Modulo 4 – Quiz finale: Gestione dei rischi e politiche di sicurezza

1 - Cosa significa "rischio di sicurezza informatica"?

A) Qualsiasi situazione che migliora le prestazioni del sistema
B) Il potenziale di perdita o danno dovuto a minacce che sfruttano le vulnerabilità
C) Una patch software programmata
D) Un piano di backup dei dati

2 - Quale delle seguenti definizioni descrive meglio la differenza tra una minaccia e una vulnerabilità?

A) Una minaccia è un punto debole; una vulnerabilità è un pericolo esterno
B) Una minaccia è un pericolo esterno; una vulnerabilità è un punto debole interno
C) Entrambi i termini hanno lo stesso significato
D) Una vulnerabilità impedisce sempre il rischio

3 - Quale formula descrive meglio il concetto di rischio?

A) Rischio = Vulnerabilità × Velocità del sistema
B) Rischio = Minaccia × Vulnerabilità × Impatto
C) Rischio = Crittografia ÷ Probabilità
D) Rischio = Controllo × Consapevolezza

4 - Perché la gestione del rischio è importante nella sicurezza informatica?

A) Rende i sistemi più veloci
B) Assicura che i rischi vengano identificati, classificati in ordine di priorità e mitigati prima che si verifichino danni
C) Sostituisce la necessità di software antivirus
D) Garantisce la sicurezza al 100%

5 - Quale metodo si concentra sulla misurazione della probabilità e dell'impatto con numeri e costi?

A) Valutazione qualitativa del rischio
B) Valutazione quantitativa del rischio
C) Solo modellizzazione delle minacce
D) Analisi soggettiva

6 - Qual è un esempio di valutazione qualitativa del rischio?

A) Stima dei tempi di inattività in dollari all'ora
B) Classificazione dei rischi come "Alto, Medio, Basso"
C) Calcolo della perdita attesa annualizzata (ALE)
D) Esecuzione di un'analisi costi-benefici

7 - Quale dei seguenti è un quadro di valutazione del rischio?

A) Modello TCP/IP
B) NIST RMF
C) Standard WPA3
D) Livelli RAID

8 - Quale di questi NON è un tipo di controllo di sicurezza?

A) Preventivo
B) Investigativo
C) Correttivo
D) Espansivo

6 - Quale esempio rappresenta meglio un controllo preventivo?

A) Installazione di un firewall per bloccare il traffico dannoso
B) Utilizzo dei registri di rilevamento delle intrusioni
C) Ripristino dei dati dai backup
D) Revisione dei rapporti di audit di sicurezza

10 - Quale tipo di controllo include i sistemi di rilevamento delle intrusioni (IDS)?

A) Preventivo
B) Investigativo
C) Correttivo
D) Amministrativo

11 - Che cos'è una politica di sicurezza?

A) Una serie di linee guida che definiscono l'uso accettabile, le responsabilità e le protezioni
B) Un controllo tecnico che crittografa il traffico
C) Una regola di accesso basata sull'hardware
D) Una soluzione temporanea durante un incidente

12 - Chi è solitamente responsabile della governance della sicurezza?

A) Solo gli utenti finali
B) Il senior management e gli organismi di governance designati
C) Solo i team di supporto tecnico
D) Appaltatori terzi

13 - Cosa NON fa parte del ciclo di vita della politica di sicurezza?

A) Redazione
B) Applicazione
C) Archiviazione senza aggiornamenti
D) Revisione e modifica

14 - Perché i programmi di sensibilizzazione alla sicurezza sono importanti?

A) La tecnologia da sola non può risolvere gli errori umani
B) Eliminano tutti gli attacchi di phishing
C) Garantiscono automaticamente la conformità
D) Sono facoltativi e raramente efficaci

15 - Qual è un esempio di metodo di formazione per i programmi di sensibilizzazione?

A) Esercizi di phishing simulato
B) Installazione di firewall più potenti
C) Aggiornamento delle patch del sistema operativo
D) Crittografia delle e-mail

Laboratorio 4.1 – Creazione di un registro dei rischi

16 - Che cos'è un registro dei rischi?

A) Un registro delle regole del firewall
B) Un documento strutturato che tiene traccia dei rischi, della probabilità e dell'impatto
C) Un sistema di archiviazione di backup
D) Un database antivirus

17 - Quale delle seguenti voci è una colonna fondamentale in un registro dei rischi?

A) Descrizione del rischio, probabilità, impatto, controlli
B) Soddisfazione dei dipendenti, risparmio sui costi, produttività
C) Dimensione dei caratteri, stile delle tabelle, regole di formattazione
D) Solo percentuale di uptime del server

18 - Nell'esempio di voce di rischio "e-mail di phishing", cosa rende questa voce valida nel registro dei rischi?

A) Tiene traccia solo dei costi
B) Collega una minaccia (phishing) alle vulnerabilità e ai possibili impatti
C) Elenca solo la probabilità
D) Ignora i fattori umani

16 - Perché è utile valutare il rischio?

A) Sostituisce la necessità di politiche
B) Dà priorità ai rischi che richiedono un intervento urgente
C) Rende la gestione dei rischi facoltativa
D) Elimina automaticamente le vulnerabilità

20 - Quale delle seguenti è un'applicazione strategica di un registro dei rischi?

A) Dare priorità ai rischi per la leadership e monitorare i cambiamenti nel tempo
B) Crittografare i file sensibili
C) Monitorare le prestazioni della CPU
D) Formare solo gli amministratori di sistema

Risposte

1. **B** – Rischio informatico = potenziale danno quando le minacce sfruttano le vulnerabilità.
2. **B** – Minaccia = pericolo; vulnerabilità = debolezza sfruttata.
3. **B** – Definizione standard di rischio nella sicurezza informatica.
4. **B** – L'obiettivo è dare priorità/mitigare i rischi prima che si verifichino incidenti.
5. **B** – L'approccio quantitativo utilizza numeri misurabili e costi.
6. **B** – Il metodo qualitativo utilizza scale relative (ad esempio, Alto/Medio/Basso).
7. **B** – NIST RMF è un quadro di riferimento per la gestione dei rischi.
8. **D** – Espansivo non è una categoria di controllo.
9. **A** – I firewall sono preventivi.
10. **B** – IDS = controllo investigativo.
11. **A** – Politiche = regole e aspettative scritte.
12. **B** – La governance è una responsabilità dell'alta dirigenza.
13. **C** – L'archiviazione senza aggiornamenti non fa parte del ciclo di vita.
14. **A** – Le persone sono la prima linea; la consapevolezza riduce l'errore umano.
15. **A** – Il phishing simulato è un metodo di formazione classico.
16. **B** – Registro dei rischi = monitoraggio strutturato dei rischi.
17. **A** – Descrizione del rischio, probabilità, impatto e controlli sono campi fondamentali.
18. **B** – L'esempio collega la minaccia di phishing alle vulnerabilità/all'impatto.
19. **B** – Il punteggio aiuta a classificare/dare priorità ai rischi.
20. **A** – Il registro viene utilizzato strategicamente per la rendicontazione delle priorità C.