নাম: _____ তারিখ: _____ নম্বর: _____

ডেটা সুরক্ষা ও এন্টারপ্রাইজ স্টোরেজ নিরাপত্তা গাইড

ডেটা মাস্কিং, টোকেনাইজেশন, অ্যাট-রেস্ট বনাম ইন-ট্রানজিট এনক্রিপশন, অফলাইন ব্যাকআপ

ডেটা সুরক্ষা শিক্ষণ পরিচিতি

সুরক্ষিত
ডেটা এনক্রিপশন
256-বিট AES স্ট্যান্ডার্ড

সম্মতিপূর্ণ
বৈশ্বিক মান
GDPR ও CCPA কাঠামো

জিরো-ট্রাস্ট
অ্যাক্সেস নীতি
মাল্টি-ফ্যাক্টর অথেনটিকেশন

স্বাগতম! এই অ্যাক্টিভিটি প্যাকেট আপনাকে ডেটা সুরক্ষার মান ও নিয়ন্ত্রণ বিষয়ে গাইড করবে। আপনি ফুল-ডিস্ক এনক্রিপশন, নিরাপদ অ্যাক্সেস নিয়ন্ত্রণ, হার্ডওয়্যার ব্যাকআপ, ক্লাউড নিরাপত্তা অবস্থান এবং ডেটা মাস্কিং কৌশল সম্পর্কে জানবেন।

ওয়ার্কশিট চেকপয়েন্ট

- [ ] **অংশ 1-4: সাইবার নিরাপত্তা ও হুমকি প্রতিরোধে দক্ষতা অর্জন করুন।**
- [ ] **অংশ 5-7: ক্রসওয়ার্ড ও ওয়ার্ড সার্চ ধাঁধা সমাধান করুন।**
- [ ] **অংশ 8-9: কেস স্টাডি ও সংকেতবার্তা চ্যালেঞ্জ সমাধান করুন।**
- [ ] **অংশ 10: প্রাথমিক ও উন্নত স্তরের FAQ পেজ পর্যালোচনা করুন।**
- [ ] **অংশ 11: 10টি আকর্ষণীয় বাস্তব তথ্য অন্বেষণ করুন।**
- [ ] **অতিরিক্ত: দ্রুত ভাবুন চ্যালেঞ্জ।**

VPN.com সাইবার নিরাপত্তা গাইড খুলুন

URL: https://www.vpn.com/bn/saibar-nirapotta/data-surakkha/

আপনার ডেটা সুরক্ষা কৌশল শেখার রোডম্যাপ

- ডেটা মাস্কিং ও টোকেনাইজেশন কৌশলের মধ্যে পার্থক্য করুন।
- স্টোরেজ ড্রাইভের জন্য সংরক্ষিত অবস্থায় এনক্রিপশন এবং TLS ব্যবহার করে ট্রানজিটে এনক্রিপশন বাস্তবায়ন করুন।
- র‍্যানসমওয়্যার সুরক্ষার জন্য অফলাইন, নেটওয়ার্ক-বিচ্ছিন্ন ব্যাকআপ সিস্টেম নকশা করুন।

ডেটা সুরক্ষা নির্দেশিকার নির্দেশনা

বহুনির্বাচনী ও সত্য/মিথ্যা প্রশ্নের উত্তর দিন, শব্দভাণ্ডার ব্যবহার করে শূন্যস্থান পূরণ করুন, সংজ্ঞা মেলান এবং ক্রসওয়ার্ড ও শব্দ খোঁজার ধাঁধা সমাধান করুন। ডেটা সুরক্ষা বিষয়ে আপনার জ্ঞান প্রয়োগ করুন। শেষে অতিরিক্ত কার্যক্রম দ্রুত ভাবুন সম্পন্ন করুন।

ডেটা সুরক্ষা ও এন্টারপ্রাইজ স্টোরেজ নিরাপত্তা (ভূমিকা)

ডেটা সুরক্ষা মাস্কিং, টোকেনাইজেশন, অ্যাট-রেস্ট ডেটাবেস এনক্রিপশন ও নিরাপদ ট্রানজিট প্রোটোকলের মাধ্যমে কর্পোরেট ডেটা সম্পদ রক্ষা করে। নেটওয়ার্ক-বিচ্ছিন্ন ব্যাকআপ নকশা করলে সক্রিয় অনুপ্রবেশের ঘটনায়ও গুরুত্বপূর্ণ ডেটাবেস পুনরুদ্ধার করা যায়।

প্রতিটি চেকপয়েন্ট মনোযোগ দিয়ে পড়ুন এবং সঠিক উত্তরটি বেছে নিন বা লিখুন।

চেকপয়েন্ট 1: বহুনির্বাচনী চ্যালেঞ্জ

1. ডেটা মাস্কিংয়ের প্রধান উদ্দেশ্য কী?
   - A. গোপনীয়তা রক্ষায় সংবেদনশীল শনাক্তকারীকে কাল্পনিক কিন্তু বাস্তবসদৃশ অক্ষর দিয়ে প্রতিস্থাপন করা
   - B. ফিজিক্যাল সার্ভারের স্টোরেজ স্থান বাঁচাতে বড় ডেটাবেস ফাইল কমপ্রেস করা
   - C. আর্কাইভ ব্যাকআপ সিস্টেম থেকে পুরোনো গ্রাহক যোগাযোগের ইমেইল মুছে ফেলা
   - D. ইন্টারনেট স্ক্যান থেকে ডাটাবেস সার্ভারের পাবলিক IP ঠিকানা লুকানো

2. কোন প্রক্রিয়া ডেটাবেস সার্ভারের হার্ড ড্রাইভে রাখা ফাইল এনক্রিপ্ট করে?
   - A. বিশ্রামে থাকা অবস্থায় ফুল-ডিস্ক এনক্রিপশন
   - B. ট্রানজিটে থাকা TLS সেশন হ্যান্ডশেক প্রোটোকল
   - C. ডাইনামিক DNS নেমসার্ভার ফরওয়ার্ডিং রুল
   - D. হার্ডওয়্যার কী ব্যবহার করে মাল্টি-ফ্যাক্টর প্রমাণীকরণ

3. ট্রানজিটে থাকা ডেটা কী বোঝায়?
   - A. নেটওয়ার্ক রাউটার ও সুইচের মধ্য দিয়ে চলাচলকারী ডেটা প্যাকেট
   - B. কোল্ড ব্যাকআপ ড্রাইভে সংরক্ষিত ডেটাবেস লেনদেন লগ
   - C. বিচ্ছিন্ন ক্লাউড ভল্টে সংরক্ষিত আর্কাইভ করা ব্যবহারকারীর ফাইল
   - D. স্থানীয় ডেস্কটপ স্টোরেজে স্ট্যাটিক সিস্টেম কনফিগারেশন ফাইল

4. র‍্যানসমওয়্যার থেকে সুরক্ষায় নিয়মিত অফলাইন ব্যাকআপ কেন গুরুত্বপূর্ণ?
   - A. এটি মুক্তিপণ না দিয়ে ফাইল পুনরুদ্ধারের জন্য একটি পরিষ্কার, অফলাইন কপি দেয়
   - B. এটি হ্যাকারদের খোলা পোর্ট কনফিগারেশন স্ক্যান করা প্রতিরোধ করে
   - C. এটি স্থানীয় নেটওয়ার্ক ট্রান্সমিশনের ব্যান্ডউইথ গতি বাড়ায়
   - D. এটি ব্রাউজারে কুকি সম্মতি অপ্ট-ইন লগ স্বয়ংক্রিয় করে

5. ডেটা টোকেনাইজেশন কী করে?
   - A. এটি সংবেদনশীল কার্ড নম্বরকে অসংবেদনশীল এলোমেলো টোকেন দিয়ে প্রতিস্থাপন করে
   - B. এটি একাধিক নিরাপদ onion নোডের মধ্য দিয়ে ওয়েব ট্র্যাফিক রাউট করে
   - C. এটি সিগনেচারভিত্তিক ম্যালওয়্যারের জন্য সিস্টেম ডিরেক্টরি স্ক্যান করে
   - D. এটি ডাটাবেস প্রশাসকের লগইন সেশন সময় নিরীক্ষা করে

চেকপয়েন্ট 2: সত্য বা মিথ্যা চ্যালেঞ্জ

6 প্রশ্ন 6

6. ডেটা মাস্কিং প্রোডাকশন পরিবেশে ডেটাবেস রেকর্ড স্থায়ীভাবে বদলে দেয়।

○ সত্য ○ মিথ্যা

7 প্রশ্ন 7

7. র‍্যানসমওয়্যার ছড়ানো ঠেকাতে অফসাইট ব্যাকআপ মূল কর্পোরেট নেটওয়ার্ক থেকে আলাদা রাখতে হবে।

○ সত্য ○ মিথ্যা

8 প্রশ্ন 8

8. SSL/TLS সার্টিফিকেট ফিজিক্যাল মিডিয়ায় সংরক্ষিত ডেটা এনক্রিপ্ট করে ডেটাবেস সুরক্ষিত করে।

○ সত্য ○ মিথ্যা

9 প্রশ্ন 9

9. জিরো-ট্রাস্ট নেটওয়ার্ক অ্যাক্সেস (ZTNA) ডেটাবেস অ্যাক্সেস দেওয়ার আগে প্রতিটি ব্যবহারকারীর পরিচয় যাচাই করে।

○ সত্য ○ মিথ্যা

10 প্রশ্ন 10

10. ভল্ট-ভিত্তিক টোকেনাইজেশন মূল কার্ড মানগুলো একটি নিরাপদ, কেন্দ্রীয় টোকেন ভল্টে সংরক্ষণ করে।

○ সত্য ○ মিথ্যা

চেকপয়েন্ট 3: মূল পরিভাষা বসানো

নিচের প্রতিটি বাক্য পড়ুন এবং ওয়ার্ড ব্যাংক থেকে সঠিক শব্দ দিয়ে শূন্যস্থান পূরণ করুন।

1. ব্যক্তিগত নামের জায়গায় বাস্তবসম্মত প্লেসহোল্ডার বসানোকে বলা হয় ডেটা _____ ।
2. ভৌত স্টোরেজ ব্লক এনক্রিপ্ট করলে ডেটাবেস সম্পদ সুরক্ষিত থাকে _____ অবস্থায়।
3. TLS প্রোটোকল সক্রিয় ডেটা প্যাকেটকে এনক্রিপ্ট করে, যা _____ রয়েছে।
4. ভূমিকা-ভিত্তিক অনুমতি ঠিক করে কোন ব্যবহারকারীরা ডেটাবেসে _____ পেতে পারে।
5. লঙ্ঘনের পর পরিষ্কার কর্পোরেট ফাইল পুনরুদ্ধারে প্রয়োজন একটি নিরাপদ অফলাইন _____ ।
6. ক্লাউড কনফিগারেশন অডিট করলে একটি প্রতিষ্ঠানের নিরাপত্তা _____ মূল্যায়ন করা হয়।

পরিভাষা শব্দভাণ্ডার

অবস্থান | চলাচলের মধ্যে | ডেটা লঙ্ঘন | প্রবেশাধিকার | ব্যাকআপ | মাস্কিং | সম্মতি | স্থির

এখানে আপনার উত্তর লিখুন:

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

চেকপয়েন্ট 4: নিরাপত্তা ধারণা মিলান

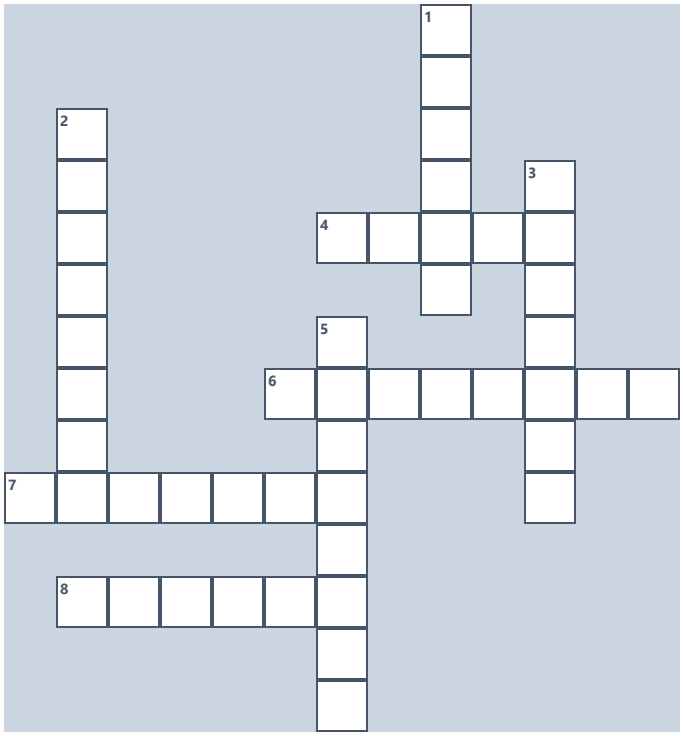
সংজ্ঞা মেলানো

পূরণযোগ্য ইনপুট বক্সে সংশ্লিষ্ট অক্ষর (A-H) লিখে বামদিকের প্রতিটি শব্দভাণ্ডার-পদকে ডানদিকের সঠিক সংজ্ঞার সঙ্গে মেলান।

☐	**1. এনক্রিপশন**	**A**	সিস্টেম ব্যর্থতার ক্ষেত্রে পুনরুদ্ধারের জন্য ডেটার নিরাপদ অফসাইট কপি তৈরি করা।
☐	**2. ব্যাকআপ**	**B**	প্লেইনটেক্সটকে পড়ার অযোগ্য সাইফারটেক্সটে রূপান্তর করা, যাতে আটকে নেওয়া ডেটা গোপন থাকে।
☐	**3. ন্যূনতমকরণ**	**C**	একটি প্রতিষ্ঠানের ক্লাউডের সামগ্রিক নিরাপত্তা অবস্থা ও প্রতিরক্ষা প্রস্তুতি।
☐	**4. অ্যাক্সেস**	**D**	ব্যক্তিগত ব্যবহারকারীর তথ্য পরিচালনায় GDPR বা CCPA-র মতো নিয়ন্ত্রক মান পূরণ করা।
☐	**5. পোস্চার**	**E**	এমন নিরাপত্তা ঘটনা যেখানে সুরক্ষিত ডেটায় অনুমতি ছাড়া প্রবেশ বা তা প্রকাশ করা হয়।
☐	**6. নিরাপত্তা লঙ্ঘন**	**F**	ডেটাবেসের পড়া ও লেখার অনুমতি অথেনটিকেটেড ব্যবহারকারী ভূমিকায় সীমিত করা।
☐	**7. সম্মতি**	**G**	ব্যক্তিগত পরিচয় সুরক্ষিত রাখতে ডেটাবেসের ফিল্ডে সংবেদনশীল অক্ষর প্রতিস্থাপন করা।
☐	**8. মাস্কিং**	**H**	কার্যক্রমের জন্য একেবারে প্রয়োজনীয় ন্যূনতম পর্যন্ত ব্যক্তিগত তথ্য সংগ্রহ সীমিত রাখা।

চেকপয়েন্ট 5: ক্রসওয়ার্ড ধাঁধা

সক্রিয় সাদা ঘরে অক্ষর লিখে ক্রসওয়ার্ড পাজল সমাধান করুন। সংখ্যাগুলো নিচের সূত্রের সঙ্গে মেলে।



পাশাপাশি

4. অনুমতি ছাড়া সুরক্ষিত ডেটায় প্রবেশ বা প্রকাশের নিরাপত্তা-ঘটনা (5)

6. ব্যক্তিগত পরিচয় রক্ষায় ডেটাবেস ক্ষেত্রের সংবেদনশীল অক্ষর প্রতিস্থাপন (8)

7. প্রতিষ্ঠানের ক্লাউডের সামগ্রিক নিরাপত্তা-অবস্থা ও প্রতিরক্ষা-প্রস্তুতি (7)

8. সিস্টেম বিকল হলে পুনরুদ্ধারের জন্য নিরাপদ অফসাইট কপি তৈরি (6)

উপর-নিচ

1. ব্যক্তিগত ব্যবহারকারী-তথ্য পরিচালনায় GDPR বা CCPA-র মতো নিয়ন্ত্রক মান পূরণ (6)

2. প্রমাণীকৃত ব্যবহারকারী-ভূমিকায় ডেটাবেস পড়া-লেখার অনুমতি সীমিত করা (8)

3. কার্যক্রমের জন্য ন্যূনতম প্রয়োজনীয় পরিমাণে ব্যক্তিগত ডেটা সংগ্রহ সীমিত করা (7)

5. প্লেইনটেক্সটকে অপাঠ্য সাইফারটেক্সটে রূপান্তর, যাতে আটকানো ডেটা গোপন থাকে (8)

চেকপয়েন্ট 5, বিকল্প: সহজবোধ্য ক্রসওয়ার্ড সূত্র

স্ক্রিন-রিডার ও কিবোর্ড ব্যবহারকারীরা নিচের টেক্সট ফিল্ডে সরাসরি ক্রসওয়ার্ডের উত্তর লিখতে পারেন।

পাশাপাশি

4 পাশাপাশি: অনুমতি ছাড়া সুরক্ষিত ডেটায় প্রবেশ বা প্রকাশের নিরাপত্তা-ঘটনা (5 অক্ষর):

6 পাশাপাশি: ব্যক্তিগত পরিচয় রক্ষায় ডেটাবেস ক্ষেত্রের সংবেদনশীল অক্ষর প্রতিস্থাপন (8 অক্ষর):

7 পাশাপাশি: প্রতিষ্ঠানের ক্লাউডের সামগ্রিক নিরাপত্তা-অবস্থা ও প্রতিরক্ষা-প্রস্তুতি (7 অক্ষর):

8 পাশাপাশি: সিস্টেম বিকল হলে পুনরুদ্ধারের জন্য নিরাপদ অফসাইট কপি তৈরি (6 অক্ষর):

উপর-নিচ

1 উপর-নিচ: ব্যক্তিগত ব্যবহারকারী-তথ্য পরিচালনায় GDPR বা CCPA-র মতো নিয়ন্ত্রক মান পূরণ (6 অক্ষর):

2 উপর-নিচ: প্রমাণীকৃত ব্যবহারকারী-ভূমিকায় ডেটাবেস পড়া-লেখার অনুমতি সীমিত করা (8 অক্ষর):

3 উপর-নিচ: কার্যক্রমের জন্য ন্যূনতম প্রয়োজনীয় পরিমাণে ব্যক্তিগত ডেটা সংগ্রহ সীমিত করা (7 অক্ষর):

5 উপর-নিচ: প্লেইনটেক্সটকে অপাঠ্য সাইফারটেক্সটে রূপান্তর, যাতে আটকানো ডেটা গোপন থাকে (8 অক্ষর):

চেকপয়েন্ট 6: লুকানো শব্দ খোঁজা

নিচের গ্রিডে লুকানো ৪টি মূল শব্দভাণ্ডারের শব্দ খুঁজুন। শব্দগুলো অনুভূমিক, উল্লম্ব বা কোণাকুণি হতে পারে।

তে না নে ছ য প উ অ উ ঋ মা বা য ফ বা
ম দে তি ভ ঘ রে ষ ফ ন্যূ ঘ দ হ স ভ রি
মি ঢ ষ ষ রি সি না তি তা ন ড ঊ নি রা কি
থ সে ন স্থা ব অ ক্ষা র সু ঊ ত লি গ নি জা
ণ ন পি ঋ জি ডে লি ট প ভ ণ ম জে গ স
র ঙ্ঘ ঘ রে দি টা মি ডে ঋ আ পা উ ক অ জে
ক ল কা গ ম এ আ ঘ টা কি ক ঘ ঝ র ণ
ল টা ধ গ সি ন রি শ ছ প্র দ ব্যা সে জি ণ
ড়া ডে নি ঝ রে ক্রি পে জ আ আ বে রে টা মা স
আ মে তি দে রি প নি ফ সি তি সে শা খ ডে স
টা বে উ ট সে শ য় দি দা প আ সি ধি জে বি
ডে বি য ড দ ন ম ষ সা ফ ল ল তা কা কে
ণ রা রি ণ জে ই পা কে পে ঠ পি ঊ বে সে র
বে উ ণ ল জে ঢ ল ফ কি মে কা দা ঋ ল জে
বে ঠ বি কে লে পা ন ম পি মি উ কা লা তা ল

পরিভাষা শব্দতালিকা

ডেটাএনক্রিপশন ডেটাব্যাকআপ ন্যূনতমকরণ ডেটাপ্রবেশাধিকার সুরক্ষাঅবস্থান
ডেটালঙ্ঘন নিয়মপালন ডেটাআড়ালকরণ

চেকপয়েন্ট 6, বিকল্প: সহজবোধ্য শব্দভাণ্ডার মিলান

ফাঁকা জায়গায় অক্ষর (A-H) লিখে ওয়ার্ড সার্চের ৪টি শব্দভাণ্ডার-পদের প্রতিটিকে তার সঠিক সংজ্ঞার সঙ্গে মেলান।

পরিভাষা

A. ডেটাএনক্রিপশন

B. ডেটাব্যাকআপ

C. ন্যূনতমকরণ

D. ডেটাপ্রবেশাধিকার

E. সুরক্ষাঅবস্থান

F. ডেটালঙ্ঘন

G. নিয়মপালন

H. ডেটাআড়ালকরণ

সংজ্ঞা ও মিলের ঘর

1. অনুমতি ছাড়া সুরক্ষিত ডেটায় প্রবেশ বা প্রকাশের নিরাপত্তা-ঘটনা।

2. ব্যক্তিগত পরিচয় রক্ষায় ডেটাবেস ক্ষেত্রের সংবেদনশীল অক্ষর প্রতিস্থাপন।

3. প্রমাণীকৃত ব্যবহারকারী-ভূমিকায় ডেটাবেস পড়া-লেখার অনুমতি সীমিত করা।

4. প্রতিষ্ঠানের ক্লাউডের সামগ্রিক নিরাপত্তা-অবস্থা ও প্রতিরক্ষা-প্রস্তুতি।

5. ব্যক্তিগত ব্যবহারকারী-তথ্য পরিচালনায় GDPR বা CCPA-র মতো নিয়ন্ত্রক মান পূরণ।

6. কার্যক্রমের জন্য ন্যূনতম প্রয়োজনীয় পরিমাণে ব্যক্তিগত ডেটা সংগ্রহ সীমিত করা।

7. প্লেইনটেক্সটকে অপাঠ্য সাইফারটেক্সটে রূপান্তর, যাতে আটকানো ডেটা গোপন থাকে।

8. সিস্টেম বিকল হলে পুনরুদ্ধারের জন্য নিরাপদ অফসাইট কপি তৈরি।

চেকপয়েন্ট 7: এলোমেলো শব্দ চ্যালেঞ্জ

সাইবার নিরাপত্তার মূল ধারণা ও পরিভাষা জানতে নিচের অক্ষরগুলো সাজান। উত্তর দেওয়া ইনপুট বাক্সে লিখুন।

1. শনক্রিডেপটানএ
2. ন্যূতণরকমন
3. অসুবনক্ষাস্থার
4. নপামলনিয়
5. কব্যাপডেআটা
6. কারবেধিডেশাটাপ্র
7. ঙঘনডেলটা
8. ড়াটালণডেরকআ

অতিরিক্ত কার্যক্রম: দ্রুত ভাবুন

প্রতিটি বিভাগে ৩টি উত্তর। যে প্রথমে তালিকা পূরণ করবে, সে জিতবে।

1	যা যা আপনি ব্যাকআপ করেন			
2	সাইবার নিরাপত্তার সঙ্গে সম্পর্কিত শব্দ			
3	সংবেদনশীল ডেটা দেখার অনুমতিপ্রাপ্ত ব্যক্তি			
4	নিরাপদে ডেটা মুছে ফেলার উপায়			
5	যেসব জায়গায় ডেটা সংরক্ষিত থাকে			
6	যেসব জিনিস এনক্রিপ্ট করা উচিত			
7	একটি হাসপাতালকে যে ডেটা সুরক্ষিত রাখতে হয়			
8	ব্যাকআপের ধরন			
9	যে তথ্য আপনার কখনো শেয়ার করা উচিত নয়			
10	ইমেইলে সতর্কতার লক্ষণ			
11	যেসব নিরাপদ অভ্যাস আপনি আজই শুরু করতে পারেন			
12	IT সাহায্যের জন্য আপনি যাদের জিজ্ঞাসা করতে পারেন			
13	যেসব ডিভাইস হ্যাক হতে পারে			
14	ডেটা সুরক্ষার উপায়			
15	যেসব জিনিস ডেটা নষ্ট করে দিতে পারে			

চেকপয়েন্ট 8: সাইবার নিরাপত্তা কেস স্টাডি

নিচের বাস্তব পরিস্থিতিগুলো সমাধান করতে শেখা ধারণাগুলো প্রয়োগ করুন।

কেস স্টাডি 1: এন্টারপ্রাইজ ডাটাবেস অ্যাট-রেস্ট এনক্রিপশন আপগ্রেড

👷

পরিস্থিতি: একটি অনলাইন খুচরা বিক্রেতা পূর্ণ ডিস্ক এনক্রিপশন ছাড়াই ক্লাউড স্টোরেজে লেনদেনের ডেটাবেস রাখে। একটি সাম্প্রতিক কমপ্লায়েন্স অডিট এটিকে গুরুতর CCPA ডেটা-নিরাপত্তা ঝুঁকি হিসেবে চিহ্নিত করেছে। একটি পুনরুদ্ধার স্থাপত্য পরিকল্পনা করুন।

আলোচনার প্রশ্ন: CCPA কমপ্লায়েন্স ঝুঁকিগুলো বিশ্লেষণ করুন এবং একটি অ্যাট-রেস্ট এনক্রিপশন কৌশলের প্রস্তাব করুন।

কেস স্টাডি 2: র‍্যানসমওয়্যার নিয়ন্ত্রণ ও ডেটা পুনরুদ্ধার

👷

পরিস্থিতি: একটি সক্রিয় র‍্যানসমওয়্যার আক্রমণ একটি কর্পোরেট লোকাল নেটওয়ার্কের নেটওয়ার্ক ড্রাইভ এনক্রিপ্ট করছে। অ্যাডমিনিস্ট্রেটর সংক্রমণ আগেভাগেই শনাক্ত করেছেন। নিয়ন্ত্রণ ও পুনরুদ্ধারের ধাপগুলো পরিকল্পনা করুন।

আলোচনার প্রশ্ন: তাৎক্ষণিক নিয়ন্ত্রণমূলক পদক্ষেপগুলো বিস্তারিত বর্ণনা করুন এবং একটি নিরাপদ পুনরুদ্ধার প্রক্রিয়ার পরিকল্পনা করুন।

চেকপয়েন্ট 9: সংকেতবার্তা ডিকোড করুন

একজন সাইবার নিরাপত্তা পেশাজীবী অনলাইন হুমকিদাতাদের হাত থেকে নেটওয়ার্ক সম্পদ রক্ষা করেন। নিচের অক্ষর-থেকে-সংখ্যা কী ব্যবহার করে ফাঁকা ঘরে মিলে যাওয়া অক্ষর লিখে বার্তাটি ডিক্রিপ্ট করুন।

অক্ষর-থেকে-সংখ্যা এনক্রিপশন কী

অ=1 আ=2 ই=3 ঈ=4 উ=5 ঊ=6 ঋ=7 এ=8 ঐ=9 ও=10 ঔ=11 ক=12

খ=13 গ=14 ঘ=15 ঙ=16 চ=17 ছ=18 জ=19 ঝ=20 ঞ=21 ট=22 ঠ=23 ড=24

ঢ=25 ণ=26 ত=27 থ=28 দ=29 ধ=30 ন=31 প=32 ফ=33 ব=34 ভ=35 ম=36

য=37 র=38 ল=39 শ=40 ষ=41 স=42 হ=43 ৎ=44 া=45 ি=46 ী=47 ু=48

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

31	46	38	45	32	29		31	46	37	59	31	58	27	58	38	26	51

34	58	37	12	58	27	46	14	27		24	51	22	45		38	12	58	41	45

ডিকোড করা বার্তা:

পরামর্শ: প্রতিটি সংখ্যা বর্ণমালায় সেই অক্ষরের অবস্থান বোঝায় (যেমন 1 = অ, 2 = আ, 63 = ়)।

চেকপয়েন্ট 10: মৌলিক সাইবার নিরাপত্তা FAQ (অংশ A)

অনলাইন হুমকি প্রশমন নিয়ে প্রচলিত প্রশ্ন ও উত্তরগুলো দেখে নিন।

Q1: ডেটা সুরক্ষা কী?

এটি প্রযুক্তিগত নিয়ন্ত্রণের মাধ্যমে ব্যক্তিগত ও ব্যবসায়িক ডেটা অননুমোদিত অ্যাক্সেস, ক্ষতি বা বিকৃতি থেকে সুরক্ষিত রাখার প্রক্রিয়া।

Q2: ফুল-ডিস্ক এনক্রিপশন কেন গুরুত্বপূর্ণ?

এটি ভৌত ড্রাইভে সংরক্ষিত ডেটা ব্লক সুরক্ষিত করে, ফলে কেউ হার্ড ড্রাইভ চুরি করলেও ডেটা পড়তে পারে না।

Q3: সংরক্ষিত অবস্থায় ও স্থানান্তরকালীন এনক্রিপশনের মধ্যে পার্থক্য কী?

অ্যাট-রেস্ট এনক্রিপশন ড্রাইভে সংরক্ষিত ফাইল সুরক্ষিত করে, আর ইন-ট্রানজিট এনক্রিপশন রাউটারের মধ্য দিয়ে চলমান সক্রিয় নেটওয়ার্ক প্যাকেট সুরক্ষিত করে।

Q4: ডেটা মাস্কিং কী?

এটি সংবেদনশীল তথ্য (যেমন ক্রেডিট কার্ড নম্বর) কাল্পনিক কিন্তু বাস্তবসম্মত ডেটা দিয়ে প্রতিস্থাপন করে, ফলে আসল রেকর্ড প্রকাশ না করেই পরীক্ষা করা যায়।

Q5: অফলাইন ব্যাকআপ কেন গুরুত্বপূর্ণ?

এটি আপনার ফাইলের একটি পরিষ্কার কপি নেটওয়ার্ক থেকে বিচ্ছিন্ন রাখে, যা র‍্যানসমওয়্যার দ্বারা আপনার ব্যাকআপ এনক্রিপ্ট হওয়া থেকে রক্ষা করতে সাহায্য করে।

চেকপয়েন্ট 10: মৌলিক সাইবার নিরাপত্তা FAQ (অংশ B)

অনলাইন হুমকি প্রশমন নিয়ে প্রচলিত প্রশ্ন ও উত্তরগুলো দেখে নিন।

Q6: ডেটা টোকেনাইজেশন ভল্ট কী?

এলোমেলো টোকেনকে তাদের মূল সংবেদনশীল মানের (যেমন প্রাথমিক ক্রেডিট কার্ড নম্বর) সঙ্গে ম্যাপ করা একটি নিরাপদ, বিচ্ছিন্ন ডেটাবেস।

Q7: জিরো-ট্রাস্ট ডেটাবেস অ্যাক্সেস বলতে কী বোঝায়?

এর অর্থ, নেটওয়ার্কের ভেতরের কাউকে বিশ্বাস করার পরিবর্তে প্রতিটি লগইনে প্রতিটি ব্যবহারকারীর পরিচয় ও ডিভাইসের অবস্থা যাচাই করা।

Q8: TLS কীভাবে স্থানান্তরকালীন ডেটা সুরক্ষিত রাখে?

TLS TCP সেশনের পেলোড এনক্রিপ্ট করে, ফলে পাবলিক নেটওয়ার্কে থাকা ক্ষতিকর ব্যক্তিরা ট্রানজিটে থাকা প্যাকেট স্নিফ বা পরিবর্তন করতে পারে না।

Q9: ডেটাবেস অ্যাক্সেস অডিটিং কী?

অননুমোদিত অ্যাক্সেসের ধরন বা নিরাপত্তার অসংগতি শনাক্ত করতে ডেটাবেস কোয়েরি ও লগইনের ধারাবাহিক রেকর্ড রাখা।

Q10: ক্লাউড নিরাপত্তা পোস্চার অডিট কী?

ক্লাউড কনফিগারেশন বিশ্লেষণ করে খোলা পোর্ট, ভুলভাবে কনফিগার করা অ্যাক্সেস নিয়ম ও নিরাপত্তা কমপ্লায়েন্সের ফাঁক শনাক্ত করার প্রক্রিয়া।

চেকপয়েন্ট 10: উন্নত নিরাপত্তা FAQ (অংশ C)

নিরাপত্তা কাঠামো, ম্যালওয়্যার বিশ্লেষণ ও ডেটা সম্মতির উন্নত প্রযুক্তিগত দিক অন্বেষণ করুন।

Q1: এনভেলপ এনক্রিপশন কীভাবে কাজ করে?

এটি একটি ডেটা কী দিয়ে ডেটা এনক্রিপ্ট করে, তারপর সেই ডেটা কী একটি মাস্টার কী দিয়ে এনক্রিপ্ট করে, ফলে কী সংরক্ষণ ও রোটেশন সহজ হয়।

Q2: হোমোমরফিক এনক্রিপশন কী?

একটি উন্নত এনক্রিপশন পদ্ধতি, যা ডিক্রিপ্ট না করেই এনক্রিপ্টেড ডেটার ওপর সরাসরি কার্যক্রম চালানোর সুযোগ দেয়।

Q3: ডেটাবেসে কলাম-স্তরের এনক্রিপশন কেন ব্যবহার করা হয়?

এটি নির্দিষ্ট সংবেদনশীল কলাম (যেমন SSN) আলাদাভাবে এনক্রিপ্ট করে, ফলে অ্যাডমিনরা সাধারণ টেবিল পড়ার অ্যাক্সেস পেলেও সেগুলো সুরক্ষিত থাকে।

Q4: ডেটা লস প্রিভেনশন (DLP) কী?

সংবেদনশীল ফাইলের অননুমোদিত বহির্গামী স্থানান্তর শনাক্ত ও ব্লক করতে নেটওয়ার্ক এগ্রেস পয়েন্ট পর্যবেক্ষণকারী সফটওয়্যার।

Q5: রাইট-ওয়ান্স-রিড-মেনি (WORM) ব্যাকআপ কীভাবে র‍্যানসমওয়্যার থেকে সুরক্ষা দেয়?

WORM ব্যাকআপ একটি নির্দিষ্ট সময়ের জন্য ফাইল মুছে ফেলা বা পরিবর্তন করা রোধ করে, ফলে র‍্যানসমওয়্যার বিদ্যমান ব্যাকআপ এনক্রিপ্ট করতে পারে না।

চেকপয়েন্ট 10: উন্নত নিরাপত্তা FAQ (অংশ D)

নিরাপত্তা কাঠামো, ম্যালওয়্যার বিশ্লেষণ ও ডেটা সম্মতির উন্নত প্রযুক্তিগত দিক অন্বেষণ করুন।

Q6: কী পুনরায় ব্যবহারের ঝুঁকি কী?

বিভিন্ন ডেটাবেসে একই ক্রিপ্টোগ্রাফিক কী পুনর্ব্যবহার করলে একটি কী আপস হলেই সব ডেটাবেস উন্মুক্ত হয়ে যায়।

Q7: ডেটাবেস টোকেনাইজেশন কীভাবে CCPA কমপ্লায়েন্স উন্নত করে?

টোকেন নন-প্রোডাকশন সিস্টেমে রেকর্ডকে ছদ্মনামে রূপান্তর করে এবং ডেটা ফাঁসের ঝুঁকি সীমিত করে, তবে টোকেনাইজড ডেটাও ব্যক্তিগত তথ্য হতে পারে।

Q8: ডেটা শ্রেণিবিন্যাস কেন গুরুত্বপূর্ণ?

এটি ফাইলগুলোকে সংবেদনশীলতার স্তর অনুযায়ী শ্রেণিবদ্ধ করে, ফলে প্রতিষ্ঠানগুলো উচ্চ-ঝুঁকির ডেটায় সবচেয়ে শক্তিশালী এনক্রিপশন ও অ্যাক্সেস নিয়ন্ত্রণ প্রয়োগ করতে পারে।

Q9: কী রোটেশনের ভূমিকা কী?

এনক্রিপশন কী নিয়মিত হালনাগাদ করলে কোনো একটি কী শেষ পর্যন্ত ভেঙে গেলেও ঐতিহাসিক ডেটার যতটুকু উন্মুক্ত হয় তা সীমিত থাকে।

Q10: সিকিউর এনক্লেভ কীভাবে মেমরিতে ডেটাবেস কোয়েরি সুরক্ষিত রাখে?

সিকিউর এনক্লেভ CPU-সুরক্ষিত মেমোরি ব্লকে কোয়েরি অপারেশন আলাদা করে রাখে, ফলে হোস্ট অ্যাডমিনিস্ট্রেটররা RAM-এ ক্লিয়ারটেক্সট দেখতে পারেন না।

অংশ 11: 10টি বাস্তব সাইবার নিরাপত্তা তথ্য ও অন্তর্দৃষ্টি

নিরাপত্তা লঙ্ঘন, প্রতিরক্ষা কৌশল ও সম্মতির মান সম্পর্কে বাস্তব তথ্য দেখে নিন।

1. নিরাপত্তা ইনসাইট

GDPR বিধিমালা 2018 সালের মে মাসে কার্যকর হয়, যা বিশ্বজুড়ে ওয়েবসাইটের কুকি সম্মতি ও ব্যক্তিগত তথ্যের রেজিস্ট্রি পরিচালনার ধরন বদলে দেয়।

2. নিরাপত্তা ইনসাইট

GDPR লঙ্ঘনের জরিমানা 20 মিলিয়ন ইউরো বা বৈশ্বিক টার্নওভারের 4% পর্যন্ত হতে পারে, যা উল্লেখযোগ্য আইনি ঝুঁকি নির্দেশ করে। [4]

3. নিরাপত্তা ইনসাইট

CCPA 2020 সালের জানুয়ারিতে কার্যকর হয়, যা যুক্তরাষ্ট্রে ডিজিটাল গোপনীয়তা বিষয়ে ভোক্তা অধিকারের পথিকৃৎ।

4. নিরাপত্তা ইনসাইট

ডেটা মিনিমাইজেশন ডেটাবেসের স্টোরেজ আকার কমায়, সার্ভার পরিচালনার খরচ কমায় এবং ব্রিচের প্রভাবের মাত্রাও কমায়।

5. নিরাপত্তা ইনসাইট

ক্রিপ্টোগ্রাফিক শ্রেডিং ঐতিহাসিক ব্যাকআপ টেপ ফাইল সম্পাদনার বদলে কী মুছে ফেলার মাধ্যমে ব্যাকআপ মুছে ফেলার চ্যালেঞ্জ সমাধান করে।

6. নিরাপত্তা ইনসাইট

ভোক্তার গোপনীয়তার অধিকার রক্ষায় বিশ্বের বেশিরভাগ দেশ এখন ব্যক্তিগত তথ্য সুরক্ষা আইন প্রণয়ন করেছে।

7. সিকিউরিটি ইনসাইট

ইউরোপীয় ডেটা গোপনীয়তা নিয়ন্ত্রক সংজ্ঞায় আগে থেকে টিক দেওয়া বাক্সসহ অপ্ট-ইন সম্মতি ফর্ম স্পষ্টভাবে নিষিদ্ধ।

8. সিকিউরিটি ইনসাইট

GDPR অনুযায়ী ব্যক্তিগত তথ্য ফাঁসের ঘটনা জানার পর সম্ভব হলে 72 ঘণ্টার মধ্যে তদারকি কর্তৃপক্ষকে জানাতে হয়। [3]

9. সিকিউরিটি ইনসাইট

bcrypt বা Argon2-এর মতো ধীর অ্যালগরিদমে পাসওয়ার্ড হ্যাশ করলে চুরি হওয়া হ্যাশের অফলাইন ক্র্যাকিং অনেক কঠিন হয়। [6]

10. নিরাপত্তা ইনসাইট

অ্যাট-রেস্ট ডেটা মানে সংরক্ষিত ডেটাবেস ফাইল, আর ইন-ট্রানজিট ডেটা মানে নেটওয়ার্ক রাউটারের মধ্য দিয়ে সক্রিয়ভাবে চলমান প্যাকেট।

প্রযুক্তিগত তথ্যসূত্র ও উৎস

স্টাডি গাইড ও ইন্টারঅ্যাক্টিভ ধাঁধাগুলো বৈশ্বিক NIST, OWASP এবং ডেটা গোপনীয়তা সম্মতির মানদণ্ড থেকে সংকলিত।

গবেষণামূলক ও শিল্পক্ষেত্রের তথ্যসূত্র

[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

উত্তরমালা: চেকপয়েন্ট 1 – বহুনির্বাচনী

1 প্রশ্ন 1

সঠিক উত্তর: A

শিক্ষণ নোট

ডেটা মাস্কিংয়ের প্রধান উদ্দেশ্য কী? → গোপনীয়তা রক্ষায় সংবেদনশীল শনাক্তকারীকে কাল্পনিক কিন্তু বাস্তবসদৃশ অক্ষর দিয়ে প্রতিস্থাপন করা

2 প্রশ্ন 2

সঠিক উত্তর: A

শিক্ষণ নোট

কোন প্রক্রিয়া ডেটাবেস সার্ভারের হার্ড ড্রাইভে রাখা ফাইল এনক্রিপ্ট করে? → বিশ্রামে থাকা অবস্থায় ফুল-ডিস্ক এনক্রিপশন

3 প্রশ্ন 3

সঠিক উত্তর: A

শিক্ষণ নোট

ট্রানজিটে থাকা ডেটা কী বোঝায়? → নেটওয়ার্ক রাউটার ও সুইচের মধ্য দিয়ে চলাচলকারী ডেটা প্যাকেট

4 প্রশ্ন 4

সঠিক উত্তর: A

শিক্ষণ নোট

র‍্যানসমওয়্যার থেকে সুরক্ষায় নিয়মিত অফলাইন ব্যাকআপ কেন গুরুত্বপূর্ণ? → এটি মুক্তিপণ না দিয়ে ফাইল পুনরুদ্ধারের জন্য একটি পরিষ্কার, অফলাইন কপি দেয়

5 প্রশ্ন 5

সঠিক উত্তর: A

শিক্ষণ নোট

ডেটা টোকেনাইজেশন কী করে? → এটি সংবেদনশীল কার্ড নম্বরকে অসংবেদনশীল এলোমেলো টোকেন দিয়ে প্রতিস্থাপন করে

উত্তরমালা: চেকপয়েন্ট 2 – সত্য বা মিথ্যা

6 প্রশ্ন 6 — সঠিক উত্তর: মিথ্যা

শিক্ষণ নোট

মাস্কিং টেস্ট কপি বদলে দেয় বা কোয়েরির সময় মান লুকায়; প্রোডাকশন রেকর্ড অপরিবর্তিত থাকে।

7 প্রশ্ন 7 — সঠিক উত্তর: সত্য

শিক্ষণ নোট

র‍্যানসমওয়্যার ছড়ানো ঠেকাতে অফসাইট ব্যাকআপ মূল কর্পোরেট নেটওয়ার্ক থেকে আলাদা রাখতে হবে।

8 প্রশ্ন 8 — সঠিক উত্তর: মিথ্যা

শিক্ষণ নোট

TLS সার্টিফিকেট ট্রানজিটে থাকা ডেটা সুরক্ষিত করে; স্থির অবস্থায় থাকা ডেটার জন্য ডিস্ক, ফাইল বা ডেটাবেস এনক্রিপশন লাগে।

9 প্রশ্ন 9 — সঠিক উত্তর: সত্য

শিক্ষণ নোট

জিরো-ট্রাস্ট নেটওয়ার্ক অ্যাক্সেস (ZTNA) ডেটাবেস অ্যাক্সেস দেওয়ার আগে প্রতিটি ব্যবহারকারীর পরিচয় যাচাই করে।

10 প্রশ্ন 10 — সঠিক উত্তর: সত্য

শিক্ষণ নোট

ভল্ট-ভিত্তিক টোকেনাইজেশন মূল মানগুলো একটি নিরাপদ টোকেন ভল্টে রাখে, যা প্রতিটি টোকেনকে তার ডেটার সঙ্গে মেলায়।

শব্দভাণ্ডারের উত্তরমালা ও মূল্যায়ন রুব্রিক

শিক্ষকের মূল্যায়ন রুব্রিক: প্রতিটি সঠিক মিলের জন্য (মোট ৪ নম্বর) এবং প্রসঙ্গ পরিভাষার জন্য (মোট 6 নম্বর) 1 নম্বর দিন।

চেকপয়েন্ট 4: উত্তর – ধারণা মিলান

B 1. এনক্রিপশন	A 2. ব্যাকআপ	H 3. ন্যূনতমকরণ	F 4. অ্যাক্সেস
C 5. পোস্‌চার	E 6. নিরাপত্তা লঙ্ঘন	D 7. সম্মতি	G 8. মাস্কিং

চেকপয়েন্ট 3: উত্তর – মূল পরিভাষা

1 মাস্কিং	2 স্থির	3 চলাচলের মধ্যে	4 প্রবেশাধিকার
5 ব্যাকআপ	6 অবস্থান		

চেকপয়েন্ট 6, বিকল্প: উত্তর – শব্দ মিলান

1 F – ডেটালঙ্ঘন	2 H – ডেটাআড়ালকরণ	3 D – ডেটাপ্রবেশাধিকার	4 E – সুরক্ষাঅবস্থান
5 G – নিয়মপালন	6 C – ন্যূনতমকরণ	7 A – ডেটাএনক্রিপশন	8 B – ডেটাব্যাকআপ

শিক্ষকদের জন্য আলোচনা নোট

মূল পরিভাষা:
যাচাই করুন শিক্ষার্থীরা এনক্রিপশন, ব্যাকআপ ও ন্যূনতমকরণ নিজের ভাষায় ব্যাখ্যা করতে এবং প্রতিটির একটি উদাহরণ দিতে পারে কি না।

কেস স্টাডি:
শিক্ষার্থীদের বলুন তারা যেন মতামতের বদলে ওয়ার্কশিটের তথ্যের ভিত্তিতে সুপারিশ করে।

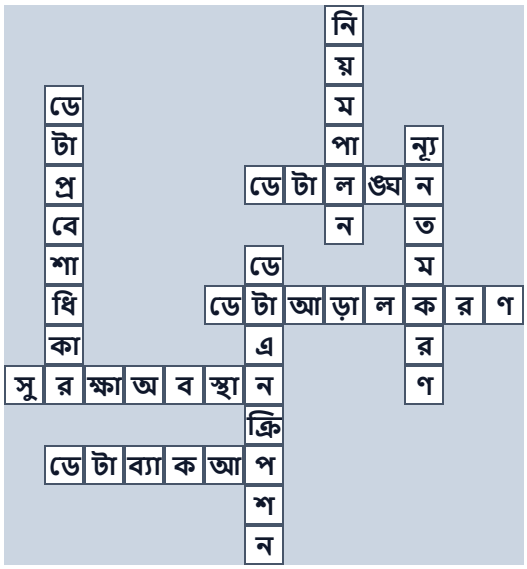
উৎস মূল্যায়ন:
শিক্ষার্থীদের ওয়ার্কশিটের উৎসে অন্তত একটি তথ্য যাচাই করতে বলুন এবং আলোচনা করুন কেন সংখ্যা, দাম ও নিয়ম সময়ের সঙ্গে বদলাতে পারে।

ধাঁধার উত্তরমালা ও শিক্ষকের নোট

শব্দ খোঁজার সমাধান

তে	না	নে	ছ	য	প	উ	অ	উ	ঋ	মা	বা	য	ফ	বা
ম	দে	তি	ভ	ঘ	রে	ষ	ফ	ন্যূ	ঘ	দ	হ	স	ভ	রি
মি	ঢ	ষ	ষ	রি	সি	না	তি	তা	ন	ড	ঊ	নি	রা	কি
থ	সে	ন	স্থা	ব	অ	ক্ষা	র	সু	ঊ	ত	লি	গ	নি	জা
ণ	ন	পি	ঋ	জি	ডে	লি	ট	প	ভ	ণ	ম	জে	গ	স
র	ঙ্ঘ	ঘ	রে	দি	টা	মি	ডে	ঋ	আ	পা	উ	ক	অ	জে
ক	ল	কা	গ	ম	এ	আ	ঘ	টা	কি	ক	ঘ	ঝ	র	ণ
ল	টা	ধ	গ	সি	ন	রি	শ	ছ	প্র	দ	ব্যা	সে	জি	ণ
ড়া	ডে	নি	ঝ	রে	ক্রি	পে	জ	আ	আ	বে	রে	টা	মা	স
আ	মে	তি	দে	রি	প	নি	ফ	সি	তি	সে	শা	খ	ডে	স
টা	বে	উ	ট	সে	শ	য়	দি	দা	প	আ	সি	ধি	জে	বি
ডে	বি	য	ড	দ	ন	ম	ষ	সা	ফ	ল	ল	তা	কা	কে
ণ	রা	রি	ণ	জে	ই	পা	কে	পে	ঠ	পি	ঊ	বে	সে	র
বে	উ	ণ	ল	জে	ঢ	ল	ফ	কি	মে	কা	দা	ঋ	ল	জে
বে	ঠ	বি	কে	লে	পা	ন	ম	পি	মি	উ	কা	লা	তা	ল

ক্রসওয়ার্ডের সমাধান



ক্রসওয়ার্ড সমাধানের জন্য শিক্ষকের নির্দেশিকা

পাশাপাশি

4 পাশাপাশি: ডেটালঙ্ঘন অনুমতি ছাড়া সুরক্ষিত ডেটায় প্রবেশ বা প্রকাশের নিরাপত্তা-ঘটনা (5 অক্ষর)

6 পাশাপাশি: ডেটাআড়ালকরণ ব্যক্তিগত পরিচয় রক্ষায় ডেটাবেস ক্ষেত্রের সংবেদনশীল অক্ষর প্রতিস্থাপন (8 অক্ষর)

7 পাশাপাশি: সুরক্ষাঅবস্থান প্রতিষ্ঠানের ক্লাউডের সামগ্রিক নিরাপত্তা-অবস্থা ও প্রতিরক্ষা-প্রস্তুতি (7 অক্ষর)

8 পাশাপাশি: ডেটাব্যাকআপ সিস্টেম বিকল হলে পুনরুদ্ধারের জন্য নিরাপদ অফসাইট কপি তৈরি (6 অক্ষর)

উপর-নিচ

1 উপর-নিচ: নিয়মপালন ব্যক্তিগত ব্যবহারকারী-তথ্য পরিচালনায় GDPR বা CCPA-র মতো নিয়ন্ত্রক মান পূরণ (6 অক্ষর)

2 উপর-নিচ: ডেটাপ্রবেশাধিকার প্রমাণীকৃত ব্যবহারকারী-ভূমিকায় ডেটাবেস পড়া-লেখার অনুমতি সীমিত করা (8 অক্ষর)

3 উপর-নিচ: ন্যূনতমকরণ কার্যক্রমের জন্য ন্যূনতম প্রয়োজনীয় পরিমাণে ব্যক্তিগত ডেটা সংগ্রহ সীমিত করা (7 অক্ষর)

5 উপর-নিচ: ডেটাএনক্রিপশন প্লেইনটেক্সটকে অপাঠ্য সাইফারটেক্সটে রূপান্তর, যাতে আটকানো ডেটা গোপন থাকে (8 অক্ষর)

এলোমেলো শব্দ ও সংকেতবার্তা সমাধানের উত্তরমালা

শব্দভাণ্ডার অক্ষর-সাজানো কার্যক্রম ও Secret Cipher Challenge-এর মূল্যায়ন উত্তরমালা।

শব্দ সাজানোর উত্তরমালা

1. শনক্রিডেপটানএ — **ডেটাএনক্রিপশন**
2. ন্যূতণরকমন — **ন্যূনতমকরণ**
3. অসুবনক্ষাস্থার — **সুরক্ষাঅবস্থান**
4. নপামলনিয় — **নিয়মপালন**
5. কব্যাপডেআটা — **ডেটাব্যাকআপ**
6. কারবেধিডেশাটাপ্র — **ডেটাপ্রবেশাধিকার**
7. ঙ্ঘনডেলটা — **ডেটালঙ্ঘন**
8. ড়াটালণডেরকআ — **ডেটাআড়ালকরণ**

গোপন সংকেত চ্যালেঞ্জের উত্তরমালা

"নিরাপদ নিয়ন্ত্রণে ব্যক্তিগত ডেটা রক্ষা"

কেস স্টাডির উত্তর

A কেস স্টাডি 1: এন্টারপ্রাইজ ডাটাবেস অ্যাট-রেস্ট এনক্রিপশন আপগ্রেড

শিক্ষকের সমাধান

মূল্যায়ন নির্দেশিকা

শিক্ষার্থীদের উত্তরে নিচের বিষয়গুলো থাকা উচিত:

- পরিস্থিতি বিশ্লেষণ: একটি অনলাইন খুচরা বিক্রেতা পূর্ণ-ডিস্ক এনক্রিপশন ছাড়াই ক্লাউড স্টোরেজে লেনদেনের ডেটাবেস রাখে। সাম্প্রতিক একটি কমপ্লায়েন্স অডিটে এটিকে CCPA-র আওতায় গুরুতর ডেটা-নিরাপত্তা ঝুঁকি হিসেবে চিহ্নিত করা হয়েছে। একটি রিকভারি আর্কিটেকচার ডিজাইন করুন।
- প্রস্তাবিত কৌশল ও সমাধান: সব ফাইল সিস্টেমে অব্যবহৃত অবস্থায় AES-256 ফুল-ডিস্ক এনক্রিপশন প্রয়োগ করুন। স্বয়ংক্রিয় রোটেশনসহ একটি কেন্দ্রীভূত Key Management Service (KMS) ব্যবহার করুন এবং ডিক্রিপশনের প্রবেশাধিকার নিয়ন্ত্রণে কঠোর IAM নীতি কার্যকর করুন।

B কেস স্টাডি 2: র‍্যানসমওয়্যার নিয়ন্ত্রণ ও ডেটা পুনরুদ্ধার

শিক্ষকের সমাধান

মূল্যায়ন নির্দেশিকা

শিক্ষার্থীদের উত্তরে নিচের বিষয়গুলো থাকা উচিত:

- পরিস্থিতি বিশ্লেষণ: একটি কর্পোরেট লোকাল নেটওয়ার্কে সক্রিয় র‍্যান্সমওয়্যার আক্রমণ নেটওয়ার্ক ড্রাইভ এনক্রিপ্ট করছে। অ্যাডমিনিস্ট্রেটর সংক্রমণ শুরুতেই শনাক্ত করেছেন। নিয়ন্ত্রণ ও পুনরুদ্ধারের ধাপগুলোর পরিকল্পনা করুন।
- প্রস্তাবিত কৌশল ও সমাধান: আপসকৃত সেগমেন্ট অবিলম্বে আলাদা করুন। আক্রান্ত এন্ডপয়েন্ট ফরম্যাট করে সর্বশেষ অফলাইন write-once-read-many (WORM) ব্যাকআপ থেকে পুনরুদ্ধার করুন। সিস্টেম আবার সংযুক্ত করার আগে ব্যাকআপের অখণ্ডতা যাচাই করুন।