Provkonstruktion

Årskurs: Gymnasiet

Ämne: Datorsamordning och support

Tema: Säkerhet och dataskydd

Syfte

Syftet med provet är att bedöma elevernas kunskaper och förståelse för säkerhetshot och metoder för dataskydd inom IT-miljöer. Provets utformning syftar till att ge eleverna möjlighet att visa sin förmåga att identifiera och diskutera viktiga aspekter av dataskydd och säkerhetsåtgärder.

Koppling till styrdokument

Centralt innehåll

Denna lektion handlar om säkerhet och skydd av data inom IT-system och nätverk. Eleverna kommer att lära sig om olika typer av säkerhetshot, strategier för att skydda data och vikten av att upprätthålla säkerhetsstandarder.

Kunskapskrav

Eleverna ska kunna identifiera säkerhetshot, förstå metoder för dataskydd och diskutera vikten av att implementera säkerhetsåtgärder i IT-miljöer.

Prov

Faktafrågor

1. Vad är ett säkerhetshot?

A) En metod för dataskydd

B) Ett angrepp mot information

C) En potentiell fara för data

D) En databehandlingsmetod

2. Vilken typ av programvara används för att skydda datorer mot virus?

A) Brandvägg

B) Antivirusprogram

C) Krypteringsprogram

D) Operativsystem

3. Vad står förkortningen ‘DDoS’ för?

A) Digital Distribution of Service

B) Data Denial of Service

C) Distributed Denial of Service

D) Direct Data Operation System

4. Vad är syftet med kryptering?

A) Att öka dataöverföringshastigheten

B) Att skydda data genom kodning

C) Att skapa säkerhetskopior

D) Att skanna efter virus

5. Vad innebär social ingenjörskonst?

A) Att manipulera människor för att få dem att avslöja information

B) En metod för att skydda data

C) En teknik för att analysera dataöverträdelser

D) En typ av kryptering

6. Vilken åtgärd är nödvändig för att återställa data efter en attack?

A) Kryptering

B) Brandväggar

C) Säkerhetskopiering

D) Programuppdateringar

7. Vad är en brandvägg?

A) Ett hårdvaruverktyg för dataåterställning

B) En programvara som skyddar mot obehörig åtkomst

C) En typ av antivirusprogram

D) En metod att kryptera data

8. Vad innebär phishing?

A) Att lura användare att avslöja känslig information

B) Att installera antivirusprogram

C) Att kryptera data

D) Att skapa säkerhetskopior

9. Hur kan en organisation förebygga insiderhot?

A) Genom att öka lagringsutrymmet

B) Genom att utbilda medarbetare om säkerhetsrisker

C) Genom att skaffa fler servrar

D) Genom att installera fler programvaror

10. Vilken lag gäller för dataskydd inom EU?

A) GDPR

B) Dataskyddsförordningen

C) IT-säkerhetslagen

D) Personuppgiftslagen

11. Vad är syftet med en säkerhetsplan?

A) Att utöka nätverkets kapacitet

B) Att identifiera hot och skyddsåtgärder

C) Att öka datalagring

D) Att skapa programvaror

12. Vilken typ av attack innebär att överbelasta en tjänst med trafik?

A) Malware

B) DoS-attack

C) Ransomware

D) Phishing

13. Vad är en informationssäkerhetspolicy?

A) En programvara för dataskydd

B) En uppsättning av riktlinjer för att skydda information

C) En typ av databas

D) En lag för dataskydd

14. Vad innebär tvåfaktorsautentisering?

A) En metod för att kryptera data

B) En säkerhetsåtgärd som kräver två typer av verifiering

C) En typ av virusprogram

D) En rapport om säkerhetshot

15. Hur kan regelbundna programuppdateringar bidra till dataskydd?

A) Genom att öka lagringsutrymmet

B) Genom att skydda mot nya säkerhetshot

C) Genom att skapa säkerhetskopior

D) Genom att förbättra nätverkshastigheten

Resonerande frågor

1. Diskutera vikten av dataskydd inom en organisation och hur det kan påverka förtroendet hos kunder och anställda. Frågan syftar till att få eleverna att reflektera över de praktiska konsekvenserna av bristande dataskydd.

2. Hur kan ett företag förbättra sin säkerhetspolicy för att skydda känslig information? Frågan ger eleverna möjlighet att föreslå konkreta åtgärder och visa sin förståelse för säkerhetsstrategier.

3. Analysera en aktuell dataöverträdelse och diskutera dess konsekvenser för de drabbade. Denna fråga uppmanar eleverna att koppla teori till praktiska exempel.

4. Vilka metoder kan användas för att utbilda personal om IT-säkerhet och varför är detta viktigt? Eleverna förväntas resonera kring utbildningens roll i säkerhetsarbetet.

5. Reflektera över skillnaderna mellan olika typer av säkerhetshot och hur dessa kan hanteras. Eleverna kan visa djup förståelse för ämnet genom att jämföra olika hot.

6. Hur påverkar lagar och förordningar, som GDPR, hur företag hanterar dataskydd? Denna fråga uppmanar eleverna att tänka kritiskt kring juridiska aspekter av dataskydd.

7. Diskutera hur digitaliseringen påverkar behovet av dataskydd. Frågan ger en möjlighet att knyta an ämnet till samtida utvecklingar.

8. Hur kan teknik, som AI och maskininlärning, användas för att förbättra säkerheten? Eleverna kan visa kreativitet och nyfikenhet i sina svar.

Bedömning

Faktafrågor: Varje korrekt svar ger 1 poäng, totalt 15 poäng möjliga.

Resonerande frågor: Varje fråga bedöms upp till 3 poäng, totalt 24 poäng möjliga.

För betyg E krävs sammanlagt minst 8 poäng. För betyg C krävs minst 12 poäng (varav minst 3 poäng från resonerande frågor). För betyg A krävs minst 18 poäng (varav minst 5 poäng från resonerande frågor).

Tags: Prov