نام: _____ تاریخ: _____ نمبر: _____

ڈیٹا کا تحفظ اور انٹرپرائز اسٹوریج سیکیورٹی گائیڈ

ڈیٹا ماسکنگ، ٹوکنائزیشن، ایٹ ریسٹ بمقابلہ اِن ٹرانزٹ خفیہ کاری، آف لائن بیک اپس

ڈیٹا کے تحفظ کا تعلیمی جائزہ

محفوظ شدہ

ڈیٹا کی خفیہ کاری

256 بٹ AES معیار

تعمیل شدہ

عالمی معیارات

GDPR اور CCPA فریم ورکس

زیرو ٹرسٹ

رسائی کی پالیسی

ملٹی فیکٹر تصدیق

خوش آمدید! یہ سرگرمی پیکٹ آپ کو ڈیٹا تحفظ کے معیارات اور کنٹرولز سے متعارف کراتا ہے۔ آپ مکمل ڈسک خفیہ کاری، محفوظ رسائی کنٹرولز، ہارڈ ویئر بیک اپس، کلاؤڈ سیکیورٹی پوسچر، اور ڈیٹا ماسکنگ تکنیکوں کا جائزہ لیں گے۔

ورک شیٹ کے چیک پوائنٹس

- ☐ **حصہ 1-4: سائبر سیکیورٹی اور خطرات سے بچاؤ میں مہارت حاصل کریں۔**
- ☐ **حصہ 5-7: کراس ورڈ اور ورڈ سرچ پہیلیاں حل کریں۔**
- ☐ **حصہ 8-9: کیس اسٹڈیز اور سائفر چیلنج حل کریں۔**
- ☐ **حصہ 10: بنیادی اور اعلیٰ FAQ صفحات کا جائزہ لیں۔**
- ☐ **حصہ 11: 10 دلچسپ حقیقی دنیا کے حقائق دریافت کریں۔**
- ☐ **اضافی: تیزی سے سوچیں چیلنج**

VPN.com سائبر سیکیورٹی گائیڈ کھولیں

URL: https://www.vpn.com/cybersecurity/data-protection/

آپ کی ڈیٹا تحفظ کی حکمت عملی کا لرننگ روڈ میپ

- ڈیٹا ماسکنگ اور ٹوکنائزیشن کی تکنیکوں میں فرق واضح کریں۔
- اسٹوریج ڈرائیوز کے لیے ذخیرہ شدہ حالت میں خفیہ کاری اور TLS کے ذریعے منتقلی کے دوران خفیہ کاری نافذ کریں۔
- رینسم ویئر سے تحفظ کے لیے آف لائن، نیٹ ورک سے الگ بیک اپ سسٹمز ڈیزائن کریں۔

ڈیٹا کے تحفظ کی رہنمائی کی ہدایات

کثیر انتخابی اور درست/غلط سوالات حل کریں، لفظوں کے ذخیرے کی مدد سے خالی جگہیں پُر کریں، تعریفوں کا ملان کریں، اور کراس ورڈ اور ورڈ سرچ پہیلیاں حل کریں۔ اپنے علم کو ڈیٹا کے تحفظ پر لاگو کریں۔ اور آخر میں اضافی سرگرمی "تیزی سے سوچیں"۔

ڈیٹا کا تحفظ اور انٹرپرائز اسٹوریج کی سیکیورٹی (تعارف)

ڈیٹا پروٹیکشن کارپوریٹ ڈیٹا اثاثوں کو ماسکنگ، ٹوکنائزیشن، ایٹ ریسٹ ڈیٹا بیس خفیہ کاری اور محفوظ ٹرانزٹ پروٹوکولز کے ذریعے محفوظ بناتی ہے۔ نیٹ ورک سے الگ بیک اپس بنانا اس بات کو یقینی بنانے میں مدد دیتا ہے کہ فعال دراندازی کی صورت میں اہم ڈیٹا بیسز بحال کیے جا سکیں۔

ہر چیک پوائنٹ کو غور سے پڑھیں اور درست جواب منتخب کریں یا لکھیں۔

چیک پوائنٹ 1: کثیر انتخابی چیلنج

1 1. ڈیٹا ماسکنگ کا بنیادی مقصد کیا ہے؟

- A. رازداری کے تحفظ کے لیے حساس شناخت کنندگان کو فرضی مگر حقیقت پسندانہ حروف سے بدلنا
- B. فزیکل سرور اسٹوریج بچانے کے لیے بڑی ڈیٹا بیس فائلوں کو کمپریس کرنا
- C. آرکائیو بیک اپ سسٹمز سے پرانی کسٹمر رابطہ ای میلز حذف کرنا
- D. ڈیٹا بیس سرور کے عوامی IP ایڈریس کو انٹرنیٹ اسکینز سے چھپانا

2 2. ڈیٹا بیس سرور کی ہارڈ ڈرائیو پر محفوظ فائلوں کو کون سا میکانزم خفیہ کرتا ہے؟

- A. اسٹوریج کی حالت میں مکمل ڈسک خفیہ کاری
- B. ترسیل کے دوران TLS سیشن ہینڈ شیک پروٹوکولز
- C. متحرک DNS نیم سرور فارورڈنگ رولز
- D. ہارڈ ویئر کیز کے ساتھ ملٹی فیکٹر توثیق

3 3. ٹرانزٹ میں موجود ڈیٹا کی نمائندگی کیا کرتا ہے؟

- A. نیٹ ورک راؤٹرز اور سوئچز سے گزرنے والے ڈیٹا پیکٹس
- B. کولڈ بیک اپ ڈرائیو پر محفوظ ڈیٹا بیس ٹرانزیکشن لاگز
- C. الگ تھلگ کلاؤڈ والٹ میں محفوظ کی گئی آرکائیو شدہ صارف فائلیں
- D. مقامی ڈیسک ٹاپ اسٹوریج پر جامد سسٹم کنفیگریشن فائلیں

4 4. رینسم ویئر سے تحفظ کے لیے باقاعدہ آف لائن بیک اپ کیوں اہم ہے؟

- A. یہ تاوان ادا کیے بغیر فائلیں بحال کرنے کے لیے صاف، آف لائن کاپی فراہم کرتا ہے
- B. یہ ہیکرز کو کھلے پورٹ کنفیگریشنز اسکین کرنے سے روکتا ہے
- C. یہ مقامی نیٹ ورک ٹرانسمیشن کی بینڈ وڈتھ رفتار بڑھاتا ہے
- D. یہ براؤزرز پر کوکی رضامندی کے آپٹ اِن لاگز کو خودکار بناتا ہے

5 5. ڈیٹا ٹوکنائزیشن کیا کرتی ہے؟

- A. یہ حساس کارڈ نمبروں کو غیر حساس بے ترتیب ٹوکنز سے بدل دیتا ہے
- B. یہ ویب ٹریفک کو متعدد محفوظ اونین نوڈز سے گزارتا ہے
- C. یہ سسٹم ڈائریکٹریز میں دستخط پر مبنی میل ویئر تلاش کرتا ہے
- D. یہ ڈیٹا بیس ایڈمنسٹریٹر کے لاگ اِن سیشن کے اوقات کا آڈٹ کرتا ہے

چیک پوائنٹ 2: درست یا غلط چیلنج

6 سوال 6

6. ڈیٹا ماسکنگ پروڈکشن ماحول میں ڈیٹا بیس ریکارڈز کو مستقل طور پر بدل دیتی ہے۔

○ درست ○ غلط

7 سوال 7

7. رینسم ویئر کے پھیلاؤ کو روکنے کے لیے آف سائٹ بیک اپس کو مرکزی کارپوریٹ نیٹ ورک سے الگ رکھنا ضروری ہے۔

○ درست ○ غلط

8 سوال 8

8. SSL/TLS سرٹیفکیٹس فزیکل میڈیا پر محفوظ ڈیٹا کو خفیہ کر کے ڈیٹا بیسز کو محفوظ بناتے ہیں۔

○ درست ○ غلط

9 سوال 9

9. زیرو ٹرسٹ نیٹ ورک ایکسیس (ZTNA) ڈیٹا بیس تک رسائی دینے سے پہلے ہر صارف کی شناخت کی تصدیق کرتا ہے۔

○ درست ○ غلط

10 سوال 10

10. والٹ پر مبنی ٹوکنائزیشن اصل کارڈ ویلیوز کو ایک محفوظ، مرکزی ٹوکن والٹ میں محفوظ کرتی ہے۔

○ درست ○ غلط

چیک پوائنٹ 3: کلیدی اصطلاح شامل کرنا

ذیل میں ہر جملہ پڑھیں اور خالی جگہ کو ورڈ بینک سے درست اصطلاح کے ساتھ پُر کریں۔

1. ذاتی ناموں کو حقیقت پسندانہ متبادل سے بدلنا ڈیٹا _____ کہلاتا ہے۔
2. طبعی اسٹوریج بلاکس کو انکرپٹ کرنا ڈیٹا بیس اثاثوں کو _____ محفوظ رکھتا ہے۔
3. TLS پروٹوکولز حرکت کرنے والے فعال ڈیٹا پیکٹس کو _____ انکرپٹ کرتے ہیں۔
4. رول پر مبنی اجازتیں محدود کرتی ہیں کہ کون سے صارفین ڈیٹا بیس تک _____ حاصل کر سکتے ہیں۔
5. ڈیٹا بریچ کے بعد کلین کارپوریٹ فائلیں بحال کرنے کے لیے ایک محفوظ آف لائن _____ درکار ہوتا ہے۔
6. کلاؤڈ کنفیگریشنز کا آڈٹ ادارے کی سیکیورٹی _____ کا جائزہ لیتا ہے۔

الفاظ کا بینک

بریچ | بیک اپ | پوسچر | ترسیل کے دوران | تعمیل | رسائی | ساکن حالت میں | ماسکنگ

اپنے جوابات یہاں لکھیں:

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

چیک پوائنٹ 4: سیکیورٹی تصورات کا ملان

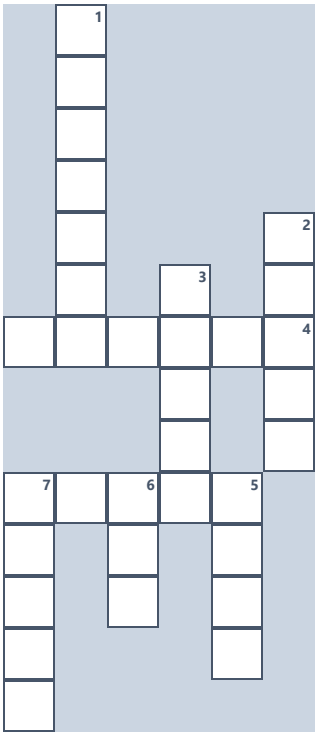
تعریفوں کا ملان

دائیں جانب کی ہر اصطلاح کو بائیں جانب کی درست تعریف سے ملائیں اور بھرے جانے والے ان پٹ باکس میں متعلقہ حرف (A-H) لکھیں۔

1. خفیہ کاری	A	سسٹم کی ناکامی کی صورت میں بحالی کے لیے ڈیٹا کی محفوظ آف سائٹ کاپیاں بنانا۔
2. بیک اپ	B	سادہ متن کو ناقابل مطالعہ سائفر ٹیکسٹ میں تبدیل کرنا تاکہ روکا گیا ڈیٹا نجی رہے۔
3. کم سے کم کرنا	C	کسی ادارے کے کلاؤڈ کی مجموعی سیکیورٹی حالت اور دفاعی تیاری۔
4. رسائی	D	نجی صارف معلومات کے انتظام کے لیے GDPR یا CCPA جیسے ریگولیٹری معیارات پر پورا اترنا۔
5. پوسچر	E	سیکیورٹی واقعہ جس میں محفوظ ڈیٹا تک بغیر اجازت رسائی یا اس کا انکشاف ہو جائے۔
6. بریچ	F	ڈیٹا بیس کی پڑھنے اور لکھنے کی اجازتیں تصدیق شدہ صارف کرداروں تک محدود کرنا۔
7. تعمیل	G	ذاتی شناخت کے تحفظ کے لیے ڈیٹا بیس فیلڈز میں حساس حروف تبدیل کرنا۔
8. ماسکنگ	H	آپریشنز کے لیے ضروری کم سے کم حد تک ذاتی ڈیٹا اکٹھا کرنے کو محدود کرنا۔

چیک پوائنٹ 5: کراس ورڈ پہیلی

فعال سفید خانوں میں حروف ٹائپ کر کے کراس ورڈ پہیلی حل کریں۔ نمبر نیچے دیے گئے سراغوں سے مطابقت رکھتے ہیں۔



افقی

4. ڈیٹا بیس فیلڈز میں حساس حروف بدلنا تاکہ ذاتی شناختیں محفوظ رہیں (6)

5. سسٹم کی ناکامی کی صورت میں بحال کرنے کے لیے ڈیٹا کی محفوظ آف سائٹ کاپیاں بنانا (5)

عمودی

1. سادہ متن کو ناقابل مطالعہ سائفر ٹیکسٹ میں بدلنا تاکہ روکا گیا ڈیٹا نجی رہے (7)

2. GDPR یا CCPA جیسے ضابطہ جاتی معیارات پر پورا اترنا جو نجی صارف معلومات کے انتظام کے لیے ہیں (5)

3. ڈیٹا بیس کے پڑھنے اور لکھنے کی اجازتوں کو تصدیق شدہ صارف کرداروں تک محدود کرنا (5)

5. سیکیورٹی کا ایسا واقعہ جس میں محفوظ ڈیٹا بغیر اجازت دیکھا یا افشا کیا جائے (4)

6. ذاتی ڈیٹا کی وصولی کو کارروائیوں کے لیے ضروری کم سے کم حد تک محدود کرنا (3)

7. ادارے کے کلاؤڈ کی مجموعی سیکیورٹی حالت اور دفاعی تیاری (5)

چیک پوائنٹ 5 – متبادل سرگرمی: قابلِ رسائی کراس ورڈ سراغ

اسکرین ریڈر اور کی بورڈ استعمال کرنے والے صارفین نیچے دیے گئے ٹیکسٹ فیلڈز میں کراس ورڈ کے جوابات براہ راست ٹائپ کر سکتے ہیں۔

افقی

4 افقی: ڈیٹا بیس فیلڈز میں حساس حروف بدلنا تاکہ ذاتی شناختیں محفوظ رہیں (6 حروف):

5 افقی: سسٹم کی ناکامی کی صورت میں بحال کرنے کے لیے ڈیٹا کی محفوظ آف سائٹ کاپیاں بنانا (5 حروف):

عمودی

1 عمودی: سادہ متن کو ناقابل مطالعہ سائفر ٹیکسٹ میں بدلنا تاکہ روکا گیا ڈیٹا نجی رہے (7 حروف):

2 عمودی: GDPR یا CCPA جیسے ضابطہ جاتی معیارات پر پورا اترنا جو نجی صارف معلومات کے انتظام کے لیے ہیں (5 حروف):

3 عمودی: ڈیٹا بیس کے پڑھنے اور لکھنے کی اجازتوں کو تصدیق شدہ صارف کرداروں تک محدود کرنا (5 حروف):

5 عمودی: سیکیورٹی کا ایسا واقعہ جس میں محفوظ ڈیٹا بغیر اجازت دیکھا یا افشا کیا جائے (4 حروف):

6 عمودی: ذاتی ڈیٹا کی وصولی کو کارروائیوں کے لیے ضروری کم سے کم حد تک محدود کرنا (3 حروف):

7 عمودی: ادارے کے کلاؤڈ کی مجموعی سیکیورٹی حالت اور دفاعی تیاری (5 حروف):

چیک پوائنٹ 6: پوشیدہ الفاظ کی تلاش

نیچے گرڈ میں چھپی 8 اہم اصطلاحات تلاش کریں۔ الفاظ افقی، عمودی یا ترچھے ہو سکتے ہیں۔

ب	ش	ل	ج	س	گ	ل	ش	ت	ن	ئ	و	ے	چ	ت
چ	ک	ا	ت	ت	ع	ت	چ	گ	ر	ن	ا	ت	ی	و
ا	ع	ن	ب	ت	ع	ر	ل	ٹ	ک	ٹ	ک	و	ئ	د
ی	م	ک	ا	م	ی	ن	گ	ع	د	د	ہ	ر	ا	چ
ش	ل	ج	ی	ئ	ل	ع	ش	ے	ا	ر	ت	ر	س	م
گ	ل	ل	ے	ل	ش	م	ب	ک	ن	ج	د	ن	ر	پ
ئ	گ	پ	ب	ا	ب	ی	د	س	ک	ت	و	ن	ہ	پ
ت	ر	ش	م	ت	ک	ر	و	ے	ر	س	ئ	ر	س	ر
ن	م	م	ش	ا	ش	ج	ل	ل	پ	س	ک	ک	د	چ
ت	ی	ب	پ	ن	چ	گ	ل	ن	ش	ب	ج	و	و	س
ب	ٹ	ی	ع	پ	ہ	ع	ن	گ	ن	ک	س	ا	م	و
ا	ر	ب	ہ	ب	ل	ے	م	ت	ک	پ	ع	چ	ر	پ
م	م	ی	پ	د	چ	ٹ	ت	گ	ت	ا	س	ت	ک	ع
گ	م	ا	چ	ا	ٹ	ی	م	ٹ	ن	ع	ن	د	ت	ش
ن	ٹ	ب	ئ	ک	پ	ن	و	ن	ر	ل	ئ	و	ل	ک

الفاظ کی فہرست

انکرپشن
بیکاپ
کمی
رسائی
پوسچر
بریچ
تعمیل
ماسکنگ

چیک پوائنٹ 6 – متبادل سرگرمی: قابلِ رسائی الفاظ کا ملان

ورڈ سرچ کی 8 اصطلاحات میں سے ہر ایک کو اس کی درست تعریف سے ملائیں اور خالی جگہ میں حرف (A-H) لکھیں۔

اصطلاحات
A. انکرپشن
B. بیکاپ
C. کمی
D. رسائی
E. پوسچر
F. بریچ
G. تعمیل
H. ماسکنگ

تعریفیں اور ملان کے خانے	
1. سیکیورٹی کا ایسا واقعہ جس میں محفوظ ڈیٹا بغیر اجازت دیکھا یا افشا کیا جائے۔	
2. ڈیٹا بیس فیلڈز میں حساس حروف بدلنا تاکہ ذاتی شناختیں محفوظ رہیں۔	
3. ڈیٹا بیس کے پڑھنے اور لکھنے کی اجازتوں کو تصدیق شدہ صارف کرداروں تک محدود کرنا۔	
4. ادارے کے کلاؤڈ کی مجموعی سیکیورٹی حالت اور دفاعی تیاری۔	
5. GDPR یا CCPA جیسے ضابطہ جاتی معیارات پر پورا اترنا جو نجی صارف معلومات کے انتظام کے لیے ہیں۔	
6. ذاتی ڈیٹا کی وصولی کو کارروائیوں کے لیے ضروری کم سے کم حد تک محدود کرنا۔	
7. سادہ متن کو ناقابل مطالعہ سائفر ٹیکسٹ میں بدلنا تاکہ روکا گیا ڈیٹا نجی رہے۔	
8. سسٹم کی ناکامی کی صورت میں بحال کرنے کے لیے ڈیٹا کی محفوظ آف سائٹ کاپیاں بنانا۔	

چیک پوائنٹ 7: الجھے الفاظ کا چیلنج

سائبر سیکیورٹی کے اہم تصورات اور اصطلاحات ظاہر کرنے کے لیے نیچے دیے گئے حروف کو درست ترتیب میں لائیں۔ اپنے جوابات دیے گئے ان پٹ باکسز میں لکھیں۔

1. ر ش ا پ ن ک ن
2. ی م ک
3. س پ ر چ و
4. م ل ی ت ع
5. ک پ ب ا ی
6. ئ ر ا ی س
7. ی ب چ ر
8. س گ م ن ک ا

اضافی سرگرمی: تیزی سے سوچیں

ہر زمرے کے لیے 3 جوابات لکھیں۔ جو سب سے پہلے فہرست مکمل کرے وہ جیتتا ہے۔

1. وہ چیزیں جن کا آپ بیک اپ لیتے ہیں
2. سائبر سیکیورٹی سے متعلق الفاظ
3. حساس ڈیٹا دیکھنے کے مجاز لوگ
4. ڈیٹا کو محفوظ طریقے سے حذف کرنے کے طریقے
5. وہ مقامات جہاں ڈیٹا محفوظ کیا جاتا ہے
6. وہ چیزیں جنہیں خفیہ کیا جانا چاہیے
7. وہ ڈیٹا جس کی حفاظت ہسپتال پر لازم ہے
8. بیک اپ کی اقسام
9. وہ معلومات جو آپ کو کبھی شیئر نہیں کرنی چاہئیں
10. ای میل میں انتباہی علامات
11. محفوظ عادات جو آپ آج شروع کر سکتے ہیں
12. وہ لوگ جن سے آپ آئی ٹی مدد مانگ سکتے ہیں
13. وہ ڈیوائسز جنہیں ہیک کیا جا سکتا ہے
14. ڈیٹا کی حفاظت کے طریقے
15. وہ چیزیں جو ڈیٹا کو تباہ کر سکتی ہیں

چیک پوائنٹ 8: سائبر سیکیورٹی کیس اسٹڈیز

جو تصورات آپ نے سیکھے ہیں انہیں نیچے دیے گئے حقیقی منظرناموں کو حل کرنے میں استعمال کریں۔

کیس اسٹڈی 1: انٹرپرائز ڈیٹا بیس کی ایٹ ریسٹ خفیہ کاری کی اپ گریڈ



منظرنامہ: ایک آن لائن ریٹیلر لین دین کے ڈیٹا بیسز کلاؤڈ اسٹوریج پر مکمل ڈسک انکرپشن کے بغیر محفوظ کرتا ہے۔ ایک حالیہ کمپلائنس آڈٹ نے اسے CCPA ڈیٹا سیکیورٹی کا سنگین خطرہ قرار دیا۔ ریکوری آرکیٹیکچر ڈیزائن کریں۔

بحث کا سوال: CCPA کمپلائنس کے خطرات کا تجزیہ کریں، اور ایٹ ریسٹ خفیہ کاری کی حکمت عملی تجویز کریں۔

کیس اسٹڈی 2: رینسم ویئر کی روک تھام اور ڈیٹا کی بحالی



منظرنامہ: ایک ایکٹو رینسم ویئر حملہ کارپوریٹ لوکل نیٹ ورک کی نیٹ ورک ڈرائیوز کو خفیہ کر رہا ہے۔ ایڈمنسٹریٹر نے انفیکشن کا جلد پتا لگا لیا ہے۔ کنٹینمنٹ اور ریکوری کے اقدامات کی منصوبہ بندی کریں۔

بحث کا سوال: فوری کنٹینمنٹ اقدامات تفصیل سے بیان کریں، اور محفوظ بحالی کے عمل کی منصوبہ بندی کریں۔

چیک پوائنٹ 9: سائفر حل کریں

سائبر سیکیورٹی پیشہ ور نیٹ ورک اثاثوں کو آن لائن خطرات پیدا کرنے والوں سے بچاتا ہے۔ نیچے دی گئی حرف سے عدد کی کلید استعمال کر کے خالی جگہوں میں متعلقہ حروف لکھ کر پیغام ڈی کرپٹ کریں۔

حرف سے عدد خفیہ کاری کی کلید

ا=1 ب=2 پ=3 ت=4 ٹ=5 ث=6 ج=7 چ=8 ح=9 خ=10 د=11 ڈ=12 ذ=13

ر=14 ڑ=15 ز=16 ژ=17 س=18 ش=19 ص=20 ض=21 ط=22 ظ=23 ع=24 غ=25 ف=26

ق=27 ک=28 گ=29 ل=30 م=31 ن=32 ں=33 و=34 ہ=35 ھ=36 ی=37 ے=38 ئ=39

37	7	32	38	18	16	30	34	14	5	32	28	23	34	26	9	31

33	37	39	1	8	2	1	5	37	12

ڈی کوڈ شدہ پیغام:

ٹپ: ہر نمبر اوپر دی گئی کلید کے ایک اردو حرف کو ظاہر کرتا ہے۔

چیک پوائنٹ 10: سائبر سیکیورٹی عمومی سوالات – بنیادی (حصہ A)

آن لائن خطرات کی روک تھام کے بارے میں عام سوالات اور جوابات کا جائزہ لیں۔

Q1: ڈیٹا کا تحفظ کیا ہے؟

یہ تکنیکی کنٹرولز کے ذریعے ذاتی اور کاروباری ڈیٹا کو غیر مجاز رسائی، نقصان یا خرابی سے محفوظ بنانے کا عمل ہے۔

Q2: مکمل ڈسک خفیہ کاری کیوں اہم ہے؟

یہ فزیکل ڈرائیوز پر ذخیرہ شدہ ڈیٹا بلاکس کو محفوظ بناتا ہے، جس سے ہارڈ ڈرائیو چوری ہونے پر بھی کوئی ڈیٹا نہیں پڑھ سکتا۔

Q3: ذخیرہ شدہ ڈیٹا اور منتقلی کے دوران ڈیٹا کی خفیہ کاری میں کیا فرق ہے؟

ایٹ ریسٹ خفیہ کاری ڈرائیوز پر محفوظ فائلوں کو محفوظ بناتی ہے، جبکہ اِن ٹرانزٹ خفیہ کاری راؤٹرز پر چلنے والے فعال نیٹ ورک پیکٹس کو محفوظ بناتی ہے۔

Q4: ڈیٹا ماسکنگ کیا ہے؟

یہ حساس تفصیلات (جیسے کریڈٹ کارڈ نمبرز) کو فرضی لیکن حقیقت پسندانہ ڈیٹا سے بدل دیتا ہے تاکہ حقیقی ریکارڈز ظاہر کیے بغیر ٹیسٹنگ ہو سکے۔

Q5: آف لائن بیک اپ اہم کیوں ہے؟

یہ آپ کی فائلوں کی ایک صاف کاپی نیٹ ورک سے الگ رکھتا ہے، جو آپ کے بیک اپس کو رینسم ویئر سے خفیہ ہونے سے بچانے میں مدد دیتی ہے۔

چیک پوائنٹ 10: سائبر سیکیورٹی عمومی سوالات – بنیادی (حصہ B)

آن لائن خطرات کی روک تھام کے بارے میں عام سوالات اور جوابات کا جائزہ لیں۔

Q6: ڈیٹا ٹوکنائزیشن والٹ کیا ہے؟

محفوظ، الگ تھلگ ڈیٹا بیس جو بے ترتیب ٹوکنز کو ان کی اصل حساس قدروں (جیسے بنیادی کریڈٹ کارڈ نمبرز) سے جوڑتا ہے۔

Q7: زیرو ٹرسٹ ڈیٹا بیس رسائی کا کیا مطلب ہے؟

اس کا مطلب ہے ہر لاگ اِن پر ہر صارف کی شناخت اور ڈیوائس کی حالت کی تصدیق کرنا، نیٹ ورک کے اندر موجود کسی پر بھروسا کرنے کے بجائے۔

Q8: TLS منتقلی کے دوران ڈیٹا کا تحفظ کیسے کرتا ہے؟

TLS TCP سیشن پے لوڈ کو خفیہ کرتا ہے، جس سے عوامی نیٹ ورکس پر موجود بدنیت عناصر ترسیل میں موجود پیکٹس کو سونگھ نہیں سکتے اور نہ ان میں ردوبدل کر سکتے ہیں۔

Q9: ڈیٹا بیس رسائی کا آڈٹ کیا ہے؟

غیر مجاز رسائی کے نمونوں یا سیکیورٹی بے قاعدگیوں کا پتا لگانے کے لیے ڈیٹا بیس کوئریز اور لاگ اِنز کی مسلسل ریکارڈنگ۔

Q10: کلاؤڈ سیکیورٹی پوسچر آڈٹ کیا ہے؟

ایسا عمل جو کلاؤڈ کنفیگریشنز کا تجزیہ کر کے کھلے پورٹس، غلط ترتیب شدہ رسائی اصول اور سیکیورٹی تعمیل کی خامیاں شناخت کرتا ہے۔

چیک پوائنٹ 10: سیکیورٹی عمومی سوالات – اعلیٰ (حصہ C)

سیکیورٹی فریم ورکس، میل ویئر تجزیے اور ڈیٹا کمپلائنس کے جدید تکنیکی پہلوؤں کا جائزہ لیں۔

Q1: انویلپ انکرپشن کیسے کام کرتی ہے؟

یہ ڈیٹا کو ڈیٹا کلید سے خفیہ کرتا ہے، پھر اس ڈیٹا کلید کو ماسٹر کلید سے خفیہ کرتا ہے، جس سے کلید کا ذخیرہ اور گردش آسان ہو جاتی ہے۔

Q2: ہومو مارفک خفیہ کاری کیا ہے؟

جدید خفیہ کاری کا طریقہ جو خفیہ کردہ ڈیٹا پر پہلے ڈی کرپٹ کیے بغیر براہِ راست عمل کی اجازت دیتا ہے۔

Q3: ڈیٹا بیس کالم لیول خفیہ کاری کیوں استعمال کی جاتی ہے؟

یہ مخصوص حساس کالمز (جیسے SSNs) کو انفرادی طور پر خفیہ کرتا ہے، اور اگر ایڈمنز کو ٹیبل کی عمومی ریڈ رسائی مل بھی جائے تو انہیں محفوظ رکھتا ہے۔

Q4: ڈیٹا لاس پریوینشن (DLP) کیا ہے؟

ایسا سافٹ ویئر جو نیٹ ورک ایگریس پوائنٹس کی نگرانی کرتا ہے تاکہ حساس فائلوں کی غیر مجاز آؤٹ باؤنڈ منتقلی کا پتا لگائے اور اسے روکے۔

Q5: ایک بار لکھیں-بار بار پڑھیں (WORM) بیک اپس رینسم ویئر سے تحفظ کیسے دیتے ہیں؟

WORM بیک اپس فائلوں کو ایک مقررہ مدت تک حذف یا تبدیل ہونے سے روکتے ہیں، جس سے رینسم ویئر موجودہ بیک اپس کو خفیہ نہیں کر پاتا۔

چیک پوائنٹ 10: سیکیورٹی عمومی سوالات – اعلیٰ (حصہ D)

سیکیورٹی فریم ورکس، میل ویئر تجزیے اور ڈیٹا کمپلائنس کے جدید تکنیکی پہلوؤں کا جائزہ لیں۔

Q6: کلید کو دوبارہ استعمال کرنے کا کیا خطرہ ہے؟

مختلف ڈیٹا بیسز میں ایک ہی کرپٹوگرافک کلید دوبارہ استعمال کرنے کا مطلب ہے کہ ایک کلید کے سمجھوتے سے تمام ڈیٹا بیسز متاثر ہو جاتے ہیں۔

Q7: ڈیٹا بیس ٹوکنائزیشن CCPA کی تعمیل کو کیسے بہتر بناتی ہے؟

ٹوکنز غیر پروڈکشن سسٹمز میں ریکارڈز کو فرضی نام دیتے ہیں اور خلاف ورزی کے خطرے کو محدود کرتے ہیں، لیکن ٹوکنائز شدہ ڈیٹا پھر بھی ذاتی معلومات ہو سکتا ہے۔

Q8: ڈیٹا کی درجہ بندی انتہائی اہم کیوں ہے؟

یہ فائلوں کو حساسیت کی سطح کے لحاظ سے درجہ بند کرتا ہے، جس سے تنظیموں کو زیادہ خطرے والے ڈیٹا پر مضبوط ترین خفیہ کاری اور رسائی کے کنٹرولز لاگو کرنے میں مدد ملتی ہے۔

Q9: کلید کی روٹیشن کا کیا کردار ہے؟

خفیہ کاری کی کیز کو باقاعدگی سے اپ ڈیٹ کرنے سے، اگر کوئی ایک کی آخرکار توڑ دی جائے، تو ظاہر ہونے والا تاریخی ڈیٹا محدود رہتا ہے۔

Q10: سیکیور انکلیوز میموری میں ڈیٹا بیس کوئریز کا تحفظ کیسے کرتے ہیں؟

سیکیور انکلیوز کوئری آپریشنز کو CPU سے محفوظ میموری بلاکس میں الگ تھلگ رکھتے ہیں، جس سے ہوسٹ ایڈمنسٹریٹرز RAM میں موجود غیر خفیہ متن نہیں دیکھ پاتے۔

حصہ 11: 10 حقیقی دنیا کے سائبر سیکیورٹی حقائق اور بصیرتیں

سیکیورٹی خلاف ورزیوں، دفاعی نظاموں اور تعمیل کے معیارات کے بارے میں حقیقی دنیا کے حقائق کا جائزہ لیں۔

1. سیکیورٹی بصیرت

GDPR ضوابط مئی 2018 میں نافذ ہوئے، جنہوں نے عالمی سائٹس کے کوکی رضامندیوں اور ذاتی ڈیٹا رجسٹریوں کے انتظام کا طریقہ بدل دیا۔

2. سیکیورٹی بصیرت

GDPR کی خلاف ورزی پر جرمانہ 20 ملین یورو یا عالمی کاروبار کے 4% تک پہنچ سکتا ہے، جو قانونی طور پر کافی بڑا خطرہ ہے۔ [4]

3. سیکیورٹی بصیرت

CCPA جنوری 2020 میں نافذ ہوا، جس نے امریکہ میں ڈیجیٹل رازداری کے صارفی حقوق کی اولین بنیاد رکھی۔

4. سیکیورٹی بصیرت

ڈیٹا کو کم سے کم رکھنا ڈیٹا بیس اسٹوریج کا حجم گھٹاتا ہے، جس سے سرور چلانے کی لاگت کم ہوتی ہے اور بریچ کے اثرات بھی کم ہوتے ہیں۔

5. سیکیورٹی بصیرت

کرپٹوگرافک شریڈنگ بیک اپ حذف کرنے کے چیلنج کو یوں حل کرتی ہے کہ تاریخی بیک اپ ٹیپ فائلوں میں ترمیم کرنے کے بجائے کیز مٹا دی جاتی ہیں۔

6. سیکیورٹی بصیرت

دنیا کے زیادہ تر ممالک اب صارفین کے رازداری کے حقوق کے تحفظ کے لیے ذاتی ڈیٹا کے تحفظ کے قوانین نافذ کر چکے ہیں۔

7. سیکیورٹی کی بصیرت

یورپی ڈیٹا پرائیویسی ضوابط کی تعریفوں کے تحت پہلے سے نشان زد باکسز والے آپٹ اِن رضامندی فارمز پر واضح پابندی ہے۔

8. سیکیورٹی کی بصیرت

GDPR تقاضا کرتا ہے کہ جہاں ممکن ہو، ذاتی ڈیٹا کی خلاف ورزیوں کی اطلاع علم ہونے کے 72 گھنٹوں کے اندر نگران ادارے کو دی جائے۔ [3]

9. سیکیورٹی کی بصیرت

bcrypt یا Argon2 جیسے سست الگورتھمز سے پاس ورڈز کی ہیشنگ چوری شدہ ہیشز کو آف لائن کریک کرنا کہیں زیادہ مشکل بنا دیتی ہے۔ [6]

10. سیکیورٹی بصیرت

محفوظ شدہ ڈیٹا بیس فائلیں ڈیٹا ایٹ ریسٹ کہلاتی ہیں، جبکہ نیٹ ورک راؤٹرز پر فعال طور پر منتقل ہوتے پیکٹس ڈیٹا اِن ٹرانزٹ ہیں۔

تکنیکی حوالہ جات اور ماخذ

مطالعاتی گائیڈ اور انٹرایکٹو پہیلیاں عالمی NIST، OWASP اور ڈیٹا پرائیویسی کمپلائنس معیارات سے مرتب کی گئی ہیں۔

علمی اور صنعتی حوالہ جات

[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

جوابی کلید: چیک پوائنٹ 1 – کثیر انتخابی

1 سوال 1 — درست جواب: A

تدریسی نوٹ

ڈیٹا ماسکنگ کا بنیادی مقصد کیا ہے؟ → رازداری کے تحفظ کے لیے حساس شناخت کنندگان کو فرضی مگر حقیقت پسندانہ حروف سے بدلنا

2 سوال 2 — درست جواب: A

تدریسی نوٹ

ڈیٹا بیس سرور کی ہارڈ ڈرائیو پر محفوظ فائلوں کو کون سا میکانزم خفیہ کرتا ہے؟ → اسٹوریج کی حالت میں مکمل ڈسک خفیہ کاری

3 سوال 3 — درست جواب: A

تدریسی نوٹ

ٹرانزٹ میں موجود ڈیٹا کی نمائندگی کیا کرتا ہے؟ → نیٹ ورک راؤٹرز اور سوئچز سے گزرنے والے ڈیٹا پیکٹس

4 سوال 4 — درست جواب: A

تدریسی نوٹ

رینسم ویئر سے تحفظ کے لیے باقاعدہ آف لائن بیک اپ کیوں اہم ہے؟ → یہ تاوان ادا کیے بغیر فائلیں بحال کرنے کے لیے صاف، آف لائن کاپی فراہم کرتا ہے

5 سوال 5 — درست جواب: A

تدریسی نوٹ

ڈیٹا ٹوکنائزیشن کیا کرتی ہے؟ → یہ حساس کارڈ نمبروں کو غیر حساس بے ترتیب ٹوکنز سے بدل دیتا ہے

جوابی کلید: چیک پوائنٹ 2 – درست یا غلط

6 سوال 6

درست جواب: غلط

تدریسی نوٹ

ماسکنگ ٹیسٹ کاپیوں کو تبدیل کرتی ہے یا کوئری کے وقت ویلیوز کو چھپاتی ہے؛ پروڈکشن ریکارڈز میں کوئی تبدیلی نہیں ہوتی۔

7 سوال 7

درست جواب: درست

تدریسی نوٹ

رینسم ویئر کے پھیلاؤ کو روکنے کے لیے آف سائٹ بیک اپس کو مرکزی کارپوریٹ نیٹ ورک سے الگ رکھنا ضروری ہے۔

8 سوال 8

درست جواب: غلط

تدریسی نوٹ

TLS سرٹیفیکیٹس ترسیل میں موجود ڈیٹا کی حفاظت کرتے ہیں؛ ایٹ ریسٹ ڈیٹا کو ڈسک، فائل یا ڈیٹا بیس کی خفیہ کاری درکار ہوتی ہے۔

9 سوال 9

درست جواب: درست

تدریسی نوٹ

زیرو ٹرسٹ نیٹ ورک ایکسیس (ZTNA) ڈیٹا بیس تک رسائی دینے سے پہلے ہر صارف کی شناخت کی تصدیق کرتا ہے۔

10 سوال 10

درست جواب: درست

تدریسی نوٹ

والٹ پر مبنی ٹوکنائزیشن اصل ویلیوز کو ایک محفوظ ٹوکن والٹ میں رکھتی ہے جو ہر ٹوکن کو اس کے ڈیٹا سے ملاتا ہے۔

الفاظ کی کلید اور درجہ بندی کا معیار

استاد کی گریڈنگ روبرک: ہر درست ملان (کل 8 نمبر) اور سیاقی اصطلاح (کل 6 نمبر) کے لیے 1 نمبر دیں۔

چیک پوائنٹ 4: جوابی کلید – تصورات کا ملان

B 1. خفیہ کاری	A 2. بیک اپ	H 3. کم سے کم کرنا	F 4. رسائی
C 5. پوسچر	E 6. بریچ	D 7. تعمیل	G 8. ماسکنگ

چیک پوائنٹ 3: جوابی کلید – اہم اصطلاحات

1 ماسکنگ	2 ساکن حالت میں	3 ترسیل کے دوران	4 رسائی
5 بیک اپ	6 پوسچر		

چیک پوائنٹ 6 – متبادل سرگرمی: جوابی کلید – الفاظ کا ملان

1 F – بریچ	2 H – ماسکنگ	3 D – رسائی	4 E – پوسچر
5 G – تعمیل	6 C – کمی	7 A – انکرپشن	8 B – بیکاپ

اساتذہ کے لیے بحث کے نوٹس

اہم اصطلاحات:
یقینی بنائیں کہ طلبہ خفیہ کاری، بیک اپ اور کم سے کم کرنا کو اپنے الفاظ میں سمجھا سکیں اور ہر ایک کی مثال دے سکیں۔

کیس اسٹڈیز:
طلبہ سے کہیں کہ اپنی سفارشات کو ورک شیٹ کے حقائق پر مبنی رکھیں، ذاتی رائے پر نہیں۔

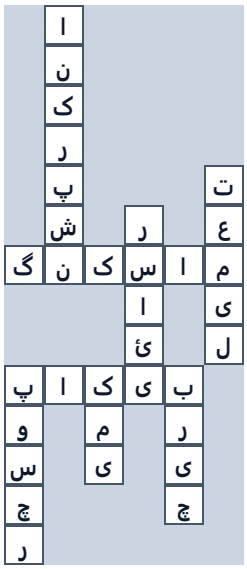
ماخذ کی جانچ:
طلبہ سے کہیں کہ ورک شیٹ کے ماخذ میں کم از کم ایک دعوے کی تصدیق کریں، اور اس پر بات کریں کہ اعداد و شمار، قیمتیں اور قواعد وقت کے ساتھ کیوں بدل سکتے ہیں۔

پہیلیوں کی کلیدیں اور استاد کے نوٹس

الفاظ کی تلاش کا حل

ب	ش	ل	چ	س	گ	ل	ش	ت	ن	ئ	و	ے	چ	ت
چ	ک	ا	ت	ت	ع	ت	چ	گ	ر	ن	ا	ت	ی	و
ا	ع	ن	ب	ت	ع	ر	ل	ٹ	ک	ٹ	ک	و	ئ	د
ی	م	ک	ا	م	ی	ن	گ	ع	د	د	ہ	ر	ا	چ
ش	ل	چ	ی	ئ	ل	ع	ش	ے	ا	ر	ت	ر	س	م
گ	ل	ل	ے	ش	ل	م	ب	ک	ن	چ	د	ن	ر	پ
ئ	گ	پ	ب	ا	ب	ی	د	س	ک	ت	و	ن	ہ	پ
ت	ر	ش	م	ت	ک	ر	و	ے	ر	س	ئ	ر	س	ر
ن	م	م	ش	ا	ش	چ	ل	ل	پ	س	ک	ک	د	چ
ت	ی	ب	پ	ن	چ	گ	ل	ن	ش	ب	چ	و	و	س
ب	ٹ	ی	پ	ہ	ع	ن	گ	ن	ک	س	ا	م	و	
ا	ر	ب	ہ	ب	ل	ے	م	ت	ک	پ	ع	چ	ر	پ
م	ی	پ	د	چ	ٹ	ت	گ	ت	ا	س	ت	ک	ع	
گ	م	ا	چ	ا	ٹ	ی	م	ٹ	ع	ن	د	ت	ش	
ن	ٹ	ب	ئ	ک	پ	ن	و	ن	ر	ل	ئ	و	ل	ک

کراس ورڈ کا حل



کراس ورڈ حل کے لیے استاد کی گائیڈ

افقی

4 افقی: ماسکنگ ڈیٹا بیس فیلڈز میں حساس حروف بدلنا تاکہ ذاتی شناختیں محفوظ رہیں (6 حروف)

5 افقی: بیکاپ سسٹم کی ناکامی کی صورت میں بحال کرنے کے لیے ڈیٹا کی محفوظ آف سائٹ کاپیاں بنانا (5 حروف)

عمودی

1 عمودی: انکرپشن سادہ متن کو ناقابل مطالعہ سائفر ٹیکسٹ میں بدلنا تاکہ روکا گیا ڈیٹا نجی رہے (7 حروف)

2 عمودی: تعمیل GDPR یا CCPA جیسے ضابطہ جاتی معیارات پر پورا اترنا جو نجی صارف معلومات کے انتظام کے لیے ہیں (5 حروف)

3 عمودی: رسائی ڈیٹا بیس کے پڑھنے اور لکھنے کی اجازتوں کو تصدیق شدہ صارف کرداروں تک محدود کرنا (5 حروف)

5 عمودی: بریچ سیکیورٹی کا ایسا واقعہ جس میں محفوظ ڈیٹا بغیر اجازت دیکھا یا افشا کیا جائے (4 حروف)

6 عمودی: کمی ذاتی ڈیٹا کی وصولی کو کارروائیوں کے لیے ضروری کم سے کم حد تک محدود کرنا (3 حروف)

7 عمودی: پوسچر ادارے کے کلاؤڈ کی مجموعی سیکیورٹی حالت اور دفاعی تیاری (5 حروف)

الفاظ کی ترتیب اور سائفر حل کی کلید

الفاظ کی ترتیب درست کرنے کی سرگرمی اور Secret Cipher Challenge کی گریڈنگ کلید۔

الفاظ کی ترتیب درست کرنے کی کلید

1. رشاپنکن — انکرپشن
2. یمک — کمی
3. سپرچو — پوسچر
4. ملیتع — تعمیل
5. کپبای — بیکاپ
6. ئرایس — رسائی
7. ییچر — بریچ
8. سگمنکا — ماسکنگ

خفیہ سائفر چیلنج کی کلید

"محفوظ کنٹرولز سے نجی ڈیٹا بچائیں"

کیس اسٹڈیز کی جوابی کلید

A کیس اسٹڈی 1: انٹرپرائز ڈیٹا بیس کی ایٹ ریسٹ خفیہ کاری کی اپ گریڈ

استاد کا حل

گریڈنگ کی ہدایت

طلبہ کے جوابات میں درج ذیل نکات شامل ہونے چاہییں:

- منظرنامے کا تجزیہ: ایک آن لائن ریٹیلر ٹرانزیکشن ڈیٹا بیسز کو مکمل ڈسک خفیہ کاری کے بغیر کلاؤڈ اسٹوریج پر رکھتا ہے۔ حالیہ کمپلائنس آڈٹ نے اسے CCPA کے تحت ڈیٹا سیکیورٹی کا سنگین خطرہ قرار دیا۔ ایک ریکوری آرکیٹیکچر ڈیزائن کریں۔
- تجویز کردہ حکمت عملی اور حل: تمام فائل سسٹمز پر ڈیٹا ایٹ ریسٹ کے لیے AES-256 فل ڈسک خفیہ کاری نافذ کریں۔ خودکار روٹیشن والی مرکزی کی مینجمنٹ سروس (KMS) استعمال کریں اور ڈی کرپشن تک رسائی کنٹرول کرنے کے لیے سخت IAM پالیسیاں نافذ کریں۔

B کیس اسٹڈی 2: رینسم ویئر کی روک تھام اور ڈیٹا کی بحالی

استاد کا حل

گریڈنگ کی ہدایت

طلبہ کے جوابات میں درج ذیل نکات شامل ہونے چاہییں:

- منظرنامے کا تجزیہ: ایک فعال رینسم ویئر حملہ کارپوریٹ لوکل نیٹ ورک پر نیٹ ورک ڈرائیوز کو خفیہ کر رہا ہے۔ ایڈمنسٹریٹر نے انفیکشن کا جلد پتا لگا لیا ہے۔ روک تھام اور بحالی کے مراحل کی منصوبہ بندی کریں۔
- تجویز کردہ حکمت عملی اور حل: متاثرہ سیگمنٹ کو فوراً الگ کریں۔ متاثرہ اینڈ پوائنٹس کو فارمیٹ کریں اور تازہ ترین آف لائن، ایک بار لکھیں بار بار پڑھیں (WORM) بیک اپ سے بحال کریں۔ سسٹمز کو دوبارہ جوڑنے سے پہلے بیک اپ کی سالمیت کی تصدیق کریں۔