Navn: _____ Dato: _____ Poeng: _____

Zero Trust-arkitektur og sikkerhet

Kontinuerlig verifisering, mikrosegmentering av nettverk, identitets- og tilgangsstyring, minste privilegium og kontroller av sikkerhetstilstand.

LÆRINGSOVERSIKT OM ZERO TRUST-SIKKERHET

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 arkitektur og sikkerhet for Zero Trust. Du skal utforske kontinuerlig verifisering, mikrosegmentering av nettverk, identitets- og tilgangsstyring (IAM), minste privilegium og øktrevisjon.

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/zero-trust-cybersikkerhet/

Din læringsveiledning for Zero Trust-strategi

- Forstå kjerneprinsippet om kontinuerlig verifisering.
- Innfør mikrosegmentering av nettverket og tilgang med minste privilegium.
- Konfigurer kontroller av enhetens sikkerhetstilstand og aktiv revisjon av økter.

VEILEDNING I ZERO TRUST-SIKKERHET

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

ZERO TRUST-ARKITEKTUR OG SIKKERHET (INNLEDNING)

Zero Trust-sikkerhet erstatter gamle modeller med nettverksperimeter med en streng policy om «aldri stol på noe, verifiser alltid». Mikrosegmentering, identitets- og tilgangsstyring (IAM), minste privilegium og tilstandskontroller blokkerer lateral bevegelse for trusler.

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

Kontrollpunkt 1: Flervalgsutfordring

1. Hva er kjerneprinsippet i Zero Trust-sikkerhet?

- A. Aldri stol på noen, verifiser alltid hver tilgangsforespørsel uavhengig av kilde
- B. Å anta at all trafikk innenfor bedriftens brannmur er trygg
- C. Å lagre databasefiler uten kryptering for å øke hastigheten
- D. Å håndheve e-postautentisering kun med SPF-oppføringer

2. Hva er mikrosegmentering av nettverk?

- A. Å dele nettverk inn i små, isolerte soner for å begrense lateral bevegelse
- B. Å kryptere nettverkskort under dataoverføring
- C. Å koble alle lokale servere til én enkelt offentlig IP-adresse
- D. Å overvåke brukerens tastetrykk i nettleserøkter

3. Hva er prinsippet om minste privilegium?

- A. Å begrense brukernes tilgangstillatelser til det som er nødvendig for jobben deres
- B. Å gi alle brukere alle systemrettigheter som standard
- C. Å tillate anonyme påloggінger til bedriftens databaseservere
- D. Å konfigurere offentlige Wi-Fi-rutere uten passord

4. Hva er Identity and Access Management (IAM)?

- A. Rammeverk som administrerer digitale identiteter og kontrollerer systemprivilegier
- B. Antivirusverktøy som skanner lokale filkataloger
- C. Et lagringssystem for sikkerhetskopier som bruker medier uten nettverkstilkobling (air-gap)
- D. En gatewayprotokoll for e-post som avviser forfalskede domener

5. Hva betyr kontinuerlig autentisering?

- A. Å gjentatte ganger verifisere brukerens identitet og enhetens tilstand under en aktiv økt
- B. Å bytte hovedpassordet hvert 10. minutt
- C. Å hashe databaseposter med flere algoritmer
- D. Å kryptere nettverkspakker under overføring med TLS-nøkler

Kontrollpunkt 2: Utfordring med sant eller usant

6 Spørsmål 6

6. Zero Trust forutsetter at all trafikk innenfor bedriftens brannmur er trygg.

○ Sant ○ Usant

7 Spørsmål 7

7. Mikrosegmentering begrenser angripernes mulighet til å bevege seg lateralt på tvers av interne servere.

○ Sant ○ Usant

8 Spørsmål 8

8. Minste privilegium gir tilgang til alle databasefiler som standard.

○ Sant ○ Usant

9 Spørsmål 9

9. Kontinuerlig verifisering validerer enhetens helse og legitimasjon gjennom hele en påloggingsøkt.

○ Sant ○ Usant

10 Spørsmål 10

10. Innføring av Zero Trust reduserer konsekvensene av kompromitterte bedriftsinnlogginger.

○ Sant ○ Usant

Kontrollpunkt 3: Sett inn nøkkelbegreper

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

1. Å kreve påloggingsopplysninger ved hvert tilgangspunkt er kontinuerlig _____ .
2. Å dele bedriftsnettverket inn i små soner kalles mikro- _____ .
3. Å konfigurere digitale identiteter og tilgangskontroll bruker et _____ -system.
4. Å begrense brukertillatelser bruker prinsippet om minste _____ .
5. Å vurdere tilkoblede enheter skanner enhetens _____ .
6. Å logge og gjennomgå aktive økter er sikkerhets- _____ .

ORDBANK

BRANNMUR HELSESTATUS IAM PRIVILEGIUM REVISJON ROUTER SEGMENTERING VERIFISERING

Skriv svarene dine her:

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

Kontrollpunkt 4: Koble sikkerhetsbegreper

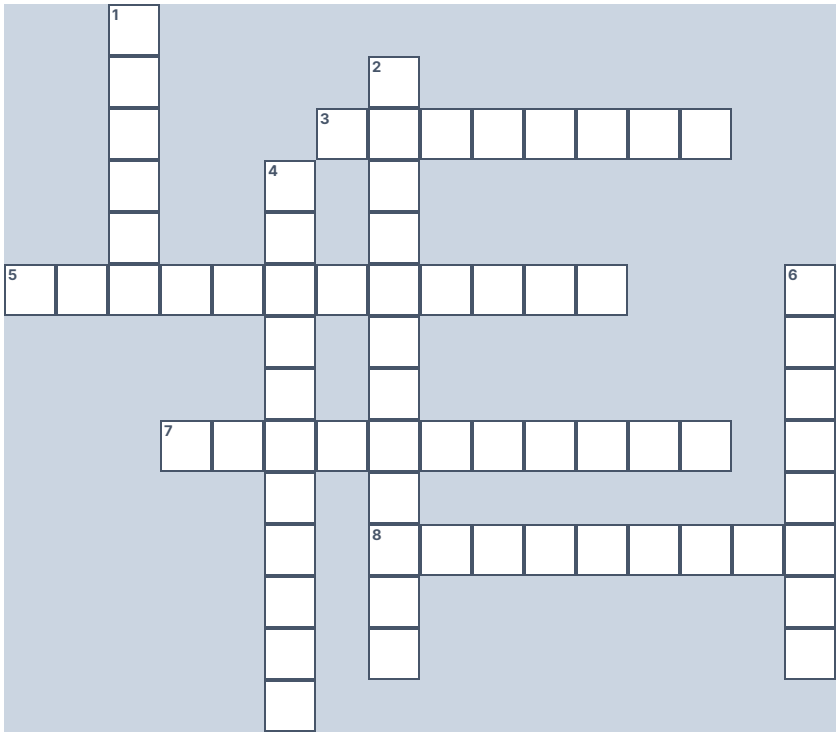
KOBLE DEFINISJONER

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

☐	1. VERIFISERING	A	Administrere tilgang til brukerlegitimasjon.
☐	2. SEGMENTERING	B	Prinsippet om minst mulig tilgangsrettigheter.
☐	3. IAM	C	Ruting av nettverkspakketrafikk.
☐	4. PRIVILEGIE	D	Beskyttelse ved ytre nettverksbarriere.
☐	5. SIKKERHETSTILSTAND	E	Gjennomgang av loggførte tilgangsøkter.
☐	6. REVISJON	F	Dele opp interne nettverkssoner.
☐	7. BRANNMUR	G	Kontrollerer alltid brukerlegitimasjon.
☐	8. RUTER	H	Vurdere enhetens helsestatus.

Kontrollpunkt 5: Kryssord

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



VANNRETT

3. Gjennomgang av loggførte tilgangsøkter. (8)

5. Alltid kontrollere brukerens påloggingsopplysninger. (12)

7. Evaluering av enhetens helsetilstand. (11)

8. Administrasjon av brukernes tilgang til påloggingsopplysninger. (9)

LODDRETT

1. Ruting av nettverkspakketrafikk. (6)

2. Deling av interne nettverkssoner. (12)

4. Prinsippet om minst mulige tilgangsrettigheter. (11)

6. Beskyttelse ved ytre nettverksbarriere. (8)

Kontrollpunkt 5, alternativ: Tilgjengelige kryssordhint

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

VANNRETT

3 vannrett: Gjennomgang av loggførte tilgangsøkter. (8 bokstaver):

5 vannrett: Alltid kontrollere brukerens påloggingsopplysninger. (12 bokstaver):

7 vannrett: Evaluering av enhetens helsetilstand. (11 bokstaver):

8 vannrett: Administrasjon av brukernes tilgang til påloggingsopplysninger. (9 bokstaver):

LODDRETT

1 loddrett: Ruting av nettverkspakketrafikk. (6 bokstaver):

2 loddrett: Deling av interne nettverkssoner. (12 bokstaver):

4 loddrett: Prinsippet om minst mulige tilgangsrettigheter. (11 bokstaver):

6 loddrett: Beskyttelse ved ytre nettverksbarriere. (8 bokstaver):

Kontrollpunkt 6: Skjult ordsøk

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

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

ORDLISTE

VERIFISERING SEGMENTERING IAMSYSTEM PRIVILEGIUM HELSESTATUS
REVISJON BRANNMUR ROUTER

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. VERIFISERING
B. SEGMENTERING
C. IAMSYSTEM
D. PRIVILEGIUM
E. HELSESTATUS
F. REVISJON
G. BRANNMUR
H. ROUTER

DEFINISJONER OG TILHØRENDE FELT

_____ 1. Beskyttelse ved ytre nettverksbarriere.

_____ 2. Gjennomgang av loggførte tilgangsøkter.

_____ 3. Prinsippet om minst mulige tilgangsrettigheter.

_____ 4. Deling av interne nettverkssoner.

_____ 5. Ruting av nettverkspakketrafikk.

_____ 6. Evaluering av enhetens helsetilstand.

_____ 7. Administrasjon av brukernes tilgang til påloggingsopplysninger.

_____ 8. Alltid kontrollere brukerens påloggingsopplysninger.

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. **RIEFESIVNRGI**
2. **MIESASTYM**
3. **HTSALEUSETS**
4. **NURMNBRA**
5. **EIETGGERNSNM**
6. **IMLGUIPREIV**
7. **RNSJOEIV**
8. **URRETO**

Bonusaktivitet: Tenk raskt

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

1	Informasjon du aldri bør dele			
2	Trygge vaner du kan begynne med i dag			
3	Ting som kontrolleres på en enhet			
4	Ting som logges			
5	Ord knyttet til cybersikkerhet			
6	Ting Zero Trust kontrollerer			
7	Steder der du viser ID i hverdagen			
8	Måter å bevise at det virkelig er deg			
9	Ting å gjøre etter en datalekkasje			
10	Tegn på at en datamaskin er infisert			
11	Grunner til å oppdatere programvare			
12	Tilgangsnivåer i et selskap			
13	Sikkerhetsverktøy du kjenner til			
14	Soner et nettverk kan deles inn i			
15	Ordtak om tillit			

Kontrollpunkt 8: Casestudier om cybersikkerhet

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

CASESTUDIE 1: OVERGANG TIL NULLTILLIT-NETTVERKSARKITEKTUR



Scenario: Et stort selskap bruker i dag et flatt internt nettverk der enhver enhet på det lokale nettverket kan få tilgang til alle servere og databaser i selskapet.

Diskusjonsspørsmål: Utform en strategi for nettverksmikrosegmentering for å begrense lateral bevegelse.

CASESTUDIE 2: INNFØRE TILGANGSKONTROLL MED MINSTE PRIVILEGIUM



Scenario: Revisjonslogger viser at midlertidige databasebrukere og ansatte på lavt nivå har globale lese- og skrivetillatelser til kritiske regnskapsdatabaser.

Diskusjonsspørsmål: Revider og begrens IAM-rettigheter i databasen for å håndheve minste privilegium.

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

22	5	18	9	6	9	19	5	18	1	12	12	20	9	4	13	5	4	
14	21	12	12	20	9	12	12	9	20	19	1	18	11	9	20	5	11	20	21	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 Zero Trust?

Zero Trust er et sikkerhetsrammeverk som forutsetter at trusler finnes både utenfor og innenfor nettverksgrensen, og som krever verifisering for hver forespørsel. [1]

Q2: Hva er kjerneregelen i Zero Trust?

Stol aldri på noe, verifiser alltid.

Q3: Hva er mikrosegmentering?

Å dele et nettverk inn i små, sikre logiske segmenter for å kontrollere trafikk og begrense skadene ved innbrudd.

Q4: Hva er minste privilegium (least privilege)?

Å gi brukere bare de minste tilgangsrettighetene som kreves for å utføre de aktuelle arbeidsoppgavene. [2]

Q5: Hva står IAM for?

Identitets- og tilgangsstyring.

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

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

Q6: Hvordan hjelper en enhetssjekk av sikkerhetstilstand (device posture check)?

Den verifiserer at en enhet er oppdatert, kjører aktiv antivirus og er sikker før den gir tilgang.

Q7: Hva er lateral bevegelse?

Prosessen angripere bruker for å bevege seg gjennom et nettverk fra en første kompromittert node til systemer med høyere verdi.

Q8: Erstatter Zero Trust brannmurer?

Nei, den styrker dem ved å legge til identitetsbaserte kontroller og interne segmenteringsbrannmurer.

Q9: Hva er kontinuerlig autentisering?

Kontinuerlig verifisering av brukerens identitet gjennom en aktiv påloggingsøkt, ikke bare ved første pålogging.

Q10: Hvorfor er et flatt nettverk farlig?

I flate nettverk gjør én enkelt kompromittert node det enkelt for angripere å få tilgang til alle databaser i nettverket.

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

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

Q1: Hvordan løser Zero Trust perimetermodellen?

Den erstatter den utdaterte «borg og vollgrav»-modellen og flytter forsvaret fra yttergrensene i nettverket til bestemte brukeridentiteter og ressurser.

Q2: Hva er et policybeslutningspunkt (PDP)?

Systemkomponenten som vurderer autorisasjonsforespørsler mot sikkerhetsregler for å avgjøre om tilgang skal gis.

Q3: Hva er et policyhåndhevingspunkt (PEP)?

Systemnoden (som en gateway eller proxy) som fysisk tillater eller blokkerer tilkoblingsforespørsler basert på PDP-avgjørelsen.

Q4: Hvordan støtter rollebasert tilgangskontroll (RBAC) Zero Trust?

RBAC grupperer tillatelser i bestemte roller, noe som bidrar til å hindre at brukere arver for omfattende administrative rettigheter.

Q5: Hva er kontekstuell tilgangskontroll?

Vurdere påloggingsforespørsler ved hjelp av sekundære holdepunkter som geografisk lokasjon, enhetens sikkerhetstilstand og påloggingstidspunkt for å vurdere risiko.

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

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

Q6: Hvordan skiller mikrosegmentering seg fra vanlige VLAN-er?

VLAN-er deler nettverk inn i brede logiske segmenter på lag 2, mens mikrosegmentering bruker programvarebaserte retningslinjer for å isolere enkeltstående arbeidsbelastninger.

Q7: Hva er just-in-time-tilgang (JIT)?

Å gi midlertidig forhøyede administratorrettigheter og trekke dem tilbake automatisk når oppgaven er ferdig.

Q8: Hvordan sikrer du API-er i et Zero Trust-rammeverk?

Ved å kreve kryptografisk signerte OAuth-tokens og revidere forespørselssignaturer ved hver API-gateway.

Q9: Hva er en klient for zero trust-nettverkstilgang (ZTNA)?

En programvareagent som etablerer sikre, krypterte utgående tilkoblinger til bestemte applikasjoner i stedet for rå nettverksundernett.

Q10: Hvordan bidrar loggrevisjon til Zero Trust?

Kontinuerlig loggføring lar automatiserte sikkerhetsanalyseverktøy oppdage avvik og umiddelbart suspendere uautoriserte påloggingar.

Del 11: 10 fakta om cybersikkerhet fra virkeligheten og innsikt

Gå gjennom virkelighetsnære fakta om sikkerhetsbrudd, forsvarsmekanismer og samsvarsstandarder.

1. SIKKERHETSINNSIKT

Zero Trust-arkitekturer erstatter den gamle slottsgrav-modellen med identitetssentrerte verifiseringsregler.

2. SIKKERHETSINNSIKT

Mikrosegmentering av nettverket krymper området skadevare kan nå ved å isolere arbeidsbelastninger i små beskyttede soner.

3. SIKKERHETSINNSIKT

Zero Trust fokuserer på å beskytte ressurser som eiendeler, tjenester og kontoer, i stedet for nettverkssegmenter. [1]

4. SIKKERHETSINNSIKT

Tilgangsregler basert på minste privilegium reduserer risikoen for at innsidere lekker data ut fra kjernedatabaser.

5. SIKKERHETSINNSIKT

Validering av enhetens sikkerhetstilstand kontrollerer oppdateringsnivået i operativsystemet og status for aktivt antivirus i sanntid.

6. SIKKERHETSINNSIKT

Zero Trust Network Access (ZTNA)-meglere kan erstatte eller supplere VPN-er i bedrifter for å begrense omfanget av brukertilgang.

7. SIKKERHETSINNSIKT

Just-in-Time (JIT)-delegering av administrative rettigheter reduserer risikoen for tyveri av påloggingsinformasjon på domenekontrollere.

8. SIKKERHETSINNSIKT

Kontinuerlig validering logger og reviderer øktatferd og suspenderer brukere som viser uvanlige mønstre i skriptkjøring.

9. SIKKERHETSINNSIKT

Tradisjonelle perimeterforsvar klarer ikke å blokkere sideveis angrep når en administrativ legitimasjon er lekket.

10. SIKKERHETSINNSIKT

NIST Special Publication 800-207 (2020) gir en abstrakt definisjon av Zero Trust-arkitektur, med distribusjonsmodeller. [1]

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. (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

Fasit: Kontrollpunkt 1 – flervalg

1 Spørsmål 1

Riktig svar: A

MERKNAD TIL LÆREREN

Hva er kjerneprinsippet i Zero Trust-sikkerhet? → Aldri stol på noen, verifiser alltid hver tilgangsforespørsel uavhengig av kilde

2 Spørsmål 2

Riktig svar: A

MERKNAD TIL LÆREREN

Hva er mikrosegmentering av nettverk? → Å dele nettverk inn i små, isolerte soner for å begrense lateral bevegelse

3 Spørsmål 3

Riktig svar: A

MERKNAD TIL LÆREREN

Hva er prinsippet om minste privilegium? → Å begrense brukernes tilgangstillatelser til det som er nødvendig for jobben deres

4 Spørsmål 4

Riktig svar: A

MERKNAD TIL LÆREREN

Hva er Identity and Access Management (IAM)? → Rammeverk som administrerer digitale identiteter og kontrollerer systemprivilegier

5 Spørsmål 5

Riktig svar: A

MERKNAD TIL LÆREREN

Hva betyr kontinuerlig autentisering? → Å gjentatte ganger verifisere brukerens identitet og enhetens tilstand under en aktiv økt

Fasit: Kontrollpunkt 2 – sant eller usant

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

MERKNAD TIL LÆREREN

Usant: Zero Trust gir ingen implisitt tillit basert på nettverksplassering, verken innenfor eller utenfor.

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

MERKNAD TIL LÆREREN

Sant: små isolerte soner begrenser hvor langt en inntrenger kan bevege seg mellom servere.

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

MERKNAD TIL LÆREREN

Usant: minste privilegium gir bare den minste tilgangen hver rolle trenger.

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

MERKNAD TIL LÆREREN

Kontinuerlig verifisering validerer enhetens helse og legitimasjon gjennom hele en påloggingsøkt.

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

MERKNAD TIL LÆREREN

Innføring av Zero Trust reduserer konsekvensene av kompromitterte bedriftsinnlogginger.

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

G 1. VERIFISERING	F 2. SEGMENTERING	A 3. IAM	B 4. PRIVILEGIE
H 5. SIKKERHETSTILSTAND	E 6. REVISJON	D 7. BRANNMUR	C 8. RUTER

KONTROLLPUNKT 3: FASIT – NØKKELBEGREPER

1 VERIFISERING	2 SEGMENTERING	3 IAM	4 PRIVILEGIUM
5 HELSESTATUS	6 REVISJON		

KONTROLLPUNKT 6, ALTERNATIV: FASIT – KOBLE ORD

1 G – BRANNMUR	2 F – REVISJON	3 D – PRIVILEGIUM	4 B – SEGMENTERING
5 H – ROUTER	6 E – HELSESTATUS	7 C – IAMSYSTEM	8 A – VERIFISERING

DISKUSJONSNOTATER TIL LÆRERE

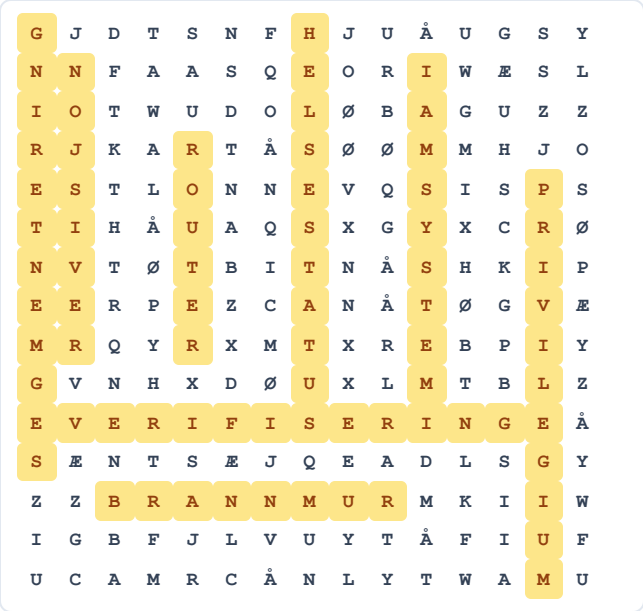
Nøkkelbegreper:
Kontroller at elevene kan forklare VERIFISERING, SEGMENTERING og IAM med egne ord og gi et eksempel på hvert.

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.

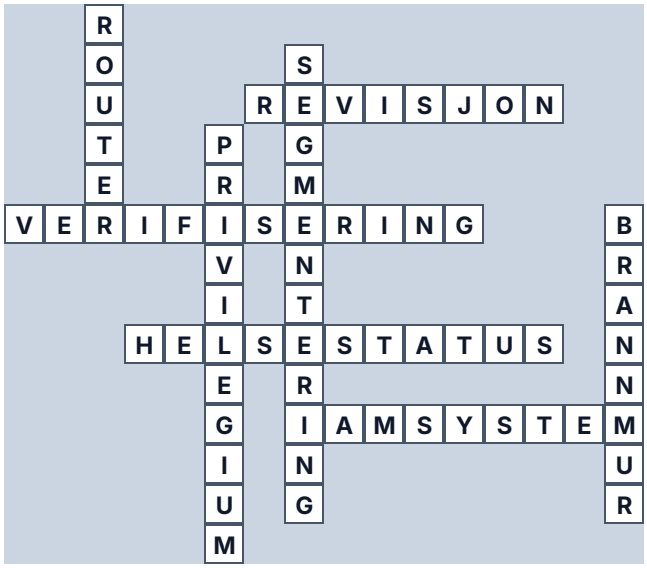
Fasit for oppgavene og merknader til læreren

LØSNING PÅ ORDSØKET



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

KRYSSORDLØSNING



LÆRERVEILEDNING FOR KRYSSORDLØSNINGER

VANNRETT

3 vannrett: REVISJON Gjennomgang av loggførte tilgangsøkter. (8 bokstaver)

5 vannrett: VERIFISERING Alltid kontrollere brukerens påloggingsopplysninger. (12 bokstaver)

7 vannrett: HELSESTATUS Evaluering av enhetens helsetilstand. (11 bokstaver)

8 vannrett: IAMSYSTEM Administrasjon av brukernes tilgang til påloggingsopplysninger. (9 bokstaver)

LODDRETT

1 loddrett: ROUTER Ruting av nettverkspakketrafikk. (6 bokstaver)

2 loddrett: SEGMENTERING Deling av interne nettverkssoner. (12 bokstaver)

4 loddrett: PRIVILEGIUM Prinsippet om minst mulige tilgangsrettigheter. (11 bokstaver)

6 loddrett: BRANNMUR Beskyttelse ved ytre nettverksbarriere. (8 bokstaver)

Fasit for kodeord og chiffer

Fasit for vokabularøvelsen med ordstokking og den hemmelige chifferutfordringen.

FASIT: BOKSTAVBLANDING

1.	R I E F E S I V N R G I	VERIFISERING	5.	E I E T G G E R N S N M	SEGMENTERING
2.	M I E S A S T Y M	IAMSYSTEM	6.	I M L G U I P R E I V	PRIVILEGIUM
3.	H T S A L E U S E T S	HELSESTATUS	7.	R N S J O E I V	REVISJON
4.	N U R M N B R A	BRANNMUR	8.	U R R E T O	ROUTER

FASIT TIL DEN HEMMELIGE CHIFFERUTFORDRINGEN

"VERIFISER ALLTID MED NULLTILLITSARKITEKTUR"

Fasit til casestudiene

A Casestudie 1: Overgang til nulltillit-nettverksarkitektur

Løsning for læreren

RETTEVEILEDNING

Elevsvar bør dekke følgende punkter:

- Scenarioanalyse: En stor bedrift bruker i dag et flatt internt nettverk der enhver enhet på det lokale nettverket har tilgang til alle bedriftens servere og databaser.
- Anbefalt strategi og løsning: Del det flate nettverket inn i isolerte avdelingssoner. Installer interne brannmurer for å kontrollere trafikken mellom sonene, og krev validering av tilkoblingstoken for all tilgang.

B Casestudie 2: Innføre tilgangskontroll med minste privilegium

Løsning for læreren

RETTEVEILEDNING

Elevsvar bør dekke følgende punkter:

- Scenarioanalyse: Revisjonslogger avslører at midlertidige databasebrukere og ansatte på lavt nivå har globale lese- og skrivetillatelser til kritiske regnskapsdatabaser.
- Anbefalt strategi og løsning: Trekk tilbake alle globale administrative rettigheter. Innfør rollebasert tilgangskontroll (RBAC) som samsvarer med de nøyaktige stillingsrollene, og etabler ukentlige automatiserte gjennomganger av tillatelser.