Navn: _____ Dato: _____ Point: _____

Ransomwareangreb og genopretning af virksomheden

Afvikling af payload, kryptografisk filkryptering, offline-backups, inddæmningsprocedurer og katastrofegenopretning.

OVERBLIK OVER RANSOMWAREANGREB

SIKRET
DATAKRYPTERING
256-bit AES-standard

OVERHOLDER KRAV
GLOBALE STANDARDER
GDPR- og CCPA-rammer

ZERO-TRUST
ADGANGSPOLITIK
Multifaktorgodkendelse

Velkommen! Dette opgavehæfte guider dig gennem ransomwareangreb og genopretning af virksomheden. Du vil udforske kørsel af skadelig kode, kryptering af filer, offline backup, isolering af trusler, betaling i kryptovaluta og planer for genopretning efter katastrofer.

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/ransomware-angreb/

Din læringsplan for genopretning efter ransomware

- Skeln mellem trojanere, ransomware og spyware.
- Analysér skadelige filer i sikre sandkasser.
- Formulér procedurer for hurtig isolering af netværket.

VEJLEDNING TIL GUIDEN OM RANSOMWAREANGREB

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 genopretning efter ransomware. Slut af med bonusaktiviteten Tænk hurtigt.

RANSOMWAREANGREB OG GENOPRETNING EFTER KATASTROFER (INTRODUKTION)

Ransomware låser systemets lager kryptografisk og kræver betaling i kryptovaluta for nøglerne. Truslen afværges med regler for isolering af netværket, analyse af malware i sandkasser og solide offline backups helt adskilt fra netværket.

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

Kontrolpunkt 1: Flervalgsopgave

1. Hvordan virker et ransomwareangreb primært?

- A. Kryptografisk kryptering af filer, så adgangen spærres
- B. Skadelige SQL-kommandoer i formularfelter
- C. Aflytning af pakker på offentligt wi-fi
- D. Forfalskede e-mailheadere, der omgår SPF

2. Hvad er en offline backup?

- A. En kopi, der er koblet fra netværket, så malware ikke kan nå den
- B. En backup på webserverens egen disk
- C. En midlertidig cache af registreringslogfiler
- D. Et værktøj til at nulstille adgangskoder

3. Hvordan bør sikkerhedsteams isolere smittede systemer under et angreb?

- A. Tag netværkskablerne ud, og slå trådløst fra med det samme
- B. Opgrader antivirusdatabasen
- C. Luk den primære DNS-server
- D. Omdøb de ramte filendelser

4. Hvorfor fraråder myndighederne at betale løsesum?

- A. Betaling opmuntrer angriberne og garanterer ikke, at man får nøglen
- B. Den ugyldiggør automatisk alle forsikringer
- C. Det giver automatisk alle kunder besked via e-mail
- D. Den ødelægger de resterende backups

5. Hvad er en plan for genopretning efter katastrofer (DRP)?

- A. En fast proces for at genoprette drift og data efter et brud
- B. En firewallopsætning for indgående porte
- C. Et databaseskema over administratorrettigheder
- D. En protokol, der afviser forfalskede domæner

Kontrolpunkt 2: Sandt eller falsk-udfordring

6 Spørgsmål 6

6. Ransomware kan let sprede sig til online backups, der er koblet på netværket.

○ Sandt ○ Falsk

7 Spørgsmål 7

7. Betaler man løsesummen i kryptovaluta, er det sikkert, at filerne bliver dekrypteret.

○ Sandt ○ Falsk

8 Spørgsmål 8

8. At koble inficerede systemer fra netværket hjælper med at forhindre, at ransomware spreder sig til tilstødende systemer.

○ Sandt ○ Falsk

9 Spørgsmål 9

9. Ransomware bruger aldrig symmetrisk kryptering til at låse lageret.

○ Sandt ○ Falsk

10 Spørgsmål 10

10. Jævnlige test af gendannelse er en vigtig del af genopretning efter katastrofer.

○ Sandt ○ Falsk

Kontrolpunkt 3: Indsæt nøglebegreber

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

1. Adgangen til lokale filer spærres med _____ .
2. Den aktive skadelige kode, der køres på et system, kaldes _____ .
3. Afkoblede kopier uden for huset er en sikker _____ .
4. Spredningen af malware stoppes ved _____ .
5. Den betaling i kryptovaluta, som de kriminelle kræver, er en _____ .
6. Gendannelse af driftsdata efter en katastrofe kaldes _____ .

ORDBANK MED FAGUDTRYK

GENOPRETNING ISOLERING KATASTROFE KRYPTERING LØSESUM
OFFLINE-BACKUP PAYLOAD TROJANER

Skriv dine svar her:

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

Kontrolpunkt 4: Match sikkerhedsbegreber

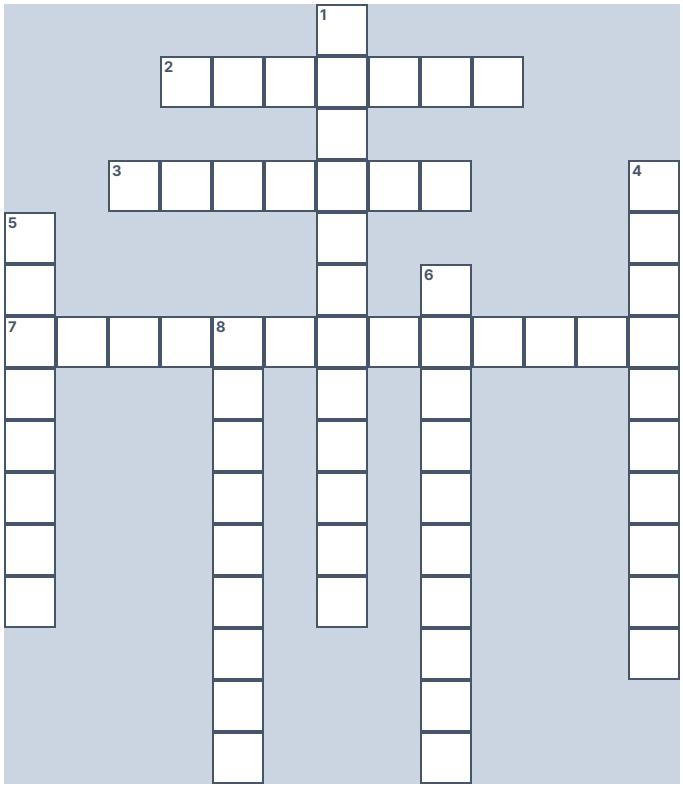
MATCH BEGREBER OG DEFINITIONER

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

☐	1. KRYPTERING	A	Afkobling af smittede systemer.
☐	2. PAYLOAD	B	Skadelig fil forklædt som ren.
☐	3. OFFLINE-BACKUP	C	Kryptografisk låsning af filer.
☐	4. ISOLERING	D	Alvorligt nedbrud i systemerne.
☐	5. LØSESUM	E	Kørsel af skadeligt software.
☐	6. GENOPRETNING	F	Afkoblet offline kopi.
☐	7. KATASTROFE	G	Gendannelse af databasen fra backup.
☐	8. TROJANER	H	Krav om betaling for nøglen.

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

2. Betalingen i kryptovaluta, som de kriminelle kræver (7)

3. Den aktive skadelige kode, der køres på et system (7)

7. Afkoblet kopi uden for huset, som malware ikke kan nå (13)

LODRETTE NØGLER

1. Gendannelse af driftsdata efter en katastrofe (12)

4. Det, ransomware bruger til at spærre adgangen til lokale filer (10)

5. Skadelig fil, der er forklædt som et rent program (8)

6. Alvorligt nedbrud, som en DRP-plan skal håndtere (10)

8. Afkobling af smittede enheder, så malwaren ikke spreder sig (9)

Kontrolpunkt 5, alternativ: Tilgængelige krydsordsnøgler

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

VANDRETTE NØGLER

2 vandret: Betalingen i kryptovaluta, som de kriminelle kræver (7 bogstaver):

3 vandret: Den aktive skadelige kode, der køres på et system (7 bogstaver):

7 vandret: Afkoblet kopi uden for huset, som malware ikke kan nå (13 bogstaver):

LODRETTE NØGLER

1 lodret: Gendannelse af driftsdata efter en katastrofe (12 bogstaver):

4 lodret: Det, ransomware bruger til at spærre adgangen til lokale filer (10 bogstaver):

5 lodret: Skadelig fil, der er forklædt som et rent program (8 bogstaver):

6 lodret: Alvorligt nedbrud, som en DRP-plan skal håndtere (10 bogstaver):

8 lodret: Afkobling af smittede enheder, så malwaren ikke spreder sig (9 bogstaver):

Kontrolpunkt 6: Skjult ordjagt

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

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

ORDLISTE MED FAGUDTRYK

KRYPTERING PAYLOAD OFFLINEBACKUP ISOLERING LØSESUM
GENOPRETNING KATASTROFE TROJANER

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. KRYPTERING**
- **B. PAYLOAD**
- **C. OFFLINEBACKUP**
- **D. ISOLERING**
- **E. LØSESUM**
- **F. GENOPRETNING**
- **G. KATASTROFE**
- **H. TROJANER**

DEFINITIONER OG MATCHFELTER

1. Afkoblet kopi uden for huset, som malware ikke kan nå.
2. Skadelig fil, der er forklædt som et rent program.
3. Det, ransomware bruger til at spærre adgangen til lokale filer.
4. Betalingen i kryptovaluta, som de kriminelle kræver.
5. Afkobling af smittede enheder, så malwaren ikke spreder sig.
6. Alvorligt nedbrud, som en DRP-plan skal håndtere.
7. Den aktive skadelige kode, der køres på et system.
8. Gendannelse af driftsdata efter en katastrofe.

Kontrolpunkt 7: Bogstavrod-udfordring

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

1. **NRETRKIGPY** _____
2. **UIFNFOKEPACBL** _____
3. **ELSMSUØ** _____
4. **TFSEAORKAT** _____
5. **ODLYPAA** _____
6. **NLSIRIEGO** _____
7. **TNPGEEGINNRO** _____
8. **JRARTENO** _____

Bonusaktivitet: Tænk hurtigt

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

1	Oplysninger, du aldrig bør dele			
2	Enheder, der kan blive hacket			
3	Grunde til ikke at betale løsesum			
4	Sikkerhedsvaner, du kan starte i dag			
5	Sikkerhedsværktøjer, du kender			
6	Måder at beskytte dine konti			
7	Tegn på, at en computer er inficeret			
8	Steder at gemme en backup			
9	Filer, du ikke vil miste			
10	Måder, ransomware spreder sig			
11	Ting at gøre i den første time af et angreb			
12	Personer, du skal kontakte ved et angreb			
13	Ting, ransomware kan låse			
14	Ord, der har med cybersikkerhed at gøre			
15	Organisationer, der ofte bliver ramt			

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.

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

CASESTUDIE 2: VURDERING AF OFFLINE BACKUP



Scenarie: En virksomhed vil udforme en strategi for databackup, der mindsker risikoen for, at backups kan blive kompromitteret, selv hvis det primære lokale netværk bliver fuldstændig overtaget af ransomware.

Diskussion: Design et sikkert offline backuparkiv.

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

8	15	12	4		4	9	14		2	1	3	11	21	16

15	6	6	12	9	14	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 ransomware?

Skadeligt software, der spærrer adgangen til systemer eller filer, indtil en løsesum er betalt.

Q2: Hvordan spreder ransomware sig?

Via vedhæftede filer i phishingmails, urettede sårbarheder og kompromitteret fjernadgang. [1]

Q3: Hvorfor kræves betaling i kryptovaluta?

Kryptovalutaer som Bitcoin er forholdsvis anonyme, så politiet har svært ved at spore pengene.

Q4: Blokerer antivirus ransomware?

Ja, men signaturbaseret antivirus kan fejle over for helt ny zero-day-ransomware.

Q5: Hvad er en air-gapped backup?

En kopi uden fysisk eller logisk forbindelse til netværket, så smitten ikke kan nå den.

Kontrolpunkt 10: Grundlæggende FAQ om cybersikkerhed (del B)

Gennemgå almindelige spørgsmål og svar om afværgelse af trusler online.

Q6: Hvad er dobbelt afpresning?

Når angribere både krypterer filer og stjæler data og truer med at lække dem, hvis der ikke betales.

Q7: Hvad er et dekrypteringsværktøj?

Et program med den nøgle, der skal til for at låse filerne op igen.

Q8: Hvordan opdager man ransomware tidligt?

Ved at overvåge filsystemet for pludselige massive ændringer og omdøbninger.

Q9: Hvilken rolle spiller forsikring?

En cyberforsikring kan hjælpe med at dække omkostninger til genopretning, men dækningsvilkår og regler for betaling af løsesum varierer fra police til police.

Q10: Skal jeg genstarte et smittet system?

Nej, en genstart kan slette spor i hukommelsen; isolér det i stedet fra netværket. [1]

Kontrolpunkt 10: Avanceret FAQ om sikkerhed (del C)

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

Q1: Hvordan bruger ransomware asymmetrisk kryptering?

Den krypterer med en offentlig nøgle i malwaren, så kun angriberens private nøgle kan dekryptere.

Q2: Hvorfor bruges også symmetrisk kryptering?

Symmetrisk kryptering (som AES) er hurtig og låser store databaser på minutter, mens asymmetriske nøgler beskytter AES-nøglen.

Q3: Hvad er logisk segmentering?

Opdeling af netværket i isolerede zoner, så malware ikke kan bevæge sig fra arbejdsstationer til centrale servere.

Q4: Hvad er WORM-lagring?

Medier, der skrives én gang og læses mange gange, så ransomware ikke kan ændre, overskrive eller slette backups.

Q5: Hvad er skyggekopier?

Lokale øjebliksbilleder fra Windows; ransomware sletter dem typisk først med administratorværktøjer.

Kontrolpunkt 10: Avanceret FAQ om sikkerhed (del D)

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

Q6: Hvordan baner stjålne logins vejen for ransomware?

Angribere køber lækkede administratorlogins, logger ind via fjernskrivebord og kører selv ransomwaren på netværket.

Q7: Hvad er prøvegendannelse?

Jævnlig gendannelse til isolerede testmiljøer for at bekræfte, at hastighed og datakvalitet lever op til kravene.

Q8: Hvordan stopper EDR ransomware?

Ved at analysere processers adfærd (f.eks. hurtig kryptering) og hurtigt sætte det ondsindede program på pause.

Q9: Hvad er ransomware as a service (RaaS)?

En franchisemodel, hvor udviklere udlejer ransomware til partnere mod en andel af løsesummerne.

Q10: Hvordan fører urettet RDP til ransomware?

Åbne, urettede RDP-adgange lader angribere gætte logins og starte malware manuelt.

Del 11: 10 fakta og indsigter om cybersikkerhed fra virkeligheden

Gennemgå fakta om sikkerhedsbrud, forsvarsmekanismer og krav til overholdelse.

1. SIKKERHEDSINDSIGT

Ransomware-aktører bruger ofte værktøjer som vssadmin.exe til at slette Windows' skyggekopier og blokere lokale gendannelser. [1]

2. SIKKERHEDSINDSIGT

Filerne krypteres typisk med symmetriske AES-256-nøgler, som derefter låses med offentlige RSA-nøgler.

3. SIKKERHEDSINDSIGT

Genopretning efter et vellykket ransomwareangreb kan tage uger, og derfor er testede offline backups vigtige.

4. SIKKERHEDSINDSIGT

FBI støtter ikke betaling af løsesum og advarer om, at betaling ikke garanterer, at du får nogen data tilbage. [2]

5. SIKKERHEDSINDSIGT

Katastrofeberedskabsplaner (DRP) bør fastlægge et Recovery Time Objective (RTO) og et Recovery Point Objective (RPO).

6. SIKKERHEDSINDSIGT

FBI anbefaler backups, der er krypterede og uforanderlige, dvs. at de ikke kan ændres eller slettes. [3]

7. SIKKERHEDSINDSIGT

Ransomwareudviklere bruger avanceret sløring for at snyde signaturbaseret antivirus.

8. SIKKERHEDSINDSIGT

Netværkssegmentering begrænser lateral bevægelse og hjælper med at forhindre ransomware i at sprede sig ud over den første inficerede vært. [3]

9. SIKKERHEDSINDSIGT

Eksponerede, dårligt sikrede fjerntjenester som Remote Desktop Protocol (RDP) er et almindeligt indgangspunkt for ransomware. [1]

10. SIKKERHEDSINDSIGT

CISA råder til at opbevare krypterede backups offline, da mange ransomwarevarianter leder efter og sletter backups, de kan nå. [1]

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. (2023). #StopRansomware Guide.

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

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

https://www.ic3.gov/CrimeInfo/Ransomware

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

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

[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 **Spørgsmål 1** — **Rigtigt svar: A**

UNDERVISNINGSNOTE

Hvordan virker et ransomwareangreb primært? → Kryptografisk kryptering af filer, så adgangen spærres

2 **Spørgsmål 2** — **Rigtigt svar: A**

UNDERVISNINGSNOTE

Hvad er en offline backup? → En kopi, der er koblet fra netværket, så malware ikke kan nå den

3 **Spørgsmål 3** — **Rigtigt svar: A**

UNDERVISNINGSNOTE

Hvordan bør sikkerhedsteams isolere smittede systemer under et angreb? → Tag netværkskablerne ud, og slå trådløst fra med det samme

4 **Spørgsmål 4** — **Rigtigt svar: A**

UNDERVISNINGSNOTE

Hvorfor fraråder myndighederne at betale løsesum? → Betaling opmuntrer angriberne og garanterer ikke, at man får nøglen

5 **Spørgsmål 5** — **Rigtigt svar: A**

UNDERVISNINGSNOTE

Hvad er en plan for genopretning efter katastrofer (DRP)? → En fast proces for at genoprette drift og data efter et brud

Facitliste: Kontrolpunkt 2 – Sandt eller falsk

6 Spørgsmål 6

Rigtigt svar: Sandt

UNDERVISNINGSNOTE

Ransomware kan let sprede sig til online backups, der er koblet på netværket.

7 Spørgsmål 7

Rigtigt svar: Falsk

UNDERVISNINGSNOTE

Falsk: FBI advarer om, at betaling ikke garanterer, at du får nogen data tilbage. [2]

8 Spørgsmål 8

Rigtigt svar: Sandt

UNDERVISNINGSNOTE

Sandt: CISA råder til at frakoble inficerede værter eller tage netværket offline for at begrænse spredningen.

9 Spørgsmål 9

Rigtigt svar: Falsk

UNDERVISNINGSNOTE

Falsk: ransomware krypterer som regel filer med hurtige symmetriske algoritmer som AES.

10 Spørgsmål 10

Rigtigt svar: Sandt

UNDERVISNINGSNOTE

Jævnlige test af gendannelse er en vigtig del af genopretning efter katastrofer.

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

C 1. KRYPTERING	E 2. PAYLOAD	F 3. OFFLINE-BACKUP	A 4. ISOLERING
H 5. LØSESUM	G 6. GENOPRETNING	D 7. KATASTROFE	B 8. TROJANER

KONTROLPUNKT 3: FACIT TIL NØGLEBEGREBER

1 KRYPTERING	2 PAYLOAD	3 OFFLINE-BACKUP	4 ISOLERING
5 LØSESUM	6 GENOPRETNING		

KONTROLPUNKT 6, ALTERNATIV: FACIT TIL ORDMATCHNING

1 C – OFFLINEBACKUP	2 H – TROJANER	3 A – KRYPTERING	4 E – LØSESUM
5 D – ISOLERING	6 G – KATASTROFE	7 B – PAYLOAD	8 F – GENOPRETNING

DISKUSSIONSNOTER TIL UNDERVISERE

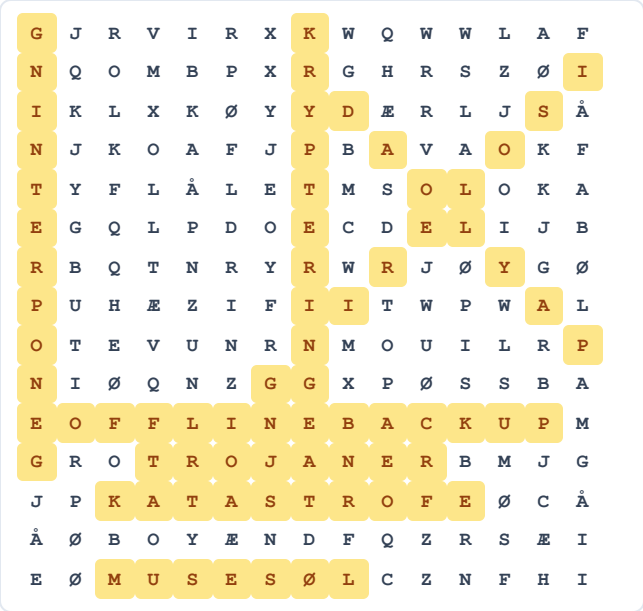
Fagbegreber:
Kontrollér, at eleverne kan forklare KRYPTERING, PAYLOAD og OFFLINE-BACKUP med egne ord og give et eksempel på hvert begreb.

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

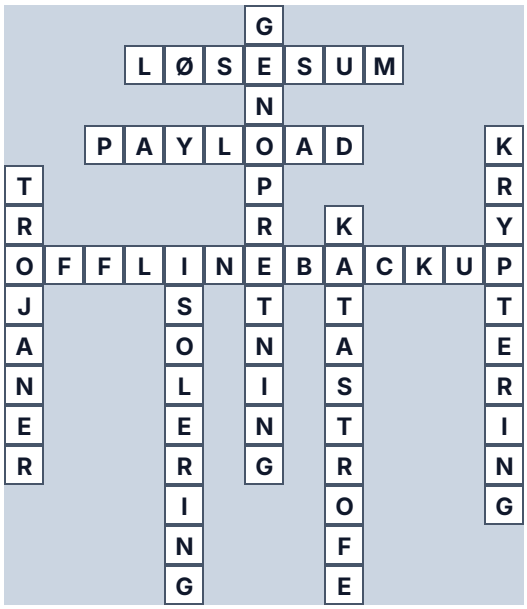
Kildekritik:
Lad eleverne efterprøve mindst én påstand mod referencerne i opgavearket, og drøft, hvorfor tal, priser og regler kan ændre sig over tid.

Facit til opgaver og undervisernoter

LØSNING PÅ ORDJAGT



LØSNING PÅ KRYDS OG TVÆRS



UNDERVISERVEJLEDNING TIL KRYDSORDSLØSNINGER

VANDRETTE NØGLER

2 vandret: LØSESUM Betalingen i kryptovaluta, som de kriminelle kræver (7 bogstaver)

3 vandret: PAYLOAD Den aktive skadelige kode, der køres på et system (7 bogstaver)

7 vandret: OFFLINEBACKUP Afkoblet kopi uden for huset, som malware ikke kan nå (13 bogstaver)

LODRETTE NØGLER

1 lodret: GENOPRETNING Gendannelse af driftsdata efter en katastrofe (12 bogstaver)

4 lodret: KRYPTERING Det, ransomware bruger til at spærre adgangen til lokale filer (10 bogstaver)

5 lodret: TROJANER Skadelig fil, der er forklædt som et rent program (8 bogstaver)

6 lodret: KATASTROFE Alvorligt nedbrud, som en DRP-plan skal håndtere (10 bogstaver)

8 lodret: ISOLERING Afkobling af smittede enheder, så malwaren ikke spreder sig (9 bogstaver)

Facit til bogstavrod og chiffer

Bedømmelsesfacit til bogstavrod-øvelsen og den hemmelige chifferudfordring.

FACIT TIL BOGSTAVROD

1. N R E T R K I G P Y — **KRYPTERING**
2. U I F N F O K E P A C B L — **OFFLINEBACKUP**
3. E L S M S U Ø — **LØSESUM**
4. T F S E A O R K A T — **KATASTROFE**
5. O D L Y P A A — **PAYLOAD**
6. N L S I R I E G O — **ISOLERING**
7. T N P G E E G I N N R O — **GENOPRETNING**
8. J R A R T E N O — **TROJANER**

FACIT TIL HEMMELIG CHIFFERUDFORDRING

"HOLD DIN BACKUP OFFLINE"

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: Vurdering af offline backup

Underviserens løsning

BEDØMMELSESVEJLEDNING

Elevens svar bør dække følgende punkter:

- Scenarieanalyse: En virksomhed vil udforme en strategi for databackup, der mindsker risikoen for, at backups bliver kompromitteret, selv hvis det primære lokale netværk bliver fuldstændig overtaget af ransomware.
- Anbefalet strategi og løsning: Brug WORM-lagring, kobl backupsystemet fra alle netværk, og skift de fysiske medier dagligt.