Navn: _____ Dato: _____ Point: _____

Zero trust-arkitektur og sikkerhed

Løbende verifikation, mikrosegmentering af netværket, identitets- og adgangsstyring (IAM), mindste rettighed og tilstandskontrol.

OVERBLIK OVER ZERO TRUST

SIKRET
DATAKRYPTERING
256-bit AES-standard

OVERHOLDER KRAV
GLOBALE STANDARDER
GDPR- og CCPA-rammer

ZERO-TRUST
ADGANGSPOLITIK
Multifaktorgodkendelse

Velkommen! Denne opgavepakke fører dig gennem zero trust-arkitektur og sikkerhed. Du vil udforske løbende kontrol, mikrosegmentering, identitets- og adgangsstyring (IAM), mindste rettigheder og revision af sessioner.

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/zero-trust-cybersikkerhed/

Din læringsplan for zero trust

- Forstå kerneprincippet om løbende kontrol.
- Indfør mikrosegmentering og mindste rettigheder.
- Opsæt kontrol af enheders tilstand og revision af aktive sessioner.

VEJLEDNING TIL GUIDEN OM ZERO TRUST

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 zero trust-arkitektur. Slut af med bonusaktiviteten Tænk hurtigt.

ZERO TRUST-ARKITEKTUR OG SIKKERHED (INTRODUKTION)

Zero trust erstatter de gamle perimetermodeller med en streng regel: 'stol aldrig, kontrollér altid'. Mikrosegmentering, identitets- og adgangsstyring (IAM), mindste rettigheder og kontrol af enheder stopper angriberes bevægelse inde i netværket.

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

Kontrolpunkt 1: Flervalgsopgave

1. Hvad er kerneprincippet i zero trust?

- A. Stol aldrig, kontrollér altid hver anmodning uanset kilde
- B. At al trafik inden for firewallen er sikker
- C. At gemme databaser ukrypteret for hastighedens skyld
- D. At godkende e-mail kun med SPF

2. Hvad er mikrosegmentering?

- A. Opdeling af netværket i små, isolerede zoner, der begrænser angriberes bevægelse
- B. Kryptering af netkort under overførsel
- C. Alle servere på én offentlig IP-adresse
- D. Overvågning af tastetryk i browseren

3. Hvad er princippet om mindste rettigheder?

- A. At brugere kun får den adgang, deres arbejde kræver
- B. At alle brugere får alle rettigheder som standard
- C. At tillade anonymt login på databaseservere
- D. At opsætte offentlige routere uden adgangskode

4. Hvad er identitets- og adgangsstyring (IAM)?

- A. Rammer, der styrer digitale identiteter og rettigheder
- B. Antivirus, der scanner lokale mapper
- C. Et backupsystem med afkoblede medier
- D. En protokol, der afviser forfalskede domæner

5. Hvad betyder løbende godkendelse?

- A. Gentagen kontrol af identitet og enhedens tilstand under en aktiv session
- B. Ny hovedadgangskode hvert 10. minut
- C. Hashing af poster med flere algoritmer
- D. Kryptering af pakker med TLS-nøgler

Kontrolpunkt 2: Sandt eller falsk-udfordring

6 Spørgsmål 6

6. Zero trust går ud fra, at al trafik inden for firewallen er sikker.

○ Sandt ○ Falsk

7 Spørgsmål 7

7. Mikrosegmentering begrænser angribernes mulighed for at bevæge sig lateralt mellem interne servere.

○ Sandt ○ Falsk

8 Spørgsmål 8

8. Mindste rettigheder giver adgang til alle databasefiler som standard.

○ Sandt ○ Falsk

9 Spørgsmål 9

9. Løbende kontrol tjekker enhedens tilstand og loginoplysninger under hele sessionen.

○ Sandt ○ Falsk

10 Spørgsmål 10

10. Zero trust mindsker skaden ved kompromitterede firmalogins.

○ Sandt ○ Falsk

Kontrolpunkt 3: Indsæt nøglebegreber

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

1. Krav om legitimation ved hvert adgangspunkt kaldes løbende _____ .
2. Opdeling af firmanetværket i små zoner kaldes mikro- _____ .
3. Digitale identiteter og adgangskontrol styres med _____ systemet.
4. Begrænsning af brugerrettigheder følger princippet om mindste _____ .
5. Kontrol af tilsluttede enheder vurderer enhedens _____ .
6. Logning og gennemgang af aktive sessioner kaldes _____ .

ORDBANK MED FAGUDTRYK

FIREWALL IAM RETTIGHEDER REVISION ROUTER SEGMENTERING TILSTAND VERIFIKATION

Skriv dine svar her:

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

Kontrolpunkt 4: Match sikkerhedsbegreber

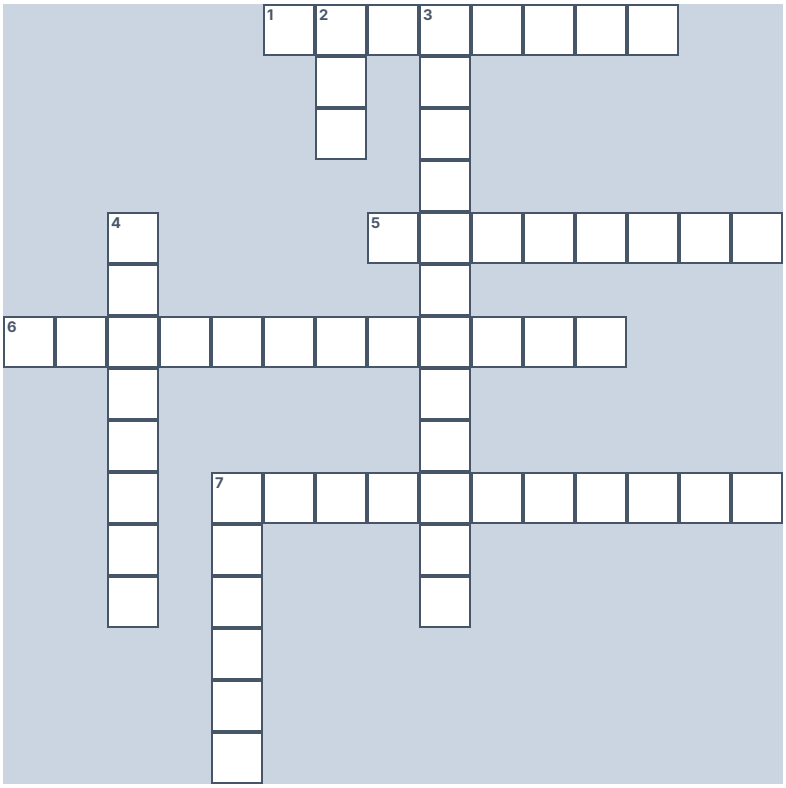
MATCH BEGREBER OG DEFINITIONER

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

☐	1. VERIFIKATION	A	Styring af brugeres identitet og adgang.
☐	2. SEGMENTERING	B	Princippet om mindst mulig adgang.
☐	3. IAM	C	Videresendelse af datapakker.
☐	4. RETTIGHEDER	D	Barriere mod det eksterne netværk.
☐	5. TILSTAND	E	Gennemgang af loggede sessioner.
☐	6. REVISION	F	Opdeling af netværket i interne zoner.
☐	7. FIREWALL	G	Altid at kontrollere brugerens legitimation.
☐	8. ROUTER	H	Vurdering af enhedens tilstand.

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

1. Det, der vurderes, når tilsluttede enheder kontrolleres (8)

5. Logning og gennemgang af aktive sessioner (8)

6. Løbende kontrol af legitimation ved hvert adgangspunkt (12)

7. Princippet om mindste … begrænser, hvad brugere må (11)

LODRETTE NØGLER

2. Forkortelse for styring af digitale identiteter og adgang (3)

3. Mikro…: opdeling af netværket i små, isolerede zoner (12)

4. Barriere, der beskytter mod det eksterne netværk (8)

7. Enhed, der videresender datapakker mellem net (6)

Kontrolpunkt 5, alternativ: Tilgængelige krydsordsnøgler

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

VANDRETTE NØGLER

1 vandret: Det, der vurderes, når tilsluttede enheder kontrolleres (8 bogstaver):

5 vandret: Logning og gennemgang af aktive sessioner (8 bogstaver):

6 vandret: Løbende kontrol af legitimation ved hvert adgangspunkt (12 bogstaver):

7 vandret: Princippet om mindste … begrænser, hvad brugere må (11 bogstaver):

LODRETTE NØGLER

2 lodret: Forkortelse for styring af digitale identiteter og adgang (3 bogstaver):

3 lodret: Mikro…: opdeling af netværket i små, isolerede zoner (12 bogstaver):

4 lodret: Barriere, der beskytter mod det eksterne netværk (8 bogstaver):

7 lodret: Enhed, der videresender datapakker mellem net (6 bogstaver):

Kontrolpunkt 6: Skjult ordjagt

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

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

ORDLISTE MED FAGUDTRYK

VERIFIKATION SEGMENTERING IAM RETTIGHEDER TILSTAND REVISION FIREWALL ROUTER

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. VERIFIKATION
B. SEGMENTERING
C. IAM
D. RETTIGHEDER
E. TILSTAND
F. REVISION
G. FIREWALL
H. ROUTER

DEFINITIONER OG MATCHFELTER
[ ] 1. Barriere, der beskytter mod det eksterne netværk.
[ ] 2. Logning og gennemgang af aktive sessioner.
[ ] 3. Princippet om mindste ... begrænser, hvad brugere må.
[ ] 4. Mikro...: opdeling af netværket i små, isolerede zoner.
[ ] 5. Enhed, der videresender datapakker mellem net.
[ ] 6. Det, der vurderes, når tilsluttede enheder kontrolleres.
[ ] 7. Forkortelse for styring af digitale identiteter og adgang.
[ ] 8. Løbende kontrol af legitimation ved hvert adgangspunkt.

Kontrolpunkt 7: Bogstavrod-udfordring

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

1. TIAFEKIVORNI
2. MAI
3. SITTADNL
4. ELLAWFIR
5. EIETGGERNSNM
6. IRGEEDREHTT
7. RNSIOEIV
8. URRETO

Bonusaktivitet: Tænk hurtigt

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

1	Oplysninger, du aldrig bør dele			
2	Sikkerhedsvaner, du kan starte i dag			
3	Ting, der tjekkes på en enhed			
4	Ting, der bliver logget			
5	Ord, der har med cybersikkerhed at gøre			
6	Ting, Zero Trust kontrollerer			
7	Steder, hvor du viser id i hverdagen			
8	Måder at bevise, at det er dig			
9	Ting at gøre efter et datalæk			
10	Tegn på, at en computer er inficeret			
11	Grunde til at opdatere software			
12	Adgangsniveauer i et firma			
13	Sikkerhedsværktøjer, du kender			
14	Områder, et netværk kan deles op i			
15	Ordsprog om tillid			

Kontrolpunkt 8: Casestudier om cybersikkerhed

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

CASESTUDIE 1: OVERGANG TIL ZERO TRUST



Scenarie: En stor virksomhed har et fladt internt netværk, hvor enhver enhed på det lokale netværk kan nå alle firmaets servere og databaser.

Diskussion: Design en strategi for mikrosegmentering, der begrænser angriberes bevægelse.

CASESTUDIE 2: INDFØRELSE AF MINDSTE RETTIGHEDER



Scenarie: Revisionslogfiler viser, at midlertidige databasebrugere og menige medarbejdere har fuld læse- og skriveadgang til vigtige regnskabsdatabaser.

Diskussion: Gennemgå og begræns rettighederne i IAM, så princippet om mindste rettigheder overholdes.

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

19	20	15	12		1	12	4	18	9	7

11	15	14	20	18	15	12	12	5	18		1	12	20	9	4

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 zero trust?

En sikkerhedsramme, der går ud fra, at trusler findes både uden for og inden for netværket, og som kræver kontrol af hver anmodning. [1]

Q2: Hvad er grundreglen i zero trust?

Stol aldrig, kontrollér altid.

Q3: Hvad er mikrosegmentering?

Opdeling af netværket i små, sikre logiske segmenter, der styrer trafikken og begrænser brud.

Q4: Hvad er mindste rettigheder?

At brugere kun får de rettigheder, deres opgaver kræver. [2]

Q5: Hvad står IAM for?

Identity and Access Management (identitets- og adgangsstyring).

Kontrolpunkt 10: Grundlæggende FAQ om cybersikkerhed (del B)

Gennemgå almindelige spørgsmål og svar om afværgelse af trusler online.

Q6: Hvordan hjælper kontrol af enhedens tilstand?

Den bekræfter, at enheden er opdateret, kører antivirus og er sikker, før der gives adgang.

Q7: Hvad er lateral bevægelse?

Når angribere bevæger sig fra den første ramte enhed videre til mere værdifulde systemer.

Q8: Erstatter zero trust firewalls?

Nej, den styrker dem med kontrol af identitet og interne firewalls mellem segmenter.

Q9: Hvad er løbende godkendelse?

Kontrol af brugerens identitet under hele sessionen, ikke kun ved login.

Q10: Hvorfor er et fladt netværk farligt?

I et fladt netværk giver én kompromitteret enhed let adgang til alle databaser.

Kontrolpunkt 10: Avanceret FAQ om sikkerhed (del C)

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

Q1: Hvordan gør zero trust op med perimetermodellen?

Den erstatter den forældede model med borg og voldgrav og flytter forsvaret fra netværkets grænse til identiteter og ressourcer.

Q2: Hvad er et policy decision point (PDP)?

Den del af systemet, der vurderer anmodninger mod reglerne og afgør, om der gives adgang.

Q3: Hvad er et policy enforcement point (PEP)?

Det led (f.eks. en gateway eller proxy), der tillader eller blokerer forbindelser ud fra PDP's afgørelse.

Q4: Hvordan støtter rollebaseret adgangskontrol (RBAC) zero trust?

RBAC samler tilladelser i bestemte roller og hjælper med at forhindre, at brugere arver for mange administratorrettigheder.

Q5: Hvad er kontekstbaseret adgangskontrol?

Vurdering af login ud fra spor som placering, enhedens tilstand og tidspunkt.

Kontrolpunkt 10: Avanceret FAQ om sikkerhed (del D)

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

Q6: Hvordan adskiller mikrosegmentering sig fra VLAN?

VLAN'er opdeler netværk i brede logiske segmenter på lag 2, mens mikrosegmentering bruger softwarepolitikker til at isolere enkelte arbejdsbelastninger.

Q7: Hvad er just-in-time-adgang (JIT)?

Midlertidige administratorrettigheder, der automatisk fjernes, når opgaven er løst.

Q8: Hvordan sikres API'er med zero trust?

Med krav om kryptografisk signerede OAuth-tokens og kontrol af signaturer i hver API-gateway.

Q9: Hvad er en ZTNA-klient?

Et program, der opretter sikre, krypterede forbindelser til bestemte programmer i stedet for hele undernet.

Q10: Hvordan hjælper revision af logfiler zero trust?

Løbende logning lader automatiske værktøjer opdage afvigelser og straks spærre mistænkelige logins.

Del 11: 10 fakta og indsigter om cybersikkerhed fra virkeligheden

Gennemgå fakta om sikkerhedsbrud, forsvarsmekanismer og krav til overholdelse.

1. SIKKERHEDSINDSIGT

Zero trust erstatter modellen med borg og voldgrav med regler, der tager udgangspunkt i identiteten.

2. SIKKERHEDSINDSIGT

Mikrosegmentering af netværket mindsker det område, malware kan nå, ved at isolere arbejdsbelastninger i små beskyttede zoner.

3. SIKKERHEDSINDSIGT

Zero Trust fokuserer på at beskytte ressourcer som aktiver, tjenester og konti frem for netværkssegmenter. [1]

4. SIKKERHEDSINDSIGT

Mindste rettigheder mindsker risikoen for, at insidere trækker data ud af centrale databaser.

5. SIKKERHEDSINDSIGT

Kontrol af enhedens tilstand tjekker opdateringer og antivirus i realtid.

6. SIKKERHEDSINDSIGT

Zero Trust Network Access (ZTNA)-mæglere kan erstatte eller supplere virksomheders VPN'er for at begrænse brugernes adgang.

7. SIKKERHEDSINDSIGT

Just-in-time-rettigheder mindsker risikoen for tyveri af logins på domænecontrollere.

8. SIKKERHEDSINDSIGT

Løbende kontrol logger og reviderer adfærd og spærrer brugere med unormal kørsel af scripts.

9. SIKKERHEDSINDSIGT

Traditionelt perimeterforsvar stopper ikke angreb indefra, når et administratorlogin er lækket.

10. SIKKERHEDSINDSIGT

NIST Special Publication 800-207 (2020) giver en abstrakt definition af Zero Trust-arkitektur med udrulningsmodeller. [1]

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. (2020). SP 800-207: Zero Trust Architecture.
https://csrc.nist.gov/pubs/sp/800/207/final

[2] CISA. (2023). Zero Trust Maturity Model.
https://www.cisa.gov/zero-trust-maturity-model

[3] NIST. (2025). SP 800-63B-4: Digital Identity Guidelines: Authentication and Authenticator Management.
https://pages.nist.gov/800-63-4/sp800-63b.html

[4] FBI Internet Crime Complaint Center. (2026). 2025 IC3 Annual Report.
https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

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

Facitliste: Kontrolpunkt 1 – Flervalg

1 Spørgsmål 1

Rigtigt svar: A

UNDERVISNINGSNOTE

Hvad er kerneprincippet i zero trust? → Stol aldrig, kontrollér altid hver anmodning uanset kilde

2 Spørgsmål 2

Rigtigt svar: A

UNDERVISNINGSNOTE

Hvad er mikrosegmentering? → Opdeling af netværket i små, isolerede zoner, der begrænser angriberes bevægelse

3 Spørgsmål 3

Rigtigt svar: A

UNDERVISNINGSNOTE

Hvad er princippet om mindste rettigheder? → At brugere kun får den adgang, deres arbejde kræver [2]

4 Spørgsmål 4

Rigtigt svar: A

UNDERVISNINGSNOTE

Hvad er identitets- og adgangsstyring (IAM)? → Rammer, der styrer digitale identiteter og rettigheder

5 Spørgsmål 5

Rigtigt svar: A

UNDERVISNINGSNOTE

Hvad betyder løbende godkendelse? → Gentagen kontrol af identitet og enhedens tilstand under en aktiv session

Facitliste: Kontrolpunkt 2 – Sandt eller falsk

6 **Spørgsmål 6** **Rigtigt svar: Falsk**

UNDERVISNINGSNOTE

Falsk: Zero Trust giver ingen implicit tillid baseret på placering i netværket, hverken indenfor eller udenfor.

7 **Spørgsmål 7** **Rigtigt svar: Sandt**

UNDERVISNINGSNOTE

Sandt: små isolerede zoner begrænser, hvor langt en ubuden gæst kan bevæge sig mellem servere.

8 **Spørgsmål 8** **Rigtigt svar: Falsk**

UNDERVISNINGSNOTE

Falsk: mindste rettighed giver kun den minimale adgang, hver rolle har brug for.

9 **Spørgsmål 9** **Rigtigt svar: Sandt**

UNDERVISNINGSNOTE

Løbende kontrol tjekker enhedens tilstand og loginoplysninger under hele sessionen.

10 **Spørgsmål 10** **Rigtigt svar: Sandt**

UNDERVISNINGSNOTE

Zero trust mindsker skaden ved kompromitterede firmalogins.

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

G 1. VERIFIKATION	F 2. SEGMENTERING	A 3. IAM	B 4. RETTIGHEDER
H 5. TILSTAND	E 6. REVISION	D 7. FIREWALL	C 8. ROUTER

KONTROLPUNKT 3: FACIT TIL NØGLEBEGREBER

1 VERIFIKATION	2 SEGMENTERING	3 IAM	4 RETTIGHEDER
5 TILSTAND	6 REVISION		

KONTROLPUNKT 6, ALTERNATIV: FACIT TIL ORDMATCHNING

1 G – FIREWALL	2 F – REVISION	3 D – RETTIGHEDER	4 B – SEGMENTERING
5 H – ROUTER	6 E – TILSTAND	7 C – IAM	8 A – VERIFIKATION

DISKUSSIONSNOTER TIL UNDERVISERE

Fagbegreber:
Kontrollér, at eleverne kan forklare VERIFIKATION, SEGMENTERING og IAM med egne ord og give et eksempel på hvert begreb.

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

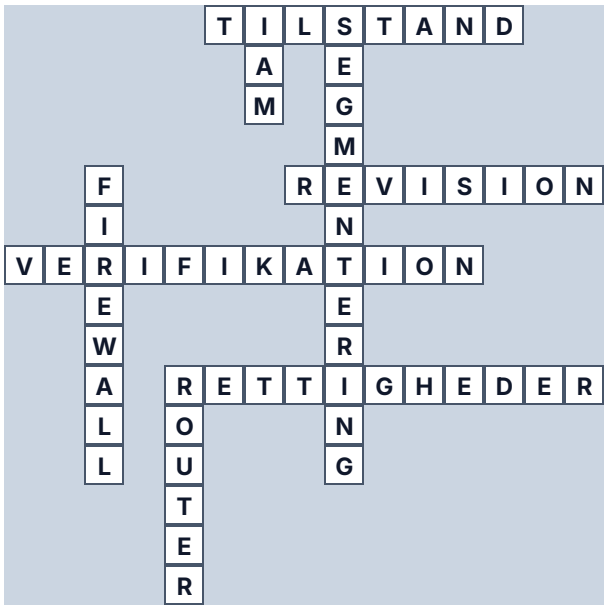
Kildekritik:
Lad eleverne efterprøve mindst én påstand mod referencerne i opgavearket, og drøft, hvorfor tal, priser og regler kan ændre sig over tid.

Facit til opgaver og undervisernoter

LØSNING PÅ ORDJAGT

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

LØSNING PÅ KRYDS OG TVÆRS



UNDERVISERVEJLEDNING TIL KRYDSORDSLØSNINGER

VANDRETTE NØGLER

1 vandret: TILSTAND Det, der vurderes, når tilsluttede enheder kontrolleres (8 bogstaver)

5 vandret: REVISION Logning og gennemgang af aktive sessioner (8 bogstaver)

6 vandret: VERIFIKATION Løbende kontrol af legitimation ved hvert adgangspunkt (12 bogstaver)

7 vandret: RETTIGHEDER Princippet om mindste … begrænser, hvad brugere må (11 bogstaver)

LODRETTE NØGLER

2 lodret: IAM Forkortelse for styring af digitale identiteter og adgang (3 bogstaver)

3 lodret: SEGMENTERING Mikro…: opdeling af netværket i små, isolerede zoner (12 bogstaver)

4 lodret: FIREWALL Barriere, der beskytter mod det eksterne netværk (8 bogstaver)

7 lodret: ROUTER Enhed, der videresender datapakker mellem net (6 bogstaver)

Facit til bogstavrod og chiffer

Bedømmelsesfacit til bogstavrod-øvelsen og den hemmelige chifferudfordring.

FACIT TIL BOGSTAVROD

1. T I A F E K I V O R N I	VERIFIKATION	5. E I E T G G E R N S N M	SEGMENTERING
2. M A I	IAM	6. I R G E E D R E H T T	RETTIGHEDER
3. S I T T A D N L	TILSTAND	7. R N S I O E I V	REVISION
4. E L L A W F I R	FIREWALL	8. U R R E T O	ROUTER

FACIT TIL HEMMELIG CHIFFERUDFORDRING

"STOL ALDRIG KONTROLLER ALTID"

Facit til casestudier

A Casestudie 1: Overgang til zero trust

Underviserens løsning

BEDØMMELSESVEJLEDNING

Elevens svar bør dække følgende punkter:

- Analyse af scenariet: En stor virksomhed har et fladt netværk, hvor enhver enhed kan nå alle servere og databaser.
- Anbefalet strategi og løsning: Opdel netværket i isolerede afdelingszoner, styr trafikken mellem dem med interne firewalls, og kræv kontrol af adgangstokens ved al adgang.

B Casestudie 2: Indførelse af mindste rettigheder

Underviserens løsning

BEDØMMELSESVEJLEDNING

Elevens svar bør dække følgende punkter:

- Analyse af scenariet: Logfiler viser, at midlertidige brugere og menige medarbejdere har fuld adgang til regnskabsdatabaserne.
- Anbefalet strategi og løsning: Fjern alle globale administratorrettigheder, indfør rollebaseret adgang (RBAC) efter jobfunktion, og gennemgå rettighederne automatisk hver uge.