नाम: _____ दिनांक: _____ अंक: _____

डेटा सुरक्षा और एंटरप्राइज़ स्टोरेज सुरक्षा गाइड

डेटा मास्किंग, टोकनाइज़ेशन, एट-रेस्ट बनाम इन-ट्रांज़िट एन्क्रिप्शन, ऑफ़लाइन बैकअप

डेटा सुरक्षा सीखने का अवलोकन

सुरक्षित किया गया
डेटा एन्क्रिप्शन
256-बिट AES मानक

अनुपालक
वैश्विक मानक
GDPR और CCPA फ़्रेमवर्क

ज़ीरो-ट्रस्ट
एक्सेस नीति
मल्टी-फ़ैक्टर ऑथेंटिकेशन

स्वागत है! यह गतिविधि पैकेट आपको डेटा सुरक्षा मानकों और नियंत्रणों से परिचित कराता है। आप फ़ुल-डिस्क एन्क्रिप्शन, सुरक्षित एक्सेस नियंत्रण, हार्डवेयर बैकअप, क्लाउड सुरक्षा स्थिति और डेटा मास्किंग तकनीकों का अध्ययन करेंगे।

वर्कशीट चेकपॉइंट

- [ ] **भाग 1-4: साइबर सुरक्षा और खतरों की रोकथाम में महारत हासिल करें।**
- [ ] **भाग 5-7: क्रॉसवर्ड और वर्ड सर्च पहेलियाँ हल करें।**
- [ ] **भाग 8-9: केस स्टडी और कूट संदेश की चुनौती हल करें।**
- [ ] **भाग 10: बुनियादी और उन्नत FAQ पेज देखें।**
- [ ] **भाग 11: 10 रोचक वास्तविक तथ्यों को जानें।**
- [ ] **अतिरिक्त: झटपट सोचें चुनौती।**

VPN.com साइबर सुरक्षा गाइड खोलें

URL: https://www.vpn.com/hi/saibhar-suraksha/data-suraksha/

आपका डेटा सुरक्षा रणनीति लर्निंग रोडमैप

- डेटा मास्किंग और टोकनाइज़ेशन तकनीकों में अंतर करें।
- स्टोरेज ड्राइव के लिए एन्क्रिप्शन-एट-रेस्ट और TLS का उपयोग करके एन्क्रिप्शन-इन-ट्रांज़िट लागू करें।
- रैनसमवेयर से सुरक्षा के लिए ऑफ़लाइन, नेटवर्क से अलग बैकअप सिस्टम तैयार करें।

डेटा सुरक्षा गाइड के निर्देश

बहुविकल्पीय और सही/गलत प्रश्नों के उत्तर दें, शब्द बैंक की मदद से रिक्त स्थान भरें, परिभाषाओं का मिलान करें, और क्रॉसवर्ड तथा वर्ड सर्च पहेलियाँ हल करें। अपने ज्ञान को डेटा सुरक्षा पर लागू करें। अंत में अतिरिक्त गतिविधि झटपट सोचें पूरी करें।

डेटा सुरक्षा और एंटरप्राइज़ स्टोरेज सुरक्षा (परिचय)

डेटा सुरक्षा मास्किंग, टोकनाइज़ेशन, एट-रेस्ट डेटाबेस एन्क्रिप्शन और सुरक्षित ट्रांज़िट प्रोटोकॉल के ज़रिए कॉर्पोरेट डेटा संपत्तियों की रक्षा करती है। नेटवर्क से अलग रखे गए बैकअप बनाने से यह सुनिश्चित करने में मदद मिलती है कि सक्रिय घुसपैठ की स्थिति में भी प्रमुख डेटाबेस बहाल किए जा सकें।

प्रत्येक चेकपॉइंट को ध्यान से पढ़ें और सही उत्तर चुनें या लिखें।

चेकपॉइंट 1: बहुविकल्पीय चुनौती

1 **1. डेटा मास्किंग का मुख्य उद्देश्य क्या है?**

- A. गोपनीयता की रक्षा के लिए संवेदनशील पहचानकर्ताओं को काल्पनिक लेकिन यथार्थवादी वर्णों से बदलना
- B. भौतिक सर्वर स्टोरेज बचाने के लिए बड़ी डेटाबेस फ़ाइलों को कंप्रेस करना
- C. आर्काइव बैकअप सिस्टम से पुराने ग्राहक संपर्क ईमेल मिटाना
- D. डेटाबेस सर्वर के सार्वजनिक IP पते को इंटरनेट स्कैन से छिपाना

2 **2. कौन-सा तंत्र डेटाबेस सर्वर की हार्ड ड्राइव पर संग्रहीत फ़ाइलों को एन्क्रिप्ट करता है?**

- A. स्टोरेज में फ़ुल-डिस्क एन्क्रिप्शन
- B. ट्रांज़िट में TLS सेशन हैंडशेक प्रोटोकॉल
- C. डायनेमिक DNS नेमसर्वर फ़ॉरवर्डिंग नियम
- D. हार्डवेयर कुंजियों का उपयोग करके बहु-कारक प्रमाणीकरण

3 **3. ट्रांज़िट में डेटा क्या दर्शाता है?**

- A. नेटवर्क राउटर और स्विच के पार जाते डेटा पैकेट
- B. कोल्ड बैकअप ड्राइव पर रखे गए डेटाबेस लेन-देन लॉग
- C. अलग-थलग क्लाउड वॉल्ट में सहेजी गई संग्रहीत उपयोगकर्ता फ़ाइलें
- D. लोकल डेस्कटॉप स्टोरेज पर स्थिर सिस्टम कॉन्फ़िगरेशन फ़ाइलें

4 **4. रैनसमवेयर से सुरक्षा के लिए नियमित ऑफ़लाइन बैकअप क्यों महत्वपूर्ण है?**

- A. यह फिरौती दिए बिना फ़ाइलें बहाल करने के लिए साफ़, ऑफ़लाइन कॉपी देता है
- B. यह हैकरों को खुले पोर्ट कॉन्फ़िगरेशन स्कैन करने से रोकता है
- C. यह स्थानीय नेटवर्क ट्रांसमिशन बैंडविड्थ की गति बढ़ाता है
- D. यह ब्राउज़र पर कुकी सहमति के ऑप्ट-इन लॉग स्वचालित करता है

5 **5. डेटा टोकनाइज़ेशन क्या करता है?**

- A. यह संवेदनशील कार्ड नंबरों को गैर-संवेदनशील यादृच्छिक टोकन से बदल देता है
- B. यह वेब ट्रैफ़िक को कई सुरक्षित onion नोड से गुज़ारता है
- C. यह सिग्नेचर-आधारित मैलवेयर के लिए सिस्टम डायरेक्टरी स्कैन करता है
- D. यह डेटाबेस एडमिनिस्ट्रेटर के लॉगिन सत्र समय का ऑडिट करता है

चेकपॉइंट 2: सही या गलत चुनौती

6 प्रश्न 6

6. डेटा मास्किंग प्रोडक्शन वातावरण में डेटाबेस रिकॉर्ड को स्थायी रूप से बदल देती है।

○ सही ○ गलत

7 प्रश्न 7

7. रैंसमवेयर के प्रसार को रोकने के लिए ऑफ़साइट बैकअप को मुख्य कॉर्पोरेट नेटवर्क से अलग रखना चाहिए।

○ सही ○ गलत

8 प्रश्न 8

8. SSL/TLS सर्टिफ़िकेट भौतिक मीडिया पर सहेजे गए डेटा (एट रेस्ट) को एन्क्रिप्ट करके डेटाबेस को सुरक्षित करते हैं।

○ सही ○ गलत

9 प्रश्न 9

9. ज़ीरो-ट्रस्ट नेटवर्क एक्सेस (ZTNA) डेटाबेस पहुँच देने से पहले हर उपयोगकर्ता की पहचान सत्यापित करता है।

○ सही ○ गलत

10 प्रश्न 10

10. वॉल्ट-आधारित टोकनाइज़ेशन मूल कार्ड मानों को एक सुरक्षित, केंद्रीय टोकन वॉल्ट में स्टोर करता है।

○ सही ○ गलत

चेकपॉइंट 3: मुख्य शब्द भरें

नीचे दिए गए प्रत्येक वाक्य को पढ़ें और रिक्त स्थान को वर्ड बैंक के सही शब्द से भरें।

1. ज़रूरत से ज़्यादा व्यक्तिगत जानकारी न जुटाना डेटा सुरक्षा के लिए _____ का सिद्धांत है।

2. भौतिक स्टोरेज ब्लॉक को एन्क्रिप्ट करने से डेटाबेस संपत्तियां _____ सुरक्षित रहती हैं।

3. TLS जैसे प्रोटोकॉल डेटा को एक _____ से भेजते समय पैकेट एन्क्रिप्ट करते हैं।

4. भूमिका-आधारित अनुमतियां तय करने वाली संगठन की _____ बताती है कि डेटाबेस तक कौन पहुंच सकता है।

5. उल्लंघन के बाद साफ़ कॉर्पोरेट फ़ाइलें बहाल करने के लिए सुरक्षित ऑफ़लाइन _____ चाहिए।

6. क्लाउड कॉन्फ़िगरेशन की ऑडिटिंग से किसी संगठन की सुरक्षा _____ का आकलन होता है।

शब्दावली शब्द-बैंक

उल्लंघन | डेटा न्यूनीकरण | बैकअप | मास्किंग | सुरक्षा नीति | सुरक्षा स्थिति | सुरक्षित नेटवर्क | स्थिर अवस्था में

अपने उत्तर यहाँ लिखें:

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

चेकपॉइंट 4: सुरक्षा अवधारणा मिलान

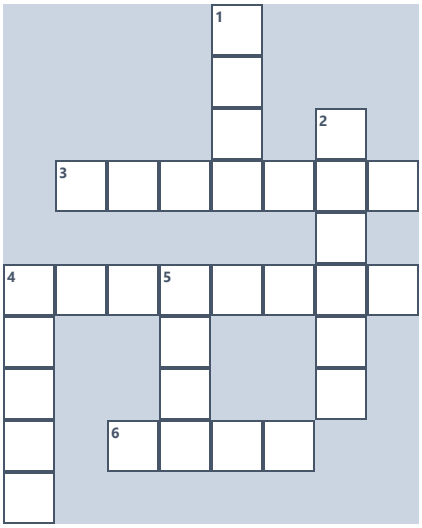
परिभाषा मिलान

बाईं ओर के प्रत्येक शब्दावली पद को दाईं ओर की सही परिभाषा से मिलाएँ; भरने योग्य इनपुट बॉक्स में संबंधित अक्षर (A-H) लिखें।

☐	**1. एन्क्रिप्शन**	**A**	सिस्टम विफलता की स्थिति में बहाल करने के लिए डेटा की सुरक्षित ऑफ़साइट प्रतियाँ बनाना।
☐	**2. बैकअप**	**B**	प्लेनटेक्स्ट को अपठनीय सिफ़रटेक्स्ट में बदलना ताकि बीच में पकड़ा गया डेटा निजी रहे।
☐	**3. न्यूनीकरण**	**C**	किसी संगठन के क्लाउड की समग्र सुरक्षा स्थिति और बचाव की तैयारी।
☐	**4. एक्सेस**	**D**	निजी उपयोगकर्ता जानकारी के प्रबंधन के लिए GDPR या CCPA जैसे नियामक मानकों का पालन करना।
☐	**5. पॉश्चर**	**E**	ऐसी सुरक्षा घटना जिसमें सुरक्षित डेटा तक बिना अनुमति पहुँच बनती है या उसे उजागर किया जाता है।
☐	**6. उल्लंघन**	**F**	डेटाबेस की रीड और राइट अनुमतियाँ प्रमाणित उपयोगकर्ता भूमिकाओं तक सीमित करना।
☐	**7. अनुपालन**	**G**	व्यक्तिगत पहचान की रक्षा के लिए डेटाबेस फ़ील्ड के संवेदनशील अक्षरों को बदलना।
☐	**8. मास्किंग**	**H**	व्यक्तिगत डेटा संग्रह को संचालन के लिए ज़रूरी न्यूनतम स्तर तक सीमित रखना।

चेकपॉइंट 5: क्रॉसवर्ड पहेली

सक्रिय सफ़ेद खानों में अक्षर टाइप करके क्रॉसवर्ड पहेली हल करें। संख्याएँ नीचे दिए गए संकेतों से मेल खाती हैं।



बाएँ से दाएँ

3. संचालन के लिए ज़रूरी न्यूनतम सीमा तक ही निजी डेटा संग्रह सीमित करना (7)

4. ऐसा कनेक्शन, जिसमें भेजा गया डेटा बाहरी लोगों से सुरक्षित रहता है (8)

6. सिस्टम विफलता की स्थिति में बहाल करने के लिए डेटा की सुरक्षित ऑफ़साइट प्रतियां बनाना (4)

ऊपर से नीचे

1. संदिग्ध गतिविधियों पर लगातार नज़र रखना (4)

2. डेटा की वह दशा, जब वह स्टोरेज में रखा हो और कहीं भेजा न जा रहा हो (6)

4. सुरक्षा के नियमों और कदमों का लिखित ढांचा (5)

5. किसी काम को कुशलता से करने की वैज्ञानिक विधि और औज़ार (4)

चेकपॉइंट 5, वैकल्पिक: सुलभ क्रॉसवर्ड संकेत

स्क्रीन-रीडर और कीबोर्ड उपयोगकर्ता क्रॉसवर्ड के उत्तर सीधे नीचे दिए गए टेक्स्ट फ़ील्ड में टाइप कर सकते हैं।

बाएँ से दाएँ

3 बाएँ से दाएँ: संचालन के लिए ज़रूरी न्यूनतम सीमा तक ही निजी डेटा संग्रह सीमित करना (7 अक्षर):

4 बाएँ से दाएँ: ऐसा कनेक्शन, जिसमें भेजा गया डेटा बाहरी लोगों से सुरक्षित रहता है (8 अक्षर):

6 बाएँ से दाएँ: सिस्टम विफलता की स्थिति में बहाल करने के लिए डेटा की सुरक्षित ऑफ़साइट प्रतियां बनाना (4 अक्षर):

ऊपर से नीचे

1 ऊपर से नीचे: संदिग्ध गतिविधियों पर लगातार नज़र रखना (4 अक्षर):

2 ऊपर से नीचे: डेटा की वह दशा, जब वह स्टोरेज में रखा हो और कहीं भेजा न जा रहा हो (6 अक्षर):

4 ऊपर से नीचे: सुरक्षा के नियमों और कदमों का लिखित ढांचा (5 अक्षर):

5 ऊपर से नीचे: किसी काम को कुशलता से करने की वैज्ञानिक विधि और औज़ार (4 अक्षर):

चेकपॉइंट 6: छिपे शब्द खोजें

नीचे दी गई ग्रिड में छिपे 8 प्रमुख शब्दावली शब्द खोजें। शब्द क्षैतिज, ऊर्ध्वाधर या तिरछे हो सकते हैं।

द	में	प	ति	के	ट	मि	नि	ट	सा	य	च	ऊ	नी	जी
इ	स्था	त	म	पे	ब	प	ग	सु	जि	मी	ने	ले	इ	सी
य	व	छ	र	दे	कि	जा	रा	सा	र	वा	ड	रे	स	ख
नि	अ	फ	ढ	मा	ना	का	नी	रे	दे	क्षा	सि	मी	क	पि
ता	र	ति	ज	श	सु	भ	ऊ	अ	ऊ	ए	स्थि	रि	बै	वि
श	स्थि	य	वि	व	र	वा	डे	पा	ल	च	से	ति	क	कि
क	नी	क	त	य	क्षि	घ	प	टा	के	की	व	सि	अ	री
ति	त	की	कि	सि	त	ना	ने	पा	न्यू	ते	ण	ए	प	ता
नी	सा	मी	न	नी	ने	ऋ	ले	घ	ति	नी	जि	ला	ए	जी
क्षा	ले	ड	ल	द	ट	जे	घ	के	च	से	क	दे	री	ए
र	पी	उ	अ	जे	व	मि	घ	व	आ	च	मी	र	च	ट
सु	थ	फ	ग	ना	र्क	सी	का	ज	फ	नी	जी	ता	ण	ठ
से	लि	ट	आ	इ	से	रा	के	री	पा	वा	सि	य	नि	पि
ने	ख	के	वे	ऊ	ड	नी	दे	दि	भ	आ	नि	जे	वे	वे
ष	ण	प	कि	से	य	ह	ह	ते	रा	द	सा	सी	थ	जे

शब्दावली शब्द-सूची

बैकअप, तकनीक, डेटान्यूनीकरण, सुरक्षितनेटवर्क, सुरक्षानीति, स्थिरअवस्थामें, निगरानी, सुरक्षास्थिति

चेकपॉइंट 6, वैकल्पिक: सुलभ शब्दावली मिलान

वर्ड सर्च के 8 शब्दावली पदों में से प्रत्येक को उसकी सही परिभाषा से मिलाएँ; खाली स्थान में अक्षर (A-H) लिखें।

शब्दावली के शब्द
A. बैकअप
B. तकनीक
C. डेटान्यूनीकरण
D. सुरक्षितनेटवर्क
E. सुरक्षानीति
F. स्थिरअवस्थामें
G. निगरानी
H. सुरक्षास्थिति

परिभाषाएँ और मिलान फ़ील्ड	
	1. डेटा की वह दशा, जब वह स्टोरेज में रखा हो और कहीं भेजा न जा रहा हो।
	2. किसी संगठन की साइबर सुरक्षा की कुल मज़बूती का आकलन।
	3. ऐसा कनेक्शन, जिसमें भेजा गया डेटा बाहरी लोगों से सुरक्षित रहता है।
	4. सुरक्षा के नियमों और कदमों का लिखित ढांचा।
	5. संदिग्ध गतिविधियों पर लगातार नज़र रखना।
	6. संचालन के लिए ज़रूरी न्यूनतम सीमा तक ही निजी डेटा संग्रह सीमित करना।
	7. सिस्टम विफलता की स्थिति में बहाल करने के लिए डेटा की सुरक्षित ऑफ़साइट प्रतियां बनाना।
	8. किसी काम को कुशलता से करने की वैज्ञानिक विधि और औज़ार।

चेकपॉइंट 7: उलझे शब्दों की चुनौती

नीचे के अक्षरों को सुलझाकर साइबर सुरक्षा की प्रमुख अवधारणाएँ और शब्द पता करें। अपने उत्तर दिए गए इनपुट बॉक्स में लिखें।

1. **अ बै प क**

2. **डे न्यू ण र क नी टा**

3. **क्षा सु ति नी र**

4. **नी रा नि ग**

5. **क त नी क**

6. **व र्क त ट सु ने र क्षि**

7. **स्था स्थि व में अ र**

8. **ति सु क्षा स्थि र**

अतिरिक्त गतिविधि: झटपट सोचें

हर श्रेणी में 3 उत्तर। जो सबसे पहले सूची भर दे, वह जीतता है।

1	ऐसी चीज़ें जिनका आप बैकअप लेते हैं			
2	साइबर सुरक्षा से जुड़े शब्द			
3	संवेदनशील डेटा देखने की अनुमति वाले लोग			
4	डेटा को सुरक्षित रूप से हटाने के तरीके			
5	ऐसी जगहें जहाँ डेटा स्टोर होता है			
6	ऐसी चीज़ें जिन्हें एन्क्रिप्ट किया जाना चाहिए			
7	ऐसा डेटा जिसे अस्पताल को सुरक्षित रखना होता है			
8	बैकअप के प्रकार			
9	ऐसी जानकारी जो आपको कभी साझा नहीं करनी चाहिए			
10	ईमेल में चेतावनी के संकेत			
11	सुरक्षित आदतें जो आप आज से शुरू कर सकते हैं			
12	IT मदद के लिए आप जिनसे पूछ सकते हैं			
13	ऐसे डिवाइस जिन्हें हैक किया जा सकता है			
14	डेटा की सुरक्षा के तरीके			
15	ऐसी चीज़ें जो डेटा नष्ट कर सकती हैं			

चेकपॉइंट 8: साइबर सुरक्षा केस स्टडी

नीचे दिए गए वास्तविक परिदृश्यों को हल करने के लिए सीखी हुई अवधारणाओं का उपयोग करें।

केस स्टडी 1: एंटरप्राइज़ डेटाबेस एट-रेस्ट एन्क्रिप्शन अपग्रेड



परिदृश्य: एक ऑनलाइन रिटेलर लेन-देन डेटाबेस को पूर्ण डिस्क एन्क्रिप्शन के बिना क्लाउड स्टोरेज पर रखता है। हाल के एक अनुपालन ऑडिट ने इसे गंभीर CCPA डेटा-सुरक्षा जोखिम बताया। एक रिकवरी आर्किटेक्चर डिज़ाइन कीजिए।

चर्चा प्रश्न: CCPA अनुपालन जोखिमों का विश्लेषण कीजिए और एट-रेस्ट एन्क्रिप्शन रणनीति प्रस्तावित कीजिए।

केस स्टडी 2: रैंसमवेयर की रोकथाम और डेटा बहाली



परिदृश्य: एक सक्रिय रैनसमवेयर हमला कॉर्पोरेट लोकल नेटवर्क पर नेटवर्क ड्राइव को एन्क्रिप्ट कर रहा है। एडमिनिस्ट्रेटर ने संक्रमण का जल्दी पता लगा लिया है। रोकथाम और रिकवरी के चरणों की योजना बनाइए।

चर्चा प्रश्न: तत्काल रोकथाम की कार्रवाइयों का विवरण दीजिए और सुरक्षित बहाली प्रक्रिया की योजना बनाइए।

चेकपॉइंट 9: कूट संदेश को डिकोड करें

साइबर सुरक्षा पेशेवर नेटवर्क संपत्तियों को ऑनलाइन ख़तरा पैदा करने वालों से बचाता है। नीचे दी गई अक्षर-से-संख्या कुंजी का उपयोग करके संदेश को डिक्रिप्ट करें और खाली स्थानों में मेल खाते अक्षर लिखें।

अक्षर-से-संख्या एन्क्रिप्शन कुंजी

अ=1 आ=2 इ=3 ई=4 उ=5 ऊ=6 ऋ=7 ए=8 ऐ=9 ओ=10 औ=11 ऑ=12

क=13 ख=14 ग=15 घ=16 ङ=17 च=18 छ=19 ज=20 झ=21 ञ=22 ट=23 ठ=24

ड=25 ढ=26 ण=27 त=28 थ=29 द=30 ध=31 न=32 प=33 फ=34 ब=35 भ=36

म=37 य=38 र=39 ल=40 व=41 श=42 ष=43 स=44 ह=45 ा=46 ि=47 ी=48

ु=49 ू=50 ृ=51 े=52 ै=53 ो=54 ौ=55 ॉ=56 ं=57 ँ=58 ः=59 ़=60

्=61

44	49	39	13	61	43	47	28		32	47	38	57	28	61	39	27		44	52

32	47	20	48		25	52	23	46		35	18	46	8	57

डिकोड किया गया संदेश:

सुझाव: हर संख्या वर्णमाला में उस अक्षर की स्थिति दर्शाती है (जैसे 1 = अ, 2 = आ, 61 = ्)।

चेकपॉइंट 10: बुनियादी साइबर सुरक्षा FAQ (भाग A)

ऑनलाइन खतरों को कम करने से जुड़े आम सवाल और जवाब देखें।

Q1: डेटा संरक्षण क्या है?

यह तकनीकी नियंत्रणों के ज़रिए व्यक्तिगत और व्यावसायिक डेटा को अनधिकृत एक्सेस, हानि या करप्शन से सुरक्षित करने की प्रक्रिया है।

Q2: फ़ुल-डिस्क एन्क्रिप्शन क्यों ज़रूरी है?

यह भौतिक ड्राइव पर संग्रहीत डेटा ब्लॉक सुरक्षित करता है, जिससे हार्ड ड्राइव की भौतिक चोरी होने पर भी कोई डेटा नहीं पढ़ सकता।

Q3: एन्क्रिप्शन एट रेस्ट और इन ट्रांज़िट में क्या अंतर है?

एट-रेस्ट एन्क्रिप्शन ड्राइव पर संग्रहीत फ़ाइलों को सुरक्षित करता है, जबकि इन-ट्रांज़िट एन्क्रिप्शन राउटरों से गुज़रते सक्रिय नेटवर्क पैकेटों को सुरक्षित करता है।

Q4: डेटा मास्किंग क्या है?

यह संवेदनशील विवरण (जैसे क्रेडिट कार्ड नंबर) को असली रिकॉर्ड उजागर किए बिना परीक्षण के लिए काल्पनिक लेकिन यथार्थवादी डेटा से बदल देता है।

Q5: ऑफ़लाइन बैकअप क्यों महत्वपूर्ण है?

यह आपकी फ़ाइलों की एक साफ़ कॉपी नेटवर्क से अलग रखता है, जिससे आपके बैकअप को रैनसमवेयर द्वारा एन्क्रिप्ट किए जाने से बचाने में मदद मिलती है।

चेकपॉइंट 10: बुनियादी साइबर सुरक्षा FAQ (भाग B)

ऑनलाइन खतरों को कम करने से जुड़े आम सवाल और जवाब देखें।

Q6: डेटा टोकनाइज़ेशन वॉल्ट क्या है?

सुरक्षित, अलग रखा गया डेटाबेस जो यादृच्छिक टोकन को उनके मूल संवेदनशील मानों (जैसे प्राथमिक क्रेडिट कार्ड नंबर) से जोड़ता है।

Q7: ज़ीरो-ट्रस्ट डेटाबेस एक्सेस का क्या अर्थ है?

इसका अर्थ है नेटवर्क के भीतर किसी पर भरोसा करने के बजाय हर लॉगिन पर हर उपयोगकर्ता की पहचान और डिवाइस की स्थिति को सत्यापित करना।

Q8: TLS ट्रांज़िट में डेटा की सुरक्षा कैसे करता है?

TLS TCP सेशन पेलोड को एन्क्रिप्ट करता है, जिससे सार्वजनिक नेटवर्क पर मौजूद दुर्भावनापूर्ण तत्व पारगमन में पैकेट को स्निफ़ या संशोधित नहीं कर पाते।

Q9: डेटाबेस एक्सेस ऑडिटिंग क्या है?

डेटाबेस क्वेरी और लॉगिन की लगातार रिकॉर्डिंग, ताकि अनधिकृत एक्सेस के पैटर्न या सुरक्षा विसंगतियाँ पकड़ी जा सकें।

Q10: क्लाउड सुरक्षा पॉश्चर ऑडिट क्या है?

ऐसी प्रक्रिया जो क्लाउड कॉन्फ़िगरेशन का विश्लेषण करके खुले पोर्ट, गलत कॉन्फ़िगर किए गए एक्सेस नियम और सुरक्षा अनुपालन की कमियाँ पहचानती है।

चेकपॉइंट 10: उन्नत सुरक्षा FAQ (भाग C)

सुरक्षा फ़्रेमवर्क, मैलवेयर विश्लेषण और डेटा अनुपालन के उन्नत तकनीकी पहलुओं को जानें।

Q1: एनवेलप एन्क्रिप्शन कैसे काम करता है?

यह डेटा को डेटा कुंजी से एन्क्रिप्ट करता है, फिर उस डेटा कुंजी को मास्टर कुंजी से एन्क्रिप्ट करता है, जिससे कुंजी का भंडारण और रोटेशन सरल हो जाता है।

Q2: होमोमॉर्फ़िक एन्क्रिप्शन क्या है?

उन्नत एन्क्रिप्शन विधि जो एन्क्रिप्टेड डेटा को पहले डिक्रिप्ट किए बिना सीधे उस पर संचालन करने देती है।

Q3: डेटाबेस में कॉलम-स्तर का एन्क्रिप्शन क्यों उपयोग किया जाता है?

यह विशिष्ट संवेदनशील कॉलम (जैसे SSN) को अलग-अलग एन्क्रिप्ट करता है, जिससे एडमिन को सामान्य टेबल रीड एक्सेस मिलने पर भी वे सुरक्षित रहते हैं।

Q4: डेटा लॉस प्रिवेंशन (DLP) क्या है?

नेटवर्क एग्ज़िट पॉइंट की निगरानी करने वाला सॉफ़्टवेयर, जो संवेदनशील फ़ाइलों के अनधिकृत आउटबाउंड ट्रांसफ़र को पहचानकर ब्लॉक करता है।

Q5: राइट-वन्स-रीड-मैनी (WORM) बैकअप रैनसमवेयर से कैसे बचाते हैं?

WORM बैकअप फ़ाइलों को एक निश्चित अवधि तक हटाए या बदले जाने से रोकते हैं, जिससे रैनसमवेयर मौजूदा बैकअप को एन्क्रिप्ट नहीं कर पाता।

चेकपॉइंट 10: उन्नत सुरक्षा FAQ (भाग D)

सुरक्षा फ़्रेमवर्क, मैलवेयर विश्लेषण और डेटा अनुपालन के उन्नत तकनीकी पहलुओं को जानें।

Q6: कुंजी दोबारा उपयोग करने का जोखिम क्या है?

अलग-अलग डेटाबेस में एक ही क्रिप्टोग्राफ़िक कुंजी दोबारा इस्तेमाल करने का मतलब है कि एक कुंजी के compromise होने से सभी डेटाबेस उजागर हो जाते हैं।

Q7: डेटाबेस टोकनाइज़ेशन CCPA अनुपालन को कैसे बेहतर करता है?

टोकन गैर-उत्पादन सिस्टमों में रिकॉर्ड को छद्मनामित करते हैं और ब्रीच के जोखिम को सीमित करते हैं, लेकिन टोकनाइज़ किया गया डेटा फिर भी व्यक्तिगत जानकारी हो सकता है।

Q8: डेटा क्लासिफ़िकेशन महत्वपूर्ण क्यों है?

यह फ़ाइलों को संवेदनशीलता स्तर के आधार पर वर्गीकृत करता है, जिससे संगठन उच्च-जोखिम डेटा पर सबसे मज़बूत एन्क्रिप्शन और एक्सेस नियंत्रण लागू कर पाते हैं।

Q9: कुंजी रोटेशन की क्या भूमिका है?

एन्क्रिप्शन कुंजियों को नियमित रूप से बदलने से, किसी एक कुंजी के अंततः क्रैक हो जाने पर उजागर होने वाला ऐतिहासिक डेटा सीमित रहता है।

Q10: सिक्योर एन्क्लेव मेमोरी में डेटाबेस क्वेरी की रक्षा कैसे करते हैं?

सिक्योर एन्क्लेव क्वेरी ऑपरेशन को CPU-सुरक्षित मेमोरी ब्लॉक में अलग रखते हैं, जिससे होस्ट एडमिनिस्ट्रेटर RAM में क्लियरटेक्स्ट नहीं देख पाते।

भाग 11: 10 वास्तविक साइबर सुरक्षा तथ्य और अंतर्दृष्टियाँ

सुरक्षा उल्लंघनों, बचाव तंत्रों और अनुपालन मानकों से जुड़े वास्तविक तथ्य देखें।

1. सुरक्षा इनसाइट

GDPR नियम मई 2018 में लागू हुए, जिससे वैश्विक साइटें कुकी सहमति और व्यक्तिगत डेटा रजिस्ट्री को प्रबंधित करने का तरीका बदल गया।

2. सुरक्षा इनसाइट

GDPR उल्लंघन का जुर्माना 20 मिलियन यूरो या वैश्विक टर्नओवर के 4% तक पहुँच सकता है, जो काफ़ी कानूनी जोखिम दर्शाता है। [4]

3. सुरक्षा इनसाइट

CCPA जनवरी 2020 में लागू हुआ और इसने अमेरिका में डिजिटल गोपनीयता से जुड़े उपभोक्ता अधिकारों की अग्रणी नींव रखी।

4. सुरक्षा इनसाइट

डेटा न्यूनतमीकरण डेटाबेस स्टोरेज का आकार घटाता है, जिससे सर्वर संचालन लागत कम होती है और उल्लंघन का प्रभाव भी घटता है।

5. सुरक्षा इनसाइट

क्रिप्टोग्राफ़िक श्रेडिंग ऐतिहासिक बैकअप टेप फ़ाइलों को बदलने के बजाय कुंजियाँ मिटाकर बैकअप हटाने की चुनौती हल करती है।

6. सुरक्षा इनसाइट

दुनिया के ज़्यादातर देशों ने अब उपभोक्ताओं के गोपनीयता अधिकारों की रक्षा के लिए व्यक्तिगत डेटा सुरक्षा कानून बना लिए हैं।

7. सिक्योरिटी इनसाइट

यूरोपीय डेटा गोपनीयता नियामक परिभाषाओं के तहत पहले से टिक किए गए बॉक्स वाले ऑप्ट-इन सहमति फ़ॉर्म स्पष्ट रूप से प्रतिबंधित हैं।

8. सिक्योरिटी इनसाइट

GDPR के अनुसार जहाँ संभव हो, व्यक्तिगत डेटा उल्लंघन की जानकारी मिलने के 72 घंटों के भीतर पर्यवेक्षी प्राधिकरण को रिपोर्ट करना ज़रूरी है। [3]

9. सिक्योरिटी इनसाइट

bcrypt या Argon2 जैसे धीमे एल्गोरिदम से पासवर्ड हैश करने पर चोरी हुए हैश को ऑफ़लाइन क्रैक करना कहीं अधिक कठिन हो जाता है। [6]

10. सुरक्षा इनसाइट

एट-रेस्ट डेटा सहेजी गई डेटाबेस फ़ाइलों को दर्शाता है, जबकि इन-ट्रांज़िट डेटा नेटवर्क राउटरों से गुज़रते सक्रिय पैकेटों को।

तकनीकी संदर्भ और स्रोत

यह अध्ययन गाइड और इंटरैक्टिव पहेलियाँ वैश्विक NIST, OWASP और डेटा गोपनीयता अनुपालन मानकों से तैयार की गई हैं।

शैक्षणिक और उद्योग संदर्भ

[1] NIST. (2025). SP 800-88 Rev. 2, Guidelines for Media Sanitization.
https://csrc.nist.gov/pubs/sp/800/88/r2/final

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

[3] Intersoft Consulting. (n.d.). Art. 33 GDPR – Notification of a personal data breach to the supervisory authority.
https://gdpr-info.eu/art-33-gdpr/

[4] Intersoft Consulting. (n.d.). Art. 83 GDPR – General conditions for imposing administrative fines.
https://gdpr-info.eu/art-83-gdpr/

[5] California Privacy Protection Agency. (n.d.). Frequently Asked Questions (FAQs).
https://cppa.ca.gov/faq.html

[6] OWASP. (n.d.). Password Storage Cheat Sheet.
https://cheatsheetseries.owasp.org/cheatsheets/Password_Storage_Cheat_Sheet.html

उत्तर कुंजी: चेकपॉइंट 1 – बहुविकल्पीय

1 **प्रश्न 1** **सही उत्तर: A**

शिक्षण नोट

डेटा मास्किंग का मुख्य उद्देश्य क्या है? → गोपनीयता की रक्षा के लिए संवेदनशील पहचानकर्ताओं को काल्पनिक लेकिन यथार्थवादी वर्णों से बदलना

2 **प्रश्न 2** **सही उत्तर: A**

शिक्षण नोट

कौन-सा तंत्र डेटाबेस सर्वर की हार्ड ड्राइव पर संग्रहीत फ़ाइलों को एन्क्रिप्ट करता है? → स्टोरेज में फ़ुल-डिस्क एन्क्रिप्शन

3 **प्रश्न 3** **सही उत्तर: A**

शिक्षण नोट

ट्रांज़िट में डेटा क्या दर्शाता है? → नेटवर्क राउटर और स्विच के पार जाते डेटा पैकेट

4 **प्रश्न 4** **सही उत्तर: A**

शिक्षण नोट

रैनसमवेयर से सुरक्षा के लिए नियमित ऑफ़लाइन बैकअप क्यों महत्वपूर्ण है? → यह फिरौती दिए बिना फ़ाइलें बहाल करने के लिए साफ़, ऑफ़लाइन कॉपी देता है

5 **प्रश्न 5** **सही उत्तर: A**

शिक्षण नोट

डेटा टोकनाइज़ेशन क्या करता है? → यह संवेदनशील कार्ड नंबरों को गैर-संवेदनशील यादृच्छिक टोकन से बदल देता है

उत्तर कुंजी: चेकपॉइंट 2 – सही या गलत

6 **प्रश्न 6** **सही उत्तर: गलत**

शिक्षण नोट

मास्किंग टेस्ट कॉपी बदलती है या केरी के समय मान छिपाती है; प्रोडक्शन रिकॉर्ड अपरिवर्तित रहते हैं।

7 **प्रश्न 7** **सही उत्तर: सही**

शिक्षण नोट

रैंसमवेयर के प्रसार को रोकने के लिए ऑफ़साइट बैकअप को मुख्य कॉर्पोरेट नेटवर्क से अलग रखना चाहिए।

8 **प्रश्न 8** **सही उत्तर: गलत**

शिक्षण नोट

TLS सर्टिफ़िकेट ट्रांज़िट में डेटा की रक्षा करते हैं; स्टोर किए गए डेटा के लिए डिस्क, फ़ाइल या डेटाबेस एन्क्रिप्शन चाहिए।

9 **प्रश्न 9** **सही उत्तर: सही**

शिक्षण नोट

ज़ीरो-ट्रस्ट नेटवर्क एक्सेस (ZTNA) डेटाबेस पहुँच देने से पहले हर उपयोगकर्ता की पहचान सत्यापित करता है।

10 **प्रश्न 10** **सही उत्तर: सही**

शिक्षण नोट

वॉल्ट-आधारित टोकनाइज़ेशन मूल मानों को एक सुरक्षित टोकन वॉल्ट में रखता है जो हर टोकन को उसके डेटा से जोड़ता है।

शब्दावली कुंजियाँ और ग्रेडिंग रूब्रिक

शिक्षक के लिए ग्रेडिंग रूब्रिक: हर सही मिलान (कुल 8 अंक) और संदर्भ शब्द (कुल 6 अंक) के लिए 1 अंक दें।

चेकपॉइंट 4: उत्तर – अवधारणा मिलान

B 1. एन्क्रिप्शन	A 2. बैकअप	H 3. न्यूनीकरण	F 4. एक्सेस
C 5. पॉश्चर	E 6. उल्लंघन	D 7. अनुपालन	G 8. मास्किंग

चेकपॉइंट 3: उत्तर – प्रमुख शब्द

1 डेटा न्यूनीकरण	2 स्थिर अवस्था में	3 सुरक्षित नेटवर्क	4 सुरक्षा नीति
5 बैकअप	6 सुरक्षा स्थिति		

चेकपॉइंट 6, वैकल्पिक: उत्तर – शब्द मिलान

1 F – स्थिरअवस्थामें	2 H – सुरक्षास्थिति	3 D – सुरक्षितनेटवर्क	4 E – सुरक्षानीति
5 G – निगरानी	6 C – डेटान्यूनीकरण	7 A – बैकअप	8 B – तकनीक

शिक्षकों के लिए चर्चा नोट

प्रमुख शब्द:
जाँचें कि क्या विद्यार्थी एन्क्रिप्शन, बैकअप और न्यूनीकरण को अपने शब्दों में समझा सकते हैं और हर एक का उदाहरण दे सकते हैं।

केस स्टडी:
विद्यार्थियों से कहें कि वे अपनी सिफ़ारिशें राय के बजाय वर्कशीट के तथ्यों पर आधारित करें।

स्रोतों का मूल्यांकन:
विद्यार्थियों से वर्कशीट के स्रोतों में कम से कम एक कथन की पुष्टि करवाएँ और चर्चा करें कि आँकड़े, कीमतें और नियम समय के साथ क्यों बदल सकते हैं।

पहेलियों की कुंजियाँ और शिक्षक नोट

शब्द खोज समाधान

द	में	प	ति	के	ट	मि	नि	ट	सा	य	च	ऊ	नी	जी
इ	स्था	त	म	पे	ब	प	ग	सु	जि	मी	ने	ले	इ	सी
य	व	छ	र	दे	कि	जा	रा	सा	र	वा	ड	रे	स	ख
नि	अ	फ	ढ	मा	ना	का	नी	रे	दे	क्षा	सि	मी	क	पि
ता	र	ति	ज	श	सु	भ	ऊ	अ	ऊ	ए	स्थि	रि	बै	वि
श	स्थि	य	वि	व	र	वा	डे	पा	ल	च	से	ति	क	कि
क	नी	क	त	य	क्षि	घ	प	टा	के	की	व	सि	अ	री
ति	त	की	कि	सि	त	ना	ने	पा	न्यू	ते	ण	ए	प	ता
नी	सा	मी	न	नी	ने	ऋ	ले	घ	ति	नी	जि	ला	ए	जी
क्षा	ले	ड	ल	द	ट	जे	घ	के	च	से	क	दे	री	ए
र	पी	उ	अ	जे	व	मि	घ	व	आ	च	मी	र	च	ट
सु	थ	फ	ग	ना	र्क	सी	का	ज	फ	नी	जी	ता	ण	ठ
से	लि	ट	आ	इ	से	रा	के	री	पा	वा	सि	य	नि	पि
ने	ख	के	वे	ऊ	ड	नी	दे	दि	भ	आ	नि	जे	वे	वे
ष	ण	प	कि	से	य	ह	ह	ते	रा	द	सा	सी	थ	जे

क्रॉसवर्ड समाधान



क्रॉसवर्ड समाधान के लिए शिक्षक गाइड

बाएँ से दाएँ

3 बाएँ से दाएँ: डेटान्यूनीकरण संचालन के लिए ज़रूरी न्यूनतम सीमा तक ही निजी डेटा संग्रह सीमित करना (7 अक्षर)

4 बाएँ से दाएँ: सुरक्षितनेटवर्क ऐसा कनेक्शन, जिसमें भेजा गया डेटा बाहरी लोगों से सुरक्षित रहता है (8 अक्षर)

6 बाएँ से दाएँ: बैकअप सिस्टम विफलता की स्थिति में बहाल करने के लिए डेटा की सुरक्षित ऑफ़साइट प्रतियां बनाना (4 अक्षर)

ऊपर से नीचे

1 ऊपर से नीचे: निगरानी संदिग्ध गतिविधियों पर लगातार नज़र रखना (4 अक्षर)

2 ऊपर से नीचे: स्थिरअवस्थामें डेटा की वह दशा, जब वह स्टोरेज में रखा हो और कहीं भेजा न जा रहा हो (6 अक्षर)

4 ऊपर से नीचे: सुरक्षानीति सुरक्षा के नियमों और कदमों का लिखित ढांचा (5 अक्षर)

5 ऊपर से नीचे: तकनीक किसी काम को कुशलता से करने की वैज्ञानिक विधि और औज़ार (4 अक्षर)

अक्षर-फेर शब्द और कूट संदेश हल कुंजी

शब्द-अनस्क्रैम्बल गतिविधि और Secret Cipher Challenge की ग्रेडिंग कुंजी।

शब्द अनस्क्रैम्बल कुंजी

1. अबैपक — **बैकअप**
2. डेन्यूणरकनीटा — **डेटान्यूनीकरण**
3. क्षासुतिनीर — **सुरक्षानीति**
4. नीरानिग — **निगरानी**
5. कतनीक — **तकनीक**
6. वर्कतटसुनेरक्षि — **सुरक्षितनेटवर्क**
7. स्थास्थिवमेंअर — **स्थिरअवस्थामें**
8. तिसुक्षास्थिर — **सुरक्षास्थिति**

गुप्त कूट चुनौती कुंजी

"सुरक्षित नियंत्रण से निजी डेटा बचाएं"

केस स्टडी के उत्तर

A केस स्टडी 1: एंटरप्राइज़ डेटाबेस एट-रेस्ट एन्क्रिप्शन अपग्रेड

शिक्षक समाधान

ग्रेडिंग दिशानिर्देश

छात्रों के उत्तरों में निम्नलिखित बिंदु शामिल होने चाहिए:

- परिदृश्य विश्लेषण: एक ऑनलाइन रिटेलर लेन-देन के डेटाबेस क्लाउड स्टोरेज पर फ़ुल-डिस्क एन्क्रिप्शन के बिना रखता है। हाल के अनुपालन ऑडिट में इसे CCPA के तहत डेटा-सुरक्षा का गंभीर जोखिम बताया गया। एक रिकवरी आर्किटेक्चर डिज़ाइन करें।
- अनुशंसित रणनीति और समाधान: सभी फ़ाइल सिस्टम पर AES-256 फ़ुल-डिस्क एन्क्रिप्शन (एट रेस्ट) लागू करें। स्वचालित रोटेशन वाली केंद्रीकृत Key Management Service (KMS) का उपयोग करें और डिक्रिप्शन की पहुँच नियंत्रित करने के लिए सख़्त IAM नीतियाँ लागू करें।

B केस स्टडी 2: रैंसमवेयर की रोकथाम और डेटा बहाली

शिक्षक समाधान

ग्रेडिंग दिशानिर्देश

छात्रों के उत्तरों में निम्नलिखित बिंदु शामिल होने चाहिए:

- परिदृश्य विश्लेषण: एक सक्रिय रैनसमवेयर हमला कॉर्पोरेट लोकल नेटवर्क पर नेटवर्क ड्राइव एन्क्रिप्ट कर रहा है। एडमिनिस्ट्रेटर ने संक्रमण का जल्दी पता लगा लिया है। रोकथाम और रिकवरी के चरणों की योजना बनाएँ।
- अनुशंसित रणनीति और समाधान: प्रभावित सेगमेंट को तुरंत अलग करें। प्रभावित एंडपॉइंट फ़ॉर्मैट करें और नवीनतम ऑफ़लाइन राइट-वन्स-रीड-मेनी (WORM) बैकअप से रिस्टोर करें। सिस्टम दोबारा जोड़ने से पहले बैकअप की अखंडता जाँचें।