Navn: _____ Dato: _____ Point: _____

Analyse af malware og afværgning af trusler

Trojanere, ransomware, spyware, rootkits, virtuelle sandkasser, isolering

OVERBLIK OVER ANALYSE AF MALWARE

SIKRET

DATAKRYPTERING

256-bit AES-standard

OVERHOLDER KRAV

GLOBALE STANDARDER

GDPR- og CCPA-rammer

ZERO-TRUST

ADGANGSPOLITIK

Multifaktorgodkendelse

Velkommen! Denne opgavepakke fører dig gennem analyse og forebyggelse af malware. Du vil udforske spyware, trojanere, ransomware, værktøjer til reverse engineering, rootkits og strategier for isolering.

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/malware/

Din læringsplan for afværgning af malware

- Skeln mellem trojanere, orme og rootkits.
- Brug virtuelle sandkasser til analyse af kode.
- Design planer for isolering og oprydning ved aktiv ransomware.

VEJLEDNING TIL GUIDEN OM ANALYSE AF MALWARE

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 afværgning af malware. Slut af med bonusaktiviteten Tænk hurtigt.

ANALYSE AF MALWARE OG ISOLERING AF TRUSLER (INTRODUKTION)

Skadelig kode som trojanere, orme og ransomware er alvorlige trusler mod endepunkter og servere. Sikkerhedsteams analyserer malware i virtuelle sandkasser og isolerer hurtigt netværket for at stoppe spredningen.

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

Kontrolpunkt 1: Flervalgsopgave

1. Hvad kendetegner en trojansk hest?

- A. Den udgiver sig for at være lovligt software, så brugeren kører den
- B. Den kopierer sig selv automatisk på det lokale netværk
- C. Den smitter filer i isolerede sandkasser
- D. Den opsnapper udbyderens trafik

2. Hvilken type malware krypterer filer og kræver betaling?

- A. Ransomware
- B. Spyware
- C. Rootkit
- D. Adware

3. Hvad er spyware?

- A. Malware, der i al hemmelighed overvåger tastetryk og surfing
- B. Kode, der kører i en virtuel sandkasse
- C. Opdateringer til antimalware fra databaser
- D. Automatisk justering af skærmens lysstyrke

4. Hvorfor bruger malwareudviklere rootkits?

- A. For at skjule aktive processer og skadelige filer for styresystemet
- B. For at gøre processoren hurtigere
- C. For at tage backup af databaser i skyen
- D. For at forlænge batteritiden på bærbare computere

5. Hvad betyder sandboxing i analyse af malware?

- A. At køre mistænkelige filer i et isoleret virtuelt rum for sikkert at iagttage dem
- B. At sammenligne filhashes med kendte trusler
- C. At gendanne backups efter et indbrud
- D. At koble routere fra offentlige linjer

Kontrolpunkt 2: Sandt eller falsk-udfordring

6 Spørgsmål 6

6. Orme kræver, at en bruger gør noget, før de kan sprede sig på netværket.

- ◯ Sandt
- ◯ Falsk

7 Spørgsmål 7

7. Adware er altid harmløs og sporer hverken adfærd eller browserhistorik.

- ◯ Sandt
- ◯ Falsk

8 Spørgsmål 8

8. Gendannelse fra rene offline-backups lader ofrene genskabe krypterede filer uden at betale løsesummen.

- ◯ Sandt
- ◯ Falsk

9 Spørgsmål 9

9. Signaturbaseret antivirus stopper pålideligt zero-day-malware, før der findes en signatur for den.

- ◯ Sandt
- ◯ Falsk

10 Spørgsmål 10

10. Filløs malware kører skadelige scripts i hukommelsen uden at skrive filer til disken.

- ◯ Sandt
- ◯ Falsk

Kontrolpunkt 3: Indsæt nøglebegreber

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

1. Malware forklædt som et ufarligt hjælpeprogram er en _____ .
2. Skadelig kode, der låser databaser for at få penge, er _____ .
3. Keyloggere, der i al hemmelighed optager adgangskoder, er _____ .
4. At gemme sig dybt i styresystemets kerne kræver et _____ .
5. Analyse af mistænkelige filer i et isoleret rum bruger en virtuel _____ .
6. Spredning af aktiv malware stoppes ved øjeblikkelig _____ .

ORDBANK MED FAGUDTRYK

FILLØS ISOLERING ORM RANSOMWARE ROOTKIT SANDKASSE SPYWARE TROJANER

Skriv dine svar her:

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

Kontrolpunkt 4: Match sikkerhedsbegreber

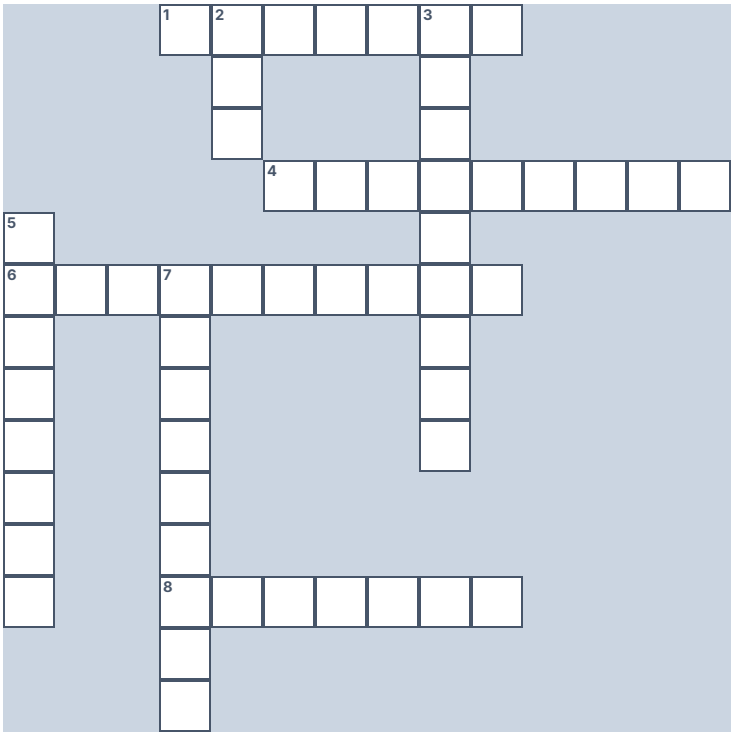
MATCH BEGREBER OG DEFINITIONER

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

☐	1. TROJANER	A	Program, der i al hemmelighed overvåger og optager brugerens aktivitet.
☐	2. RANSOMWARE	B	Malware, der kører direkte i RAM for at undgå diskscannere.
☐	3. SPYWARE	C	Afspærring af smittede enheder, så truslen ikke spreder sig.
☐	4. ROOTKIT	D	Skadeligt software forklædt som et ufarligt eller nyttigt program.
☐	5. SANDKASSE	E	Selvkopierende malware, der spreder sig på netværket uden menneskelig hjælp.
☐	6. ISOLERING	F	Malware, der krypterer lageret og kræver betaling for nøglen.
☐	7. ORM	G	Isoleret virtuelt miljø til sikker analyse af skadelige filer.
☐	8. FILLØS	H	Skjult malware dybt i kernen, der bevarer administratorkontrol.

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

1. Skjult malware, der gemmer sig dybt i styresystemets kerne (7)

4. Program, der registrerer alt, hvad brugeren taster (9)

6. Skadelig kode, der låser data og kræver betaling for nøglen (10)

8. Software, der i al hemmelighed optager tastetryk og adgangskoder (7)

LODRETTE NØGLER

2. Selvkopierende malware, der spreder sig uden menneskelig hjælp (3)

3. Det, der straks skal til for at stoppe spredningen af aktiv malware (9)

5. Malware forklædt som et ufarligt hjælpeprogram (8)

7. Isoleret virtuelt rum, hvor mistænkelige filer kan analyseres sikkert (9)

Kontrolpunkt 5, alternativ: Tilgængelige krydsordsnøgler

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

VANDRETTE NØGLER

1 vandret: Skjult malware, der gemmer sig dybt i styresystemets kerne (7 bogstaver):

4 vandret: Program, der registrerer alt, hvad brugeren taster (9 bogstaver):

6 vandret: Skadelig kode, der låser data og kræver betaling for nøglen (10 bogstaver):

8 vandret: Software, der i al hemmelighed optager tastetryk og adgangskoder (7 bogstaver):

LODRETTE NØGLER

2 lodret: Selvkopierende malware, der spreder sig uden menneskelig hjælp (3 bogstaver):

3 lodret: Det, der straks skal til for at stoppe spredningen af aktiv malware (9 bogstaver):

5 lodret: Malware forklædt som et ufarligt hjælpeprogram (8 bogstaver):

7 lodret: Isoleret virtuelt rum, hvor mistænkelige filer kan analyseres sikkert (9 bogstaver):

Kontrolpunkt 6: Skjult ordjagt

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

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

ORDLISTE MED FAGUDTRYK

TROJANER RANSOMWARE SPYWARE ROOTKIT SANDKASSE ISOLERING ORM KEYLOGGER

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. TROJANER
B. RANSOMWARE
C. SPYWARE
D. ROOTKIT
E. SANDKASSE
F. ISOLERING
G. ORM
H. KEYLOGGER

DEFINITIONER OG MATCHFELTER	
	1. Skjult malware, der gemmer sig dybt i styresystemets kerne.
	2. Det, der straks skal til for at stoppe spredningen af aktiv malware.
	3. Program, der registrerer alt, hvad brugeren taster.
	4. Selvkopierende malware, der spreder sig uden menneskelig hjælp.
	5. Skadelig kode, der låser data og kræver betaling for nøglen.
	6. Software, der i al hemmelighed optager tastetryk og adgangskoder.
	7. Malware forklædt som et ufarligt hjælpeprogram.
	8. Isoleret virtuelt rum, hvor mistænkelige filer kan analyseres sikkert.

Kontrolpunkt 7: Bogstavrod-udfordring

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

1. EJATNRRO
2. SYERAWP
3. SAKASEDSN
4. RMO
5. AMEASWORRN
6. IOKRTTO
7. RINGILSEO
8. ROEKLEGGY

Bonusaktivitet: Tænk hurtigt

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

1	Steder at hente sikre apps			
2	Enheder, der kan blive hacket			
3	Ting, du tager backup af			
4	Advarselstegn i en e-mail			
5	Tegn på, at telefonen har malware			
6	Typer af malware, du kender			
7	Filtyper, du skal passe på med			
8	Måder, malware kommer ind på en pc			
9	Sikkerhedsvaner, du kan starte i dag			
10	Ord, der har med cybersikkerhed at gøre			
11	Ting at gøre efter et datalæk			
12	Grunde til at opdatere software			
13	Dyr eller figurer med navne som malware			
14	Ting, malware kan stjæle			
15	Ting at gøre, hvis du klikkede forkert			

Kontrolpunkt 8: Casestudier om cybersikkerhed

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

CASESTUDIE 1: ISOLERING AF RANSOMWARE I VIRKSOMHEDEN



Scenarie: Et firmanetværk er ramt af aktiv ransomware. Vigtige filservere viser nu filendelsen .locked. Fastlæg regler for isolering.

Diskussion: Beskriv skridtene til isolering, og skitsér gendannelsen af data i en protokol.

CASESTUDIE 2: FILLØS MALWARE I HUKOMMELSEN



Scenarie: En analytiker opdager mistænkelige scripts, der kører direkte i systemets RAM via almindelige administratorværktøjer, men der findes ingen skadelige filer på disken.

Diskussion: Forklar strategien for analyse af hukommelsen, og angiv værktøjer, der blokerer filløs kørsel.

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

9	19	15	12	5	18		19	13	9	20	20	5	4	5

5	14	8	5	4	5	18		19	20	18	1	11	19

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 malware?

Skadeligt software, som angribere bruger til at skade, kapre eller stjæle data fra enheder og netværk.

Q2: Hvad er forskellen på en virus og en orm?

En virus kræver en menneskelig handling (som at åbne en fil) for at sprede sig, mens en orm spreder sig automatisk.

Q3: Hvordan smitter en trojansk hest en computer?

Den udgiver sig for at være et harmløst program og skjuler den skadelige kode indeni.

Q4: Hvad er ransomware?

Malware, der krypterer filerne på systemet og kræver betaling for nøglen. [1]

Q5: Hvad er spyware?

Skadeligt software, der i al hemmelighed optager tastetryk, adgangskoder og surfing og sender dem til angribere.

Kontrolpunkt 10: Grundlæggende FAQ om cybersikkerhed (del B)

Gennemgå almindelige spørgsmål og svar om afværgelse af trusler online.

Q6: Hvad betyder sandboxing?

At køre mistænkelige filer i et sikkert, isoleret virtuelt miljø og iagttage dem uden risiko for driften.

Q7: Hvad er filløs malware?

Malware, der kører direkte i hukommelsen via lovlige værktøjer og undgår at skrive filer til disken for at snyde scannere.

Q8: Hvordan beskytter et rootkit malware?

Det skjuler skadelige processer og filer, ofte ved at undergrave operativsystemets kerne, så antivirusscannere kan overse dem.

Q9: Hvad er dynamisk adfærdsovervågning?

Scanning, der overvåger processer i realtid og stopper typisk malwareadfærd som massekryptering af filer.

Q10: Hvorfor haster isolering under hændelseshåndtering?

Isolering af ramte enheder forhindrer, at malwaren spreder sig til andre enheder.

Kontrolpunkt 10: Avanceret FAQ om sikkerhed (del C)

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

Q1: Hvordan snyder malwareudviklere signaturbaserede scannere?

Med polymorfi: filens hash og kode ændres ved hver smitte, mens den skadelige adfærd er den samme.

Q2: Hvad er risikoen ved værktøjer med dobbelt anvendelse?

Angribere bruger lovlige værktøjer (som PowerShell eller Sysinternals) og gemmer sig i den normale trafik, så de er svære at opdage.

Q3: Hvordan kører process hollowing skadelig kode?

Den starter en lovlig proces sat på pause, udskifter koden i hukommelsen med malware og lader den køre videre.

Q4: Hvad gør en Command and Control-server (C2)?

En fjernserver, som hackere bruger til at sende ordrer og kode til malware på kaprede maskiner.

Q5: Hvorfor er keyloggere svære at opdage?

De bruger næsten ingen processorkraft og skjuler sig i lovlige program-mer.

Kontrolpunkt 10: Avanceret FAQ om sikkerhed (del D)

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

Q6: Hvordan forsinker sløring af kode analysen?

Koden krypteres eller omrokeres, så analyseværktøjer og scannere ikke kan læse den.

Q7: Hvad er et bootkit?

Et rootkit, der inficerer opstartsprocessen (MBR, bootsektoren eller UEFI-firmwaren), så det kører, før operativsystemet indlæses.

Q8: Hvordan finder heuristisk scanning zero-day-trusler?

Den leder efter mistænkelige mønstre og kommandoer i stedet for en kendt hash.

Q9: Hvad er faren ved DLL-kapring?

Et lovligt program tvinges til at indlæse en skadelig DLL, som er lagt i programmets mappe.

Q10: Hvordan bruger automatisk analyse virtualisering?

Mistænkelige filer køres i flere virtuelle maskiner, og der dannes automatisk adfærdslogfiler og PCAP-filer.

Del 11: 10 fakta og indsigter om cybersikkerhed fra virkeligheden

Gennemgå fakta om sikkerhedsbrud, forsvarsmekanismer og krav til overholdelse.

1. SIKKERHEDSINDSIGT

Trojanske heste er fortsat en almindelig infektionsmetode, fordi de skjuler skadelig kode i programmer, der ser harmløse ud.

2. SIKKERHEDSINDSIGT

FBI's IC3 modtog over 3,600 klager over ransomware i 2025 med rapporterede tab på over $32 millioner. [3]

3. SIKKERHEDSINDSIGT

Orme kan sprede sig hurtigt på tværs af netværk ved at udnytte ulappede protokolsårbarheder, fx EternalBlue i SMB.

4. SIKKERHEDSINDSIGT

Filløs malware er svær at opdage, fordi den kører i hukommelsen via legitime værktøjer og efterlader få spor på disken.

5. SIKKERHEDSINDSIGT

Sandkasser til analyse vender typisk tilbage til et rent øjebliksbillede efter hver kørsel, så hver test starter fra en kendt tilstand.

6. SIKKERHEDSINDSIGT

Rootkits kan ændre kernens systemkald og give falske resultater til anti-malware.

7. SIKKERHEDSINDSIGT

Sløring bruger pakkeprogrammer til at komprimere og skjule malwarens egentlige kode.

8. SIKKERHEDSINDSIGT

Polymorf malware ændrer sin kode, og dermed sin fil-hash, for hver ny kopi for at undgå signaturkontrol.

9. SIKKERHEDSINDSIGT

DLL-kapring udnytter søgerækkefølgen i styresystemer som Windows.

10. SIKKERHEDSINDSIGT

Sikkerhedsleverandører finder et enormt antal nye malwareprøver dagligt, så signaturer kræver konstant opdatering.

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

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

[2] CISA. (2023). #StopRansomware Guide.

https://www.cisa.gov/stopransomware/ransomware-guide

[3] FBI Internet Crime Complaint Center. (2026). 2025 IC3 Annual Report.

https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

[4] FBI Internet Crime Complaint Center. (n.d.). Ransomware.

https://www.ic3.gov/CrimeInfo/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 Spørgsmål 1

Rigtigt svar: A

UNDERVISNINGSNOTE

Hvad kendetegner en trojansk hest? → Den udgiver sig for at være lovligt software, så brugeren kører den

2 Spørgsmål 2

Rigtigt svar: A

UNDERVISNINGSNOTE

Hvilken type malware krypterer filer og kræver betaling? → Ransomware

3 Spørgsmål 3

Rigtigt svar: A

UNDERVISNINGSNOTE

Hvad er spyware? → Malware, der i al hemmelighed overvåger tastetryk og surfing

4 Spørgsmål 4

Rigtigt svar: A

UNDERVISNINGSNOTE

Hvorfor bruger malwareudviklere rootkits? → For at skjule aktive processer og skadelige filer for styresystemet

5 Spørgsmål 5

Rigtigt svar: A

UNDERVISNINGSNOTE

Hvad betyder sandboxing i analyse af malware? → At køre mistænkelige filer i et isoleret virtuelt rum for sikkert at iagttage dem

Facitliste: Kontrolpunkt 2 – Sandt eller falsk

6 Spørgsmål 6

Rigtigt svar: Falsk

UNDERVISNINGSNOTE

Falsk: orme kopierer sig selv og spreder sig på tværs af netværk uden nogen handling fra brugeren.

7 Spørgsmål 7

Rigtigt svar: Falsk

UNDERVISNINGSNOTE

Falsk: adware er ikke altid harmløs; meget af den sporer browsing for at målrette annoncer.

8 Spørgsmål 8

Rigtigt svar: Sandt

UNDERVISNINGSNOTE

Sandt: rene offline-backups gendanner krypterede filer uden betaling, selvom stjålne data stadig kan blive lækket.

9 Spørgsmål 9

Rigtigt svar: Falsk

UNDERVISNINGSNOTE

Falsk: signaturscannere kræver en kendt prøve, så helt ny zero-day-malware kan slippe forbi dem.

10 Spørgsmål 10

Rigtigt svar: Sandt

UNDERVISNINGSNOTE

Filløs malware kører skadelige scripts i hukommelsen uden at skrive filer til disken.

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

D 1. TROJANER	F 2. RANSOMWARE	A 3. SPYWARE	H 4. ROOTKIT
G 5. SANDKASSE	C 6. ISOLERING	E 7. ORM	B 8. FILLØS

KONTROLPUNKT 3: FACIT TIL NØGLEBEGREBER

1 TROJANER	2 RANSOMWARE	3 SPYWARE	4 ROOTKIT
5 SANDKASSE	6 ISOLERING		

KONTROLPUNKT 6, ALTERNATIV: FACIT TIL ORDMATCHNING

1 D – ROOTKIT	2 F – ISOLERING	3 H – KEYLOGGER	4 G – ORM
5 B – RANSOMWARE	6 C – SPYWARE	7 A – TROJANER	8 E – SANDKASSE

DISKUSSIONSNOTER TIL UNDERVISERE

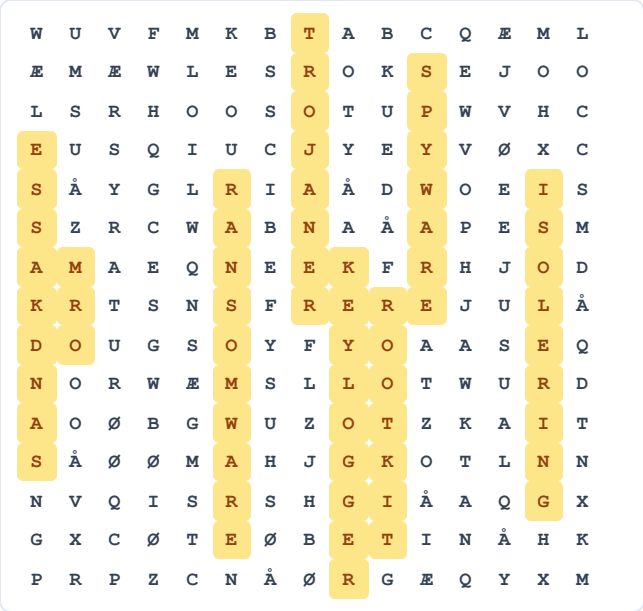
Fagbegreber:
Kontrollér, at eleverne kan forklare TROJANER, RANSOMWARE og SPYWARE med egne ord og give et eksempel på hvert begreb.

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

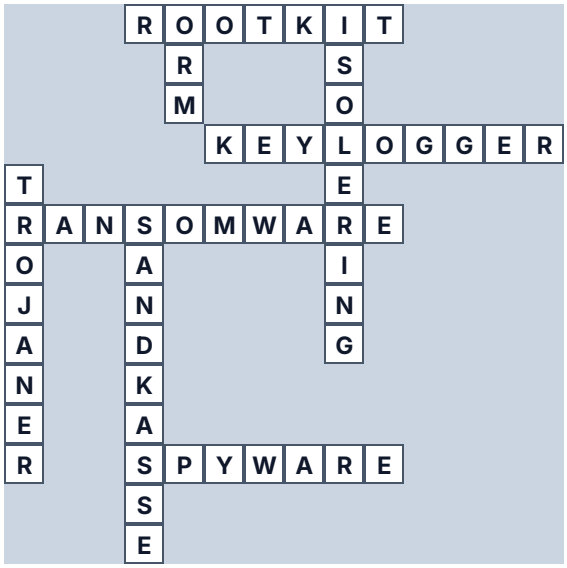
Kildekritik:
Lad eleverne efterprøve mindst én påstand mod referencerne i opgavearket, og drøft, hvorfor tal, priser og regler kan ændre sig over tid.

Facit til opgaver og undervisernoter

LØSNING PÅ ORDJAGT



LØSNING PÅ KRYDS OG TVÆRS



UNDERVISERVEJLEDNING TIL KRYDSORDSLØSNINGER

VANDRETTE NØGLER

1 vandret: ROOTKIT Skjult malware, der gemmer sig dybt i styresystemets kerne (7 bogstaver)

4 vandret: KEYLOGGER Program, der registrerer alt, hvad brugeren taster (9 bogstaver)

6 vandret: RANSOMWARE Skadelig kode, der låser data og kræver betaling for nøglen (10 bogstaver)

8 vandret: SPYWARE Software, der i al hemmelighed optager tastetryk og adgangskoder (7 bogstaver)

LODRETTE NØGLER

2 lodret: ORM Selvkopierende malware, der spreder sig uden menneskelig hjælp (3 bogstaver)

3 lodret: ISOLERING Det, der straks skal til for at stoppe spredningen af aktiv malware (9 bogstaver)

5 lodret: TROJANER Malware forklædt som et ufarligt hjælpeprogram (8 bogstaver)

7 lodret: SANDKASSE Isoleret virtuelt rum, hvor mistænkelige filer kan analyseres sikkert (9 bogstaver)

Facit til bogstavrod og chiffer

Bedømmelsesfacit til bogstavrod-øvelsen og den hemmelige chifferudfordring.

FACIT TIL BOGSTAVROD

1. EJATNRRO — **TROJANER**
2. SYERAWP — **SPYWARE**
3. SAKASEDSN — **SANDKASSE**
4. RMO — **ORM**
5. AMEASWORRN — **RANSOMWARE**
6. IOKRTTO — **ROOTKIT**
7. RINGILSEO — **ISOLERING**
8. ROEKLEGGY — **KEYLOGGER**

FACIT TIL HEMMELIG CHIFFERUDFORDRING

"ISOLER SMITTEDE ENHEDER STRAKS"

Facit til casestudier

A Casestudie 1: Isolering af ransomware i virksomheden

Underviserens løsning

BEDØMMELSESVEJLEDNING

Elevens svar bør dække følgende punkter:

- Analyse af scenariet: Firmanetværket er ramt af aktiv ransomware, og vigtige filservere viser filendelsen .locked.
- Anbefalet strategi og løsning: Kobl alle ramte servere fra netværket, afbryd aktive administratorsessioner, og gendan rene filer fra en sikker, skrivebeskyttet offline backup.

B Casestudie 2: Filløs malware i hukommelsen

Underviserens løsning

BEDØMMELSESVEJLEDNING

Elevens svar bør dække følgende punkter:

- Analyse af scenariet: En analytiker opdager mistænkelige scripts i RAM via almindelige værktøjer, men ingen skadelige filer på disken.
- Anbefalet strategi og løsning: Isolér de berørte enheder, og tag først et hukommelsesbillede. Gennemgå PowerShell- og WMI-logs, bloker ikke-godkendte scripts med AppLocker, og genstart derefter for at fjerne den skadelige kode.