Navn: _____ Dato: _____ Point: _____

Dark web og deep web: sikkerhed og forskelle

Søgemaskiners indeksering, databaser på det dybe net, Tor onion-routing, anonymitet på netværket og risici

OVERBLIK OVER DARK WEB OG DEEP WEB

SIKRET

DATAKRYPTERING

256-bit AES-standard

OVERHOLDER KRAV

GLOBALE STANDARDER

GDPR- og CCPA-rammer

ZERO-TRUST

ADGANGSPOLITIK

Multifaktorgodkendelse

Velkommen! Dette opgavehæfte guider dig gennem forskellene mellem deep web og dark web. Du vil udforske uindekserede databaser, onion routing i Tor Browser, kryptografiske .onion-domæner og risici ved anonymitet.

OPGAVEARKETS KONTROLPUNKTER

- [ ] **Del 1-4: Lær cybersikkerhed og trusselsforebyggelse.**
- [ ] **Del 5-7: Løs kryds og tværs samt ordjagt.**
- [ ] **Del 8-9: Løs casestudier og chifferudfordring.**
- [ ] **Del 10: Gennemgå grundlæggende og avanceret FAQ.**
- [ ] **Del 11: Udforsk 10 interessante fakta fra virkeligheden.**
- [ ] **Bonus: Tænk hurtigt-udfordring.**

Åbn VPN.com's guide til cybersikkerhed

URL: https://www.vpn.com/da/cybersikkerhed/dark-web-vs-deep-web/

Din læringsplan for deep web og dark web

- Sammenlign deep web (uindekserede databaser) med dark web (onion-tjenester).
- Forstå, hvordan onion routing krypterer og videresender trafik.
- Vurdér risikoen ved at besøge ukontrollerede sider på Tor-netværket.
- Indfør sikre gateways og sandkasser, når der indsamles trusselsdata.
- Analysér det kryptografiske adresseformat for onion-domæner.

VEJLEDNING TIL GUIDEN OM DEEP WEB OG DARK WEB

Besvar flervalgs- og sandt/falsk-spørgsmålene, udfyld sætningerne med ord fra ordbanken, match definitionerne, og løs kryds og tværs samt ordjagten. Anvend din viden om privatliv på deep web og dark web. Slut af med bonusaktiviteten Tænk hurtigt.

DATABASER PÅ DEEP WEB OG ONION ROUTING PÅ DARK WEB (INTRODUKTION)

Deep web består af uindekserede sider bag adgangskoder og logins, som private e-mails og netbanker. Dark web er en bevidst skjult del af deep web, som kræver særlige browsere (som Tor) og onion-netværk for at kunne tilgås anonymt.

LÆS HVERT KONTROLPUNKT GRUNDIGT, OG VÆLG ELLER SKRIV DET RIGTIGE SVAR.

Kontrolpunkt 1: Flervalgsopgave

1. Hvad adskiller deep web fra det almindelige net?

- A. Sider på deep web indekseres ikke af offentlige søgemaskiner
- B. Trafik på deep web er ulovlig og overvåges af politiet
- C. Sider på deep web kræver særlige browsere som Tor
- D. Sider på deep web indlæses altid hurtigere end sider på det åbne net

2. Hvordan tilgås dark web?

- A. Med særlige browsere, der bruger onion routing
- B. Med egne DNS-indstillinger på almindelige routere
- C. Via private søgeværktøjer kun for inviterede
- D. Ved at søge med en almindelig søgemaskine som Google

3. Hvad udgør den største del af deep web?

- A. Brugerdatabaser og private konti bag adgangskoder
- B. Ulovlige markedsfora, der handler med ulovlige varer
- C. Ukrypterede protokoller til fildeling
- D. Offentlige søgemaskiners cachedatabaser

4. Hvad gør onion routing ved trafikken?

- A. Den krypterer pakker og sender dem gennem flere relæer
- B. Den øger hastigheden ved at gå uden om udbyderen
- C. Den kobler enheders serienumre til IP-adresser
- D. Den sletter cookies efter hvert klik

5. Hvilken domæneendelse bruges kun på Tor?

- A. Det kryptografiske topdomæne .onion
- B. Det klassiske kommercielle .com
- C. Det decentrale Web3-domæne .eth
- D. Landekoden .ai

Kontrolpunkt 2: Sandt eller falsk-udfordring

6 Spørgsmål tf 6

6. Deep web og dark web er det samme.

○ Sandt ○ Falsk

7 Spørgsmål tf 7

7. Firmaers intranet er en del af deep web.

○ Sandt ○ Falsk

8 Spørgsmål tf 8

8. Onion routing dekrypterer pakkerne helt i hver node.

○ Sandt ○ Falsk

9 Spørgsmål tf 9

9. Besøg på dark web udsætter enheder for stor risiko for malware.

○ Sandt ○ Falsk

10 Spørgsmål tf 10

10. Almindelige søgemaskiner gennemsøger og indekserer onion-sider.

○ Sandt ○ Falsk

Kontrolpunkt 3: Indsæt nøglebegreber

Læs hver sætning nedenfor, og udfyld det tomme felt med det rigtige ord fra ordbanken.

1. Private netbanker ligger i den uindekserede del, kaldet _____ .
2. Særlige Tor-noder hoster skjulte tjenester på _____ .
3. Tor-websteder bruger det kryptografiske topdomæne _____ .
4. Krypteret trafik sendt gennem flere lag kaldes onion _____ .
5. Almindelige søgemaskiner gennemsøger sider, der er offentligt _____ .
6. Onion-netværk skjuler brugerens IP for at bevare _____ .

ORDBANK MED FAGUDTRYK

ANONYMITET | DARK WEB | DATABASE | DEEP WEB | INDEKSERET | INDGANG | ONION | ROUTING

Skriv dine svar her:

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

Kontrolpunkt 4: Match sikkerhedsbegreber

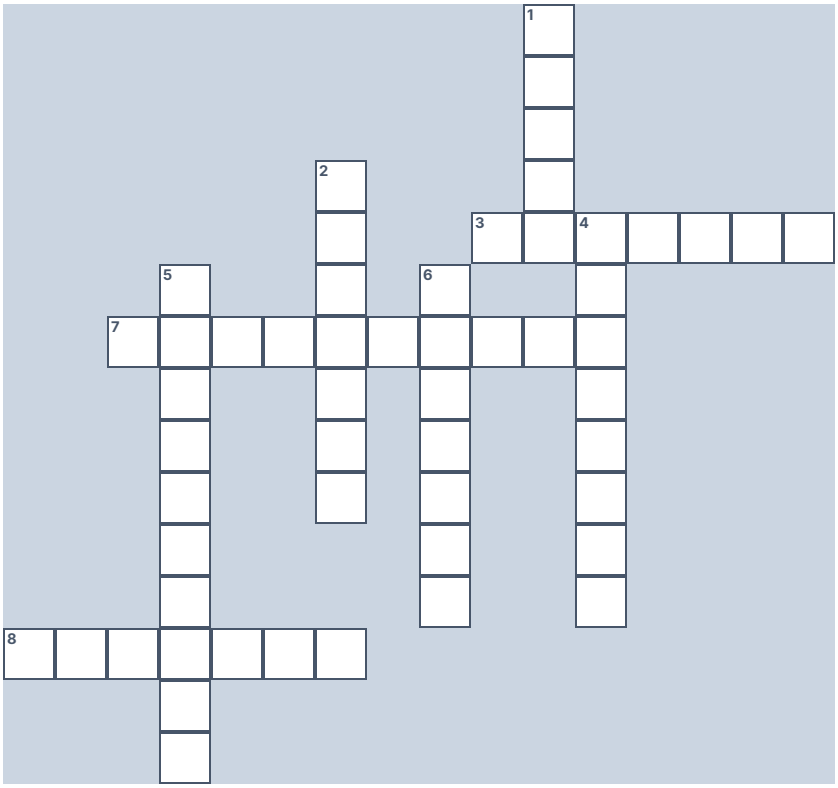
MATCH BEGREBER OG DEFINITIONER

Match hvert fagudtryk til venstre med den rigtige definition til højre ved at skrive det tilhørende bogstav (A-H) i indtastningsfeltet.

☐	1. Deep web-segment	A	Krypteret del af nettet, der kun kan tilgås med særlige browsere.
☐	2. Dark web-portal	B	Kryptering i lag og videresendelse gennem tre noder.
☐	3. Onion-endelse	C	Sikker lagring af uindekserede poster bag systemet.
☐	4. Tor-routing	D	Kryptografisk topdomæne, der bruges på Tor.
☐	5. Indekserede sider	E	Den node, man går ind på Tor-netværket igennem.
☐	6. Brugerens anonymitet	F	Indhold på det almindelige net, som kan findes på Google.
☐	7. Privat database	G	At holde brugerens offentlige IP-adresse skjult for servere.
☐	8. Indgangsnode	H	Uindekseret indhold som private logins, e-mails og databaseposter.

Kontrolpunkt 5: Kryds og tværs

Løs kryds og tværs ved at skrive bogstaver i de aktive hvide felter. Tallene svarer til nøglerne nedenfor.



VANDRETTE NØGLER

3. Den første node, trafikken passerer på vej ind i Tor-netværket (7)

7. Det, sider skal være, for at almindelige søgemaskiner kan finde dem (10)

8. Når trafikken sendes krypteret gennem flere lag, kaldes det onion … (7)

LODRETTE NØGLER

1. Det kryptografiske topdomæne, som Tor-websteder bruger (5)

2. Den bevidst skjulte del, der kun kan tilgås med særlige browsere (7)

4. Sikker lagring af poster, der ikke kan findes af søgemaskiner (8)

5. Det, onion-netværk bevarer ved at skjule brugerens IP-adresse (10)

6. Den uindekserede del af nettet, hvor netbanker og private konti ligger (7)

Kontrolpunkt 5, alternativ: Tilgængelige krydsordsnøgler

Brugere af skærmlæser og tastatur kan skrive krydsordssvarene direkte i tekstfelterne nedenfor.

VANDRETTE NØGLER

3 vandret: Den første node, trafikken passerer på vej ind i Tor-netværket (7 bogstaver):

7 vandret: Det, sider skal være, for at almindelige søgemaskiner kan finde dem (10 bogstaver):

8 vandret: Når trafikken sendes krypteret gennem flere lag, kaldes det onion … (7 bogstaver):

LODRETTE NØGLER

1 lodret: Det kryptografiske topdomæne, som Tor-websteder bruger (5 bogstaver):

2 lodret: Den bevidst skjulte del, der kun kan tilgås med særlige browsere (7 bogstaver):

4 lodret: Sikker lagring af poster, der ikke kan findes af søgemaskiner (8 bogstaver):

5 lodret: Det, onion-netværk bevarer ved at skjule brugerens IP-adresse (10 bogstaver):

6 lodret: Den uindekserede del af nettet, hvor netbanker og private konti ligger (7 bogstaver):

Kontrolpunkt 6: Skjult ordjagt

Find de 8 vigtige fagudtryk, der er skjult i gitteret nedenfor. Ordene kan stå vandret, lodret eller diagonalt.

L Z O Ø R Æ G R B R N D T J G

P T N N R Æ S O E Q I C W U V

T F O M K B A U W B N C Q Æ M

E L I Æ M Æ W T K L D E S O K

T E N J O I O I R L G S R D H

I O O O S N T N A U A W V A H

M C U S Q D I G D U N C Y T E

Y V Ø X C E Å Y E G G L I A Å

N D O E S K Z R E C W B A B Å

O P E M A S E Q P E F H J A D

N T S N F E J U W Å U G S S Y

A F A A S R Q O E R W Æ S E L

T W U D O E Ø B B G U Z Z K A

T Å Ø Ø M T H J O T L N N V Q

I S S H Å A Q X G X C Ø T Ø B

ORDLISTE MED FAGUDTRYK

DEEPWEB DARKWEB ONION ROUTING INDEKSERET ANONYMITET DATABASE INDGANG

Kontrolpunkt 6, alternativ: Tilgængelig ordmatchning

Match hvert af de 8 fagudtryk fra ordjagten med den rigtige definition ved at skrive bogstavet (A-H) i det tomme felt.

FAGUDTRYK
A. DEEPWEB
B. DARKWEB
C. ONION
D. ROUTING
E. INDEKSERET
F. ANONYMITET
G. DATABASE
H. INDGANG

DEFINITIONER OG MATCHFELTER

1. Det, onion-netværk bevarer ved at skjule brugerens IP-adresse.
2. Sikker lagring af poster, der ikke kan findes af søgemaskiner.
3. Når trafikken sendes krypteret gennem flere lag, kaldes det onion ....
4. Den uindekserede del af nettet, hvor netbanker og private konti ligger.
5. Den bevidst skjulte del, der kun kan tilgås med særlige browsere.
6. Det kryptografiske topdomæne, som Tor-websteder bruger.
7. Den første node, trafikken passerer på vej ind i Tor-netværket.
8. Det, sider skal være, for at almindelige søgemaskiner kan finde dem.

Kontrolpunkt 7: Bogstavrod-udfordring

Sæt bogstaverne nedenfor i den rigtige rækkefølge, og find vigtige cybersikkerhedsbegreber. Skriv dine svar i indtastningsfelterne.

1. **PEDWBEE** _____

2. **ONOIN** _____

3. **ISEENKTERD** _____

4. **ASEABDAT** _____

5. **WBKRDEA** _____

6. **NUIRTGO** _____

7. **NNAIMTETYO** _____

8. **NGGINAD** _____

Bonusaktivitet: Tænk hurtigt

3 SVAR I HVER KATEGORI. DEN FØRSTE, DER UDFYLDER HELE LISTEN, VINDER.

1	Grunde til at holde sig fra det mørke web			
2	Ting, en søgemaskine ikke kan finde			
3	Enheder, der kan blive hacket			
4	Lovlige grunde til at bruge Tor			
5	Grunde til at opdatere software			
6	Advarselstegn i en e-mail			
7	Ting, der sælges ulovligt på det mørke web			
8	Personer, du kan spørge om it-hjælp			
9	Sikkerhedsvaner, du kan starte i dag			
10	Ting at gøre efter et datalæk			
11	Ting, der hører til det dybe web			
12	Sider, du bruger med login			
13	Ord, der har med anonymitet at gøre			
14	Oplysninger, du aldrig bør dele			
15	Ting, der ligger 'under overfladen'			

Kontrolpunkt 8: Casestudier om cybersikkerhed

Anvend de begreber, du har lært, til at løse de virkelige scenarier nedenfor.

CASESTUDIE 1: OPSPORING AF DATALÆK



Scenarie: En sikkerhedsrevision opdager, at følsomme kundeposter fra en database handles på en onion-markedsplads. Dataene kan ikke findes på Google.

Diskussion: Forklar, hvilke dele af nettet der er involveret, og hvordan lækket opstod.

CASESTUDIE 2: ANONYMITET MOD RISIKO FOR MALWARE



Scenarie: En analytiker vil tjekke trusselsdata på et Tor-websted og henter Tor Browser for at besøge siden.

Diskussion: Vurdér fordelene ved anonymiteten, og beskriv, hvordan risikoen for malware begrænses.

Kontrolpunkt 9: Afkod chifferet

En cybersikkerhedsekspert beskytter netværkets aktiver mod trusselsaktører online. Brug bogstav-til-tal-nøglen nedenfor til at afkode beskeden ved at skrive de tilsvarende bogstaver i de tomme felter.

BOGSTAV-TIL-TAL-KRYPTERINGSNØGLE

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

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

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

20	15	18		19	11	10	21	12	5	18		4	9	14		9	16

1	4	18	5	19	19	5

Afkodet besked:

TIP: HVERT TAL ANGIVER BOGSTAVETS PLADS I ALFABETET (F.EKS. 1 = A, 2 = B, 26 = Z, 27 = Æ, 28 = Ø, 29 = Å).

Kontrolpunkt 10: Grundlæggende FAQ om cybersikkerhed (del A)

Gennemgå almindelige spørgsmål og svar om afværgelse af trusler online.

Q1: Hvad er deep web?

Alle sider, som søgemaskiner ikke kan indeksere, bl.a. netbanker, e-maildatabaser og tidsskrifter bag betalingsmur.

Q2: Hvad er dark web?

En lille, bevidst skjult del af deep web, som kun kan tilgås med særlige browsere via onion-netværk.

Q3: Hvordan indekserer søgemaskiner sider?

Automatiske programmer (spiders) følger offentlige links og indekserer sider, der ikke blokerer dem med robotregler.

Q4: Hvorfor hører netbank til deep web?

Netbanker ligger bag login og adgangskoder, så søgemaskiner ikke kan indeksere kontoudtog.

Q5: Hvad er onion routing i Tor Browser?

En metode, der krypterer trafikken i lag og sender den gennem flere relæer, så brugerens IP skjules.

Kontrolpunkt 10: Grundlæggende FAQ om cybersikkerhed (del B)

Gennemgå almindelige spørgsmål og svar om afværgelse af trusler online.

Q6: Er det ulovligt at besøge dark web?

Nej, det er lovligt i de fleste lande, men ulovlig handel og cyberkriminalitet er forbudt.

Q7: Hvorfor er sider på dark web langsomme?

Trafikken går gennem mindst tre relæer (indgang, midte, udgang), hvilket øger forsinkelsen.

Q8: Hvad betyder endelsen .onion?

Et særligt topdomæne på Tor, der peger på kryptografisk dannede adresser i stedet for almindelige DNS-servere.

Q9: Hvilke risici er der ved links på dark web?

Siderne kontrolleres ikke, så brugerne udsættes for malware, phishing og svindel ved handler.

Q10: Hvem udviklede Tor?

Teknikken blev udviklet af U.S. Naval Research Laboratory i 1990'erne for at beskytte statslig kommunikation.

Kontrolpunkt 10: Avanceret FAQ om sikkerhed (del C)

Udforsk avancerede tekniske aspekter af sikkerhedsrammer, malwareanalyse og overholdelse af databeskyttelsesregler.

Q1: Hvordan beskytter mellemnoderne anonymiteten i Tor?

Hver node dekrypterer kun ét lag og kender kun forrige og næste led, aldrig både afsender og modtager.

Q2: Hvad gør udgangsnoden?

Den fjerner det sidste lag kryptering og sender trafikken videre til målserveren eller onion-serveren.

Q3: Hvad er en Tor-bro?

Broer er hemmelige indgangsrelæer, der omgår blokering og censur i områder, hvor Tor er begrænset.

Q4: Hvordan udnytter aktører på dark web kryptovaluta?

De bruger anonyme kryptovalutaer til handler på skjulte markeder uden om bankernes kontrol.

Q5: Hvorfor kan søgemaskiner ikke gennemsøge dybe databaser?

De kan ikke logge ind, løse CAPTCHA eller køre de databaseforespørgsler, der kræves for at nå indholdet.

Kontrolpunkt 10: Avanceret FAQ om sikkerhed (del D)

Udforsk avancerede tekniske aspekter af sikkerhedsrammer, malwareanalyse og overholdelse af databeskyttelsesregler.

Q6: Hvad er en katalogserver i Tor?

En betroet server med listen over aktive relæer, som klienterne bruger til at danne ruter.

Q7: Hvordan aflytter ondsindede udgangsnoder trafik?

Ondsindede operatører kan opsnappe ukrypteret HTTP-trafik, når den forlader Tor, og stjæle brugernavne og cookies.

Q8: Hvad er forskellen på Tor og I2P?

Tor bruger et centralt katalog og udgangsnoder til det åbne net, mens I2P er et decentralt netværk til intern hosting.

Q9: Hvordan sporer politiet markeder på dark web?

Med analyse af blockchains, lokalisering af fysiske servere og lokkeoperationer, der afslører operatørerne.

Q10: Hvordan skader DNS-lækager anonymiteten?

Når browserens DNS-opslag går direkte til udbyderen i stedet for gennem det krypterede Tor-netværk.

Del 11: 10 fakta og indsigter om cybersikkerhed fra virkeligheden

Gennemgå fakta om sikkerhedsbrud, forsvarsmekanismer og krav til overholdelse.

1. SIKKERHEDSINDSIGT

Deep web er langt større end det søgbare surface web, da det meste indhold ligger bag logins og i databaser.

2. SIKKERHEDSINDSIGT

Dark web er en lille, bevidst skjult del af deep web, som man når med værktøjer som Tor.

3. SIKKERHEDSINDSIGT

Tor krypterer pakkerne tre gange og skræller et lag af i hvert relæ som på et løg.

4. SIKKERHEDSINDSIGT

Tor udsprang af det onion routing-projekt, som U.S. Naval Research Lab drev, og koden blev udgivet som fri software. [1]

5. SIKKERHEDSINDSIGT

Onion-adresser er strenge på 56 tegn, der dannes kryptografisk ud fra offentlige nøgler.

6. SIKKERHEDSINDSIGT

Udgangsnoder kan læse ukrypteret trafik, så TLS/HTTPS stadig er nødvendig på Tor.

7. SIKKERHEDSINDSIGT

Intranet, skydrev og private databaser er de største dele af deep web.

8. SIKKERHEDSINDSIGT

Søgemaskiner som DuckDuckGo har onion-adresser, så man kan søge anonymt via Tor.

9. SIKKERHEDSINDSIGT

Over 2 millioner bruger dagligt Tor til at omgå censur og beskytte deres kommunikation.

10. SIKKERHEDSINDSIGT

Internationale politiaktioner (som Operation Bayonet) har lukket store markeder ved at beslaglægge servere.

Tekniske referencer og kilder

Studieguiden og de interaktive opgaver er sammensat ud fra globale standarder fra NIST, OWASP og regler om databeskyttelse.

VIDENSKABELIGE OG BRANCHEMÆSSIGE REFERENCER

[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

Facitliste: Kontrolpunkt 1 – Flervalg

1 **Indeksering i søgemaskiner** DEEP WEB — Rigtigt svar: A

UNDERVISNINGSNOTE

Sider på deep web ligger bag login og i databaser, så søgemaskinernes spiders ikke kan nå dem.

2 **Adgang via Tor** DARK WEB — Rigtigt svar: A

UNDERVISNINGSNOTE

Dark web består af skjulte onion-tjenester, der kun kan tilgås med browsere som Tor.

3 **Dybe databaser** DATABASER — Rigtigt svar: A

UNDERVISNINGSNOTE

Konti bag adgangskoder og firmadata udgør den største del af deep web.

4 **Onion routing** TOR-NETVÆRKET — Rigtigt svar: A

UNDERVISNINGSNOTE

Onion routing krypterer pakker i lag og sender dem gennem flere noder for anonymitetens skyld.

5 **Onion-domæne** ENDELSE — Rigtigt svar: A

UNDERVISNINGSNOTE

Det kryptografiske.onion sender trafikken internt på Tor uden offentlig DNS.

Facitliste: Kontrolpunkt 2 – Sandt eller falsk

6 **Dele af nettet** OPBYGNING — Rigtigt svar: Falsk

UNDERVISNINGSNOTE

Deep web dækker alle uindekserede sider, mens dark web er en lille, krypteret onion-del.

7 **Firmaers intranet** DEEP WEB — Rigtigt svar: Sandt

UNDERVISNINGSNOTE

Intranet ligger bag adgangskoder og indekseres ikke, så det hører til deep web.

8 **Kryptering i lag** RELÆER — Rigtigt svar: Falsk

UNDERVISNINGSNOTE

Relæerne dekrypterer kun ét lag for at beskytte anonymiteten, aldrig hele pakken.

9 **Risiko for malware** TRUSLER — Rigtigt svar: Sandt

UNDERVISNINGSNOTE

Markeder på dark web har ingen sikkerhedsfiltre og giver meget stor risiko for malware.

10 **Spørgsmål 10** — Rigtigt svar: Falsk

UNDERVISNINGSNOTE

Almindelige søgemaskiners crawlere bruger ikke Tor, så de kan ikke nå eller indeksere .onion-websteder.

Ordfacit og bedømmelsesvejledning

Bedømmelsesvejledning til underviseren: Giv 1 point for hver korrekt matchning (8 point i alt) og hvert korrekt kontekstord (6 point i alt).

KONTROLPUNKT 4: FACIT TIL BEGREBSMATCHNING

H 1. Deep web-segment	A 2. Dark web-portal	D 3. Onion-endelse	B 4. Tor-routing
F 5. Indekserede sider	G 6. Brugerens anonymitet	C 7. Privat database	E 8. Indgangsnode

KONTROLPUNKT 3: FACIT TIL NØGLEBEGREBER

1 DEEP WEB	2 DARK WEB	3 ONION	4 ROUTING
5 INDEKSERET	6 ANONYMITET		

KONTROLPUNKT 6, ALTERNATIV: FACIT TIL ORDMATCHNING

1 F – ANONYMITET	2 G – DATABASE	3 D – ROUTING	4 A – DEEPWEB
5 B – DARKWEB	6 C – ONION	7 H – INDGANG	8 E – INDEKSERET

DISKUSSIONSNOTER TIL UNDERVISERE

Fagbegreber:
Kontrollér, at eleverne kan forklare Deep web-segment, Dark web-portal og Onion-endelse med egne ord og give et eksempel på hvert begreb.

Casestudier:
Bed eleverne begrunde deres anbefalinger med fakta fra opgavearket frem for antagelser.

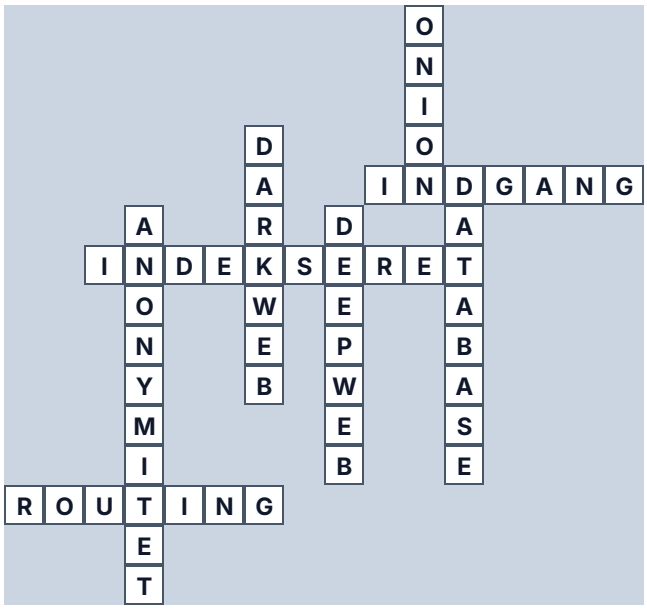
Kildekritik:
Lad eleverne efterprøve mindst én påstand mod referencerne i opgavearket, og drøft, hvorfor tal, priser og regler kan ændre sig over tid.

Facit til opgaver og undervisernoter

LØSNING PÅ ORDJAGT

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

LØSNING PÅ KRYDS OG TVÆRS



UNDERVISERVEJLEDNING TIL KRYDSORDSLØSNINGER

VANDRETTE NØGLER

3 vandret: INDGANG Den første node, trafikken passerer på vej ind i Tor-netværket (7 bogstaver)

7 vandret: INDEKSERET Det, sider skal være, for at almindelige søgemaskiner kan finde dem (10 bogstaver)

8 vandret: ROUTING Når trafikken sendes krypteret gennem flere lag, kaldes det onion ... (7 bogstaver)

LODRETTE NØGLER

1 lodret: ONION Det kryptografiske topdomæne, som Tor-websteder bruger (5 bogstaver)

2 lodret: DARKWEB Den bevidst skjulte del, der kun kan tilgås med særlige browsere (7 bogstaver)

4 lodret: DATABASE Sikker lagring af poster, der ikke kan findes af søgemaskiner (8 bogstaver)

5 lodret: ANONYMITET Det, onion-netværk bevarer ved at skjule brugerens IP-adresse (10 bogstaver)

6 lodret: DEEPWEB Den uindekserede del af nettet, hvor netbanker og private konti ligger (7 bogstaver)

Facit til bogstavrod og chiffer

Bedømmelsesfacit til bogstavrod-øvelsen og den hemmelige chifferudfordring.

FACIT TIL BOGSTAVROD

1. PEDWBEE — **DEEPWEB**
2. ONOIN — **ONION**
3. ISEENKTERD — **INDEKSERET**
4. ASEABDAT — **DATABASE**
5. WBKRDEA — **DARKWEB**
6. NUIRTGO — **ROUTING**
7. NNAIMTETYO — **ANONYMITET**
8. NGGINAD — **INDGANG**

FACIT TIL HEMMELIG CHIFFERUDFORDRING

"TOR SKJULER DIN IP ADRESSE"

Facit til casestudier

A Casestudie 1: Opsporing af datalæk

Underviserens løsning

BEDØMMELSESVEJLEDNING

Elevens svar bør dække følgende punkter:

- Analyse af scenariet: En revision opdager, at følsomme kundeposter handles på en onion-markedsplads. Dataene findes ikke på Google.
- Anbefalet strategi og løsning: Involverede dele: Den private database hører til deep web (uindekseret, men sikret). Markedet, der sælger dataene, ligger på dark web (onion-netværket). Forløb: Hackere brød forsvaret, stjal databasen fra deep web og satte den anonymt til salg på dark web for at undgå politiet.

B Casestudie 2: Anonymitet mod risiko for malware

Underviserens løsning

BEDØMMELSESVEJLEDNING

Elevens svar bør dække følgende punkter:

- Analyse af scenariet: En analytiker vil tjekke trusselsdata på et Tor-websted og henter Tor Browser.
- Anbefalet strategi og løsning: Fordele: Tor sender trafikken gennem tre noder og skjuler firmaets IP. Risici og tiltag: Links på dark web kontrolleres ikke. Kør Tor i en isoleret virtuel maskine, slå JavaScript fra, og hent ingen filer, så firmaets netværk beskyttes.