Naam: _____ Datum: _____ Score: _____

Darkweb versus diep web: beveiliging en Verschillen

Indexering door zoekmachines, deepwebdatabases, Tor-onionrouting, netwerkanonimiteit en risico's

LEEROVERZICHT DARK WEB VERSUS DEEP WEB

BEVEILIGD
GEGEVENSVERSLEUTELING
256-bits AES-standaard

COMPLIANT
WERELDWIJDE NORMEN
AVG- en CCPA-kaders

ZERO-TRUST
TOEGANGSBELEID
Multifactorauthenticatie

Welkom! Dit activiteitenpakket leidt je door de verschillen tussen het deep web en het dark web. Je verkent niet-geïndexeerde databases, onion routing van de Tor-browser, cryptografische .onion-domeinen en veiligheidsrisico's voor anonimiteit.

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/dark-web-vs-deep-web/

Jouw leertraject: strategie voor het deep web en dark web

- Vergelijk het deep web (niet-geïndexeerde databases) met het dark web (onion-services).
- Begrijp hoe onion-routering netwerkverkeer versleutelt en doorgeeft.
- Beoordeel de beveiligingsrisico's van het bezoeken van niet-geverifieerde sites op het Tor-netwerk.
- Implementeer beveiligde gateway- en sandboxingbeleidsregels voor het crawlen van dreigingsinformatie.
- Analyseer het cryptografische adresformaat van domeinen van onion-services.

INSTRUCTIES GIDS DIEP EN DONKER WEB

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 privacy op het deep web en het dark web. Sluit af met de bonusopdracht Snel denken.

DATABASES VAN HET DIEPE WEB VERSUS ONION-ROUTING VAN HET DARKWEB (INLEIDING)

Het deepweb bestaat uit niet-geïndexeerde pagina's achter wachtwoorden en aanmeldingen, zoals privé-e-mail of bankportalen van bedrijven. Het darkweb is een deel van het deepweb dat opzettelijk verborgen is en waarvoor je gespecialiseerde browsers (zoals Tor) en onion-netwerken nodig hebt om anoniem toegang te krijgen.

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

Controlepunt 1: Meerkeuzeopdracht

1. Wat onderscheidt het deep web van het surface web?

- A. Deep-webpagina's worden niet geïndexeerd door openbare zoekmachines
- B. Verkeer op het deep web is illegaal en wordt gemonitord door de politie
- C. Voor sites op het deep web zijn gespecialiseerde browsers zoals Tor nodig
- D. Deep-webpagina's laden altijd sneller dan pagina's van het surface web

2. Hoe krijg je toegang tot het darkweb?

- A. Via gespecialiseerde browsers die onion-routeringsnetwerken gebruiken
- B. Door aangepaste DNS-instellingen te configureren op standaardrouters
- C. Via besloten zoekconsoles voor het surface web, alleen op uitnodiging
- D. Door een standaard browserextensie voor het blokkeren van advertenties te installeren

3. Welke structuur vormt het grootste deel van het deep web?

- A. Met wachtwoord beveiligde gebruikersdatabases en privéaccounts
- B. Illegale zwarte-marktforums waar illegale goederen worden verhandeld
- C. Onversleutelde peer-to-peer-bestandsdeelprotocollen
- D. Openbare cachedatabases van zoekmachines

4. Wat doet Onion Routing met netwerkverkeer?

- A. Het versleutelt pakketten en routeert ze via meerdere relays
- B. Het verhoogt de downloadsnelheid door knooppunten van de internetprovider te omzeilen
- C. Het koppelt serienummers van apparaathardware aan IP-records
- D. Het verwijdert cookies van de webbrowser na elke klik

5. Welk domeinachtervoegsel wordt uitsluitend op Tor-netwerken gebruikt?

- A. De cryptografische .onion-topleveldomeinextensie
- B. De klassieke standaardextensie .com voor commerciële sites
- C. De gedecentraliseerde Web3-blockchainextensie .eth
- D. De landcode-extensie .ai voor technologie

Controlepunt 2: Waar-of-onwaar-opdracht

6 Vraag (waar/onwaar) 6

6. Het deepweb en het darkweb verwijzen naar hetzelfde netwerksegment.

- ◯ Waar
- ◯ Onwaar

7 Vraag (waar/onwaar) 7

7. Bedrijfsintranetportalen maken deel uit van het deep web.

- ◯ Waar
- ◯ Onwaar

8 Vraag (waar/onwaar) 8

8. Onion-routering ontsleutelt gegevenspakketten volledig bij elk doorgangsknooppunt.

- ◯ Waar
- ◯ Onwaar

9 Vraag (waar/onwaar) 9

9. Toegang tot het dark web stelt apparaten bloot aan grote malwarerisico's.

- ◯ Waar
- ◯ Onwaar

10 Vraag (waar/onwaar) 10

10. Standaard webzoekmachines crawlen en indexeren onionsites.

- ◯ Waar
- ◯ Onwaar

Controlepunt 3: Kernbegrippen invullen

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

1. Particuliere bankportalen bevinden zich in het niet-geïndexeerde deel van het _____ .

2. Gespecialiseerde Tor-knooppunten hosten verborgen _____ -diensten.

3. Tor-websites gebruiken de cryptografische topleveldomeinextensie _____ .

4. Het versleutelde, meerlagige routeren van verkeer heet _____ .

5. Zoekmachines voor het openbare web doorzoeken pagina's die openbaar _____ zijn.

6. Onion-netwerken versleutelen client-IP's om de _____ van gebruikers te behouden.

WOORDENBANK

ANONIMITEIT | DARK WEB | DATABASE | DEEP WEB | ENTRYNODE | GEÏNDEXEERD | ONION | ROUTERING

Schrijf hier je antwoorden:

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

Controlepunt 4: Beveiligingsbegrippen koppelen

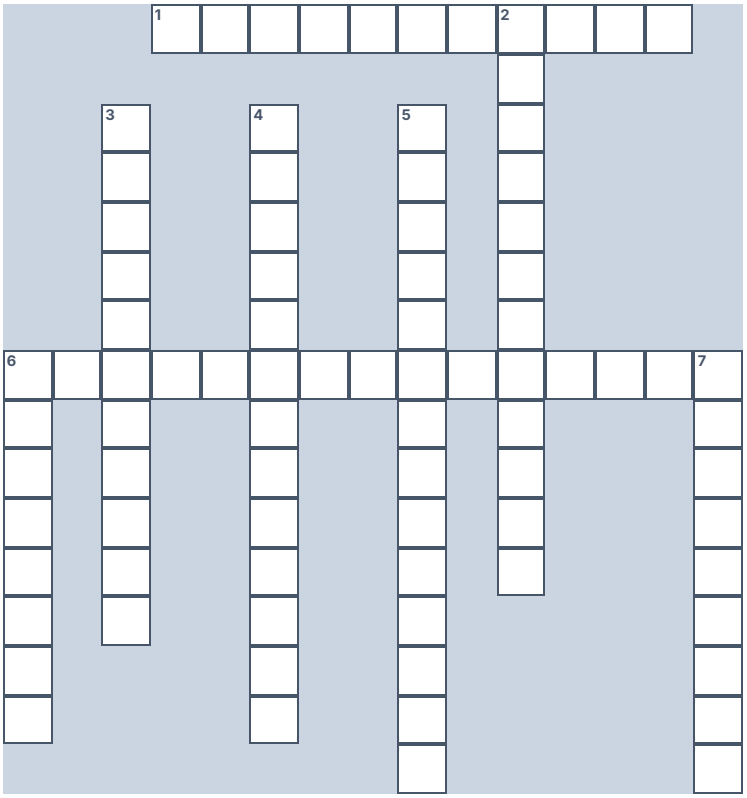
DEFINITIES KOPPELEN

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. Deel van het deep web	**A**	Versleuteld netwerksegment dat alleen toegankelijk is via speciale browsers.
☐	2. Dark web-portaal	**B**	Gegevens in lagen versleutelen en via drie nodes doorsturen.
☐	3. Onion-extensie	**C**	Beveiligde backendopslag voor niet-geïndexeerde systeemrecords.
☐	4. Tor-routering	**D**	Cryptografisch topleveldomeinachtervoegsel dat op Tor-netwerken wordt gebruikt.
☐	5. Geïndexeerde pagina's	**E**	De ingangsnode waarmee je toegang krijgt tot het Tor-netwerk.
☐	6. Anonimiteit van gebruikers	**F**	Content van het surface web die is verzameld en doorzoekbaar is op Google.
☐	7. Privédatabase	**G**	Het openbare IP-adres van de client verborgen houden voor servers.
☐	8. Toegangsgateway	**H**	Niet-geïndexeerde webinhoud zoals privéaanmeldingen, e-mail en databaserecords.

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. De openbare IP-adressen van clients verborgen houden voor servers (11)

6. Niet-geïndexeerde webcontent zoals privé-logins, e-mails en databasegegevens (15)

VERTICAAL

2. Gegevens in lagen versleutelen en via drie knooppunten doorsturen (12)

3. Content van het openbare web die door Google is verzameld en doorzoekbaar is (11)

4. Cryptografisch topleveldomeinachtervoegsel dat op Tor-netwerken wordt gebruikt (13)

5. Versleuteld netwerkgedeelte dat alleen via speciale browsers toegankelijk is (14)

6. Beveiligde back-endopslag die niet-geïndexeerde systeemgegevens host (8)

7. Het ingangsknooppunt waarmee toegang tot het Tor-netwerk wordt verkregen (9)

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: De openbare IP-adressen van clients verborgen houden voor servers (11 letters):

6 horizontaal: Niet-geïndexeerde webcontent zoals privé-logins, e-mails en databasegegevens (15 letters):

VERTICAAL

2 verticaal: Gegevens in lagen versleutelen en via drie knooppunten doorsturen (12 letters):

3 verticaal: Content van het openbare web die door Google is verzameld en doorzoekbaar is (11 letters):

4 verticaal: Cryptografisch topleveldomeinachtervoegsel dat op Tor-netwerken wordt gebruikt (13 letters):

5 verticaal: Versleuteld netwerkgedeelte dat alleen via speciale browsers toegankelijk is (14 letters):

6 verticaal: Beveiligde back-endopslag die niet-geïndexeerde systeemgegevens host (8 letters):

7 verticaal: Het ingangsknooppunt waarmee toegang tot het Tor-netwerk wordt verkregen (9 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.

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

WOORDENLIJST

DEEPWEBGEDEELTE DARKWEBPORTAAL ONIONEXTENSIE TORROUTERING
GEINDEXEERD ANONIMITEIT DATABASE ENTRYNODE

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. DEEPWEBGEDEELTE**
- **B. DARKWEBPORTAAL**
- **C. ONIONEXTENSIE**
- **D. TORROUTERING**
- **E. GEINDEXEERD**
- **F. ANONIMITEIT**
- **G. DATABASE**
- **H. ENTRYNODE**

DEFINITIES EN KOPPELVELDEN

1. De openbare IP-adressen van clients verborgen houden voor servers.
2. Beveiligde back-endopslag die niet-geïndexeerde systeemgegevens host.
3. Gegevens in lagen versleutelen en via drie knooppunten doorsturen.
4. Niet-geïndexeerde webcontent zoals privé-logins, e-mails en databasegegevens.
5. Versleuteld netwerkgedeelte dat alleen via speciale browsers toegankelijk is.
6. Cryptografisch topleveldomeinachtervoegsel dat op Tor-netwerken wordt gebruikt.
7. Het ingangsknooppunt waarmee toegang tot het Tor-netwerk wordt verkregen.
8. Content van het openbare web die door Google is verzameld en doorzoekbaar is.

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. EBDEEEGEELD TPEW
2. INNEIOSXEEN TO
3. GXEEIERDDEN
4. ASEABDAT
5. RRAAPOWLET BDAK
6. GORIUNETOT RR
7. TIANITEIOMN
8. EYDERNNOT

Bonusopdracht: Snel denken

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

1	Redenen om bij het dark web weg te blijven			
2	Dingen die een zoekmachine niet kan vinden			
3	Apparaten die gehackt kunnen worden			
4	Legale redenen om Tor te gebruiken			
5	Redenen om software bij te werken			
6	Waarschuwingssignalen in een e-mail			
7	Dingen die illegaal op het dark web worden verkocht			
8	Mensen die je om IT-hulp kunt vragen			
9	Veilige gewoonten die je vandaag kunt beginnen			
10	Dingen die je doet na een datalek			
11	Dingen die bij het deep web horen			
12	Sites die je met een login gebruikt			
13	Woorden die met anonimiteit te maken hebben			
14	Informatie die je nooit zou moeten delen			
15	Dingen die 'onder de oppervlakte' liggen			

Controlepunt 8: Casestudy's cyberbeveiliging

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

CASESTUDY 1: HERKENNEN VAN EEN DATALEK



Scenario: Een beveiligingsaudit van een bedrijf ontdekt dat gevoelige databaserecords van klanten worden verhandeld op een onion-marktplaats. De gegevens zijn niet geïndexeerd door Google.

Discussievraag: Leg uit welke delen van het web hierbij betrokken zijn en hoe dit lek is ontstaan.

CASESTUDY 2: ANONIMITEIT VERSUS MALWARERISICO'S



Scenario: Een analist wil dreigingsinformatiefeeds op een Tor-website controleren. Hij downloadt de Tor Browser en opent de site.

Discussievraag: Evalueer de voordelen voor anonimiteit en schets de stappen om malware te beperken.

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

2	12	9	10	6		1	14	15	14	9	5	13		13	5	20
22	5	9	12	9	7	5		15	14	9	15	14				
18	15	21	20	5	18	9	14	7								

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 het deep web?

Het deepweb bestaat uit alle webpagina's die zoekmachines niet kunnen indexeren, waaronder internetbankieren, e-maildatabases en tijdschriften achter een betaalmuur.

Q2: Wat is het dark web?

Het darkweb is een klein deel van het deepweb dat opzettelijk verborgen is en alleen toegankelijk is via gespecialiseerde browsers die onion-netwerken gebruiken.

Q3: Hoe indexeren zoekmachines pagina's?

Zoekmachines laten geautomatiseerde programma's (spiders) openbare links volgen en indexeren pagina's die crawlen niet blokkeren via robotrichtlijnen.

Q4: Waarom wordt online bankieren gerekend tot het deep web?

Bankportalen zitten achter inlogschermen en wachtwoorden, waardoor openbare zoekmachines pagina's met rekeningafschriften niet kunnen indexeren.

Q5: Wat is onion routing in de Tor-browser?

Onion-routering is een transmissiemethode die verkeer in lagen versleutelt en via meerdere relays doorstuurt om de IP-adressen van gebruikers te maskeren.

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

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

Q6: Is toegang tot het dark web illegaal?

Nee. Toegang tot het dark web is in de meeste landen legaal, hoewel deelname aan illegale marktplaatsen of cyberactiviteiten verboden is.

Q7: Waarom laden sites op het dark web langzaam?

Verkeer wordt via ten minste drie wereldwijde relays (ingang, midden, uitgang) gerouteerd en ontsleuteld, wat de transmissielatentie verhoogt.

Q8: Wat betekent een .onion-domeinachtervoegsel?

Het is een gespecialiseerd topleveldomeinachtervoegsel dat op Tor-netwerken wordt gebruikt en verwijst naar cryptografisch gegenereerde adressen in plaats van naar standaard DNS-servers.

Q9: Welke risico's zijn verbonden aan links naar het dark web?

Sites hebben geen beveiligingscontrole, waardoor gebruikers worden blootgesteld aan hoge besmettingspercentages met malware, phishingscripts en transactiefraude.

Q10: Wie heeft het routeringsprotocol van het Tor-netwerk gemaakt?

De technologie is in de jaren negentig oorspronkelijk ontwikkeld door het U.S. Naval Research Laboratory om overheidscommunicatie te beschermen.

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

Verken geavanceerde technische aspecten van beveiligingsframeworks, malwareanalyse en gegevenscompliance.

Q1: Hoe beschermen tussenliggende knooppunten de anonimiteit van Tor?

Elke node ontsleutelt slechts één laag routeringsgegevens en kent alleen de vorige en de volgende hop, nooit zowel bron als bestemming.

Q2: Wat is de rol van het exitknooppunt?

De uitgangsnode ontsleutelt de laatste versleutelingslaag en stuurt het verkeer door naar de openbare bestemmingsserver of onion-server.

Q3: Wat is een Tor-bridgesgateway?

Bridges zijn niet-vermelde Tor-ingangsrelays die worden gebruikt om blokkades en censuur door internetproviders te omzeilen in regio's die toegang via de Tor-browser beperken.

Q4: Hoe misbruiken actoren op het dark web cryptovaluta?

Actoren gebruiken anonieme cryptovaluta's om financiële transacties op darkwebmarktplaatsen uit te voeren, waarbij ze standaard bankcontroles ontlopen.

Q5: Waarom lukt het gewone zoekmachines niet om diepe databases te crawlen?

Crawlers kunnen geen inloggegevens invoeren, geen beveiligings-CAPTCHA's oplossen en geen SQL-queryscripts op de backend uitvoeren die nodig zijn voor toegang tot deep-webdatabases.

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

Verken geavanceerde technische aspecten van beveiligingsframeworks, malwareanalyse en gegevenscompliance.

Q6: Wat is een directoryserver in Tor-netwerken?

Het is een vertrouwde server die de lijst bijhoudt van actieve entry-, middle- en exitrelays die clients gebruiken om routeringspaden op te bouwen.

Q7: Hoe voeren kwaadwillenden exitnode-sniffing uit?

Frauduleuze exitnode-operators kunnen onversleuteld HTTP-verkeer onderscheppen terwijl het het Tor-netwerk verlaat, en zo gebruikersnamen en cookies stelen.

Q8: Wat is het verschil tussen Tor en I2P?

Tor gebruikt een gecentraliseerde relaygids en exitnodes voor openbare webtoegang, terwijl I2P een gedecentraliseerde peer-to-peerstructuur voor interne hosting gebruikt.

Q9: Hoe volgen wetshandhavingsinstanties markten op het dark web?

Instanties gebruiken blockchainanalyse, sporen fysieke serverhostingopstellingen op en voeren lokoperaties uit om beheerders te identificeren.

Q10: Hoe brengt een DNS-lek de anonimiteit van de client in gevaar?

DNS-lekken treden op wanneer DNS-verzoeken van de browser rechtstreeks via de lokale isp worden verstuurd in plaats van via het versleutelde Tor-netwerk.

Deel 11: 10 cyberbeveiligingsfeiten en inzichten uit de praktijk

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

1. BEVEILIGINGSINZICHT

Het deepweb is veel groter dan het doorzoekbare oppervlakteweb, omdat de meeste inhoud achter aanmeldingen en databases staat.

2. BEVEILIGINGSINZICHT

Het darkweb is een klein, opzettelijk verborgen deel van het deepweb, dat je bereikt met hulpmiddelen zoals Tor.

3. BEVEILIGINGSINZICHT

Tor-routering versleutelt datapakketten drie keer en pelt bij elke relaynode versleutelingslagen af, als bij een ui.

4. BEVEILIGINGSINZICHT

Tor is voortgekomen uit het onion-routingproject van het U.S. Naval Research Lab, en de code is uitgebracht als vrije software. [1]

5. BEVEILIGINGSINZICHT

Onion-adressen zijn alfanumerieke tekenreeksen van 56 tekens die cryptografisch worden gegenereerd uit publieke sleutelparen.

6. BEVEILIGINGSINZICHT

Exitnodes kunnen verkeer in leesbare tekst lezen, wat betekent dat TLS/HTTPS ook op Tor nodig blijft voor beveiligde sessiegegevens.

7. BEVEILIGINGSINZICHT

Intranetsites, clouddrives en privédatabases vormen de grootste segmenten van gegevensopslag op het deep web.

8. BEVEILIGINGSINZICHT

Gespecialiseerde zoekmachines zoals DuckDuckGo beheren onionportalen om anoniem zoeken op Tor-netwerken mogelijk te maken.

9. BEVEILIGINGSINZICHT

Meer dan 2 miljoen gebruikers maken dagelijks verbinding met het Tor-netwerk om censuur te omzeilen en privé te kunnen communiceren.

10. BEVEILIGINGSINZICHT

Wereldwijde opsporingsoperaties (zoals Operation Bayonet) schakelen grote darkwebmarkten uit door hostinghardware in beslag te nemen.

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] Tor Project. (n.d.). Why is it called Tor?
https://support.torproject.org/about/why-is-it-called-tor/

[2] Tor Project. (n.d.). How do Onion Services work?
https://community.torproject.org/onion-services/overview/

[3] Tor Project. (n.d.). Users – Tor Metrics.
https://metrics.torproject.org/userstats-relay-country.html

[4] CISA. (n.d.). Malware, Phishing, and Ransomware.
https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

[5] 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

Antwoordsleutel: Controlepunt 1 - Meerkeuze

1 **Zoekmachine-indexering** DIEP WEB — **Juist antwoord: A**

DOCENTENNOTITIE

Pagina's van het diepe web zitten achter inlogschermen en databases, waardoor zoekspiders ze niet kunnen crawlen. Bronvermelding: IETF RFC 3986.

2 **Toegang tot Tor** DARK WEB — **Juist antwoord: A**

DOCENTENNOTITIE

Het darkweb bestaat uit verborgen onion-diensten die alleen toegankelijk zijn via browsers zoals Tor. Bron: IETF RFC 3986.

3 **Diepe databases** DATABASES — **Juist antwoord: A**

DOCENTENNOTITIE

Met wachtwoord beveiligde accounts en bedrijfsgegevens vormen het grootste deel van het deep web. Bron: NIST Digital Identity.

4 **Onion-routering** TOR-NETWERK — **Juist antwoord: A**

DOCENTENNOTITIE

Onion-routering versleutelt gegevenspakketten in lagen en stuurt ze via meerdere knooppunten door voor anonimiteit. Bron: IETF RFC 3986.

5 **Onion-domein** ACHTERVOEGSEL — **Juist antwoord: A**

DOCENTENNOTITIE

Het cryptografische domeinachtervoegsel.onion routeert verkeer intern binnen Tor, zonder openbare DNS. Bron: IETF RFC 3986.

Antwoordsleutel: Controlepunt 2 - Waar of onwaar

6 **Websegmenten** STRUCTUUR — **Juist antwoord: Onwaar**

DOCENTENNOTITIE

Het deepweb omvat alle niet-geïndexeerde pagina's, terwijl het darkweb een klein, versleuteld onion-subsegment is. Bron: IETF RFC 3986.

7 **Bedrijfsintranetten** DIEP WEB — **Juist antwoord: Waar**

DOCENTENNOTITIE

Intranetsites zitten achter wachtwoordportalen en worden niet geïndexeerd, wat betekent dat ze tot het deep web behoren. Bron: NIST Digital Identity.

8 **Versleuteling in lagen** RELAYS — **Juist antwoord: Onwaar**

DOCENTENNOTITIE

Onion-relays ontsleutelen slechts één routeringslaag om de anonimiteit van de gebruiker te beschermen, nooit het hele pakket. Bron: IETF RFC 3986.

9 **Blootstelling aan malware** DREIGINGEN — **Juist antwoord: Waar**

DOCENTENNOTITIE

Marktplaatsen op het darkweb hebben geen beveiligingsfiltering en brengen extreem grote risico's op malware-infecties met zich mee. Bronvermelding: Center for Internet Security (CIS).

10 **Vraag 10** — **Juist antwoord: Onwaar**

DOCENTENNOTITIE

Gewone crawlers van zoekmachines gebruiken Tor niet, dus ze kunnen .onion-sites niet bereiken of indexeren.

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

H 1. Deel van het deep web	A 2. Dark web-portaal	D 3. Onion-extensie	B 4. Tor-routering
F 5. Geïndexeerde pagina's	G 6. Anonimiteit van gebruikers	C 7. Privédatabase	E 8. Toegangsgateway

CONTROLEPUNT 3: ANTWOORDEN KERNBEGRIPPEN

1 DEEP WEB	2 DARK WEB	3 ONION	4 ROUTERING
5 GEÏNDEXEERD	6 ANONIMITEIT		

CONTROLEPUNT 6, ALTERNATIEF: ANTWOORDEN WOORDEN KOPPELEN

1 F – ANONIMITEIT	2 G – DATABASE	3 D – TORROUTERING	4 A – DEEPWEBGEDEELTE
5 B – DARKWEBPORTAAL	6 C – ONIONEXTENSIE	7 H – ENTRYNODE	8 E – GEINDEXEERD

DISCUSSIENOTITIES VOOR DOCENTEN

Kernbegrippen:
Controleer of leerlingen Deel van het deep web, Dark web-portaal en Onion-extensie 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.

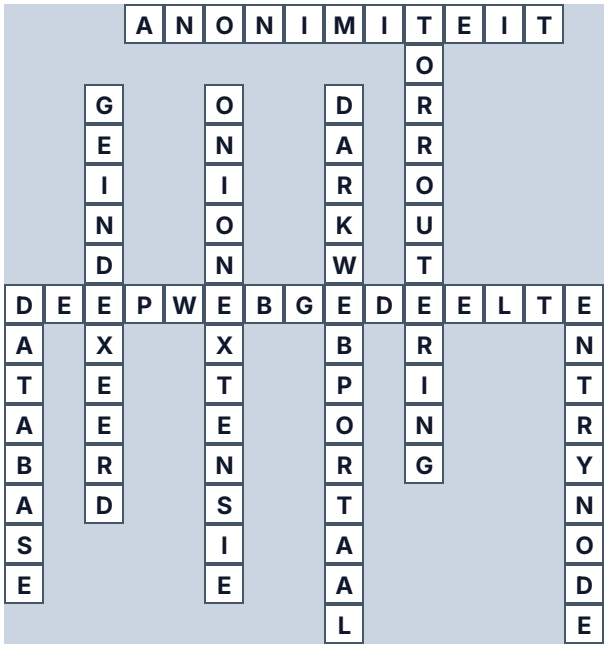
Bronnen beoordelen:
Laat leerlingen ten minste één bewering controleren aan de hand van de bronnen in het werkblad en bespreek waarom cijfers, prijzen en regels kunnen veranderen.

Puzzelsleutels en docentennotities

OPLOSSING WOORDZOEKER

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

OPLOSSING VAN DE KRUISWOORDPUZZEL



DOCENTENGIDS VOOR DE OPLOSSINGEN VAN DE KRUISWOORDPUZZEL

HORIZONTAAL

1 horizontaal: ANONIMITEIT De openbare IP-adressen van clients verborgen houden voor servers (11 letters)

6 horizontaal: DEEPWEBGEDEELTE Niet-geïndexeerde webcontent zoals privé-logins, e-mails en databasegegevens (15 letters)

VERTICAAL

2 verticaal: TORROUTERING Gegevens in lagen versleutelen en via drie knooppunten doorsturen (12 letters)

3 verticaal: GEINDEXEERD Content van het openbare web die door Google is verzameld en doorzoekbaar is (11 letters)

4 verticaal: ONIONEXTENSIE Cryptografisch topleveldomeinachtervoegsel dat op Tor-netwerken wordt gebruikt (13 letters)

5 verticaal: DARKWEBPORTAAL Versleuteld netwerkgedeelte dat alleen via speciale browsers toegankelijk is (14 letters)

6 verticaal: DATABASE Beveiligde back-endopslag die niet-geïndexeerde systeemgegevens host (8 letters)

7 verticaal: ENTRYNODE Het ingangsknooppunt waarmee toegang tot het Tor-netwerk wordt verkregen (9 letters)

Sleutel voor husselwoorden en coderaadsel

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

SLEUTEL WOORDEN ORDENEN

1. EBDEEEGEELDTPEW — DEEPWEBGEDEELTE
2. INNEIOSXEENTO — ONIONEXTENSIE
3. GXEEIERDDEN — GEINDEXEERD
4. ASEABDAT — DATABASE
5. RRAAPOWLETBDAK — DARKWEBPORTAAL
6. GORIUNETOTRR — TORROUTERING
7. TIANITEIOMN — ANONIMITEIT
8. EYDERNNOT — ENTRYNODE

SLEUTEL VOOR DE GEHEIME CODE-OPDRACHT

"BLIJF ANONIEM MET VEILIGE ONION ROUTERING"

Antwoordsleutel casestudy's

A Casestudy 1: Herkennen van een datalek

Oplossing voor docenten

BEOORDELINGSRICHTLIJN

De antwoorden van leerlingen moeten de volgende punten behandelen:

- Scenarioanalyse: Een beveiligingsaudit bij een bedrijf ontdekt dat gevoelige records uit de klantendatabase worden verhandeld op een onion-marktplaats. De gegevens zijn niet geïndexeerd door Google.
- Aanbevolen strategie en oplossing: Betrokken segmenten: De privédatabase behoort tot het deep web (niet geïndexeerd maar beveiligd). De marktplaats waar de gestolen gegevens worden verhandeld, bevindt zich op het dark web (onion-netwerk). Hoe het gebeurde: Hackers omzeilden de serverbeveiliging, stalen de database uit het deep web en boden deze anoniem aan op het dark web om aan opsporing door de politie te ontkomen.

B Casestudy 2: Anonimiteit versus malwarerisico's

Oplossing voor docenten

BEOORDELINGSRICHTLIJN

De antwoorden van leerlingen moeten de volgende punten behandelen:

- Scenarioanalyse: Een analist wil dreigingsinformatiefeeds controleren op een Tor-website. Hij downloadt de Tor-browser en opent de site.
- Aanbevolen strategie en oplossing: Voordelen: Tor routeert verkeer via drie nodes, waardoor het bedrijfs-IP van de analist wordt gemaskeerd. Risico's en beperking: Links naar het dark web hebben geen reputatiecontrole. Analisten moeten Tor binnen geïsoleerde virtuele machines (VM's) uitvoeren, JavaScript in de Tor-instellingen uitschakelen en geen bestanden downloaden om het bedrijfsnetwerk te beschermen.