήθευση ασφαλείας που απαιτεί δύο ή περισσότερους παράγοντες ταυτοποίησης (10 γράμματα):

7 κάθετα: Βέλτιστες πρακτικές για τη διαχείριση διαπιστευτηρίων και κλειδιών ταυτοποίησης (7 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 Θ Δ Ρ Π Μ Ε Π Θ Ρ Ω Σ Ε Π Υ

Σ Ε Α Α Π Ξ Ν Α Ο Τ Α Χ Π Κ Ρ

Υ Η Τ Ρ Γ Ν Ψ Ρ Β Ζ Ν Ρ Χ Φ Ι

Ε Ν Α Ρ Τ Ω Ψ Α Ψ Λ Τ Ζ Θ Μ Ο

Λ Ι Π Κ Ε Μ Μ Γ Σ Ξ Ι Η Ο Ι Π

Λ Ε Η Ω Ι Α Ξ Ο Υ Ζ Δ Υ Σ Β Ψ

Α Ι Ρ Ψ Χ Β Η Ν Μ Ω Ρ Ι Η Κ Ξ

Τ Γ Ο Ν Ο Χ Γ Τ Μ Ω Α Ψ Ζ Ψ Ξ

Ε Υ Φ Υ Σ Λ Υ Ε Ο Λ Σ Β Ν Φ Τ

Μ Μ Η Υ Γ Ψ Υ Σ Π Κ Η Ρ Α Χ Ω

Κ Λ Υ Τ Ρ Ο Λ Ο Γ Ι Σ Μ Ι Κ Ο

Ε Ψ Μ Ρ Π Χ Θ Ξ Δ Α Γ Κ Π Φ Χ

Χ Λ Π Α Γ Ι Δ Α Ι Θ Τ Θ Ζ Β Ε

Θ Κ Σ Ρ Φ Π Ω Ε Θ Ε Ρ Γ Α Λ Ο

Γ Ω Μ Κ Φ Ρ Υ Α Ρ Χ Κ Μ Μ Η Θ

ΛΙΣΤΑ ΛΕΞΕΩΝ

ΑΝΤΙΔΡΑΣΗ · ΛΥΤΡΟΛΟΓΙΣΜΙΚΟ · ΠΑΡΑΓΟΝΤΕΣ · ΕΚΜΕΤΑΛΛΕΥΣΗ · ΠΑΓΙΔΑ · ΤΕΙΧΟΣ · ΥΓΙΕΙΝΗ · ΠΛΑΙΣΙΟ

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. ΛΥΤΡΟΛΟΓΙΣΜΙΚΟ**
- **B. ΠΑΡΑΓΟΝΤΕΣ**
- **C. ΕΚΜΕΤΑΛΛΕΥΣΗ**
- **D. ΠΑΓΙΔΑ**
- **E. ΤΕΙΧΟΣ**
- **F. ΑΝΤΙΔΡΑΣΗ**
- **G. ΥΓΙΕΙΝΗ**
- **H. ΠΛΑΙΣΙΟ**

ΟΡΙΣΜΟΙ ΚΑΙ ΠΕΔΙΑ ΑΝΤΙΣΤΟΙΧΙΣΗΣ

1. Φραγμός δικτύου που φιλτράρει την κίνηση βάσει κανόνων ασφαλείας.
2. Δομημένο σχέδιο για τον χειρισμό και τον περιορισμό των παραβιάσεων ασφαλείας.
3. Κακόβουλο λογισμικό που κρυπτογραφεί δεδομένα και απαιτεί οικονομική πληρωμή για την αποκρυπτογράφησή τους.
4. Επαλήθευση ασφαλείας που απαιτεί δύο ή περισσότερους παράγοντες ταυτοποίησης.
5. Βέλτιστες πρακτικές για τη διαχείριση διαπιστευτηρίων και κλειδιών ταυτοποίησης.
6. Δομημένες κατευθυντήριες γραμμές, όπως το NIST, για τη διαχείριση των κινδύνων στον κυβερνοχώρο.
7. Εκμετάλλευση ευπάθειας που στοχεύεται πριν κυκλοφορήσει διόρθωση από τον κατασκευαστή.
8. Σύστημα-δόλωμα που στήνεται για να προσελκύσει και να αναλύσει κακόβουλους παράγοντες.

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. **ΜΛΓΣΟΤΥΙΙΛΚΟΟΡ**
2. **ΗΚΤΑΕΥΣΜΛΕΛΕ**
3. **ΤΙΧΣΟΕ**
4. **ΗΓΙΕΝΥΙ**
5. **ΤΟΣΑΑΝΓΠΕΡ**
6. **ΔΙΠΓΑΑ**
7. **ΡΑΣΗΑΙΝΔΤ**
8. **ΛΙΟΠΙΣΑ**

Δραστηριότητα μπόνους: Σκέψου γρήγορα

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

1	**Επαγγέλματα στην κυβερνοασφάλεια**			
2	**Λόγοι για να ενημερώνεις το λογισμικό**			
3	**Πράγματα που μπορεί να μπλοκάρει ένα τείχος προστασίας**			
4	**Προειδοποιητικά σημάδια σε ένα email**			
5	**Πράγματα που παίρνεις αντίγραφο ασφαλείας**			
6	**Γνωστοί τύποι κυβερνοεπιθέσεων**			
7	**Πράγματα που μπορεί να παρασύρει ένα honeypot**			
8	**Πληροφορίες που δεν πρέπει ποτέ να μοιράζεσαι**			
9	**Ενδείξεις ότι ένας υπολογιστής έχει μολυνθεί**			
10	**Ταινίες ή σειρές για χάκερ**			
11	**Επίπεδα ασφάλειας που μπορείς να χτίσεις**			
12	**Πράγματα που εξασκείς σε μια άσκηση ασφαλείας**			
13	**Εργαλεία ασφαλείας που γνωρίζεις**			
14	**Άνθρωποι που μπορείς να ρωτήσεις για βοήθεια στην πληροφορική**			
15	**Λέξεις που ξεκινούν με «cyber»**			

Σημείο ελέγχου 8: Μελέτες περίπτωσης κυβερνοασφάλειας

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

ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ 1: ΣΤΡΑΤΗΓΙΚΗ ΑΝΑΚΑΜΨΗΣ ΑΠΟ RANSOMWARE



Σενάριο: Ένα εταιρικό δίκτυο έχει μολυνθεί με ransomware, που κλειδώνει κρίσιμες βάσεις δεδομένων. Οι επιτιθέμενοι απαιτούν λύτρα 100.000 $ σε κρυπτονόμισμα. Η εταιρεία διαθέτει αντίγραφα ασφαλείας εκτός δικτύου από πριν 24 ώρες.

Ερώτηση συζήτησης: Ανάλυσε τους κινδύνους της πληρωμής και αξιολόγησε τη στρατηγική αποκατάστασης.

ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ 2: ΑΜΥΝΑ ΑΠΕΝΑΝΤΙ ΣΕ CREDENTIAL STUFFING



Σενάριο: Μια διαδικτυακή υπηρεσία υφίσταται επίθεση credential stuffing, με χάκερ να δοκιμάζουν εκατομμύρια ζεύγη ονόματος χρήστη/κωδικού πρόσβασης που κλάπηκαν από άλλους ιστότοπους.

Ερώτηση συζήτησης: Περίγραψε αναλυτικά τον μηχανισμό αυτής της επίθεσης και περίγραψε συνοπτικά δύο συστήματα άμυνας.

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

1	18	21	1	11	9	18	5		19	15		18	20	18	19	7	12	1

12	5		16	15	11	11	1	16	11	15	20	18		

5	11	5	3	22	15	20	18

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: Ποιος είναι ο κύριος στόχος της κυβερνοασφάλειας;

Ο βασικός στόχος είναι η προστασία δικτύων, συσκευών και δεδομένων από μη εξουσιοδοτημένη πρόσβαση, επιθέσεις και τυχαία ζημιά.

Q2: Σε τι διαφέρει το ηλεκτρονικό ψάρεμα από το spear phishing;

Το ηλεκτρονικό ψάρεμα είναι μια ευρεία εκστρατεία email που στοχεύει τυχαίους χρήστες, ενώ το spear phishing στοχεύει συγκεκριμένα άτομα με εξατομικευμένα δεδομένα.

Q3: Τι είναι ένα τείχος προστασίας δικτύου;

Ένα τείχος προστασίας είναι ένα σύστημα ασφάλειας δικτύου που παρακολουθεί και φιλτράρει την εισερχόμενη και εξερχόμενη κίνηση βάσει προκαθορισμένων κανόνων ασφαλείας.

Q4: Γιατί είναι απαραίτητος ο έλεγχος ταυτότητας πολλαπλών παραγόντων (MFA);

Το MFA προσθέτει ένα κρίσιμο επίπεδο άμυνας, εμποδίζοντας την πρόσβαση ακόμη κι αν οι επιτιθέμενοι κλέψουν ή σπάσουν τα βασικά διαπιστευτήρια κωδικού πρόσβασης.

Q5: Τι ορίζει έναν ιό υπολογιστή;

Ο ιός είναι κακόβουλο λογισμικό που αναπαράγεται μόνο του, προσκολλάται σε ακίνδυνα αρχεία και εξαπλώνεται στα συστήματα μόλις εκτελεστεί.

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 κλειδώνει το ransomware τα τοπικά δεδομένα;

Το ransomware χρησιμοποιεί κρυπτογραφικούς αλγορίθμους για να κρυπτογραφήσει τα αρχεία των χρηστών, καθιστώντας τα δυσανάγνωστα μέχρι να εφαρμοστεί ένα κλειδί αποκρυπτογράφησης.

Q7: Τι είναι μια ευπάθεια μηδενικής ημέρας (zero-day);

Ένα zero-day είναι ένα κενό ασφαλείας στο λογισμικό που είναι άγνωστο στον προμηθευτή, χωρίς να μένει χρόνος για ανάπτυξη κώδικα επιδιόρθωσης πριν από την εκμετάλλευση.

Q8: Ποιος είναι ο ρόλος του πλαισίου NIST;

Το πλαίσιο NIST παρέχει εθελοντικές κατευθυντήριες γραμμές και πρότυπα που βοηθούν τους οργανισμούς να διαχειρίζονται και να μειώνουν τους κινδύνους κυβερνοασφάλειας.

Q9: Τι είναι ένα σχέδιο αντιμετώπισης περιστατικών ασφαλείας;

Είναι ένα τεκμηριωμένο σύνολο διαδικασιών για τον εντοπισμό, τον περιορισμό και την ανάκαμψη από παραβιάσεις ασφαλείας και συμβιβασμό του δικτύου.

Q10: Πώς εκμεταλλεύεται η κοινωνική μηχανική τους χρήστες;

Η κοινωνική μηχανική χρησιμοποιεί ψυχολογική χειραγώγηση για να εξαπατήσει τους υπαλλήλους ώστε να αποκαλύψουν κωδικούς πρόσβασης ή να κατεβάσουν κακόβουλα αρχεία.

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 κατακλύζει μια επίθεση DDoS τους διακομιστές ιστού;

Μια επίθεση DDoS συντονίζει εκατομμύρια παραβιασμένες συσκευές botnet για να κατακλύσει έναν διακομιστή με κίνηση, εξαντλώντας τα όρια εύρους ζώνης και επεξεργαστή.

Q2: Ποια είναι η διαφορά μεταξύ συμμετρικής και ασύμμετρης κρυπτογράφησης;

Η συμμετρική κρυπτογράφηση χρησιμοποιεί ένα μόνο κλειδί για κρυπτογράφηση και αποκρυπτογράφηση, ενώ η ασύμμετρη κρυπτογράφηση χρησιμοποιεί ένα ζεύγος δημόσιου και ιδιωτικού κλειδιού.

Q3: Πώς εκτελούν οι χάκερ επιθέσεις SQL injection;

Οι επιτιθέμενοι εισάγουν κακόβουλες εντολές SQL σε πεδία φορμών, εξαπατώντας τη βάση δεδομένων του διακομιστή ώστε να αποκαλύψει μη εξουσιοδοτημένες εγγραφές χρηστών.

Q4: Τι είναι η πλευρική κίνηση (lateral movement) σε εισβολές δικτύου;

Είναι η τεχνική όπου οι επιτιθέμενοι εκμεταλλεύονται την αρχική πρόσβαση σε διακομιστή για να παραβιάσουν άλλα διασυνδεδεμένα συστήματα στο εσωτερικό δίκτυο.

Q5: Πώς ανακατευθύνει την κίνηση ιστού η πλαστογράφηση DNS (DNS spoofing);

Η πλαστογράφηση DNS αλλοιώνει τις εγγραφές της κρυφής μνήμης των διακομιστών ονομάτων, οδηγώντας τους νόμιμους χρήστες σε κακόβουλους ιστοτόπους-μιμητές αντί για τους προορισμούς τους.

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: Τι είναι ένα φυσικό κλειδί ασφαλείας (hardware security token);

Είναι μια φυσική συσκευή (όπως το YubiKey) που δημιουργεί κρυπτογραφικές αποδείξεις ταυτότητας, προσφέροντας μέγιστη άμυνα απέναντι σε απομακρυσμένο ηλεκτρονικό ψάρεμα.

Q7: Πώς χρησιμοποιούν οι ομάδες ασφαλείας τα παραπλανητικά honeypots;

Οι ομάδες εγκαθιστούν διακομιστές-δολώματα εκτός παραγωγής για να εντοπίζουν νωρίς εισβολές και να αναλύουν τα μοτίβα επίθεσης μη εξουσιοδοτημένων παραγόντων.

Q8: Ποια είναι η αρχή των ελάχιστων δικαιωμάτων;

Είναι το πρότυπο ασφαλείας του περιορισμού των δικαιωμάτων πρόσβασης των χρηστών στο απολύτως ελάχιστο που απαιτείται για την εκτέλεση των ρόλων εργασίας τους.

Q9: Πώς εκμεταλλεύεται μια επίθεση Man-in-the-Middle τις συνδέσεις;

Ένας επιτιθέμενος υποκλέπτει και αλλοιώνει τις επικοινωνίες μεταξύ δύο συσκευών σε μη κρυπτογραφημένα δίκτυα, κλέβοντας διακριτικά συνεδρίας και διαπιστευτήρια.

Q10: Τι είναι οι δείκτες παραβίασης (IOC);

Τα IOC είναι εγκληματολογικές ενδείξεις δεδομένων, όπως ασυνήθιστες τροποποιήσεις μητρώου ή παράνομη κίνηση IP, που δείχνουν ότι ένα σύστημα παραβιάστηκε.

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 επιτιθέμενοι σαρώνουν συνεχώς το διαδίκτυο για ευάλωτους διακομιστές και στέλνουν email ηλεκτρονικού ψαρέματος (phishing) στα εισερχόμενα των εργαζομένων.

2. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Το ανθρώπινο λάθος, όπως το κλικ σε συνδέσμους ηλεκτρονικού ψαρέματος (phishing), είναι συχνός παράγοντας στις παραβιάσεις δεδομένων, γι' αυτό η εκπαίδευση έχει σημασία.

3. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Το κόστος μιας παραβίασης δεδομένων περιλαμβάνει νομικά πρόστιμα, απώλεια πελατών, έρευνα και αποκατάσταση, και μπορεί να φτάσει σε εκατομμύρια δολάρια.

4. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Το MFA ανθεκτικό στο ηλεκτρονικό ψάρεμα, όπως τα φυσικά κλειδιά ασφαλείας, είναι ο ισχυρότερος τύπος MFA και το πρότυπο που προτρέπει να υιοθετηθεί η CISA. [2]

5. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Το ransomware παραμένει σημαντική απειλή για τα επιχειρησιακά δίκτυα και η CISA προτρέπει σε κρυπτογραφημένα αντίγραφα ασφαλείας εκτός σύνδεσης ως βασική άμυνα. [4]

6. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Το Πλαίσιο Κυβερνοασφάλειας NIST 2.0 (2024) έχει έξι βασικές λειτουργίες: Διακυβέρνηση, Αναγνώριση, Προστασία, Ανίχνευση, Ανταπόκριση, Ανάκτηση. [1]

7. ΕΙΔΗΣΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Τα ρομπότ credential stuffing δοκιμάζουν σε μεγάλη κλίμακα διαρρεύσαντα ζεύγη ονόματος χρήστη και κωδικού πρόσβασης σε πύλες σύνδεσης τραπεζών και ηλεκτρονικού εμπορίου.

8. ΕΙΔΗΣΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Παγκοσμίως υπάρχουν αγορές εκμεταλλεύσεων zero-day, όπου ευπάθειες υψηλής σοβαρότητας μπορούν να πωληθούν για μεγάλα ποσά πριν διορθωθούν.

9. ΕΙΔΗΣΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Ένα σύστημα δολώματος honeypot αναφέρει αμέσως ειδοποιήσεις εισβολής, αφού οι νόμιμοι χρήστες δεν έχουν λόγο να έχουν πρόσβαση σε αυτό.

10. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Το Transport Layer Security (TLS) κρυπτογραφεί τις συνεδρίες του προγράμματος περιήγησης, αποτρέποντας το packet sniffing σε δημόσια δίκτυα Wi-Fi.

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. (2024). The NIST Cybersecurity Framework (CSF) 2.0.
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

[2] CISA. (n.d.). More than a Password.
https://www.cisa.gov/MFA

[3] CISA. (2023). Phishing Guidance: Stopping the Attack Cycle at Phase One.
https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one

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

[5] CISA. (n.d.). Malware, Phishing, and Ransomware.
https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

[6] NIST. (2025). SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile.
https://csrc.nist.gov/pubs/sp/800/61/r3/final

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

[8] OWASP. (n.d.). SQL Injection.
https://owasp.org/www-community/attacks/SQL_Injection

Λύσεις: Σημείο ελέγχου 1 – Πολλαπλής επιλογής

1 **Επιθέσεις ηλεκτρονικού ψαρέματος** ΗΛΕΚΤΡΟΝΙΚΟ ΨΑΡΕΜΑ — **Σωστή απάντηση: A**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Οι εκστρατείες ηλεκτρονικού ψαρέματος επιχειρούν να κλέψουν διαπιστευτήρια και ευαίσθητα δεδομένα χρηστών μέσω πλαστών email. Παραπομπή: OWASP Secure Configuration.

2 **Προστασία λογαριασμού** ΚΛΕΙΔΙ MFA — **Σωστή απάντηση: A**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Ο έλεγχος ταυτότητας πολλαπλών παραγόντων (MFA) με φυσικά διακριτικά παρέχει την ισχυρότερη άμυνα στην πρόσβαση λογαριασμού. Παραπομπή: NIST Digital Identity.

3 **Απειλή Ransomware** RANSOMWARE — **Σωστή απάντηση: A**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Το ransomware κρυπτογραφεί κρίσιμα συστήματα και δεδομένα, απαιτώντας πληρωμή σε κρυπτονομίσματα για τα κλειδιά αποκρυπτογράφησης. Πηγή: Center for Internet Security (CIS).

4 **Ευπάθεια zero-day** ZERO-DAY — **Σωστή απάντηση: A**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Οι απειλές zero-day εκμεταλλεύονται άγνωστα κενά ασφαλείας χωρίς διόρθωση πριν διατεθεί ενημέρωση από τον κατασκευαστή. Παραπομπή: OWASP Secure Configuration.

5 **Πλαίσια ασφαλείας** ΠΛΑΙΣΙΑ — **Σωστή απάντηση: A**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Πλαίσια όπως το NIST παρέχουν δομημένες κατευθυντήριες γραμμές που βοηθούν τους οργανισμούς να διαχειρίζονται και να μειώνουν τους κινδύνους στον κυβερνοχώρο. Παραπομπή: NIST Digital Identity.

Λύσεις: Σημείο ελέγχου 2 – Σωστό ή Λάθος

6 **Στοχευμένο ηλεκτρονικό ψάρεμα** ΗΛΕΚΤΡΟΝΙΚΟ ΨΑΡΕΜΑ — **Σωστή απάντηση: Λάθος**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Οι επιθέσεις ηλεκτρονικού ψαρέματος στοχεύουν τόσο εταιρικά δίκτυα όσο και προσωπικούς λογαριασμούς για να διευρύνουν τους φορείς εκμετάλλευσης. Παραπομπή: OWASP Secure Configuration.

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

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Το MFA απαιτεί δεύτερο παράγοντα, οπότε ένας κλεμμένος κωδικός πρόσβασης από μόνος του συνήθως δεν αρκεί για τη σύνδεση.

8 **Τείχος προστασίας κίνησης** ΤΕΙΧΟΣ ΠΡΟΣΤΑΣΙΑΣ — **Σωστή απάντηση: Σωστό**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Τα τείχη προστασίας ελέγχουν και αποκλείουν την κίνηση σε συγκεκριμένες θύρες δικτύου, ώστε να φιλτράρουν τις μη εξουσιοδοτημένες συνδέσεις. Παραπομπή: Center for Internet Security (CIS).

9 **Αντιμετώπιση zero-day** ZERO-DAY — **Σωστή απάντηση: Λάθος**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Η αντιμετώπιση των ευπαθειών zero-day απαιτεί επιδιορθώσεις κώδικα και φιλτράρισμα WAF, αφού δεν υπάρχουν ακόμη υπογραφές. Παραπομπή: OWASP Secure Configuration.

10 **Δολώματα honeypot** ΠΑΓΙΔΑ ΗΟΝΕΥΡΟΤ — **Σωστή απάντηση: Σωστό**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Τα honeypot είναι παραπλανητικοί διακομιστές που χρησιμοποιούν οι ομάδες ασφαλείας για να προσελκύουν, να ειδοποιούνται και να μελετούν κακόβουλους παράγοντες. Παραπομπή: Center for Internet Security (CIS).

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

D 1. Απειλή ransomware	G 2. Πολυπαραγοντική ταυτοποίηση	E 3. Εκμετάλλευση zero-day	H 4. Παγίδα-δόλωμα (honeypot)
C 5. Τείχος προστασίας ανίχνευσης εισβολών	B 6. Αντιμετώπιση περιστατικών	F 7. Υγιεινή κωδικών πρόσβασης	A 8. Πλαίσιο ασφάλειας

ΣΗΜΕΙΟ ΕΛΕΓΧΟΥ 3: ΛΥΣΕΙΣ – ΒΑΣΙΚΟΙ ΟΡΟΙ

1 ΤΕΙΧΟΣ ΠΡΟΣΤΑΣΙΑΣ	2 ΕΚΜΕΤΑΛΛΕΥΣΗ	3 ΗΛΕΚΤΡΟΝΙΚΟ ΨΑΡΕΜΑ	4 ΚΑΚΟΒΟΥΛΟ ΛΟΓΙΣΜΙΚΟ
5 ΥΓΙΕΙΝΗ	6 ΚΡΥΠΤΟΓΡΑΦΗΣΗ		

ΣΗΜΕΙΟ ΕΛΕΓΧΟΥ 6, ΕΝΑΛΛΑΚΤΙΚΑ: ΛΥΣΕΙΣ – ΑΝΤΙΣΤΟΙΧΙΣΗ ΛΕΞΕΩΝ

1 Ε – ΤΕΙΧΟΣ	2 F – ΑΝΤΙΔΡΑΣΗ	3 A – ΛΥΤΡΟΛΟΓΙΣΜΙΚΟ	4 B – ΠΑΡΑΓΟΝΤΕΣ
5 G – ΥΓΙΕΙΝΗ	6 H – ΠΛΑΙΣΙΟ	7 C – ΕΚΜΕΤΑΛΛΕΥΣΗ	8 D – ΠΑΓΙΔΑ

ΣΗΜΕΙΩΣΕΙΣ ΣΥΖΗΤΗΣΗΣ ΓΙΑ ΕΚΠΑΙΔΕΥΤΙΚΟΥΣ

Βασικοί όροι:
Έλεγξε αν οι μαθητές μπορούν να εξηγήσουν με δικά τους λόγια τους όρους Απειλή ransomware, Πολυπαραγοντική ταυτοποίηση και Εκμετάλλευση zero-day 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	Θ	Δ	Ρ	Π	Μ	Ε	Π	Θ	Ρ	Ω	Σ	Ε	Π	Υ
Σ	Ε	Α	Α	Π	Ξ	Ν	Α	Ο	Τ	Α	Χ	Π	Κ	Ρ
Υ	Η	Τ	Ρ	Γ	Ν	Ψ	Ρ	Β	Ζ	Ν	Ρ	Χ	Φ	Ι
Ε	Ν	Α	Ρ	Τ	Ω	Ψ	Α	Ψ	Λ	Τ	Ζ	Θ	Μ	Ο
Λ	Ι	Π	Κ	Ε	Μ	Μ	Γ	Σ	Ξ	Ι	Η	Ο	Ι	Π
Λ	Ε	Η	Ω	Ι	Α	Ξ	Ο	Υ	Ζ	Δ	Υ	Σ	Β	Ψ
Α	Ι	Ρ	Ψ	Χ	Β	Η	Ν	Μ	Ω	Ρ	Ι	Η	Κ	Ξ
Τ	Γ	Ο	Ν	Ο	Χ	Γ	Τ	Μ	Ω	Α	Ψ	Ζ	Ψ	Ξ
Ε	Υ	Φ	Υ	Σ	Λ	Υ	Ε	Ο	Λ	Σ	Β	Ν	Φ	Τ
Μ	Μ	Η	Υ	Γ	Ψ	Υ	Σ	Π	Κ	Η	Ρ	Α	Χ	Ω
Κ	Λ	Υ	Τ	Ρ	Ο	Λ	Ο	Γ	Ι	Σ	Μ	Ι	Κ	Ο
Ε	Ψ	Μ	Ρ	Π	Χ	Θ	Ξ	Δ	Α	Γ	Κ	Π	Φ	Χ
Χ	Λ	Π	Α	Γ	Ι	Δ	Α	Ι	Θ	Τ	Θ	Ζ	Β	Ε
Θ	Κ	Σ	Ρ	Φ	Π	Ω	Ε	Θ	Ε	Ρ	Γ	Α	Λ	Ο
Γ	Ω	Μ	Κ	Φ	Ρ	Υ	Α	Ρ	Χ	Κ	Μ	Μ	Η	Θ

ΛΥΣΗ ΣΤΑΥΡΟΛΕΞΟΥ

							Π							
							Λ							
			Ε			Π	Α	Γ	Ι	Δ	Α			
			Κ				Ι							
			Μ		Π		Σ							
			Ε	Α	Ν	Τ	Ι	Δ	Ρ	Α	Σ	Η		
			Τ	Ρ			Ο							
			Α	Α										
Λ	Υ	Τ	Ρ	Ο	Λ	Ο	Γ	Ι	Σ	Μ	Ι	Κ	Ο	
	Γ				Λ		Ο							
	Ι				Ε		Ν							
	Ε				Υ		Τ	Ε	Ι	Χ	Ο	Σ		
	Ι				Σ		Ε							
	Ν				Η		Σ							
	Η													

ΟΔΗΓΟΣ ΕΚΠΑΙΔΕΥΤΙΚΟΥ ΓΙΑ ΤΙΣ ΛΥΣΕΙΣ ΤΟΥ ΣΤΑΥΡΟΛΕΞΟΥ

ΟΡΙΖΟΝΤΙΑ

3 οριζόντια: ΠΑΓΙΔΑ Σύστημα-δόλωμα που στήνεται για να προσελκύσει και να αναλύσει κακόβουλους παράγοντες (6 γράμματα)

5 οριζόντια: ΑΝΤΙΔΡΑΣΗ Δομημένο σχέδιο για τον χειρισμό και τον περιορισμό των παραβιάσεων ασφαλείας (9 γράμματα)

6 οριζόντια: ΛΥΤΡΟΛΟΓΙΣΜΙΚΟ Κακόβουλο λογισμικό που κρυπτογραφεί δεδομένα και απαιτεί οικονομική πληρωμή για την αποκρυπτογράφησή τους (14 γράμματα)

8 οριζόντια: ΤΕΙΧΟΣ Φραγμός δικτύου που φιλτράρει την κίνηση βάσει κανόνων ασφαλείας (6 γράμματα)

ΚΑΘΕΤΑ

1 κάθετα: ΠΛΑΙΣΙΟ Δομημένες κατευθυντήριες γραμμές, όπως το NIST, για τη διαχείριση των κινδύνων στον κυβερνοχώρο (7 γράμματα)

2 κάθετα: ΕΚΜΕΤΑΛΛΕΥΣΗ Εκμετάλλευση ευπάθειας που στοχεύεται πριν κυκλοφορήσει διόρθωση από τον κατασκευαστή (12 γράμματα)

4 κάθετα: ΠΑΡΑΓΟΝΤΕΣ Επαλήθευση ασφαλείας που απαιτεί δύο ή περισσότερους παράγοντες ταυτοποίησης (10 γράμματα)

7 κάθετα: ΥΓΙΕΙΝΗ Βέλτιστες πρακτικές για τη διαχείριση διαπιστευτηρίων και κλειδιών ταυτοποίησης (7 γράμματα)

Λύσεις: ανακατεμένες λέξεις και λύση κώδικα

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

ΛΥΣΕΙΣ ΑΝΑΜΕΙΞΗΣ ΛΕΞΕΩΝ

1. ΜΛΓΣΟΤΥΙΙΛΚΟΟΡ — **ΛΥΤΡΟΛΟΓΙΣΜΙΚΟ**
2. ΗΚΤΑΕΥΣΜΛΕΛΕ — **ΕΚΜΕΤΑΛΛΕΥΣΗ**
3. ΤΙΧΣΟΕ — **ΤΕΙΧΟΣ**
4. ΗΓΙΕΝΥΙ — **ΥΓΙΕΙΝΗ**
5. ΤΟΣΑΑΝΓΠΕΡ — **ΠΑΡΑΓΟΝΤΕΣ**
6. ΔΙΠΓΑΑ — **ΠΑΓΙΔΑ**
7. ΡΑΣΗΑΙΝΔΤ — **ΑΝΤΙΔΡΑΣΗ**
8. ΛΙΟΠΙΣΑ — **ΠΛΑΙΣΙΟ**

ΚΛΕΙΔΙ ΠΡΟΚΛΗΣΗΣ ΜΥΣΤΙΚΟΥ ΚΩΔΙΚΑ

"ΑΣΦΑΛΙΣΕ ΤΟ ΣΥΣΤΗΜΑ ΜΕ ΠΟΛΛΑΠΛΟΥΣ ΕΛΕΓΧΟΥΣ"

Λύσεις των μελετών περίπτωσης

A Μελέτη περίπτωσης 1: Στρατηγική ανάκαμψης από ransomware

Λύση για τον εκπαιδευτικό

ΟΔΗΓΙΕΣ ΒΑΘΜΟΛΟΓΗΣΗΣ

Οι απαντήσεις των μαθητών πρέπει να καλύπτουν τα εξής σημεία:

- Ανάλυση σεναρίου: Ένα εταιρικό δίκτυο έχει μολυνθεί από ransomware, που κλειδώνει κρίσιμες βάσεις δεδομένων. Οι επιτιθέμενοι απαιτούν πληρωμή $100.000 σε κρυπτονόμισμα. Η εταιρεία έχει αντίγραφα ασφαλείας εκτός σύνδεσης από 24 ώρες πριν.
- Προτεινόμενη στρατηγική και λύση: Κίνδυνοι πληρωμής: Η πληρωμή δεν εγγυάται την αποκρυπτογράφηση των αρχείων, χαρακτηρίζει την εταιρεία ως στόχο που πληρώνει και χρηματοδοτεί εγκληματική δραστηριότητα. Στρατηγική ανάκτησης: Η ομάδα πρέπει να απομονώσει τους μολυσμένους υπολογιστές, να διαγράψει τους παραβιασμένους διακομιστές και να επαναφέρει τα δεδομένα από αντίγραφα ασφαλείας εκτός σύνδεσης. Πρέπει να διορθώσει το αρχικό σημείο εισόδου (ηλεκτρονικό ψάρεμα ή εκμετάλλευση ευπάθειας) για να αποφευχθεί άμεση επαναμόλυνση.

B Μελέτη περίπτωσης 2: Άμυνα απέναντι σε credential stuffing

Λύση για τον εκπαιδευτικό

ΟΔΗΓΙΕΣ ΒΑΘΜΟΛΟΓΗΣΗΣ

Οι απαντήσεις των μαθητών πρέπει να καλύπτουν τα εξής σημεία:

- Ανάλυση σεναρίου: Μια διαδικτυακή υπηρεσία δέχεται επίθεση credential stuffing, με χάκερ να δοκιμάζουν εκατομμύρια ζεύγη ονόματος χρήστη και κωδικού πρόσβασης που έχουν κλαπεί από άλλους ιστότοπους.
- Προτεινόμενη στρατηγική και λύση: Μηχανισμός: Οι επιτιθέμενοι εκμεταλλεύονται την επαναχρησιμοποίηση κωδικών πρόσβασης σε διάφορους ιστότοπους, με αυτοματοποιημένα bots που συνδέονται σε λογαριασμούς χρηστών. Άμυνες: 1. Ο έλεγχος ταυτότητας πολλαπλών παραγόντων (MFA) αποκλείει τις προσπάθειες σύνδεσης ακόμη και αν ο κωδικός είναι σωστός. 2. Ο περιορισμός ρυθμού και τα CAPTCHA αποκλείουν την αυτοματοποιημένη κίνηση bots που πλημμυρίζει τα σημεία σύνδεσης.