Nome: _____ **Data:** _____ **Punteggio:** _____

Attacchi ransomware e continuità aziendale Ripristino

Esecuzione del payload, crittografia dei file, backup offline, procedure di contenimento e disaster recovery.

PANORAMICA DI APPRENDIMENTO: ATTACCHI RANSOMWARE

PROTETTO
CRITTOGRAFIA DEI DATI
Standard AES a 256 bit

CONFORME
STANDARD GLOBALI
Framework GDPR e CCPA

ZERO-TRUST
POLITICA DI ACCESSO
Autenticazione a più fattori

Benvenuto! Questo pacchetto di attività ti guida attraverso gli attacchi ransomware e il ripristino aziendale. Esplorerai l'esecuzione del payload, la crittografia dei file, i backup offline, il contenimento delle minacce, i pagamenti in criptovalute e i piani di disaster recovery.

PUNTI DI CONTROLLO DELLA SCHEDA DI LAVORO

- [ ] **Parti 1-4: Padroneggia la sicurezza informatica e la prevenzione delle minacce.**
- [ ] **Parti 5-7: Risolvi cruciverba e parole nascoste.**
- [ ] **Parti 8-9: Risolvi casi di studio e la sfida del codice.**
- [ ] **Parte 10: Consulta le pagine delle domande frequenti di base e avanzate.**
- [ ] **Parte 11: Esplora 10 fatti interessanti dal mondo reale.**
- [ ] **Bonus: sfida Pensa veloce.**

Apri la guida alla sicurezza informatica di VPN.com

URL: https://www.vpn.com/it/sicurezza-informatica/attacco-ransomware/

Il tuo percorso di apprendimento sul ripristino dopo un ransomware

- Distingui tra payload di trojan, ransomware e spyware.
- Analizza i file dannosi all'interno di ambienti sandbox sicuri.
- Definire procedure rapide di isolamento e contenimento della rete.

ISTRUZIONI DELLA GUIDA SUGLI ATTACCHI RANSOMWARE

Rispondi alle domande a scelta multipla e vero/falso, completa le frasi con gli spazi vuoti usando l'elenco di parole, abbina le definizioni e risolvi il cruciverba e la ricerca di parole. Applica le tue conoscenze al ripristino dopo un attacco ransomware. Concludi con l'attività bonus Pensa veloce.

ATTACCHI RANSOMWARE E RIPRISTINO DI EMERGENZA (INTRODUZIONE)

I payload del ransomware bloccano crittograficamente l'archiviazione del sistema, chiedendo pagamenti in criptovalute in cambio delle chiavi di decifratura. Mitigare questa minaccia comporta regole di isolamento della rete, analisi del malware in sandbox e solidi backup offline air-gapped.

LEGGI CON ATTENZIONE OGNI PUNTO DI CONTROLLO E SELEZIONA O SCRIVI LA RISPOSTA CORRETTA.

Punto di controllo 1: Sfida a scelta multipla

1. Qual è il meccanismo principale di un attacco ransomware?

- A. Cifratura crittografica dei file dell'utente per negare l'accesso al sistema
- B. Inserire comandi SQL dannosi nei campi dei moduli
- C. Intercettare i pacchetti di rete su una connessione Wi-Fi pubblica
- D. Falsificare le intestazioni delle email per aggirare la convalida SPF

2. Che cos'è un backup offline (a freddo)?

- A. Una copia di archiviazione scollegata dalla rete per proteggerla dalla propagazione del malware
- B. Un backup archiviato sul disco rigido del server web principale
- C. Una cache temporanea dei log del registro di sistema
- D. Uno strumento amministrativo usato per reimpostare le password degli utenti

3. Come dovrebbero isolare i team di sicurezza i sistemi infetti durante un attacco ransomware?

- A. Scollegare subito i cavi di rete e disattivare le interfacce wireless
- B. Aggiornare il database delle firme dell'antivirus
- C. Spegnere il server DNS primario
- D. Rinominare le estensioni dei file compromessi

4. Perché le agenzie di sicurezza sconsigliano di pagare le richieste di riscatto dei ransomware?

- A. Pagare incoraggia gli aggressori e non garantisce la consegna della chiave di decifratura
- B. Invalida automaticamente tutte le polizze assicurative aziendali
- C. Avvisa automaticamente ogni cliente via email
- D. Corrompe i restanti file di backup del sistema

5. Che cos'è un piano di ripristino di emergenza (DRP)?

- A. Un processo strutturato per ripristinare le operazioni e i dati dopo la compromissione di un sistema
- B. Una configurazione del firewall che mappa le porte di rete in ingresso
- C. Uno schema di database che elenca i privilegi amministrativi degli utenti
- D. Un protocollo di autenticazione delle email che rifiuta i domini contraffatti

Punto di controllo 2: Sfida Vero o Falso

6 Domanda 6

6. I payload del ransomware possono propagarsi facilmente ai backup online collegati alla rete.

- ◯ Vero
- ◯ Falso

7 Domanda 7

7. Pagare il riscatto in criptovaluta garantisce che i file verranno decifrati con successo.

- ◯ Vero
- ◯ Falso

8 Domanda 8

8. Scollegare i sistemi infetti dalla rete aiuta a impedire che il ransomware si diffonda ai sistemi adiacenti.

- ◯ Vero
- ◯ Falso

9 Domanda 9

9. La crittografia simmetrica non viene mai usata dai ransomware per crittografare l'archiviazione di sistema.

- ◯ Vero
- ◯ Falso

10 Domanda 10

10. Testare regolarmente le procedure di ripristino dei dati è una parte fondamentale del disaster recovery.

- ◯ Vero
- ◯ Falso

Punto di controllo 3: Inserimento dei termini chiave

Leggi ogni frase qui sotto e completa lo spazio vuoto con il termine corretto dell'elenco di parole.

1. Negare l'accesso ai file locali si fa con la _____ crittografica.
2. Il codice dannoso attivo eseguito su un sistema è il _____ .
3. Le copie di archiviazione scollegate e fuori sede sono un sicuro _____ .
4. Impedire la diffusione del malware richiede l' _____ di rete degli endpoint.
5. Il pagamento in criptovaluta richiesto dai criminali informatici è il _____ .
6. Riportare in funzione i file di dati operativi dopo un disastro significa eseguire il _____ .

BANCA DELLE PAROLE DEL VOCABOLARIO

BACKUP OFFLINE CIFRATURA DISASTRO ISOLAMENTO PAYLOAD RIPRISTINO RISCATTO TROJAN

Scrivi qui le tue risposte:

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

Punto di controllo 4: Abbinamento di concetti sulla sicurezza

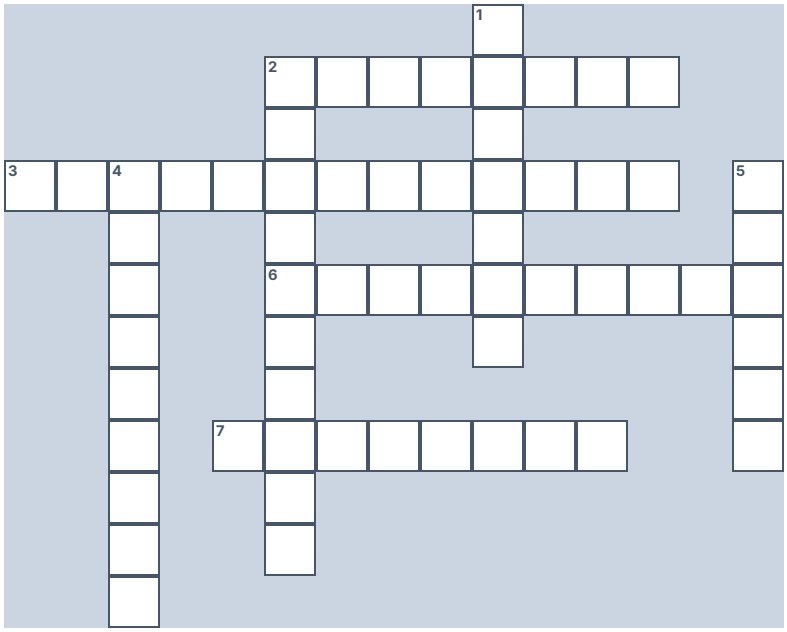
ABBINAMENTO DELLE DEFINIZIONI

Abbina ogni termine del vocabolario a sinistra alla sua definizione corretta a destra scrivendo la lettera corrispondente (A-H) nella casella compilabile.

☐	1. CRITTOGRAFIA	A	Scollegare i sistemi di rete infetti.
☐	2. PAYLOAD	B	File dannoso camuffato da file pulito.
☐	3. BACKUP A FREDDO	C	Bloccare i file con la crittografia.
☐	4. ISOLAMENTO	D	Evento di grave interruzione del sistema.
☐	5. RISCATTO	E	Esecuzione di software dannoso.
☐	6. RIPRISTINO	F	Copia offline scollegata.
☐	7. DISASTRO	G	Ripristino del database dal backup.
☐	8. TROJAN	H	Richiesta di pagamento in chiavi crittografiche.

Punto di controllo 5: Cruciverba

Risolvi il cruciverba digitando le lettere nelle caselle bianche attive. I numeri corrispondono alle definizioni qui sotto.



ORIZZONTALI

2. Richiesta di pagamento per la chiave crittografica. (8)

3. Copia offline scollegata. (13)

6. Scollegamento dei sistemi di rete infetti. (10)

7. Evento di grave interruzione del sistema. (8)

VERTICALI

1. Esecuzione di software dannoso. (7)

2. Recupero del database da un backup. (10)

4. Blocco dei file tramite crittografia. (9)

5. File dannoso camuffato da file innocuo. (6)

Punto di controllo 5, alternativa: Indizi accessibili del cruciverba

Gli utenti di screen reader e di tastiera possono digitare le risposte del cruciverba direttamente nei campi di testo qui sotto.

ORIZZONTALI

2 orizzontale: Richiesta di pagamento per la chiave crittografica. (8 lettere):

3 orizzontale: Copia offline scollegata. (13 lettere):

6 orizzontale: Scollegamento dei sistemi di rete infetti. (10 lettere):

7 orizzontale: Evento di grave interruzione del sistema. (8 lettere):

VERTICALI

1 verticale: Esecuzione di software dannoso. (7 lettere):

2 verticale: Recupero del database da un backup. (10 lettere):

4 verticale: Blocco dei file tramite crittografia. (9 lettere):

5 verticale: File dannoso camuffato da file innocuo. (6 lettere):

Punto di controllo 6: Cerca la parola nascosta

Trova gli 8 termini chiave del vocabolario nascosti nella griglia qui sotto. Le parole possono essere orizzontali, verticali o diagonali.

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

ELENCO DELLE PAROLE DEL VOCABOLARIO

CIFRATURA PAYLOAD BACKUPOFFLINE ISOLAMENTO RISCATTO RIPRISTINO DISASTRO TROJAN

Punto di controllo 6, alternativa: Abbinamento accessibile del vocabolario

Abbina ciascuno degli 8 termini del vocabolario della Ricerca di parole alla sua definizione corretta scrivendo la lettera (A-H) nello spazio vuoto.

TERMINI DEL VOCABOLARIO
A. CIFRATURA
B. PAYLOAD
C. BACKUPOFFLINE
D. ISOLAMENTO
E. RISCATTO
F. RIPRISTINO
G. DISASTRO
H. TROJAN

DEFINIZIONI E CAMPI DI ABBINAMENTO
1. Copia offline scollegata.
2. File dannoso camuffato da file innocuo.
3. Blocco dei file tramite crittografia.
4. Richiesta di pagamento per la chiave crittografica.
5. Scollegamento dei sistemi di rete infetti.
6. Evento di grave interruzione del sistema.
7. Esecuzione di software dannoso.
8. Recupero del database da un backup.

Punto di controllo 7: Sfida delle parole mescolate

Riordina le lettere qui sotto per scoprire concetti e termini chiave della sicurezza informatica. Scrivi le tue risposte nelle caselle fornite.

1. TARICURAF
2. NUAPCBIOEFLFK
3. CIRATOTS
4. AROTSDIS
5. ODLYPAA
6. TALENISMOO
7. IRRTSINOIP
8. ONTAJR

Attività bonus: Pensa veloce

3 RISPOSTE PER CATEGORIA. VINCE CHI COMPLETA PER PRIMO LA LISTA.

1	Informazioni che non dovresti mai condividere			
2	Dispositivi che possono essere hackerati			
3	Motivi per non pagare un riscatto			
4	Buone abitudini sicure che puoi iniziare oggi			
5	Strumenti di sicurezza che conosci			
6	Modi per proteggere i tuoi account			
7	Segnali che indicano che un computer è infetto			
8	Luoghi in cui conservare un backup			
9	File che non vuoi mai perdere			
10	Modi in cui si diffonde il ransomware			
11	Cose da fare nella prima ora di un attacco			
12	Persone da contattare durante un attacco			
13	Cose che un ransomware può bloccare			
14	Parole legate alla sicurezza informatica			
15	Organizzazioni che vengono spesso prese di mira			

Punto di controllo 8: Casi di studio sulla sicurezza informatica

Applica i concetti che hai imparato per risolvere gli scenari reali qui sotto.

CASO DI STUDIO 1: CONTENIMENTO DEL PAYLOAD DI UN RANSOMWARE AZIENDALE

👷

Scenario: La rete locale (LAN) di un'azienda è stata violata da un ransomware attivo. I file server principali hanno iniziato a mostrare file con estensione .locked.

Domanda di discussione: Descrivi nel dettaglio i passaggi di contenimento e illustra il protocollo di recupero dei dati.

CASO DI STUDIO 2: VALUTARE LE ARCHITETTURE DI BACKUP OFFLINE

👷

Scenario: Un'azienda vuole progettare una strategia di backup dei dati che riduca il rischio che i backup possano essere compromessi, anche se la rete locale principale viene completamente dirottata da un ransomware.

Domanda di discussione: progetta un sistema sicuro di caveau per backup offline.

Punto di controllo 9: Decifrare il codice

Un professionista della sicurezza informatica protegge le risorse di rete dagli attori delle minacce online. Usa la chiave lettera-numero qui sotto per decifrare il messaggio scrivendo le lettere corrispondenti negli spazi vuoti.

CHIAVE DI CIFRATURA LETTERA-NUMERO

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

18	9	16	18	9	19	20	9	14	1		9		4	1	20	9
3	9	6	18	1	20	9		4	1		21	14		2	1	3	11	21	16
							15	6	6	12	9	14	5						

Messaggio decifrato:

SUGGERIMENTO: OGNI NUMERO RAPPRESENTA LA POSIZIONE DI QUELLA LETTERA NELL'ALFABETO (AD ES. 1 = A, 2 = B, 26 = Z).

Punto di controllo 10: Domande frequenti di base sulla sicurezza informatica (Parte A)

Rivedi domande e risposte comuni sulla mitigazione delle minacce online.

Q1: Che cos'è il ransomware?

Il ransomware è un software dannoso progettato per bloccare l'accesso a sistemi informatici o file finché non viene pagata una somma di riscatto.

Q2: Come si diffonde il ransomware?

Tramite allegati di email di phishing, vulnerabilità del software non corretto con patch e sistemi di accesso remoto compromessi. [1]

Q3: Perché il pagamento viene richiesto in criptovalute?

Le criptovalute come Bitcoin offrono un anonimato relativo, rendendo difficile per le forze dell'ordine tracciare i fondi.

Q4: L'antivirus blocca il ransomware?

Sì, ma l'antivirus basato sulle firme può fallire contro payload ransomware zero-day di nuova creazione.

Q5: Cos'è un backup air-gapped?

Una copia di backup priva di qualsiasi collegamento fisico o logico con la rete principale, che la protegge dalla propagazione.

Punto di controllo 10: Domande frequenti di base sulla sicurezza informatica (Parte B)

Rivedi domande e risposte comuni sulla mitigazione delle minacce online.

Q6: Cos'è la doppia estorsione?

Quando gli aggressori non solo crittografano i file, ma rubano anche dati sensibili per minacciare fughe di notizie pubbliche se non viene pagato il riscatto.

Q7: Cos'è un decryptor?

Un'utilità software che contiene la chiave crittografica necessaria per ripristinare in chiaro i file bloccati.

Q8: Come si individua precocemente il ransomware?

Monitorando i file system per rilevare improvvise e massicce attività di modifica e ridenominazione dei file.

Q9: Qual è il ruolo dell'assicurazione?

L'assicurazione informatica può aiutare a coprire i costi di ripristino, ma le condizioni di copertura e le regole sul pagamento del riscatto variano a seconda della polizza.

Q10: Devo riavviare un sistema infetto?

No, il riavvio può distruggere le prove nella memoria volatile; isola invece la macchina dalla rete. [1]

Punto di controllo 10: Domande frequenti avanzate sulla sicurezza (Parte C)

Esplora gli aspetti tecnici avanzati dei framework di sicurezza, dell'analisi del malware e della conformità dei dati.

Q1: Come usa il ransomware la crittografia asimmetrica?

Usa una chiave pubblica incorporata nel malware per cifrare i file, richiedendo la chiave privata dell'aggressore per decifrarli.

Q2: Perché si usa anche la cifratura simmetrica?

La crittografia simmetrica (come AES) è veloce e può bloccare enormi database in pochi minuti, mentre le chiavi asimmetriche proteggono la chiave AES.

Q3: Cos'è la segmentazione logica?

Dividere le reti in zone isolate, impedendo al malware di propagarsi lateralmente dalle workstation ai server principali.

Q4: Cos'è lo storage WORM?

Supporti Write-Once, Read-Many (scrivi una volta, leggi molte), che impediscono ai payload dei ransomware di modificare, sovrascrivere o eliminare i dati di backup.

Q5: Cosa sono le copie shadow?

Snapshot di backup locali creati da Windows; il ransomware di solito li elimina per primi usando strumenti amministrativi.

Punto di controllo 10: Domande frequenti avanzate sulla sicurezza (Parte D)

Esplora gli aspetti tecnici avanzati dei framework di sicurezza, dell'analisi del malware e della conformità dei dati.

Q6: Come rende possibile il ransomware il furto di credenziali?

Gli aggressori acquistano credenziali di amministratore trapelate per accedere tramite desktop remoto ed eseguire manualmente il ransomware in tutta la rete.

Q7: Cos'è il test di ripristino in modalità simulata (dry-run)?

Ripristinare regolarmente i database di backup in ambienti di test isolati per verificare che la velocità di ripristino e l'integrità dei dati rispettino le metriche di disaster recovery.

Q8: Come blocca il ransomware il rilevamento sugli endpoint (EDR)?

Analizzando il comportamento dei processi (ad esempio la crittografia rapida) e sospendendo rapidamente l'applicazione anomala.

Q9: Cos'è un modello ransomware-as-a-service (RaaS)?

Un modello in franchising in cui gli sviluppatori di malware concedono in licenza i builder di ransomware agli affiliati in cambio di una percentuale dei pagamenti.

Q10: Come fa un RDP privo di patch a scatenare un ransomware?

I gateway Remote Desktop Protocol esposti e non aggiornati permettono agli aggressori di forzare i login con attacchi brute force e di lanciare manualmente il malware.

Parte 11: 10 fatti e spunti reali sulla sicurezza informatica

Rivedi fatti reali su violazioni della sicurezza, meccanismi di difesa e standard di conformità.

1. APPROFONDIMENTO SULLA SICUREZZA

Gli autori di ransomware usano spesso strumenti come vssadmin.exe per eliminare le copie shadow di Windows e bloccare i ripristini locali. [1]

2. APPROFONDIMENTO SULLA SICUREZZA

Le chiavi simmetriche AES-256 vengono in genere usate per crittografare i payload dei file, che sono poi bloccati con chiavi pubbliche RSA.

3. APPROFONDIMENTO SULLA SICUREZZA

Riprendersi da un attacco ransomware riuscito può richiedere settimane, ed è per questo che i backup offline testati sono importanti.

4. APPROFONDIMENTO SULLA SICUREZZA

L'FBI non sostiene il pagamento di un riscatto e avverte che pagare non garantisce di riavere i dati. [2]

5. APPROFONDIMENTO SULLA SICUREZZA

I piani di disaster recovery (DRP) dovrebbero definire un Recovery Time Objective (RTO) e un Recovery Point Objective (RPO).

6. APPROFONDIMENTO SULLA SICUREZZA

L'FBI raccomanda backup cifrati e immutabili, cioè che non possono essere modificati né eliminati. [3]

7. APPROFONDIMENTO SULLA SICUREZZA

Gli sviluppatori di ransomware usano tecniche di offuscamento avanzate per aggirare gli scanner antivirus tradizionali basati sulle firme.

8. APPROFONDIMENTO SULLA SICUREZZA

La segmentazione della rete limita il movimento laterale, contribuendo a impedire che il ransomware si diffonda oltre il primo host infetto. [3]

9. APPROFONDIMENTO SULLA SICUREZZA

I servizi remoti esposti e poco protetti, come il Remote Desktop Protocol (RDP), sono un punto di ingresso comune del ransomware. [1]

10. APPROFONDIMENTO SULLA SICUREZZA

La CISA consiglia di conservare offline i backup crittografati, perché molte varianti di ransomware cercano ed eliminano i backup raggiungibili. [1]

Riferimenti tecnici e fonti

La guida di studio e i puzzle interattivi sono compilati a partire dagli standard globali NIST, OWASP e di conformità alla privacy dei dati.

RIFERIMENTI ACCADEMICI E DI SETTORE

[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

Soluzioni: Punto di controllo 1 – Scelta multipla

1 Domanda 1

Risposta corretta: A

NOTA DIDATTICA

Qual è il meccanismo principale di un attacco ransomware? → Cifratura crittografica dei file dell'utente per negare l'accesso al sistema

2 Domanda 2

Risposta corretta: A

NOTA DIDATTICA

Che cos'è un backup offline (a freddo)? → Una copia di archiviazione scollegata dalla rete per proteggerla dalla propagazione del malware

3 Domanda 3

Risposta corretta: A

NOTA DIDATTICA

Come dovrebbero isolare i team di sicurezza i sistemi infetti durante un attacco ransomware? → Scollegare subito i cavi di rete e disattivare le interfacce wireless

4 Domanda 4

Risposta corretta: A

NOTA DIDATTICA

Perché le agenzie di sicurezza sconsigliano di pagare le richieste di riscatto dei ransomware? → Pagare incoraggia gli aggressori e non garantisce la consegna della chiave di decifratura

5 Domanda 5

Risposta corretta: A

NOTA DIDATTICA

Che cos'è un piano di ripristino di emergenza (DRP)? → Un processo strutturato per ripristinare le operazioni e i dati dopo la compromissione di un sistema

Soluzioni: Punto di controllo 2 – Vero o falso

6 **Domanda 6** — **Risposta corretta: Vero**

NOTA DIDATTICA

I payload del ransomware possono propagarsi facilmente ai backup online collegati alla rete.

7 **Domanda 7** — **Risposta corretta: Falso**

NOTA DIDATTICA

Falso: l'FBI avverte che pagare non garantisce di riavere alcun dato.

8 **Domanda 8** — **Risposta corretta: Vero**

NOTA DIDATTICA

Vero: la CISA consiglia di scollegare gli host infetti o di mettere la rete offline per contenere la diffusione.

9 **Domanda 9** — **Risposta corretta: Falso**

NOTA DIDATTICA

Falso: il ransomware di solito cifra i file con cifrari simmetrici veloci come AES.

10 **Domanda 10** — **Risposta corretta: Vero**

NOTA DIDATTICA

Testare regolarmente le procedure di ripristino dei dati è una parte fondamentale del disaster recovery.

Chiavi del vocabolario e griglia di valutazione

Griglia di valutazione per l'insegnante: assegna 1 punto per ogni abbinamento corretto (8 punti in totale) e per ogni termine di contesto (6 punti in totale).

PUNTO DI CONTROLLO 4: SOLUZIONI ABBINAMENTO DI CONCETTI

C 1. CRITTOGRAFIA	E 2. PAYLOAD	F 3. BACKUP A FREDDO	A 4. ISOLAMENTO
H 5. RISCATTO	G 6. RIPRISTINO	D 7. DISASTRO	B 8. TROJAN

PUNTO DI CONTROLLO 3: SOLUZIONI TERMINI CHIAVE

1 CIFRATURA	2 PAYLOAD	3 BACKUP OFFLINE	4 ISOLAMENTO
5 RISCATTO	6 RIPRISTINO		

PUNTO DI CONTROLLO 6, ALTERNATIVA: SOLUZIONI ABBINAMENTO DI PAROLE

1 C – BACKUPOFFLINE	2 H – TROJAN	3 A – CIFRATURA	4 E – RISCATTO
5 D – ISOLAMENTO	6 G – DISASTRO	7 B – PAYLOAD	8 F – RIPRISTINO

NOTE DI DISCUSSIONE PER GLI INSEGNANTI

Termini chiave:
Verifica che gli studenti sappiano spiegare CRITTOGRAFIA, PAYLOAD e BACKUP A FREDDO con parole proprie e fare un esempio per ciascuno.

Casi di studio:
Chiedi agli studenti di motivare le loro raccomandazioni con fatti tratti dalla scheda anziché con supposizioni.

Valutazione delle fonti:
Fai verificare almeno un'affermazione con le fonti della scheda e discuti perché cifre, prezzi e regole possono cambiare nel tempo.

Soluzioni dei rompicapi e note per l'insegnante

SOLUZIONE DELLA RICERCA DELLE PAROLE

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

SOLUZIONE DEL CRUCIVERBA

						P								
				R	I	S	C	A	T	T	O			
				I				Y						
B	A	C	K	U	P	O	F	F	L	I	N	E		T
		I			R				O					R
		F			I	S	O	L	A	M	E	N	T	O
		R			S				D					J
		A			T									A
		T		D	I	S	A	S	T	R	O			N
		U			N									
		R			O									
		A												

GUIDA PER L'INSEGNANTE: SOLUZIONI DEL CRUCIVERBA

ORIZZONTALI

2 orizzontale: RISCATTO Richiesta di pagamento per la chiave crittografica. (8 lettere)

3 orizzontale: BACKUPOFFLINE Copia offline scollegata. (13 lettere)

6 orizzontale: ISOLAMENTO Scollegamento dei sistemi di rete infetti. (10 lettere)

7 orizzontale: DISASTRO Evento di grave interruzione del sistema. (8 lettere)

VERTICALI

1 verticale: PAYLOAD Esecuzione di software dannoso. (7 lettere)

2 verticale: RIPRISTINO Recupero del database da un backup. (10 lettere)

4 verticale: CIFRATURA Blocco dei file tramite crittografia. (9 lettere)

5 verticale: TROJAN File dannoso camuffato da file innocuo. (6 lettere)

Soluzioni delle parole mescolate e del codice cifrato

Chiave di valutazione per l'attività di riordino delle parole del vocabolario e per la sfida del codice segreto.

CHIAVE DELLE PAROLE DA RIORDINARE

1. TARICURAF — **CIFRATURA**
2. NUAPCBIOEFLFK — **BACKUPOFFLINE**
3. CIRATOTS — **RISCATTO**
4. AROTSDIS — **DISASTRO**
5. ODLYPAA — **PAYLOAD**
6. TALENISMOO — **ISOLAMENTO**
7. IRRTSINOIP — **RIPRISTINO**
8. ONTAJR — **TROJAN**

CHIAVE DELLA SFIDA DEL CODICE SEGRETO

"RIPRISTINA I DATI CIFRATI DA UN BACKUP OFFLINE"

Soluzioni dei casi di studio

A Caso di studio 1: contenimento del payload di un ransomware aziendale

Soluzione per l'insegnante

LINEA GUIDA DI VALUTAZIONE

Le risposte degli studenti dovrebbero coprire i seguenti punti:

- Analisi dello scenario: una rete locale aziendale è stata violata da un ransomware attivo. I file server principali hanno iniziato a mostrare file con estensione .locked.
- Strategia e soluzione consigliate: scollegare tutti i server interessati dalla rete locale. Terminare le sessioni amministrative attive. Ripristinare i file non compromessi da un sistema di backup offline sicuro con protezione dalla scrittura.

B Caso di studio 2: Valutare le architetture di backup offline

Soluzione per l'insegnante

LINEA GUIDA DI VALUTAZIONE

Le risposte degli studenti dovrebbero coprire i seguenti punti:

- Analisi dello scenario: Un'azienda vuole progettare una strategia di backup dei dati che riduca il rischio di compromissione dei backup anche se la rete locale principale viene completamente sequestrata da un ransomware.
- Strategia e soluzione consigliate: Implementa l'archiviazione write-once-read-many (WORM). Crea un air gap logico scollegando il sistema di backup da tutte le reti e applica una rotazione quotidiana dei supporti fisici.