Provkonstruktion

Årskurs: Gymnasiet

Ämne: Digital kommunikationsteknik

Tema: Nätverkssäkerhet

Syfte

Syftet med provet är att bedöma elevernas kunskap och förståelse för grundläggande koncept inom nätverkssäkerhet, inklusive säkerhetshot och försvarsåtgärder, samt deras förmåga att diskutera och analysera dessa i praktiska sammanhang.

Koppling till styrdokument

Centralt innehåll

Denna lektion fokuserar på grunderna i nätverkssäkerhet, inklusive vanliga hot mot nätverksinfrastruktur och metoder för att skydda data och system. Eleverna får en översikt över säkerhetsprinciper och bästa praxis.

Kunskapskrav

Eleverna ska kunna beskriva vanliga säkerhetshot, förstå grundläggande säkerhetsåtgärder och diskutera metoder för att skydda nätverksinfrastruktur och data.

Prov

Faktafrågor

1. Vad innebär nätverkssäkerhet?
A. Skydd av nätverksinfrastruktur och data från obehörig åtkomst och attacker.
B. Att installera flera datorer i ett nätverk.
C. Att öka hastigheten på internetuppkoppling.
D. Att designa visuella element för en webbplats.

2. Vilket av följande är en form av skadlig programvara?
A. Brandvägg
B. Virus

C. Router
D. Modem

3. Vad är phishing?
A. En metod för att ta bort virus från system.
B. En metod för att lura användare att avslöja personlig information.
C. En typ av hårdvara som används för att skydda nätverk.
D. Ett sätt att förbättra internetanslutningens hastighet.

4. Vilken åtgärd kan hjälpa till att skydda mot DDoS-attacker?
A. Använda en VPN.
B. Skriva mer kod.
C. Öka bandbredden på ditt internetabonnemang.
D. Installera ett antivirusprogram.

5. Vilken av följande är en säkerhetsåtgärd?
A. Att ha flera användarkonton med olika lösenord.
B. Att lämna brandväggen avstängd.
C. Att skicka känsliga uppgifter via osäker e-post.
D. Att lita på alla länkar i mejl du mottar.

6. Vad gör en brandvägg?
A. Fungerar som en skyddande barriär mellan interna nätverk och externa hot.
B. Förbättrar datorns hastighet.
C. Ökar lagringsutrymme för filer.
D. Ger tillgång till internet.

7. Hur kan antivirusprogram skydda nätverk?
A. Genom att öka hastigheten på nätverksanslutning.
B. Genom att identifiera och eliminera skadlig programvara.
C. Genom att blockera alla typer av internetåtkomst.
D. Genom att kräva flera användarkonton.

8. Vilket hot kan leda till informationsstöld?
A. DDoS-attacker.
B. Virus.
C. Phishing.
D. Brandväggar.

9. Vad är tvåfaktorsautentisering?
A. Att ha två olika lösenord för samma konto.
B. Ett sätt att öka säkerheten genom att kräva två former av identifiering.
C. En typ av försvar mot DDoS-attacker.
D. Att ha två av varje typ av säkerhetsprogram installerat.

10. Vilka av följande är konsekvenser av säkerhetsöverträdelser?
A. Förbättrat rykte.
B. Ekonomiska förluster och påverkan på företagsanslutningar.
C. Ökad användartrohet.
D. Förbättrad nätverkslikviditet.

11. Vilket är ett exempel på ett säkerhetshot?
A. Förbättrade brandväggar.
B. Kryptering.
C. Skadlig programvara.
D. Starka lösenord.

12. Vad gör en VPN?
A. Förbättrar ljudkvalitet under samtal.
B. Kryptar och skyddar internetanslutning.
C. Ökar hastigheten på arbetsstationer.
D. Blockerar oförenlig programvara.

13. Vilken åtgärd minskar risken för intrång?
A. Att dela sitt lösenord med vänner.
B. Att använda starka och unika lösenord.
C. Att alltid klicka på alla länkar i mejl.
D. Att inte uppdatera programvara.

14. Vad är en konsekvens av en DDoS-attack?
A. Ökad hastighet på webbsidan.
B. Oanvändbar webbplats eller tjänst.
C. Förbättrad säkerhet.
D. Ökad lagringskapacitet.

15. Vilka är de bästa metoderna för att skydda nätverksinfrastruktur?
A. Att ignorera säkerhetsuppdateringar.
B. Att utbilda användare i säkerhetsmedvetenhet och installera säkerhetsåtgärder.
C. Att lita på att programvaran inte har några sårbarheter.
D. Att inte använda pålitliga källor.

Resonerande frågor

1. Diskutera varför nätverkssäkerhet är avgörande i dagens samhälle.
Denna fråga ger eleverna möjlighet att analysera och förklara betydelsen av nätverkssäkerhet i ett digitaliserat samhälle.

2. Reflektera över hur ett säkerhetsintrång kan påverka ett företag ekonomiskt och socialt.
Denna fråga uppmanar eleverna att koppla teoretiska kunskaper till

praktiska konsekvenser i verksamheter.

3. Analysera skillnaderna mellan olika typer av säkerhetshot.
Denna fråga ger eleverna möjlighet att tydligt redovisa och jämföra olika säkerhetshot och deras effekter.

4. Diskutera hur användarbeteende påverkar nätverkssäkerheten.
Eleverna får möjlighet att reflektera över hur individuella beslut kan påverka säkerheten i nätverket.

5. Skapa en strategi för att hantera ett säkerhetsintrång.
Denna fråga låter eleverna visa sin förståelse för krishantering inom nätverksmiljöer.

6. Analysera hur teknologi såsom kryptering ökar säkerheten i nätverk.
Eleverna får möjligheten att förklara specifika teknologiska åtgärder och deras fördelar.

7. Diskutera etiska aspekter av hacking och dataskydd.
Denna fråga ger eleverna utrymme att utforska komplicerade etiska dilemman inom området nätverkssäkerhet.

8. Reflektera över forskningsrön om framtida säkerhetshot.
Eleverna utmanas att tänka framåt och identifiera potentiella hot baserat på nuvarande trender och teknologi.

Bedömning

Faktafrågorna bedöms med 1 poäng per korrekt svar. Resonerande frågor bedöms med mellan 1-3 poäng beroende på djup och kvalitet i svaret.

För betyg E krävs totalt 8 poäng, för betyg C krävs totalt 12 poäng (minst 3 poäng från resonerande frågor), och för betyg A krävs totalt 18 poäng (minst 5 poäng från resonerande frågor).

Tags: Digital kommunikationsteknik, Gymnasiet