Όνομα: _____ Ημερομηνία: _____ Βαθμολογία: _____

Επιθέσεις Ransomware και επιχειρησιακή Ανάκτηση

Εκτέλεση κακόβουλου φορτίου, κρυπτογράφηση αρχείων, αντίγραφα ασφαλείας εκτός σύνδεσης, διαδικασίες περιορισμού και αποκατάσταση καταστροφών.

ΕΠΙΣΚΟΠΗΣΗ ΜΑΘΗΣΗΣ ΓΙΑ ΤΙΣ ΕΠΙΘΕΣΕΙΣ RANSOMWARE

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 επιθέσεις ransomware και την επιχειρησιακή αποκατάσταση. Θα εξερευνήσεις την εκτέλεση ωφέλιμου φορτίου, την κρυπτογράφηση αρχείων, τα αντίγραφα ασφαλείας εκτός σύνδεσης, τον περιορισμό απειλών, τις πληρωμές σε κρυπτονομίσματα και τα σχέδια αποκατάστασης από καταστροφές.

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/epithe-ransomware/

Η πορεία μάθησής σου: αποκατάσταση από ransomware

- Διαχώρισε τα ωφέλιμα φορτία Trojan, ransomware και spyware.
- Ανάλυσε κακόβουλα αρχεία μέσα σε ασφαλή περιβάλλοντα sandbox.
- Σχεδίασε διαδικασίες άμεσης απομόνωσης και περιορισμού του δικτύου.

ΟΔΗΓΙΕΣ ΓΙΑ ΤΙΣ ΕΠΙΘΕΣΕΙΣ RANSOMWARE

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 ανάκτηση μετά από ransomware. Ολοκλήρωσε με τη δραστηριότητα μπόνους Σκέψου γρήγορα.

ΕΠΙΘΕΣΕΙΣ RANSOMWARE ΚΑΙ ΑΝΑΚΤΗΣΗ ΜΕΤΑ ΑΠΟ ΚΑΤΑΣΤΡΟΦΗ (ΕΙΣΑΓΩΓΗ)

Τα φορτία ransomware κλειδώνουν κρυπτογραφικά τον αποθηκευτικό χώρο του συστήματος, απαιτώντας πληρωμές σε κρυπτονομίσματα για τα κλειδιά αποκρυπτογράφησης. Ο μετριασμός αυτής της απειλής περιλαμβάνει κανόνες απομόνωσης δικτύου, ανάλυση κακόβουλου λογισμικού σε sandbox και ισχυρά air-gapped ψυχρά αντίγραφα ασφαλείας.

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

Σημείο ελέγχου 1: Πρόκληση πολλαπλής επιλογής

1 **1. Ποιος είναι ο κύριος μηχανισμός μιας επίθεσης ransomware;**

- A. Κρυπτογράφηση των αρχείων του χρήστη ώστε να απαγορεύεται η πρόσβαση στο σύστημα
- B. Έγχυση κακόβουλων εντολών SQL σε πεδία φορμών
- C. Υποκλοπή πακέτων δικτύου σε δημόσιο Wi-Fi
- D. Πλαστογράφηση κεφαλίδων email για παράκαμψη της επικύρωσης SPF

2 **2. Τι είναι ένα αντίγραφο ασφαλείας εκτός σύνδεσης (cold);**

- A. Ένα αντίγραφο αποθήκευσης αποσυνδεδεμένο από το δίκτυο για να προστατεύεται από τη διάδοση κακόβουλου λογισμικού
- B. Ένα αντίγραφο ασφαλείας αποθηκευμένο στον σκληρό δίσκο του κύριου διακομιστή ιστού
- C. Μια προσωρινή μνήμη (cache) αρχείων καταγραφής του μητρώου συστήματος
- D. Ένα διοικητικό εργαλείο που χρησιμοποιείται για επαναφορά κωδικών πρόσβασης χρηστών

3 **3. Πώς πρέπει οι ομάδες ασφαλείας να απομονώνουν τα μολυσμένα συστήματα κατά τη διάρκεια μιας επίθεσης ransomware;**

- A. Αποσύνδεση των καλωδίων δικτύου και άμεση απενεργοποίηση των ασύρματων διεπαφών
- B. Αναβάθμιση της βάσης δεδομένων υπογραφών του antivirus
- C. Απενεργοποίηση του κύριου διακομιστή DNS
- D. Μετονομασία των επεκτάσεων των παραβιασμένων αρχείων

4 **4. Γιατί οι υπηρεσίες ασφαλείας συμβουλεύουν να μην πληρώνονται οι απαιτήσεις ransomware;**

- A. Η καταβολή χρημάτων ενθαρρύνει τους επιτιθέμενους και δεν εγγυάται την παράδοση του κλειδιού αποκρυπτογράφησης
- B. Ακυρώνει αυτόματα όλα τα εταιρικά ασφαλιστήρια συμβόλαια
- C. Ειδοποιεί αυτόματα κάθε πελάτη με email
- D. Καταστρέφει τα υπόλοιπα αρχεία αντιγράφων ασφαλείας του συστήματος

5 **5. Τι είναι ένα σχέδιο αποκατάστασης καταστροφών (DRP);**

- A. Μια δομημένη διαδικασία επαναφοράς των λειτουργιών και των δεδομένων μετά από παραβίαση του συστήματος
- B. Μια διαμόρφωση τείχους προστασίας που αντιστοιχίζει τις εισερχόμενες θύρες δικτύου
- C. Ένα σχήμα βάσης δεδομένων που απαριθμεί τα διαχειριστικά δικαιώματα χρηστών
- D. Ένα πρωτόκολλο ταυτοποίησης email που απορρίπτει πλαστά domain

Σημείο ελέγχου 2: Πρόκληση Σωστό ή Λάθος

6 Ερώτηση 6

6. Τα φορτία (payloads) ransomware μπορούν εύκολα να εξαπλωθούν σε διαδικτυακά αντίγραφα ασφαλείας που είναι συνδεδεμένα με το δίκτυο.

○ Σωστό ○ Λάθος

7 Ερώτηση 7

7. Η πληρωμή λύτρων σε κρυπτονόμισμα εγγυάται ότι τα αρχεία θα αποκρυπτογραφηθούν με επιτυχία.

○ Σωστό ○ Λάθος

8 Ερώτηση 8

8. Η αποσύνδεση των μολυσμένων συστημάτων από το δίκτυο βοηθά να σταματήσει η εξάπλωση του ransomware σε γειτονικά συστήματα.

○ Σωστό ○ Λάθος

9 Ερώτηση 9

9. Η συμμετρική κρυπτογραφία δεν χρησιμοποιείται ποτέ από ransomware για την κρυπτογράφηση της αποθήκευσης του συστήματος.

○ Σωστό ○ Λάθος

10 Ερώτηση 10

10. Η τακτική δοκιμή των διαδικασιών επαναφοράς δεδομένων είναι κρίσιμο μέρος της ανάκτησης από καταστροφή.

○ 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 άρνηση πρόσβασης σε τοπικά αρχεία χρησιμοποιεί κρυπτογραφική _____ .

2. Ο ενεργός κακόβουλος κώδικας που εκτελείται σε ένα σύστημα είναι το ωφέλιμο _____ .

3. Τα αποσυνδεδεμένα αντίγραφα αποθήκευσης εκτός χώρου αποτελούν ένα ασφαλές _____ .

4. Η παύση της εξάπλωσης κακόβουλου λογισμικού απαιτεί _____ των τερματικών του δικτύου.

5. Η πληρωμή σε κρυπτονόμισμα που απαιτούν οι κυβερνοεγκληματίες είναι τα _____ .

6. Η επαναφορά λειτουργικών αρχείων δεδομένων αποτελεί _____ από καταστροφή.

ΤΡΑΠΕΖΑ ΛΕΞΕΩΝ

ΑΝΑΚΤΗΣΗ ΑΠΟΜΟΝΩΣΗ ΔΟΥΡΕΙΟΣ ΙΠΠΟΣ ΚΑΤΑΣΤΡΟΦΗ ΚΡΥΠΤΟΓΡΑΦΗΣΗ ΛΥΤΡΑ ΦΟΡΤΙΟ ΨΥΧΡΟ ΑΝΤΙΓΡΑΦΟ

Γράψε τις απαντήσεις σου εδώ:

1. **2.**

3. **4.**

5. **6.**

Σημείο ελέγχου 4: Αντιστοίχιση εννοιών ασφάλειας

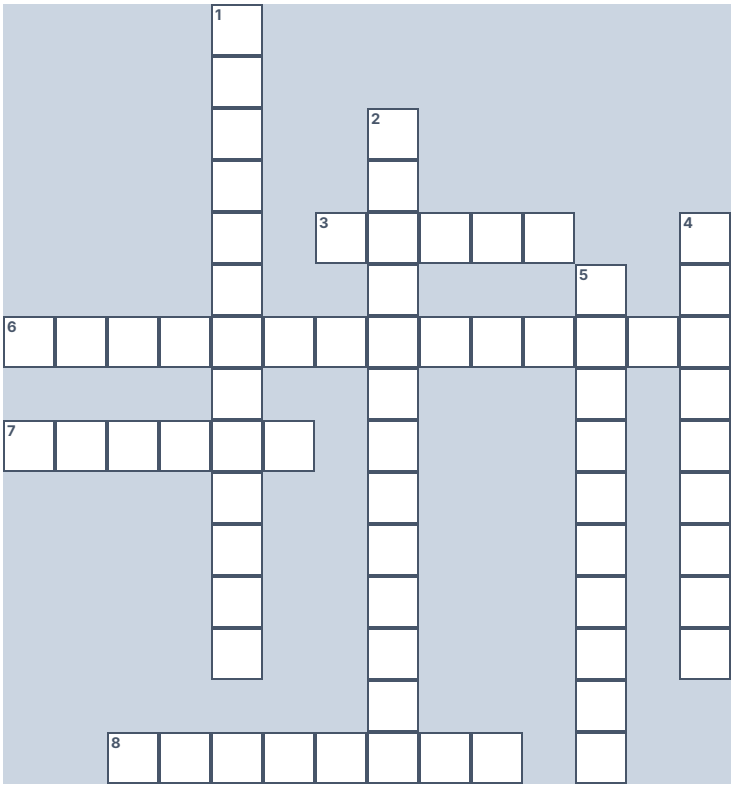
ΑΝΤΙΣΤΟΙΧΙΣΗ ΟΡΙΣΜΩΝ

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**	Αποσύνδεση των μολυσμένων συστημάτων δικτύου.
☐	2. ΦΟΡΤΙΟ	**B**	Κακόβουλο αρχείο μεταμφιεσμένο σε αβλαβές.
☐	3. ΨΥΧΡΟ ΑΝΤΙΓΡΑΦΟ ΑΣΦΑΛΕΙΑΣ	**C**	Κλείδωμα αρχείων με κρυπτογραφικό τρόπο.
☐	4. ΑΠΟΜΟΝΩΣΗ	**D**	Συμβάν μείζονος διακοπής του συστήματος.
☐	5. ΛΥΤΡΑ	**E**	Εκτέλεση κακόβουλου λογισμικού.
☐	6. ΑΝΑΚΤΗΣΗ	**F**	Αποσυνδεδεμένο αντίγραφο εκτός σύνδεσης.
☐	7. ΚΑΤΑΣΤΡΟΦΗ	**G**	Επαναφορά βάσης δεδομένων από αντίγραφο ασφαλείας.
☐	8. ΤΡΟΪΚΟΣ ΙΟΣ	**H**	Αίτημα εξαγωγής κρυπτογραφικού κλειδιού.

Σημείο ελέγχου 5: Σταυρόλεξο

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



ΟΡΙΖΟΝΤΙΑ

3. Αίτημα πληρωμής για το κρυπτογραφικό κλειδί (5)

6. Αποσυνδεδεμένο αντίγραφο εκτός σύνδεσης (14)

7. Εκτέλεση κακόβουλου λογισμικού (6)

8. Επαναφορά της βάσης δεδομένων από αντίγραφο ασφαλείας (8)

ΚΑΘΕΤΑ

1. Κακόβουλο αρχείο μεταμφιεσμένο σε αθώο (13)

2. Κρυπτογραφικό κλείδωμα αρχείων (13)

4. Αποσύνδεση μολυσμένων συστημάτων δικτύου (9)

5. Σοβαρό περιστατικό διακοπής του συστήματος (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

3 οριζόντια: Αίτημα πληρωμής για το κρυπτογραφικό κλειδί (5 γράμματα):

6 οριζόντια: Αποσυνδεδεμένο αντίγραφο εκτός σύνδεσης (14 γράμματα):

7 οριζόντια: Εκτέλεση κακόβουλου λογισμικού (6 γράμματα):

8 οριζόντια: Επαναφορά της βάσης δεδομένων από αντίγραφο ασφαλείας (8 γράμματα):

ΚΑΘΕΤΑ

1 κάθετα: Κακόβουλο αρχείο μεταμφιεσμένο σε αθώο (13 γράμματα):

2 κάθετα: Κρυπτογραφικό κλείδωμα αρχείων (13 γράμματα):

4 κάθετα: Αποσύνδεση μολυσμένων συστημάτων δικτύου (9 γράμματα):

5 κάθετα: Σοβαρό περιστατικό διακοπής του συστήματος (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.

Η Τ Θ Ζ Β Ε Θ Κ Σ Ρ Φ Π Ω Ε Θ

Σ Ε Η Φ Ο Ρ Τ Σ Α Τ Α Κ Ρ Φ Α

Η Γ Α Λ Ο Γ Ω Ρ Μ Κ Φ Ρ Ο Ν Υ

Φ Α Ρ Χ Κ Μ Τ Μ Η Θ Ν Ρ Α Θ Π

Α Ζ Λ Σ Λ Υ Ρ Χ Θ Β Τ Κ Τ Ζ Ψ

Ρ Ξ Ψ Χ Λ Σ Η Τ Χ Ι Τ Α Ο Υ Ν

Γ Ν Ω Ξ Θ Ο Σ Θ Ο Η Ο Υ Τ Ξ Υ

Ο Τ Κ Α Ε Ξ Μ Λ Σ Α Ν Υ Ζ Η Ο

Τ Π Χ Ψ Ι Κ Υ Η Ι Ω Φ Ψ Ο Κ Θ

Π Ω Ι Η Σ Ω Ν Ο Μ Ο Π Α Ι Ν Α

Υ Ψ Υ Χ Ρ Ο Α Ν Τ Ι Γ Ρ Α Φ Ο

Ρ Ε Θ Α Σ Α Ι Ε Φ Ε Κ Ω Κ Ε Κ

Κ Π Δ Ο Υ Ρ Ε Ι Ο Σ Ι Π Π Ο Σ

Ν Ι Α Ζ Ξ Κ Ν Γ Ν Γ Δ Η Θ Β Α

Ξ Ρ Λ Ο Φ Τ Θ Ψ Ζ Ω Ρ Η Χ Φ Θ

ΛΙΣΤΑ ΛΕΞΕΩΝ

ΚΡΥΠΤΟΓΡΑΦΗΣΗ ΦΟΡΤΙΟ ΨΥΧΡΟΑΝΤΙΓΡΑΦΟ ΑΠΟΜΟΝΩΣΗ ΛΥΤΡΑ
ΑΝΑΚΤΗΣΗ ΚΑΤΑΣΤΡΟΦΗ ΔΟΥΡΕΙΟΣΙΠΠΟΣ

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. ΦΟΡΤΙΟ

C. ΨΥΧΡΟΑΝΤΙΓΡΑΦΟ

D. ΑΠΟΜΟΝΩΣΗ

E. ΛΥΤΡΑ

F. ΑΝΑΚΤΗΣΗ

G. ΚΑΤΑΣΤΡΟΦΗ

H. ΔΟΥΡΕΙΟΣΙΠΠΟΣ

ΟΡΙΣΜΟΙ ΚΑΙ ΠΕΔΙΑ ΑΝΤΙΣΤΟΙΧΙΣΗΣ

_____ 1. Αποσυνδεδεμένο αντίγραφο εκτός σύνδεσης.

_____ 2. Κακόβουλο αρχείο μεταμφιεσμένο σε αθώο.

_____ 3. Κρυπτογραφικό κλείδωμα αρχείων.

_____ 4. Αίτημα πληρωμής για το κρυπτογραφικό κλειδί.

_____ 5. Αποσύνδεση μολυσμένων συστημάτων δικτύου.

_____ 6. Σοβαρό περιστατικό διακοπής του συστήματος.

_____ 7. Εκτέλεση κακόβουλου λογισμικού.

_____ 8. Επαναφορά της βάσης δεδομένων από αντίγραφο ασφαλείας.

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. ΟΥΑΧΝΦΨΑΤΟΓΡΙΡ
3. ΤΛΑΡΥ
4. ΤΦΣΗΑΟΡΚΑΤ
5. ΤΡΟΦΙΟ
6. ΣΜΠΩΝΑΟΗΟ
7. ΑΗΤΗΣΝΚΑ
8. ΙΥΕΙΠΣΣΔΟΟΟΠΡ

Δραστηριότητα μπόνους: Σκέψου γρήγορα

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

1	Πληροφορίες που δεν πρέπει ποτέ να μοιράζεσαι			
2	Συσκευές που μπορούν να παραβιαστούν			
3	Λόγοι για να μην πληρώσεις λύτρα			
4	Ασφαλείς συνήθειες που μπορείς να ξεκινήσεις σήμερα			
5	Εργαλεία ασφαλείας που γνωρίζεις			
6	Τρόποι να προστατεύσεις τους λογαριασμούς σου			
7	Ενδείξεις ότι ένας υπολογιστής έχει μολυνθεί			
8	Μέρη όπου κρατάς ένα αντίγραφο ασφαλείας			
9	Αρχεία που δεν θέλεις ποτέ να χάσεις			
10	Τρόποι με τους οποίους εξαπλώνεται το ransomware			
11	Πράγματα που κάνεις την πρώτη ώρα μιας επίθεσης			
12	Άνθρωποι με τους οποίους επικοινωνείς κατά τη διάρκεια μιας επίθεσης			
13	Πράγματα που μπορεί να κλειδώσει το ransomware			
14	Λέξεις που σχετίζονται με την κυβερνοασφάλεια			
15	Οργανισμοί που στοχοποιούνται συχνά			

Σημείο ελέγχου 8: Μελέτες περίπτωσης κυβερνοασφάλειας

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

ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ 1: ΠΕΡΙΟΡΙΣΜΟΣ ΩΦΕΛΙΜΟΥ ΦΟΡΤΙΟΥ RANSOMWARE ΣΕ ΕΠΙΧΕΙΡΗΣΗ

👷

Σενάριο: Ένα εταιρικό τοπικό δίκτυο έχει παραβιαστεί από ενεργό ransomware. Βασικοί διακομιστές αρχείων άρχισαν να εμφανίζουν επεκτάσεις αρχείων .locked.

Ερώτηση συζήτησης: Περίγραψε αναλυτικά τα βήματα περιορισμού και περίγραψε συνοπτικά το πρωτόκολλο ανάκτησης δεδομένων.

ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ 2: ΑΞΙΟΛΟΓΗΣΗ ΑΡΧΙΤΕΚΤΟΝΙΚΩΝ ΑΝΤΙΓΡΑΦΩΝ ΑΣΦΑΛΕΙΑΣ ΕΚΤΟΣ ΔΙΚΤΥΟΥ

👷

Σενάριο: Μια επιχείρηση θέλει να σχεδιάσει μια στρατηγική αντιγράφων ασφαλείας δεδομένων που μειώνει τον κίνδυνο να παραβιαστούν τα αντίγραφα, ακόμη κι αν το κύριο τοπικό δίκτυο έχει καταληφθεί πλήρως από ransomware.

Ερώτηση συζήτησης: Σχεδίασε ένα ασφαλές σύστημα θησαυροφυλακίου αντιγράφων ασφαλείας εκτός σύνδεσης.

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	13	5	21	5	17	5		4	5	4	15	12	5	13	1
1	**16**	**15**		**23**	**20**	**22**	**17**	**15**		**1**	**13**	**19**	**9**	**3**	**17**	**1**	**21**	**15**

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 ransomware;

Το ransomware είναι κακόβουλο λογισμικό που έχει σχεδιαστεί για να εμποδίζει την πρόσβαση σε υπολογιστικά συστήματα ή αρχεία μέχρι να καταβληθεί ένα ποσό λύτρων.

Q2: Πώς εξαπλώνεται το ransomware;

Μέσω συνημμένων ηλεκτρονικού ψαρέματος (phishing) σε email, ευπαθειών μη ενημερωμένου λογισμικού και παραβιασμένων συστημάτων απομακρυσμένης πρόσβασης. [1]

Q3: Γιατί ζητείται πληρωμή με κρυπτονομίσματα;

Τα κρυπτονομίσματα όπως το Bitcoin προσφέρουν σχετική ανωνυμία, γεγονός που δυσκολεύει τις αρχές επιβολής του νόμου να παρακολουθήσουν τα κεφάλαια.

Q4: Αποκλείει το antivirus το ransomware;

Ναι, αλλά το antivirus που βασίζεται σε υπογραφές μπορεί να αποτύχει απέναντι σε νεοδημιουργημένα ωφέλιμα φορτία ransomware zero-day.

Q5: Τι είναι ένα air-gapped αντίγραφο ασφαλείας;

Ένα αντίγραφο ασφαλείας χωρίς φυσική ή λογική σύνδεση με το κύριο δίκτυο, που το προστατεύει από τη διάδοση.

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 ο διπλός εκβιασμός;

Όταν οι επιτιθέμενοι όχι μόνο κρυπτογραφούν αρχεία αλλά κλέβουν και ευαίσθητα δεδομένα, για να απειλήσουν με δημόσια διαρροή αν δεν πληρωθούν.

Q7: Τι είναι ένα εργαλείο αποκρυπτογράφησης (decryptor);

Ένα βοηθητικό πρόγραμμα λογισμικού που περιέχει το κρυπτογραφικό κλειδί που χρειάζεται για να επαναφερθούν τα κλειδωμένα αρχεία σε απλό κείμενο.

Q8: Πώς εντοπίζεις έγκαιρα το ransomware;

Παρακολουθώντας τα συστήματα αρχείων για ξαφνική, μαζική τροποποίηση και μετονομασία αρχείων.

Q9: Ποιος είναι ο ρόλος της ασφάλισης;

Η ασφάλιση κυβερνοκινδύνων μπορεί να βοηθήσει στην κάλυψη του κόστους αποκατάστασης, αλλά οι όροι κάλυψης και οι κανόνες πληρωμής λύτρων διαφέρουν ανάλογα με το συμβόλαιο.

Q10: Πρέπει να κάνω επανεκκίνηση σε ένα μολυσμένο σύστημα;

Όχι, η επανεκκίνηση μπορεί να καταστρέψει τα στοιχεία της πτητικής μνήμης· απομόνωσέ το από το δίκτυο. [1]

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 χρησιμοποιεί το ransomware ασύμμετρη κρυπτογράφηση;

Χρησιμοποιεί ένα δημόσιο κλειδί ενσωματωμένο στο κακόβουλο λογισμικό για να κρυπτογραφήσει αρχεία, απαιτώντας το ιδιωτικό κλειδί του επιτιθέμενου για την αποκρυπτογράφησή τους.

Q2: Γιατί χρησιμοποιείται επίσης συμμετρική κρυπτογράφηση;

Η συμμετρική κρυπτογράφηση (όπως το AES) είναι γρήγορη και μπορεί να κλειδώσει τεράστιες βάσεις δεδομένων σε λίγα λεπτά, ενώ τα ασύμμετρα κλειδιά ασφαλίζουν το κλειδί AES.

Q3: Τι είναι ο λογικός κατακερματισμός δικτύου (logical segmentation);

Διαίρεση των δικτύων σε απομονωμένες ζώνες, εμποδίζοντας το κακόβουλο λογισμικό να εξαπλώνεται πλευρικά από τους σταθμούς εργασίας στους κεντρικούς διακομιστές.

Q4: Τι είναι η αποθήκευση WORM;

Μέσα Write-Once, Read-Many, που εμποδίζουν τα δεδομένα αντιγράφων ασφαλείας να επεξεργαστούν, να αντικατασταθούν ή να διαγραφούν από ωφέλιμα φορτία ransomware.

Q5: Τι είναι τα στιγμιότυπα σκιάς (shadow copies);

Τοπικά στιγμιότυπα αντιγράφων ασφαλείας που δημιουργούνται από τα Windows· το ransomware συνήθως τα διαγράφει πρώτα με εργαλεία διαχείρισης.

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: Πώς διευκολύνει η κλοπή διαπιστευτηρίων το ransomware;

Οι επιτιθέμενοι αγοράζουν διαρρεύσαντα διαπιστευτήρια διαχειριστών για να συνδεθούν μέσω απομακρυσμένων επιφανειών εργασίας και να εκτελέσουν χειροκίνητα ransomware σε όλο το δίκτυο.

Q7: Τι είναι η δοκιμή επαναφοράς dry-run;

Τακτική επαναφορά βάσεων δεδομένων αντιγράφων ασφαλείας σε απομονωμένα περιβάλλοντα δοκιμών, για να επαληθευτεί ότι η ταχύτητα επαναφοράς και η ακεραιότητα των δεδομένων πληρούν τις μετρικές ανάκτησης από καταστροφή.

Q8: Πώς σταματά το ransomware ο εντοπισμός σε τερματικά (EDR);

Αναλύοντας τη συμπεριφορά των διεργασιών (π.χ. ταχεία κρυπτογράφηση) και αναστέλλοντας γρήγορα την επιβλαβή εφαρμογή.

Q9: Τι είναι το μοντέλο ransomware-as-a-service (RaaS);

Ένα μοντέλο franchise όπου οι δημιουργοί κακόβουλου λογισμικού εκμισθώνουν εργαλεία δημιουργίας ransomware σε συνεργάτες με αντάλλαγμα ένα ποσοστό των πληρωμών.

Q10: Πώς προκαλεί ransomware ένα RDP χωρίς ενημερώσεις;

Οι εκτεθειμένες πύλες Remote Desktop Protocol χωρίς ενημερώσεις επιτρέπουν στους επιτιθέμενους να σπάνε τα στοιχεία σύνδεσης με brute force και να εκτελούν χειροκίνητα κακόβουλο λογισμικό.

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 δράστες ransomware χρησιμοποιούν συχνά εργαλεία όπως το vssadmin.exe για να διαγράψουν τα στιγμιότυπα σκιάς (shadow copies) των Windows και να εμποδίσουν τις τοπικές επαναφορές. [1]

2. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Τα συμμετρικά κλειδιά AES-256 χρησιμοποιούνται συνήθως για την κρυπτογράφηση του φορτίου των αρχείων, τα οποία στη συνέχεια κλειδώνονται με δημόσια κλειδιά RSA.

3. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Η ανάκαμψη από μια επιτυχημένη επίθεση ransomware μπορεί να διαρκέσει εβδομάδες, γι' αυτό έχουν σημασία τα δοκιμασμένα αντίγραφα ασφαλείας εκτός σύνδεσης.

4. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Το FBI δεν υποστηρίζει την καταβολή λύτρων και προειδοποιεί ότι η πληρωμή δεν εγγυάται ότι θα ανακτήσεις τα δεδομένα σου. [2]

5. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Τα σχέδια αποκατάστασης καταστροφών (DRP) πρέπει να ορίζουν έναν Στόχο Χρόνου Αποκατάστασης (RTO) και έναν Στόχο Σημείου Αποκατάστασης (RPO).

6. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Το FBI συνιστά αντίγραφα ασφαλείας που είναι κρυπτογραφημένα και αμετάβλητα, δηλαδή δεν μπορούν να τροποποιηθούν ή να διαγραφούν. [3]

7. ΕΙΔΗΣΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Οι προγραμματιστές ransomware χρησιμοποιούν προηγμένες τεχνικές συσκότισης (obfuscation) για να παρακάμψουν τους παραδοσιακούς σαρωτές antivirus που βασίζονται σε υπογραφές.

8. ΕΙΔΗΣΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Η τμηματοποίηση δικτύου περιορίζει την πλευρική κίνηση, βοηθώντας να μην εξαπλωθεί το ransomware πέρα από τον πρώτο μολυσμένο υπολογιστή. [3]

9. ΕΙΔΗΣΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Οι εκτεθειμένες, κακά ασφαλισμένες απομακρυσμένες υπηρεσίες, όπως το Remote Desktop Protocol (RDP), είναι συνηθισμένο σημείο εισόδου για ransomware. [1]

10. ΠΡΟΟΠΤΙΚΗ ΓΙΑ ΤΗΝ ΑΣΦΑΛΕΙΑ

Η CISA συνιστά τη διατήρηση κρυπτογραφημένων αντιγράφων ασφαλείας εκτός δικτύου, καθώς πολλές παραλλαγές ransomware αναζητούν και διαγράφουν τα προσβάσιμα αντίγραφα. [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] CISA. (2023). #StopRansomware Guide.

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

[2] FBI Internet Crime Complaint Center. (n.d.). Ransomware.

https://www.ic3.gov/CrimeInfo/Ransomware

[3] FBI Internet Crime Complaint Center. (2026). 2025 IC3 Annual Report.

https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

[4] CISA. (n.d.). Malware, Phishing, and Ransomware.

https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

[5] 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

Λύσεις: Σημείο ελέγχου 1 – Πολλαπλής επιλογής

1 **Ερώτηση 1** — **Σωστή απάντηση: A**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Ποιος είναι ο κύριος μηχανισμός μιας επίθεσης ransomware; → Κρυπτογράφηση των αρχείων του χρήστη ώστε να απαγορεύεται η πρόσβαση στο σύστημα

2 **Ερώτηση 2** — **Σωστή απάντηση: A**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Τι είναι ένα αντίγραφο ασφαλείας εκτός σύνδεσης (cold); → Ένα αντίγραφο αποθήκευσης αποσυνδεδεμένο από το δίκτυο για να προστατεύεται από τη διάδοση κακόβουλου λογισμικού

3 **Ερώτηση 3** — **Σωστή απάντηση: A**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Πώς πρέπει οι ομάδες ασφαλείας να απομονώνουν τα μολυσμένα συστήματα κατά τη διάρκεια μιας επίθεσης ransomware; → Αποσύνδεση των καλωδίων δικτύου και άμεση απενεργοποίηση των ασύρματων διεπαφών

4 **Ερώτηση 4** — **Σωστή απάντηση: A**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Γιατί οι υπηρεσίες ασφαλείας συμβουλεύουν να μην πληρώνονται οι απαιτήσεις ransomware; → Η καταβολή χρημάτων ενθαρρύνει τους επιτιθέμενους και δεν εγγυάται την παράδοση του κλειδιού αποκρυπτογράφησης

5 **Ερώτηση 5** — **Σωστή απάντηση: A**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Τι είναι ένα σχέδιο αποκατάστασης καταστροφών (DRP); → Μια δομημένη διαδικασία επαναφοράς των λειτουργιών και των δεδομένων μετά από παραβίαση του συστήματος

Λύσεις: Σημείο ελέγχου 2 – Σωστό ή Λάθος

6 **Ερώτηση 6** — **Σωστή απάντηση: Σωστό**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Τα φορτία (payloads) ransomware μπορούν εύκολα να εξαπλωθούν σε διαδικτυακά αντίγραφα ασφαλείας που είναι συνδεδεμένα με το δίκτυο.

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

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Λάθος: το FBI προειδοποιεί ότι η πληρωμή δεν εγγυάται ότι θα ανακτήσεις οποιαδήποτε δεδομένα.

8 **Ερώτηση 8** — **Σωστή απάντηση: Σωστό**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Σωστό: η CISA συμβουλεύει να αποσυνδέονται οι μολυσμένοι υπολογιστές ή να τίθεται το δίκτυο εκτός σύνδεσης για να περιοριστεί η εξάπλωση.

9 **Ερώτηση 9** — **Σωστή απάντηση: Λάθος**

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Λάθος: το ransomware συνήθως κρυπτογραφεί τα αρχεία με γρήγορους συμμετρικούς αλγορίθμους όπως το AES.

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

ΣΗΜΕΙΩΣΗ ΓΙΑ ΤΟΝ ΕΚΠΑΙΔΕΥΤΙΚΟ

Η τακτική δοκιμή των διαδικασιών επαναφοράς δεδομένων είναι κρίσιμο μέρος της ανάκτησης από καταστροφή.

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

C 1. ΚΡΥΠΤΟΓΡΑΦΗΣΗ	E 2. ΦΟΡΤΙΟ	F 3. ΨΥΧΡΟ ΑΝΤΙΓΡΑΦΟ ΑΣΦΑΛΕΙΑΣ	A 4. ΑΠΟΜΟΝΩΣΗ
H 5. ΛΥΤΡΑ	G 6. ΑΝΑΚΤΗΣΗ	D 7. ΚΑΤΑΣΤΡΟΦΗ	B 8. ΤΡΟΪΚΟΣ ΙΟΣ

ΣΗΜΕΙΟ ΕΛΕΓΧΟΥ 3: ΛΥΣΕΙΣ – ΒΑΣΙΚΟΙ ΟΡΟΙ

1 ΚΡΥΠΤΟΓΡΑΦΗΣΗ	2 ΦΟΡΤΙΟ	3 ΨΥΧΡΟ ΑΝΤΙΓΡΑΦΟ	4 ΑΠΟΜΟΝΩΣΗ
5 ΛΥΤΡΑ	6 ΑΝΑΚΤΗΣΗ		

ΣΗΜΕΙΟ ΕΛΕΓΧΟΥ 6, ΕΝΑΛΛΑΚΤΙΚΑ: ΛΥΣΕΙΣ – ΑΝΤΙΣΤΟΙΧΙΣΗ ΛΕΞΕΩΝ

1 C – ΨΥΧΡΟΑΝΤΙΓΡΑΦΟ	2 H – ΔΟΥΡΕΙΟΣΙΠΠΟΣ	3 A – ΚΡΥΠΤΟΓΡΑΦΗΣΗ	4 E – ΛΥΤΡΑ
5 D – ΑΠΟΜΟΝΩΣΗ	6 G – ΚΑΤΑΣΤΡΟΦΗ	7 B – ΦΟΡΤΙΟ	8 F – ΑΝΑΚΤΗΣΗ

ΣΗΜΕΙΩΣΕΙΣ ΣΥΖΗΤΗΣΗΣ ΓΙΑ ΕΚΠΑΙΔΕΥΤΙΚΟΥΣ

Βασικοί όροι:
Έλεγξε αν οι μαθητές μπορούν να εξηγήσουν με δικά τους λόγια τους όρους ΚΡΥΠΤΟΓΡΑΦΗΣΗ, ΦΟΡΤΙΟ και ΨΥΧΡΟ ΑΝΤΙΓΡΑΦΟ ΑΣΦΑΛΕΙΑΣ 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.

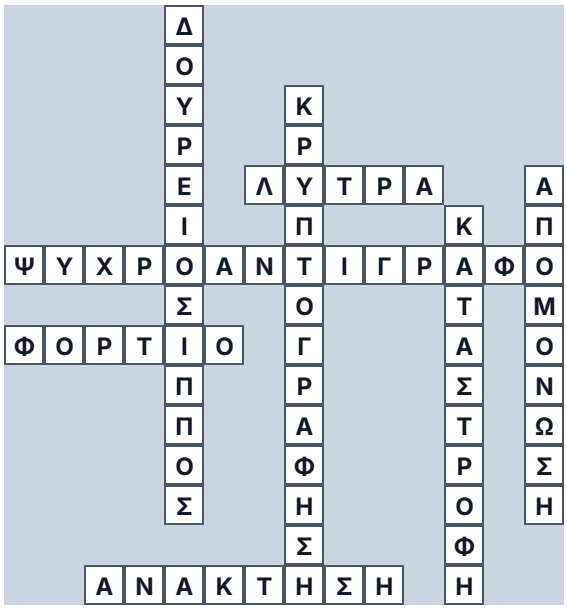
Αξιολόγηση πηγών:
Ζήτησε από τους μαθητές να επαληθεύσουν τουλάχιστον έναν ισχυρισμό στις πηγές του φύλλου και συζητήστε γιατί οι αριθμοί, οι τιμές και οι κανόνες μπορεί να αλλάζουν με τον χρόνο.

Λύσεις γρίφων και σημειώσεις για τον εκπαιδευτικό

ΛΥΣΗ ΓΡΙΦΟΥ ΛΕΞΕΩΝ

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

ΛΥΣΗ ΣΤΑΥΡΟΛΕΞΟΥ



ΟΔΗΓΟΣ ΕΚΠΑΙΔΕΥΤΙΚΟΥ ΓΙΑ ΤΙΣ ΛΥΣΕΙΣ ΤΟΥ ΣΤΑΥΡΟΛΕΞΟΥ

ΟΡΙΖΟΝΤΙΑ

3 οριζόντια: ΛΥΤΡΑ Αίτημα πληρωμής για το κρυπτογραφικό κλειδί (5 γράμματα)

6 οριζόντια: ΨΥΧΡΟΑΝΤΙΓΡΑΦΟ Αποσυνδεδεμένο αντίγραφο εκτός σύνδεσης (14 γράμματα)

7 οριζόντια: ΦΟΡΤΙΟ Εκτέλεση κακόβουλου λογισμικού (6 γράμματα)

8 οριζόντια: ΑΝΑΚΤΗΣΗ Επαναφορά της βάσης δεδομένων από αντίγραφο ασφαλείας (8 γράμματα)

ΚΑΘΕΤΑ

1 κάθετα: ΔΟΥΡΕΙΟΣΙΠΠΟΣ Κακόβουλο αρχείο μεταμφιεσμένο σε αθώο (13 γράμματα)

2 κάθετα: ΚΡΥΠΤΟΓΡΑΦΗΣΗ Κρυπτογραφικό κλείδωμα αρχείων (13 γράμματα)

4 κάθετα: ΑΠΟΜΟΝΩΣΗ Αποσύνδεση μολυσμένων συστημάτων δικτύου (9 γράμματα)

5 κάθετα: ΚΑΤΑΣΤΡΟΦΗ Σοβαρό περιστατικό διακοπής του συστήματος (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. ΓΥΑΣΟΡΡΦΚΗΗΤΠ — **ΚΡΥΠΤΟΓΡΑΦΗΣΗ**
2. ΟΥΑΧΝΦΨΑΤΟΓΡΙΡ — **ΨΥΧΡΟΑΝΤΙΓΡΑΦΟ**
3. ΤΛΑΡΥ — **ΛΥΤΡΑ**
4. ΤΦΣΗΑΟΡΚΑΤ — **ΚΑΤΑΣΤΡΟΦΗ**
5. ΤΡΟΦΙΟ — **ΦΟΡΤΙΟ**
6. ΣΜΠΩΝΑΟΗΟ — **ΑΠΟΜΟΝΩΣΗ**
7. ΑΗΤΗΣΝΚΑ — **ΑΝΑΚΤΗΣΗ**
8. ΙΥΕΙΠΣΣΔΟΟΟΠΡ — **ΔΟΥΡΕΙΟΣΙΠΠΟΣ**

ΚΛΕΙΔΙ ΠΡΟΚΛΗΣΗΣ ΜΥΣΤΙΚΟΥ ΚΩΔΙΚΑ

"ΕΠΑΝΕΦΕΡΕ ΔΕΔΟΜΕΝΑ ΑΠΟ ΨΥΧΡΟ ΑΝΤΙΓΡΑΦΟ"

Λύσεις των μελετών περίπτωσης

A Μελέτη περίπτωσης 1: Περιορισμός ωφέλιμου φορτίου ransomware σε επιχείρηση

Λύση για τον εκπαιδευτικό

ΟΔΗΓΙΕΣ ΒΑΘΜΟΛΟΓΗΣΗΣ

Οι απαντήσεις των μαθητών πρέπει να καλύπτουν τα εξής σημεία:

- Ανάλυση σεναρίου: Ένα εταιρικό τοπικό δίκτυο έχει παραβιαστεί από ενεργό ransomware. Βασικοί διακομιστές αρχείων έχουν αρχίσει να εμφανίζουν αρχεία με κατάληξη .locked.
- Προτεινόμενη στρατηγική και λύση: Αποσύνδεσε όλους τους επηρεασμένους διακομιστές από το τοπικό δίκτυο (LAN). Τερμάτισε τις ενεργές διαχειριστικές συνεδρίες. Επανάφερε τα μη παραβιασμένα αρχεία από ένα ασφαλές σύστημα αντιγράφων ασφαλείας εκτός σύνδεσης με προστασία εγγραφής.

B Μελέτη περίπτωσης 2: Αξιολόγηση αρχιτεκτονικών αντιγράφων ασφαλείας εκτός δικτύου

Λύση για τον εκπαιδευτικό

ΟΔΗΓΙΕΣ ΒΑΘΜΟΛΟΓΗΣΗΣ

Οι απαντήσεις των μαθητών πρέπει να καλύπτουν τα εξής σημεία:

- Ανάλυση σεναρίου: Μια επιχείρηση θέλει να σχεδιάσει μια στρατηγική αντιγράφων ασφαλείας που μειώνει τον κίνδυνο παραβίασης των αντιγράφων ακόμη και αν το κύριο τοπικό δίκτυο καταληφθεί πλήρως από ransomware.
- Προτεινόμενη στρατηγική και λύση: Εφάρμοσε αποθήκευση εγγραφής-μία-φορά-ανάγνωσης-πολλές (WORM). Δημιούργησε λογικό air-gap αποσυνδέοντας το σύστημα αντιγράφων ασφαλείας από όλα τα δίκτυα και επίβαλε καθημερινή εναλλαγή φυσικών μέσων.