Namn: _____ Datum: _____ Poäng: _____

Darknet jämfört med djupa webben: säkerhet och Skillnader

Indexering i sökmotorer, deep web-databaser, Tor-lökroutning, nätverksanonymitet och risker

LÄRÖVERSIKT: DARK WEB MOT DEEP WEB

SÄKRAD
DATAKRYPTERING
256-bitars AES-standard

EFTERLEVANDE
GLOBALA STANDARDER
Ramverken GDPR och CCPA

ZERO TRUST
ÅTKOMSTPOLICY
Multifaktorautentisering

Välkommen! Det här aktivitetshäftet guidar dig genom skillnaderna mellan den djupa webben (Deep Web) och den mörka webben (Dark Web). Du utforskar oindexerade databaser, Tor-webbläsarens Onion Routing, kryptografiska .onion-domäner och säkerhetsrisker för anonymitet.

KONTROLLPUNKTER I ARBETSBLADET

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

Öppna VPN.com:s guide om cybersäkerhet

URL: https://www.vpn.com/sv/cybersakerhet/dark-web-vs-deep-web/

Din inlärningsplan för strategi för djup och mörk webb

- Jämför deep web (ej indexerade databaser) med dark web (onion-tjänster).
- Förstå hur onion routing krypterar och vidarebefordrar nätverkstrafik.
- Utvärdera säkerhetsriskerna med att besöka overifierade webbplatser i Tor-nätverket.
- Distribuera policyer för säkra gateways och sandlådor för genomsökning av hotinformation.
- Analysera det kryptografiska adressformatet för onion-tjänstdomäner.

INSTRUKTIONER FÖR GUIDEN OM DJUPA OCH MÖRKA WEBBEN

Besvara flervalsfrågorna och sant/falskt-frågorna, fyll i luckorna med hjälp av ordbanken, matcha definitioner och lös korsordet och ordletarpusslet. Tillämpa dina kunskaper om integritet på det djupa och mörka webben. Avsluta med bonusaktiviteten Tänk snabbt.

DATABASER PÅ DJUPA WEBBEN OCH ONION-ROUTING PÅ DARKNET (INTRODUKTION)

Den djupa webben består av oindexerade sidor bakom lösenord och inloggningar, som privat e-post eller företags bankportaler. Darkwebben är en delmängd av den djupa webben som är avsiktligt dold och kräver specialiserade webbläsare (som Tor) och onion-nätverk för att nås anonymt.

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

Kontrollpunkt 1: Utmaning med flerval

1. Vad skiljer det djupa nätet från ytnätet?

- A. Sidor på det djupa webben indexeras inte av offentliga sökmotorer
- B. Trafik på det djupa webben är olaglig och övervakas av rättsväsendet
- C. Webbplatser på det djupa webben kräver specialiserade webbläsare som Tor för åtkomst
- D. Deep web-sidor laddas alltid snabbare än sidor på ytwebben

2. Hur kommer man åt darkweb?

- A. Via specialiserade webbläsare som använder lökdirigeringsnätverk
- B. Genom att konfigurera egna DNS-inställningar på vanliga routrar
- C. Via privata sökkonsoler på ytwebben, endast för inbjudna
- D. Genom att installera ett vanligt webbläsartillägg för annonsblockering

3. Vilken struktur utgör den största delen av det djupa nätet?

- A. Lösenordsskyddade användardatabaser och privata konton
- B. Olagliga forum på svarta marknaden som handlar med olagliga varor
- C. Okrypterade peer-to-peer-protokoll för fildelning
- D. Cachedatabaser i offentliga sökmotorer

4. Vad gör Onion Routing med nätverkstrafik?

- A. Den krypterar paket och dirigerar dem via flera reläer
- B. Den ökar nedladdningshastigheten genom att förbigå internetleverantörens noder
- C. Den kopplar enheters serienummer till IP-poster
- D. Den raderar webbläsarens cookies efter varje klick

5. Vilken domänändelse används uteslutande i Tor-nätverk?

- A. Den kryptografiska toppdomänen .onion
- B. Den klassiska kommersiella .com-ändelsen
- C. Webb3-ändelsen .eth, decentraliserad på blockkedjan
- D. Landskodsändelsen .ai för teknik

Kontrollpunkt 2: Utmaning med sant eller falskt

6 Fråga sant/falskt 6

6. Den djupa webben och darkwebben avser samma nätverkssegment.

- ○ Sant
- ○ Falskt

7 Fråga sant/falskt 7

7. Företagsintranätportaler är en del av deep web.

- ○ Sant
- ○ Falskt

8 Fråga sant/falskt 8

8. Onion-routning dekrypterar datapaket helt vid varje transitnod.

- ○ Sant
- ○ Falskt

9 Fråga sant/falskt 9

9. Åtkomst till det mörka nätet (dark web) utsätter enheter för stor risk för skadlig kod.

- ○ Sant
- ○ Falskt

10 Fråga sant/falskt 10

10. Vanliga webbsökmotorer genomsöker och indexerar onion-webbplatser.

- ○ Sant
- ○ Falskt

Kontrollpunkt 3: Infoga nyckelbegrepp

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

1. Privata bankportaler finns i det oindexerade segmentet som kallas _____ .
2. Specialiserade Tor-noder är värdar för dolda tjänster på _____ .
3. Tor-webbplatser använder den kryptografiska toppdomänsändelsen _____ .
4. Krypterad trafik som tar en väg i flera lager kallas _____ .
5. Vanliga sökmotorer genomsöker sidor som är offentligt _____ .
6. Onion-nätverk krypterar klienternas IP-adresser för att bevara användarnas _____ .

ORDBANK

ANONYMITET | DATABAS | DJUPA WEBBEN | INDEXERADE | INGÅNGSNOD | MÖRKA WEBBEN | ONION | ONION-DIRIGERING

Skriv dina svar här:

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

Kontrollpunkt 4: Matchning av säkerhetsbegrepp

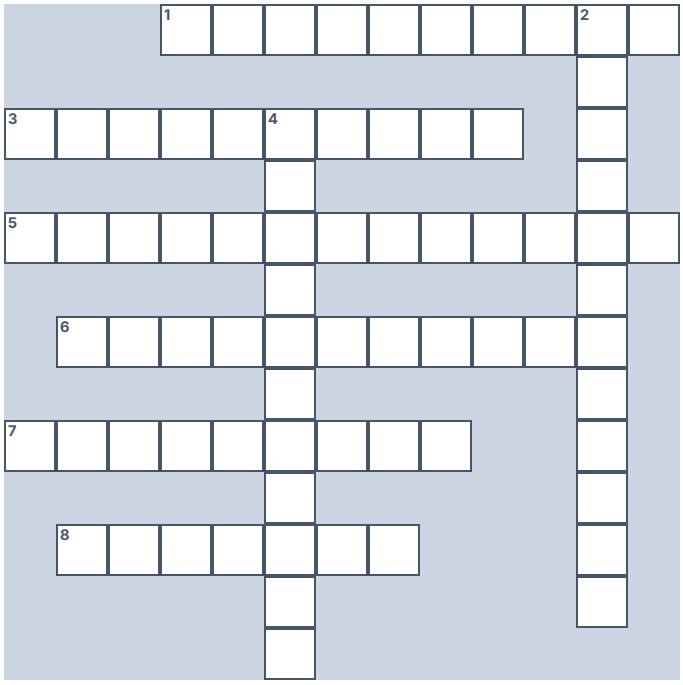
MATCHNING AV DEFINITIONER

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

☐	1. Segment av det djupa webben	A	Krypterat nätverkssegment som bara kan nås via särskilda webbläsare.
☐	2. Portal på det mörka nätet	B	Att kryptera data i lager och vidarebefordra den via tre noder.
☐	3. Onion-ändelse	C	Säker backend-lagring som innehåller oindexerade systemposter.
☐	4. Tor-dirigering	D	Kryptografisk toppdomänändelse som används i Tor-nätverk.
☐	5. Indexerade sidor	E	Ingångsnoden som används för att komma åt Tor-nätverket.
☐	6. Användaranonymitet	F	Innehåll på ytwebben som är sammanställt och sökbart på Google.
☐	7. Privat databas	G	Att hålla klienters publika IP-adresser dolda för servrar.
☐	8. Ingångsgateway	H	Oindexerat webbinnehåll som privata inloggningar, e-post och databasposter.

Kontrollpunkt 5: Korsord

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



VÅGRÄTT

1. Den nod som används som ingång till Tor-nätverket (10)

3. Att hålla klientens publika IP-adress dold för servrar (10)

5. Kryptering av data i lager och vidarebefordran via tre noder (13)

6. Oindexerat webbinnehåll som privata inloggningar, e-post och databasposter (11)

7. Webbinnehåll på ytan som är sammanställt och sökbart på Google (9)

8. Säker lagring i bakgrunden som innehåller oindexerade systemposter (7)

LODRÄTT

2. Kryptografisk toppdomänsändelse som används i Tor-nätverk (12)

4. Krypterat nätverkssegment som bara nås med särskilda webbläsare (11)

Kontrollpunkt 5, alternativ: Tillgängliga korsordsledtrådar

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

VÅGRÄTT

1 vågrätt: Den nod som används som ingång till Tor-nätverket (10 bokstäver):

3 vågrätt: Att hålla klientens publika IP-adress dold för servrar (10 bokstäver):

5 vågrätt: Kryptering av data i lager och vidarebefordran via tre noder (13 bokstäver):

6 vågrätt: Oindexerat webbinnehåll som privata inloggningar, e-post och databasposter (11 bokstäver):

7 vågrätt: Webbinnehåll på ytan som är sammanställt och sökbart på Google (9 bokstäver):

8 vågrätt: Säker lagring i bakgrunden som innehåller oindexerade systemposter (7 bokstäver):

LODRÄTT

2 lodrätt: Kryptografisk toppdomänsändelse som används i Tor-nätverk (12 bokstäver):

4 lodrätt: Krypterat nätverkssegment som bara nås med särskilda webbläsare (11 bokstäver):

Kontrollpunkt 6: Dolt ordsök

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

E Ö N L Y T W A U Z K N N H I

S N E B B E W A K R Ö M O I T

L G M V I N D E X E R A D M T

E Z I B W G Ä S P Ä Z U I V Å

D A R X P P A Ö Q J R V I R X

N W Q W W B L A F Q O M B P X

Ä G H R A S Z Ä K L X K Ä Y Å

N R L T D O N S G N Å G N I J

O Ö A J K O A F J B V A K F Y

I D T E T I M Y N O N A F L Ö

N T O R D I R I G E R I N G L

O E M S O K A G Q L P D O C D

I J D J U P A W E B B E N B B

Q T N R Y W J Ä G Ä U H Å Z I

F T W P W L T E V U N R M O U

ORDLISTA

DJUPAWEBBEN, MÖRKAWEBBEN, ONIONÄNDELSE, TORDIRIGERING, INDEXERAD, ANONYMITET, DATABAS, INGÅNGSNOD

Kontrollpunkt 6, alternativ: Tillgänglig matchning av ordförråd

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

ORDLISTA

- **A. DJUPAWEBBEN**
- **B. MÖRKAWEBBEN**
- **C. ONIONÄNDELSE**
- **D. TORDIRIGERING**
- **E. INDEXERAD**
- **F. ANONYMITET**
- **G. DATABAS**
- **H. INGÅNGSNOD**

DEFINITIONER OCH MATCHNINGSFÄLT

1. Att hålla klientens publika IP-adress dold för servrar.
2. Säker lagring i bakgrunden som innehåller oindexerade systemposter.
3. Kryptering av data i lager och vidarebefordran via tre noder.
4. Oindexerat webbinnehåll som privata inloggningar, e-post och databasposter.
5. Krypterat nätverkssegment som bara nås med särskilda webbläsare.
6. Kryptografisk toppdomänsändelse som används i Tor-nätverk.
7. Den nod som används som ingång till Tor-nätverket.
8. Webbinnehåll på ytan som är sammanställt och sökbart på Google.

Kontrollpunkt 7: Utmaning med blandade ord

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

1. AEEJWBDBUNP
2. ENNÄOLSIDENO
3. IEXNRDEAD
4. SABAADT
5. BÖBERNAWMEK
6. IRIRIRNETOGGD
7. NNAIMTETYO
8. OÅGDINNSNG

Bonusaktivitet: Tänk snabbt

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

1	Skäl till att hålla sig borta från darkweb			
2	Saker som en sökmotor inte kan hitta			
3	Enheter som kan hackas			
4	Lagliga skäl till att använda Tor			
5	Skäl till att uppdatera programvara			
6	Varningstecken i ett e-postmeddelande			
7	Saker som säljs olagligt på darkweb			
8	Personer du kan fråga om IT-hjälp			
9	Säkra vanor du kan börja med i dag			
10	Saker att göra efter en dataläcka			
11	Saker som hör till det djupa webben			
12	Webbplatser du använder med inloggning			
13	Ord som hör ihop med anonymitet			
14	Information du aldrig bör dela			
15	Saker som ligger "under ytan"			

Kontrollpunkt 8: Fallstudier om cybersäkerhet

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

FALLSTUDIE 1: IDENTIFIERA DATALÄCKA



Scenario: En säkerhetsgranskning i ett företag upptäcker att känsliga poster ur kunddatabasen handlas på en marknadsplats på onion-nätet. Uppgifterna är inte indexerade i Google.

Diskussionsfråga: Förklara vilka delar av webben som är inblandade och hur den här läckan uppstod.

FALLSTUDIE 2: ANONYMITET MOT RISKER MED SKADLIG KOD



Scenario: En analytiker vill kontrollera flöden med hotunderrättelser på en Tor-webbplats. Hen laddar ner Tor-webbläsaren och går in på webbplatsen.

Diskussionsfråga: Utvärdera fördelarna med anonymitet och redogör för stegen för att minska risken för skadlig kod.

Kontrollpunkt 9: Knäck chiffret

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

KRYPTERINGSNYCKEL FÖR BOKSTAV TILL SIFFRA

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

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

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

2	5	8	27	12	12		1	14	15	14	25	13	9	20	5	20	5	14
13	5	4		19	28	11	5	18		15	14	9	15	14				
4	9	18	9	7	5	18	9	14	7									

Avkodat meddelande:

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

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

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

Q1: Vad är det djupa webben (deep web)?

Den djupa webben består av alla webbsidor som sökmotorer inte kan indexera, inklusive nätbank, e-postdatabaser och tidskrifter bakom betalvägg.

Q2: Vad är darkweb?

Darkwebben är en liten delmängd av den djupa webben som avsiktligt är dold och bara nås via specialiserade webbläsare som använder onion-nätverk.

Q3: Hur indexerar sökmotorer sidor?

Sökmotorer kör automatiserade program (spindlar) som följer offentliga länkar och indexerar sidor som inte blockerar genomsökning via robotdirektiv.

Q4: Varför räknas nätbank som en del av det djupa webben (deep web)?

Bankportaler ligger bakom inloggningar och lösenord, vilket hindrar offentliga sökmotorer från att indexera sidor med kontoutdrag.

Q5: Vad är lökrouting i Tor-webbläsaren?

Onion-routning är en överföringsmetod som krypterar trafik i lager och skickar den genom flera reläer för att maskera användarnas IP-adresser.

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

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

Q6: Är det olagligt att besöka darkweb?

Nej. Att komma åt darkweb är lagligt i de flesta länder, även om det är förbjudet att delta i olagliga marknadsplatser eller cyberaktiviteter.

Q7: Varför laddas webbplatser på darkweb långsamt?

Trafiken dirigeras och dekrypteras via minst tre globala reläer (ingång, mellan, utgång), vilket ökar överföringsfördröjningen.

Q8: Vad betyder domänsuffixet .onion?

Det är ett specialiserat toppdomänsuffix som används i Tor-nätverk och pekar på kryptografiskt genererade adresser i stället för vanliga DNS-servrar.

Q9: Vilka risker är förknippade med länkar på darkweb?

Webbplatserna saknar säkerhetskontroll, vilket utsätter användare för hög risk för skadlig kod, nätfiskeskript och transaktionsbedrägerier.

Q10: Vem skapade routningsprotokollet i Tor-nätverket?

Tekniken utvecklades ursprungligen av U.S. Naval Research Laboratory på 1990-talet för att skydda statlig kommunikation.

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

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

Q1: Hur skyddar mellanliggande noder anonymiteten i Tor?

Varje nod dekrypterar bara ett lager av routningsdata och känner bara till föregående och nästa hopp, aldrig både källa och mål.

Q2: Vilken roll har utgångsnoden?

Utgångsnoden dekrypterar det sista krypteringslagret och skickar ut trafiken till den publika målservern eller onion-servern.

Q3: Vad är en Tor-bryggport (Tor bridges)?

Bryggor är olistade ingångsreläer för Tor som används för att kringgå blockeringar och censur hos internetleverantörer i regioner som begränsar åtkomst till Tor-webbläsaren.

Q4: Hur utnyttjar aktörer på darkweb kryptovaluta?

Aktörer använder anonyma kryptovalutor för att genomföra finansiella affärer på mörka marknadsplatser och undviker därmed vanliga kontroller av banktransaktioner.

Q5: Varför misslyckas vanliga sökmotorer med att genomsöka djupa databaser?

Sökrobotar kan inte ange inloggningsuppgifter, lösa CAPTCHA-säkerhetstest eller köra de SQL-frågeskript på serversidan som krävs för att nå deep web-databaser.

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

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

Q6: Vad är en katalogserver i Tor-nätverk?

Det är en betrodd server som för listan över aktiva ingångs-, mellan- och utgångsreläer som klienter använder för att bygga routningsvägar.

Q7: Hur utför illasinnade aktörer avlyssning vid utgångsnoder?

Oärliga operatörer av utgångsnoder kan avlyssna okrypterad HTTP-trafik när den lämnar Tor-nätverket och stjäla användarnamn och cookies.

Q8: Vad är skillnaden mellan Tor och I2P?

Tor använder en centraliserad relädatakatalog och utgångsnoder för åtkomst till den publika webben, medan I2P använder en decentraliserad peer-to-peer-struktur för intern värdhantering.

Q9: Hur spårar brottsbekämpande myndigheter marknadsplatser på darkweb?

Myndigheter använder blockkedjeanalys, lokaliserar fysiska serverinstallationer och genomför lockbetesoperationer för att identifiera operatörerna.

Q10: Hur äventyrar DNS-läckor klientens anonymitet?

DNS-läckor uppstår när webbläsarens DNS-frågor skickas direkt via den lokala ISP:n i stället för att dirigeras via det krypterade Tor-nätverket.

Del 11: 10 verkliga fakta och insikter om cybersäkerhet

Gå igenom verkliga fakta om säkerhetsintrång, försvarsmekanismer och efterlevnadsstandarder.

1. SÄKERHETSINSIKT

Den djupa webben är mycket större än den sökbara ytwebben, eftersom det mesta innehållet ligger bakom inloggningar och databaser.

2. SÄKERHETSINSIKT

Darkwebben är en liten, avsiktligt dold del av den djupa webben och nås med verktyg som Tor.

3. SÄKERHETSINSIKT

Tor-routning krypterar datapaket tre gånger och skalar bort krypteringslager som i en lök vid varje relänod.

4. SÄKERHETSINSIKT

Tor växte fram ur onion routing-projektet som drevs av U.S. Naval Research Lab, och dess kod släpptes som fri programvara. [1]

5. SÄKERHETSINSIKT

Onion-adresser är alfanumeriska strängar på 56 tecken som genereras kryptografiskt från offentliga nyckelpar.

6. SÄKERHETSINSIKT

Utgångsnoder kan läsa trafik i klartext, vilket innebär att TLS/HTTPS fortfarande krävs i Tor för säkra sessionsdata.

7. SÄKERHETSINSIKT

Intranätsplatser, molnenheter och privata databaser utgör de största datalagringssegmenten på den djupa webben.

8. SÄKERHETSINSIKT

Specialiserade sökmotorer som DuckDuckGo driver onion-portaler som möjliggör anonym sökning i Tor-nätverk.

9. SÄKERHETSINSIKT

Över 2 miljoner användare ansluter till Tor-nätverket varje dag för att kringgå censur och behålla integriteten i sin kommunikation.

10. SÄKERHETSINSIKT

Globala polisoperationer (som Operation Bayonet) stänger ned stora mörka marknadsplatser genom att beslagta hostinghårdvara.

Tekniska referenser och källor

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

VETENSKAPLIGA OCH BRANSCHRELATERADE REFERENSER

[1] 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

Facit: Kontrollpunkt 1 – Flerval

1 **Sökindexering** DJUPA WEBBEN **Rätt svar: A**

ANTECKNING FÖR LÄRAREN

Sidor på djupa webben ligger bakom inloggningar och databaser, vilket hindrar sökrobotar från att genomsöka dem. Källa: IETF RFC 3986.

2 **Tor-åtkomst** DARK WEB **Rätt svar: A**

ANTECKNING FÖR LÄRAREN

Darkwebben består av dolda onion-tjänster som bara nås via webbläsare som Tor. Källa: IETF RFC 3986.

3 **Djupa databaser** DATABASER **Rätt svar: A**

ANTECKNING FÖR LÄRAREN

Lösenordsskyddade konton och företagsregister utgör det största segmentet av det djupa webben (deep web). Källa: NIST Digital Identity.

4 **Onion-routning** TOR-NÄTVERK **Rätt svar: A**

ANTECKNING FÖR LÄRAREN

Onion-routning krypterar datapaket i lager och vidarebefordrar dem via flera noder för anonymitet. Källa: IETF RFC 3986.

5 **Onion-domän** ÄNDELSE **Rätt svar: A**

ANTECKNING FÖR LÄRAREN

Domänsuffixet.onion, som bygger på kryptografi, dirigerar trafik internt i Tor utan publik DNS. Källa: IETF RFC 3986.

Facit: Kontrollpunkt 2 – Sant eller falskt

6 **Webbsegment** STRUKTUR — **Rätt svar: Falskt**

ANTECKNING FÖR LÄRAREN

Den djupa webben omfattar alla oindexerade sidor, medan darkwebben är ett litet, krypterat onion-delsegment. Källa: IETF RFC 3986.

7 **Företagsintranät** DJUPA WEBBEN — **Rätt svar: Sant**

ANTECKNING FÖR LÄRAREN

Intranätsplatser ligger bakom lösenordsportaler och indexeras inte, vilket innebär att de tillhör den djupa webben. Källa: NIST Digital Identity.

8 **Krypteringslager** RELÄER — **Rätt svar: Falskt**

ANTECKNING FÖR LÄRAREN

Onion-reläer dekrypterar bara ett routningslager för att skydda användarens anonymitet, aldrig hela paketet. Källa: IETF RFC 3986.

9 **Exponering för skadlig kod** HOT — **Rätt svar: Sant**

ANTECKNING FÖR LÄRAREN

Marknadsplatser på darknet saknar säkerhetsfiltrering och medför extrema risker för infektion med skadlig kod. Källa: Center for Internet Security (CIS).

10 **Fråga 10** — **Rätt svar: Falskt**

ANTECKNING FÖR LÄRAREN

Vanliga sökmotorers sökrobotar använder inte Tor, så de kan inte nå eller indexera .onion-webbplatser.

Facit för ordförråd och bedömningsmall

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

KONTROLLPUNKT 4: FACIT – MATCHNING AV BEGREPP

H 1. Segment av det djupa webben	A 2. Portal på det mörka nätet	D 3. Onion-ändelse	B 4. Tor-dirigering
F 5. Indexerade sidor	G 6. Användaranonymitet	C 7. Privat databas	E 8. Ingångsgateway

KONTROLLPUNKT 3: FACIT – NYCKELBEGREPP

1 DJUPA WEBBEN	2 MÖRKA WEBBEN	3 ONION	4 ONION-DIRIGERING
5 INDEXERADE	6 ANONYMITET		

KONTROLLPUNKT 6, ALTERNATIV: FACIT – MATCHNING AV ORD

1 F – ANONYMITET	2 G – DATABAS	3 D – TORDIRIGERING	4 A – DJUPAWEBBEN
5 B – MÖRKAWEBBEN	6 C – ONIONÄNDELSE	7 H – INGÅNGSNOD	8 E – INDEXERAD

DISKUSSIONSANTECKNINGAR FÖR LÄRAREN

Nyckelbegrepp:
Kontrollera att eleverna kan förklara Segment av det djupa webben, Portal på det mörka nätet och Onion-ändelse med egna ord och ge ett exempel på varje.

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

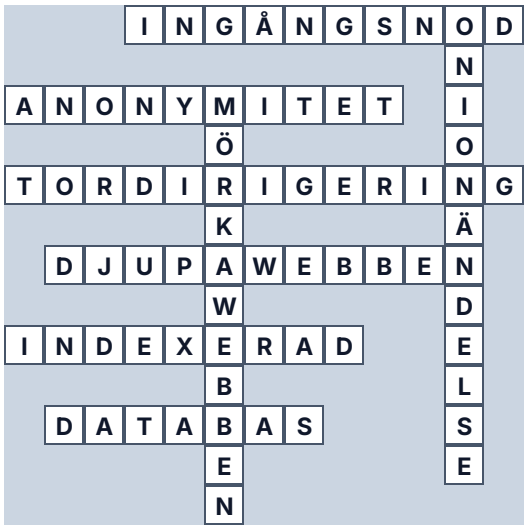
Källkritik:
Be eleverna att kontrollera minst ett påstående i arbetsbladets källor och diskutera varför siffror, priser och regler kan ändras över tid.

Facit till pussel och anteckningar för läraren

LÖSNING PÅ ORDSÖKET

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

LÖSNING PÅ KORSORDET



LÄRARHANDLEDNING MED LÖSNINGAR TILL KORSORDET

VÅGRÄTT

1 vågrätt: INGÅNGSNOD Den nod som används som ingång till Tor-nätverket (10 bokstäver)

3 vågrätt: ANONYMITET Att hålla klientens publika IP-adress dold för servrar (10 bokstäver)

5 vågrätt: TORDIRIGERING Kryptering av data i lager och vidarebefordran via tre noder (13 bokstäver)

6 vågrätt: DJUPAWEBBEN Oindexerat webbinnehåll som privata inloggningar, e-post och databasposter (11 bokstäver)

7 vågrätt: INDEXERAD Webbinnehåll på ytan som är sammanställt och sökbart på Google (9 bokstäver)

8 vågrätt: DATABAS Säker lagring i bakgrunden som innehåller oindexerade systemposter (7 bokstäver)

LODRÄTT

2 lodrätt: ONIONÄNDELSE Kryptografisk toppdomänsändelse som används i Tor-nätverk (12 bokstäver)

4 lodrätt: MÖRKAWEBBEN Krypterat nätverkssegment som bara nås med särskilda webbläsare (11 bokstäver)

Facit för blandade ord och chiffer

Facit för övningen med ordvärlden och utmaningen Hemliga chiffret.

FACIT FÖR ORDBLANDNING

1. AEEJWBDBUNP — DJUPAWEBBEN
2. ENNÄOLSIDENO — ONIONÄNDELSE
3. IEXNRDEAD — INDEXERAD
4. SABAADT — DATABAS
5. BÖBERNAWMEK — MÖRKAWEBBEN
6. IRIRIRNETOGGD — TORDIRIGERING
7. NNAIMTETYO — ANONYMITET
8. OÅGDINNSNG — INGÅNGSNOD

NYCKEL TILL UTMANINGEN MED HEMLIGT CHIFFER

"BEHÅLL ANONYMITETEN MED SÄKER ONION DIRIGERING"

Facit till fallstudierna

A Fallstudie 1: Identifiera dataläcka

Lärarens lösning

BEDÖMNINGSRIKTLINJE

Elevernas svar bör täcka följande punkter:

- Scenarioanalys: En säkerhetsgranskning i ett företag upptäcker att känsliga klientdatabasposter säljs på en marknadsplats i onion-nätverket. Uppgifterna är inte indexerade av Google.
- Rekommenderad strategi och lösning: Berörda segment: Den privata databasen tillhör den djupa webben (inte indexerad men säker). Marknadsplatsen där de stulna uppgifterna säljs finns på den mörka webben (onion-nätverket). Hur det gick till: Hackare kringgick serverns skydd, stal databasen från den djupa webben och annonserade ut den anonymt på den mörka webben för att undgå brottsbekämpningens spårning.

B Fallstudie 2: Anonymitet mot risker med skadlig kod

Lärarens lösning

BEDÖMNINGSRIKTLINJE

Elevernas svar bör täcka följande punkter:

- Scenarioanalys: En analytiker vill kontrollera flöden med hotunderrättelser på en Tor-webbplats. Hen laddar ned Tor-webbläsaren och öppnar webbplatsen.
- Rekommenderad strategi och lösning: Fördelar: Tor dirigerar trafiken genom tre noder och maskerar analytikerns företags-IP-adress. Risker och åtgärder: Länkar på darkweb har ingen granskning av rykte. Analytiker måste köra Tor i isolerade virtuella maskiner (VM), inaktivera JavaScript i Tor-inställningarna och undvika att ladda ned filer för att skydda företagsnätverket.