Họ tên: _____ Ngày: _____ Điểm: _____

Bảo vệ dữ liệu và lưu trữ doanh nghiệp Hướng dẫn bảo mật

Che giấu dữ liệu, mã hóa thành token, mã hóa khi lưu trữ so với khi truyền, sao lưu ngoại tuyến

TỔNG QUAN HỌC TẬP VỀ BẢO VỆ DỮ LIỆU

ĐÃ BẢO MẬT
MÃ HÓA DỮ LIỆU
Chuẩn AES 256 bit

TUÂN THỦ
TIÊU CHUẨN TOÀN CẦU
Khung GDPR và CCPA

ZERO TRUST
CHÍNH SÁCH TRUY CẬP
Xác thực đa yếu tố

Chào mừng bạn! Bộ hoạt động này hướng dẫn bạn về các tiêu chuẩn và biện pháp kiểm soát bảo vệ dữ liệu. Bạn sẽ khám phá mã hóa toàn bộ ổ đĩa, kiểm soát truy cập an toàn, sao lưu phần cứng, tư thế bảo mật đám mây và các kỹ thuật che giấu dữ liệu.

CÁC ĐIỂM KIỂM TRA CỦA PHIẾU HỌC TẬP

- [ ] **Phần 1-4: Nắm vững an ninh mạng và phòng chống mối đe dọa.**
- [ ] **Phần 5-7: Giải các câu đố ô chữ và tìm từ.**
- [ ] **Phần 8-9: Giải các nghiên cứu tình huống và thử thách mật thư.**
- [ ] **Phần 10: Xem lại các trang câu hỏi thường gặp cơ bản và nâng cao.**
- [ ] **Phần 11: Khám phá 10 sự thật thú vị trong thực tế.**
- [ ] **Thưởng: thử thách Nghĩ nhanh.**

Mở Hướng dẫn an ninh mạng của VPN.com

URL: https://www.vpn.com/vi/an-ninh-mang/bao-ve-du-lieu/

Lộ trình học về chiến lược bảo vệ dữ liệu của bạn

- Phân biệt kỹ thuật che giấu dữ liệu và mã hóa thành token.
- Triển khai mã hóa khi lưu trữ cho ổ đĩa lưu trữ và mã hóa khi truyền bằng TLS.
- Thiết kế hệ thống sao lưu ngoại tuyến, cách ly khỏi mạng để chống ransomware.

HƯỚNG DẪN VỀ BẢO VỆ DỮ LIỆU

Trả lời các câu hỏi trắc nghiệm và đúng/sai, hoàn thành các câu điền vào chỗ trống bằng ngân hàng từ, ghép các định nghĩa, rồi giải ô chữ và tìm từ. Hãy vận dụng kiến thức của bạn về việc bảo vệ dữ liệu. Kết thúc với hoạt động thưởng Nghĩ nhanh.

BẢO VỆ DỮ LIỆU VÀ BẢO MẬT LƯU TRỮ DOANH NGHIỆP (GIỚI THIỆU)

Bảo vệ dữ liệu giúp bảo vệ tài sản dữ liệu của doanh nghiệp thông qua che giấu dữ liệu, mã hóa thành token, mã hóa cơ sở dữ liệu khi lưu trữ và các giao thức truyền tải an toàn. Thiết kế các bản sao lưu cách ly khỏi mạng giúp đảm bảo có thể khôi phục các cơ sở dữ liệu quan trọng khi đang xảy ra xâm nhập.

ĐỌC KỸ TỪNG ĐIỂM KIỂM TRA VÀ CHỌN HOẶC VIẾT CÂU TRẢ LỜI ĐÚNG.

Điểm kiểm tra 1: Thử thách trắc nghiệm

1. Mục đích chính của việc che giấu dữ liệu (data masking) là gì?

- A. Thay các định danh nhạy cảm bằng ký tự hư cấu nhưng thực tế để bảo vệ quyền riêng tư
- B. Nén các tệp cơ sở dữ liệu lớn để tiết kiệm dung lượng lưu trữ trên máy chủ vật lý
- C. Xóa email liên hệ khách hàng cũ khỏi hệ thống sao lưu lưu trữ
- D. Ẩn địa chỉ IP công cộng của máy chủ cơ sở dữ liệu khỏi các lần quét internet

2. Cơ chế nào mã hóa các tệp lưu trên ổ cứng của máy chủ cơ sở dữ liệu?

- A. Mã hóa toàn bộ ổ đĩa khi lưu trữ
- B. Giao thức bắt tay phiên TLS khi đang truyền
- C. Quy tắc chuyển tiếp máy chủ tên miền DNS động
- D. Xác thực đa yếu tố bằng khóa phần cứng

3. Điều gì đại diện cho dữ liệu đang truyền?

- A. Các gói dữ liệu di chuyển qua router và switch mạng
- B. Nhật ký giao dịch cơ sở dữ liệu được lưu trên ổ sao lưu ngoại tuyến
- C. Tệp người dùng đã lưu trữ, được lưu trong kho đám mây cô lập
- D. Các tệp cấu hình hệ thống tĩnh trên bộ lưu trữ máy tính để bàn cục bộ

4. Vì sao bản sao lưu ngoại tuyến thường xuyên lại quan trọng để chống ransomware?

- A. Cung cấp bản sao sạch, ngoại tuyến để khôi phục tệp mà không phải trả tiền chuộc
- B. Ngăn tin tặc quét cấu hình các cổng đang mở
- C. Nó tăng tốc độ băng thông truyền tải của mạng cục bộ
- D. Nó tự động ghi nhật ký đồng ý cookie trên trình duyệt

5. Mã hóa thành token dữ liệu (data tokenization) làm gì?

- A. Thay số thẻ nhạy cảm bằng các mã thông báo ngẫu nhiên không nhạy cảm
- B. Định tuyến lưu lượng web qua nhiều nút onion an toàn
- C. Nó quét thư mục hệ thống để tìm phần mềm độc hại dựa trên chữ ký
- D. Nó kiểm toán thời gian phiên đăng nhập của quản trị viên cơ sở dữ liệu

Điểm kiểm tra 2: Thử thách Đúng hoặc Sai

6 Câu hỏi 6

6. Che giấu dữ liệu thay đổi vĩnh viễn các bản ghi cơ sở dữ liệu trên môi trường sản xuất.

○ Đúng ○ Sai

7 Câu hỏi 7

7. Bản sao lưu ngoài địa điểm phải được tách biệt khỏi mạng doanh nghiệp chính để ngăn mã độc tống tiền (ransomware) lây lan.

○ Đúng ○ Sai

8 Câu hỏi 8

8. Chứng chỉ SSL/TLS bảo mật cơ sở dữ liệu bằng cách mã hóa dữ liệu lưu trữ ở trạng thái nghỉ trên phương tiện vật lý.

○ Đúng ○ Sai

9 Câu hỏi 9

9. Truy cập mạng zero-trust (ZTNA) xác minh danh tính của từng người dùng trước khi cấp quyền truy cập cơ sở dữ liệu.

○ Đúng ○ Sai

10 Câu hỏi 10

10. Mã hóa thành token dựa trên kho lưu trữ giữ các giá trị thẻ gốc trong một kho token trung tâm an toàn.

○ Đúng ○ Sai

Điểm kiểm tra 3: Điền thuật ngữ chính

Đọc từng câu dưới đây và điền vào chỗ trống thuật ngữ đúng từ Ngân hàng từ.

1. Thay tên cá nhân bằng các giá trị giữ chỗ thực tế được gọi là _____ dữ liệu.

2. Mã hóa các khối lưu trữ vật lý bảo vệ tài sản cơ sở dữ liệu ở trạng thái _____ .

3. Các giao thức TLS mã hóa các gói dữ liệu đang hoạt động trong quá trình _____ .

4. Quyền dựa trên vai trò giới hạn những người dùng nào có thể giành được _____ cơ sở dữ liệu.

5. Khôi phục các tệp doanh nghiệp sạch sau vi phạm cần có một bản _____ ngoại tuyến an toàn.

6. Kiểm toán cấu hình đám mây đánh giá _____ của tổ chức.

NGÂN HÀNG TỪ VỰNG

CHE GIẤU SAO LƯU TĨNH TRUY CẬP TRUYỀN TẢI TUÂN THỦ
TƯ THẾ BẢO MẬT VI PHẠM DỮ LIỆU

Viết câu trả lời của bạn tại đây:

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

Điểm kiểm tra 4: Ghép nối khái niệm bảo mật

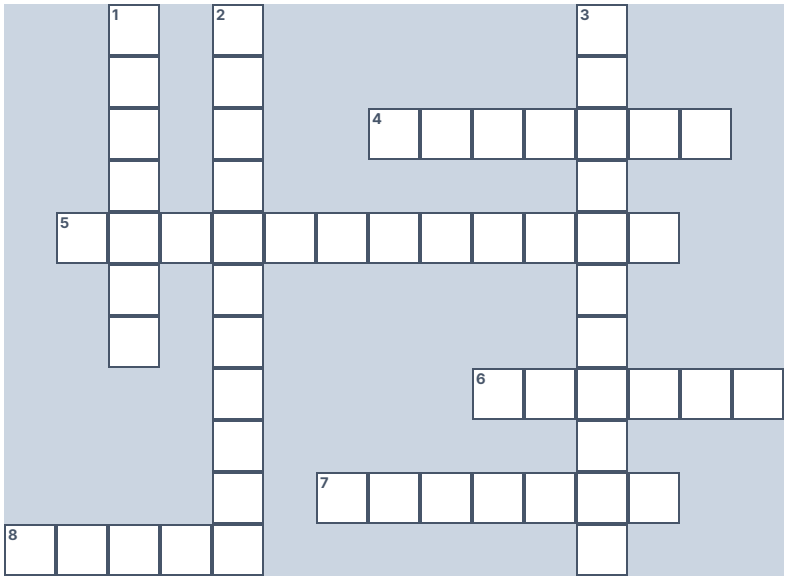
GHÉP ĐỊNH NGHĨA

Ghép mỗi thuật ngữ từ vựng ở bên trái với định nghĩa đúng ở bên phải bằng cách nhập chữ cái tương ứng (A-H) vào ô nhập liệu.

☐	1. MÃ HÓA	A	Tạo bản sao dữ liệu an toàn ở nơi khác để khôi phục khi hệ thống gặp sự cố.
☐	2. SAO LƯU	B	Biến văn bản thuần thành bản mã không đọc được để dữ liệu bị chặn bắt vẫn được giữ kín.
☐	3. TỐI THIỂU HÓA	C	Tình trạng bảo mật tổng thể và mức độ sẵn sàng phòng thủ của đám mây một tổ chức.
☐	4. TRUY CẬP	D	Đáp ứng các tiêu chuẩn quy định như GDPR hoặc CCPA khi quản lý thông tin riêng tư của người dùng.
☐	5. TƯ THẾ AN NINH	E	Sự cố bảo mật trong đó dữ liệu được bảo vệ bị truy cập hoặc tiết lộ mà không được phép.
☐	6. VI PHẠM DỮ LIỆU	F	Hạn chế quyền đọc và ghi cơ sở dữ liệu cho các vai trò người dùng đã xác thực.
☐	7. TUÂN THỦ	G	Thay thế các ký tự nhạy cảm trong các trường cơ sở dữ liệu để bảo vệ danh tính cá nhân.
☐	8. CHE GIẤU	H	Hạn chế việc thu thập dữ liệu cá nhân ở mức tối thiểu tuyệt đối cần thiết cho hoạt động.

Điểm kiểm tra 5: Trò chơi ô chữ

Giải ô chữ bằng cách nhập chữ cái vào các ô trắng đang hoạt động. Các số tương ứng với các gợi ý bên dưới.



HÀNG NGANG

4. Đáp ứng các tiêu chuẩn quy định như GDPR hoặc CCPA khi quản lý thông tin người dùng riêng tư (7)

5. Sự cố bảo mật trong đó dữ liệu được bảo vệ bị truy cập hoặc tiết lộ trái phép (12)

6. Tạo các bản sao an toàn ngoài địa điểm để khôi phục khi hệ thống gặp lỗi (6)

7. Giới hạn quyền đọc và ghi cơ sở dữ liệu cho các vai trò người dùng đã xác thực (7)

8. Biến văn bản thuần thành bản mã không đọc được để dữ liệu bị chặn bắt vẫn riêng tư (5)

HÀNG DỌC

1. Thay các ký tự nhạy cảm trong trường cơ sở dữ liệu để bảo vệ danh tính cá nhân (7)

2. Giới hạn việc thu thập dữ liệu cá nhân ở mức tối thiểu tuyệt đối cần cho hoạt động (11)

3. Trạng thái bảo mật tổng thể và mức sẵn sàng phòng vệ của đám mây của một tổ chức (11)

Điểm kiểm tra 5, phương án khác: Gợi ý ô chữ dễ tiếp cận

Người dùng trình đọc màn hình và bàn phím có thể nhập trực tiếp đáp án ô chữ vào các trường văn bản bên dưới.

HÀNG NGANG

4 hàng ngang: Đáp ứng các tiêu chuẩn quy định như GDPR hoặc CCPA khi quản lý thông tin người dùng riêng tư (7 chữ cái):

5 hàng ngang: Sự cố bảo mật trong đó dữ liệu được bảo vệ bị truy cập hoặc tiết lộ trái phép (12 chữ cái):

6 hàng ngang: Tạo các bản sao an toàn ngoài địa điểm để khôi phục khi hệ thống gặp lỗi (6 chữ cái):

7 hàng ngang: Giới hạn quyền đọc và ghi cơ sở dữ liệu cho các vai trò người dùng đã xác thực (7 chữ cái):

8 hàng ngang: Biến văn bản thuần thành bản mã không đọc được để dữ liệu bị chặn bắt vẫn riêng tư (5 chữ cái):

HÀNG DỌC

1 hàng dọc: Thay các ký tự nhạy cảm trong trường cơ sở dữ liệu để bảo vệ danh tính cá nhân (7 chữ cái):

2 hàng dọc: Giới hạn việc thu thập dữ liệu cá nhân ở mức tối thiểu tuyệt đối cần cho hoạt động (11 chữ cái):

3 hàng dọc: Trạng thái bảo mật tổng thể và mức sẵn sàng phòng vệ của đám mây của một tổ chức (11 chữ cái):

Điểm kiểm tra 6: Tìm từ ẩn

Tìm 8 thuật ngữ từ vựng chính ẩn trong lưới bên dưới. Các từ có thể nằm ngang, dọc hoặc chéo.

S Q U R D K H T P Ă A Ă Â O V
A K Ư I V K V U Â S C I C Ơ M
O H L C G M M Â C I H Ơ Ô E M
H M O Ơ P Q S N Y R E E Â Q Ơ
U A A O Ê Q Â T U U G C R T X
Ê O S T Â Y U H R Đ I I Ê Ư Y
I H B M C Ơ Ư U T Ô Â Â S T Ă
H A A Y N C K A C O U C D H E
T M G B P Ơ L D G Q Y Q Đ Ê Ơ
I U D A A Ơ O M Ô S V Ơ I B P
Ô V I P H A M D Ư L I Ê U A S
T Q B M X Ă Đ Q Ư Ư H A P O Y
X X K E G M P I L L R O Ê M Ơ
Ơ E Y A O T Đ T Â X P X Ă Â Ê
L Y E H N Ô N Ư Â L Y X Đ T V

DANH SÁCH TỪ VỰNG

MAHOA SAOLƯU TÔITHIÊUHOA TRUYCẬP TƯTHÊBAOMÂT VIPHAMDƯLIÊU TUÂNTHU CHEGIÂU

Điểm kiểm tra 6, phương án khác: Ghép từ vựng dễ tiếp cận

Ghép từng thuật ngữ trong số 8 thuật ngữ từ vựng ở phần Tìm từ với định nghĩa đúng bằng cách viết chữ cái (A-H) vào chỗ trống.

THUẬT NGỮ TỪ VỰNG

- **A. MAHOA**
- **B. SAOLƯU**
- **C. TÔITHIÊUHOA**
- **D. TRUYCẬP**
- **E. TƯTHÊBAOMÂT**
- **F. VIPHAMDƯLIÊU**
- **G. TUÂNTHU**
- **H. CHEGIÂU**

ĐỊNH NGHĨA VÀ CÁC TRƯỜNG GHÉP

1. Sự cố bảo mật trong đó dữ liệu được bảo vệ bị truy cập hoặc tiết lộ trái phép.
2. Thay các ký tự nhạy cảm trong trường cơ sở dữ liệu để bảo vệ danh tính cá nhân.
3. Giới hạn quyền đọc và ghi cơ sở dữ liệu cho các vai trò người dùng đã xác thực.
4. Trạng thái bảo mật tổng thể và mức sẵn sàng phòng vệ của đám mây của một tổ chức.
5. Đáp ứng các tiêu chuẩn quy định như GDPR hoặc CCPA khi quản lý thông tin người dùng riêng tư.
6. Giới hạn việc thu thập dữ liệu cá nhân ở mức tối thiểu tuyệt đối cần cho hoạt động.
7. Biến văn bản thuần thành bản mã không đọc được để dữ liệu bị chặn bắt vẫn riêng tư.
8. Tạo các bản sao an toàn ngoài địa điểm để khôi phục khi hệ thống gặp lỗi.

Điểm kiểm tra 7: Thử thách từ bị xáo trộn

Sắp xếp lại các chữ cái bên dưới để tìm ra các khái niệm và thuật ngữ chính về an ninh mạng. Viết đáp án của bạn vào các ô nhập đã cung cấp.

1. **OHMAA** _____

2. **HAÔTOIIHUÊT** _____

3. **TABOTƯÂTÊMH** _____

4. **UUTNHTÂ** _____

5. **LOUSƯA** _____

6. **ÂUCTYPR** _____

7. **ƯLAVIDUIÊPMH** _____

8. **HGUCÂIE** _____

Hoạt động thưởng: Nghĩ nhanh

3 CÂU TRẢ LỜI CHO MỖI CHỦ ĐỀ. AI HOÀN THÀNH DANH SÁCH TRƯỚC SẼ THẮNG.

1	Những thứ bạn sao lưu			
2	Những từ liên quan đến an ninh mạng			
3	Những người được phép xem dữ liệu nhạy cảm			
4	Những cách xóa dữ liệu an toàn			
5	Những nơi lưu trữ dữ liệu			
6	Những thứ nên được mã hóa			
7	Những dữ liệu mà một bệnh viện phải bảo vệ			
8	Những loại sao lưu			
9	Những thông tin bạn không bao giờ nên chia sẻ			
10	Những dấu hiệu cảnh báo trong một email			
11	Những thói quen an toàn bạn có thể bắt đầu ngay hôm nay			
12	Những người bạn có thể nhờ giúp về CNTT			
13	Những thiết bị có thể bị tấn công			
14	Những cách bảo vệ dữ liệu			
15	Những thứ có thể phá hủy dữ liệu			

Điểm kiểm tra 8: Nghiên cứu tình huống về an ninh mạng

Hãy vận dụng các khái niệm bạn đã học để giải các tình huống thực tế dưới đây.

NGHIÊN CỨU TÌNH HUỐNG 1: NÂNG CẤP MÃ HÓA CƠ SỞ DỮ LIỆU DOANH NGHIỆP KHI LƯU TRỮ

👷

Tình huống: Một nhà bán lẻ trực tuyến lưu các cơ sở dữ liệu giao dịch trên bộ nhớ đám mây mà không mã hóa toàn bộ ổ đĩa. Một cuộc kiểm toán tuân thủ gần đây đã gắn cờ điều này là rủi ro nghiêm trọng về bảo mật dữ liệu theo CCPA. Hãy thiết kế một kiến trúc khôi phục.

Câu hỏi thảo luận: Hãy phân tích các rủi ro tuân thủ CCPA, và đề xuất một chiến lược mã hóa dữ liệu lưu trữ.

NGHIÊN CỨU TÌNH HUỐNG 2: NGĂN CHẶN MÃ ĐỘC TỐNG TIỀN VÀ KHÔI PHỤC DỮ LIỆU

👷

Tình huống: Một cuộc tấn công mã độc tống tiền đang diễn ra đang mã hóa các ổ đĩa mạng trên mạng cục bộ của công ty. Quản trị viên đã phát hiện sớm sự nhiễm. Hãy lập kế hoạch các bước ngăn chặn và khôi phục.

Câu hỏi thảo luận: Hãy trình bày chi tiết các hành động ngăn chặn ngay lập tức, và lập kế hoạch cho một quy trình khôi phục an toàn.

Điểm kiểm tra 9: Giải mã mật thư

Chuyên gia an ninh mạng bảo vệ tài sản mạng khỏi các tác nhân đe dọa trực tuyến. Hãy dùng bảng khóa Chữ-Số bên dưới để giải mã thông điệp bằng cách viết các chữ cái tương ứng vào chỗ trống.

KHÓA MÃ HÓA CHỮ SANG SỐ

A=1 Ă=2 Â=3 B=4 C=5 D=6 Đ=7 E=8 Ê=9 G=10

H=11 I=12 K=13 L=14 M=15 N=16 O=17 Ô=18 Ơ=19 P=20

Q=21 R=22 S=23 T=24 U=25 Ư=26 V=27 X=28 Y=29

4	1	17		27	9		6	26		14	12	9	25		22	12	9	16	10
24	26		4	2	16	10		13	12	9	15		23	17	1	24		1	16
								24	17	1	16								

Thông điệp đã giải mã:

MẸO: MỖI SỐ ĐẠI DIỆN CHO VỊ TRÍ CỦA CHỮ CÁI ĐÓ TRONG BẢNG CHỮ CÁI (VÍ DỤ 1 = A, 2 = B, 29 = Y).

Điểm kiểm tra 10: Câu hỏi thường gặp cơ bản về an ninh mạng (Phần A)

Xem lại các câu hỏi và câu trả lời thường gặp về cách giảm thiểu các mối đe dọa trực tuyến.

Q1: Bảo vệ dữ liệu là gì?

Đây là quá trình bảo vệ dữ liệu cá nhân và doanh nghiệp khỏi truy cập trái phép, mất mát hoặc hỏng hóc thông qua các biện pháp kiểm soát kỹ thuật.

Q2: Vì sao mã hóa toàn bộ ổ đĩa lại quan trọng?

Nó bảo mật các khối dữ liệu lưu trữ trên ổ đĩa vật lý, ngăn bất kỳ ai đọc dữ liệu nếu họ đánh cắp ổ cứng.

Q3: Mã hóa khi lưu trữ và khi truyền tải khác nhau như thế nào?

Mã hóa khi lưu trữ bảo vệ các tệp đã lưu trên ổ đĩa, còn mã hóa khi truyền bảo vệ các gói tin mạng đang di chuyển qua router.

Q4: Che giấu dữ liệu là gì?

Nó thay thế các chi tiết nhạy cảm (như số thẻ tín dụng) bằng dữ liệu hư cấu nhưng thực tế để kiểm thử mà không lộ hồ sơ thật.

Q5: Vì sao sao lưu ngoại tuyến quan trọng?

Nó giữ một bản sao sạch của các tệp của bạn, cô lập khỏi mạng, giúp bảo vệ bản sao lưu của bạn khỏi bị ransomware mã hóa.

Điểm kiểm tra 10: Câu hỏi thường gặp cơ bản về an ninh mạng (Phần B)

Xem lại các câu hỏi và câu trả lời thường gặp về cách giảm thiểu các mối đe dọa trực tuyến.

Q6: Kho mã hóa dữ liệu bằng token (tokenization vault) là gì?

Cơ sở dữ liệu an toàn, biệt lập ánh xạ các mã thông báo ngẫu nhiên với giá trị nhạy cảm gốc của chúng (như số thẻ tín dụng chính).

Q7: Truy cập cơ sở dữ liệu zero-trust nghĩa là gì?

Nó có nghĩa là xác minh danh tính và trạng thái thiết bị của mọi người dùng ở mỗi lần đăng nhập, thay vì tin tưởng bất kỳ ai bên trong mạng.

Q8: TLS bảo vệ dữ liệu khi truyền tải như thế nào?

TLS mã hóa tải trọng phiên TCP, ngăn kẻ xấu trên mạng công cộng nghe lén hoặc sửa đổi các gói tin đang truyền.

Q9: Kiểm toán truy cập cơ sở dữ liệu là gì?

Việc ghi liên tục các truy vấn cơ sở dữ liệu và lượt đăng nhập để phát hiện các mẫu truy cập trái phép hoặc bất thường về bảo mật.

Q10: Kiểm toán tình trạng bảo mật đám mây là gì?

Quy trình phân tích cấu hình đám mây để xác định các cổng mở, quy tắc truy cập cấu hình sai và lỗ hổng tuân thủ bảo mật.

Điểm kiểm tra 10: Câu hỏi thường gặp nâng cao về bảo mật (Phần C)

Khám phá các khía cạnh kỹ thuật nâng cao của khung bảo mật, phân tích phần mềm độc hại và tuân thủ dữ liệu.

Q1: Mã hóa phong bì (envelope encryption) hoạt động như thế nào?

Nó mã hóa dữ liệu bằng một khóa dữ liệu, rồi mã hóa khóa dữ liệu đó bằng một khóa chính, giúp đơn giản hóa việc lưu trữ và xoay vòng khóa.

Q2: Mã hóa đồng cấu (homomorphic encryption) là gì?

Phương pháp mã hóa nâng cao cho phép thực hiện các phép toán trực tiếp trên dữ liệu đã mã hóa mà không cần giải mã trước.

Q3: Vì sao dùng mã hóa ở cấp cột trong cơ sở dữ liệu?

Nó mã hóa riêng từng cột nhạy cảm cụ thể (như SSN), bảo vệ chúng ngay cả khi quản trị viên có quyền đọc bảng nói chung.

Q4: Ngăn ngừa thất thoát dữ liệu (DLP) là gì?

Phần mềm giám sát các điểm đi ra của mạng để phát hiện và chặn việc truyền trái phép các tệp nhạy cảm ra ngoài.

Q5: Bản sao lưu ghi một lần, đọc nhiều lần (WORM) bảo vệ chống ransomware như thế nào?

Sao lưu WORM ngăn tệp bị xóa hoặc sửa đổi trong một khoảng thời gian định sẵn, giúp ransomware không thể mã hóa các bản sao lưu hiện có.

Điểm kiểm tra 10: Câu hỏi thường gặp nâng cao về bảo mật (Phần D)

Khám phá các khía cạnh kỹ thuật nâng cao của khung bảo mật, phân tích phần mềm độc hại và tuân thủ dữ liệu.

Q6: Rủi ro của việc tái sử dụng khóa là gì?

Dùng lại cùng một khóa mật mã cho nhiều cơ sở dữ liệu khác nhau nghĩa là chỉ một khóa bị xâm phạm sẽ làm lộ tất cả cơ sở dữ liệu.

Q7: Mã hóa dữ liệu bằng token (tokenization) cơ sở dữ liệu cải thiện việc tuân thủ CCPA như thế nào?

Token giả danh hóa các bản ghi trong hệ thống không phải sản xuất và hạn chế mức độ lộ khi bị vi phạm, nhưng dữ liệu đã token hóa vẫn có thể là thông tin cá nhân.

Q8: Vì sao phân loại dữ liệu lại quan trọng?

Nó phân loại các tệp theo mức độ nhạy cảm, giúp tổ chức áp dụng mã hóa và kiểm soát truy cập mạnh nhất cho dữ liệu rủi ro cao.

Q9: Xoay vòng khóa đóng vai trò gì?

Cập nhật khóa mã hóa thường xuyên giới hạn lượng dữ liệu lịch sử bị lộ nếu một khóa cuối cùng bị bẻ.

Q10: Vùng bảo mật (secure enclave) bảo vệ các truy vấn cơ sở dữ liệu trong bộ nhớ như thế nào?

Các enclave bảo mật cô lập hoạt động truy vấn trong các khối bộ nhớ được CPU bảo vệ, ngăn quản trị viên máy chủ xem văn bản rõ trong RAM.

Phần 11: 10 sự thật và hiểu biết thực tế về an ninh mạng

Xem lại các sự thật thực tế về vi phạm bảo mật, cơ chế phòng thủ và tiêu chuẩn tuân thủ.

1. THÔNG TIN VỀ AN NINH

Quy định GDPR có hiệu lực từ tháng 5 năm 2018, thay đổi cách các trang web toàn cầu quản lý sự đồng ý về cookie và hồ sơ dữ liệu cá nhân.

2. THÔNG TIN VỀ AN NINH

Mức phạt vi phạm GDPR có thể lên tới 20 triệu Euro hoặc 4% doanh thu toàn cầu, thể hiện rủi ro pháp lý đáng kể. [4]

3. THÔNG TIN VỀ AN NINH

CCPA có hiệu lực từ tháng 1 năm 2020, thiết lập các quyền tiên phong của người tiêu dùng về quyền riêng tư kỹ thuật số tại Hoa Kỳ.

4. THÔNG TIN VỀ AN NINH

Tối thiểu hóa dữ liệu giảm dung lượng lưu trữ cơ sở dữ liệu, cắt giảm chi phí vận hành máy chủ đồng thời giảm quy mô tác động của vi phạm.

5. THÔNG TIN VỀ AN NINH

Hủy bằng mật mã giải quyết thách thức xóa bản sao lưu bằng cách xóa khóa thay vì chỉnh sửa các tệp băng sao lưu lịch sử.

6. THÔNG TIN VỀ AN NINH

Hiện nay hầu hết các quốc gia trên thế giới đã ban hành luật bảo vệ dữ liệu cá nhân để bảo vệ quyền riêng tư của người tiêu dùng.

7. THÔNG TIN VỀ BẢO MẬT

Biểu mẫu đồng ý chủ động (opt-in) có ô đã chọn sẵn bị cấm rõ ràng theo các định nghĩa quy định về quyền riêng tư dữ liệu của châu Âu.

8. THÔNG TIN VỀ BẢO MẬT

GDPR yêu cầu báo cáo các vụ vi phạm dữ liệu cá nhân cho cơ quan giám sát trong vòng 72 giờ kể từ khi biết, nếu khả thi. [3]

9. THÔNG TIN VỀ BẢO MẬT

Băm mật khẩu bằng các thuật toán chậm như bcrypt hoặc Argon2 khiến việc bẻ khóa ngoại tuyến các giá trị băm bị đánh cắp khó hơn nhiều. [6]

10. THÔNG TIN VỀ AN NINH

Dữ liệu lưu trữ là các tệp cơ sở dữ liệu đã lưu, còn dữ liệu đang truyền là các gói tin đang di chuyển qua bộ định tuyến mạng.

Tài liệu tham khảo kỹ thuật và nguồn

Tài liệu học tập và các câu đố tương tác được biên soạn từ các tiêu chuẩn toàn cầu của NIST, OWASP và tuân thủ quyền riêng tư dữ liệu.

TÀI LIỆU THAM KHẢO HỌC THUẬT VÀ NGÀNH

[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

Đáp án: Điểm kiểm tra 1 – Trắc nghiệm

1 Câu hỏi 1 — **Đáp án đúng: A**

GHI CHÚ CHO GIÁO VIÊN

Mục đích chính của việc che giấu dữ liệu (data masking) là gì? → Thay các định danh nhạy cảm bằng ký tự hư cấu nhưng thực tế để bảo vệ quyền riêng tư

2 Câu hỏi 2 — **Đáp án đúng: A**

GHI CHÚ CHO GIÁO VIÊN

Cơ chế nào mã hóa các tệp lưu trên ổ cứng của máy chủ cơ sở dữ liệu? → Mã hóa toàn bộ ổ đĩa khi lưu trữ

3 Câu hỏi 3 — **Đáp án đúng: A**

GHI CHÚ CHO GIÁO VIÊN

Điều gì đại diện cho dữ liệu đang truyền? → Các gói dữ liệu di chuyển qua router và switch mạng

4 Câu hỏi 4 — **Đáp án đúng: A**

GHI CHÚ CHO GIÁO VIÊN

Vì sao bản sao lưu ngoại tuyến thường xuyên lại quan trọng để chống ransomware? → Cung cấp bản sao sạch, ngoại tuyến để khôi phục tệp mà không phải trả tiền chuộc

5 Câu hỏi 5 — **Đáp án đúng: A**

GHI CHÚ CHO GIÁO VIÊN

Mã hóa thành token dữ liệu (data tokenization) làm gì? → Thay số thẻ nhạy cảm bằng các mã thông báo ngẫu nhiên không nhạy cảm

Đáp án: Điểm kiểm tra 2 – Đúng hay Sai

6 **Câu hỏi 6** — **Đáp án đúng: Sai**

GHI CHÚ CHO GIÁO VIÊN

Che giấu dữ liệu (masking) thay đổi các bản sao thử nghiệm hoặc ẩn các giá trị tại thời điểm truy vấn; bản ghi sản xuất không thay đổi.

7 **Câu hỏi 7** — **Đáp án đúng: Đúng**

GHI CHÚ CHO GIÁO VIÊN

Bản sao lưu ngoài địa điểm phải được tách biệt khỏi mạng doanh nghiệp chính để ngăn mã độc tống tiền (ransomware) lây lan.

8 **Câu hỏi 8** — **Đáp án đúng: Sai**

GHI CHÚ CHO GIÁO VIÊN

Chứng chỉ TLS bảo vệ dữ liệu đang truyền; dữ liệu lưu trữ cần mã hóa ổ đĩa, tệp hoặc cơ sở dữ liệu.

9 **Câu hỏi 9** — **Đáp án đúng: Đúng**

GHI CHÚ CHO GIÁO VIÊN

Truy cập mạng zero-trust (ZTNA) xác minh danh tính của từng người dùng trước khi cấp quyền truy cập cơ sở dữ liệu.

10 **Câu hỏi 10** — **Đáp án đúng: Đúng**

GHI CHÚ CHO GIÁO VIÊN

Mã hóa thành token dựa trên kho lưu trữ giữ các giá trị gốc trong một kho token an toàn, nơi ánh xạ mỗi token trở lại dữ liệu của nó.

Đáp án từ vựng và thang chấm điểm

Thang chấm điểm cho giáo viên: Cho 1 điểm với mỗi cặp ghép đúng (tổng cộng 8 điểm) và mỗi thuật ngữ ngữ cảnh (tổng cộng 6 điểm).

ĐIỂM KIỂM TRA 4: ĐÁP ÁN – GHÉP NỐI KHÁI NIỆM

B 1. MÃ HÓA	A 2. SAO LƯU	H 3. TỐI THIỂU HÓA	F 4. TRUY CẬP
C 5. TƯ THẾ AN NINH	E 6. VI PHẠM DỮ LIỆU	D 7. TUÂN THỦ	G 8. CHE GIẤU

ĐIỂM KIỂM TRA 3: ĐÁP ÁN – THUẬT NGỮ CHÍNH

1 CHE GIẤU	2 TĨNH	3 TRUYỀN TẢI	4 TRUY CẬP
5 SAO LƯU	6 TƯ THẾ BẢO MẬT		

ĐIỂM KIỂM TRA 6, PHƯƠNG ÁN KHÁC: ĐÁP ÁN – GHÉP TỪ

1 F – VIPHAMDULIÊU	2 H – CHEGIÂU	3 D – TRUYCÂP	4 E – TUTHÊBAOMÂT
5 G – TUÂNTHU	6 C – TÔITHIÊUHOA	7 A – MAHOA	8 B – SAOLUU

GHI CHÚ THẢO LUẬN CHO GIÁO VIÊN

Thuật ngữ chính:
Kiểm tra xem học sinh có giải thích được MÃ HÓA, SAO LƯU và TỐI THIỂU HÓA bằng lời của mình và nêu một ví dụ cho mỗi thuật ngữ hay không.

Nghiên cứu tình huống:
Yêu cầu học sinh dùng dữ kiện trong phiếu, không dùng phỏng đoán, để chứng minh khuyến nghị của mình.

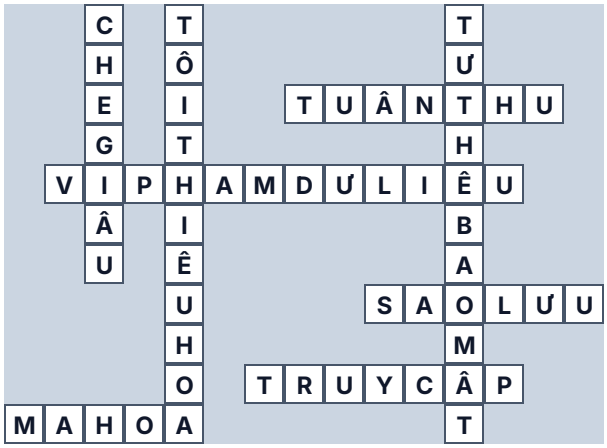
Đánh giá nguồn:
Yêu cầu học sinh kiểm chứng ít nhất một nhận định trong các nguồn của phiếu và thảo luận vì sao số liệu, giá cả và quy định có thể thay đổi theo thời gian.

Đáp án câu đố và ghi chú cho giáo viên

ĐÁP ÁN TÌM TỪ

S	Q	U	R	D	K	H	T	P	Ă	A	Ă	Â	O	V
A	K	Ư	I	V	K	V	U	Â	S	C	I	C	Ơ	M
O	H	L	C	G	M	M	Â	C	I	H	Ơ	Ô	E	M
H	M	O	Ơ	P	Q	S	N	Y	R	E	E	Â	Q	Ơ
U	A	A	O	Ê	Q	Â	T	U	U	G	C	R	T	X
Ê	O	S	T	Â	Y	U	H	R	Đ	I	I	Ê	Ư	Y
I	H	B	M	C	Ơ	Ư	U	T	Ô	Â	Â	S	T	Ă
H	A	A	Y	N	C	K	A	C	O	U	C	D	H	E
T	M	G	B	P	Ơ	L	D	G	Q	Y	Q	Đ	Ê	Ơ
I	U	D	A	A	Ơ	O	M	Ô	S	V	Ơ	I	B	P
Ô	V	I	P	H	A	M	D	Ư	L	I	Ê	U	A	S
T	Q	B	M	X	Ă	Đ	Q	Ư	Ư	H	A	P	O	Y
X	X	K	E	G	M	P	I	L	L	R	O	Ê	M	Ơ
Ơ	E	Y	A	O	T	Đ	T	Â	X	P	X	Ă	Â	Ê
L	Y	E	H	N	Ô	N	Ư	Â	L	Y	X	Đ	T	V

ĐÁP ÁN Ô CHỮ



HƯỚNG DẪN CHO GIÁO VIÊN VỀ ĐÁP ÁN Ô CHỮ

HÀNG NGANG

4 hàng ngang: TUÂNTHU Đáp ứng các tiêu chuẩn quy định như GDPR hoặc CCPA khi quản lý thông tin người dùng riêng tư (7 chữ cái)

5 hàng ngang: VIPHAMDƯLIÊU Sự cố bảo mật trong đó dữ liệu được bảo vệ bị truy cập hoặc tiết lộ trái phép (12 chữ cái)

6 hàng ngang: SAOLƯU Tạo các bản sao an toàn ngoài địa điểm để khôi phục khi hệ thống gặp lỗi (6 chữ cái)

7 hàng ngang: TRUYCÂP Giới hạn quyền đọc và ghi cơ sở dữ liệu cho các vai trò người dùng đã xác thực (7 chữ cái)

8 hàng ngang: MAHOA Biến văn bản thuần thành bản mã không đọc được để dữ liệu bị chặn bắt vẫn riêng tư (5 chữ cái)

HÀNG DỌC

1 hàng dọc: CHEGIÂU Thay các ký tự nhạy cảm trong trường cơ sở dữ liệu để bảo vệ danh tính cá nhân (7 chữ cái)

2 hàng dọc: TÔITHIÊUHOA Giới hạn việc thu thập dữ liệu cá nhân ở mức tối thiểu tuyệt đối cần cho hoạt động (11 chữ cái)

3 hàng dọc: TƯTHÊBAOMÂT Trạng thái bảo mật tổng thể và mức sẵn sàng phòng vệ của đám mây của một tổ chức (11 chữ cái)

Đáp án: Từ bị xáo trộn và mật thư

Đáp án cho hoạt động sắp xếp lại chữ cái từ vựng và Thử thách mật mã bí mật.

ĐÁP ÁN SẮP XẾP LẠI CHỮ CÁI

1. OHMAA — **MAHOA**
2. HAÔTOIIHUÊT — **TÔITHIÊUHOA**
3. TABOTƯÂTÊMH — **TƯTHÊBAOMÂT**
4. UUTNHTÂ — **TUÂNTHU**
5. LOUSƯA — **SAOLƯU**
6. ÂUCTYPR — **TRUYCÂP**
7. ƯLAVIDUIÊPMH — **VIPHAMDƯLIÊU**
8. HGUCÂIE — **CHEGIÂU**

KHÓA THỬ THÁCH MẬT THƯ BÍ MẬT

"BAO VÊ DƯ LIÊU RIÊNG TƯ BĂNG KIÊM SOAT AN TOAN"

Đáp án nghiên cứu tình huống

A Nghiên cứu tình huống 1: Nâng cấp mã hóa cơ sở dữ liệu doanh nghiệp khi lưu trữ

Lời giải dành cho giáo viên

HƯỚNG DẪN CHẤM ĐIỂM

Câu trả lời của học sinh cần đề cập các điểm sau:

- Phân tích tình huống: Một nhà bán lẻ trực tuyến lưu cơ sở dữ liệu giao dịch trên lưu trữ đám mây mà không mã hóa toàn bộ ổ đĩa. Một cuộc kiểm toán tuân thủ gần đây đã gắn cờ đây là rủi ro nghiêm trọng về bảo mật dữ liệu theo CCPA. Hãy thiết kế kiến trúc khôi phục.
- Chiến lược và giải pháp đề xuất: Triển khai mã hóa toàn bộ ổ đĩa AES-256 khi lưu trữ trên mọi hệ thống tệp. Dùng Dịch vụ quản lý khóa (KMS) tập trung với cơ chế xoay vòng tự động và áp dụng nghiêm ngặt các chính sách IAM để kiểm soát quyền giải mã.

B Nghiên cứu tình huống 2: Ngăn chặn mã độc tống tiền và khôi phục dữ liệu

Lời giải dành cho giáo viên

HƯỚNG DẪN CHẤM ĐIỂM

Câu trả lời của học sinh cần đề cập các điểm sau:

- Phân tích tình huống: Một cuộc tấn công ransomware đang hoạt động đang mã hóa các ổ đĩa mạng trên mạng cục bộ của doanh nghiệp. Quản trị viên đã phát hiện sớm việc nhiễm. Hãy lập kế hoạch các bước ngăn chặn và khôi phục.
- Chiến lược và giải pháp đề xuất: Cô lập ngay phân đoạn bị xâm nhập. Định dạng lại các điểm cuối bị ảnh hưởng và khôi phục từ bản sao lưu ngoại tuyến ghi một lần đọc nhiều lần (WORM) mới nhất. Xác minh tính toàn vẹn của bản sao lưu trước khi kết nối lại các hệ thống.