Läxa i Digital Teknik – Datasäkerhet: Principer och Metoder

Redogörelse:
Årskurs: Gymnasiet
Ämne: Digital Teknik
Tema: Datasäkerhet: Principer och Metoder

Ordkollen

Här listas tio ämnesord på läxans tema som är bra att känna till betydelsen av.

1. **Kryptering:** En metod för att skydda data genom att omvandla den till en kod som endast kan avläsas med rätt nyckel.
2. **Firewall (Brandvägg):** En säkerhetsanordning som övervakar och kontrollerar inkommande och utgående nätverkstrafik baserat på säkerhetsregler.
3. **Malware:** Skadlig programvara som är designad för att infiltrera, skada eller störa datorer och nätverk.
4. **Phishing:** En bedräglig metod där angripare försöker lura individer att avslöja känslig information genom falska kommunikationer.
5. **Autentisering:** Processen att verifiera en användares identitet innan åtkomst till system eller data ges.
6. **VPN (Virtual Private Network):** En tjänst som skapar en säker och krypterad anslutning över ett mindre säkert nätverk, som internet.
7. **Dataskyddsförordningen (GDPR):** EU-lagstiftning som reglerar insamling, lagring och behandling av personuppgifter.
8. **Backup:** En kopia av data som görs för att kunna återställas vid dataförlust eller systemfel.
9. **Intrångsdetektering:** System eller metoder som används för att identifiera obehöriga åtkomstförsök till nätverk eller system.
10. **Sårbarhet:** En svaghet i ett system som kan utnyttjas av angripare för att få obehörig åtkomst eller orsaka skada.

Instuderingsfrågor

1. Vad innebär begreppet "kryptering" och varför är det viktigt för datasäkerheten?
2. Förklara hur en brandvägg fungerar och ge ett exempel på dess användning.
3. Vad är skillnaden mellan malware och adware?

4. Beskriv vad phishing är och hur man kan skydda sig mot det.
5. Varför är autentisering en kritisk del av datasäkerhet?
6. Hur bidrar VPN-tjänster till ökad datasäkerhet för användare?
7. Vad reglerar GDPR och vilken betydelse har det för företag?
8. Varför är det viktigt att regelbundet ta backup på sina data?
9. Förklara vad intrångsdetektering innebär och ge ett exempel på en sådan teknik.
10. Ge ett exempel på en sårbarhet i ett informationssystem och hur den kan åtgärdas.

Övning

Nedan listas uppgifter och fyra svarsalternativ. Du ska ringa in det alternativ som är korrekt. Observera att av de fyra alternativen är endast ett korrekt.

Uppgift	A	B	C	D
1. Vad står VPN för?	Virtual Public Network	Virtual Private Network	Verified Personal Network	Virtual Protected Network
2. Vilket av följande är en form av malware?	Firewall	Antivirus	Ransomware	VPN
3. Vad är syftet med kryptering?	Att öka internetanslutningens hastighet	Att skydda data genom att göra den oläslig	Att organisera filer på en dator	Att optimera datorns prestanda
4. Vilken lagstiftning reglerar personuppgifter inom EU?	HIPAA	GDPR	CCPA	SOX
5. Vilken teknik används för att upptäcka obehöriga inloggningsförsök?	Firewall	Intrångsdetekteringssystem	Backup program	Krypteringsprogram
6. Vad är phishing främst inriktat på?	Att infektera datorer med virus	Att lura individer att avslöja känslig data	Att skapa säkerhetskopior av data	Att optimera nätverkshastigheten
7. Vilken av följande är en typ av autentisering?	Lösenord	Firewall	Malware	Backup
8. Vad innebär termen "sårbarhet" inom datasäkerhet?	En svaghet i ett system som kan utnyttjas	En stark säkerhetsfunktion	En typ av backup-lösning	En krypteringsmetod
9. Vilken komponent är central i ett brandväggssystem?	Operativsystem	Regler som styr trafiken	Antivirusprogram	Användarautentisering
10. Vad är en backup?	En krypteringsnyckel	En säkerhetskopierad kopia av data	Ett antivirusprogram	En typ av brandvägg

---

Skrivuppgifter

Här presenteras tre olika skrivuppgifter som är utformade på tre olika svårighetsnivåer: enkel, medel och svår.

Skrivuppgift 1: Förklara Kryptering

Beskriv vad kryptering är och ge exempel på hur det används i vardagen för att skydda information.
Svarslängd: ca. 200 ord (En halv sida)

Skrivuppgift 2: Analysera ett Datasäkerhetsincident

Välj en verklig händelse där datasäkerheten bröts (t.ex. en dataintrång eller ett phishing-attentat). Beskriv vad som hände, vilka konsekvenser det fick och vilka åtgärder som vidtogs för att åtgärda situationen.
Svarslängd: ca. 400 ord (En och en halv sida)

Skrivuppgift 3: Utforma en Datasäkerhetspolicy för en Skola

Skola X vill förbättra sin datasäkerhet och behöver en ny policy. Beskriv de viktigaste delarna som bör ingå i denna policy, inklusive autentisering, backup, och utbildning av personal och elever. Motivera dina val och förklara hur de bidrar till en säkrare digital miljö.
Svarslängd: ca. 600 ord (Två och en halv sida)

Tags: Läxa