Nome: _____ Data: _____ Punteggio: _____

Nozioni di base sulla sicurezza informatica e minacce online Prevenzione

Minacce alla sicurezza informatica, firewall di rete, autenticazione a più fattori, framework di sicurezza

PANORAMICA DI APPRENDIMENTO SULLE NOZIONI DI BASE DELLA SICUREZZA INFORMATICA

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 i principi fondamentali della sicurezza informatica di base e della prevenzione delle minacce online. Esplorerai le minacce malware, l'autenticazione a più fattori, i firewall di rete e i framework di risposta agli incidenti.

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/

Il tuo percorso di apprendimento sui fondamenti della sicurezza informatica

- Individua i vettori comuni di malware, phishing e intrusione nelle reti aziendali.
- Implementa controlli standard di sicurezza informatica, tra cui MFA, firewall e difesa degli endpoint.
- Valuta le procedure di risposta agli incidenti per attenuare l'impatto delle violazioni dei dati.
- Analizza i fattori di rischio organizzativi e l'allineamento della sicurezza secondo le linee guida NIST.
- Configura buone pratiche di sicurezza per mitigare il credential stuffing automatizzato.

ISTRUZIONI DELLA GUIDA ALLA SICUREZZA INFORMATICA

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 alla prevenzione delle minacce. Concludi con l'attività bonus Pensa veloce.

NOZIONI DI BASE SULLA SICUREZZA INFORMATICA E PREVENZIONE DELLE MINACCE (INTRODUZIONE)

La sicurezza informatica protegge reti, sistemi e dati da attacchi digitali non autorizzati. Sviluppare solide abitudini di sicurezza, configurare i firewall, richiedere l'autenticazione a più fattori e formare il personale a riconoscere le minacce sono componenti essenziali della difesa della rete aziendale.

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 l'obiettivo principale di un attacco di phishing?

- A. Rubare credenziali e dati sensibili degli utenti
- B. Migliorare la visibilità del sito web sui motori di ricerca
- C. Aumentare la capacità di banda della rete
- D. Gestire la replica del data center di backup

2. Quale meccanismo offre la protezione più forte dell'account?

- A. Autenticazione multifattore con chiavi hardware
- B. Password complesse aggiornate ogni trenta giorni
- C. Limitare l'accesso all'account all'orario di lavoro
- D. Nascondere il nome utente dell'account dalle directory pubbliche

3. Che cosa definisce il payload di un'infezione da ransomware?

- A. Cifrare i file di sistema e chiedere un pagamento
- B. Registrare di nascosto i tasti premuti e inviarli a server remoti
- C. Inserire pubblicità non autorizzata nei browser
- D. Usare le risorse della CPU locale per estrarre criptovaluta

4. Che impatto ha un exploit zero-day sulle difese di sicurezza?

- A. Prende di mira vulnerabilità sconosciute e senza patch
- B. Disattiva automaticamente il firewall aziendale
- C. Costringe il sistema a eseguire un riavvio forzato
- D. Non richiede alcun budget per la risoluzione

5. Quale framework disciplina i controlli di sicurezza aziendali?

- A. Linee guida del NIST Cybersecurity Framework
- B. Specifiche dello schema dei documenti W3C HTML5
- C. Manuali di installazione dei driver della stampante
- D. Definizioni dei protocolli di instradamento IETF

Punto di controllo 2: Sfida Vero o Falso

6 Domanda V/F 6

6. Gli attacchi di phishing prendono di mira solo gli account email personali.

- ◯ Vero
- ◯ Falso

7 Domanda V/F 7

7. L'autenticazione a più fattori aiuta a bloccare gli attacchi di credential stuffing.

- ◯ Vero
- ◯ Falso

8 Domanda V/F 8

8. I firewall ispezionano il traffico di rete per bloccare l'accesso non autorizzato alle porte.

- ◯ Vero
- ◯ Falso

9 Domanda V/F 9

9. La correzione degli exploit zero-day richiede i normali aggiornamenti delle definizioni antivirus.

- ◯ Vero
- ◯ Falso

10 Domanda V/F 10

10. Un honeypot è un server esca usato per attirare i criminali informatici.

- ◯ 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. Gli amministratori di rete installano un _____ per filtrare il traffico in ingresso.

2. Un aggressore usa un _____ zero-day per aggirare le patch di sistema.

3. Gli aggressori inviano email contraffatte per condurre campagne di _____ contro i dipendenti.

4. Il ransomware è una forma distruttiva di _____ che blocca i dati degli utenti.

5. Stabilire una solida _____ delle password riduce i rischi di furto delle credenziali.

6. Per proteggere le comunicazioni sensibili, gli utenti applicano protocolli di _____ .

BANCA DELLE PAROLE DEL VOCABOLARIO

CRITTOGRAFIA EXPLOIT FIREWALL IGIENE MALWARE MULTIFATTORE PHISHING RANSOMWARE

Scrivi qui le tue risposte:

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

Punto di controllo 4: Abbinamento di concetti sulla sicurezza

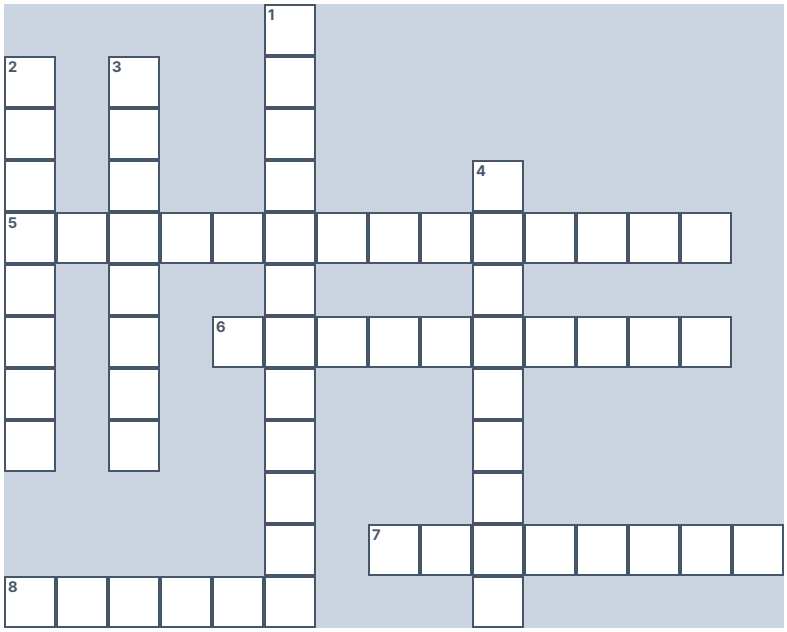
ABBINAMENTO DELLE DEFINIZIONI

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

☐	**1. Minaccia ransomware**	**A**	Linee guida strutturate come quelle del NIST usate per gestire i rischi informatici.
☐	**2. Autenticazione a più fattori**	**B**	Piano strutturato per gestire e mitigare le violazioni della sicurezza.
☐	**3. Exploit zero-day**	**C**	Barriera di rete che filtra il traffico in base alle regole di sicurezza.
☐	**4. Honeypot esca**	**D**	Malware che crittografa i dati e chiede un pagamento in denaro per la decrittazione.
☐	**5. Firewall anti-intrusione**	**E**	Sfruttamento di una vulnerabilità prima del rilascio di una patch da parte del fornitore.
☐	**6. Risposta agli incidenti**	**F**	Buone pratiche per la gestione delle credenziali e delle chiavi di autenticazione.
☐	**7. Igiene delle password**	**G**	Convalida di sicurezza che richiede due o più fattori di autenticazione.
☐	**8. Framework di sicurezza**	**H**	Sistema esca creato per attirare e analizzare gli attori malevoli.

Punto di controllo 5: Cruciverba

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



ORIZZONTALI

5. Exploit di una vulnerabilità sfruttata prima del rilascio della patch del fornitore (14)

6. Malware che cifra i dati e chiede un pagamento in denaro per decifrarli (10)

7. Barriera di rete che filtra il traffico in base a regole di sicurezza (8)

8. Buone pratiche per la gestione di credenziali e chiavi di autenticazione (6)

VERTICALI

1. Convalida di sicurezza che richiede due o più fattori di autenticazione (12)

2. Sistema esca allestito per attirare e analizzare gli attori malevoli (8)

3. Piano strutturato per gestire e mitigare le violazioni della sicurezza (8)

4. Linee guida strutturate come il NIST usate per gestire i rischi informatici (9)

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

5 orizzontale: Exploit di una vulnerabilità sfruttata prima del rilascio della patch del fornitore (14 lettere):

6 orizzontale: Malware che cifra i dati e chiede un pagamento in denaro per decifrarli (10 lettere):

7 orizzontale: Barriera di rete che filtra il traffico in base a regole di sicurezza (8 lettere):

8 orizzontale: Buone pratiche per la gestione di credenziali e chiavi di autenticazione (6 lettere):

VERTICALI

1 verticale: Convalida di sicurezza che richiede due o più fattori di autenticazione (12 lettere):

2 verticale: Sistema esca allestito per attirare e analizzare gli attori malevoli (8 lettere):

3 verticale: Piano strutturato per gestire e mitigare le violazioni della sicurezza (8 lettere):

4 verticale: Linee guida strutturate come il NIST usate per gestire i rischi informatici (9 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.

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

ELENCO DELLE PAROLE DEL VOCABOLARIO

RANSOMWARE MULTIFATTORE EXPLOITZERODAY HONEYPOT FIREWALL
RISPOSTA IGIENE FRAMEWORK

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. RANSOMWARE
B. MULTIFATTORE
C. EXPLOITZERODAY
D. HONEYPOT
E. FIREWALL
F. RISPOSTA
G. IGIENE
H. FRAMEWORK

DEFINIZIONI E CAMPI DI ABBINAMENTO
_____ 1. Barriera di rete che filtra il traffico in base a regole di sicurezza.
_____ 2. Piano strutturato per gestire e mitigare le violazioni della sicurezza.
_____ 3. Malware che cifra i dati e chiede un pagamento in denaro per decifrarli.
_____ 4. Convalida di sicurezza che richiede due o più fattori di autenticazione.
_____ 5. Buone pratiche per la gestione di credenziali e chiavi di autenticazione.
_____ 6. Linee guida strutturate come il NIST usate per gestire i rischi informatici.
_____ 7. Exploit di una vulnerabilità sfruttata prima del rilascio della patch del fornitore.
_____ 8. Sistema esca allestito per attirare e analizzare gli attori malevoli.

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. RWMOARAESN
2. OXIPTAEDZY ROEL
3. EIFWALLR
4. EEINIG
5. UOTAELITFM RT
6. OTEPHYON
7. RAOSTIPS
8. KERFMRWOA

Attività bonus: Pensa veloce

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

1	Lavori nella sicurezza informatica			
2	Motivi per aggiornare il software			
3	Cose che un firewall può bloccare			
4	Segnali di allarme in un'email			
5	Cose di cui fai il backup			
6	Tipi di attacco informatico più noti			
7	Cose che un honeypot può attirare			
8	Informazioni che non dovresti mai condividere			
9	Segnali che indicano che un computer è infetto			
10	Film o serie sugli hacker			
11	Livelli di sicurezza che puoi costruire			
12	Cose da esercitare in un'esercitazione di sicurezza			
13	Strumenti di sicurezza che conosci			
14	Persone a cui puoi chiedere aiuto per l'IT			
15	Parole che iniziano con 'cyber'			

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: STRATEGIA DI RIPRISTINO DA RANSOMWARE

👷

Scenario: Una rete aziendale è infettata da ransomware, che blocca database critici. Gli aggressori chiedono un pagamento di 100.000 $ in criptovaluta. L'azienda ha backup offline di 24 ore prima.

Domanda di discussione: analizza i rischi del pagamento e valuta la strategia di ripristino.

CASO DI STUDIO 2: DIFESE CONTRO IL CREDENTIAL STUFFING

👷

Scenario: Un servizio online subisce un attacco di credential stuffing, con hacker che provano milioni di coppie di nome utente e password rubate da altri siti.

Domanda di discussione: Descrivi nel dettaglio il meccanismo di questo attacco e illustra due sistemi di difesa.

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

16	18	15	20	5	7	7	9		9	12		19	9	19	20	5	13	1
3	**15**	**14**		**9**	**12**		**13**	**21**	**12**	**20**	**9**	**6**	**1**	**20**	**20**	**15**	**18**	**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: Qual è l'obiettivo principale della sicurezza informatica?

L'obiettivo principale è proteggere reti, dispositivi e dati da accessi non autorizzati, attacchi e danni accidentali.

Q2: In che cosa il phishing differisce dallo spear phishing?

Il phishing è una campagna email ad ampio raggio che colpisce utenti a caso, mentre lo spear phishing colpisce persone specifiche usando dati personalizzati.

Q3: Cos'è un firewall di rete?

Un firewall è un sistema di sicurezza di rete che monitora e filtra il traffico in entrata e in uscita in base a regole di sicurezza predefinite.

Q4: Perché l'autenticazione a più fattori (MFA) è necessaria?

L'MFA aggiunge un livello di difesa fondamentale, impedendo l'accesso anche se gli attaccanti rubano o violano le credenziali della password principale.

Q5: Cosa definisce un virus informatico?

Un virus è un malware autoreplicante che si attacca a file sicuri e si diffonde tra i sistemi una volta eseguito.

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

Rivedi domande e risposte comuni sulla mitigazione delle minacce online.

Q6: Come blocca i dati locali il ransomware?

Il ransomware usa algoritmi crittografici per cifrare i file degli utenti, rendendoli illeggibili finché non viene applicata una chiave di decifratura.

Q7: Cos'è una vulnerabilità zero-day?

Uno zero-day è una falla di sicurezza in un software sconosciuta al produttore, che non lascia tempo per sviluppare una patch prima dello sfruttamento.

Q8: Qual è il ruolo del framework NIST?

Il framework NIST fornisce linee guida e standard volontari per aiutare le organizzazioni a gestire e ridurre i rischi per la sicurezza informatica.

Q9: Cos'è un piano di risposta agli incidenti di sicurezza?

È un insieme documentato di procedure per rilevare, contenere e ripristinare dopo violazioni della sicurezza e compromissioni della rete.

Q10: Come sfrutta l'ingegneria sociale gli utenti?

L'ingegneria sociale usa la manipolazione psicologica per indurre i dipendenti a rivelare password o a scaricare file dannosi.

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 sovraccarica i server web un attacco DDoS?

Un attacco DDoS coordina milioni di dispositivi botnet compromessi per inondare un server di traffico, esaurendo i limiti di banda e di CPU.

Q2: Qual è la differenza tra crittografia simmetrica e asimmetrica?

La crittografia simmetrica usa una sola chiave per cifrare e decifrare, mentre la crittografia asimmetrica usa una coppia di chiavi pubblica e privata.

Q3: Come eseguono gli hacker gli attacchi di SQL injection?

Gli aggressori inseriscono comandi SQL dannosi nei campi dei moduli, inducendo il database di backend a rilasciare record utente non autorizzati.

Q4: Cos'è il movimento laterale nelle intrusioni di rete?

È la tecnica con cui gli aggressori sfruttano l'accesso iniziale a un server per compromettere altri sistemi interconnessi sulla rete interna.

Q5: Come reindirizza il traffico web lo spoofing DNS?

Lo spoofing DNS altera i record nella cache dei nameserver, indirizzando gli utenti legittimi verso siti malevoli identici anziché verso i domini di destinazione.

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: Cos'è un token di sicurezza hardware?

È un dispositivo fisico (come una YubiKey) che genera prove di autenticazione crittografiche, offrendo la massima difesa contro il phishing da remoto.

Q7: Come usano i team di sicurezza gli honeypot esca?

I team installano server esca non di produzione per rilevare tempestivamente le intrusioni e analizzare i modelli di attacco degli attori non autorizzati.

Q8: Qual è il principio del privilegio minimo?

È lo standard di sicurezza che limita i diritti di accesso degli utenti al minimo assoluto necessario per svolgere i propri ruoli lavorativi.

Q9: Come sfrutta le connessioni un attacco Man-in-the-Middle?

Un aggressore intercetta e altera le comunicazioni tra due dispositivi su reti non cifrate, rubando token di sessione e credenziali.

Q10: Che cosa sono gli indicatori di compromissione (IOC)?

Gli IOC sono indizi forensi, come modifiche insolite al registro di sistema o traffico IP anomalo, che mostrano che un sistema è stato violato.

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 aggressori scansionano continuamente Internet alla ricerca di server vulnerabili e inviano email di phishing alle caselle di posta dei dipendenti.

2. APPROFONDIMENTO SULLA SICUREZZA

L'errore umano, come fare clic su link di phishing, è un fattore comune nelle violazioni dei dati, ed è per questo che la formazione è importante.

3. APPROFONDIMENTO SULLA SICUREZZA

I costi di una violazione dei dati comprendono sanzioni legali, perdita di clienti, indagini e ripristino, e possono raggiungere milioni di dollari.

4. APPROFONDIMENTO SULLA SICUREZZA

L'MFA resistente al phishing, come le chiavi di sicurezza hardware, è il tipo di MFA più forte e lo standard raccomandato con insistenza dalla CISA. [2]

5. APPROFONDIMENTO SULLA SICUREZZA

Il ransomware resta una grave minaccia per le reti aziendali, e la CISA raccomanda backup offline e cifrati come difesa fondamentale. [4]

6. APPROFONDIMENTO SULLA SICUREZZA

Il NIST Cybersecurity Framework 2.0 (2024) ha sei funzioni principali: Govern, Identify, Protect, Detect, Respond, Recover. [1]

7. APPROFONDIMENTO SULLA SICUREZZA

I bot di credential stuffing provano su larga scala coppie di nome utente e password trapelate sui portali di accesso di banche e siti di e-commerce.

8. APPROFONDIMENTO SULLA SICUREZZA

Esistono mercati di exploit zero-day in tutto il mondo, dove le vulnerabilità di alta gravità possono essere vendute a cifre elevate prima di essere corrette.

9. APPROFONDIMENTO SULLA SICUREZZA

Un sistema esca honeypot segnala immediatamente gli avvisi di intrusione, perché gli utenti legittimi non hanno motivo di accedervi.

10. APPROFONDIMENTO SULLA SICUREZZA

Il Transport Layer Security (TLS) cifra le sessioni del browser, impedendo lo sniffing dei pacchetti sulle reti Wi-Fi pubbliche.

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] NIST. (2024). The NIST Cybersecurity Framework (CSF) 2.0.
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

[2] CISA. (n.d.). More than a Password.
https://www.cisa.gov/MFA

[3] 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

[4] CISA. (2023). #StopRansomware Guide.
https://www.cisa.gov/stopransomware/ransomware-guide

[5] CISA. (n.d.). Malware, Phishing, and Ransomware.
https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

[6] NIST. (2025). SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile.
https://csrc.nist.gov/pubs/sp/800/61/r3/final

[7] NIST. (2025). SP 800-63B-4: Digital Identity Guidelines: Authentication and Authenticator Management.
https://pages.nist.gov/800-63-4/sp800-63b.html

[8] OWASP. (n.d.). SQL Injection.
https://owasp.org/www-community/attacks/SQL_Injection

Soluzioni: Punto di controllo 1 – Scelta multipla

1 **Attacchi di phishing** PHISHING — **Risposta corretta: A**

NOTA DIDATTICA

Le campagne di phishing cercano di rubare credenziali e dati sensibili degli utenti usando email falsificate. Fonte: OWASP Secure Configuration.

2 **Protezione dell'account** CHIAVE MFA — **Risposta corretta: A**

NOTA DIDATTICA

L'autenticazione a più fattori (MFA) con token hardware offre la difesa più solida per l'accesso agli account. Citazione: NIST Digital Identity.

3 **Minaccia ransomware** RANSOMWARE — **Risposta corretta: A**

NOTA DIDATTICA

Il ransomware cifra sistemi e dati critici, chiedendo un pagamento in criptovalute in cambio delle chiavi di decifratura. Citazione: Center for Internet Security (CIS) [Rif. 8].

4 **Vulnerabilità zero-day** ZERO-DAY — **Risposta corretta: A**

NOTA DIDATTICA

Le minacce zero-day sfruttano falle di sicurezza sconosciute e non corrette prima che il fornitore renda disponibile una patch. Citazione: OWASP Secure Configuration.

5 **Framework di sicurezza** FRAMEWORK — **Risposta corretta: A**

NOTA DIDATTICA

Framework come NIST forniscono linee guida strutturate che aiutano le organizzazioni a gestire e ridurre i rischi informatici. Citazione: NIST Digital Identity.

Soluzioni: Punto di controllo 2 – Vero o falso

6 **Phishing mirato** PHISHING — **Risposta corretta: Falso**

NOTA DIDATTICA

Gli attacchi di phishing prendono di mira sia le reti aziendali sia gli account personali per ampliare i vettori di attacco. Fonte: OWASP Secure Configuration.

7 **Domanda 7** — **Risposta corretta: Vero**

NOTA DIDATTICA

L'MFA richiede un secondo fattore, quindi una password rubata da sola di solito non basta per accedere.

8 **Firewall del traffico** FIREWALL — **Risposta corretta: Vero**

NOTA DIDATTICA

I firewall ispezionano e bloccano il traffico su specifiche porte di rete per filtrare le connessioni non autorizzate. Citazione: Center for Internet Security (CIS).

9 **Risposta agli zero-day** ZERO-DAY — **Risposta corretta: Falso**

NOTA DIDATTICA

Correggere le falle zero-day richiede patch del codice e filtraggio WAF, poiché non esistono ancora firme. Citazione: OWASP Secure Configuration.

10 **Honeypot esca** HONEYPOT — **Risposta corretta: Vero**

NOTA DIDATTICA

Gli honeypot sono server ingannevoli usati dai team di sicurezza per attirare, segnalare e studiare gli autori di attività dannose. Citazione: Center for Internet Security (CIS).

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

D 1. Minaccia ransomware	G 2. Autenticazione a più fattori	E 3. Exploit zero-day	H 4. Honeypot esca
C 5. Firewall anti-intrusione	B 6. Risposta agli incidenti	F 7. Igiene delle password	A 8. Framework di sicurezza

PUNTO DI CONTROLLO 3: SOLUZIONI TERMINI CHIAVE

1 FIREWALL	2 EXPLOIT	3 PHISHING	4 MALWARE
5 IGIENE	6 CRITTOGRAFIA		

PUNTO DI CONTROLLO 6, ALTERNATIVA: SOLUZIONI ABBINAMENTO DI PAROLE

1 E – FIREWALL	2 F – RISPOSTA	3 A – RANSOMWARE	4 B – MULTIFATTORE
5 G – IGIENE	6 H – FRAMEWORK	7 C – EXPLOITZERODAY	8 D – HONEYPOT

NOTE DI DISCUSSIONE PER GLI INSEGNANTI

Termini chiave:
Verifica che gli studenti sappiano spiegare Minaccia ransomware, Autenticazione a più fattori e Exploit zero-day 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.

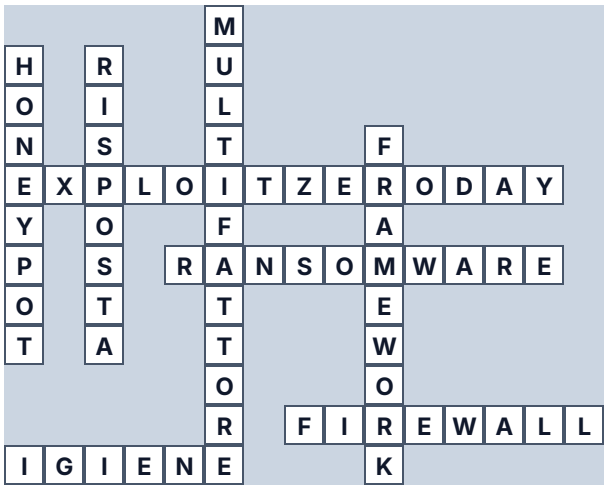
Valutazione delle fonti:
Fai verificare almeno un'affermazione con le fonti della scheda e discuti perché cifre, prezzi e regole possono cambiare nel tempo.

Soluzioni dei rompicapi e note per l'insegnante

SOLUZIONE DELLA RICERCA DELLE PAROLE

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

SOLUZIONE DEL CRUCIVERBA



GUIDA PER L'INSEGNANTE: SOLUZIONI DEL CRUCIVERBA

ORIZZONTALI

5 orizzontale: EXPLOITZERODAY Exploit di una vulnerabilità sfruttata prima del rilascio della patch del fornitore (14 lettere)

6 orizzontale: RANSOMWARE Malware che cifra i dati e chiede un pagamento in denaro per decifrarli (10 lettere)

7 orizzontale: FIREWALL Barriera di rete che filtra il traffico in base a regole di sicurezza (8 lettere)

8 orizzontale: IGIENE Buone pratiche per la gestione di credenziali e chiavi di autenticazione (6 lettere)

VERTICALI

1 verticale: MULTIFATTORE Convalida di sicurezza che richiede due o più fattori di autenticazione (12 lettere)

2 verticale: HONEYPOT Sistema esca allestito per attirare e analizzare gli attori malevoli (8 lettere)

3 verticale: RISPOSTA Piano strutturato per gestire e mitigare le violazioni della sicurezza (8 lettere)

4 verticale: FRAMEWORK Linee guida strutturate come il NIST usate per gestire i rischi informatici (9 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. R W M O A R A E S N — **RANSOMWARE**
2. O X I P T A E D Z Y R O E L — **EXPLOITZERODAY**
3. E I F W A L L R — **FIREWALL**
4. E E I N I G — **IGIENE**
5. U O T A E L I T F M R T — **MULTIFATTORE**
6. O T E P H Y O N — **HONEYPOT**
7. R A O S T I P S — **RISPOSTA**
8. K E R F M R W O A — **FRAMEWORK**

CHIAVE DELLA SFIDA DEL CODICE SEGRETO

"PROTEGGI IL SISTEMA CON IL MULTIFATTORE"

Soluzioni dei casi di studio

A Caso di studio 1: strategia di ripristino da ransomware

Soluzione per l'insegnante

LINEA GUIDA DI VALUTAZIONE

Le risposte degli studenti dovrebbero coprire i seguenti punti:

- Analisi dello scenario: una rete aziendale è infettata da un ransomware che blocca database critici. Gli aggressori chiedono un riscatto di 100.000 $ in criptovaluta. L'azienda ha backup offline di 24 ore prima.
- Strategia e soluzione consigliate: Rischi del pagamento: pagare non garantisce la decifrazione dei file, etichetta l'azienda come bersaglio disposto a pagare e finanzia attività criminali. Strategia di recupero: il team dovrebbe isolare gli host infetti, ripulire i server compromessi e ripristinare i dati dai backup offline. Deve correggere il vettore di accesso iniziale (phishing o exploit) per evitare una reinfezione immediata.

B Caso di studio 2: Difese contro il credential stuffing

Soluzione per l'insegnante

LINEA GUIDA DI VALUTAZIONE

Le risposte degli studenti dovrebbero coprire i seguenti punti:

- Analisi dello scenario: Un servizio online subisce un attacco di credential stuffing, con hacker che provano milioni di coppie nome utente/password sottratte ad altri siti.
- Strategia e soluzione consigliate: Meccanismo: gli aggressori sfruttano il riutilizzo delle password su più siti usando bot automatizzati per accedere agli account degli utenti. Difese: 1. L'autenticazione a più fattori (MFA) blocca i tentativi di accesso anche se la password è corretta. 2. L'implementazione di limiti di frequenza e CAPTCHA blocca il traffico dei bot automatizzati che inondano gli endpoint di accesso.