Ενότητα 4 – Τελικό Κουίζ: Διαχείριση Κινδύνων και Πολιτικές Ασφαλείας

1 - Τι σημαίνει «κίνδυνος στον κυβερνοχώρο»;

A) Οποιαδήποτε κατάσταση που βελτιώνει την απόδοση του συστήματος
B) Η πιθανότητα απώλειας ή ζημιάς λόγω απειλών που εκμεταλλεύονται αδυναμίες
C) Προγραμματισμένη ενημέρωση λογισμικού
D) Εναλλακτικό σχέδιο για τα δεδομένα σας

2 - Ποια είναι η βασική διαφορά μεταξύ απειλής και ευπάθειας;

A) Η απειλή είναι αδυναμία· η ευπάθεια είναι εξωτερικός κίνδυνος
B) Η απειλή είναι εξωτερικός κίνδυνος· η ευπάθεια είναι εσωτερική αδυναμία
C) Και οι δύο όροι σημαίνουν το ίδιο
D) Η ευπάθεια πάντα αποτρέπει τον κίνδυνο

3 - Ποιος τύπος περιγράφει καλύτερα την έννοια του κινδύνου;

A) Κίνδυνος = Ευπάθεια × Ταχύτητα Συστήματος
B) Κίνδυνος = Απειλή × Ευπάθεια × Επίπτωση
C) Κίνδυνος = Κρυπτογράφηση ÷ Πιθανότητα
D) Κίνδυνος = Έλεγχος × Ενημέρωση

4 - Γιατί είναι σημαντική η διαχείριση κινδύνων στην κυβερνοασφάλεια;

A) Βοηθά τα συστήματα να λειτουργούν πιο γρήγορα
B) Εξασφαλίζει ότι οι κίνδυνοι εντοπίζονται, αξιολογούνται και αντιμετωπίζονται πριν προκληθεί ζημιά
C) Αντικαθιστά την ανάγκη για λογισμικό προστασίας από ιούς
D) Εγγυάται απόλυτη ασφάλεια

5 - Ποια μέθοδος επικεντρώνεται στη μέτρηση της πιθανότητας και της επίπτωσης με αριθμούς και κόστη;

A) Ποιοτική εκτίμηση κινδύνου
B) Ποσοτική εκτίμηση κινδύνου
C) Μοντελοποίηση απειλών μόνο
D) Υποκειμενική ανάλυση

6 - Ποιο από τα παρακάτω αποτελεί παράδειγμα ποιοτικής εκτίμησης κινδύνου;

A) Εκτίμηση του κόστους διακοπής λειτουργίας σε δολάρια ανά ώρα
B) Κατάταξη κινδύνων ως «Υψηλός, Μεσαίος, Χαμηλός»
C) Υπολογισμός της ετήσιας αναμενόμενης απώλειας (ALE)
D) Εκτέλεση ανάλυσης κόστους-οφέλους

7 - Ποιο από τα παρακάτω αποτελεί πλαίσιο αξιολόγησης κινδύνου;

A) Μοντέλο TCP/IP
B) NIST RMF
C) Πρότυπο WPA3
D) Επίπεδα RAID

8 - Ποιο από αυτά ΔΕΝ είναι τύπος μέτρου ασφαλείας;

A) Προληπτικό
B) Ανιχνευτικό
C) Διορθωτικό
D) Επεκτατικό

9 - Ποιο από τα παρακάτω παραδείγματα αποτυπώνει καλύτερα έναν προληπτικό έλεγχο;

A) Εγκατάσταση τείχους προστασίας για φραγή κακόβουλης κυκλοφορίας
B) Χρήση καταγραφών ανίχνευσης εισβολών
C) Επαναφορά δεδομένων από αντίγραφα ασφαλείας
D) Έλεγχος αναφορών ασφάλειας

10 - Ποιος τύπος ελέγχου περιλαμβάνει τα συστήματα ανίχνευσης εισβολών (IDS);

A) Προληπτικός
B) Ανιχνευτικός
C) Διορθωτικός
D) Διοικητικός

11 - Τι είναι η πολιτική ασφάλειας;

A) Ένα σύνολο οδηγιών που καθορίζουν τη σωστή χρήση, τις ευθύνες και τα μέτρα προστασίας
B) Ένα τεχνικό μέτρο που κρυπτογραφεί τα δεδομένα
C) Ένας κανόνας πρόσβασης μέσω υλικού εξοπλισμού
D) Μια προσωρινή λύση σε περίπτωση περιστατικού

12 - Ποιος είναι συνήθως υπεύθυνος για τη διακυβέρνηση της ασφάλειας;

A) Μόνο οι τελικοί χρήστες
B) Η ανώτερη διοίκηση και τα αρμόδια όργανα διακυβέρνησης
C) Αποκλειστικά οι ομάδες τεχνικής υποστήριξης
D) Εξωτερικοί συνεργάτες

13 - Ποιο από τα παρακάτω ΔΕΝ αποτελεί μέρος του κύκλου ζωής μιας πολιτικής ασφάλειας;

A) Σύνταξη
B) Εφαρμογή
C) Αρχειοθέτηση χωρίς ενημερώσεις
D) Ανασκόπηση και αναθεώρηση

14 - Γιατί είναι σημαντικά τα προγράμματα ευαισθητοποίησης για την ασφάλεια;

A) Η τεχνολογία από μόνη της δεν αρκεί για να αποτρέψει ανθρώπινα λάθη
B) Δεν εξαλείφουν όλα τα phishing περιστατικά
C) Δεν διασφαλίζουν αυτόματα τη συμμόρφωση
D) Είναι προαιρετικά και σπάνια αποδίδουν πραγματικά

15 - Ποιο από τα παρακάτω αποτελεί παράδειγμα μεθόδου εκπαίδευσης για προγράμματα ευαισθητοποίησης;

A) Εικονικές ασκήσεις phishing
B) Εγκατάσταση ισχυρότερων firewalls
C) Ενημέρωση των ενημερώσεων του λειτουργικού
D) Κρυπτογράφηση των email

Εργαστήριο 4.1 – Δημιουργία Μητρώου Κινδύνων

16 - Τι είναι το μητρώο κινδύνων;

A) Ένα αρχείο με κανόνες τείχους προστασίας
B) Ένα οργανωμένο έγγραφο που καταγράφει κινδύνους, πιθανότητα εμφάνισης και επιπτώσεις
C) Ένα σύστημα αποθήκευσης αντιγράφων ασφαλείας
D) Μια βάση δεδομένων για λογισμικό προστασίας από ιούς

17 - Ποια από τις παρακάτω είναι βασική στήλη σε ένα μητρώο κινδύνων;

A) Περιγραφή κινδύνου, πιθανότητα, επίδραση, μέτρα αντιμετώπισης
B) Ικανοποίηση εργαζομένων, εξοικονόμηση κόστους, παραγωγικότητα
C) Μέγεθος γραμματοσειράς, στυλ πίνακα, κανόνες μορφοποίησης
D) Μόνο ποσοστό διαθεσιμότητας διακομιστή

18 - Στο παράδειγμα καταχώρησης κινδύνου, «phishing email», τι το κάνει έγκυρο στοιχείο στο μητρώο κινδύνων;

A) Καταγράφει μόνο το κόστος
B) Συνδέει μια απειλή (phishing) με ευπάθειες και πιθανά αποτελέσματα
C) Αναφέρει μόνο την πιθανότητα
D) Αγνοεί τον ανθρώπινο παράγοντα

19 - Γιατί είναι χρήσιμη η αξιολόγηση του κινδύνου;

A) Αντικαθιστά την ανάγκη για πολιτικές
B) Βοηθά στην ιεράρχηση των κινδύνων που απαιτούν άμεση αντιμετώπιση
C) Κάνει τη διαχείριση κινδύνου προαιρετική
D) Εντοπίζει και εξαλείφει αυτόματα τις ευπάθειες

20 - Ποια από τις παρακάτω αποτελεί στρατηγική χρήση του μητρώου κινδύνων;

A) Ιεράρχηση των κινδύνων για τη διοίκηση και παρακολούθηση της εξέλιξής τους με τον χρόνο
B) Κρυπτογράφηση ευαίσθητων αρχείων
C) Παρακολούθηση της απόδοσης της CPU
D) Εκπαίδευση αποκλειστικά των διαχειριστών συστημάτων

Κλειδιά Απαντήσεων

1. **B** – Ο κυβερνο-κίνδυνος είναι η πιθανότητα ζημιάς όταν απειλές εκμεταλλεύονται ευπάθειες.
2. **B** – Απειλή σημαίνει κίνδυνος· ευπάθεια είναι το αδύναμο σημείο που αξιοποιείται.
3. **B** – Η καθιερωμένη έννοια του κινδύνου στην κυβερνοασφάλεια.
4. **B** – Στόχος είναι η προτεραιοποίηση και μείωση των κινδύνων πριν υπάρξουν περιστατικά.
5. **B** – Η ποσοτική αξιολόγηση βασίζεται σε μετρήσιμα νούμερα και κόστη.
6. **B** – Η ποιοτική βασίζεται σε σχετικές κλίμακες (π.χ. Υψηλό/Μεσαίο/Χαμηλό).
7. **B** – Το NIST RMF είναι ένα πλαίσιο διαχείρισης κινδύνων.
8. **D** – Το “expansive” δεν ανήκει στις κατηγορίες ελέγχου.
9. **A** – Τα firewalls είναι προληπτικά μέτρα.
10. **B** – Το IDS είναι ανιχνευτικός έλεγχος.
11. **A** – Πολιτικές: Γραπτοί κανόνες και προσδοκίες.
12. **B** – Η διακυβέρνηση είναι ευθύνη της ανώτερης διοίκησης.
13. **C** – Η αρχειοθέτηση χωρίς ενημερώσεις δεν ανήκει στον κύκλο ζωής.
14. **A** – Οι άνθρωποι είναι η πρώτη γραμμή άμυνας· η ενημέρωση μειώνει τα ανθρώπινα λάθη.
15. **A** – Η προσομοίωση phishing αποτελεί κλασική μέθοδο εκπαίδευσης.
16. **B** – Το μητρώο κινδύνων είναι οργανωμένη καταγραφή των κινδύνων.
17. **A** – Περιγραφή κινδύνου, πιθανότητα, επίπτωση, έλεγχοι: βασικά πεδία.
18. **B** – Παράδειγμα που συνδέει την απειλή του phishing με ευπάθειες/επιπτώσεις.
19. **B** – Η βαθμολόγηση βοηθά στην κατάταξη και προτεραιοποίηση των κινδύνων.
20. **A** – Το μητρώο χρησιμοποιείται στρατηγικά για προτεραιοποίηση και αναφορές.