Naam: _____ Datum: _____ Score: _____

Zero Trust-architectuur en -beveiliging

Continue verificatie, micro-segmentatie van het netwerk, Identity and Access Management, minimale rechten en posture-controles.

OVERZICHT VAN LEREN OVER ZERO TRUST-BEVEILIGING

BEVEILIGD
GEGEVENSVERSLEUTELING
256-bits AES-standaard

COMPLIANT
WERELDWIJDE NORMEN
AVG- en CCPA-kaders

ZERO-TRUST
TOEGANGSBELEID
Multifactorauthenticatie

Welkom! Dit activiteitenpakket leidt je door de architectuur en beveiliging van Zero Trust. Je onderzoekt continue verificatie, netwerkmicrosegmentatie, identiteits- en toegangsbeheer (IAM), least privilege en sessie-auditing.

CONTROLEPUNTEN VAN HET WERKBLAD

- [ ] **Deel 1-4: Beheers cyberbeveiliging en dreigingspreventie.**
- [ ] **Deel 5-7: Los kruiswoord- en woordzoekpuzzels op.**
- [ ] **Deel 8-9: Los casestudy's en de codeopdracht op.**
- [ ] **Deel 10: Bekijk de pagina's met veelgestelde vragen (basis en gevorderd).**
- [ ] **Deel 11: Ontdek 10 interessante feiten uit de praktijk.**
- [ ] **Bonus: Snel denken-uitdaging.**

Open de VPN.com-gids over cyberbeveiliging

URL: https://www.vpn.com/nl/cyberbeveiliging/zero-trust-cyberbeveiliging/

Jouw leertraject: Zero Trust-strategie

- Begrijp het kernprincipe van continue verificatie.
- Voer netwerkmicrosegmentatie en toegang met minimale rechten in.
- Configureer controles van de apparaatstatus (posture) en actieve sessie-audits.

INSTRUCTIES VOOR DE ZERO TRUST-BEVEILIGINGSGIDS

Beantwoord de meerkeuzevragen en de vragen waar/onwaar, vul de zinnen aan met behulp van de woordenbank, koppel de definities en los de kruiswoordpuzzel en de woordzoeker op. Pas je kennis toe op Zero Trust-architectuur. Sluit af met de bonusopdracht Snel denken.

ZERO TRUST-ARCHITECTUUR EN -BEVEILIGING (INLEIDING)

Zero Trust-beveiliging vervangt oude netwerkperimetermodellen door een strikt beleid van 'vertrouw nooit, controleer altijd'. Microsegmentatie, Identity and Access Management (IAM), minimale rechten en posturecontroles blokkeren laterale beweging van bedreigingen.

LEES ELK CONTROLEPUNT ZORGVULDIG EN KIES OF SCHRIJF HET JUISTE ANTWOORD.

Controlepunt 1: Meerkeuzeopdracht

1. Wat is het kernprincipe van Zero Trust-beveiliging?

- A. Nooit vertrouwen, elk toegangsverzoek altijd verifiëren, ongeacht de bron
- B. Ervan uitgaan dat al het verkeer binnen de bedrijfsfirewall veilig is
- C. Databasebestanden onversleuteld opslaan om de snelheid te verbeteren
- D. E-mailauthenticatie afdwingen met alleen SPF-records

2. Wat is netwerkmicrosegmentatie?

- A. Netwerken opdelen in kleine, geïsoleerde zones om zijwaartse beweging in te dammen
- B. Netwerkkaarten versleutelen tijdens de gegevensoverdracht
- C. Alle lokale servers met één openbaar IP-adres verbinden
- D. Toetsaanslagen van gebruikers in browsersessies bewaken

3. Wat is het principe van minimale rechten (least privilege)?

- A. De toegangsrechten van gebruikers beperken tot wat voor hun werk noodzakelijk is
- B. Standaard alle systeemrechten aan elke gebruiker geven
- C. Anonieme aanmeldingen bij zakelijke databaseservers toestaan
- D. Openbare wifirouters zonder wachtwoord configureren

4. Wat is Identity and Access Management (IAM)?

- A. Raamwerken die digitale identiteiten beheren en systeembevoegdheden controleren
- B. Antivirusprogramma's die lokale bestandsmappen scannen
- C. Een back-upopslagsysteem met air-gapped media
- D. Een e-mailgatewayprotocol dat vervalste domeinen weigert

5. Wat betekent continue authenticatie?

- A. Tijdens een actieve sessie herhaaldelijk de identiteit van de gebruiker en de status van het apparaat verifiëren
- B. Het hoofdwachtwoord elke 10 minuten wijzigen
- C. Databaserecords hashen met meerdere algoritmen
- D. Netwerkverkeerspakketten versleutelen met TLS-sleutels

Controlepunt 2: Waar-of-onwaar-opdracht

6 Vraag 6

6. Zero Trust gaat ervan uit dat al het verkeer binnen de bedrijfsfirewall veilig is.

Waar Onwaar

7 Vraag 7

7. Micro-segmentatie beperkt het vermogen van aanvallers om zich zijwaarts over interne servers te bewegen.

Waar Onwaar

8 Vraag 8

8. Minimale rechten geven standaard toegang tot alle databasebestanden.

Waar Onwaar

9 Vraag 9

9. Continue verificatie valideert de gezondheid van het apparaat en de inloggegevens gedurende een hele inlogsessie.

Waar Onwaar

10 Vraag 10

10. Het implementeren van Zero Trust verkleint de impact van gecompromitteerde bedrijfslogins.

Waar Onwaar

Controlepunt 3: Kernbegrippen invullen

Lees elke zin hieronder en vul de open plek in met de juiste term uit de woordenbank.

1. Het vereisen van inloggegevens bij elk toegangspunt is continue _____ .

2. Het opdelen van het bedrijfsnetwerk in kleine zones is een vorm van _____ .

3. Het configureren van digitale identiteiten en toegangsbeheer gebeurt met een _____ .

4. Het beperken van gebruikersrechten volgt het principe van _____ .

5. Het beoordelen van de gezondheid van verbonden apparaten controleert de _____ van het apparaat.

6. Het vastleggen en beoordelen van actieve sessies heet _____ ten behoeve van de beveiliging.

WOORDENBANK

APPARAATSTATUS | AUDITING | FIREWALL | IAM-SYSTEEM | MINIMALE RECHTEN | ROUTER | SEGMENTATIE | VERIFICATIE

Schrijf hier je antwoorden:

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

Controlepunt 4: Beveiligingsbegrippen koppelen

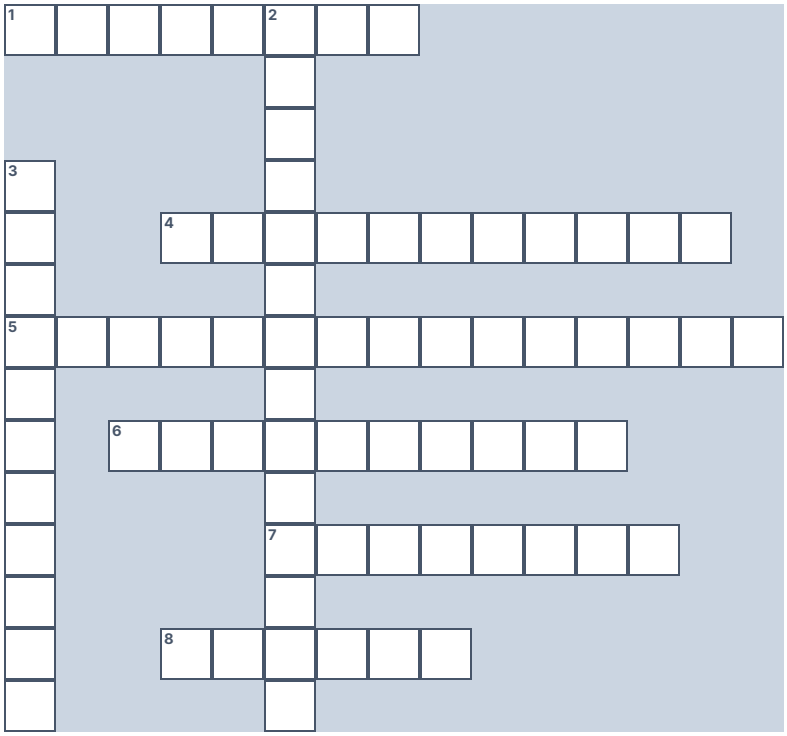
DEFINITIES KOPPELEN

Koppel elke term aan de linkerkant aan de juiste definitie aan de rechterkant door de bijbehorende letter (A-H) in het invulvak te schrijven.

☐	1. VERIFICATIE	A	Toegang tot gebruikersgegevens beheren.
☐	2. SEGMENTATIE	B	Principe van minimale toegangsrechten.
☐	3. IAM	C	Netwerkpakketverkeer routeren.
☐	4. PRIVILEGE	D	Bescherming met een externe netwerkbarrière.
☐	5. BEVEILIGINGSSTATUS	E	Gelogde toegangssessies controleren.
☐	6. AUDITEN	F	Interne netwerkzones opdelen.
☐	7. FIREWALL	G	Altijd de inloggegevens van gebruikers controleren.
☐	8. ROUTER	H	De gezondheidsstatus van het apparaat beoordelen.

Controlepunt 5: Kruiswoordpuzzel

Los de kruiswoordpuzzel op door letters in de actieve witte vakjes te typen. De nummers komen overeen met de aanwijzingen hieronder.



HORIZONTAAL

1. Beveiliging die het externe netwerk afschermt. (8)

4. Altijd de inloggegevens van gebruikers controleren. (11)

5. Principe van de minste toegangsrechten. (15)

6. Toegang van gebruikers tot inloggegevens beheren. (10)

7. Gelogde toegangssessies beoordelen. (8)

8. Netwerkpakketverkeer routeren. (6)

VERTICAAL

2. De gezondheidsstatus van apparaten beoordelen. (14)

3. Interne netwerkzones opdelen. (11)

Controlepunt 5, alternatief: Toegankelijke kruiswoordaanwijzingen

Gebruikers van schermlezers en toetsenborden kunnen de antwoorden van de kruiswoordpuzzel rechtstreeks typen in de tekstvelden hieronder.

HORIZONTAAL

1 horizontaal: Beveiliging die het externe netwerk afschermt. (8 letters):

4 horizontaal: Altijd de inloggegevens van gebruikers controleren. (11 letters):

5 horizontaal: Principe van de minste toegangsrechten. (15 letters):

6 horizontaal: Toegang van gebruikers tot inloggegevens beheren. (10 letters):

7 horizontaal: Gelogde toegangssessies beoordelen. (8 letters):

8 horizontaal: Netwerkpakketverkeer routeren. (6 letters):

VERTICAAL

2 verticaal: De gezondheidsstatus van apparaten beoordelen. (14 letters):

3 verticaal: Interne netwerkzones opdelen. (11 letters):

Controlepunt 6: Verborgen woorden zoeken

Zoek de 8 belangrijkste vakwoorden die in het onderstaande rooster verborgen zijn. Woorden kunnen horizontaal, verticaal of diagonaal staan.

A F G O K N D M N C D H I B A

P R N L P W T I I Y A F Y S G

E X I W H R F N R T P N U K R

I D T T I E S I L P P L M S H

T K I P A T H M Y P A L E W U

A N D Y M U Q A Q B R A I L F

C P U M S O B L L I A F T I I

I N A Y Y R B E Z Z A Y A B R

F N V X S M C R F P T W T Q E

I Q X H T E Y E C W S L N F W

R G H Z E W C C O R T J E X A

E X R K E Z A H N R A Z M R L

V M G S M W G T L W T J G B L

Y C C Y O U Z E O Z U U E T B

H V P X C N M N H P S X S Y Z

WOORDENLIJST

VERIFICATIE SEGMENTATIE IAMSYSTEEM MINIMALERECHTEN APPARAATSTATUS AUDITING FIREWALL ROUTER

Controlepunt 6, alternatief: Toegankelijk woordenschat koppelen

Koppel elk van de 8 vaktermen uit de woordzoeker aan de juiste definitie door de letter (A-H) in de lege ruimte te schrijven.

BEGRIPPEN
A. VERIFICATIE
B. SEGMENTATIE
C. IAMSYSTEEM
D. MINIMALERECHTEN
E. APPARAATSTATUS
F. AUDITING
G. FIREWALL
H. ROUTER

DEFINITIES EN KOPPELVELDEN

1. Beveiliging die het externe netwerk afschermt. ____
2. Gelogde toegangssessies beoordelen. ____
3. Principe van de minste toegangsrechten. ____
4. Interne netwerkzones opdelen. ____
5. Netwerkpakketverkeer routeren. ____
6. De gezondheidsstatus van apparaten beoordelen. ____
7. Toegang van gebruikers tot inloggegevens beheren. ____
8. Altijd de inloggegevens van gebruikers controleren. ____

Controlepunt 7: Opdracht met door elkaar gehaalde woorden

Ontcijfer de letters hieronder om kernbegrippen van cyberbeveiliging te onthullen. Schrijf je antwoorden in de invulvelden.

1. FCIEIAVTREI
2. ESIAYMTESM
3. ASPUTSTAPARATA
4. ELLAWFIR
5. TEATGEENSIM
6. HLTNAEEENCMIRIM
7. AGTINUID
8. URRETO

Bonusopdracht: Snel denken

3 ANTWOORDEN PER CATEGORIE. WIE DE LIJST ALS EERSTE INVULT, WINT.

1	Informatie die je nooit zou moeten delen			
2	Veilige gewoonten die je vandaag kunt beginnen			
3	Dingen die op een apparaat worden gecontroleerd			
4	Dingen die worden gelogd			
5	Woorden die met cyberbeveiliging te maken hebben			
6	Dingen die Zero Trust controleert			
7	Plekken waar je in het dagelijks leven je legitimatie laat zien			
8	Manieren om te bewijzen dat jij het echt bent			
9	Dingen die je doet na een datalek			
10	Tekenen dat een computer is geïnfecteerd			
11	Redenen om software bij te werken			
12	Toegangsniveaus in een bedrijf			
13	Beveiligingstools die je kent			
14	Zones waarin een netwerk kan worden opgedeeld			
15	Gezegden over vertrouwen			

Controlepunt 8: Casestudy's cyberbeveiliging

Pas de concepten die je hebt geleerd toe om de onderstaande praktijkscenario's op te lossen.

CASESTUDY 1: OVERSTAP NAAR EEN ZERO TRUST-NETWERKARCHITECTUUR



Scenario: Een groot bedrijf gebruikt momenteel een plat intern netwerk waarin elk apparaat op het lokale netwerk toegang heeft tot alle zakelijke servers en databases.

Discussievraag: Ontwerp een strategie voor micro-segmentatie van het netwerk om zijwaartse beweging te beperken.

CASESTUDY 2: TOEGANGSCONTROLES MET MINIMALE RECHTEN IMPLEMENTEREN



Scenario: Auditlogs laten zien dat tijdelijke databasegebruikers en medewerkers op laag niveau globale lees- en schrijfrechten hebben op kritieke boekhoudkundige databases.

Discussievraag: Controleer de IAM-rechten voor de database en beperk ze om least privilege af te dwingen.

Controlepunt 9: De code ontcijferen

Een cyberbeveiligingsprofessional beschermt netwerkmiddelen tegen online bedreigers. Gebruik de onderstaande letter-naar-cijfersleutel om het bericht te ontcijferen door de bijbehorende letters in de lege vakjes te schrijven.

LETTER-NAAR-CIJFER-VERSLEUTELINGSSLEUTEL

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

3	15	14	20	18	15	12	5	5	18		1	12	20	9	10	4		13	5	20
26	5	18	15		20	18	21	19	20											
1	18	3	8	9	20	5	3	20	21	21	18									

Ontcijferd bericht:

TIP: ELK GETAL STAAT VOOR DE POSITIE VAN DIE LETTER IN HET ALFABET (BIJV. 1 = A, 2 = B, 26 = Z).

Controlepunt 10: Veelgestelde vragen over cyberbeveiliging – basis (Deel A)

Bekijk veelgestelde vragen en antwoorden over het beperken van online dreigingen.

Q1: Wat is Zero Trust?

Zero Trust is een beveiligingsraamwerk dat ervan uitgaat dat er zowel buiten als binnen de netwerkgrens bedreigingen bestaan, en voor elk verzoek verificatie vereist. [1]

Q2: Wat is de kernregel van Zero Trust?

Vertrouw nooit, controleer altijd.

Q3: Wat is microsegmentatie?

Een netwerk opdelen in kleine, beveiligde logische segmenten om verkeer te beheersen en inbreuken in te perken.

Q4: Wat is least privilege?

Gebruikers alleen de minimale toegangsrechten geven die nodig zijn voor hun specifieke werktaken. [2]

Q5: Waar staat IAM voor?

Identity and Access Management (identiteits- en toegangsbeheer).

Controlepunt 10: Veelgestelde vragen over cyberbeveiliging – basis (Deel B)

Bekijk veelgestelde vragen en antwoorden over het beperken van online dreigingen.

Q6: Hoe helpt een apparaat-posture check?

Het controleert of een apparaat is gepatcht, actieve antivirussoftware draait en veilig is voordat toegang wordt verleend.

Q7: Wat is laterale beweging?

Het proces waarmee aanvallers zich door een netwerk bewegen, van een eerste gecompromitteerde node naar systemen met een hogere waarde.

Q8: Vervangt Zero Trust firewalls?

Nee, het versterkt ze door controles op basis van identiteit en interne segmentatiefirewalls toe te voegen.

Q9: Wat is continue authenticatie?

Voortdurende verificatie van de identiteit van de gebruiker gedurende een actieve inlogsessie, niet alleen bij de eerste aanmelding.

Q10: Waarom is een vlak netwerk gevaarlijk?

In platte netwerken geeft één gecompromitteerde node aanvallers gemakkelijk toegang tot elke database op het netwerk.

Controlepunt 10: Veelgestelde vragen over beveiliging – gevorderd (Deel C)

Verken geavanceerde technische aspecten van beveiligingsframeworks, malwareanalyse en gegevenscompliance.

Q1: Hoe pakt Zero Trust het perimetermodel aan?

Het vervangt het verouderde 'kasteel-en-slotgracht'-model en verschuift de verdediging van netwerkgrenzen naar specifieke gebruikersidentiteiten en resources.

Q2: Wat is een policy decision point (PDP)?

Het systeemonderdeel dat autorisatieverzoeken toetst aan beveiligingsregels om te bepalen of toegang moet worden verleend.

Q3: Wat is een policy enforcement point (PEP)?

De systeemnode (zoals een gateway of proxy) die verbindingsverzoeken fysiek toestaat of blokkeert op basis van de PDP-beslissing.

Q4: Hoe ondersteunt rolgebaseerd toegangsbeheer (RBAC) Zero Trust?

RBAC groepeert rechten in specifieke rollen, waardoor wordt voorkomen dat gebruikers buitensporige beheerdersrechten erven.

Q5: Wat is contextuele toegangscontrole?

Inloggegevens beoordelen aan de hand van secundaire aanwijzingen zoals geografische locatie, apparaatstatus en inlogtijd om het risico in te schatten.

Controlepunt 10: Veelgestelde vragen over beveiliging – gevorderd (Deel D)

Verken geavanceerde technische aspecten van beveiligingsframeworks, malwareanalyse en gegevenscompliance.

Q6: Waarin verschilt microsegmentatie van standaard-VLAN's?

VLAN's verdelen netwerken op laag 2 in brede logische segmenten, terwijl microsegmentatie softwarebeleid gebruikt om afzonderlijke workloads te isoleren.

Q7: Wat is just-in-time-toegang (JIT)?

Tijdelijk verhoogde beheerrechten toekennen en die automatisch intrekken zodra de taak is afgerond.

Q8: Hoe beveilig je API's in een Zero Trust-raamwerk?

Door cryptografisch ondertekende OAuth-tokens te eisen en de handtekeningen van verzoeken bij elke API-gateway te auditen.

Q9: Wat is een zero-trust-netwerktoegangsclient (ZTNA)?

Een softwareagent die beveiligde, versleutelde uitgaande verbindingen opzet met specifieke applicaties in plaats van met ruwe netwerksubnetten.

Q10: Hoe helpt het auditen van logs bij Zero Trust?

Continue logging stelt geautomatiseerde beveiligingsanalysetools in staat om afwijkingen te detecteren en ongeautoriseerde aanmeldingen direct op te schorten.

Deel 11: 10 cyberbeveiligingsfeiten en inzichten uit de praktijk

Bekijk feiten uit de praktijk over beveiligingsincidenten, verdedigingsmechanismen en compliancenormen.

1. BEVEILIGINGSINZICHT

Zero Trust-architecturen vervangen het verouderde kasteel-en-slotgrachtmodel door op identiteit gerichte verificatieregels.

2. BEVEILIGINGSINZICHT

Netwerkmicrosegmentatie verkleint het gebied dat malware kan bereiken door workloads te isoleren in kleine beschermde zones.

3. BEVEILIGINGSINZICHT

Zero Trust richt zich op het beschermen van resources zoals bedrijfsmiddelen, diensten en accounts in plaats van netwerksegmenten. [1]

4. BEVEILIGINGSINZICHT

Toegangsbeleid met minimale rechten verkleint het risico dat insiders gegevens uit kerndatabases weghalen.

5. BEVEILIGINGSINZICHT

Validatie van de apparaatstatus controleert in realtime het patchniveau van het besturingssysteem en de actieve status van het antivirusprogramma.

6. BEVEILIGINGSINZICHT

Brokers voor Zero Trust Network Access (ZTNA) kunnen bedrijfs-VPN's vervangen of aanvullen om de reikwijdte van gebruikerstoegang te beperken.

7. BEVEILIGINGSINZICHT

Just-in-Time-delegatie (JIT) van administratieve rechten verkleint het risico op diefstal van inloggegevens op domeincontrollers.

8. BEVEILIGINGSINZICHT

Continue validatie registreert en controleert sessiegedrag en schort gebruikers op die afwijkende patronen in scriptuitvoering vertonen.

9. BEVEILIGINGSINZICHT

Traditionele perimeterbeveiliging kan laterale aanvallen niet tegenhouden zodra een beheerdersreferentie is uitgelekt.

10. BEVEILIGINGSINZICHT

NIST Special Publication 800-207 (2020) geeft een abstracte definitie van de Zero Trust-architectuur, met implementatiemodellen. [1]

Technische referenties en bronnen

De studiegids en de interactieve puzzels zijn samengesteld uit wereldwijde NIST- en OWASP-standaarden en standaarden voor naleving van gegevensprivacy.

WETENSCHAPPELIJKE EN BRANCHEREFERENTIES

[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

Antwoordsleutel: Controlepunt 1 - Meerkeuze

1 Vraag 1

Juist antwoord: A

DOCENTENNOTITIE

Wat is het kernprincipe van Zero Trust-beveiliging? → Nooit vertrouwen, elk toegangsverzoek altijd verifiëren, ongeacht de bron

2 Vraag 2

Juist antwoord: A

DOCENTENNOTITIE

Wat is netwerkmicrosegmentatie? → Netwerken opdelen in kleine, geïsoleerde zones om zijwaartse beweging in te dammen

3 Vraag 3

Juist antwoord: A

DOCENTENNOTITIE

Wat is het principe van minimale rechten (least privilege)? → De toegangsrechten van gebruikers beperken tot wat voor hun werk noodzakelijk is

4 Vraag 4

Juist antwoord: A

DOCENTENNOTITIE

Wat is Identity and Access Management (IAM)? → Raamwerken die digitale identiteiten beheren en systeembevoegdheden controleren

5 Vraag 5

Juist antwoord: A

DOCENTENNOTITIE

Wat betekent continue authenticatie? → Tijdens een actieve sessie herhaaldelijk de identiteit van de gebruiker en de status van het apparaat verifiëren

Antwoordsleutel: Controlepunt 2 - Waar of onwaar

6 Vraag 6

Juist antwoord: Onwaar

DOCENTENNOTITIE

Onwaar: Zero Trust verleent geen impliciet vertrouwen op basis van de netwerklocatie, binnen of buiten.

7 Vraag 7

Juist antwoord: Waar

DOCENTENNOTITIE

Waar: kleine geïsoleerde zones beperken hoe ver een indringer zich tussen servers kan bewegen.

8 Vraag 8

Juist antwoord: Onwaar

DOCENTENNOTITIE

Onwaar: least privilege verleent alleen de minimale toegang die elke rol nodig heeft.

9 Vraag 9

Juist antwoord: Waar

DOCENTENNOTITIE

Continue verificatie valideert de gezondheid van het apparaat en de inloggegevens gedurende een hele inlogsessie.

10 Vraag 10

Juist antwoord: Waar

DOCENTENNOTITIE

Het implementeren van Zero Trust verkleint de impact van gecompromitteerde bedrijfslogins.

Woordenlijstsleutels en beoordelingsrubriek

Beoordelingsrubriek voor docenten: Geef 1 punt voor elke juiste koppeling (totaal 8 punten) en elk juist contextbegrip (totaal 6 punten).

CONTROLEPUNT 4: ANTWOORDEN BEGRIPPEN KOPPELEN

G 1. VERIFICATIE	F 2. SEGMENTATIE	A 3. IAM	B 4. PRIVILEGE
H 5. BEVEILIGINGSSTATUS	E 6. AUDITEN	D 7. FIREWALL	C 8. ROUTER

CONTROLEPUNT 3: ANTWOORDEN KERNBEGRIPPEN

1 VERIFICATIE	2 SEGMENTATIE	3 IAM-SYSTEEM	4 MINIMALE RECHTEN
5 APPARAATSTATUS	6 AUDITING		

CONTROLEPUNT 6, ALTERNATIEF: ANTWOORDEN WOORDEN KOPPELEN

1 G – FIREWALL	2 F – AUDITING	3 D – MINIMALERECHTEN	4 B – SEGMENTATIE
5 H – ROUTER	6 E – APPARAATSTATUS	7 C – IAMSYSTEEM	8 A – VERIFICATIE

DISCUSSIENOTITIES VOOR DOCENTEN

Kernbegrippen:
Controleer of leerlingen VERIFICATIE, SEGMENTATIE en IAM in eigen woorden kunnen uitleggen en van elk een voorbeeld kunnen geven.

Casestudy's:
Laat leerlingen hun aanbevelingen onderbouwen met feiten uit het werkblad in plaats van met aannames.

Bronnen beoordelen:
Laat leerlingen ten minste één bewering controleren aan de hand van de bronnen in het werkblad en bespreek waarom cijfers, prijzen en regels kunnen veranderen.

Puzzelsleutels en docentennotities

OPLOSSING WOORDZOEKER

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

OPLOSSING VAN DE KRUISWOORDPUZZEL

F	I	R	E	W	A	L	L							
					P									
					P									
S					A									
E			V	E	R	I	F	I	C	A	T	I	E	
G					A									
M	I	N	I	M	A	L	E	R	E	C	H	T	E	N
E					T									
N		I	A	M	S	Y	S	T	E	E	M			
T					T									
A					A	U	D	I	T	I	N	G		
T					T									
I			R	O	U	T	E	R						
E					S									

DOCENTENGIDS VOOR DE OPLOSSINGEN VAN DE KRUISWOORDPUZZEL

HORIZONTAAL

1 horizontaal: FIREWALL Beveiliging die het externe netwerk afschermt. (8 letters)

4 horizontaal: VERIFICATIE Altijd de inloggegevens van gebruikers controleren. (11 letters)

5 horizontaal: MINIMALERECHTEN Principe van de minste toegangsrechten. (15 letters)

6 horizontaal: IAMSYSTEEM Toegang van gebruikers tot inloggegevens beheren. (10 letters)

7 horizontaal: AUDITING Gelogde toegangssessies beoordelen. (8 letters)

8 horizontaal: ROUTER Netwerkpakketverkeer routeren. (6 letters)

VERTICAAL

2 verticaal: APPARAATSTATUS De gezondheidsstatus van apparaten beoordelen. (14 letters)

3 verticaal: SEGMENTATIE Interne netwerkzones opdelen. (11 letters)

Sleutel voor husselwoorden en coderaadsel

Beoordelingssleutel voor de woordenschatopdracht met door elkaar gehusselde woorden en de Geheime codeopdracht.

SLEUTEL WOORDEN ORDENEN

1. FCIEIAVTREI — **VERIFICATIE**
2. ESIAYMTESM — **IAMSYSTEEM**
3. ASPUTSTAPARATA — **APPARAATSTATUS**
4. ELLAWFIR — **FIREWALL**
5. TEATGEENSIM — **SEGMENTATIE**
6. HLTNAEEENCMIRIM — **MINIMALERECHTEN**
7. AGTINUID — **AUDITING**
8. URRETO — **ROUTER**

SLEUTEL VOOR DE GEHEIME CODE-OPDRACHT

"CONTROLEER ALTIJD MET ZERO TRUST ARCHITECTUUR"

Antwoordsleutel casestudy's

A Casestudy 1: Overstap naar een zero-trust-netwerkarchitectuur

Oplossing voor docenten

BEOORDELINGSRICHTLIJN

De antwoorden van leerlingen moeten de volgende punten behandelen:

- Scenarioanalyse: Een grote onderneming gebruikt momenteel een plat intern netwerk waarop elk apparaat in het lokale netwerk toegang heeft tot alle bedrijfsservers en databases.
- Aanbevolen strategie en oplossing: Verdeel het platte netwerk in geïsoleerde afdelingszones. Installeer interne firewalls om het verkeer tussen zones te beheersen en verplicht validatie van verbindingstokens voor alle toegang.

B Casestudy 2: Toegangscontroles met minimale rechten implementeren

Oplossing voor docenten

BEOORDELINGSRICHTLIJN

De antwoorden van leerlingen moeten de volgende punten behandelen:

- Scenarioanalyse: Auditlogboeken tonen aan dat tijdelijke databasegebruikers en medewerkers op laag niveau globale lees- en schrijfrechten hebben op cruciale boekhoudkundige databases.
- Aanbevolen strategie en oplossing: Trek alle globale beheerdersrechten in. Voer rolgebaseerde toegangscontrole (RBAC) in die aansluit op de exacte functierollen en stel wekelijkse geautomatiseerde machtigingscontroles in.