Namn: _____ Datum: _____ Poäng: _____

# Dataskydd och lagring i företagsmiljö Säkerhetsguide

Datamaskering, tokenisering, kryptering i vila jämfört med under överföring, offlinesäkerhetskopior

## LÄRÖVERSIKT: DATASKYDD

**SÄKRAD**
**DATAKRYPTERING**
256-bitars AES-standard

**EFTERLEVANDE**
**GLOBALA STANDARDER**
Ramverken GDPR och CCPA

**ZERO TRUST**
**ÅTKOMSTPOLICY**
Multifaktorautentisering

**Välkommen!** Det här aktivitetshäftet guidar dig genom dataskyddsstandarder och kontroller. Du utforskar fullständig diskkryptering, säkra åtkomstkontroller, maskinvarubaserade säkerhetskopior, säkerhetsläge i molnet och tekniker för datamaskering.

**KONTROLLPUNKTER I ARBETSBLADET**

- [ ] **Del 1-4: Behärska cybersäkerhet och hothantering.**
- [ ] **Del 5-7: Lös korsord och ordsökare.**
- [ ] **Del 8-9: Lös fallstudier och chifferutmaning.**
- [ ] **Del 10: Gå igenom sidorna med grundläggande och avancerade vanliga frågor.**
- [ ] **Del 11: Utforska 10 intressanta fakta från verkligheten.**
- [ ] **Bonus: utmaningen Tänk snabbt.**

**Öppna VPN.com:s guide om cybersäkerhet**

URL: https://www.vpn.com/sv/cybersakerhet/dataskydd/

# Din inlärningsplan för strategi för dataskydd

- Skilj mellan teknikerna datamaskering och tokenisering.
- Inför kryptering i vila för lagringsenheter och kryptering under överföring med TLS.
- Utforma säkerhetskopieringssystem offline och nätverksisolerade som skydd mot utpressningsprogram.

### ANVISNINGAR FÖR GUIDEN OM DATASKYDD

Besvara flervalsfrågorna och sant/falskt-frågorna, fyll i luckorna med hjälp av ordbanken, matcha definitioner och lös korsordet och ordletarpusslet. Tillämpa dina kunskaper om dataskydd. Avsluta med bonusaktiviteten Tänk snabbt.

### DATASKYDD OCH SÄKERHET FÖR FÖRETAGSLAGRING (INLEDNING)

Dataskydd skyddar företagets dataresurser genom maskering, tokenisering, databaskryptering i vila och säkra protokoll för överföring. Nätverksisolerade säkerhetskopior hjälper till att säkerställa att viktiga databaser kan återställas vid ett pågående intrång.

**LÄS VARJE KONTROLLPUNKT NOGGRANT OCH VÄLJ ELLER SKRIV DET RÄTTA SVARET.**

## Kontrollpunkt 1: Utmaning med flerval

**1. Vad är det främsta syftet med datamaskering?**

- A. Att ersätta känsliga identifierare med fiktiva men realistiska tecken för att skydda integriteten
- B. Att komprimera stora databasfiler för att spara fysiskt serverlagringsutrymme
- C. Att radera gamla kundkontakt-e-postmeddelanden från arkiverade säkerhetskopieringssystem
- D. Att dölja databasserverns publika IP-adress från internetskanningar

**2. Vilken mekanism krypterar filer som lagras på en databasservers hårddisk?**

- A. Helskiv-kryptering i vila
- B. TLS-sessionens handskakningsprotokoll under överföring
- C. Regler för vidarebefordran till dynamiska DNS-namnservrar
- D. Multifaktorautentisering med hårdvarunycklar

**3. Vad representerar data under överföring?**

- A. Datapaket som rör sig över nätverksroutrar och switchar
- B. Lagrade transaktionsloggar för databaser på en kall säkerhetskopieringsdisk
- C. Arkiverade användarfiler som sparats i ett isolerat molnvalv
- D. Statiska systemkonfigurationsfiler på en lokal skrivbordslagring

**4. Varför är en regelbunden offline-säkerhetskopia avgörande för skydd mot utpressningsvirus?**

- A. Den ger en ren, frånkopplad kopia för att återställa filer utan att betala lösen
- B. Den hindrar hackare från att skanna efter öppna portkonfigurationer
- C. Den ökar överföringshastigheten för bandbredden i det lokala nätverket
- D. Den automatiserar loggar över cookiesamtycke i webbläsare

**5. Vad gör datatokenisering?**

- A. Den ersätter känsliga kortnummer med icke-känsliga slumpmässiga tokens
- B. Den dirigerar webbtrafik via flera säkra onion-noder
- C. Den söker igenom systemkataloger efter signaturbaserad skadlig kod
- D. Den granskar databasadministratörers inloggningstider

## Kontrollpunkt 2: Utmaning med sant eller falskt

### 6 Fråga 6

6. Datamaskering ändrar databasposter permanent i produktionsmiljöer.

○ Sant ○ Falskt

### 7 Fråga 7

7. Säkerhetskopior utanför lokalen måste isoleras från företagets huvudnätverk för att förhindra att ransomware sprids.

○ Sant ○ Falskt

### 8 Fråga 8

8. SSL-/TLS-certifikat säkrar databaser genom att kryptera data som lagras i vila på fysiska medier.

○ Sant ○ Falskt

### 9 Fråga 9

9. Zero Trust Network Access (ZTNA) verifierar varje användares identitet innan databasåtkomst ges.

○ Sant ○ Falskt

### 10 Fråga 10

10. Tokenisering med valv lagrar de ursprungliga kortuppgifterna i ett säkert, centralt tokenvalv.

○ Sant ○ Falskt

## Kontrollpunkt 3: Infoga nyckelbegrepp

Läs varje mening nedan och fyll i luckan med rätt term från ordbanken.

1. Att ersätta personnamn med realistiska platshållare kallas _____ av data.
2. Kryptering av fysiska lagringsblock skyddar databastillgångar _____ .
3. TLS-protokoll krypterar aktiva datapaket som rör sig under _____ .
4. Rollbaserade behörigheter begränsar vilka användare som kan få _____ till databasen.
5. Att återställa rena företagsfiler efter ett intrång kräver en säker offline- _____ .
6. Granskning av molnkonfigurationer utvärderar organisationens säkerhets _____ .

**ORDBANK**

DATAMINIMERING I VILA KRYPTERING MASKNING SÄKERHETSKOPIA SÄKERHETSLÄGE ÅTKOMST ÖVERFÖRING

**Skriv dina svar här:**

1. 
2. 
3. 
4. 
5. 
6. 

# Kontrollpunkt 4: Matchning av säkerhetsbegrepp

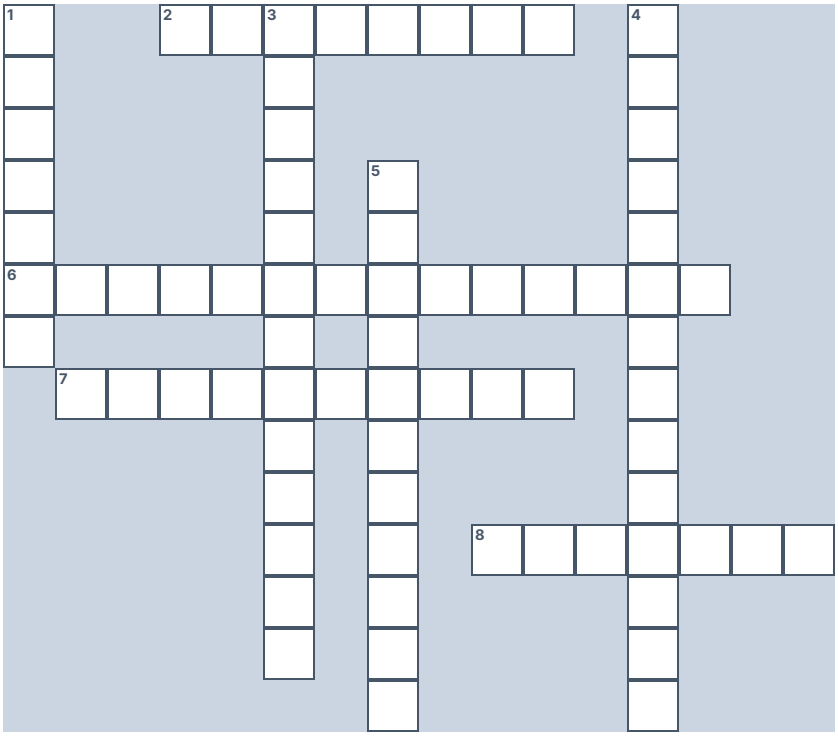
## MATCHNING AV DEFINITIONER

Para ihop varje begrepp till vänster med rätt definition till höger genom att skriva motsvarande bokstav (A–H) i det ifyllbara fältet.

| | | | |
|---|---|---|---|
| ☐ | 1. KRYPTERING | A | Att skapa säkra externa kopior av data som kan återställas vid systemfel. |
| ☐ | 2. SÄKERHETSKOPIA | B | Att omvandla klartext till oläslig chiffertext så att avlyssnad data förblir privat. |
| ☐ | 3. MINIMERING | C | Organisationens samlade säkerhetsstatus och försvarsberedskap i molnet. |
| ☐ | 4. ÅTKOMST | D | Att uppfylla regelverk som GDPR eller CCPA för hantering av privat användarinformation. |
| ☐ | 5. SÄKERHETSLÄGE | E | Säkerhetsincident där skyddade data nås eller röjs utan tillstånd. |
| ☐ | 6. INTRÅNG | F | Att begränsa läs- och skrivbehörigheter i databasen till autentiserade användarroller. |
| ☐ | 7. EFTERLEVNAD | G | Att ersätta känsliga tecken i databasfält för att skydda personliga identiteter. |
| ☐ | 8. MASKERING | H | Att begränsa insamlingen av personuppgifter till det absoluta minimum som krävs för verksamheten. |

## Kontrollpunkt 5: Korsord

Lös korsordet genom att skriva bokstäver i de aktiva vita rutorna. Siffrorna motsvarar ledtrådarna nedan.




### VÅGRÄTT

**2. Ersättning av känsliga tecken i databasfält för att skydda personers identitet (8)**

**6. Skapande av säkra kopior på annan plats som kan återställas vid systemfel (14)**

**7. Omvandling av klartext till oläsbar chiffertext så att avlyssnade data förblir privata (10)**

**8. Säkerhetsincident där skyddade data nås eller röjs utan tillstånd (7)**

### LODRÄTT

**1. Begränsning av läs- och skrivbehörighet i databaser till autentiserade användarroller (7)**

**3. Organisationens samlade säkerhetsstatus och försvarsberedskap i molnet (13)**

**4. Begränsning av insamlingen av personuppgifter till det absolut nödvändiga för verksamheten (14)**

**5. Att uppfylla regelkrav som GDPR eller CCPA vid hantering av användares privata uppgifter (11)**

# Kontrollpunkt 5, alternativ: Tillgängliga korsordsledtrådar

Användare av skärmläsare och tangentbord kan skriva korsordssvaren direkt i textfälten nedan.

## VÅGRÄTT

**2 vågrätt: Ersättning av känsliga tecken i databasfält för att skydda personers identitet (8 bokstäver):**

**6 vågrätt: Skapande av säkra kopior på annan plats som kan återställas vid systemfel (14 bokstäver):**

**7 vågrätt: Omvandling av klartext till oläsbar chiffertext så att avlyssnade data förblir privata (10 bokstäver):**

**8 vågrätt: Säkerhetsincident där skyddade data nås eller röjs utan tillstånd (7 bokstäver):**

## LODRÄTT

**1 lodrätt: Begränsning av läs- och skrivbehörighet i databaser till autentiserade användarroller (7 bokstäver):**

**3 lodrätt: Organisationens samlade säkerhetsstatus och försvarsberedskap i molnet (13 bokstäver):**

**4 lodrätt: Begränsning av insamlingen av personuppgifter till det absolut nödvändiga för verksamheten (14 bokstäver):**

**5 lodrätt: Att uppfylla regelkrav som GDPR eller CCPA vid hantering av användares privata uppgifter (11 bokstäver):**

## Kontrollpunkt 6: Dolt ordsök

Hitta de 8 viktiga ordförrådstermerna som är gömda i rutnätet nedan. Orden kan vara vågräta, lodräta eller diagonala.

D A T A M I N I M E R I N G C
N D A N V E L R E T F E Ö Ä M
G Å Q Y X M X R B P Y V N A H
X D Ä X L T B Z Ö Å N T S S Å
J Q E A D L S Y Z Z M K K I W
I G B F J L V U Y T N Ö F I F
U C A M R C Ö N L I Y T W A U
Z K N N H I O G N Å R T N I I
T T G M V M T G Z I B W G Ä P
S Ä G N I R E T P Y R K Z U I
M S Ä K E R H E T S K O P I A
O V Å A R X P P Ö Q J R V I R
K X S Ä K E R H E T S L Ä G E
T W Q W W L A F Q O M B P X G
Å H R S Z Ä K L X K Ä Y Å R L

**ORDLISTA**

KRYPTERING SÄKERHETSKOPIA DATAMINIMERING ÅTKOMST SÄKERHETSLÄGE
INTRÅNG EFTERLEVNAD MASKNING

# Kontrollpunkt 6, alternativ: Tillgänglig matchning av ordförråd

Para ihop var och en av de 8 begreppen från ordsökningen med rätt definition genom att skriva bokstaven (A–H) på den tomma raden.

**ORDLISTA**

- **A. KRYPTERING**
- **B. SÄKERHETSKOPIA**
- **C. DATAMINIMERING**
- **D. ÅTKOMST**
- **E. SÄKERHETSLÄGE**
- **F. INTRÅNG**
- **G. EFTERLEVNAD**
- **H. MASKNING**

**DEFINITIONER OCH MATCHNINGSFÄLT**

_____ 1. Säkerhetsincident där skyddade data nås eller röjs utan tillstånd.

_____ 2. Ersättning av känsliga tecken i databasfält för att skydda personers identitet.

_____ 3. Begränsning av läs- och skrivbehörighet i databaser till autentiserade användarroller.

_____ 4. Organisationens samlade säkerhetsstatus och försvarsberedskap i molnet.

_____ 5. Att uppfylla regelkrav som GDPR eller CCPA vid hantering av användares privata uppgifter.

_____ 6. Begränsning av insamlingen av personuppgifter till det absolut nödvändiga för verksamheten.

_____ 7. Omvandling av klartext till oläsbar chiffertext så att avlyssnade data förblir privata.

_____ 8. Skapande av säkra kopior på annan plats som kan återställas vid systemfel.

## Kontrollpunkt 7: Utmaning med blandade ord

Avkoda bokstäverna nedan för att avslöja viktiga begrepp och termer inom cybersäkerhet. Skriv dina svar i rutorna.

1. NRETRKIGPY
2. MAITNNDIIGE RMA
3. ÄSTLSGEKER HÄE
4. EADLTRNVEF E
5. KKPÄTSRAHO ESIE
6. SKMÅOTT
7. INÅGNRT
8. KANGMNIS

# Bonusaktivitet: Tänk snabbt

3 SVAR PER KATEGORI. DEN SOM FÖRST FYLLER I LISTAN VINNER.

| | | | | |
|---|---|---|---|---|
| 1 | Saker du säkerhetskopierar | | | |
| 2 | Ord som hör ihop med cybersäkerhet | | | |
| 3 | Personer som får se känsliga uppgifter | | | |
| 4 | Sätt att radera data på ett säkert sätt | | | |
| 5 | Platser där data lagras | | | |
| 6 | Saker som bör krypteras | | | |
| 7 | Data som ett sjukhus måste skydda | | | |
| 8 | Typer av säkerhetskopia | | | |
| 9 | Information du aldrig bör dela | | | |
| 10 | Varningstecken i ett e-postmeddelande | | | |
| 11 | Säkra vanor du kan börja med i dag | | | |
| 12 | Personer du kan fråga om IT-hjälp | | | |
| 13 | Enheter som kan hackas | | | |
| 14 | Sätt att skydda data | | | |
| 15 | Saker som kan förstöra data | | | |

# Kontrollpunkt 8: Fallstudier om cybersäkerhet

Tillämpa de begrepp du har lärt dig för att lösa de verkliga scenarierna nedan.

## FALLSTUDIE 1: UPPGRADERING AV KRYPTERING AV FÖRETAGSDATABAS I VILA

👷

**Scenario:** En nätbutik lagrar transaktionsdatabaser i molnlagring utan fullständig diskkryptering. En nylig regelefterlevnadsrevision flaggade detta som en allvarlig CCPA-risk för datasäkerheten. Utforma en återställningsarkitektur.

**Diskussionsfråga:** Analysera riskerna för CCPA-efterlevnaden och föreslå en strategi för kryptering av lagrade data.

## FALLSTUDIE 2: BEGRÄNSA RANSOMWARE OCH ÅTERSTÄLLA DATA

👷

**Scenario:** En pågående attack med utpressningsprogram krypterar nätverksenheter i ett lokalt företagsnätverk. Administratören har upptäckt infektionen tidigt. Planera stegen för isolering och återställning.

**Diskussionsfråga:** Beskriv de omedelbara åtgärderna för isolering och planera en säker återställningsprocess.

## Kontrollpunkt 9: Knäck chiffret

En cybersäkerhetsexpert skyddar nätverkstillgångar mot hotaktörer online. Använd bokstav-till-siffra-nyckeln nedan för att avkoda meddelandet genom att skriva de matchande bokstäverna på de tomma raderna.

**KRYPTERINGSNYCKEL FÖR BOKSTAV TILL SIFFRA**

A=1 B=2 C=3 D=4 E=5 F=6 G=7 H=8 I=9 J=10

K=11 L=12 M=13 N=14 O=15 P=16 Q=17 R=18 S=19 T=20

U=21 V=22 W=23 X=24 Y=25 Z=26 Å=27 Ä=28 Ö=29

19 11 25 4 4 1 4 9 14 1 16 18 9 22 1 20 1

4 1 20 1 13 5 4 19 28 11 18 1

11 15 14 20 18 15 12 12 5 18

**Avkodat meddelande:**

TIPS: VARJE SIFFRA MOTSVARAR BOKSTAVENS PLATS I ALFABETET (T.EX. 1 = A, 2 = B, 29 = Ö).

# Kontrollpunkt 10: Grundläggande vanliga frågor om cybersäkerhet (Del A)

Gå igenom vanliga frågor och svar om att begränsa hot på nätet.

### Q1: Vad är dataskydd?

Det är processen att skydda person- och företagsdata från obehörig åtkomst, förlust eller skada med hjälp av tekniska kontroller.

### Q2: Varför är helskiktskryptering av disken viktig?

Den säkrar lagrade datablock på fysiska enheter och hindrar alla från att läsa data om de fysiskt stjäl hårddisken.

### Q3: Vad är skillnaden mellan kryptering i vila och under överföring?

Kryptering i vila skyddar lagrade filer på enheter, medan kryptering under överföring skyddar aktiva nätverkspaket som rör sig över routrar.

### Q4: Vad är datamaskering?

Den ersätter känsliga uppgifter (som kreditkortsnummer) med fiktiva men realistiska data för testning utan att verkliga poster exponeras.

### Q5: Varför är säkerhetskopiering offline viktig?

Den håller en ren kopia av dina filer isolerad från nätverket, vilket hjälper till att skydda dina säkerhetskopior från att krypteras av ransomware.

# Kontrollpunkt 10: Grundläggande vanliga frågor om cybersäkerhet (Del B)

Gå igenom vanliga frågor och svar om att begränsa hot på nätet.

### Q6: Vad är ett tokeniseringsvalv för data?

En säker, isolerad databas som kopplar slumpmässiga tokens till deras ursprungliga känsliga värden (som primära kreditkortsnummer).

### Q7: Vad innebär databasåtkomst enligt Zero Trust?

Det innebär att man verifierar varje användares identitet och enhetens status vid varje inloggning, i stället för att lita på alla som finns inne i nätverket.

### Q8: Hur skyddar TLS data under överföring?

TLS krypterar nyttolasten i TCP-sessionen och hindrar illasinnade aktörer på offentliga nätverk från att avlyssna eller ändra paket under transport.

### Q9: Vad är granskning av databasåtkomst?

Kontinuerlig registrering av databasfrågor och inloggningar för att upptäcka mönster för obehörig åtkomst eller säkerhetsavvikelser.

### Q10: Vad är en granskning av säkerhetsstatus i molnet?

En process som analyserar molnkonfigurationer för att identifiera öppna portar, felkonfigurerade åtkomstregler och brister i säkerhetsefterlevnaden.

# Kontrollpunkt 10: Avancerade vanliga frågor om säkerhet (Del C)

Utforska avancerade tekniska aspekter av säkerhetsramverk, analys av skadlig kod och dataefterlevnad.

### Q1: Hur fungerar kuvertkryptering (envelope encryption)?

Den krypterar data med en datanyckel och krypterar sedan datanyckeln med en huvudnyckel, vilket förenklar lagring och rotation av nycklar.

### Q2: Vad är homomorf kryptering?

En avancerad krypteringsmetod som gör det möjligt att utföra operationer direkt på krypterade data utan att dekryptera dem först.

### Q3: Varför används kryptering på kolumnnivå i databaser?

Den krypterar vissa känsliga kolumner (som personnummer) var för sig och skyddar dem även om administratörer får allmän läsåtkomst till tabellen.

### Q4: Vad är skydd mot dataläckage (DLP)?

Programvara som övervakar nätverkets utgångspunkter för att upptäcka och blockera obehöriga utgående överföringar av känsliga filer.

### Q5: Hur skyddar säkerhetskopior av typen skriv en gång, läs många gånger (WORM) mot ransomware?

WORM-säkerhetskopior hindrar filer från att raderas eller ändras under en viss tid, vilket stoppar utpressningsvirus från att kryptera befintliga säkerhetskopior.

# Kontrollpunkt 10: Avancerade vanliga frågor om säkerhet (Del D)

Utforska avancerade tekniska aspekter av säkerhetsramverk, analys av skadlig kod och dataefterlevnad.

### Q6: Vilken risk innebär återanvändning av nycklar?

Att återanvända samma kryptografiska nyckel i olika databaser innebär att en enda kompromitterad nyckel exponerar alla databaser.

### Q7: Hur förbättrar tokenisering av databaser efterlevnaden av CCPA?

Tokens pseudonymiserar poster i icke-produktionssystem och begränsar exponeringen vid dataintrång, men tokeniserade data kan fortfarande vara personuppgifter.

### Q8: Varför är dataklassificering avgörande?

Den kategoriserar filer efter känslighetsnivå, vilket hjälper organisationer att tillämpa den starkaste krypteringen och åtkomstkontrollerna på högriskdata.

### Q9: Vilken roll har nyckelrotation?

Att uppdatera krypteringsnycklar regelbundet begränsar hur mycket historiska data som exponeras om en enskild nyckel till slut knäcks.

### Q10: Hur skyddar säkra enklaver databasfrågor i minnet?

Säkra enklaver isolerar frågeoperationer i CPU-skyddade minnesblock, vilket hindrar värdadministratörer från att se klartext i RAM.

# Del 11: 10 verkliga fakta och insikter om cybersäkerhet

Gå igenom verkliga fakta om säkerhetsintrång, försvarsmekanismer och efterlevnadsstandarder.

**1. SÄKERHETSINSIKT**

GDPR trädde i kraft i maj 2018 och ändrade hur webbplatser världen över hanterar samtycke till cookies och register över personuppgifter.

**2. SÄKERHETSINSIKT**

Ett böter för brott mot GDPR kan uppgå till 20 miljoner euro eller 4 % av den globala omsättningen, vilket innebär en betydande juridisk exponering. [4]

**3. SÄKERHETSINSIKT**

CCPA trädde i kraft i januari 2020 och införde banbrytande konsumenträttigheter för digital integritet i USA.

**4. SÄKERHETSINSIKT**

Dataminimering minskar databasens lagringsutrymme, vilket sänker serverkostnaderna och minskar konsekvenserna av ett dataintrång.

**5. SÄKERHETSINSIKT**

Kryptografisk strimling löser problemet med radering av säkerhetskopior genom att rensa nycklar i stället för att redigera historiska backupband.

**6. SÄKERHETSINSIKT**

De flesta länder världen över har numera antagit lagar om skydd av personuppgifter för att skydda konsumenters integritetsrättigheter.

**7. SÄKERHETSINSIKT**

Samtyckesformulär med förkryssade rutor (opt-in) är uttryckligen förbjudna enligt europeiska regelverk om dataintegritet.

**8. SÄKERHETSINSIKT**

GDPR kräver att personuppgiftsincidenter rapporteras till tillsynsmyndigheten inom 72 timmar efter att man fått kännedom om dem, om det är möjligt. [3]

**9. SÄKERHETSINSIKT**

Hashning av lösenord med långsamma algoritmer som bcrypt eller Argon2 gör offlineknäckning av stulna hashar mycket svårare. [6]

**10. SÄKERHETSINSIKT**

Data i vila är sparade databasfiler, medan data under överföring är paket som aktivt rör sig genom nätverksroutrar.

# Tekniska referenser och källor

Studieguiden och de interaktiva pusslen är sammanställda utifrån globala standarder från NIST och OWASP samt standarder för efterlevnad av dataskydd.

## VETENSKAPLIGA OCH BRANSCHRELATERADE REFERENSER

[1] NIST. (2025). SP 800-88 Rev. 2, Guidelines for Media Sanitization.
https://csrc.nist.gov/pubs/sp/800/88/r2/final

[2] CISA. (2023). #StopRansomware Guide.
https://www.cisa.gov/stopransomware/ransomware-guide

[3] Intersoft Consulting. (n.d.). Art. 33 GDPR – Notification of a personal data breach to the supervisory authority.
https://gdpr-info.eu/art-33-gdpr/

[4] Intersoft Consulting. (n.d.). Art. 83 GDPR – General conditions for imposing administrative fines.
https://gdpr-info.eu/art-83-gdpr/

[5] California Privacy Protection Agency. (n.d.). Frequently Asked Questions (FAQs).
https://cppa.ca.gov/faq.html

[6] OWASP. (n.d.). Password Storage Cheat Sheet.
https://cheatsheetseries.owasp.org/cheatsheets/Password_Storage_Cheat_Sheet.html

## Facit: Kontrollpunkt 1 – Flerval

**1** **Fråga 1** — **Rätt svar: A**

### ANTECKNING FÖR LÄRAREN

Vad är det främsta syftet med datamaskering? → Att ersätta känsliga identifierare med fiktiva men realistiska tecken för att skydda integriteten

**2** **Fråga 2** — **Rätt svar: A**

### ANTECKNING FÖR LÄRAREN

Vilken mekanism krypterar filer som lagras på en databasservers hårddisk? → Helskiv-kryptering i vila

**3** **Fråga 3** — **Rätt svar: A**

### ANTECKNING FÖR LÄRAREN

Vad representerar data under överföring? → Datapaket som rör sig över nätverksroutrar och switchar

**4** **Fråga 4** — **Rätt svar: A**

### ANTECKNING FÖR LÄRAREN

Varför är en regelbunden offline-säkerhetskopia avgörande för skydd mot utpressningsvirus? → Den ger en ren, frånkopplad kopia för att återställa filer utan att betala lösen

**5** **Fråga 5** — **Rätt svar: A**

### ANTECKNING FÖR LÄRAREN

Vad gör datatokenisering? → Den ersätter känsliga kortnummer med icke-känsliga slumpmässiga tokens

## Facit: Kontrollpunkt 2 – Sant eller falskt

**6** **Fråga 6** — **Rätt svar: Falskt**

### ANTECKNING FÖR LÄRAREN

Maskering ändrar testkopior eller döljer värden vid förfrågan; produktionsposter förblir oförändrade.

**7** **Fråga 7** — **Rätt svar: Sant**

### ANTECKNING FÖR LÄRAREN

Säkerhetskopior utanför lokalen måste isoleras från företagets huvudnätverk för att förhindra att ransomware sprids.

**8** **Fråga 8** — **Rätt svar: Falskt**

### ANTECKNING FÖR LÄRAREN

TLS-certifikat skyddar data under överföring; lagrade data behöver kryptering av disk, fil eller databas.

**9** **Fråga 9** — **Rätt svar: Sant**

### ANTECKNING FÖR LÄRAREN

Zero Trust Network Access (ZTNA) verifierar varje användares identitet innan databasåtkomst ges.

**10** **Fråga 10** — **Rätt svar: Sant**

### ANTECKNING FÖR LÄRAREN

Tokenisering med valv håller de ursprungliga värdena i ett säkert tokenvalv som kopplar varje token tillbaka till sina data.

# Facit för ordförråd och bedömningsmall

**Bedömningsmatris för läraren: Ge 1 poäng för varje korrekt matchning (totalt 8 poäng) och kontextbegrepp (totalt 6 poäng).**

## KONTROLLPUNKT 4: FACIT – MATCHNING AV BEGREPP

| | | | |
|---|---|---|---|
| B 1. KRYPTERING | A 2. SÄKERHETSKOPIA | H 3. MINIMERING | F 4. ÅTKOMST |
| C 5. SÄKERHETSLÄGE | E 6. INTRÅNG | D 7. EFTERLEVNAD | G 8. MASKERING |

## KONTROLLPUNKT 3: FACIT – NYCKELBEGREPP

| | | | |
|---|---|---|---|
| 1 MASKNING | 2 I VILA | 3 ÖVERFÖRING | 4 ÅTKOMST |
| 5 SÄKERHETSKOPIA | 6 SÄKERHETSLÄGE | | |

## KONTROLLPUNKT 6, ALTERNATIV: FACIT – MATCHNING AV ORD

| | | | |
|---|---|---|---|
| 1 F – INTRÅNG | 2 H – MASKNING | 3 D – ÅTKOMST | 4 E – SÄKERHETSLÄGE |
| 5 G – EFTERLEVNAD | 6 C – DATAMINIMERING | 7 A – KRYPTERING | 8 B – SÄKERHETSKOPIA |

## DISKUSSIONSANTECKNINGAR FÖR LÄRAREN

**Nyckelbegrepp:**
Kontrollera att eleverna kan förklara KRYPTERING, SÄKERHETSKOPIA och MINIMERING med egna ord och ge ett exempel på varje.

**Fallstudier:**
Be eleverna att stödja sina rekommendationer med fakta från arbetsbladet, inte med antaganden.

**Källkritik:**
Be eleverna att kontrollera minst ett påstående i arbetsbladets källor och diskutera varför siffror, priser och regler kan ändras över tid.

# Facit till pussel och anteckningar för läraren

## LÖSNING PÅ ORDSÖKET

| D | A | T | A | M | I | N | I | M | E | R | I | N | G | C |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| N | D | A | N | V | E | L | R | E | T | F | E | Ö | Ä | M |
| G | Å | Q | Y | X | M | X | R | B | P | Y | V | N | A | H |
| X | D | Ä | X | L | T | B | Z | Ö | Å | N | T | S | S | Å |
| J | Q | E | A | D | L | S | Y | Z | Z | M | K | K | I | W |
| I | G | B | F | J | L | V | U | Y | T | N | Ö | F | I | F |
| U | C | A | M | R | C | Ö | N | L | I | Y | T | W | A | U |
| Z | K | N | N | H | I | O | G | N | Å | R | T | N | I | I |
| T | T | G | M | V | M | T | G | Z | I | B | W | G | Ä | P |
| S | Ä | G | N | I | R | E | T | P | Y | R | K | Z | U | I |
| M | S | Ä | K | E | R | H | E | T | S | K | O | P | I | A |
| O | V | Å | A | R | X | P | P | Ö | Q | J | R | V | I | R |
| K | X | S | Ä | K | E | R | H | E | T | S | L | Ä | G | E |
| T | W | Q | W | W | L | A | F | Q | O | M | B | P | X | G |
| Å | H | R | S | Z | Ä | K | L | X | K | Ä | Y | Å | R | L |

## LÖSNING PÅ KORSORDET

| Å | | | M | A | S | K | N | I | N | G | | D | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| T | | | | | Ä | | | | | | | A | | |
| K | | | | | K | | | | | | | T | | |
| O | | | | | E | | E | | | | | A | | |
| M | | | | | R | | F | | | | | M | | |
| S | Ä | K | E | R | H | E | T | S | K | O | P | I | A | |
| T | | | | | E | | E | | | | | N | | |
| | K | R | Y | P | T | E | R | I | N | G | | I | | |
| | | | | | S | | L | | | | | M | | |
| | | | | | L | | E | | | | | E | | |
| | | | | | Ä | | V | | I | N | T | R | Å | N | G |
| | | | | | G | | N | | | | | I | | |
| | | | | | E | | A | | | | | N | | |
| | | | | | | | D | | | | | G | | |

## LÄRARHANDLEDNING MED LÖSNINGAR TILL KORSORDET

### VÅGRÄTT

**2 vågrätt: MASKNING** Ersättning av känsliga tecken i databasfält för att skydda personers identitet (8 bokstäver)

**6 vågrätt: SÄKERHETSKOPIA** Skapande av säkra kopior på annan plats som kan återställas vid systemfel (14 bokstäver)

**7 vågrätt: KRYPTERING** Omvandling av klartext till oläsbar chiffertext så att avlyssnade data förblir privata (10 bokstäver)

**8 vågrätt: INTRÅNG** Säkerhetsincident där skyddade data nås eller röjs utan tillstånd (7 bokstäver)

### LODRÄTT

**1 lodrätt: ÅTKOMST** Begränsning av läs- och skrivbehörighet i databaser till autentiserade användarroller (7 bokstäver)

**3 lodrätt: SÄKERHETSLÄGE** Organisationens samlade säkerhetsstatus och försvarsberedskap i molnet (13 bokstäver)

**4 lodrätt: DATAMINIMERING** Begränsning av insamlingen av personuppgifter till det absolut nödvändiga för verksamheten (14 bokstäver)

**5 lodrätt: EFTERLEVNAD** Att uppfylla regelkrav som GDPR eller CCPA vid hantering av användares privata uppgifter (11 bokstäver)

# Facit för blandade ord och chiffer

Facit för övningen med ordvärlden och utmaningen Hemliga chiffret.

### FACIT FÖR ORDBLANDNING

1. N R E T R K I G P Y — **KRYPTERING**
2. M A I T N N D I I G E R M A — **DATAMINIMERING**
3. Ä S T L S G E K E R H Ä E — **SÄKERHETSLÄGE**
4. E A D L T R N V E F E — **EFTERLEVNAD**
5. K K P Ä T S R A H O E S I E — **SÄKERHETSKOPIA**
6. S K M Å O T T — **ÅTKOMST**
7. I N Å G N R T — **INTRÅNG**
8. K A N G M N I S — **MASKNING**

### NYCKEL TILL UTMANINGEN MED HEMLIGT CHIFFER

**"SKYDDA DINA PRIVATA DATA MED SÄKRA KONTROLLER"**

# Facit till fallstudierna

## A Fallstudie 1: Uppgradering av kryptering av företagsdatabas i vila

Lärarens lösning

### BEDÖMNINGSRIKTLINJE

**Elevernas svar bör täcka följande punkter:**

- Scenarioanalys: En webbutik lagrar transaktionsdatabaser i molnlagring utan kryptering av hela disken. En nyligen genomförd efterlevnadsgranskning flaggade detta som en allvarlig dataskyddsrisk enligt CCPA. Utforma en återställningsarkitektur.
- Rekommenderad strategi och lösning: Inför AES-256-diskkryptering av lagrade data på alla filsystem. Använd en central nyckelhanteringstjänst (KMS) med automatisk rotation och tillämpa strikta IAM-policyer för att styra åtkomst till dekryptering.

## B Fallstudie 2: Begränsa ransomware och återställa data

Lärarens lösning

### BEDÖMNINGSRIKTLINJE

**Elevernas svar bör täcka följande punkter:**

- Scenarioanalys: Ett aktivt ransomware-angrepp krypterar nätverksenheter i ett lokalt företagsnätverk. Administratören har upptäckt infektionen tidigt. Planera stegen för inneslutning och återhämtning.
- Rekommenderad strategi och lösning: Isolera det komprometterade segmentet omedelbart. Formatera de påverkade slutpunkterna och återställ från den senaste offline-backupen med write-once-read-many (WORM). Verifiera backupens integritet innan systemen kopplas in igen.