Přijímací test vzor

Správná je vždy jen jedna z nabízených možností.

Okruh 1: Základy kybernetické bezpečnosti

1. **Co je kybernetická bezpečnost?**
   a) Ochrana počítačových systémů před přírodními katastrofami
   b) Ochrana počítačových systémů a sítí před útoky a zneužitím
   c) Ochrana osobních údajů na internetu
   d) Ochrana proti poruchám hardware

2. **Který z následujících nástrojů slouží k detekci a prevenci útoků na síť?**
   a) Antivirus
   b) Firewall
   c) Webový prohlížeč
   d) Operativní systém

3. **Co je phishing?**
   a) Proces šifrování dat
   b) Případ, kdy útočník podvodně získává citlivé informace tím, že se vydává za důvěryhodnou osobu nebo organizaci
   c) Automatické šíření škodlivého softwaru
   d) Ochrana proti kybernetickým útokům

4. **Co je to malware?**
   a) Program pro šifrování dat
   b) Škodlivý software, který se používá k poškození systému nebo krádeži dat
   c) Nástroj pro optimalizaci systému
   d) Bezpečnostní protokol pro ochranu sítí

5. **Co znamená pojem DDoS (Distributed Denial of Service)?**
   a) Útok na server s cílem zahlcení a zamezení přístupu k němu
   b) Útok na mobilní zařízení
   c) Nelegální přístup do uživatelského účtu
   d) Šifrování dat pro jejich bezpečné přenosy

1b, 2b, 3b, 4b, 5a

Okruh 2: Sítě a jejich bezpečnost

1. **Co je VPN?**
   a) Technologie, která umožňuje šifrovanou komunikaci mezi počítači v síti
   b) Typ firewallu pro domácí použití
   c) Software pro šifrování emailů
   d) Program pro detekci virusů v síti

2. **Který z následujících protokolů je nejčastěji používán pro zabezpečený přenos dat na internetu?**
   a) FTP
   b) HTTP
   c) HTTPS
   d) SMTP

3. **Jaký je účel firewalu?**
   a) Ochrana proti virům
   b) Filtrace síťového provozu a blokování neautorizovaného přístupu
   c) Zabezpečení šifrování dat při přenosu
   d) Správa IP adres

4. **Co je to Man-in-the-Middle útok?**
   a) Útok, kdy útočník odposlouchává a případně modifikuje komunikaci mezi dvěma stranami
   b) Útok na konkrétní software s cílem poškodit jeho funkce
   c) Útok zaměřený na přístup k databázím
   d) Útok na přihlašovací údaje uživatele

5. **Co je to SSL/TLS?**
   a) Metoda šifrování pro ochranu dat při přenosu
   b) Síťová technologie pro připojení k internetu
   c) Typ firewallu
   d) Metoda pro autentizaci uživatelů

1a, 2c, 3b, 4a, 5a

Okruh 3: Kryptografie

1. **Co je to asymetrická kryptografie?**
   a) Šifrování, které používá jeden klíč pro šifrování i dešifrování
   b) Šifrování, které používá veřejný a soukromý klíč pro šifrování a dešifrování
   c) Šifrování, které nevyžaduje žádné klíče
   d) Šifrování, které je používáno pouze pro šifrování textových zpráv

2. **Co je to hashování?**
   a) Proces šifrování dat s cílem jejich ochrany před odcizením
   b) Proces generování otisku (hash kódu) z dat, který je jedinečný pro každý vstupní soubor
   c) Proces dešifrování zašifrovaných dat
   d) Proces komprese dat

3. **Co je to digitální podpis?**
   a) Forma šifrování pro ochranu osobních údajů
   b) Kód používaný k ověření pravosti a integrity dat
   c) Způsob ochrany před phishingem
   d) Metoda pro odstranění škodlivého softwaru

4. **Jaký je hlavní účel veřejného klíče v kryptografii?**
   a) Slouží k šifrování dat, která mohou být dešifrována pouze soukromým klíčem
   b) Slouží k dešifrování zašifrovaných dat
   c) Slouží k ochraně proti DDoS útokům
   d) Slouží k ověřování pravosti dat

5. **Co je to šifrování end-to-end?**
   a) Šifrování, které se používá při komunikaci pouze v rámci jedné sítě
   b) Šifrování, při kterém je přenos dat zajištěn proti odposlechu správcem komunikačního kanálu i správcem serveru
   c) Šifrování, které chrání data pouze na serveru
   d) Šifrování, které se provádí pouze na souborových serverech

1b, 2b, 3b, 4a, 5b

Okruh 4: Bezpečnostní incidenty a reakce

1. **Co je to incident kybernetické bezpečnosti?**
   a) Jakýkoli neúmyslný výpadek systému
   b) Jakákoli událost, která může ohrozit bezpečnost informačních systémů
   c) Případ, kdy systém přestane fungovat správně kvůli poruše hardware
   d) Případ, kdy software nefunguje podle očekávání

2. **Co je to forenzní analýza v kybernetické bezpečnosti?**
   a) Analýza provozních nákladů kybernetických systémů
   b) Proces, který zahrnuje analýzu a vyšetřování kybernetických útoků pro určení jejich zdroje
   c) Metoda pro šifrování komunikace
   d) Proces testování operačních systémů pro detekci zranitelností

3. **Co by měla obsahovat plán reakce na kybernetické incidenty?**
   a) Seznam všech uživatelů systému
   b) Pokyny pro identifikaci, reakci, obnovu a prevenci incidentů kybernetické bezpečnosti
   c) Seznam dostupných softwarových nástrojů
   d) Historii všech předchozích útoků

4. **Co je to Ransomware?**
   a) Software pro ochranu proti virům
   b) Software pro zálohování dat
   c) Software pro optimalizaci výkonu systému
   d) Software, který šifruje data a požaduje výkupné za jejich dešifrování

5. **Jaké je hlavní pravidlo pro správu přístupových práv v kybernetické bezpečnosti?**
   a) Poskytnout všem uživatelům stejné úrovně přístupu
   b) Omezit přístup na základě principu nejmenších práv
   c) Dát plný přístup administrátorům
   d) Umožnit přístup všem uživatelům k citlivým datům pro zajištění flexibilního přístupu

1b, 2b, 3b, 4d, 5b