Navn: _____ Dato: _____ Poeng: _____

Angrep med løsepengevirus og virksomhetens Gjenoppretting

Kjøring av nyttelast, kryptografisk filkryptering, offline-sikkerhetskopier, inneslutningsprosedyrer og katastrofegjenoppretting.

LÆRINGSOVERSIKT OM ANGREP MED LØSEPENGEVIRUS

SIKRET
DATAKRYPTERING
256-bits AES-standard

I SAMSVAR
GLOBALE STANDARDER
Rammeverk for GDPR og CCPA

ZERO TRUST
TILGANGSPOLICY
Flerfaktorautentisering

Velkommen! Dette aktivitetsheftet veileder deg gjennom angrep med løsepengevirus og gjenoppretting av virksomheten. Du utforsker kjøring av nyttelast, filkryptering, offline sikkerhetskopier, inneslutning av trusler, betalinger i kryptovaluta og katastrofegjenopprettingsplaner.

KONTROLLPUNKTER I ARBEIDSARKET

- [ ] **Del 1-4: Behersk cybersikkerhet og forebygging av trusler.**
- [ ] **Del 5-7: Løs kryssord og ordsøk.**
- [ ] **Del 8-9: Løs casestudier og chifferutfordringen.**
- [ ] **Del 10: Gå gjennom sidene med grunnleggende og avanserte vanlige spørsmål.**
- [ ] **Del 11: Utforsk 10 interessante fakta fra virkeligheten.**
- [ ] **Bonus: Tenk raskt-utfordring.**

Åpne VPN.coms veiledning om cybersikkerhet

URL: https://www.vpn.com/no/cybersikkerhet/ransomware-angrep/

Din læringsveiledning for gjenoppretting etter løsepengevirus

- Skill mellom nyttelaster fra trojanere, løsepengevirus og spionprogrammer.
- Analyser ondsinnede filer i sikre sandkassemiljøer.
- Utform rutiner for rask nettverksisolering og inneslutning.

INSTRUKSJONER FOR VEILEDNING OM ANGREP MED LØSEPENGEVIRUS

Svar på flervalgsspørsmålene og sant/usant-spørsmålene, fyll ut setningene med ordbanken, koble sammen definisjoner, og løs kryssordet og ordsøket. Bruk kunnskapen din på gjenoppretting etter løsepengevirus. Avslutt med bonusaktiviteten Tenk raskt.

ANGREP MED LØSEPENGEVIRUS OG KATASTROFEGJENOPPRETTING (INNLEDNING)

Nyttelast fra løsepengevirus låser systemlagring kryptografisk og krever utbetaling i kryptovaluta for dekrypteringsnøklene. For å redusere denne trusselen trengs regler for nettverksisolering, analyse av skadevare i sandkasse og robuste, luftgappede kalde sikkerhetskopier.

LES HVERT KONTROLLPUNKT NØYE OG VELG ELLER SKRIV DET RIKTIGE SVARET.

Kontrollpunkt 1: Flervalgsutfordring

1. Hva er hovedmekanismen i et løsepengevirus-angrep?

- A. Kryptografisk kryptering av brukerfiler for å nekte tilgang til systemet
- B. Å injisere ondsinnede SQL-kommandoer i skjemafelt
- C. Å snuse på nettverkspakker på en offentlig Wi-Fi-tilkobling
- D. Å forfalske e-posthoder for å omgå SPF-validering

2. Hva er en frakoblet (kald) sikkerhetskopi?

- A. En lagringskopi som er koblet fra nettverket for å beskytte den mot spredning av skadevare
- B. En sikkerhetskopi lagret på harddisken til den primære webserveren
- C. En midlertidig hurtigbuffer for loggføringer i systemregisteret
- D. Et administrativt verktøy som brukes til å tilbakestille brukerpassord

3. Hvordan bør sikkerhetsteam isolere infiserte systemer under et løsepengevareangrep?

- A. Koble fra nettverkskablene og deaktivere trådløse grensesnitt umiddelbart
- B. Oppgrader databasen med antivirussignaturer
- C. Slå av den primære DNS-serveren
- D. Gi nytt navn til de kompromitterte filendelsene

4. Hvorfor fraråder sikkerhetsmyndigheter å betale krav fra løsepengevirus?

- A. Å betale oppmuntrer angripere og garanterer ikke at dekrypteringsnøkkelen leveres
- B. Den ugyldiggjør automatisk alle bedriftens forsikringer
- C. Den varsler automatisk alle kunder på e-post
- D. Den ødelegger de gjenværende sikkerhetskopifilene i systemet

5. Hva er en gjenopprettingsplan etter katastrofe (DRP)?

- A. En strukturert prosess for å gjenopprette drift og data etter at et system er kompromittert
- B. En brannmurkonfigurasjon som kartlegger innkommende nettverksporter
- C. Et databaseskjema som viser administrative rettigheter for brukere
- D. En protokoll for e-postautentisering som avviser forfalskede domener

Kontrollpunkt 2: Utfordring med sant eller usant

6 Spørsmål 6

6. Nyttelast fra løsepengevirus kan lett spre seg til nettbaserte sikkerhetskopier som er koblet til nettverket.

- ○ Sant
- ○ Usant

7 Spørsmål 7

7. Å betale løsepenger i kryptovaluta garanterer at filene blir dekryptert.

- ○ Sant
- ○ Usant

8 Spørsmål 8

8. Å koble infiserte systemer fra nettverket bidrar til å stoppe at løsepengevirus sprer seg til nærliggende systemer.

- ○ Sant
- ○ Usant

9 Spørsmål 9

9. Symmetrisk kryptografi brukes aldri av løsepengevirus til å kryptere systemlagring.

- ○ Sant
- ○ Usant

10 Spørsmål 10

10. Regelmessig testing av prosedyrer for gjenoppretting av data er en viktig del av katastrofegjenoppretting.

- ○ Sant
- ○ Usant

Kontrollpunkt 3: Sett inn nøkkelbegreper

Les hver setning nedenfor og fyll ut det tomme feltet med riktig begrep fra ordbanken.

1. Å nekte tilgang til lokale filer bruker kryptografisk _____ .
2. Den aktive skadelige koden som kjøres på et system, er _____ .
3. Lagringskopier utenfor stedet uten nettverkstilkobling utgjør en sikker _____ .
4. Å hindre at skadevare sprer seg krever _____ av endepunktene i nettverket.
5. Kryptovalutabetalingen som cyberkriminelle krever, er _____ .
6. Å få operative datafiler tilbake etter en katastrofe kalles _____ .

ORDBANK

FRAKOBLET KOPI | GJENOPPRETTING | ISOLERING | KRYPTERING | LØSEPENGER | NYTTELAST | SPIONVARE | TROJANER

Skriv svarene dine her:

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

Kontrollpunkt 4: Koble sikkerhetsbegreper

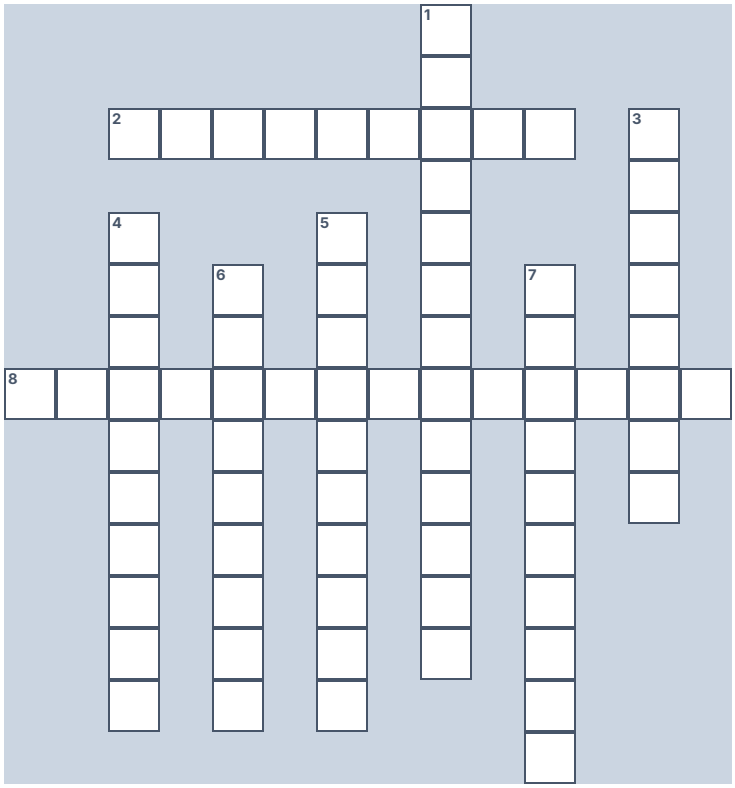
KOBLE DEFINISJONER

Koble hvert fagbegrep til venstre med riktig definisjon til høyre ved å skrive den tilhørende bokstaven (A-H) i det utfyllbare feltet.

☐	1. KRYPTERING	A	Koble infiserte nettverkssystemer fra nettet.
☐	2. NYTTELAST	B	Skadelig fil som later som den er ren.
☐	3. KALD SIKKERHETSKOPI	C	Å låse filer kryptografisk.
☐	4. ISOLASJON	D	Større systemavbrudd.
☐	5. LØSEPENGER	E	Kjøre skadelig programvare.
☐	6. GJENOPPRETTING	F	Frakoblet kopi uten nettverkstilgang.
☐	7. KATASTROFE	G	Gjenoppretting av databasen fra sikkerhetskopi.
☐	8. TROJANER	H	Forespørsel om utbetaling av kryptografisk nøkkel.

Kontrollpunkt 5: Kryssord

Løs kryssordet ved å skrive bokstaver i de aktive hvite rutene. Tallene tilsvarer hintene nedenfor.



VANNRETT

2. Kjøring av skadelig programvare. (9)

8. Gjenoppretting av database fra sikkerhetskopi. (14)

LODDRETT

1. Kopi uten tilkobling. (13)

3. Skadelig fil forkledd som ren. (8)

4. Krav om utbetaling for kryptografisk nøkkel. (10)

5. Kryptografisk låsing av filer. (10)

6. Frakobling av infiserte nettverkssystemer. (9)

7. Hendelse med stor systemforstyrrelse. (10)

Kontrollpunkt 5, alternativ: Tilgjengelige kryssordhint

Brukere av skjermleser og tastatur kan skrive inn kryssordsvarene direkte i tekstfeltene nedenfor.

VANNRETT

2 vannrett: Kjøring av skadelig programvare. (9 bokstaver):

8 vannrett: Gjenoppretting av database fra sikkerhetskopi. (14 bokstaver):

LODDRETT

1 loddrett: Kopi uten tilkobling. (13 bokstaver):

3 loddrett: Skadelig fil forkledd som ren. (8 bokstaver):

4 loddrett: Krav om utbetaling for kryptografisk nøkkel. (10 bokstaver):

5 loddrett: Kryptografisk låsing av filer. (10 bokstaver):

6 loddrett: Frakobling av infiserte nettverkssystemer. (9 bokstaver):

7 loddrett: Hendelse med stor systemforstyrrelse. (10 bokstaver):

Kontrollpunkt 6: Skjult ordsøk

Finn de 8 sentrale ordforrådsbegrepene som er skjult i rutenettet nedenfor. Ordene kan stå vannrett, loddrett eller diagonalt.

I Z U I G V Æ A R X P P Å Q J

P R V I R N X R W Q W W L A N

O F Q O M B I P E X G H R Y S

K Z Ø K L X K R Ø N Y Æ T R L

T J Å J K O A F E J A T B V A

E K F Y F L Å L E T E J M S O

L K A G Q L P D O L P C O D I

B J B B Q T N R A Y W Y J R Ø

O G Ø U H Æ Z S I F T W R P T

K W E F O R T S A T A K L K T

A G J E N O P P R E T T I N G

R E V I S O L E R I N G U N R

F M L Ø S E P E N G E R O U I

L R I Ø Q N Z X P Ø S S B A M

R O B M J G J P Ø C Å Å Ø B O

ORDLISTE

KRYPTERING NYTTELAST FRAKOBLETKOPI ISOLERING LØSEPENGER
GJENOPPRETTING KATASTROFE TROJANER

Kontrollpunkt 6, alternativ: Tilgjengelig ordkobling

Koble hvert av de 8 fagbegrepene fra ordsøket til riktig definisjon ved å skrive bokstaven (A-H) i det tomme feltet.

BEGREPER
A. KRYPTERING
B. NYTTELAST
C. FRAKOBLETKOPI
D. ISOLERING
E. LØSEPENGER
F. GJENOPPRETTING
G. KATASTROFE
H. TROJANER

DEFINISJONER OG TILHØRENDE FELT

1. Kopi uten tilkobling.
2. Skadelig fil forkledd som ren.
3. Kryptografisk låsing av filer.
4. Krav om utbetaling for kryptografisk nøkkel.
5. Frakobling av infiserte nettverkssystemer.
6. Hendelse med stor systemforstyrrelse.
7. Kjøring av skadelig programvare.
8. Gjenoppretting av database fra sikkerhetskopi.

Kontrollpunkt 7: Utfordring med blandede ord

Sett bokstavene nedenfor sammen i riktig rekkefølge for å avsløre sentrale begreper innen cybersikkerhet. Skriv svarene dine i svarboksene.

1. NRETRKIGPY
2. PORBAFOLITK EK
3. LEENØPREGS
4. TFSEAORKAT
5. AEYTLTNST
6. NLSIRIEGO
7. TNTGEJEGPIR NPO
8. JRARTENO

Bonusaktivitet: Tenk raskt

3 SVAR PER KATEGORI. DEN SOM FYLLER UT LISTEN FØRST, VINNER.

1	Informasjon du aldri bør dele			
2	Enheter som kan hackes			
3	Grunner til ikke å betale løsepenger			
4	Trygge vaner du kan begynne med i dag			
5	Sikkerhetsverktøy du kjenner til			
6	Måter å beskytte kontoene dine på			
7	Tegn på at en datamaskin er infisert			
8	Steder å oppbevare en sikkerhetskopi			
9	Filer du aldri vil miste			
10	Måter løsepengevirus sprer seg på			
11	Ting å gjøre den første timen av et angrep			
12	Personer å kontakte under et angrep			
13	Ting løsepengevirus kan låse			
14	Ord knyttet til cybersikkerhet			
15	Organisasjoner som ofte er mål for angrep			

Kontrollpunkt 8: Casestudier om cybersikkerhet

Bruk begrepene du har lært til å løse de virkelige scenarioene nedenfor.

CASESTUDIE 1: BEGRENSNING AV LØSEPENGEVIRUS-NYTTELAST I BEDRIFTER

👷

Scenario: Et lokalnett i en bedrift er brutt opp av aktivt løsepengevirus. Sentrale filservere har begynt å vise filtypene .locked.

Diskusjonsspørsmål: Beskriv i detalj trinnene for inneslutning, og skisser protokollen for datagjenoppretting.

CASESTUDIE 2: VURDERE ARKITEKTURER FOR OFFLINE-SIKKERHETSKOPIER

👷

Scenario: Et selskap vil utforme en strategi for sikkerhetskopiering som reduserer risikoen for at sikkerhetskopiene kan kompromitteres, selv om det primære lokale nettverket er fullstendig kapret av løsepengevirus.

Diskusjonsspørsmål: Utform et sikkert system med hvelv for frakoblet lagring av sikkerhetskopier.

Kontrollpunkt 9: Knekk chifferet

En cybersikkerhetsekspert beskytter nettverksressurser mot trusselaktører på nettet. Bruk nøkkelen med bokstaver og tall nedenfor til å dekryptere meldingen ved å skrive de tilhørende bokstavene i de tomme feltene.

NØKKEL FOR KRYPTERING AV BOKSTAV TIL TALL

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

7	10	5	14	15	16	16	18	5	20	20		11	18	25	16	20	5	18	20
19	25	19	20	5	13		6	18	1		6	18	1	11	15	2	12	5	20
							11	15	16	9									

Dekodet melding:

TIPS: HVERT TALL REPRESENTERER BOKSTAVENS PLASS I ALFABETET (F.EKS. 1 = A, 2 = B, 29 = Å).

Kontrollpunkt 10: Grunnleggende vanlige spørsmål om cybersikkerhet (Del A)

Gå gjennom vanlige spørsmål og svar om å redusere trusler på nettet.

Q1: Hva er løsepengevirus?

Løsepengevirus er skadelig programvare som er utviklet for å blokkere tilgang til datasystemer eller filer til en løsesum er betalt.

Q2: Hvordan sprer løsepengevirus seg?

Via e-postvedlegg med nettfiske, sårbarheter i programvare uten oppdateringer og kompromitterte systemer for fjerntilgang. [1]

Q3: Hvorfor kreves betaling i kryptovaluta?

Kryptovalutaer som Bitcoin gir relativ anonymitet, noe som gjør det vanskelig for rettshåndhevelsen å spore midlene.

Q4: Blokkerer antivirus løsepengevirus?

Ja, men signaturbasert antivirus kan svikte mot nyopprettet nulldagers-løsepengevirus.

Q5: Hva er en luftgappet sikkerhetskopi (air-gapped)?

En sikkerhetskopi uten fysisk eller logisk tilkobling til hovednettverket, som beskytter den mot spredning.

Kontrollpunkt 10: Grunnleggende vanlige spørsmål om cybersikkerhet (Del B)

Gå gjennom vanlige spørsmål og svar om å redusere trusler på nettet.

Q6: Hva er dobbel utpressing (double extortion)?

Når angripere ikke bare krypterer filer, men også stjeler sensitive data for å true med offentlig lekkasje hvis det ikke betales.

Q7: Hva er en dekrypteringsnøkkel (decryptor)?

Et programvareverktøy som inneholder den kryptografiske nøkkelen som trengs for å gjenopprette låste filer til klartekst.

Q8: Hvordan oppdager du løsepengevirus tidlig?

Ved å overvåke filsystemer for plutselig, massiv filendring og omdøping.

Q9: Hvilken rolle spiller forsikring?

Cyberforsikring kan bidra til å dekke gjenopprettingskostnader, men vilkårene for dekning og reglene for betaling av løsepenger varierer fra polise til polise.

Q10: Bør jeg starte et infisert system på nytt?

Nei, omstart kan ødelegge bevis i det flyktige minnet; isoler den fra nettverket i stedet. [1]

Kontrollpunkt 10: Avanserte vanlige spørsmål om sikkerhet (Del C)

Utforsk avanserte tekniske sider ved sikkerhetsrammeverk, analyse av skadevare og etterlevelse av datakrav.

Q1: Hvordan bruker løsepengevirus asymmetrisk kryptering?

Den bruker en offentlig nøkkel som er innebygd i skadevaren til å kryptere filer, og krever angriperens private nøkkel for å dekryptere dem.

Q2: Hvorfor brukes symmetrisk kryptering også?

Symmetrisk kryptering (som AES) er rask og kan låse enorme databaser på minutter, mens asymmetriske nøkler sikrer AES-nøkkelen.

Q3: Hva er logisk segmentering?

Å dele nettverk inn i isolerte soner hindrer at skadevare sprer seg sideveis fra arbeidsstasjoner til kjerneservere.

Q4: Hva er WORM-lagring?

Write-Once, Read-Many-medier, som hindrer at sikkerhetskopidata kan redigeres, overskrives eller slettes av løsepengevirus.

Q5: Hva er skyggekopier?

Lokale sikkerhetskopier (snapshots) som Windows lager; løsepengevirus sletter vanligvis disse først ved hjelp av administrative verktøy.

Kontrollpunkt 10: Avanserte vanlige spørsmål om sikkerhet (Del D)

Utforsk avanserte tekniske sider ved sikkerhetsrammeverk, analyse av skadevare og etterlevelse av datakrav.

Q6: Hvordan muliggjør tyveri av legitimasjon løsepengevirus?

Angripere kjøper lekkede administratorpåloginger for å logge inn via eksterne skrivebord og kjøre løsepengevirus manuelt i hele nettverket.

Q7: Hva er testing av gjenoppretting som prøvekjøring (dry run)?

Regelmessig gjenoppretting av sikkerhetskopierte databaser i isolerte testmiljøer for å verifisere at gjenopprettingshastigheten og dataintegriteten oppfyller målene for katastrofehåndtering.

Q8: Hvordan stopper endepunktdeteksjon (EDR) løsepengevirus?

Ved å analysere prosessatferd (for eksempel rask kryptering) og raskt stanse den ondsinnede appen.

Q9: Hva er en modell for løsepengevirus som tjeneste (RaaS)?

En franchisemodell der utviklere av skadevare leier ut løsepengevirus-byggere til tilknyttede aktører mot en prosentandel av utbetalingene.

Q10: Hvordan utløser en upatchet RDP løsepengevirus?

Eksponerte Remote Desktop Protocol-gatewayer uten oppdateringer lar angripere gjette påloggingsopplysninger med brute force og starte skadevare manuelt.

Del 11: 10 fakta om cybersikkerhet fra virkeligheten og innsikt

Gå gjennom virkelighetsnære fakta om sikkerhetsbrudd, forsvarsmekanismer og samsvarsstandarder.

1. SIKKERHETSINNSIKT

Aktører bak løsepengevirus bruker ofte verktøy som vssadmin.exe til å slette skyggekopier i Windows og blokkere lokale gjenopprettinger. [1]

2. SIKKERHETSINNSIKT

Symmetriske AES-256-nøkler brukes vanligvis til å kryptere filnyttelast, som deretter låses med offentlige RSA-nøkler.

3. SIKKERHETSINNSIKT

Å komme seg etter et vellykket løsepengevirusangrep kan ta uker, og derfor er testede frakoblede sikkerhetskopier viktige.

4. SIKKERHETSINNSIKT

FBI går ikke inn for å betale løsepenger og advarer om at betaling ikke garanterer at du får tilbake noen data. [2]

5. SIKKERHETSINNSIKT

Planer for katastrofegjenoppretting (DRP) bør definere et mål for gjenopprettingstid (RTO) og et mål for gjenopprettingspunkt (RPO).

6. SIKKERHETSINNSIKT

FBI anbefaler sikkerhetskopier som er krypterte og uforanderlige, noe som betyr at de ikke kan endres eller slettes. [3]

7. SIKKERHETSINNSIKT

Utviklere av løsepengevirus bruker avanserte obfuskeringsteknikker for å omgå tradisjonelle signaturbaserte antivirusskannere.

8. SIKKERHETSINNSIKT

Nettverkssegmentering begrenser lateral bevegelse og bidrar til å stoppe løsepengevirus fra å spre seg utover den første infiserte verten. [3]

9. SIKKERHETSINNSIKT

Eksponerte, dårlig sikrede eksterne tjenester som Remote Desktop Protocol (RDP) er et vanlig inngangspunkt for løsepengevirus. [1]

10. SIKKERHETSINNSIKT

CISA anbefaler å oppbevare krypterte sikkerhetskopier offline, siden mange varianter av løsepengevirus leter etter og sletter sikkerhetskopier som er tilgjengelige. [1]

Tekniske referanser og kilder

Studieveiledningen og de interaktive oppgavene er satt sammen fra globale standarder fra NIST og OWASP og standarder for etterlevelse av personvern.

FAGLIGE REFERANSER OG BRANSJEREFERANSER

[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

Fasit: Kontrollpunkt 1 – flervalg

1 Spørsmål 1

Riktig svar: A

MERKNAD TIL LÆREREN

Hva er hovedmekanismen i et løsepengevirus-angrep? → Kryptografisk kryptering av brukerfiler for å nekte tilgang til systemet

2 Spørsmål 2

Riktig svar: A

MERKNAD TIL LÆREREN

Hva er en frakoblet (kald) sikkerhetskopi? → En lagringskopi som er koblet fra nettverket for å beskytte den mot spredning av skadevare

3 Spørsmål 3

Riktig svar: A

MERKNAD TIL LÆREREN

Hvordan bør sikkerhetsteam isolere infiserte systemer under et løsepengevareangrep? → Koble fra nettverkskablene og deaktivere trådløse grensesnitt umiddelbart

4 Spørsmål 4

Riktig svar: A

MERKNAD TIL LÆREREN

Hvorfor fraråder sikkerhetsmyndigheter å betale krav fra løsepengevirus? → Å betale oppmuntrer angripere og garanterer ikke at dekrypteringsnøkkelen leveres

5 Spørsmål 5

Riktig svar: A

MERKNAD TIL LÆREREN

Hva er en gjenopprettingsplan etter katastrofe (DRP)? → En strukturert prosess for å gjenopprette drift og data etter at et system er kompromittert

Fasit: Kontrollpunkt 2 – sant eller usant

6 **Spørsmål 6** — **Riktig svar: Sant**

MERKNAD TIL LÆREREN

Nyttelast fra løsepengevirus kan lett spre seg til nettbaserte sikkerhetskopier som er koblet til nettverket.

7 **Spørsmål 7** — **Riktig svar: Usant**

MERKNAD TIL LÆREREN

Usant: FBI advarer om at betaling ikke gir noen garanti for at du får tilbake noen data. [2]

8 **Spørsmål 8** — **Riktig svar: Sant**

MERKNAD TIL LÆREREN

Sant: CISA anbefaler å trekke ut kontakten på infiserte verter eller ta nettverket offline for å begrense spredningen.

9 **Spørsmål 9** — **Riktig svar: Usant**

MERKNAD TIL LÆREREN

Usant: løsepengevirus krypterer vanligvis filer med raske symmetriske chiffer som AES.

10 **Spørsmål 10** — **Riktig svar: Sant**

MERKNAD TIL LÆREREN

Regelmessig testing av prosedyrer for gjenoppretting av data er en viktig del av katastrofegjenoppretting.

Fasit for ordforråd og vurderingsmatrise

Rettemal for læreren: Gi 1 poeng for hver riktige kobling (totalt 8 poeng) og hvert kontekstbegrep (totalt 6 poeng).

KONTROLLPUNKT 4: FASIT – KOBLE BEGREPER

C 1. KRYPTERING	E 2. NYTTELAST	F 3. KALD SIKKERHETSKOPI	A 4. ISOLASJON
H 5. LØSEPENGER	G 6. GJENOPPRETTING	D 7. KATASTROFE	B 8. TROJANER

KONTROLLPUNKT 3: FASIT – NØKKELBEGREPER

1 KRYPTERING	2 NYTTELAST	3 FRAKOBLET KOPI	4 ISOLERING
5 LØSEPENGER	6 GJENOPPRETTING		

KONTROLLPUNKT 6, ALTERNATIV: FASIT – KOBLE ORD

1 C – FRAKOBLETKOPI	2 H – TROJANER	3 A – KRYPTERING	4 E – LØSEPENGER
5 D – ISOLERING	6 G – KATASTROFE	7 B – NYTTELAST	8 F – GJENOPPRETTING

DISKUSJONSNOTATER TIL LÆRERE

Nøkkelbegreper:
Kontroller at elevene kan forklare KRYPTERING, NYTTELAST og KALD SIKKERHETSKOPI med egne ord og gi et eksempel på hvert.

Casestudier:
Be elevene begrunne anbefalingene sine med fakta fra arbeidsarket i stedet for antakelser.

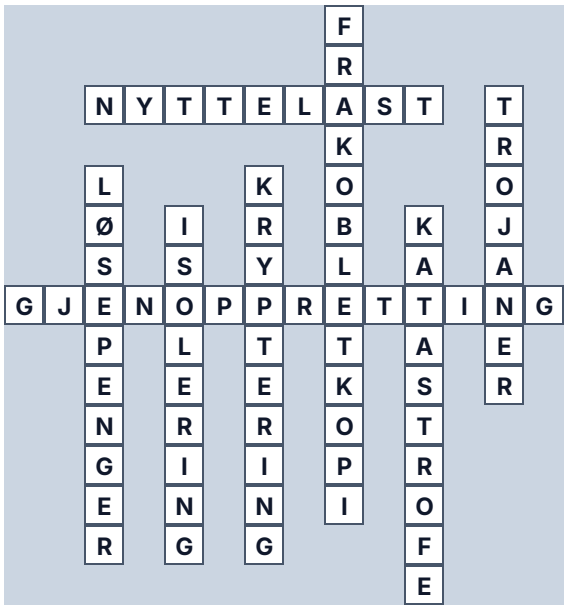
Kildevurdering:
La elevene kontrollere minst én påstand mot kildene i arbeidsarket, og drøft hvorfor tall, priser og regler kan endre seg over tid.

Fasit for oppgavene og merknader til læreren

LØSNING PÅ ORDSØKET

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

KRYSSORDLØSNING



LÆRERVEILEDNING FOR KRYSSORDLØSNINGER

VANNRETT

2 vannrett: NYTTELAST Kjøring av skadelig programvare. (9 bokstaver)

8 vannrett: GJENOPPRETTING Gjenoppretting av database fra sikkerhetskopi. (14 bokstaver)

LODDRETT

1 loddrett: FRAKOBLETKOPI Kopi uten tilkobling. (13 bokstaver)

3 loddrett: TROJANER Skadelig fil forkledd som ren. (8 bokstaver)

4 loddrett: LØSEPENGER Krav om utbetaling for kryptografisk nøkkel. (10 bokstaver)

5 loddrett: KRYPTERING Kryptografisk låsing av filer. (10 bokstaver)

6 loddrett: ISOLERING Frakobling av infiserte nettverkssystemer. (9 bokstaver)

7 loddrett: KATASTROFE Hendelse med stor systemforstyrrelse. (10 bokstaver)

Fasit for kodeord og chiffer

Fasit for vokabularøvelsen med ordstokking og den hemmelige chifferutfordringen.

FASIT: BOKSTAVBLANDING

1. N R E T R K I G P Y — **KRYPTERING**
2. P O R B A F O L I T K E K — **FRAKOBLETKOPI**
3. L E E N Ø P R E G S — **LØSEPENGER**
4. T F S E A O R K A T — **KATASTROFE**
5. A E Y T L T N S T — **NYTTELAST**
6. N L S I R I E G O — **ISOLERING**
7. T N T G E J E G P I R N P O — **GJENOPPRETTING**
8. J R A R T E N O — **TROJANER**

FASIT TIL DEN HEMMELIGE CHIFFERUTFORDRINGEN

"GJENOPPRETT KRYPTERT SYSTEM FRA FRAKOBLET KOPI"

Fasit til casestudiene

A Casestudie 1: Begrensning av løsepengevirus-nyttelast i bedrifter

Løsning for læreren

RETTEVEILEDNING

Elevsvar bør dekke følgende punkter:

- Scenarioanalyse: Et lokalt nettverk i et selskap er brutt gjennom av aktivt løsepengevirus. Viktige filservere har begynt å vise filtypene .locked.
- Anbefalt strategi og løsning: Koble alle berørte servere fra det lokale nettverket. Avslutt aktive administrative økter. Gjenopprett uskadde filer fra et sikkert, skrivebeskyttet frakoblet sikkerhetskopisystem.

B Casestudie 2: Vurdere arkitekturer for offline-sikkerhetskopier

Løsning for læreren

RETTEVEILEDNING

Elevsvar bør dekke følgende punkter:

- Scenarioanalyse: En bedrift vil utforme en strategi for sikkerhetskopiering som reduserer risikoen for at sikkerhetskopiene blir kompromittert, selv om det primære lokalnettet blir fullstendig kapret av løsepengevirus.
- Anbefalt strategi og løsning: Innfør WORM-lagring (write-once-read-many). Lag et logisk luftgap ved å koble sikkerhetskopisystemet fra alle nettverk, og håndhev daglig fysisk rotasjon av medier.