Namn: _____ **Datum:** _____ **Poäng:** _____

Zero Trust-arkitektur och säkerhet

Kontinuerlig verifiering, mikrosegmentering av nätverk, Identity and Access Management, minsta möjliga behörighet och kontroller av enhetens status.

ÖVERSIKT AV INLÄRNING OM ZERO TRUST-SÄKERHET

SÄKRAD
DATAKRYPTERING
256-bitars AES-standard

EFTERLEVANDE
GLOBALA STANDARDER
Ramverken GDPR och CCPA

ZERO TRUST
ÅTKOMSTPOLICY
Multifaktorautentisering

Välkommen! Det här aktivitetshäftet guidar dig genom Zero Trust-arkitektur och säkerhet. Du utforskar kontinuerlig verifiering, nätverksmikrosegmentering, identitets- och åtkomsthantering (IAM), minsta möjliga behörighet och sessionsgranskning.

KONTROLLPUNKTER I ARBETSBLADET

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

Öppna VPN.com:s guide om cybersäkerhet

URL: https://www.vpn.com/sv/cybersakerhet/zero-trust-cybersakerhet/

Din inlärningsplan för strategi för noll förtroende (Zero Trust)

- Förstå kärnprincipen med kontinuerlig verifiering.
- Inför mikrosegmentering av nätverket och åtkomst med minsta möjliga behörighet.
- Konfigurera kontroller av enhetens status (posture) och aktiv sessionsgranskning.

INSTRUKTIONER FÖR GUIDEN OM ZERO TRUST-SÄKERHET

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

ZERO TRUST-ARKITEKTUR OCH SÄKERHET (INTRODUKTION)

Zero Trust-säkerhet ersätter gamla modeller med nätverksperimeter med en strikt policy om att 'aldrig lita på någon, alltid verifiera'. Mikrosegmentering, identitets- och åtkomsthantering (IAM), minsta möjliga behörighet och kontroller av enhetens status blockerar lateral förflyttning av hot.

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

Kontrollpunkt 1: Utmaning med flerval

1. **1. Vad är kärnprincipen i Zero Trust-säkerhet?**
   - A. Lita aldrig på något, verifiera alltid varje åtkomstförfrågan oavsett källa
   - B. Att anta att all trafik innanför företagets brandvägg är säker
   - C. Att lagra databasfiler utan kryptering för att öka hastigheten
   - D. Att upprätthålla e-postautentisering endast med SPF-poster

2. **2. Vad är mikrosegmentering av nätverk?**
   - A. Att dela upp nätverk i små, isolerade zoner för att begränsa lateral förflyttning
   - B. Att kryptera nätverkskort under dataöverföring
   - C. Att ansluta alla lokala servrar till en enda offentlig IP-adress
   - D. Att övervaka användares tangenttryckningar i webbläsarsessioner

3. **3. Vad är principen om minsta möjliga behörighet?**
   - A. Att begränsa användarnas åtkomstbehörigheter till det som är nödvändigt för deras arbete
   - B. Att ge alla användare alla systembehörigheter som standard
   - C. Att tillåta anonyma inloggningar på företagets databasservrar
   - D. Att konfigurera offentliga Wi-Fi-routrar utan lösenord

4. **4. Vad är Identity and Access Management (IAM)?**
   - A. Ramverk som hanterar digitala identiteter och styr systembehörigheter
   - B. Antivirusverktyg som skannar lokala filkataloger
   - C. Ett säkerhetskopieringssystem som använder isolerade (air-gapped) medier
   - D. Ett gatewayprotokoll för e-post som avvisar förfalskade domäner

5. **5. Vad innebär kontinuerlig autentisering?**
   - A. Att upprepade gånger verifiera användarens identitet och enhetens hälsotillstånd under en aktiv session
   - B. Att byta huvudlösenord var 10:e minut
   - C. Att hasha databasposter med flera algoritmer
   - D. Att kryptera nätverkspaket under överföring med TLS-nycklar

Kontrollpunkt 2: Utmaning med sant eller falskt

6 Fråga 6

6. Zero Trust utgår från att all trafik innanför företagets brandvägg är säker.

○ Sant ○ Falskt

7 Fråga 7

7. Mikrosegmentering begränsar angripares möjlighet att röra sig lateralt över interna servrar.

○ Sant ○ Falskt

8 Fråga 8

8. Minsta möjliga behörighet ger som standard åtkomst till alla databasfiler.

○ Sant ○ Falskt

9 Fråga 9

9. Kontinuerlig verifiering validerar enhetens skick och inloggningsuppgifter under hela inloggningssessionen.

○ Sant ○ Falskt

10 Fråga 10

10. Att införa Zero Trust minskar effekten av komprometterade företagsinloggningar.

○ Sant ○ Falskt

Kontrollpunkt 3: Infoga nyckelbegrepp

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

1. Att kräva inloggningsuppgifter vid varje åtkomstpunkt är kontinuerlig _____ .
2. Att dela in företagsnätverket i små zoner kallas mikro- _____ .
3. Att konfigurera digitala identiteter och åtkomstkontroll sker med ett _____ .
4. Att bara ge användare de rättigheter de behöver kallas principen om minsta _____ .
5. Att utvärdera anslutna enheters hälsa innebär att skanna enheternas _____ .
6. Att logga och granska aktiva sessioner är säkerhets- _____ .

ORDBANK

BEHÖRIGHET BRANDVÄGG ENHETSHÄLSA GRANSKNING IAM-SYSTEM
ROUTER SEGMENTERING VERIFIERING

Skriv dina svar här:

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

Kontrollpunkt 4: Matchning av säkerhetsbegrepp

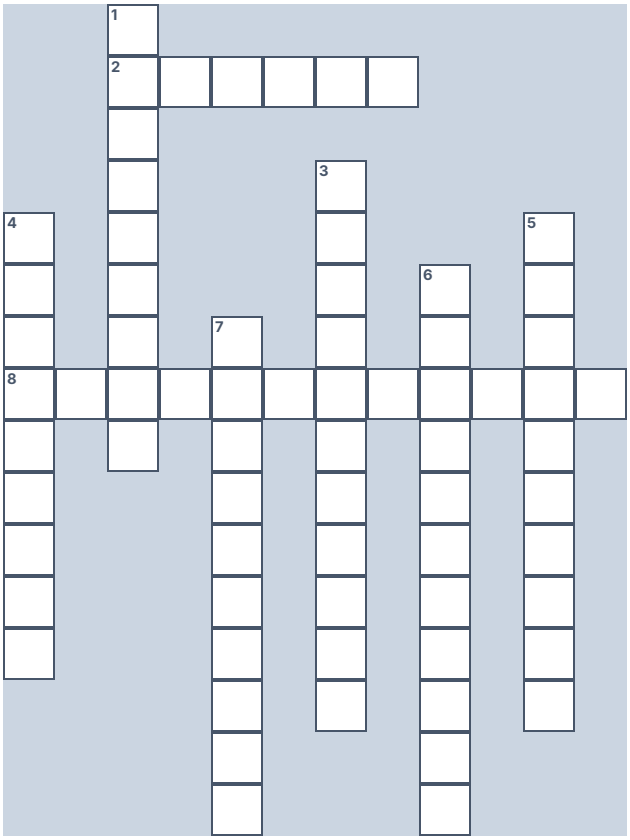
MATCHNING AV DEFINITIONER

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

☐	1. VERIFIERING	A	Hantering av åtkomst till användaruppgifter.
☐	2. SEGMENTERING	B	Principen om minsta åtkomsträttigheter.
☐	3. IAM	C	Att dirigera nätverkspaket.
☐	4. BEHÖRIGHET	D	Skydd av yttre nätverksbarriär.
☐	5. SÄKERHETSLÄGE	E	Granskning av loggade åtkomstsessioner.
☐	6. GRANSKNING	F	Att dela upp interna nätverkszoner.
☐	7. BRANDVÄGG	G	Kontrollerar alltid användarens inloggningsuppgifter.
☐	8. ROUTER	H	Utvärdering av enhetens hälsostatus.

Kontrollpunkt 5: Korsord

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



VÅGRÄTT

2. Dirigering av nätverkspaketens trafik. (6)

8. Uppdelning av interna nätverkszoner. (12)

LODRÄTT

1. Skydd mot nätverk utifrån. (9)

3. Utvärdering av enhetens hälsostatus. (11)

4. Hantering av åtkomst till användaruppgifter. (9)

5. Genomgång av loggade åtkomstsessioner. (10)

6. Att alltid kontrollera användarens inloggningsuppgifter. (11)

7. Principen om minsta åtkomsträttigheter. (10)

Kontrollpunkt 5, alternativ: Tillgängliga korsordsledtrådar

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

VÅGRÄTT

2 vågrätt: Dirigering av nätverkspaketens trafik. (6 bokstäver):

8 vågrätt: Uppdelning av interna nätverkszoner. (12 bokstäver):

LODRÄTT

1 lodrätt: Skydd mot nätverk utifrån. (9 bokstäver):

3 lodrätt: Utvärdering av enhetens hälsostatus. (11 bokstäver):

4 lodrätt: Hantering av åtkomst till användaruppgifter. (9 bokstäver):

5 lodrätt: Genomgång av loggade åtkomstsessioner. (10 bokstäver):

6 lodrätt: Att alltid kontrollera användarens inloggningsuppgifter. (11 bokstäver):

7 lodrätt: Principen om minsta åtkomsträttigheter. (10 bokstäver):

Kontrollpunkt 6: Dolt ordsök

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

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

ORDLISTA

VERIFIERING SEGMENTERING IAMSYSTEM BEHÖRIGHET ENHETSHÄLSA
GRANSKNING BRANDVÄGG ROUTER

Kontrollpunkt 6, alternativ: Tillgänglig matchning av ordförråd

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

ORDLISTA

- **A. VERIFIERING**
- **B. SEGMENTERING**
- **C. IAMSYSTEM**
- **D. BEHÖRIGHET**
- **E. ENHETSHÄLSA**
- **F. GRANSKNING**
- **G. BRANDVÄGG**
- **H. ROUTER**

DEFINITIONER OCH MATCHNINGSFÄLT

1. Skydd mot nätverk utifrån. ____
2. Genomgång av loggade åtkomstsessioner. ____
3. Principen om minsta åtkomsträttigheter. ____
4. Uppdelning av interna nätverkszoner. ____
5. Dirigering av nätverkspaketens trafik. ____
6. Utvärdering av enhetens hälsostatus. ____
7. Hantering av åtkomst till användaruppgifter. ____
8. Att alltid kontrollera användarens inloggningsuppgifter. ____

Kontrollpunkt 7: Utmaning med blandade ord

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

1. FENEIRVIRGI
2. MIESASTYM
3. EHSÄHNSATLE
4. DGGNÄVBRA
5. EIETGGERNSNM
6. ERÖGHBEITH
7. RNGNKINGSA
8. URRETO

Bonusaktivitet: Tänk snabbt

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

1	Information du aldrig bör dela			
2	Säkra vanor du kan börja med i dag			
3	Saker som kontrolleras på en enhet			
4	Saker som loggas			
5	Ord som hör ihop med cybersäkerhet			
6	Saker som Zero Trust kontrollerar			
7	Platser där du visar legitimation i vardagen			
8	Sätt att bevisa att det verkligen är du			
9	Saker att göra efter en dataläcka			
10	Tecken på att en dator är infekterad			
11	Skäl till att uppdatera programvara			
12	Åtkomstnivåer i ett företag			
13	Säkerhetsverktyg du känner till			
14	Zoner som ett nätverk kan delas upp i			
15	Ordspråk om förtroende			

Kontrollpunkt 8: Fallstudier om cybersäkerhet

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

FALLSTUDIE 1: ÖVERGÅNG TILL NOLLTILLITSARKITEKTUR FÖR NÄTVERK



Scenario: Ett stort företag använder för närvarande ett plant internt nätverk där alla enheter i det lokala nätverket kommer åt alla företagets servrar och databaser.

Diskussionsfråga: Utforma en strategi för mikrosegmentering av nätverket för att begränsa lateral rörelse.

FALLSTUDIE 2: INFÖRA ÅTKOMSTKONTROLL MED MINSTA MÖJLIGA BEHÖRIGHET



Scenario: Granskningsloggar visar att tillfälliga databasanvändare och anställda på låg nivå har globala läs- och skrivbehörigheter till kritiska bokföringsdatabaser.

Diskussionsfråga: Granska och begränsa databasens IAM-behörigheter för att tillämpa minsta möjliga behörighet.

Kontrollpunkt 9: Knäck chiffret

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

KRYPTERINGSNYCKEL FÖR BOKSTAV TILL SIFFRA

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

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

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

22	5	18	9	6	9	5	18	1	1	12	12	20	9	4	13	5	4	
26	5	18	15	20	18	21	19	20	1	18	11	9	20	5	11	20	21	18

Avkodat meddelande:

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

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

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

Q1: Vad är Zero Trust?

Zero Trust är ett säkerhetsramverk som utgår från att hot finns både utanför och innanför nätverksgränsen och som kräver verifiering av varje förfrågan. [1]

Q2: Vad är grundregeln i Zero Trust?

Lita aldrig på något, verifiera alltid.

Q3: Vad är mikrosegmentering?

Att dela upp ett nätverk i små, säkra logiska segment för att styra trafik och begränsa intrång.

Q4: Vad är minsta möjliga behörighet (least privilege)?

Att ge användare endast de minsta åtkomsträttigheter som krävs för deras specifika arbetsuppgifter. [2]

Q5: Vad står IAM för?

Hantering av identiteter och åtkomst.

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

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

Q6: Hur hjälper en enhetshållningskontroll (device posture check)?

Den verifierar att en enhet är uppdaterad, kör aktivt antivirusprogram och är säker innan åtkomst tillåts.

Q7: Vad är lateral rörelse?

Metoden som angripare använder för att ta sig genom ett nätverk från en första kompromitterad nod till system med högre värde.

Q8: Ersätter Zero Trust brandväggar?

Nej, den förstärker dem genom att lägga till identitetscentrerade kontroller och interna segmenteringsbrandväggar.

Q9: Vad är kontinuerlig autentisering?

Löpande verifiering av användarens identitet under en pågående inloggningssession, inte bara vid den första inloggningen.

Q10: Varför är ett platt nätverk farligt?

I platta nätverk ger en enda kompromitterad nod angripare enkel åtkomst till alla databaser i nätverket.

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

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

Q1: Hur hanterar Zero Trust perimetermodellen?

Den ersätter den föråldrade modellen med slott och vallgrav och flyttar försvaret från gränsnätverk till specifika användaridentiteter och resurser.

Q2: Vad är en policybeslutspunkt (PDP)?

Systemkomponenten som utvärderar auktoriseringsförfrågningar mot säkerhetsregler för att avgöra om åtkomst ska beviljas.

Q3: Vad är en policytillämpningspunkt (PEP)?

Systemnoden (som en gateway eller proxy) som fysiskt tillåter eller blockerar anslutningsförfrågningar utifrån PDP-beslutet.

Q4: Hur stöder rollbaserad åtkomstkontroll (RBAC) Zero Trust?

RBAC grupperar behörigheter i specifika roller, vilket hjälper till att förhindra att användare ärver alltför omfattande administrativa rättigheter.

Q5: Vad är kontextuell åtkomstkontroll?

Att utvärdera inloggningsförfrågningar med sekundära ledtrådar som geografisk plats, enhetens säkerhetsläge och inloggningstid för att bedöma risk.

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

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

Q6: Hur skiljer sig mikrosegmentering från vanliga VLAN?

VLAN delar upp nätverk i breda logiska segment på lager 2, medan mikrosegmentering använder programvarupolicyer för att isolera enskilda arbetsbelastningar.

Q7: Vad är just-in-time-åtkomst (JIT)?

Att tillfälligt ge förhöjda administratörsbehörigheter och automatiskt dra tillbaka dem när uppgiften är klar.

Q8: Hur skyddar man API:er i ett Zero Trust-ramverk?

Genom att kräva kryptografiskt signerade OAuth-token och granska förfrågningssignaturer vid varje API-gateway.

Q9: Vad är en klient för Zero Trust Network Access (ZTNA)?

Ett programagent som upprättar säkra, krypterade utgående anslutningar till specifika program i stället för råa nätverksundernät.

Q10: Hur hjälper loggrevision Zero Trust?

Kontinuerlig loggning gör att automatiserade säkerhetsanalysverktyg kan upptäcka avvikelser och omedelbart stänga av obehöriga inloggningar.

Del 11: 10 verkliga fakta och insikter om cybersäkerhet

Gå igenom verkliga fakta om säkerhetsintrång, försvarsmekanismer och efterlevnadsstandarder.

1. SÄKERHETSINSIKT

Zero Trust-arkitekturer ersätter den gamla slottsmodellen med vallgrav (castle-and-moat) med identitetscentrerade verifieringsregler.

2. SÄKERHETSINSIKT

Mikrosegmentering av nätverk krymper det område som skadlig kod kan nå genom att isolera arbetsbelastningar i små skyddade zoner.

3. SÄKERHETSINSIKT

Zero Trust fokuserar på att skydda resurser som tillgångar, tjänster och konton snarare än nätverkssegment. [1]

4. SÄKERHETSINSIKT

Policyer för minsta möjliga behörighet minskar risken att insiders för ut data från kärndatabaser.

5. SÄKERHETSINSIKT

Validering av enhetens säkerhetsläge kontrollerar i realtid operativsystemets korrigeringsnivåer och antivirusprogrammets aktiva status.

6. SÄKERHETSINSIKT

Mäklare för Zero Trust Network Access (ZTNA) kan ersätta eller komplettera företags-VPN för att begränsa användarnas åtkomstomfång.

7. SÄKERHETSINSIKT

Delegering av administrativa behörigheter Just-in-Time (JIT) minskar risken för stöld av inloggningsuppgifter på domänkontrollanter.

8. SÄKERHETSINSIKT

Kontinuerlig validering loggar och granskar sessionsbeteende och stänger av användare som visar avvikande mönster för skriptkörning.

9. SÄKERHETSINSIKT

Traditionella perimeterförsvar kan inte blockera sidledsattacker när en administratörsuppgift har läckt.

10. SÄKERHETSINSIKT

NIST Special Publication 800-207 (2020) ger en abstrakt definition av Zero Trust-arkitektur, med driftsättningsmodeller. [1]

Tekniska referenser och källor

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

VETENSKAPLIGA OCH BRANSCHRELATERADE REFERENSER

[1] NIST. (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

Facit: Kontrollpunkt 1 – Flerval

1 **Fråga 1** — **Rätt svar: A**

ANTECKNING FÖR LÄRAREN

Vad är kärnprincipen i Zero Trust-säkerhet? → Lita aldrig på något, verifiera alltid varje åtkomstförfrågan oavsett källa

2 **Fråga 2** — **Rätt svar: A**

ANTECKNING FÖR LÄRAREN

Vad är mikrosegmentering av nätverk? → Att dela upp nätverk i små, isolerade zoner för att begränsa lateral förflyttning

3 **Fråga 3** — **Rätt svar: A**

ANTECKNING FÖR LÄRAREN

Vad är principen om minsta möjliga behörighet? → Att begränsa användarnas åtkomstbehörigheter till det som är nödvändigt för deras arbete

4 **Fråga 4** — **Rätt svar: A**

ANTECKNING FÖR LÄRAREN

Vad är Identity and Access Management (IAM)? → Ramverk som hanterar digitala identiteter och styr systembehörigheter

5 **Fråga 5** — **Rätt svar: A**

ANTECKNING FÖR LÄRAREN

Vad innebär kontinuerlig autentisering? → Att upprepade gånger verifiera användarens identitet och enhetens hälsotillstånd under en aktiv session

Facit: Kontrollpunkt 2 – Sant eller falskt

6 Fråga 6

Rätt svar: Falskt

ANTECKNING FÖR LÄRAREN

Falskt: Zero Trust ger inget underförstått förtroende baserat på nätverksplats, vare sig inom eller utanför.

7 Fråga 7

Rätt svar: Sant

ANTECKNING FÖR LÄRAREN

Sant: små isolerade zoner begränsar hur långt en inkräktare kan röra sig mellan servrar.

8 Fråga 8

Rätt svar: Falskt

ANTECKNING FÖR LÄRAREN

Falskt: minsta möjliga behörighet ger bara den minsta åtkomst som varje roll behöver.

9 Fråga 9

Rätt svar: Sant

ANTECKNING FÖR LÄRAREN

Kontinuerlig verifiering validerar enhetens skick och inloggningsuppgifter under hela inloggningssessionen.

10 Fråga 10

Rätt svar: Sant

ANTECKNING FÖR LÄRAREN

Att införa Zero Trust minskar effekten av komprometterade företagsinloggningar.

Facit för ordförråd och bedömningsmall

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

KONTROLLPUNKT 4: FACIT – MATCHNING AV BEGREPP

G 1. VERIFIERING	F 2. SEGMENTERING	A 3. IAM	B 4. BEHÖRIGHET
H 5. SÄKERHETSLÄGE	E 6. GRANSKNING	D 7. BRANDVÄGG	C 8. ROUTER

KONTROLLPUNKT 3: FACIT – NYCKELBEGREPP

1 VERIFIERING	2 SEGMENTERING	3 IAM-SYSTEM	4 BEHÖRIGHET
5 ENHETSHÄLSA	6 GRANSKNING		

KONTROLLPUNKT 6, ALTERNATIV: FACIT – MATCHNING AV ORD

1 G – BRANDVÄGG	2 F – GRANSKNING	3 D – BEHÖRIGHET	4 B – SEGMENTERING
5 H – ROUTER	6 E – ENHETSHÄLSA	7 C – IAMSYSTEM	8 A – VERIFIERING

DISKUSSIONSANTECKNINGAR FÖR LÄRAREN

Nyckelbegrepp:
Kontrollera att eleverna kan förklara VERIFIERING, SEGMENTERING och IAM med egna ord och ge ett exempel på varje.

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

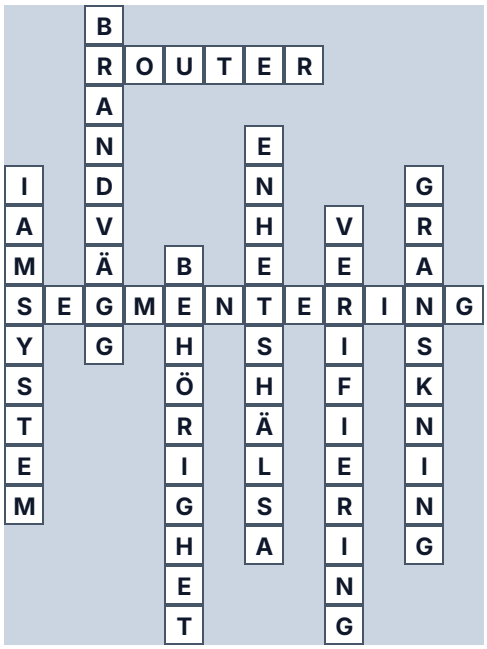
Källkritik:
Be eleverna att kontrollera minst ett påstående i arbetsbladets källor och diskutera varför siffror, priser och regler kan ändras över tid.

Facit till pussel och anteckningar för läraren

LÖSNING PÅ ORDSÖKET

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

LÖSNING PÅ KORSORDET



LÄRARHANDLEDNING MED LÖSNINGAR TILL KORSORDET

VÅGRÄTT

2 vågrätt: ROUTER Dirigering av nätverkspaketens trafik. (6 bokstäver)

8 vågrätt: SEGMENTERING Uppdelning av interna nätverkszoner. (12 bokstäver)

LODRÄTT

1 lodrätt: BRANDVÄGG Skydd mot nätverk utifrån. (9 bokstäver)

3 lodrätt: ENHETSHÄLSA Utvärdering av enhetens hälsostatus. (11 bokstäver)

4 lodrätt: IAMSYSTEM Hantering av åtkomst till användaruppgifter. (9 bokstäver)

5 lodrätt: GRANSKNING Genomgång av loggade åtkomstsessioner. (10 bokstäver)

6 lodrätt: VERIFIERING Att alltid kontrollera användarens inloggningsuppgifter. (11 bokstäver)

7 lodrätt: BEHÖRIGHET Principen om minsta åtkomsträttigheter. (10 bokstäver)

Facit för blandade ord och chiffer

Facit för övningen med ordvärlden och utmaningen Hemliga chiffret.

FACIT FÖR ORDBLANDNING

1.	FENEIRVIRGI	VERIFIERING	5.	EIETGGERNSNM	SEGMENTERING
2.	MIESASTYM	IAMSYSTEM	6.	ERÖGHBEITH	BEHÖRIGHET
3.	EHSÄHNSATLE	ENHETSHÄLSA	7.	RNGNKINGSA	GRANSKNING
4.	DGGNÄVBRA	BRANDVÄGG	8.	URRETO	ROUTER

NYCKEL TILL UTMANINGEN MED HEMLIGT CHIFFER

"VERIFIERA ALLTID MED ZERO TRUST ARKITEKTUR"

Facit till fallstudierna

A Fallstudie 1: Övergång till nolltillitsarkitektur för nätverk

Lärarens lösning

BEDÖMNINGSRIKTLINJE

Elevernas svar bör täcka följande punkter:

- Scenarioanalys: Ett stort företag använder just nu ett platt internt nätverk där varje enhet i det lokala nätverket kan komma åt alla företagets servrar och databaser.
- Rekommenderad strategi och lösning: Dela upp det platta nätverket i isolerade avdelningszoner. Installera interna brandväggar för att styra trafiken mellan zonerna och kräv validering av anslutningstoken för all åtkomst.

B Fallstudie 2: Införa åtkomstkontroll med minsta möjliga behörighet

Lärarens lösning

BEDÖMNINGSRIKTLINJE

Elevernas svar bör täcka följande punkter:

- Scenarioanalys: Granskningsloggar visar att tillfälliga databasanvändare och lågt placerade anställda har globala läs- och skrivbehörigheter till viktiga bokföringsdatabaser.
- Rekommenderad strategi och lösning: Återkalla alla globala administrativa behörigheter. Inför rollbaserad åtkomstkontroll (RBAC) som motsvarar exakta arbetsroller och inrätta veckovisa automatiska behörighetsgranskningar.