Namn: _____ Datum: _____ Poäng: _____

# Ransomware-attacker och företag Återhämtning

Körning av nyttolast, kryptografisk filkryptering, säkerhetskopior offline, inneslutningsrutiner och katastrofåterställning.

## LÄROÖVERSIKT OM RANSOMWARE-ATTACKER

**SÄKRAD**
**DATAKRYPTERING**
256-bitars AES-standard

**EFTERLEVANDE**
**GLOBALA STANDARDER**
Ramverken GDPR och CCPA

**ZERO TRUST**
**ÅTKOMSTPOLICY**
Multifaktorautentisering

**Välkommen!** Det här aktivitetshäftet guidar dig genom ransomware-attacker och företagsåterhämtning. Du utforskar körning av nyttolast, filkryptering, säkerhetskopior offline, inneslutning av hot, betalningar i kryptovaluta och katastrofåterställningsplaner.

**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/ransomware-attack/

# Din inlärningsplan för återhämtning efter ransomware

- Skilj mellan trojaner, utpressningsprogram och spionprogram.
- Analysera skadliga filer i säkra sandlådemiljöer.
- Utforma rutiner för snabb nätverksisolering och inneslutning.

## ANVISNINGAR FÖR GUIDEN OM RANSOMWARE-ATTACKER

Besvara flervalsfrågorna och sant/falskt-frågorna, fyll i luckorna med hjälp av ordbanken, matcha definitioner och lös korsordet och ordletarpusslet. Tillämpa dina kunskaper om återhämtning efter ransomware. Avsluta med bonusaktiviteten Tänk snabbt.

## RANSOMWARE-ATTACKER OCH ÅTERSTÄLLNING EFTER KATASTROF (INTRODUKTION)

Ransomware-nyttolaster låser systemlagring kryptografiskt och kräver betalning i kryptovaluta för dekrypteringsnycklar. För att minska detta hot används regler för nätverksisolering, analys av skadlig kod i sandlåda och robusta luftgapade kalla säkerhetskopior.

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

## Kontrollpunkt 1: Utmaning med flerval

**1** **1. Vad är den främsta mekanismen i en attack med utpressningsvirus?**

- A. Kryptografisk kryptering av användarfiler för att neka åtkomst till systemet
- B. Att injicera skadliga SQL-kommandon i formulärfält
- C. Att avlyssna nätverkspaket i ett offentligt Wi-Fi
- D. Att förfalska e-postrubriker för att kringgå SPF-validering

**2** **2. Vad är en offline-säkerhetskopia (kall säkerhetskopia)?**

- A. En lagringskopia som är frånkopplad från nätverket för att skydda den mot spridning av skadlig kod
- B. En säkerhetskopia lagrad på den primära webbserverns hårddisk
- C. En tillfällig cache med systemregisterloggar
- D. Ett administrativt verktyg för att återställa användares lösenord

**3** **3. Hur bör säkerhetsteam isolera infekterade system under en ransomware-attack?**

- A. Koppla omedelbart bort nätverkskablar och inaktivera trådlösa gränssnitt
- B. Uppgradera antivirusets signaturdatabas
- C. Stäng av den primära DNS-servern
- D. Byta namn på de komprometterade filändelserna

**4** **4. Varför avråder säkerhetsmyndigheter från att betala krav från utpressningsvirus?**

- A. Att betala uppmuntrar angripare och garanterar inte att dekrypteringsnyckeln levereras
- B. Den upphäver automatiskt alla företagets försäkringar
- C. Den meddelar automatiskt alla kunder via e-post
- D. Den korrumperar de återstående filerna i systemets säkerhetskopior

**5** **5. Vad är en katastrofåterställningsplan (DRP)?**

- A. En strukturerad process för att återställa verksamhet och data efter att ett system har kompromitterats
- B. En brandväggskonfiguration som mappar inkommande nätverksportar
- C. Ett databasschema som listar användarnas administrativa behörigheter
- D. Ett protokoll för e-postautentisering som avvisar förfalskade domäner

## Kontrollpunkt 2: Utmaning med sant eller falskt

### 6 Fråga 6

6. Ransomware-nyttolaster kan lätt spridas till säkerhetskopior online som är anslutna till nätverket.

- ○ Sant
- ○ Falskt

### 7 Fråga 7

7. Att betala lösensumman i kryptovaluta garanterar att filerna dekrypteras.

- ○ Sant
- ○ Falskt

### 8 Fråga 8

8. Att koppla bort infekterade system från nätverket hjälper till att stoppa att utpressningsprogram sprids till angränsande system.

- ○ Sant
- ○ Falskt

### 9 Fråga 9

9. Symmetrisk kryptografi används aldrig av ransomware för att kryptera systemlagring.

- ○ Sant
- ○ Falskt

### 10 Fråga 10

10. Att regelbundet testa rutiner för dataåterställning är en viktig del av katastrofåterställning.

- ○ Sant
- ○ Falskt

## Kontrollpunkt 3: Infoga nyckelbegrepp

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

1. Att neka åtkomst till lokala filer sker med kryptografisk _____ .
2. Den aktiva skadliga koden som körs på ett system utgör dess _____ .
3. Frånkopplade lagringskopior på en annan plats utgör en säker _____ .
4. Att stoppa skadlig kod från att spridas kräver _____ av slutpunkter i nätverket.
5. Den kryptovalutabetalning som cyberkriminella kräver är _____ .
6. Att återställa operativa datafiler ingår i _____ efter en katastrof.

**ORDBANK**

ISOLERING KATASTROF KRYPTERING LÖSENSUMMA NYTTOLAST
OFFLINE-KOPIA TROJAN ÅTERSTÄLLNING

**Skriv dina svar här:**

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

# Kontrollpunkt 4: Matchning av säkerhetsbegrepp

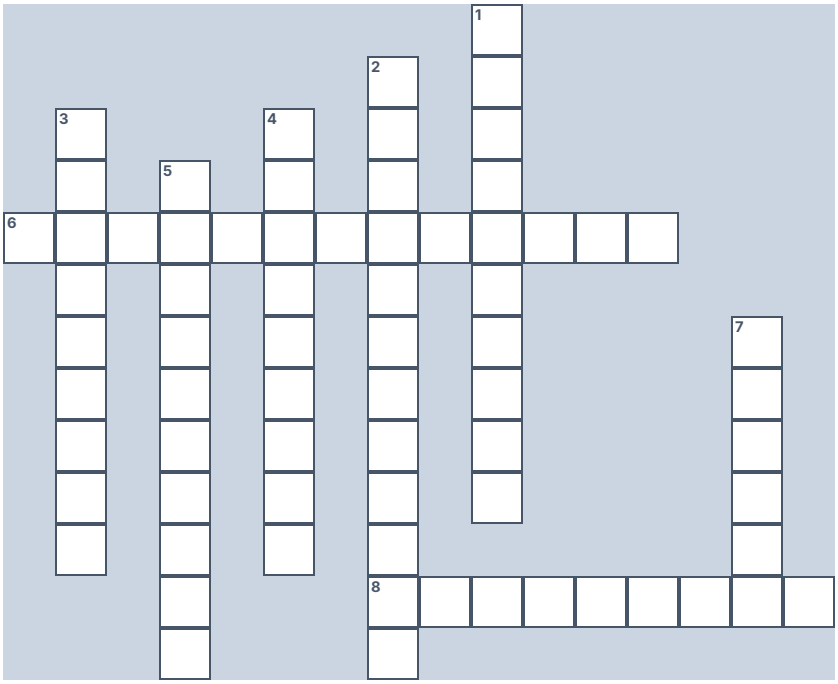
## MATCHNING AV DEFINITIONER

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

| | | | |
|---|---|---|---|
| ☐ | 1. KRYPTERING | A | Att koppla bort infekterade nätverkssystem. |
| ☐ | 2. NYTTOLAST | B | Skadlig fil som utger sig för att vara ren. |
| ☐ | 3. KALL BACKUP | C | Att låsa filer kryptografiskt. |
| ☐ | 4. ISOLERING | D | Större systemstörning. |
| ☐ | 5. LÖSEN | E | Att köra skadlig programvara. |
| ☐ | 6. ÅTERSTÄLLNING | F | Frånkopplad offlinekopia. |
| ☐ | 7. KATASTROF | G | Att återställa databasen från backup. |
| ☐ | 8. TROJAN | H | Begäran om utbetalning av kryptografisk nyckel. |

# Kontrollpunkt 5: Korsord

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




## VÅGRÄTT

**6. Återställning av databasen från säkerhetskopia. (13)**

**8. Frånkoppling av infekterade nätverkssystem. (9)**

## LODRÄTT

**1. Krav på betalning för en kryptografisk nyckel. (10)**

**2. Frånkopplad kopia utan nätverksanslutning. (12)**

**3. Större störning i systemen. (9)**

**4. Körning av skadlig programvara. (9)**

**5. Kryptografisk låsning av filer. (10)**

**7. Skadlig fil som utger sig för att vara ren. (6)**

# Kontrollpunkt 5, alternativ: Tillgängliga korsordsledtrådar

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

## VÅGRÄTT

**6 vågrätt: Återställning av databasen från säkerhetskopia. (13 bokstäver):**

**8 vågrätt: Frånkoppling av infekterade nätverkssystem. (9 bokstäver):**

## LODRÄTT

**1 lodrätt: Krav på betalning för en kryptografisk nyckel. (10 bokstäver):**

**2 lodrätt: Frånkopplad kopia utan nätverksanslutning. (12 bokstäver):**

**3 lodrätt: Större störning i systemen. (9 bokstäver):**

**4 lodrätt: Körning av skadlig programvara. (9 bokstäver):**

**5 lodrätt: Kryptografisk låsning av filer. (10 bokstäver):**

**7 lodrätt: Skadlig fil som utger sig för att vara ren. (6 bokstäver):**

## Kontrollpunkt 6: Dolt ordsök

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

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

**ORDLISTA**

KRYPTERING NYTTOLAST OFFLINEKOPIA ISOLERING LÖSENSUMMA
ÅTERSTÄLLNING KATASTROF TROJAN

# 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. KRYPTERING**
- **B. NYTTOLAST**
- **C. OFFLINEKOPIA**
- **D. ISOLERING**
- **E. LÖSENSUMMA**
- **F. ÅTERSTÄLLNING**
- **G. KATASTROF**
- **H. TROJAN**

**DEFINITIONER OCH MATCHNINGSFÄLT**

1. Frånkopplad kopia utan nätverksanslutning.
2. Skadlig fil som utger sig för att vara ren.
3. Kryptografisk låsning av filer.
4. Krav på betalning för en kryptografisk nyckel.
5. Frånkoppling av infekterade nätverkssystem.
6. Större störning i systemen.
7. Körning av skadlig programvara.
8. Återställning av databasen från säkerhetskopia.

## Kontrollpunkt 7: Utmaning med blandade ord

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

1. NRETRKIGPY
2. AFINOPIFKOEL
3. LSMUÖNAEMS
4. SFOARTKAT
5. AOYTLTNST
6. NLSIRIEGO
7. NILTÅTLSGNEÄR
8. ONTAJR

# Bonusaktivitet: Tänk snabbt

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

| | | | | |
|---|---|---|---|---|
| 1 | Information du aldrig bör dela | | | |
| 2 | Enheter som kan hackas | | | |
| 3 | Skäl till att inte betala lösensumman | | | |
| 4 | Säkra vanor du kan börja med i dag | | | |
| 5 | Säkerhetsverktyg du känner till | | | |
| 6 | Sätt att skydda dina konton | | | |
| 7 | Tecken på att en dator är infekterad | | | |
| 8 | Platser där du kan förvara en säkerhetskopia | | | |
| 9 | Filer du aldrig vill förlora | | | |
| 10 | Sätt som utpressningsprogram sprids | | | |
| 11 | Saker att göra under den första timmen av en attack | | | |
| 12 | Personer att kontakta under en attack | | | |
| 13 | Saker som utpressningsprogram kan låsa | | | |
| 14 | Ord som hör ihop med cybersäkerhet | | | |
| 15 | Organisationer som ofta utsätts för attacker | | | |

# Kontrollpunkt 8: Fallstudier om cybersäkerhet

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

## FALLSTUDIE 1: BEGRÄNSA RANSOMWARE-NYTTOLAST I FÖRETAG

👨‍💻

**Scenario: Ett lokalt nätverk (LAN) på ett företag har drabbats av pågående ransomware.** Viktiga filservrar har börjat visa filändelser med .locked.

**Diskussionsfråga:** Beskriv i detalj stegen för isolering och redogör för protokollet för dataåterställning.

## FALLSTUDIE 2: UTVÄRDERA ARKITEKTURER FÖR OFFLINE-BACKUP

👨‍💻

**Scenario:** Ett företag vill utforma en strategi för säkerhetskopiering som minskar risken för att säkerhetskopiorna kompromitteras, även om det primära lokala nätverket helt kapas av utpressningsprogram.

**Diskussionsfråga: Utforma ett säkert valvsystem för offline-lagring av säkerhetskopior.**

# 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

| | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 27 | 20 | 5 | 18 | 19 | 20 | 28 | 12 | 12 | | 11 | 18 | 25 | 16 | 20 | 5 | 18 | 1 | 4 |
| | | | | | | | | | | | | | | | | | | |
| | | | | | 4 | 1 | 20 | 1 | | 6 | 18 | 27 | 14 | | | | | |
| | | | | | | | | | | | | | | | | | | |
| | | | | 15 | 6 | 6 | 12 | 9 | 14 | 5 | 11 | 15 | 16 | 9 | 1 | | | |
| | | | | | | | | | | | | | | | | | | |

**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 ransomware?

Ransomware är skadlig programvara som är utformad för att blockera åtkomst till datorsystem eller filer tills en lösensumma har betalats.

### Q2: Hur sprids ransomware?

Via nätfiskebilagor i e-post, ej korrigerade sårbarheter i programvara och komprometterade system för fjärråtkomst. [1]

### Q3: Varför begärs betalning i kryptovaluta?

Kryptovalutor som Bitcoin erbjuder relativ anonymitet, vilket gör det svårt för brottsbekämpande myndigheter att spåra pengarna.

### Q4: Blockerar antivirusprogram ransomware?

Ja, men signaturbaserat antivirus kan misslyckas mot nyskapade zero-day-nyttolaster med utpressningsvirus.

### Q5: Vad är en luftgapad säkerhetskopia?

En säkerhetskopia utan fysisk eller logisk koppling till det primära nätverket, vilket skyddar den mot spridning.

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

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

### Q6: Vad är dubbel utpressning?

När angripare inte bara krypterar filer utan också stjäl känsliga data för att hota med offentliga läckor om de inte får betalt.

### Q7: Vad är en dekrypterare?

Ett programverktyg som innehåller den kryptografiska nyckel som behövs för att återställa låsta filer till klartext.

### Q8: Hur upptäcker man ransomware tidigt?

Genom att övervaka filsystem efter plötsliga, massiva filändringar och namnbyten.

### Q9: Vilken roll har försäkring?

Cyberförsäkring kan hjälpa till att täcka återhämtningskostnader, men villkoren och reglerna för betalning av lösen varierar mellan försäkringar.

### Q10: Ska jag starta om ett infekterat system?

Nej, en omstart kan förstöra flyktiga minnesbevis; isolera den från nätverket i stället. [1]

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

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

### Q1: Hur använder ransomware asymmetrisk kryptering?

Den använder en publik nyckel inbäddad i den skadliga koden för att kryptera filer, och angriparens privata nyckel krävs för att dekryptera dem.

### Q2: Varför används symmetrisk kryptering också?

Symmetrisk kryptering (som AES) är snabb och kan låsa enorma databaser på några minuter, medan asymmetriska nycklar skyddar AES-nyckeln.

### Q3: Vad är logisk segmentering?

Att dela upp nätverk i isolerade zoner, vilket hindrar skadlig kod från att sprida sig i sidled från arbetsstationer till centrala servrar.

### Q4: Vad är WORM-lagring?

Write-Once, Read-Many-media, som hindrar säkerhetskopierad data från att redigeras, skrivas över eller raderas av nyttolaster från utpressningsvirus.

### Q5: Vad är skuggkopior?

Lokala säkerhetskopior (ögonblicksbilder) som skapas av Windows; ransomware tar vanligtvis bort dem först med administrativa verktyg.

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

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

### Q6: Hur möjliggör stöld av inloggningsuppgifter ransomware?

Angripare köper läckta administratörsinloggningar för att logga in via fjärrskrivbord och köra ransomware manuellt i hela nätverket.

### Q7: Vad är återställningstest i testläge (dry-run)?

Att regelbundet återställa backupdatabaser i isolerade testmiljöer för att verifiera att återställningshastigheten och dataintegriteten uppfyller målen för katastrofåterställning.

### Q8: Hur stoppar slutpunktsdetektering (EDR) ransomware?

Genom att analysera processbeteende (t.ex. snabb kryptering) och snabbt stoppa det skadliga programmet.

### Q9: Vad är en modell med ransomware som tjänst (RaaS)?

En franchisemodell där utvecklare av skadlig kod hyr ut ransomware-byggare till affiliates mot en procentandel av utbetalningarna.

### Q10: Hur utlöser ett ouppdaterat RDP ransomware?

Exponerade, ej korrigerade gateways för Remote Desktop Protocol gör det möjligt för angripare att gissa inloggningar med brute force och starta skadlig kod manuellt.

# Del 11: 10 verkliga fakta och insikter om cybersäkerhet

Gå igenom verkliga fakta om säkerhetsintrång, försvarsmekanismer och efterlevnadsstandarder.

**1. SÄKERHETSINSIKT**

Ransomware-aktörer använder ofta verktyg som vssadmin.exe för att radera skuggkopior i Windows och blockera lokala återställningar. [1]

**2. SÄKERHETSINSIKT**

Symmetriska AES-256-nycklar används vanligtvis för att kryptera filers nyttolast, som sedan låses med publika RSA-nycklar.

**3. SÄKERHETSINSIKT**

Att återhämta sig från ett lyckat ransomware-angrepp kan ta veckor, och därför är testade offline-backuper viktiga.

**4. SÄKERHETSINSIKT**

FBI stöder inte att man betalar lösen och varnar för att betalning inte garanterar att du får tillbaka några data. [2]

**5. SÄKERHETSINSIKT**

Katastrofåterställningsplaner (DRP) bör definiera ett mål för återställningstid (RTO) och ett mål för återställningspunkt (RPO).

**6. SÄKERHETSINSIKT**

FBI rekommenderar säkerhetskopior som är krypterade och oföränderliga, vilket innebär att de inte kan ändras eller raderas. [3]

**7. SÄKERHETSINSIKT**

Utvecklare av ransomware använder avancerade obfuskeringstekniker för att kringgå traditionella signaturbaserade antivirusskannrar.

**8. SÄKERHETSINSIKT**

Nätverkssegmentering begränsar rörelser i sidled och hjälper till att stoppa ransomware från att spridas bortom den första infekterade värden. [3]

**9. SÄKERHETSINSIKT**

Exponerade, dåligt skyddade fjärrtjänster som Remote Desktop Protocol (RDP) är en vanlig ingång för utpressningsprogram. [1]

**10. SÄKERHETSINSIKT**

CISA rekommenderar att krypterade säkerhetskopior förvaras offline, eftersom många varianter av ransomware söker efter och raderar åtkomliga säkerhetskopior. [1]

# 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] 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

## Facit: Kontrollpunkt 1 – Flerval

### 1 Fråga 1

**Rätt svar: A**

#### ANTECKNING FÖR LÄRAREN

Vad är den främsta mekanismen i en attack med utpressningsvirus? → Kryptografisk kryptering av användarfiler för att neka åtkomst till systemet

### 2 Fråga 2

**Rätt svar: A**

#### ANTECKNING FÖR LÄRAREN

Vad är en offline-säkerhetskopia (kall säkerhetskopia)? → En lagringskopia som är frånkopplad från nätverket för att skydda den mot spridning av skadlig kod

### 3 Fråga 3

**Rätt svar: A**

#### ANTECKNING FÖR LÄRAREN

Hur bör säkerhetsteam isolera infekterade system under en ransomware-attack? → Koppla omedelbart bort nätverkskablar och inaktivera trådlösa gränssnitt

### 4 Fråga 4

**Rätt svar: A**

#### ANTECKNING FÖR LÄRAREN

Varför avråder säkerhetsmyndigheter från att betala krav från utpressningsvirus? → Att betala uppmuntrar angripare och garanterar inte att dekrypteringsnyckeln levereras

### 5 Fråga 5

**Rätt svar: A**

#### ANTECKNING FÖR LÄRAREN

Vad är en katastrofåterställningsplan (DRP)? → En strukturerad process för att återställa verksamhet och data efter att ett system har komprometterats

## Facit: Kontrollpunkt 2 – Sant eller falskt

### 6 Fråga 6

**Rätt svar: Sant**

**ANTECKNING FÖR LÄRAREN**

Ransomware-nyttolaster kan lätt spridas till säkerhetskopior online som är anslutna till nätverket.

### 7 Fråga 7

**Rätt svar: Falskt**

**ANTECKNING FÖR LÄRAREN**

Falskt: FBI varnar för att betalning inte garanterar att du får tillbaka några data. [2]

### 8 Fråga 8

**Rätt svar: Sant**

**ANTECKNING FÖR LÄRAREN**

Sant: CISA rekommenderar att infekterade värdar kopplas ur eller att nätverket tas offline för att begränsa spridningen.

### 9 Fråga 9

**Rätt svar: Falskt**

**ANTECKNING FÖR LÄRAREN**

Falskt: utpressningsprogram krypterar vanligtvis filer med snabba symmetriska chiffer som AES.

### 10 Fråga 10

**Rätt svar: Sant**

**ANTECKNING FÖR LÄRAREN**

Att regelbundet testa rutiner för dataåterställning är en viktig del av katastrofåterställning.

# 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

| | | | |
|---|---|---|---|
| C 1. KRYPTERING | E 2. NYTTOLAST | F 3. KALL BACKUP | A 4. ISOLERING |
| H 5. LÖSEN | G 6. ÅTERSTÄLLNING | D 7. KATASTROF | B 8. TROJAN |

## KONTROLLPUNKT 3: FACIT – NYCKELBEGREPP

| | | | |
|---|---|---|---|
| 1 KRYPTERING | 2 NYTTOLAST | 3 OFFLINE-KOPIA | 4 ISOLERING |
| 5 LÖSENSUMMA | 6 ÅTERSTÄLLNING | | |

## KONTROLLPUNKT 6, ALTERNATIV: FACIT – MATCHNING AV ORD

| | | | |
|---|---|---|---|
| 1 C – OFFLINEKOPIA | 2 H – TROJAN | 3 A – KRYPTERING | 4 E – LÖSENSUMMA |
| 5 D – ISOLERING | 6 G – KATASTROF | 7 B – NYTTOLAST | 8 F – ÅTERSTÄLLNING |

## DISKUSSIONSANTECKNINGAR FÖR LÄRAREN

**Nyckelbegrepp:**
Kontrollera att eleverna kan förklara KRYPTERING, NYTTOLAST och KALL BACKUP 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

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

## LÖSNING PÅ KORSORDET

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | L | | | | | |
| | | | | | | O | | | Ö | | | | | |
| | | K | | | N | F | | | S | | | | | |
| | | A | | K | Y | F | | | E | | | | | |
| Å | T | E | R | S | T | Ä | L | L | N | I | N | G | | |
| | | A | | Y | T | I | | | S | | | | | |
| | | S | | P | O | N | | | U | | | | T | |
| | | T | | T | L | E | | | M | | | | R | |
| | | R | | E | A | K | | | M | | | | O | |
| | | O | | R | S | O | | | A | | | | J | |
| | | F | | I | T | P | | | | | | | A | |
| | | | | N | | I | S | O | L | E | R | I | N | G |
| | | | | G | | A | | | | | | | | |

## LÄRARHANDLEDNING MED LÖSNINGAR TILL KORSORDET

### VÅGRÄTT

**6 vågrätt: ÅTERSTÄLLNING** Återställning av databasen från säkerhetskopia. (13 bokstäver)

**8 vågrätt: ISOLERING** Frånkoppling av infekterade nätverkssystem. (9 bokstäver)

### LODRÄTT

**1 lodrätt: LÖSENSUMMA** Krav på betalning för en kryptografisk nyckel. (10 bokstäver)

**2 lodrätt: OFFLINEKOPIA** Frånkopplad kopia utan nätverksanslutning. (12 bokstäver)

**3 lodrätt: KATASTROF** Större störning i systemen. (9 bokstäver)

**4 lodrätt: NYTTOLAST** Körning av skadlig programvara. (9 bokstäver)

**5 lodrätt: KRYPTERING** Kryptografisk låsning av filer. (10 bokstäver)

**7 lodrätt: TROJAN** Skadlig fil som utger sig för att vara ren. (6 bokstäver)

# Facit för blandade ord och chiffer

Facit för övningen med ordvärlden och utmaningen Hemliga chiffret.

### FACIT FÖR ORDBLANDNING

1. NRETRKIGPY — **KRYPTERING**
2. AFINOPIFKOEL — **OFFLINEKOPIA**
3. LSMUÖNAEMS — **LÖSENSUMMA**
4. SFOARTKAT — **KATASTROF**
5. AOYTLTNST — **NYTTOLAST**
6. NLSIRIEGO — **ISOLERING**
7. NILTÅTLSGNEÄR — **ÅTERSTÄLLNING**
8. ONTAJR — **TROJAN**

### NYCKEL TILL UTMANINGEN MED HEMLIGT CHIFFER

**"ÅTERSTÄLL KRYPTERAD DATA FRÅN OFFLINEKOPIA"**

# Facit till fallstudierna

## A Fallstudie 1: Begränsa ransomware-nyttolast i företag

Lärarens lösning

### BEDÖMNINGSRIKTLINJE

**Elevernas svar bör täcka följande punkter:**

- Scenarioanalys: Ett lokalt företagsnätverk har drabbats av ett aktivt ransomware-angrepp. Viktiga filservrar har börjat visa filändelsen .locked.
- Rekommenderad strategi och lösning: Koppla bort alla berörda servrar från det lokala nätverket. Avsluta aktiva administrativa sessioner. Återställ ej komprometterade filer från ett säkert, skrivskyddat säkerhetskopieringssystem offline.

## B Fallstudie 2: Utvärdera arkitekturer för offline-backup

Lärarens lösning

### BEDÖMNINGSRIKTLINJE

**Elevernas svar bör täcka följande punkter:**

- Scenarioanalys: Ett företag vill utforma en strategi för säkerhetskopiering som minskar risken att säkerhetskopior kompromitteras även om det primära lokala nätverket helt kapas av ransomware.
- Rekommenderad strategi och lösning: Använd WORM-lagring (write-once-read-many). Skapa ett logiskt luftgap genom att koppla bort backupsystemet från alla nätverk och tillämpa daglig fysisk rotation av lagringsmedier.