Navn: _____ Dato: _____ Point: _____

Databeskyttelse og sikker lagring i virksomheder

Maskering, tokenisering, kryptering i hvile og under overførsel, offline backup

OVERBLIK OVER DATABESKYTTELSE

SIKRET
DATAKRYPTERING
256-bit AES-standard

OVERHOLDER KRAV
GLOBALE STANDARDER
GDPR- og CCPA-rammer

ZERO-TRUST
ADGANGSPOLITIK
Multifaktorgodkendelse

Velkommen! Denne opgavepakke fører dig gennem standarder og kontroller for databeskyttelse. Du vil udforske kryptering af hele diske, sikker adgangskontrol, fysisk backup, sikkerhedsniveauet i skyen og maskering af data.

OPGAVEARKETS KONTROLPUNKTER

- [ ] **Del 1-4: Lær cybersikkerhed og trusselsforebyggelse.**
- [ ] **Del 5-7: Løs kryds og tværs samt ordjagt.**
- [ ] **Del 8-9: Løs casestudier og chifferudfordring.**
- [ ] **Del 10: Gennemgå grundlæggende og avanceret FAQ.**
- [ ] **Del 11: Udforsk 10 interessante fakta fra virkeligheden.**
- [ ] **Bonus: Tænk hurtigt-udfordring.**

Åbn VPN.com's guide til cybersikkerhed

URL: https://www.vpn.com/da/cybersikkerhed/data-protection/

Din læringsplan for databeskyttelse

- Skeln mellem maskering og tokenisering af data.
- Indfør kryptering i hvile på lagerdrev og kryptering under overførsel med TLS.
- Design offline backup adskilt fra netværket som værn mod ransomware.

VEJLEDNING TIL GUIDEN OM DATABESKYTTELSE

Besvar flervalgs- og sandt/falsk-spørgsmålene, udfyld sætningerne med ord fra ordbanken, match definitionerne, og løs kryds og tværs samt ordjagten. Anvend din viden om databeskyttelse. Slut af med bonusaktiviteten Tænk hurtigt.

DATABESKYTTELSE OG SIKKER LAGRING I VIRKSOMHEDER (INTRODUKTION)

Databeskyttelse sikrer virksomhedens dataaktiver gennem maskering, tokenisering, kryptering af databaser i hvile og sikre transmissionsprotokoller. Netværksisolerede sikkerhedskopier hjælper med at sikre, at vigtige databaser kan gendannes i tilfælde af et aktivt indbrud.

LÆS HVERT KONTROLPUNKT GRUNDIGT, OG VÆLG ELLER SKRIV DET RIGTIGE SVAR.

Kontrolpunkt 1: Flervalgsopgave

1. Hvad er hovedformålet med maskering af data?

- A. At erstatte følsomme oplysninger med opdigtede, men realistiske tegn for at beskytte privatlivet
- B. At komprimere store databasefiler for at spare plads på serveren
- C. At slette gamle kundemails fra arkiverede backups
- D. At skjule databaseserverens offentlige IP-adresse for scanninger

2. Hvilken mekanisme krypterer filer på databaseserverens harddisk?

- A. Kryptering af hele disken i hvile
- B. TLS-håndtryk under overførsel
- C. Regler for videresendelse i dynamisk DNS
- D. Flerfaktorgodkendelse med hardwarenøgler

3. Hvad er data under overførsel?

- A. Datapakker, der bevæger sig gennem routere og switche
- B. Transaktionslogfiler gemt på et offline backupdrev
- C. Arkiverede brugerfiler i et isoleret skyarkiv
- D. Faste konfigurationsfiler på en lokal computer

4. Hvorfor er jævnlig offline backup afgørende mod ransomware?

- A. Den giver en ren kopi, så filer kan gendannes uden at betale løsesum
- B. Den forhindrer hackere i at scanne åbne porte
- C. Den øger båndbredden på det lokale netværk
- D. Den automatiserer logning af cookiesamtykke i browsere

5. Hvad gør tokenisering af data?

- A. Den erstatter følsomme kortnumre med tilfældige, ufarlige tokens
- B. Den sender trafikken gennem flere sikre onion-noder
- C. Den scanner mapper for signaturbaseret malware
- D. Den reviderer administratorernes logintider

Kontrolpunkt 2: Sandt eller falsk-udfordring

6 Spørgsmål 6

6. Maskering ændrer posterne i produktionsdatabasen permanent.

○ Sandt ○ Falsk

7 Spørgsmål 7

7. Backup uden for huset skal være adskilt fra virksomhedens netværk, så ransomware ikke spreder sig.

○ Sandt ○ Falsk

8 Spørgsmål 8

8. SSL/TLS-certifikater beskytter databaser ved at kryptere data i hvile på fysiske medier.

○ Sandt ○ Falsk

9 Spørgsmål 9

9. Zero trust-netværksadgang (ZTNA) kontrollerer hver brugers identitet, før der gives adgang til databasen.

○ Sandt ○ Falsk

10 Spørgsmål 10

10. Vault-baseret tokenisering gemmer de oprindelige kortværdier i en sikker, central token-boks.

○ Sandt ○ Falsk

Kontrolpunkt 3: Indsæt nøglebegreber

Læs hver sætning nedenfor, og udfyld det tomme felt med det rigtige ord fra ordbanken.

1. At erstatte personnavne med realistiske pladsholdere kaldes _____ af data.
2. Kryptering af fysiske lagerblokke beskytter databasens data i _____ .
3. TLS-protokoller krypterer aktive datapakker under _____ .
4. Rollebaserede tilladelser begrænser, hvilke brugere der får _____ til databasen.
5. Gendannelse af rene firmafiler efter et brud kræver en sikker offline _____ .
6. En revision af skykonfigurationer vurderer organisationens samlede _____ .

ORDBANK MED FAGUDTRYK

BACKUP BRUD DATAMINIMERING HVILE MASKERING RETTIGHEDER SIKKERHED TRANSIT

Skriv dine svar her:

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

Kontrolpunkt 4: Match sikkerhedsbegreber

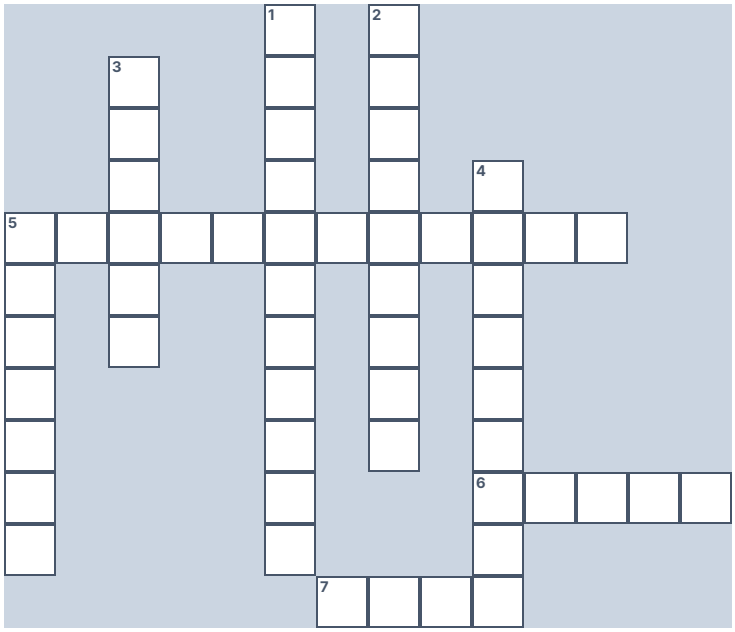
MATCH BEGREBER OG DEFINITIONER

Match hvert fagudtryk til venstre med den rigtige definition til højre ved at skrive det tilhørende bogstav (A-H) i indtastningsfeltet.

	1. KRYPTERING	A	Sikre kopier uden for huset, der kan gendannes ved systemfejl.
	2. BACKUP	B	Omdannelse af klartekst til ulæselig chiffertekst, så opsnappede data forbliver private.
	3. DATAMINIMERING	C	Den samlede sikkerhed og forsvarsberedskab i organisationens sky.
	4. ADGANG	D	Overholdelse af regler som GDPR eller CCPA for private brugeroplysninger.
	5. TILSTAND	E	Sikkerhedshændelse, hvor beskyttede data tilgås eller videregives uden tilladelse.
	6. BRUD	F	Læse- og skriverettigheder forbeholdt godkendte brugerroller.
	7. OVERHOLDELSE	G	Udskiftning af følsomme tegn i databasefelter for at beskytte identiteter.
	8. MASKERING	H	Indsamling af persondata begrænset til det absolut nødvendige.

Kontrolpunkt 5: Kryds og tværs

Løs kryds og tværs ved at skrive bogstaver i de aktive hvide felter. Tallene svarer til nøglerne nedenfor.



VANDRETTE NØGLER

5. Erstatning af kortnumre med tilfældige tokens uden følsom værdi (12)

6. Tilstanden for gemte data på lagerdrev, som diskkryptering beskytter (5)

7. Hændelse, hvor beskyttede data tilgås eller videregives uden tilladelse (4)

LODRETTE NØGLER

1. Læse- og skriveadgang til databasen, begrænset til godkendte brugerroller (11)

2. Erstatning af følsomme tegn i databasefelter for at beskytte personers identitet (9)

3. Sikre kopier af data uden for stedet, som kan gendannes ved systemnedbrud (6)

4. Organisationens samlede beskyttelsesniveau og forsvarsparathed i skyen (9)

5. Tilstanden for datapakker undervejs, som TLS krypterer (7)

Kontrolpunkt 5, alternativ: Tilgængelige krydsordsnøgler

Brugere af skærmlæser og tastatur kan skrive krydsordssvarene direkte i tekstfelterne nedenfor.

VANDRETTE NØGLER

5 vandret: Erstatning af kortnumre med tilfældige tokens uden følsom værdi (12 bogstaver):

6 vandret: Tilstanden for gemte data på lagerdrev, som diskkryptering beskytter (5 bogstaver):

7 vandret: Hændelse, hvor beskyttede data tilgås eller videregives uden tilladelse (4 bogstaver):

LODRETTE NØGLER

1 lodret: Læse- og skriveadgang til databasen, begrænset til godkendte brugerroller (11 bogstaver):

2 lodret: Erstatning af følsomme tegn i databasefelter for at beskytte personers identitet (9 bogstaver):

3 lodret: Sikre kopier af data uden for stedet, som kan gendannes ved systemnedbrud (6 bogstaver):

4 lodret: Organisationens samlede beskyttelsesniveau og forsvarsparathed i skyen (9 bogstaver):

5 lodret: Tilstanden for datapakker undervejs, som TLS krypterer (7 bogstaver):

Kontrolpunkt 6: Skjult ordjagt

Find de 8 vigtige fagudtryk, der er skjult i gitteret nedenfor. Ordene kan stå vandret, lodret eller diagonalt.

W U V F M K B T A B C Q Æ M L

R Æ E M Æ W L R E S B O K E J

E O L O L S R A H O A O S T U

D W I V H C U N S Q C I U C Y

E E V V Ø X C S Å Y K G L M I

H D H Å D O E I S Z U R C A W

G U B A Å P E T S M P A E S Q

I R E F H J D T I S N F J K U

T B Å U G S Y F K A A S Q E O

T R W Æ S L T W K U D O Ø R B

E T O K E N I S E R I N G I G

R U Z Z K A T Å R Ø Ø M H N J

O T L N N V Q I H S S H Å G A

Q X G X C Ø T Ø E B I N Å H K

P R P Z C N Å Ø D G Æ Q Y X M

ORDLISTE MED FAGUDTRYK

MASKERING, HVILE, TRANSIT, RETTIGHEDER, BACKUP, SIKKERHED, BRUD, TOKENISERING

Kontrolpunkt 6, alternativ: Tilgængelig ordmatchning

Match hvert af de 8 fagudtryk fra ordjagten med den rigtige definition ved at skrive bogstavet (A-H) i det tomme felt.

FAGUDTRYK
A. MASKERING
B. HVILE
C. TRANSIT
D. RETTIGHEDER
E. BACKUP
F. SIKKERHED
G. BRUD
H. TOKENISERING

DEFINITIONER OG MATCHFELTER

1. Organisationens samlede beskyttelsesniveau og forsvarsparathed i skyen.
2. Erstatning af kortnumre med tilfældige tokens uden følsom værdi.
3. Læse- og skriveadgang til databasen, begrænset til godkendte brugerroller.
4. Sikre kopier af data uden for stedet, som kan gendannes ved systemnedbrud.
5. Hændelse, hvor beskyttede data tilgås eller videregives uden tilladelse.
6. Tilstanden for datapakker undervejs, som TLS krypterer.
7. Erstatning af følsomme tegn i databasefelter for at beskytte personers identitet.
8. Tilstanden for gemte data på lagerdrev, som diskkryptering beskytter.

Kontrolpunkt 7: Bogstavrod-udfordring

Sæt bogstaverne nedenfor i den rigtige rækkefølge, og find vigtige cybersikkerhedsbegreber. Skriv dine svar i indtastningsfelterne.

1. **REKAMINGS** _____

2. **TATISNR** _____

3. **BCKPUA** _____

4. **DUBR** _____

5. **IEHLV** _____

6. **IRGEEDREHTT** _____

7. **RSEDHKIEK** _____

8. **EKNISGTIONRE** _____

Bonusaktivitet: Tænk hurtigt

3 SVAR I HVER KATEGORI. DEN FØRSTE, DER UDFYLDER HELE LISTEN, VINDER.

1	Ting, du tager backup af			
2	Ord, der har med cybersikkerhed at gøre			
3	Personer, der må se følsomme data			
4	Måder at slette data sikkert			
5	Steder, hvor data gemmes			
6	Ting, der bør krypteres			
7	Data, et hospital skal beskytte			
8	Typer af backup			
9	Oplysninger, du aldrig bør dele			
10	Advarselstegn i en e-mail			
11	Sikkerhedsvaner, du kan starte i dag			
12	Personer, du kan spørge om it-hjælp			
13	Enheder, der kan blive hacket			
14	Måder at beskytte data på			
15	Ting, der kan ødelægge data			

Kontrolpunkt 8: Casestudier om cybersikkerhed

Anvend de begreber, du har lært, til at løse de virkelige scenarier nedenfor.

CASESTUDIE 1: KRYPTERING AF DATABASER I HVILE

👷

Scenarie: En webbutik gemmer transaktionsdatabaser i skylager uden fuld diskkryptering. En nylig revision af regeloverholdelsen markerede dette som en alvorlig CCPA-datasikkerhedsrisiko. Design en gendannelsesarkitektur.

Diskussion: Analysér risiciene i forhold til CCPA, og foreslå en strategi for kryptering i hvile.

CASESTUDIE 2: INDDÆMNING AF RANSOMWARE OG GENDANNELSE

👷

Scenarie: Et aktivt ransomwareangreb krypterer netværksdrev på virksomhedens lokale netværk. Administratoren har opdaget smitten tidligt. Planlæg inddæmning og gendannelse.

Diskussion: Beskriv de umiddelbare tiltag, og planlæg en sikker gendannelse.

Kontrolpunkt 9: Afkod chifferet

En cybersikkerhedsekspert beskytter netværkets aktiver mod trusselsaktører online. Brug bogstav-til-tal-nøglen nedenfor til at afkode beskeden ved at skrive de tilsvarende bogstaver i de tomme felter.

BOGSTAV-TIL-TAL-KRYPTERINGSNØGLE

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

8	15	12	4		5	14		2	1	3	11	21	16

15	6	6	12	9	14	5

Afkodet besked:

TIP: HVERT TAL ANGIVER BOGSTAVETS PLADS I ALFABETET (F.EKS. 1 = A, 2 = B, 26 = Z, 27 = Æ, 28 = Ø, 29 = Å).

Kontrolpunkt 10: Grundlæggende FAQ om cybersikkerhed (del A)

Gennemgå almindelige spørgsmål og svar om afværgelse af trusler online.

Q1: Hvad er databeskyttelse?

Beskyttelse af personlige data og forretningsdata mod uautoriseret adgang, tab eller ødelæggelse med tekniske kontroller.

Q2: Hvorfor er kryptering af hele disken vigtig?

Den beskytter de gemte data, så ingen kan læse dem, selv hvis harddisken bliver stjålet.

Q3: Hvad er forskellen på kryptering i hvile og under overførsel?

Kryptering i hvile beskytter gemte filer, mens kryptering under overførsel beskytter pakker på vej gennem netværket.

Q4: Hvad er maskering af data?

Følsomme oplysninger (som kortnumre) erstattes med opdigtede, men realistiske data til test uden at afsløre ægte poster.

Q5: Hvorfor er offline backup vigtig?

Den holder en ren kopi af dine filer isoleret fra netværket, hvilket hjælper med at beskytte dine sikkerhedskopier mod at blive krypteret af ransomware.

Kontrolpunkt 10: Grundlæggende FAQ om cybersikkerhed (del B)

Gennemgå almindelige spørgsmål og svar om afværgelse af trusler online.

Q6: Hvad er et tokenarkiv?

En sikker, isoleret database, der kobler tilfældige tokens til de oprindelige følsomme værdier (som kortnumre).

Q7: Hvad betyder zero trust-adgang til databaser?

At hver brugers identitet og enhed kontrolleres ved hvert login i stedet for at stole på alle inden for netværket.

Q8: Hvordan beskytter TLS data under overførsel?

TLS krypterer indholdet i TCP-sessionen, så ondsindede aktører på offentlige net ikke kan aflytte eller ændre pakkerne.

Q9: Hvad er revision af databaseadgang?

Løbende registrering af forespørgsler og logins for at opdage uautoriseret adgang eller afvigelser.

Q10: Hvad er en revision af sikkerheden i skyen?

En gennemgang af skykonfigurationer, der finder åbne porte, forkerte adgangsregler og huller i overholdelsen.

Kontrolpunkt 10: Avanceret FAQ om sikkerhed (del C)

Udforsk avancerede tekniske aspekter af sikkerhedsrammer, malwareanalyse og overholdelse af databeskyttelsesregler.

Q1: Hvordan virker konvolutkryptering?

Data krypteres med en datanøgle, som derefter krypteres med en hovednøgle; det gør opbevaring og udskiftning af nøgler enklere.

Q2: Hvad er homomorf kryptering?

En avanceret metode, hvor der kan regnes direkte på krypterede data uden at dekryptere dem først.

Q3: Hvorfor krypteres enkelte kolonner i databasen?

Følsomme kolonner (som personnumre) krypteres hver for sig og er beskyttet, selv hvis administratorer kan læse tabellen.

Q4: Hvad er forebyggelse af datatab (DLP)?

Software, der overvåger netværkets udgange og stopper uautoriserede overførsler af følsomme filer.

Q5: Hvordan beskytter WORM-backups (write-once-read-many) mod ransomware?

WORM-backup forhindrer, at filer slettes eller ændres i en fastsat periode, så ransomware ikke kan kryptere eksisterende backups.

Kontrolpunkt 10: Avanceret FAQ om sikkerhed (del D)

Udforsk avancerede tekniske aspekter af sikkerhedsrammer, malwareanalyse og overholdelse af databeskyttelsesregler.

Q6: Hvad er risikoen ved at genbruge nøgler?

Bruges samme nøgle i flere databaser, afslører ét kompromitteret nøglepar dem alle.

Q7: Hvordan hjælper tokenisering med at overholde CCPA?

Tokens pseudonymiserer poster i ikke-produktionssystemer og begrænser eksponeringen ved brud, men tokeniserede data kan stadig være personoplysninger.

Q8: Hvorfor er klassificering af data afgørende?

Den inddeler filer efter følsomhedsniveau og hjælper organisationer med at anvende den stærkeste kryptering og adgangskontrol på højrisikodata.

Q9: Hvad er formålet med at udskifte nøgler?

Jævnlig udskiftning begrænser mængden af gamle data, der afsløres, hvis en nøgle en dag bliver knækket.

Q10: Hvordan beskytter sikre enklaver forespørgsler i hukommelsen?

De isolerer forespørgsler i hukommelse beskyttet af processoren, så værtens administratorer ikke kan se klartekst i RAM.

Del 11: 10 fakta og indsigter om cybersikkerhed fra virkeligheden

Gennemgå fakta om sikkerhedsbrud, forsvarsmekanismer og krav til overholdelse.

1. SIKKERHEDSINDSIGT

GDPR trådte i kraft i maj 2018 og ændrede, hvordan websteder verden over håndterer cookiesamtykke og persondata.

2. SIKKERHEDSINDSIGT

En bøde for brud på GDPR kan nå 20 millioner euro eller 4 % af den globale omsætning. [4]

3. SIKKERHEDSINDSIGT

CCPA trådte i kraft i januar 2020 og gav banebrydende digitale rettigheder til forbrugere i USA.

4. SIKKERHEDSINDSIGT

Dataminimering mindsker lagerforbruget, sænker driftsomkostningerne og begrænser skaden ved brud.

5. SIKKERHEDSINDSIGT

Kryptografisk makulering løser problemet med sletning i backups ved at slette nøglerne i stedet for at redigere gamle bånd.

6. SIKKERHEDSINDSIGT

De fleste lande i verden har nu vedtaget love om beskyttelse af personoplysninger for at beskytte forbrugernes ret til privatliv.

7. SIKKERHEDSINDSIGT

Samtykkeformularer med forudafkrydsede felter er udtrykkeligt forbudt efter europæiske regler.

8. SIKKERHEDSINDSIGT

GDPR kræver, at brud på persondatasikkerheden anmeldes til tilsynsmyndigheden inden for 72 timer efter, at man er blevet opmærksom på det, hvor det er muligt. [3]

9. SIKKERHEDSINDSIGT

Hashing af adgangskoder med langsomme algoritmer som bcrypt eller Argon2 gør offline-knækning af stjålne hashværdier langt sværere. [6]

10. SIKKERHEDSINDSIGT

Data i hvile er gemte databasefiler, mens data under overførsel er pakker på vej gennem netværket.

Tekniske referencer og kilder

Studieguiden og de interaktive opgaver er sammensat ud fra globale standarder fra NIST, OWASP og regler om databeskyttelse.

VIDENSKABELIGE OG BRANCHEMÆSSIGE REFERENCER

[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

Facitliste: Kontrolpunkt 1 – Flervalg

1 Spørgsmål 1

Rigtigt svar: A

UNDERVISNINGSNOTE

Hvad er hovedformålet med maskering af data? → At erstatte følsomme oplysninger med opdigtede, men realistiske tegn for at beskytte privatlivet

2 Spørgsmål 2

Rigtigt svar: A

UNDERVISNINGSNOTE

Hvilken mekanisme krypterer filer på databaseserverens harddisk? → Kryptering af hele disken i hvile

3 Spørgsmål 3

Rigtigt svar: A

UNDERVISNINGSNOTE

Hvad er data under overførsel? → Datapakker, der bevæger sig gennem routere og switche

4 Spørgsmål 4

Rigtigt svar: A

UNDERVISNINGSNOTE

Hvorfor er jævnlig offline backup afgørende mod ransomware? → Den giver en ren kopi, så filer kan gendannes uden at betale løsesum

5 Spørgsmål 5

Rigtigt svar: A

UNDERVISNINGSNOTE

Hvad gør tokenisering af data? → Den erstatter følsomme kortnumre med tilfældige, ufarlige tokens

Facitliste: Kontrolpunkt 2 – Sandt eller falsk

6 Spørgsmål 6

Rigtigt svar: Falsk

UNDERVISNINGSNOTE

Maskering ændrer testkopier eller skjuler værdier, når der foretages forespørgsler; produktionsdata forbliver uændrede.

7 Spørgsmål 7

Rigtigt svar: Sandt

UNDERVISNINGSNOTE

Backup uden for huset skal være adskilt fra virksomhedens netværk, så ransomware ikke spreder sig.

8 Spørgsmål 8

Rigtigt svar: Falsk

UNDERVISNINGSNOTE

TLS-certifikater beskytter data under overførsel; data i hvile kræver kryptering af disk, filer eller database.

9 Spørgsmål 9

Rigtigt svar: Sandt

UNDERVISNINGSNOTE

Zero trust-netværksadgang (ZTNA) kontrollerer hver brugers identitet, før der gives adgang til databasen.

10 Spørgsmål 10

Rigtigt svar: Sandt

UNDERVISNINGSNOTE

Vault-baseret tokenisering gemmer de oprindelige værdier i en sikker token-boks, der knytter hvert token til dets data.

Ordfacit og bedømmelsesvejledning

Bedømmelsesvejledning til underviseren: Giv 1 point for hver korrekt matchning (8 point i alt) og hvert korrekt kontekstord (6 point i alt).

KONTROLPUNKT 4: FACIT TIL BEGREBSMATCHNING

B 1. KRYPTERING	A 2. BACKUP	H 3. DATAMINIMERING	F 4. ADGANG
C 5. TILSTAND	E 6. BRUD	D 7. OVERHOLDELSE	G 8. MASKERING

KONTROLPUNKT 3: FACIT TIL NØGLEBEGREBER

1 MASKERING	2 HVILE	3 TRANSIT	4 RETTIGHEDER
5 BACKUP	6 SIKKERHED		

KONTROLPUNKT 6, ALTERNATIV: FACIT TIL ORDMATCHNING

1 F – SIKKERHED	2 H – TOKENISERING	3 D – RETTIGHEDER	4 E – BACKUP
5 G – BRUD	6 C – TRANSIT	7 A – MASKERING	8 B – HVILE

DISKUSSIONSNOTER TIL UNDERVISERE

Fagbegreber:
Kontrollér, at eleverne kan forklare KRYPTERING, BACKUP og DATAMINIMERING med egne ord og give et eksempel på hvert begreb.

Casestudier:
Bed eleverne begrunde deres anbefalinger med fakta fra opgavearket frem for antagelser.

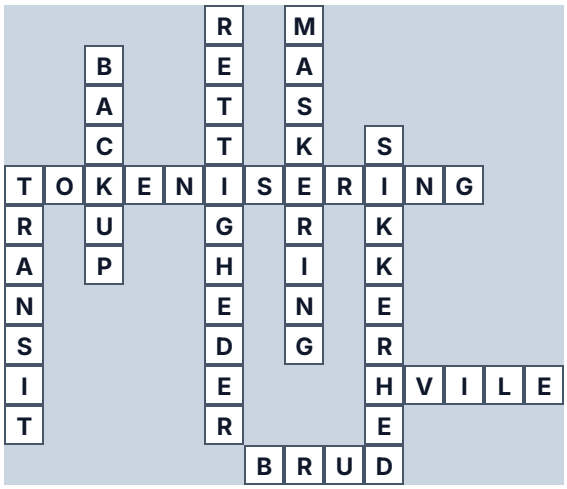
Kildekritik:
Lad eleverne efterprøve mindst én påstand mod referencerne i opgavearket, og drøft, hvorfor tal, priser og regler kan ændre sig over tid.

Facit til opgaver og undervisernoter

LØSNING PÅ ORDJAGT

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

LØSNING PÅ KRYDS OG TVÆRS



UNDERVISERVEJLEDNING TIL KRYDSORDSLØSNINGER

VANDRETTE NØGLER

5 vandret: TOKENISERING Erstatning af kortnumre med tilfældige tokens uden følsom værdi (12 bogstaver)

6 vandret: HVILE Tilstanden for gemte data på lagerdrev, som diskkryptering beskytter (5 bogstaver)

7 vandret: BRUD Hændelse, hvor beskyttede data tilgås eller videregives uden tilladelse (4 bogstaver)

LODRETTE NØGLER

1 lodret: RETTIGHEDER Læse- og skriveadgang til databasen, begrænset til godkendte brugerroller (11 bogstaver)

2 lodret: MASKERING Erstatning af følsomme tegn i databasefelter for at beskytte personers identitet (9 bogstaver)

3 lodret: BACKUP Sikre kopier af data uden for stedet, som kan gendannes ved systemnedbrud (6 bogstaver)

4 lodret: SIKKERHED Organisationens samlede beskyttelsesniveau og forsvarsparathed i skyen (9 bogstaver)

5 lodret: TRANSIT Tilstanden for datapakker undervejs, som TLS krypterer (7 bogstaver)

Facit til bogstavrod og chiffer

Bedømmelsesfacit til bogstavrod-øvelsen og den hemmelige chifferudfordring.

FACIT TIL BOGSTAVROD

1. REKAMINGS	MASKERING	5. IEHLV	HVILE
2. TATISNR	TRANSIT	6. IRGEEDREHTT	RETTIGHEDER
3. BCKPUA	BACKUP	7. RSEDHKIEK	SIKKERHED
4. DUBR	BRUD	8. EKNISGTIONRE	TOKENISERING

FACIT TIL HEMMELIG CHIFFERUDFORDRING

"HOLD EN BACKUP OFFLINE"

Facit til casestudier

A Casestudie 1: Kryptering af databaser i hvile

Underviserens løsning

BEDØMMELSESVEJLEDNING

Elevens svar bør dække følgende punkter:

- Scenarieanalyse: En webbutik gemmer transaktionsdatabaser i skylager uden fuld diskkryptering. En nylig revision af regeloverholdelsen markerede dette som en alvorlig CCPA-datasikkerhedsrisiko. Design en gendannelsesarkitektur.
- Anbefalet strategi og løsning: Indfør AES-256-kryptering af hele disken på alle filsystemer. Brug en central nøgletjeneste (KMS) med automatisk udskiftning og strenge IAM-regler for, hvem der må dekryptere.

B Casestudie 2: Inddæmning af ransomware og gendannelse

Underviserens løsning

BEDØMMELSESVEJLEDNING

Elevens svar bør dække følgende punkter:

- Analyse af scenariet: Et aktivt ransomwareangreb krypterer netværksdrev i virksomheden. Administratoren har opdaget smitten tidligt.
- Anbefalet strategi og løsning: Isolér det ramte segment med det samme. Formatér de ramte enheder, og gendan fra den nyeste offline WORM-backup. Kontrollér backuppen, før systemerne kobles på igen.