Naam: _____ Datum: _____ Score: _____

Beveiliging en versleuteling van openbaar wifi

Man-in-the-middle-aanvallen, malafide toegangspunten, packet sniffing, VPN-tunnels en HTTPS-versleuteling.

LEEROVERZICHT BEVEILIGING VAN OPENBAAR WIFI

BEVEILIGD
GEGEVENSVERSLEUTELING
256-bits AES-standaard

COMPLIANT
WERELDWIJDE NORMEN
AVG- en CCPA-kaders

ZERO-TRUST
TOEGANGSBELEID
Multifactorauthenticatie

Welkom! Dit activiteitenpakket leidt je door openbare wifi-beveiliging. Je onderzoekt onversleutelde netwerken, man-in-the-middle-aanvallen (MitM), nep-toegangspunten, packet sniffing, VPN-tunnels en HTTPS-beveiliging tijdens het transport.

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/beveiliging-openbare-wifi/

Jouw leertraject: beveiliging van openbare wifi

- Veelvoorkomende risico's van openbare wifi herkennen, waaronder packet sniffing en kwaadaardige toegangspunten.
- Zet VPN-versleutelingstunnels in om gegevens tijdens transport te beveiligen.
- Dwing HTTPS en beveiligde webbrowserinstellingen af voor medewerkers op afstand.

INSTRUCTIES VOOR DE GIDS OVER BEVEILIGING VAN OPENBAAR WIFI

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 beveiliging van externe toegang. Sluit af met de bonusopdracht Snel denken.

BEVEILIGING VAN OPENBAAR WIFI EN BESCHERMING VAN VERKEER ONDERWEG (INLEIDING)

Onversleutelde openbare wifi-hotspots stellen netwerkverkeer bloot aan packet sniffing en Evil Twin-spoofing. Door verkeer via beveiligde VPN-versleutelingstunnels te sturen en HSTS-regels met alleen HTTPS af te dwingen, worden sessies afgeschermd tegen onderschepping op het lokale netwerk.

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

Controlepunt 1: Meerkeuzeopdracht

1. Wat is een man-in-the-middle-aanval (MitM)?

- A. Communicatie tussen twee partijen op een gedeeld netwerk onderscheppen en wijzigen
- B. Een techniek om databasegegevens te onttrekken, gericht op gebruikersrecords
- C. Webservers overspoelen met netwerkverkeersaanvragen
- D. Lokale opslagvolumes van de harde schijf wissen

2. Wat is een nep-toegangspunt (rogue access point, Evil Twin)?

- A. Een kwaadaardige wifihotspot die is ingesteld met dezelfde SSID als een legitiem netwerk
- B. Een beheerprogramma voor het bewaken van databaseback-ups
- C. Een configuratie van een beveiligde VPN-gateway
- D. Een DNS-record dat geautoriseerde mailservers koppelt

3. Hoe beschermt een VPN verkeer op openbare wifi?

- A. Het verpakt alle netwerkpakketten in een versleutelde tunnel, zodat ze voor sniffers onleesbaar zijn
- B. Het blokkeert automatisch alle inkomende verbindingsverzoeken
- C. Het wijzigt het MAC-adres van de fysieke netwerkkaart
- D. Het verwijdert gecachete cookies in de webbrowser

4. Wat is packet sniffing?

- A. Hardware- of softwarehulpmiddelen gebruiken om netwerkpakketten vast te leggen en te loggen
- B. Lokale mappen scannen op dubbele bestanden
- C. Leesrechten op databases beperken op basis van gebruikersrollen
- D. Opslagschijven versleutelen met AES-256-sleutels

5. Wat is de rol van HTTPS?

- A. Sessieverkeer tussen de browser en de webserver versleutelen
- B. Binnenkomende e-mailberichten filteren op de gateway
- C. Afbeeldingen comprimeren voor sneller ladende pagina's
- D. Bestandsstructuren beheren in netwerkopslag (NAS)

Controlepunt 2: Waar-of-onwaar-opdracht

6 Vraag 6

6. Verbonden gebruikers kunnen op open openbare wifinetwerken gemakkelijk platte-tekstgegevens onderscheppen.

- ◯ Waar
- ◯ Onwaar

7 Vraag 7

7. Frauduleuze toegangspunten (Evil Twins) worden altijd goedgekeurd door netwerkbeheerders.

- ◯ Waar
- ◯ Onwaar

8 Vraag 8

8. Een VPN is niet effectief in het beschermen van verkeer tegen packet sniffing op openbare netwerken.

- ◯ Waar
- ◯ Onwaar

9 Vraag 9

9. HTTPS versleutelt alleen het URL-pad en laat de payload van het pakket als leesbare tekst achter.

- ◯ Waar
- ◯ Onwaar

10 Vraag 10

10. Wifi-hotspots met WPA3-beveiliging bieden sterkere bescherming dan open netwerken zonder wachtwoord.

- ◯ 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 vastleggen van privéwachtwoorden op openbare wifi is het _____ van communicatie.

2. Het analyseren van ruwe pakketten op een lokaal netwerk gebeurt door middel van _____ pakketten.

3. Een nephotspot die de wifi van een hotel nabootst, is een _____ .

4. Het beveiligen van webverkeer tijdens transport vereist versleuteling met _____ .

5. Het versleutelen van alle netwerkuitvoer gebeurt met een _____ .

6. Een versleuteld communicatiepad via openbare netwerken is een _____ .

WOORDENBANK

EVIL TWIN FIREWALL HTTPS ONDERSCHEPPING SNIFFING TUNNEL VPN-CLIENT WPA-DRIE

Schrijf hier je antwoorden:

1. **2.**

3. **4.**

5. **6.**

Controlepunt 4: Beveiligingsbegrippen koppelen

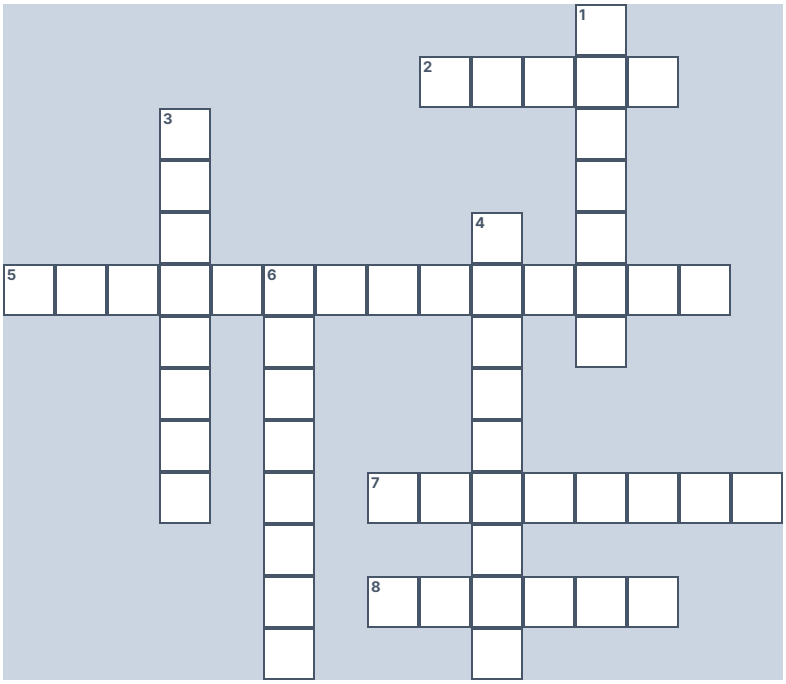
DEFINITIES KOPPELEN

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. ONDERSCHEPPING	A	Moderne wifibeveiligingsstandaard.
☐	2. SNIFFING	B	Beveiligd gegevenspad tijdens verzending.
☐	3. EVIL TWIN	C	Inkomend verkeer filteren.
☐	4. HTTPS	D	Frauduleuze hotspot die zich voordoet als wifi.
☐	5. VPN	E	Verkeer lezen tijdens verzending.
☐	6. TUNNEL	F	Netwerkdatapakketten onderscheppen.
☐	7. WPA3	G	Versleuteld virtueel privénetwerk.
☐	8. FIREWALL	H	Beveiligde webverzending.

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

2. Beveiligde webtransmissie. (5)

5. Het lezen van verkeer tijdens het transport. (14)

7. Nephotspot die een wifi-netwerk nabootst. (8)

8. Beveiligd datapad tijdens het transport. (6)

VERTICAAL

1. Moderne wifi-beveiligingsstandaard (WPA3). (7)

3. Het filteren van inkomend verkeer. (8)

4. Versleuteld virtueel privénetwerk. (9)

6. Het vastleggen van netwerkdatapakketten. (8)

Controlepunt 5, alternatief: Toegankelijke kruiswoordaanwijzingen

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

HORIZONTAAL

2 horizontaal: Beveiligde webtransmissie. (5 letters):

5 horizontaal: Het lezen van verkeer tijdens het transport. (14 letters):

7 horizontaal: Nephotspot die een wifi-netwerk nabootst. (8 letters):

8 horizontaal: Beveiligd datapad tijdens het transport. (6 letters):

VERTICAAL

1 verticaal: Moderne wifi-beveiligingsstandaard (WPA3). (7 letters):

3 verticaal: Het filteren van inkomend verkeer. (8 letters):

4 verticaal: Versleuteld virtueel privénetwerk. (9 letters):

6 verticaal: Het vastleggen van netwerkdatapakketten. (8 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.

T U N N E L I E N N K Q P G M

M Q R S T T S V G C F S Q O H

S E B W D P S I Z V I C Z W F

T I K H T Z D L N D R Q X P C

N R U T B A Z T N D E K A S D

E D H O D F H W I D W R Q N M

I A E I R Z S I F Q A V F I A

L P A Q O N P N T X L Q K F R

C W U S D N Y B F S L X W F J

N A R Z Y Y L G I M R J M I L

P O N D E R S C H E P P I N G

V T O H Q Q H Z A O V G U G B

Y R Y B H L Z G J O P N W C M

Z Y G Y O W U K V P B N V T M

G V D Y U K R B X Z Y M R Q X

WOORDENLIJST

ONDERSCHEPPING SNIFFING EVILTWIN HTTPS VPNCLIENT TUNNEL WPADRIE FIREWALL

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. ONDERSCHEPPING**
- **B. SNIFFING**
- **C. EVILTWIN**
- **D. HTTPS**
- **E. VPNCLIENT**
- **F. TUNNEL**
- **G. WPADRIE**
- **H. FIREWALL**

DEFINITIES EN KOPPELVELDEN

1. Moderne wifi-beveiligingsstandaard (WPA3).
2. Nephotspot die een wifi-netwerk nabootst.
3. Het vastleggen van netwerkdatapakketten.
4. Beveiligd datapad tijdens het transport.
5. Het filteren van inkomend verkeer.
6. Het lezen van verkeer tijdens het transport.
7. Versleuteld virtueel privénetwerk.
8. Beveiligde webtransmissie.

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. PSHPCDNEIONGRE
2. LENVIWTI
3. VILPETCNN
4. EPRDIWA
5. FINGFSNI
6. PHTST
7. ETNLNU
8. EIWLFLAR

Bonusopdracht: Snel denken

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

1	Redenen om software bij te werken			
2	Apparaten die automatisch verbinding maken met wifi			
3	Informatie die je nooit zou moeten delen			
4	Veilige gewoonten die je vandaag kunt beginnen			
5	Manieren om veilig te blijven in een café			
6	Apparaten die gehackt kunnen worden			
7	Dingen die een hacker kan zien op open wifi			
8	Tekenen van een nep-wifinetwerk			
9	Alternatieven voor openbare wifi			
10	Waarschuwingssignalen in een e-mail			
11	Dingen die je niet doet op openbare wifi			
12	Plekken met gratis wifi			
13	Manieren om je accounts te beschermen			
14	Tekenen dat een computer is geïnfecteerd			
15	Wifinamen die verdacht lijken			

Controlepunt 8: Casestudy's cyberbeveiliging

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

CASESTUDY 1: INDAMMEN VAN PAKKETSNUFFELEN OP OPENBARE WIFI



Scenario: Een verkoopmanager op afstand die met een openbaar wifinetwerk op een luchthaven is verbonden, merkt dat meerdere gevoelige zakelijke e-mails kort nadat ze in platte tekst zijn verzonden, zijn gelekt.

Discussievraag: Analyseer de risico's van openbare netwerken en schets een oplossing voor het versleutelen van verkeer.

CASESTUDY 2: VERDEDIGING TEGEN EEN EVIL TWIN-ROGUE HOTSPOT



Scenario: Aanvallers zetten een nep draadloos toegangspunt met de naam 'CoffeeShop_Guest' in dat een legitieme hotspot van een café nabootst en netwerkverkeer van nietsvermoedende gasten onderschept.

Discussievraag: Beschrijf in detail de verificatiestappen om nep-toegangspunten te detecteren en te blokkeren.

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

22	5	18	19	12	5	21	20	5	12		22	5	18	11	5	5	18		15	16
15	16	5	14	2	1	1	18		23	9	6	9		13	5	20		5	5	14
									22	16	14									

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: Waarom is openbaar wifi onveilig?

Openbaar wifi versleutelt het verkeer door de lucht niet, dus anderen in de buurt kunnen onbeschermde gegevens onderscheppen. [2]

Q2: Wat is packet sniffing?

Een packet sniffer legt de ruwe gegevens vast die over een netwerkinterface stromen, waardoor wachtwoorden in leesbare tekst en verkeersdetails zichtbaar worden.

Q3: Wat is een Evil Twin?

Een door hackers opgezet nep-toegangspunt dat de naam en instellingen van een vertrouwde lokale wifihotspot nabootst.

Q4: Hoe beschermt een VPN mij?

Het routeert je verkeer via een versleutelde tunnel en verbergt je surfactiviteit voor snuffelaars op het lokale netwerk.

Q5: Beschermt HTTPS mij op openbare wifi?

Ja, het versleutelt de gegevens die tussen je browser en de website worden uitgewisseld, en een VPN voegt nog een beschermingslaag toe.

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

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

Q6: Wat is WPA3?

De moderne Wi-Fi Protected Access-standaard, met sterkere versleuteling en bescherming tegen offline woordenboekaanvallen. [1]

Q7: Kan openbare wifi malware verspreiden?

Ja, aanvallers kunnen verkeer onderscheppen en schadelijke downloadprompts (drive-by downloads) in je browsersessie injecteren.

Q8: Wat is het risico van bestanden delen?

Als bestandsdeling is ingeschakeld, kunnen andere gebruikers op het openbare netwerk je lokale mappenstructuur lezen of wijzigen.

Q9: Wat is een captive portal?

De inlogpagina die hotel- of cafénetwerken gebruiken om internettoegang te verlenen en die soms door aanvallers kan worden vervalst.

Q10: Moet ik wifi uitzetten als ik het niet gebruik?

Ja, door wifi uit te schakelen voorkom je dat je apparaat automatisch verbinding maakt met onbetrouwbare netwerken.

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

Verken geavanceerde technische aspecten van beveiligingsframeworks, malwareanalyse en gegevenscompliance.

Q1: Hoe maakt een man-in-the-middle-aanval misbruik van DNS?

Door DNS-spoofing op een malafide router te gebruiken om browsers van doelwitten naar lookalike-phishingpagina's te leiden in plaats van naar de echte domeinen.

Q2: Wat is sessiekaping?

Een aanvaller die een onversleutelde sessiecookie op openbare wifi onderschept en importeert om inlogcontroles te omzeilen.

Q3: Wat is SSL-stripping?

Een MitM-aanval waarbij een aanvaller het beveiligde HTTPS-verzoek van een gebruiker terugzet naar onversleuteld HTTP, en zo inloggegevens in leesbare tekst onderschept.

Q4: Hoe beschermt HSTS tegen SSL-stripping?

HTTP Strict Transport Security dwingt browsers om alleen via HTTPS te verbinden en weigert onversleutelde HTTP-terugvalopties. [3]

Q5: Wat is een VPN met split tunneling?

Een configuratie die alleen zakelijk verkeer via de VPN routeert en openbare internetgegevens rechtstreeks verstuurt, wat het risico op blootstelling via lekpaden kan vergroten.

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

Verken geavanceerde technische aspecten van beveiligingsframeworks, malwareanalyse en gegevenscompliance.

Q6: Waarom is WPA2 kwetsbaar voor KRACK?

De Key Reinstallation Attack maakt misbruik van de vierwegshandshake van WPA2 om pakketten te ontsleutelen zonder het wifi-wachtwoord.

Q7: Wat is clientisolatie?

Een routerbeveiligingsinstelling die voorkomt dat verbonden wifiapparaten rechtstreeks met elkaar communiceren, waardoor lokale sniffing wordt geblokkeerd.

Q8: Hoe gebruiken aanvallers nep-DNS-servers?

Ze configureren malafide routers die clients valse DNS-servers toewijzen, waarmee ze alle webopzoekingen kunnen onderscheppen en herschrijven.

Q9: Kan een VPN mijn lokale MAC-adres verbergen?

Nee. MAC-adressen zijn lokale identificatiecodes op laag 2; gebruik in plaats daarvan de ingebouwde MAC-randomisatie-instelling (privéadres) van je apparaat.

Q10: Wat is een aanval met spoofing van een captive portal?

Een aanvaller die een nep-authenticatieportaal host op een rogue-hotspot om inloggegevens te stelen onder het mom van gratis wifitoegang.

Deel 11: 10 cyberbeveiligingsfeiten en inzichten uit de praktijk

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

1. BEVEILIGINGSINZICHT

Thuiswerkers gebruiken vaak wifi in cafés, hotels en op luchthavens, waar ze de beveiliging van het netwerk niet kunnen controleren.

2. BEVEILIGINGSINZICHT

Een rogue-hotspot van het type Evil Twin kan de exacte naam en het MAC-adres van een vertrouwd netwerk kopiëren, waardoor apparaten in verwarring raken.

3. BEVEILIGINGSINZICHT

Software voor het afluisteren van pakketten, zoals Wireshark, is gratis en kan onversleutelde HTTP-wachtwoorden in leesbare tekst tonen.

4. BEVEILIGINGSINZICHT

WPA3-beveiliging gebruikt Simultaneous Authentication of Equals (SAE) om te beschermen tegen lokale brute-forceaanvallen.

5. BEVEILIGINGSINZICHT

SSL-strippingaanvallen omzeilen de basisbescherming van HTTPS door de eerste HTTP-redirects bij de gateway te onderscheppen.

6. BEVEILIGINGSINZICHT

Responsheaders van HTTP Strict Transport Security (HSTS) voorkomen dat browsers terugvallen op onversleutelde HTTP-verbindingen. [3]

7. BEVEILIGINGSINZICHT

Als je 'Auto-Connect' uitschakelt, voorkom je dat smartphones verbinding maken met malafide netwerken die op echte netwerken lijken op openbare plekken.

8. BEVEILIGINGSINZICHT

'Always-on'-VPN-configuraties voor bedrijven dwingen al het netwerkverkeer van medewerkers op afstand via bedrijfsfirewalls.

9. BEVEILIGINGSINZICHT

Frauduleuze toegangspunten kunnen vervalste DNS-antwoorden uitdelen, waardoor doeldomeinen worden omgeleid naar phishingservers.

10. BEVEILIGINGSINZICHT

Zonder VPN kunnen andere gebruikers op een open hotspot zien welke sites en servers je apparaat benadert.

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] Wi-Fi Alliance. (n.d.). Security.

https://www.wi-fi.org/discover-wi-fi/security

[2] Federal Trade Commission. (2023). Are Public Wi-Fi Networks Safe? What You Need To Know.

https://consumer.ftc.gov/articles/are-public-wi-fi-networks-safe-what-you-need-know

[3] MDN Web Docs. (n.d.). Strict-Transport-Security header.

https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/Strict-Transport-Security

[4] CISA. (2023). Phishing Guidance: Stopping the Attack Cycle at Phase One.

https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one

[5] CISA. (n.d.). Malware, Phishing, and Ransomware.

https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

Antwoordsleutel: Controlepunt 1 - Meerkeuze

1 Vraag 1

Juist antwoord: A

DOCENTENNOTITIE

Wat is een man-in-the-middle-aanval (MitM)? → Communicatie tussen twee partijen op een gedeeld netwerk onderscheppen en wijzigen

2 Vraag 2

Juist antwoord: A

DOCENTENNOTITIE

Wat is een nep-toegangspunt (rogue access point, Evil Twin)? → Een kwaadaardige wifihotspot die is ingesteld met dezelfde SSID als een legitiem netwerk

3 Vraag 3

Juist antwoord: A

DOCENTENNOTITIE

Hoe beschermt een VPN verkeer op openbare wifi? → Het verpakt alle netwerkpakketten in een versleutelde tunnel, zodat ze voor sniffers onleesbaar zijn

4 Vraag 4

Juist antwoord: A

DOCENTENNOTITIE

Wat is packet sniffing? → Hardware- of softwarehulpmiddelen gebruiken om netwerkpakketten vast te leggen en te loggen

5 Vraag 5

Juist antwoord: A

DOCENTENNOTITIE

Wat is de rol van HTTPS? → Sessieverkeer tussen de browser en de webserver versleutelen

Antwoordsleutel: Controlepunt 2 - Waar of onwaar

6 **Vraag 6** — **Juist antwoord: Waar**

DOCENTENNOTITIE

Verbonden gebruikers kunnen op open openbare wifinetwerken gemakkelijk platte-tekstgegevens onderscheppen.

7 **Vraag 7** — **Juist antwoord: Onwaar**

DOCENTENNOTITIE

Onwaar: een Evil Twin is een onbevoegd hotspot die een aanvaller opzet om een echte na te bootsen.

8 **Vraag 8** — **Juist antwoord: Onwaar**

DOCENTENNOTITIE

Onwaar: een VPN versleutelt verkeer in een tunnel, dus lokale sniffers kunnen het niet lezen.

9 **Vraag 9** — **Juist antwoord: Onwaar**

DOCENTENNOTITIE

Onwaar: HTTPS versleutelt de hele HTTP-uitwisseling, inclusief het URL-pad en de inhoud van de pagina.

10 **Vraag 10** — **Juist antwoord: Waar**

DOCENTENNOTITIE

Wifi-hotspots met WPA3-beveiliging bieden sterkere bescherming dan open netwerken zonder wachtwoord.

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

E 1. ONDERSCHEPPING	F 2. SNIFFING	D 3. EVIL TWIN	H 4. HTTPS
G 5. VPN	B 6. TUNNEL	A 7. WPA3	C 8. FIREWALL

CONTROLEPUNT 3: ANTWOORDEN KERNBEGRIPPEN

1 ONDERSCHEPPING	2 SNIFFING	3 EVIL TWIN	4 HTTPS
5 VPN-CLIENT	6 TUNNEL		

CONTROLEPUNT 6, ALTERNATIEF: ANTWOORDEN WOORDEN KOPPELEN

1 G – WPADRIE	2 C – EVILTWIN	3 B – SNIFFING	4 F – TUNNEL
5 H – FIREWALL	6 A – ONDERSCHEPPING	7 E – VPNCLIENT	8 D – HTTPS

DISCUSSIENOTITIES VOOR DOCENTEN

Kernbegrippen:
Controleer of leerlingen ONDERSCHEPPING, SNIFFING en EVIL TWIN 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.

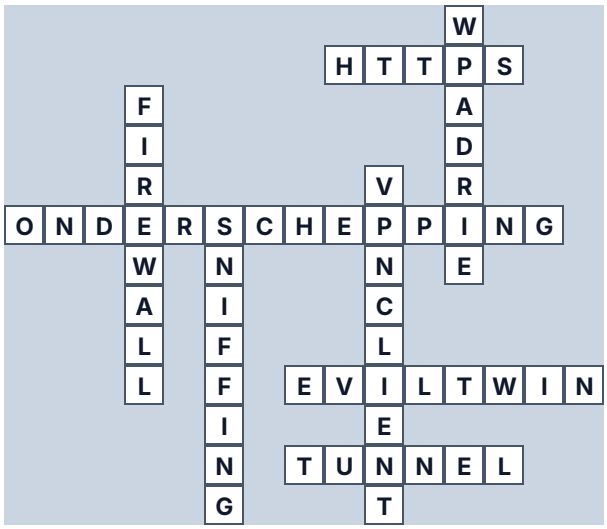
Bronnen beoordelen:
Laat leerlingen ten minste één bewering controleren aan de hand van de bronnen in het werkblad en bespreek waarom cijfers, prijzen en regels kunnen veranderen.

Puzzelsleutels en docentennotities

OPLOSSING WOORDZOEKER

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

OPLOSSING VAN DE KRUISWOORDPUZZEL



DOCENTENGIDS VOOR DE OPLOSSINGEN VAN DE KRUISWOORDPUZZEL

HORIZONTAAL

2 horizontaal: HTTPS Beveiligde webtransmissie. (5 letters)

5 horizontaal: ONDERSCHEPPING Het lezen van verkeer tijdens het transport. (14 letters)

7 horizontaal: EVILTWIN Nephotspot die een wifi-netwerk nabootst. (8 letters)

8 horizontaal: TUNNEL Beveiligd datapad tijdens het transport. (6 letters)

VERTICAAL

1 verticaal: WPADRIE Moderne wifi-beveiligingsstandaard (WPA3). (7 letters)

3 verticaal: FIREWALL Het filteren van inkomend verkeer. (8 letters)

4 verticaal: VPNCLIENT Versleuteld virtueel privénetwerk. (9 letters)

6 verticaal: SNIFFING Het vastleggen van netwerkdatapakketten. (8 letters)

Sleutel voor husselwoorden en coderaadsel

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

SLEUTEL WOORDEN ORDENEN

1. PSHPCDNEIONGRE — ONDERSCHEPPING
2. LENVIWTI — EVILTWIN
3. VILPETCNN — VPNCLIENT
4. EPRDIWA — WPADRIE
5. FINGFSNI — SNIFFING
6. PHTST — HTTPS
7. ETNLNU — TUNNEL
8. EIWLFLAR — FIREWALL

SLEUTEL VOOR DE GEHEIME CODE-OPDRACHT

"VERSLEUTEL VERKEER OP OPENBAAR WIFI MET EEN VPN"

Antwoordsleutel casestudy's

A Casestudy 1: Indammen van pakketsnuffelen op openbare wifi

Oplossing voor docenten

BEOORDELINGSRICHTLIJN

De antwoorden van leerlingen moeten de volgende punten behandelen:

- Scenarioanalyse: Een verkoopmedewerker op afstand die met een openbaar wifi-netwerk op een luchthaven is verbonden, merkt dat meerdere gevoelige zakelijke e-mails kort nadat ze in platte tekst zijn verzonden, zijn gelekt.
- Aanbevolen strategie en oplossing: Verplicht het gebruik van een zakelijke VPN-client op alle werkstations op afstand. Dwing browserextensies af die alleen HTTPS gebruiken en blokkeer onversleutelde protocollen (zoals HTTP en FTP) op de firewall van de client.

B Casestudy 2: Verdediging tegen een evil twin-rogue hotspot

Oplossing voor docenten

BEOORDELINGSRICHTLIJN

De antwoorden van leerlingen moeten de volgende punten behandelen:

- Scenarioanalyse: Aanvallers zetten een nep-draadloos toegangspunt met de naam 'CoffeeShop_Guest' op dat een legitieme hotspot van een café nabootst en netwerkverkeer onderschept van nietsvermoedende gasten.
- Aanbevolen strategie en oplossing: Controleer de BSSID-MAC-adressen van toegangspunten om de echtheid van het netwerk te verifiëren. Dwing validatie van de clientstatus (posture) af om verbinding met open netwerken te blokkeren en schrijf mobiele hotspots voor bij gevoelig werk.