Länk till Lektion. Gy. Datorteknik 1a – Säkerhet och dataskydd

Provkonstruktion

Årskurs: Gymnasiet
Ämne: Datorteknik 1a
Tema: Säkerhet och dataskydd

Syfte

Syftet med provet är att bedöma elevernas förståelse för säkerhet och dataskydd inom IT-system och nätverk, samt deras förmåga att identifiera hot och föreslå skyddande åtgärder.

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. Vilket av följande är en typ av säkerhetshot?
A) Malware
B) Server
C) Dataöverföring
D) Applikationer
Rätt svar: A)
2. Vad är syftet med kryptering?
A) Att öka hastigheten på datatransfer
B) Att skjuta upp dataöverföring
C) Att skydda data från obehörig åtkomst
D) Att göra data mer tillgängligt
Rätt svar: C)
3. Vilken metod används för att skydda en dator från virus?
A) Antivirusprogram
B) Brandväggar

C) Kryptering
D) Säkerhetskopiering
Rätt svar: A)
4. Vilket hot kategoriseras som en DDoS-attack?
A) En typ av malware
B) Otillbörlig åtkomst till data
C) Överbelastning av en server
D) Förlust av data genom sabotage
Rätt svar: C)
5. GDPR står för?
A) General Data Protection Regulation
B) Global Data Protection Regulation
C) General Digital Protection Regulation
D) Global Digital Protection Regulation
Rätt svar: A)
6. Vilken av följande är en säkerhetsåtgärd för dataskydd?
A) Delning av lösenord
B) Användning av svaga lösenord
C) Regelbundna säkerhetskopior
D) Öppen Wi-Fi-åtkomst
Rätt svar: C)
7. Vad innebär phishing?
A) En metod för att styra datorn på avstånd
B) Bedräglig insamling av känslig information
C) Överanvändning av bandbredd
D) Återställande av förlorad information
Rätt svar: B)
8. Vad syftar en brandvägg till?
A) Att dela data
B) Att mäta dataflöden
C) Att skydda nätverk från obehörig åtkomst
D) Att förstärka signaler
Rätt svar: C)
9. En trojan arbetar genom att:
A) Låsa data
B) Dölja sig som legitim programvara
C) Slanda datorns resurser
D) Bryta mot lagar
Rätt svar: B)
10. Vilken av följande åtgärder bidrar inte till dataskydd?
A) Användning av starka lösenord
B) Lämna datorn obevakad
C) Aktivera tvåfaktorsautentisering
D) Regelbundna programuppdateringar
Rätt svar: B)
11. Vilken typ av skydd är mest effektiv mot ransomware?
A) Antivirusprogram
B) Brandvägg

C) Säkerhetskopiering
D) Kryptering
Rätt svar: C)
12. Insiderhot kan komma från:
A) Utomstående hackare
B) Företagets egna anställda
C) Offentliga myndigheter
D) Företagsleverantörer
Rätt svar: B)
13. Vilken av följande riktlinjer bör följas för att förbättra cybersäkerhet?
A) Användning av samma lösenord för flera konton
B) Uppdatera programvara regelbundet
C) Lämna information offentligt tillgänglig
D) Använda svaga lösenord
Rätt svar: B)
14. Vad står förkortningen DDoS för?
A) Direct Denial of Service
B) Distributed Denial of Service
C) Digital Denial of Service
D) Data Denial of Service
Rätt svar: B)
15. Ett exempel på en metod för att öka medvetenheten om IT-säkerhet är:
A) Användarutbildning
B) Ingen utbildning
C) Delning av interna dokument
D) Hårdvaruinköp
Rätt svar: A)

Resonerande frågor

1. Diskutera hur en säkerhetsplan kan bidra till att skydda en organisation mot säkerhetshot.
Syftet är att eleverna ska visa en djup förståelse för vikten av säkerhetsplanering.
2. Hur påverkar GDPR företag och deras säkerhetsstrategier?
Syftet är att eleverna ska reflektera över lagstiftningens inverkan på verksamheter.
3. Analysera konsekvenserna av en dataintrång för ett företag.
Syftet är att ge eleverna möjlighet att diskutera ekonomiska, juridiska och sociala effekter.
4. Vilka metoder kan organisationer använda för att utbilda sina anställda i IT-säkerhet?
Syftet är att eleverna ska identifiera effektiva utbildningsstrategier.
5. Beskriv hur teknologiska framsteg kan både förbättra och försvåra IT-säkerheten.
Syftet är att eleverna ska reflektera över dubbelheten i teknologiska framsteg.
6. Vilka steg bör vidtas för att hantera en säkerhetsincident?
Syftet är att eleverna ska analysera viktig beredskap och respons.
7. Diskutera vikten av att ha en incidenthanteringsplan.
Syftet är att eleverna ska förstå hur planering kan påverka krishantering.
8. Reflektera över etiska frågor som rör dataskydd och integritet.
Syftet är att ge eleverna möjlighet att diskutera moraliska aspekter av dataskydd.

Bedömning

Faktafrågorna ger totalt 30 poäng, varje fråga ger 2 poäng. Resonerande frågor ger totalt 40 poäng, varje fråga ger 5 poäng. För betyget E krävs totalt minst 8 poäng, för betyget C minst 12 poäng (inklusive minst 3 från resonerande frågor), och för betyget A minst 18 poäng (inklusive minst 5 från resonerande frågor).