Navn: _____ Dato: _____ Poeng: _____

Databeskyttelse og lagring i bedrifter Sikkerhetsguide

Datamaskering, tokenisering, kryptering av data i hvile og under overføring, frakoblede sikkerhetskopier

LÆRINGSOVERSIKT: DATABESKYTTELSE

SIKRET
DATAKRYPTERING
256-bits AES-standard

I SAMSVAR
GLOBALE STANDARDER
Rammeverk for GDPR og CCPA

ZERO TRUST
TILGANGSPOLICY
Flerfaktorautentisering

Velkommen! Dette aktivitetsheftet veileder deg gjennom standarder og kontroller for databeskyttelse. Du utforsker full diskkryptering, sikre tilgangskontroller, maskinvarebaserte sikkerhetskopier, sikkerhetstilstand i skyen og teknikker for datamaskering.

KONTROLLPUNKTER I ARBEIDSARKET

- [ ] **Del 1-4: Behersk cybersikkerhet og forebygging av trusler.**
- [ ] **Del 5-7: Løs kryssord og ordsøk.**
- [ ] **Del 8-9: Løs casestudier og chifferutfordringen.**
- [ ] **Del 10: Gå gjennom sidene med grunnleggende og avanserte vanlige spørsmål.**
- [ ] **Del 11: Utforsk 10 interessante fakta fra virkeligheten.**
- [ ] **Bonus: Tenk raskt-utfordring.**

Åpne VPN.coms veiledning om cybersikkerhet

URL: https://www.vpn.com/no/cybersikkerhet/databeskyttelse/

Din læringsveiledning for strategi for databeskyttelse

- Skill mellom teknikkene datamaskering og tokenisering.
- Innfør kryptering i hvile for lagringsstasjoner og kryptering under overføring med TLS.
- Utform frakoblede, nettverksisolerte sikkerhetskopisystemer som beskyttelse mot løsepengevirus.

INSTRUKSJONER FOR GUIDE OM DATABESKYTTELSE

Svar på flervalgsspørsmålene og sant/usant-spørsmålene, fyll ut setningene med ordbanken, koble sammen definisjoner, og løs kryssordet og ordsøket. Bruk kunnskapen din på databeskyttelse. Avslutt med bonusaktiviteten Tenk raskt.

DATABESKYTTELSE OG SIKKERHET FOR LAGRING I BEDRIFTER (INNLEDNING)

Databeskyttelse sikrer virksomhetens dataeiendeler gjennom maskering, tokenisering, kryptering av databaser i hvile og sikre overføringsprotokoller. Sikkerhetskopier som er isolert fra nettverket, bidrar til at viktige databaser kan gjenopprettes ved et pågående innbrudd.

LES HVERT KONTROLLPUNKT NØYE OG VELG ELLER SKRIV DET RIKTIGE SVARET.

Kontrollpunkt 1: Flervalgsutfordring

1. Hva er hovedformålet med datamaskering?

- A. Å erstatte sensitive identifikatorer med fiktive, men realistiske tegn for å beskytte personvernet
- B. Å komprimere store databasefiler for å spare fysisk serverlagring
- C. Å slette gamle e-poster med kundekontakter fra arkivsystemer for sikkerhetskopiering
- D. Å skjule databaseserverens offentlige IP-adresse fra skanninger på internett

2. Hvilken mekanisme krypterer filer som er lagret på harddisken til en databaseserver?

- A. Full diskkryptering i hvile
- B. TLS-sesjonens håndtrykksprotokoller under overføring
- C. Videresendingsregler for navneservere med dynamisk DNS
- D. Flerfaktorautentisering med maskinvarenøkler

3. Hva representerer data under overføring?

- A. Datapakker som beveger seg over nettverksroutere og -svitsjer
- B. Lagrede databasetransaksjonslogger på en kald sikkerhetskopistasjon
- C. Arkiverte brukerfiler lagret i et isolert skyhvelv
- D. Statiske systemkonfigurasjonsfiler på lokal lagring på en stasjonær PC

4. Hvorfor er en jevnlig frakoblet sikkerhetskopi avgjørende for beskyttelse mot løsepengevirus?

- A. Den gir en ren kopi uten nettilkobling som kan gjenopprette filer uten å betale løsepenger
- B. Den hindrer hackere i å skanne åpne portkonfigurasjoner
- C. Den øker overføringshastigheten på det lokale nettverket
- D. Den automatiserer logger over samtykke til informasjonskapsler i nettlesere

5. Hva gjør datatokenisering?

- A. Den erstatter sensitive kortnumre med ikke-sensitive tilfeldige tokener
- B. Den ruter nettrafikk gjennom flere sikre onion-noder
- C. Den skanner systemmapper etter signaturbasert skadevare
- D. Den reviderer påloggingstidene til databaseadministratorer

Kontrollpunkt 2: Utfordring med sant eller usant

6 Spørsmål 6

6. Datamaskering endrer databaseoppføringer permanent i produksjonsmiljøer.

- ◯ Sant
- ◯ Usant

7 Spørsmål 7

7. Sikkerhetskopier utenfor lokasjonen må isoleres fra bedriftens hovednettverk for å hindre spredning av løsepengevirus.

- ◯ Sant
- ◯ Usant

8 Spørsmål 8

8. SSL/TLS-sertifikater sikrer databaser ved å kryptere data som er lagret i hvile på fysiske medier.

- ◯ Sant
- ◯ Usant

9 Spørsmål 9

9. Zero Trust Network Access (ZTNA) verifiserer identiteten til hver bruker før databasetilgang gis.

- ◯ Sant
- ◯ Usant

10 Spørsmål 10

10. Tokenisering basert på hvelv lagrer de opprinnelige kortverdiene i et sikkert, sentralt tokenhvelv.

- ◯ Sant
- ◯ Usant

Kontrollpunkt 3: Sett inn nøkkelbegreper

Les hver setning nedenfor og fyll ut det tomme feltet med riktig begrep fra ordbanken.

1. Å erstatte personnavn med realistiske plassholdere kalles _____ av data.
2. Kryptering av fysiske lagringsblokker beskytter databaseressurser som er _____ .
3. TLS-protokoller krypterer aktive datapakker som beveger seg under _____ .
4. Rollebaserte tillatelser begrenser hvilke brukere som kan få _____ til databasen.
5. Å gjenopprette rene bedriftsfiler etter et sikkerhetsbrudd krever en sikker frakoblet _____ .
6. Revisjon av skykonfigurasjoner vurderer hvilket _____ organisasjonen har.

ORDBANK

DATAMINIMERING | I HVILE | MASKERING | OVERFØRING | SIKKERHETSBRUDD | SIKKERHETSKOPI | SIKKERHETSNIVÅ | TILGANG

Skriv svarene dine her:

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

Kontrollpunkt 4: Koble sikkerhetsbegreper

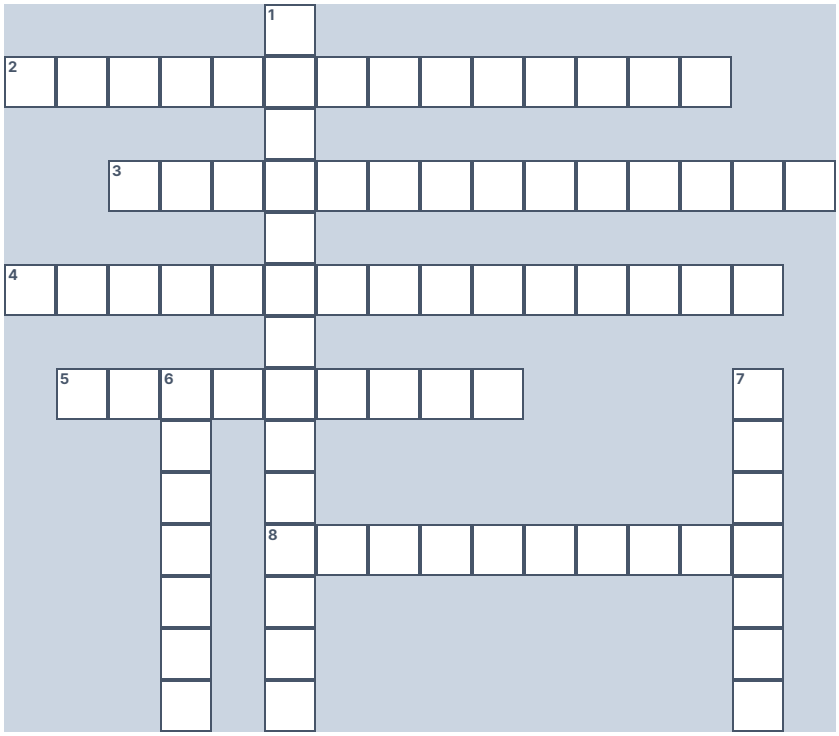
KOBLE DEFINISJONER

Koble hvert fagbegrep til venstre med riktig definisjon til høyre ved å skrive den tilhørende bokstaven (A-H) i det utfyllbare feltet.

☐	1. KRYPTERING	A	Å lage sikre kopier av data utenfor stedet som kan gjenopprettes ved systemfeil.
☐	2. SIKKERHETSKOPI	B	Å omdanne klartekst til uleselig chiffertekst slik at avskårne data forblir private.
☐	3. MINIMERING	C	Organisasjonens samlede sikkerhetsstatus og forsvarsberedskap i skyen.
☐	4. TILGANG	D	Å oppfylle regelverksstandarder som GDPR eller CCPA for håndtering av private brukeropplysninger.
☐	5. SIKKERHETSTILSTAND	E	Sikkerhetshendelse der beskyttede data blir åpnet eller utlevert uten tillatelse.
☐	6. DATABRUDD	F	Begrensning av lese- og skrivetillatelser i databasen til autentiserte brukerroller.
☐	7. OVERHOLDELSE	G	Erstatning av sensitive tegn i databasefelt for å beskytte personlige identiteter.
☐	8. MASKERING	H	Å begrense innsamling av personopplysninger til det absolutt nødvendige minimum for driften.

Kontrollpunkt 5: Kryssord

Løs kryssordet ved å skrive bokstaver i de aktive hvite rutene. Tallene tilsvarer hintene nedenfor.



VANNRETT

2. Å begrense innsamlingen av personopplysninger til det absolutt nødvendige minimum for driften (14)

3. Organisasjonens samlede sikkerhetsstatus og forsvarsberedskap i skyen (14)

4. Sikkerhetshendelse der beskyttede data åpnes eller utleveres uten tillatelse (15)

5. Å erstatte sensitive tegn i databasefelt for å beskytte personers identitet (9)

8. Omforming av klartekst til uleselig chiffertekst slik at avskjærte data forblir private (10)

LODDRETT

1. Å lage sikre kopier utenfor stedet som kan gjenopprettes ved systemfeil (14)

6. Å oppfylle regulatoriske standarder som GDPR eller CCPA ved håndtering av private brukeropplysninger (7)

7. Å begrense lese- og skrivetillatelser i databasen til autentiserte brukerroller (7)

Kontrollpunkt 5, alternativ: Tilgjengelige kryssordhint

Brukere av skjermleser og tastatur kan skrive inn kryssordsvarene direkte i tekstfeltene nedenfor.

VANNRETT

2 vannrett: Å begrense innsamlingen av personopplysninger til det absolutt nødvendige minimum for driften (14 bokstaver):

3 vannrett: Organisasjonens samlede sikkerhetsstatus og forsvarsberedskap i skyen (14 bokstaver):

4 vannrett: Sikkerhetshendelse der beskyttede data åpnes eller utleveres uten tillatelse (15 bokstaver):

5 vannrett: Å erstatte sensitive tegn i databasefelt for å beskytte personers identitet (9 bokstaver):

8 vannrett: Omforming av klartekst til uleselig chiffertekst slik at avskjærte data forblir private (10 bokstaver):

LODDRETT

1 loddrett: Å lage sikre kopier utenfor stedet som kan gjenopprettes ved systemfeil (14 bokstaver):

6 loddrett: Å oppfylle regulatoriske standarder som GDPR eller CCPA ved håndtering av private brukeropplysninger (7 bokstaver):

7 loddrett: Å begrense lese- og skrivetillatelser i databasen til autentiserte brukerroller (7 bokstaver):

Kontrollpunkt 6: Skjult ordsøk

Finn de 8 sentrale ordforrådsbegrepene som er skjult i rutenettet nedenfor. Ordene kan stå vannrett, loddrett eller diagonalt.

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

ORDLISTE

KRYPTERING SIKKERHETSKOPI DATAMINIMERING TILGANG SIKKERHETSNIVÅ
SIKKERHETSBRUDD SAMSVAR MASKERING

Kontrollpunkt 6, alternativ: Tilgjengelig ordkobling

Koble hvert av de 8 fagbegrepene fra ordsøket til riktig definisjon ved å skrive bokstaven (A-H) i det tomme feltet.

BEGREPER
A. KRYPTERING
B. SIKKERHETSKOPI
C. DATAMINIMERING
D. TILGANG
E. SIKKERHETSNIVÅ
F. SIKKERHETSBRUDD
G. SAMSVAR
H. MASKERING

DEFINISJONER OG TILHØRENDE FELT

1. Sikkerhetshendelse der beskyttede data åpnes eller utleveres uten tillatelse.
2. Å erstatte sensitive tegn i databasefelt for å beskytte personers identitet.
3. Å begrense lese- og skrivetillatelser i databasen til autentiserte brukerroller.
4. Organisasjonens samlede sikkerhetsstatus og forsvarsberedskap i skyen.
5. Å oppfylle regulatoriske standarder som GDPR eller CCPA ved håndtering av private brukeropplysninger.
6. Å begrense innsamlingen av personopplysninger til det absolutt nødvendige minimum for driften.
7. Omforming av klartekst til uleselig chiffertekst slik at avskjærte data forblir private.
8. Å lage sikre kopier utenfor stedet som kan gjenopprettes ved systemfeil.

Kontrollpunkt 7: Utfordring med blandede ord

Sett bokstavene nedenfor sammen i riktig rekkefølge for å avsløre sentrale begreper innen cybersikkerhet. Skriv svarene dine i svarboksene.

1. NRETRKIGPY
2. MAITNNDIIGE RMA
3. STIVEÅSNKH ERIK
4. RAVSASM
5. SKOIETEIRKH SPK
6. NLATGGI
7. SBHTSRIKDRU DKEE
8. GENMKARIS

Bonusaktivitet: Tenk raskt

3 SVAR PER KATEGORI. DEN SOM FYLLER UT LISTEN FØRST, VINNER.

1	Ting du tar sikkerhetskopi av			
2	Ord knyttet til cybersikkerhet			
3	Personer som har lov til å se sensitive data			
4	Måter å slette data sikkert på			
5	Steder der data lagres			
6	Ting som bør krypteres			
7	Data et sykehus må beskytte			
8	Typer sikkerhetskopi			
9	Informasjon du aldri bør dele			
10	Advarselstegn i en e-post			
11	Trygge vaner du kan begynne med i dag			
12	Personer du kan spørre om IT-hjelp			
13	Enheter som kan hackes			
14	Måter å beskytte data på			
15	Ting som kan ødelegge data			

Kontrollpunkt 8: Casestudier om cybersikkerhet

Bruk begrepene du har lært til å løse de virkelige scenarioene nedenfor.

CASESTUDIE 1: OPPGRADERING AV KRYPTERING AV BEDRIFTSDATABASE I HVILE

👷

Scenario: En nettbutikk lagrer transaksjonsdatabaser i skylagring uten full diskkryptering. En fersk samsvarsrevisjon pekte på dette som en alvorlig CCPA-datasikkerhetsrisiko. Utform en arkitektur for gjenoppretting.

Diskusjonsspørsmål: Analyser CCPA-samsvarsrisikoene og foreslå en strategi for kryptering av lagrede data.

CASESTUDIE 2: BEGRENSNING AV LØSEPENGEVIRUS OG GJENOPPRETTING AV DATA

👷

Scenario: Et aktivt løsepengevirus-angrep krypterer nettverksstasjoner på et lokalt bedriftsnettverk. Administratoren har oppdaget infeksjonen tidlig. Planlegg trinnene for inneslutning og gjenoppretting.

Diskusjonsspørsmål: Beskriv de umiddelbare tiltakene for inneslutning i detalj, og planlegg en sikker gjenopprettingsprosess.

Kontrollpunkt 9: Knekk chifferet

En cybersikkerhetsekspert beskytter nettverksressurser mot trusselaktører på nettet. Bruk nøkkelen med bokstaver og tall nedenfor til å dekryptere meldingen ved å skrive de tilhørende bokstavene i de tomme feltene.

NØKKEL FOR KRYPTERING AV BOKSTAV TIL TALL

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 Æ=27 Ø=28 Å=29

2	5	19	11	25	20	20		4	9	14	5		16	18	9	22	1	20	5
			4	1	20	1		13	5	4		19	9	11	18	5		
				11	15	14	20	18	15	12	12	5	18					

Dekodet melding:

TIPS: HVERT TALL REPRESENTERER BOKSTAVENS PLASS I ALFABETET (F.EKS. 1 = A, 2 = B, 29 = Å).

Kontrollpunkt 10: Grunnleggende vanlige spørsmål om cybersikkerhet (Del A)

Gå gjennom vanlige spørsmål og svar om å redusere trusler på nettet.

Q1: Hva er databeskyttelse?

Det er prosessen med å sikre personlige data og forretningsdata mot uautorisert tilgang, tap eller ødeleggelse gjennom tekniske kontroller.

Q2: Hvorfor er full diskkryptering viktig?

Den sikrer lagrede datablokker på fysiske stasjoner og hindrer at noen kan lese data hvis harddisken stjeles fysisk.

Q3: Hva er forskjellen mellom kryptering i hvile og under overføring?

Kryptering i hvile sikrer lagrede filer på disker, mens kryptering under overføring sikrer aktive nettverkspakker som beveger seg over rutere.

Q4: Hva er datamaskering?

Den erstatter sensitive opplysninger (som kredittkortnumre) med fiktive, men realistiske data til testing uten å eksponere ekte poster.

Q5: Hvorfor er frakoblet sikkerhetskopi viktig?

Den holder en ren kopi av filene dine isolert fra nettverket, noe som bidrar til å beskytte sikkerhetskopiene dine mot å bli kryptert av løsepengevare.

Kontrollpunkt 10: Grunnleggende vanlige spørsmål om cybersikkerhet (Del B)

Gå gjennom vanlige spørsmål og svar om å redusere trusler på nettet.

Q6: Hva er en hvelv for datatokenisering (tokenization vault)?

En sikker, isolert database som kobler tilfeldige tokener til de opprinnelige sensitive verdiene (som primære kredittkortnumre).

Q7: Hva betyr databasetilgang etter zero trust-prinsippet?

Det betyr å verifisere identiteten og enhetens tilstand til hver bruker ved hver pålogging, i stedet for å stole på alle som befinner seg inne i nettverket.

Q8: Hvordan beskytter TLS data under overføring?

TLS krypterer nyttelasten i TCP-økten og hindrer ondsinnede aktører på offentlige nettverk i å snuse på eller endre pakker under transitt.

Q9: Hva er revisjon av databasetilgang?

Den kontinuerlige registreringen av databasespørringer og innlogginger for å oppdage mønstre for uautorisert tilgang eller sikkerhetsavvik.

Q10: Hva er en revisjon av sikkerhetstilstanden i skyen?

En prosess som analyserer skykonfigurasjoner for å identifisere åpne porter, feilkonfigurerte tilgangsregler og hull i samsvar med sikkerhetskrav.

Kontrollpunkt 10: Avanserte vanlige spørsmål om sikkerhet (Del C)

Utforsk avanserte tekniske sider ved sikkerhetsrammeverk, analyse av skadevare og etterlevelse av datakrav.

Q1: Hvordan fungerer konvoluttkryptering (envelope encryption)?

Den krypterer data med en datanøkkel og krypterer deretter datanøkkelen med en hovednøkkel, noe som forenkler lagring og rotasjon av nøkler.

Q2: Hva er homomorf kryptering?

En avansert krypteringsmetode som gjør det mulig å utføre operasjoner direkte på krypterte data uten å dekryptere dem først.

Q3: Hvorfor brukes kryptering på kolonnenivå i databaser?

Den krypterer bestemte sensitive kolonner (som personnumre) hver for seg og beskytter dem selv om administratorer får generell lesetilgang til tabellen.

Q4: Hva er forebygging av datatap (DLP)?

Programvare som overvåker utgangspunkter i nettverket for å oppdage og blokkere uautoriserte utgående overføringer av sensitive filer.

Q5: Hvordan beskytter WORM-sikkerhetskopier (write-once-read-many) mot løsepengevirus?

WORM-sikkerhetskopier hindrer at filer slettes eller endres i en fastsatt periode, noe som stopper løsepengevirus fra å kryptere eksisterende sikkerhetskopier.

Kontrollpunkt 10: Avanserte vanlige spørsmål om sikkerhet (Del D)

Utforsk avanserte tekniske sider ved sikkerhetsrammeverk, analyse av skadevare og etterlevelse av datakrav.

Q6: Hva er risikoen ved gjenbruk av nøkler?

Gjenbruk av den samme kryptografiske nøkkelen på tvers av ulike databaser betyr at én enkelt nøkkelkompromittering eksponerer alle databasene.

Q7: Hvordan forbedrer databasetokenisering samsvar med CCPA?

Tokens pseudonymiserer poster i systemer som ikke er i produksjon og begrenser eksponeringen ved brudd, men tokeniserte data kan fortsatt være personopplysninger.

Q8: Hvorfor er dataklassifisering kritisk?

Den kategoriserer filer etter sensitivitetsnivå og hjelper organisasjoner med å bruke den sterkeste krypteringen og de strengeste tilgangskontrollene på data med høy risiko.

Q9: Hvilken rolle spiller nøkkelrotasjon?

Regelmessig oppdatering av krypteringsnøkler begrenser mengden historiske data som eksponeres hvis en enkelt nøkkel til slutt knekkes.

Q10: Hvordan beskytter sikre enklaver databasespørringer i minnet?

Sikre enklaver isolerer spørringsoperasjoner i CPU-beskyttede minneblokker, slik at vertsadministratorer ikke kan se klartekst i RAM.

Del 11: 10 fakta om cybersikkerhet fra virkeligheten og innsikt

Gå gjennom virkelighetsnære fakta om sikkerhetsbrudd, forsvarsmekanismer og samsvarsstandarder.

1. SIKKERHETSINNSIKT

GDPR-regelverket trådte i kraft i mai 2018 og endret hvordan globale nettsteder håndterer samtykke til informasjonskapsler og registre over personopplysninger.

2. SIKKERHETSINNSIKT

En bot for brudd på GDPR kan nå 20 millioner euro eller 4 % av global omsetning, noe som representerer betydelig juridisk eksponering. [4]

3. SIKKERHETSINNSIKT

CCPA trådte i kraft i januar 2020 og etablerte banebrytende forbrukerrettigheter for digitalt personvern i USA.

4. SIKKERHETSINNSIKT

Dataminimering reduserer databasens lagringsavtrykk, kutter serverkostnader og reduserer samtidig omfanget av et eventuelt datainnbrudd.

5. SIKKERHETSINNSIKT

Kryptografisk makulering løser utfordringen med sletting i sikkerhetskopier ved å slette nøkler i stedet for å redigere historiske sikkerhetskopibåndfiler.

6. SIKKERHETSINNSIKT

De fleste land i verden har nå innført lover om beskyttelse av personopplysninger for å ivareta forbrukernes personvernrettigheter.

7. SIKKERHETSINNSIKT

Samtykkeskjemaer med forhåndsavkryssede bokser er uttrykkelig forbudt etter de europeiske definisjonene i personvernregelverket.

8. SIKKERHETSINNSIKT

GDPR krever at brudd på personopplysningssikkerheten rapporteres til tilsynsmyndigheten innen 72 timer etter at man ble kjent med det, der det er mulig. [3]

9. SIKKERHETSINNSIKT

Hashing av passord med trege algoritmer som bcrypt eller Argon2 gjør offline-knekking av stjålne hasher langt vanskeligere. [6]

10. SIKKERHETSINNSIKT

Data i hvile er lagrede databasefiler, mens data under overføring er pakker som aktivt beveger seg gjennom nettverksrutere.

Tekniske referanser og kilder

Studieveiledningen og de interaktive oppgavene er satt sammen fra globale standarder fra NIST og OWASP og standarder for etterlevelse av personvern.

FAGLIGE REFERANSER OG BRANSJEREFERANSER

[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

Fasit: Kontrollpunkt 1 – flervalg

1 Spørsmål 1 — **Riktig svar: A**

MERKNAD TIL LÆREREN

Hva er hovedformålet med datamaskering? → Å erstatte sensitive identifikatorer med fiktive, men realistiske tegn for å beskytte personvernet

2 Spørsmål 2 — **Riktig svar: A**

MERKNAD TIL LÆREREN

Hvilken mekanisme krypterer filer som er lagret på harddisken til en databaseserver? → Full diskkryptering i hvile

3 Spørsmål 3 — **Riktig svar: A**

MERKNAD TIL LÆREREN

Hva representerer data under overføring? → Datapakker som beveger seg over nettverksroutere og -svitsjer

4 Spørsmål 4 — **Riktig svar: A**

MERKNAD TIL LÆREREN

Hvorfor er en jevnlig frakoblet sikkerhetskopi avgjørende for beskyttelse mot løsepengevirus? → Den gir en ren kopi uten nettilkobling som kan gjenopprette filer uten å betale løsepenger

5 Spørsmål 5 — **Riktig svar: A**

MERKNAD TIL LÆREREN

Hva gjør datatokenisering? → Den erstatter sensitive kortnumre med ikke-sensitive tilfeldige tokener

Fasit: Kontrollpunkt 2 – sant eller usant

6 **Spørsmål 6** — **Riktig svar: Usant**

MERKNAD TIL LÆREREN

Maskering endrer testkopier eller skjuler verdier ved spørringstidspunktet; produksjonsregistrene forblir uendret.

7 **Spørsmål 7** — **Riktig svar: Sant**

MERKNAD TIL LÆREREN

Sikkerhetskopier utenfor lokasjonen må isoleres fra bedriftens hovednettverk for å hindre spredning av løsepengevirus.

8 **Spørsmål 8** — **Riktig svar: Usant**

MERKNAD TIL LÆREREN

TLS-sertifikater beskytter data under overføring; lagrede data trenger disk-, fil- eller databasekryptering.

9 **Spørsmål 9** — **Riktig svar: Sant**

MERKNAD TIL LÆREREN

Zero Trust Network Access (ZTNA) verifiserer identiteten til hver bruker før databasetilgang gis.

10 **Spørsmål 10** — **Riktig svar: Sant**

MERKNAD TIL LÆREREN

Tokenisering basert på hvelv holder de opprinnelige verdiene i et sikkert tokenhvelv som kobler hvert token tilbake til dataene sine.

Fasit for ordforråd og vurderingsmatrise

Rettemal for læreren: Gi 1 poeng for hver riktige kobling (totalt 8 poeng) og hvert kontekstbegrep (totalt 6 poeng).

KONTROLLPUNKT 4: FASIT – KOBLE BEGREPER

B 1. KRYPTERING	A 2. SIKKERHETSKOPI	H 3. MINIMERING	F 4. TILGANG
C 5. SIKKERHETSTILSTAND	E 6. DATABRUDD	D 7. OVERHOLDELSE	G 8. MASKERING

KONTROLLPUNKT 3: FASIT – NØKKELBEGREPER

1 MASKERING	2 I HVILE	3 OVERFØRING	4 TILGANG
5 SIKKERHETSKOPI	6 SIKKERHETSNIVÅ		

KONTROLLPUNKT 6, ALTERNATIV: FASIT – KOBLE ORD

1 F – SIKKERHETSBRUDD	2 H – MASKERING	3 D – TILGANG	4 E – SIKKERHETSNIVÅ
5 G – SAMSVAR	6 C – DATAMINIMERING	7 A – KRYPTERING	8 B – SIKKERHETSKOPI

DISKUSJONSNOTATER TIL LÆRERE

Nøkkelbegreper:
Kontroller at elevene kan forklare KRYPTERING, SIKKERHETSKOPI og MINIMERING med egne ord og gi et eksempel på hvert.

Casestudier:
Be elevene begrunne anbefalingene sine med fakta fra arbeidsarket i stedet for antakelser.

Kildevurdering:
La elevene kontrollere minst én påstand mot kildene i arbeidsarket, og drøft hvorfor tall, priser og regler kan endre seg over tid.

Fasit for oppgavene og merknader til læreren

LØSNING PÅ ORDSØKET

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

KRYSSORDLØSNING

					S									
D	A	T	A	M	I	N	I	M	E	R	I	N	G	
					K									
	S	I	K	K	E	R	H	E	T	S	N	I	V	Å
					E									
S	I	K	K	E	R	H	E	T	S	B	R	U	D	D
					H									
	M	A	S	K	E	R	I	N	G					T
			A		T									I
			M		S									L
			S		K	R	Y	P	T	E	R	I	N	G
			V		O									A
			A		P									N
			R		I									G

LÆRERVEILEDNING FOR KRYSSORDLØSNINGER

VANNRETT

2 vannrett: DATAMINIMERING Å begrense innsamlingen av personopplysninger til det absolutt nødvendige minimum for driften (14 bokstaver)

3 vannrett: SIKKERHETSNIVÅ Organisasjonens samlede sikkerhetsstatus og forsvarsberedskap i skyen (14 bokstaver)

4 vannrett: SIKKERHETSBRUDD Sikkerhetshendelse der beskyttede data åpnes eller utleveres uten tillatelse (15 bokstaver)

5 vannrett: MASKERING Å erstatte sensitive tegn i databasefelt for å beskytte personers identitet (9 bokstaver)

8 vannrett: KRYPTERING Omforming av klartekst til uleselig chiffertekst slik at avskjærte data forblir private (10 bokstaver)

LODDRETT

1 loddrett: SIKKERHETSKOPI Å lage sikre kopier utenfor stedet som kan gjenopprettes ved systemfeil (14 bokstaver)

6 loddrett: SAMSVAR Å oppfylle regulatoriske standarder som GDPR eller CCPA ved håndtering av private brukeropplysninger (7 bokstaver)

7 loddrett: TILGANG Å begrense lese- og skrivetillatelser i databasen til autentiserte brukerroller (7 bokstaver)

Fasit for kodeord og chiffer

Fasit for vokabularøvelsen med ordstokking og den hemmelige chifferutfordringen.

FASIT: BOKSTAVBLANDING

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. S T I V E Å S N K H E R I K — **SIKKERHETSNIVÅ**
4. R A V S A S M — **SAMSVAR**
5. S K O I E T E I R K H S P K — **SIKKERHETSKOPI**
6. N L A T G G I — **TILGANG**
7. S B H T S R I K D R U D K E E — **SIKKERHETSBRUDD**
8. G E N M K A R I S — **MASKERING**

FASIT TIL DEN HEMMELIGE CHIFFERUTFORDRINGEN

"BESKYTT DINE PRIVATE DATA MED SIKRE KONTROLLER"

Fasit til casestudiene

A Casestudie 1: Oppgradering av kryptering av bedriftsdatabase i hvile

Løsning for læreren

RETTEVEILEDNING

Elevsvar bør dekke følgende punkter:

- Scenarioanalyse: En nettbutikk lagrer transaksjonsdatabaser i skylagring uten full diskkryptering. En fersk samsvarsrevisjon har pekt på dette som en alvorlig datasikkerhetsrisiko etter CCPA. Utform en gjenopprettingsarkitektur.
- Anbefalt strategi og løsning: Innfør AES-256 fulldiskkryptering i hvile på alle filsystemer. Bruk en sentralisert nøkkeladministrasjonstjeneste (KMS) med automatisk rotasjon, og håndhev strenge IAM-policyer for å kontrollere tilgangen til dekryptering.

B Casestudie 2: Begrensning av løsepengevirus og gjenoppretting av data

Løsning for læreren

RETTEVEILEDNING

Elevsvar bør dekke følgende punkter:

- Scenarioanalyse: Et aktivt løsepengevirusangrep krypterer nettverksstasjoner på et lokalt bedriftsnettverk. Administratoren har oppdaget infeksjonen tidlig. Planlegg trinnene for inneslutning og gjenoppretting.
- Anbefalt strategi og løsning: Isoler det kompromitterte segmentet umiddelbart. Formater de berørte endepunktene og gjenopprett fra den nyeste frakoblede WORM-sikkerhetskopien (write-once-read-many). Verifiser sikkerhetskopiens integritet før du kobler til systemene igjen.