Họ tên: _____ Ngày: _____ Điểm: _____

Tấn công ransomware và doanh nghiệp Phục hồi

Thực thi tải trọng, mã hóa tệp bằng mật mã, sao lưu ngoại tuyến, quy trình ngăn chặn và khôi phục sau thảm họa.

TỔNG QUAN HỌC TẬP VỀ TẤN CÔNG RANSOMWARE

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 cuộc tấn công ransomware và khôi phục hoạt động doanh nghiệp. Bạn sẽ khám phá việc thực thi tải trọng, mã hóa tệp, sao lưu ngoại tuyến, ngăn chặn mối đe dọa, thanh toán bằng tiền mã hóa và kế hoạch khôi phục sau thảm họa.

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/tan-cong-ransomware/

Lộ trình học về khôi phục sau ransomware của bạn

- Phân biệt tải trọng Trojan, ransomware và phần mềm gián điệp.
- Phân tích các tệp độc hại bên trong môi trường sandbox an toàn.
- Xây dựng quy trình cách ly và ngăn chặn mạng nhanh chóng.

HƯỚNG DẪN VỀ TẤN CÔNG RANSOMWARE

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 khôi phục sau mã độc tống tiền. Kết thúc với hoạt động thưởng Nghĩ nhanh.

TẤN CÔNG RANSOMWARE VÀ KHÔI PHỤC SAU THẢM HỌA (GIỚI THIỆU)

Mã độc ransomware khóa bộ lưu trữ của hệ thống bằng mật mã, đòi thanh toán bằng tiền mã hóa để đổi lấy khóa giải mã. Giảm thiểu mối đe dọa này gồm các quy tắc cách ly mạng, phân tích phần mềm độc hại trong sandbox và các bản sao lưu lạnh cách ly mạng (air-gapped) vững chắc.

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

Điểm kiểm tra 1: Thử thách trắc nghiệm

1 **1. Cơ chế chính của một cuộc tấn công ransomware là gì?**

- A. Mã hóa mật mã các tệp của người dùng để từ chối truy cập hệ thống
- B. Chèn các lệnh SQL độc hại vào trường biểu mẫu
- C. Nghe lén gói tin mạng trên kết nối Wi-Fi công cộng
- D. Giả mạo tiêu đề email để vượt qua xác thực SPF

2 **2. Bản sao lưu ngoại tuyến (cold) là gì?**

- A. Bản sao lưu trữ tách rời khỏi mạng để bảo vệ khỏi sự lây lan của phần mềm độc hại
- B. Bản sao lưu lưu trên ổ cứng của máy chủ web chính
- C. Bộ đệm tạm thời của nhật ký registry hệ thống
- D. Một công cụ quản trị dùng để đặt lại mật khẩu người dùng

3 **3. Các đội bảo mật nên cách ly hệ thống bị nhiễm như thế nào trong một cuộc tấn công ransomware?**

- A. Ngắt cáp mạng và tắt các giao diện không dây ngay lập tức
- B. Nâng cấp cơ sở dữ liệu chữ ký của phần mềm diệt virus
- C. Tắt máy chủ DNS chính
- D. Đổi tên phần mở rộng của các tệp bị xâm phạm

4 **4. Vì sao các cơ quan an ninh khuyên không nên trả tiền chuộc ransomware?**

- A. Trả tiền khuyến khích kẻ tấn công và không đảm bảo sẽ nhận được khóa giải mã
- B. Tự động làm mất hiệu lực mọi hợp đồng bảo hiểm doanh nghiệp
- C. Nó tự động thông báo cho mọi khách hàng qua email
- D. Nó làm hỏng các tệp sao lưu hệ thống còn lại

5 **5. Kế hoạch khôi phục sau thảm họa (DRP) là gì?**

- A. Quy trình có cấu trúc để khôi phục hoạt động và dữ liệu sau khi hệ thống bị xâm nhập
- B. Cấu hình tường lửa ánh xạ các cổng mạng đến
- C. Lược đồ cơ sở dữ liệu liệt kê các đặc quyền quản trị của người dùng
- D. Một giao thức xác thực email từ chối các tên miền giả mạo

Điểm kiểm tra 2: Thử thách Đúng hoặc Sai

6 Câu hỏi 6

6. Mã độc ransomware có thể dễ dàng lây lan sang các bản sao lưu trực tuyến được kết nối với mạng.

○ Đúng ○ Sai

7 Câu hỏi 7

7. Trả tiền chuộc bằng tiền mã hóa đảm bảo các tệp sẽ được giải mã thành công.

○ Đúng ○ Sai

8 Câu hỏi 8

8. Ngắt kết nối các hệ thống bị nhiễm khỏi mạng giúp ngăn mã độc tống tiền lây sang các hệ thống lân cận.

○ Đúng ○ Sai

9 Câu hỏi 9

9. Mật mã đối xứng không bao giờ được ransomware dùng để mã hóa bộ nhớ hệ thống.

○ Đúng ○ Sai

10 Câu hỏi 10

10. Kiểm tra định kỳ các quy trình khôi phục dữ liệu là một phần quan trọng của khắc phục thảm họa.

○ 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. Từ chối quyền truy cập các tệp cục bộ là dùng _____ mật mã.
2. Mã độc đang hoạt động được thực thi trên hệ thống là _____ .
3. Các bản sao lưu tách rời ở địa điểm khác là một hình thức _____ an toàn.
4. Ngăn phần mềm độc hại lây lan đòi hỏi việc _____ mạng của thiết bị đầu cuối.
5. Khoản thanh toán bằng tiền mã hóa mà tội phạm mạng đòi hỏi là _____ .
6. Phục hồi các tệp dữ liệu vận hành là việc _____ sau thảm họa.

NGÂN HÀNG TỪ VỰNG

CÔ LẬP | KHÔI PHỤC | MÃ HÓA | SAO LƯU LẠNH | TẢI TRỌNG ĐỘC | THẢM HỌA | TIỀN CHUỘC | TROJAN

Viết câu trả lời của bạn tại đây:

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

Điểm kiểm tra 4: Ghép nối khái niệm bảo mật

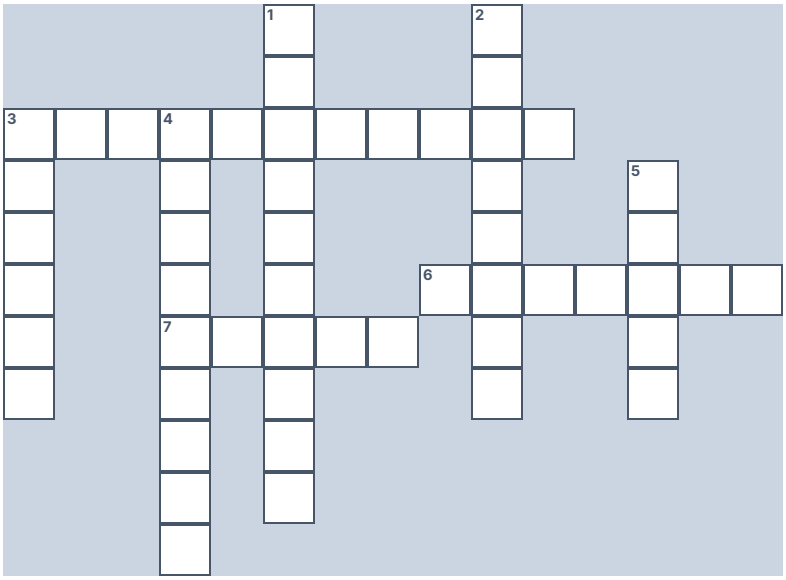
GHÉP ĐỊNH NGHĨA

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	Ngắt kết nối các hệ thống mạng bị nhiễm.
☐	2. DỮ LIỆU TẢI	B	Tệp độc hại ngụy trang thành sạch.
☐	3. SAO LƯU NGUỘI	C	Khóa tệp bằng mật mã.
☐	4. CÁCH LY	D	Sự cố gián đoạn hệ thống nghiêm trọng.
☐	5. TIỀN CHUỘC	E	Thực thi phần mềm độc hại.
☐	6. KHÔI PHỤC	F	Bản sao ngoại tuyến đã ngắt kết nối.
☐	7. THẢM HỌA	G	Khôi phục cơ sở dữ liệu từ bản sao lưu.
☐	8. TROJAN	H	Yêu cầu chi trả khóa mật mã.

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

3. Phần mềm độc hại được thực thi (11)

6. Sự kiện gián đoạn hệ thống nghiêm trọng (7)

7. Ngắt kết nối các hệ thống mạng bị nhiễm (5)

HÀNG DỌC

1. Bản sao ngoại tuyến, đã ngắt kết nối (10)

2. Phục hồi cơ sở dữ liệu từ bản sao lưu (8)

3. Tệp độc hại ngụy trang thành tệp sạch (6)

4. Yêu cầu trả tiền để lấy khóa mật mã (9)

5. Khóa tệp bằng mật mã (5)

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

3 hàng ngang: Phần mềm độc hại được thực thi (11 chữ cái):

6 hàng ngang: Sự kiện gián đoạn hệ thống nghiêm trọng (7 chữ cái):

7 hàng ngang: Ngắt kết nối các hệ thống mạng bị nhiễm (5 chữ cái):

HÀNG DỌC

1 hàng dọc: Bản sao ngoại tuyến, đã ngắt kết nối (10 chữ cái):

2 hàng dọc: Phục hồi cơ sở dữ liệu từ bản sao lưu (8 chữ cái):

3 hàng dọc: Tệp độc hại ngụy trang thành tệp sạch (6 chữ cái):

4 hàng dọc: Yêu cầu trả tiền để lấy khóa mật mã (9 chữ cái):

5 hàng dọc: Khóa tệp bằng mật mã (5 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.

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

DANH SÁCH TỪ VỰNG

MAHOA TAITRONGĐÔC SAOLƯULANH CÔLẬP TIÊNCHUÔC KHÔIPHUC THAMHOA TROJAN

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. TAITRONGĐÔC
C. SAOLƯULANH
D. CÔLÂP
E. TIÊNCHUÔC
F. KHÔIPHUC
G. THAMHOA
H. TROJAN

ĐỊNH NGHĨA VÀ CÁC TRƯỜNG GHÉP
_____ 1. Bản sao ngoại tuyến, đã ngắt kết nối.
_____ 2. Tệp độc hại ngụy trang thành tệp sạch.
_____ 3. Khóa tệp bằng mật mã.
_____ 4. Yêu cầu trả tiền để lấy khóa mật mã.
_____ 5. Ngắt kết nối các hệ thống mạng bị nhiễm.
_____ 6. Sự kiện gián đoạn hệ thống nghiêm trọng.
_____ 7. Phần mềm độc hại được thực thi.
_____ 8. Phục hồi cơ sở dữ liệu từ bản sao lưu.

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. NLSAƯHLAUO
3. THCIUCNÔÊ
4. AHHMOTA
5. ĐAGNICROTÔT
6. ÂCLPÔ
7. KCPHUHIÔ
8. ONTAJR

Hoạt động thưởng: Nghĩ nhanh

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

1	Những thông tin bạn không bao giờ nên chia sẻ			
2	Những thiết bị có thể bị tấn công			
3	Lý do không nên trả tiền chuộc			
4	Những thói quen an toàn bạn có thể bắt đầu ngay hôm nay			
5	Những công cụ bảo mật bạn biết			
6	Những cách bảo vệ tài khoản của bạn			
7	Những dấu hiệu máy tính bị nhiễm			
8	Những nơi để lưu bản sao lưu			
9	Những tệp bạn không bao giờ muốn mất			
10	Những cách mã độc tống tiền lây lan			
11	Những việc cần làm trong giờ đầu tiên của một cuộc tấn công			
12	Những người cần liên hệ trong một cuộc tấn công			
13	Những thứ mã độc tống tiền có thể khóa			
14	Những từ liên quan đến an ninh mạng			
15	Những tổ chức thường bị nhắm đến			

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: NGĂN CHẶN MÃ ĐỘC TỐNG TIỀN TRONG DOANH NGHIỆP

👷

Tình huống: Mạng cục bộ của một doanh nghiệp đã bị ransomware đang hoạt động xâm nhập. Các máy chủ tệp chính đã bắt đầu hiển thị phần mở rộng tệp .locked.

Câu hỏi thảo luận: Hãy trình bày chi tiết các bước ngăn chặn, và nêu giao thức khôi phục dữ liệu.

NGHIÊN CỨU TÌNH HUỐNG 2: ĐÁNH GIÁ CÁC KIẾN TRÚC SAO LƯU NGOẠI TUYẾN

👷

Tình huống: Một doanh nghiệp muốn thiết kế chiến lược sao lưu dữ liệu giúp giảm rủi ro các bản sao lưu bị xâm phạm, ngay cả khi mạng cục bộ chính bị mã độc tống tiền chiếm quyền hoàn toàn.

Câu hỏi thảo luận: Thiết kế hệ thống kho lưu trữ sao lưu ngoại tuyến 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

13	11	18	12		20	11	25	5		11	9		24	11	18	16	10		15	1
11	17	1		24	26		4	1	16		23	1	17		14	26	25			
							14	1	16	11										

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: Ransomware là gì?

Ransomware là phần mềm độc hại được thiết kế để chặn quyền truy cập vào hệ thống máy tính hoặc tệp cho đến khi khoản tiền chuộc được trả.

Q2: Ransomware lây lan như thế nào?

Qua tệp đính kèm email lừa đảo (phishing), các lỗ hổng phần mềm chưa được vá và các hệ thống truy cập từ xa bị xâm phạm. [1]

Q3: Vì sao yêu cầu thanh toán bằng tiền mã hóa?

Các loại tiền mã hóa như Bitcoin mang lại tính ẩn danh tương đối, gây khó khăn cho cơ quan thực thi pháp luật trong việc theo dõi dòng tiền.

Q4: Phần mềm diệt virus có chặn ransomware không?

Có, nhưng phần mềm diệt virus dựa trên chữ ký có thể thất bại trước các tải trọng ransomware zero-day mới được tạo ra.

Q5: Bản sao lưu cách ly mạng (air-gapped) là gì?

Bản sao lưu không có kết nối vật lý hay logic với mạng chính, giúp bảo vệ nó khỏi sự lây lan.

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: Tống tiền kép là gì?

Khi kẻ tấn công không chỉ mã hóa tệp mà còn đánh cắp dữ liệu nhạy cảm để dọa công khai nếu không được trả tiền.

Q7: Công cụ giải mã (decryptor) là gì?

Tiện ích phần mềm chứa khóa mật mã cần thiết để khôi phục các tệp bị khóa về dạng văn bản thuần.

Q8: Bạn phát hiện ransomware sớm như thế nào?

Bằng cách giám sát hệ thống tệp để phát hiện hoạt động sửa đổi và đổi tên hàng loạt tệp đột ngột.

Q9: Bảo hiểm đóng vai trò gì?

Bảo hiểm an ninh mạng có thể giúp chi trả chi phí khôi phục, nhưng điều khoản bảo hiểm và quy định về việc trả tiền chuộc khác nhau tùy từng hợp đồng.

Q10: Tôi có nên khởi động lại hệ thống bị nhiễm không?

Không, khởi động lại có thể phá hủy bằng chứng trong bộ nhớ tạm; hãy cô lập máy khỏi mạng thay vì khởi động lại. [1]

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: Ransomware dùng mã hóa bất đối xứng như thế nào?

Nó dùng khóa công khai nhúng trong phần mềm độc hại để mã hóa tệp, yêu cầu khóa riêng của kẻ tấn công để giải mã.

Q2: Vì sao mã hóa đối xứng cũng được sử dụng?

Mã hóa đối xứng (như AES) nhanh và có thể khóa các cơ sở dữ liệu khổng lồ trong vài phút, trong khi khóa bất đối xứng bảo vệ khóa AES.

Q3: Phân đoạn logic là gì?

Chia mạng thành các vùng cô lập, ngăn phần mềm độc hại lây lan ngang từ các máy trạm tới máy chủ cốt lõi.

Q4: Lưu trữ WORM là gì?

Phương tiện ghi một lần, đọc nhiều lần (Write-Once, Read-Many), ngăn dữ liệu sao lưu bị chỉnh sửa, ghi đè hoặc xóa bởi mã độc ransomware.

Q5: Bản sao bóng (shadow copy) là gì?

Các bản sao lưu cục bộ do Windows tạo ra; ransomware thường xóa chúng đầu tiên bằng các công cụ quản trị.

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: Đánh cắp thông tin đăng nhập tạo điều kiện cho ransomware như thế nào?

Kẻ tấn công mua thông tin đăng nhập quản trị bị rò rỉ để đăng nhập qua máy tính từ xa, rồi tự tay triển khai mã độc tống tiền trên toàn mạng.

Q7: Kiểm thử khôi phục chạy thử (dry-run) là gì?

Thường xuyên khôi phục cơ sở dữ liệu sao lưu vào các môi trường thử nghiệm cô lập để xác minh tốc độ khôi phục và tính toàn vẹn dữ liệu đáp ứng các chỉ số khắc phục thảm họa.

Q8: Phát hiện và phản ứng tại điểm cuối (EDR) ngăn chặn ransomware như thế nào?

Bằng cách phân tích hành vi tiến trình (ví dụ: mã hóa nhanh) và nhanh chóng tạm dừng ứng dụng gian lận.

Q9: Mô hình ransomware dưới dạng dịch vụ (RaaS) là gì?

Mô hình nhượng quyền trong đó các nhà phát triển phần mềm độc hại cho các đối tác thuê công cụ tạo ransomware để đổi lấy một phần trăm tiền chuộc.

Q10: RDP chưa vá gây ra ransomware như thế nào?

Các cổng Remote Desktop Protocol bị lộ, chưa vá cho phép kẻ tấn công dò mật khẩu đăng nhập bằng vét cạn và khởi chạy phần mềm độc hại thủ công.

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

Các tác nhân ransomware thường dùng các công cụ như vssadmin.exe để xóa bản sao bóng (shadow copy) của Windows và chặn việc khôi phục cục bộ. [1]

2. THÔNG TIN VỀ AN NINH

Khóa AES-256 đối xứng thường được dùng để mã hóa tải trọng tệp, sau đó được khóa bằng khóa công khai RSA.

3. THÔNG TIN VỀ AN NINH

Phục hồi sau một cuộc tấn công ransomware thành công có thể mất nhiều tuần, đó là lý do các bản sao lưu ngoại tuyến đã được thử nghiệm rất quan trọng.

4. THÔNG TIN VỀ AN NINH

FBI không ủng hộ việc trả tiền chuộc và cảnh báo rằng trả tiền không đảm bảo bạn sẽ lấy lại được dữ liệu. [2]

5. THÔNG TIN VỀ AN NINH

Kế hoạch khôi phục sau thảm họa (DRP) nên xác định Mục tiêu thời gian khôi phục (RTO) và Mục tiêu điểm khôi phục (RPO).

6. THÔNG TIN VỀ AN NINH

FBI khuyến nghị các bản sao lưu được mã hóa và bất biến, nghĩa là không thể bị thay đổi hoặc xóa. [3]

7. THÔNG TIN VỀ BẢO MẬT

Các nhà phát triển ransomware sử dụng các kỹ thuật làm rối nâng cao để vượt qua trình quét diệt virus truyền thống dựa trên chữ ký.

8. THÔNG TIN VỀ BẢO MẬT

Phân đoạn mạng hạn chế di chuyển ngang, giúp ngăn ransomware lây lan ra ngoài máy chủ bị nhiễm đầu tiên. [3]

9. THÔNG TIN VỀ BẢO MẬT

Các dịch vụ từ xa bị lộ, bảo mật kém như Remote Desktop Protocol (RDP) là điểm xâm nhập ransomware phổ biến. [1]

10. THÔNG TIN VỀ AN NINH

CISA khuyến nghị giữ các bản sao lưu đã mã hóa ở chế độ ngoại tuyến, vì nhiều biến thể mã độc tống tiền tìm và xóa các bản sao lưu có thể truy cập được. [1]

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] CISA. (2023). #StopRansomware Guide.

https://www.cisa.gov/stopransomware/ransomware-guide

[2] FBI Internet Crime Complaint Center. (n.d.). Ransomware.

https://www.ic3.gov/CrimeInfo/Ransomware

[3] FBI Internet Crime Complaint Center. (2026). 2025 IC3 Annual Report.

https://www.ic3.gov/AnnualReport/Reports/2025_IC3Report.pdf

[4] CISA. (n.d.). Malware, Phishing, and Ransomware.

https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

[5] CISA. (2023). Phishing Guidance: Stopping the Attack Cycle at Phase One.

https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one

Đáp án: Điểm kiểm tra 1 – Trắc nghiệm

1 Câu hỏi 1

Đáp án đúng: A

GHI CHÚ CHO GIÁO VIÊN

Cơ chế chính của một cuộc tấn công ransomware là gì? → Mã hóa mật mã các tệp của người dùng để từ chối truy cập hệ thống

2 Câu hỏi 2

Đáp án đúng: A

GHI CHÚ CHO GIÁO VIÊN

Bản sao lưu ngoại tuyến (cold) là gì? → Bản sao lưu trữ tách rời khỏi mạng để bảo vệ khỏi sự lây lan của phần mềm độc hại

3 Câu hỏi 3

Đáp án đúng: A

GHI CHÚ CHO GIÁO VIÊN

Các đội bảo mật nên cách ly hệ thống bị nhiễm như thế nào trong một cuộc tấn công ransomware? → Ngắt cáp mạng và tắt các giao diện không dây ngay lập tức

4 Câu hỏi 4

Đáp án đúng: A

GHI CHÚ CHO GIÁO VIÊN

Vì sao các cơ quan an ninh khuyên không nên trả tiền chuộc ransomware? → Trả tiền khuyến khích kẻ tấn công và không đảm bảo sẽ nhận được khóa giải mã

5 Câu hỏi 5

Đáp án đúng: A

GHI CHÚ CHO GIÁO VIÊN

Kế hoạch khôi phục sau thảm họa (DRP) là gì? → Quy trình có cấu trúc để khôi phục hoạt động và dữ liệu sau khi hệ thống bị xâm nhập

Đáp án: Điểm kiểm tra 2 – Đúng hay Sai

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

GHI CHÚ CHO GIÁO VIÊN

Mã độc ransomware có thể dễ dàng lây lan sang các bản sao lưu trực tuyến được kết nối với mạng.

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

GHI CHÚ CHO GIÁO VIÊN

Sai: FBI cảnh báo rằng việc trả tiền không đảm bảo bạn sẽ lấy lại được bất kỳ dữ liệu nào.

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

GHI CHÚ CHO GIÁO VIÊN

Đúng: CISA khuyên rút phích cắm các máy bị nhiễm hoặc đưa mạng ngoại tuyến để ngăn sự lây lan.

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

GHI CHÚ CHO GIÁO VIÊN

Sai: mã độc tống tiền thường mã hóa tệp bằng các thuật toán mã hóa đối xứng nhanh như AES.

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

GHI CHÚ CHO GIÁO VIÊN

Kiểm tra định kỳ các quy trình khôi phục dữ liệu là một phần quan trọng của khắc phục thảm họa.

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

C 1. MÃ HÓA	E 2. DỮ LIỆU TẢI	F 3. SAO LƯU NGUỘI	A 4. CÁCH LY
H 5. TIỀN CHUỘC	G 6. KHÔI PHỤC	D 7. THẢM HỌA	B 8. TROJAN

ĐIỂM KIỂM TRA 3: ĐÁP ÁN – THUẬT NGỮ CHÍNH

1 MÃ HÓA	2 TẢI TRỌNG ĐỘC	3 SAO LƯU LẠNH	4 CÔ LẬP
5 TIỀN CHUỘC	6 KHÔI PHỤC		

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

1 C – SAOLƯULANH	2 H – TROJAN	3 A – MAHOA	4 E – TIÊNCHUÔC
5 D – CÔLÂP	6 G – THAMHOA	7 B – TAITRONGĐÔC	8 F – KHÔIPHUC

GHI CHÚ THẢO LUẬN CHO GIÁO VIÊN

Thuật ngữ chính:
Kiểm tra xem học sinh có giải thích được MÃ HÓA, DỮ LIỆU TẢI và SAO LƯU NGUỘI 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.

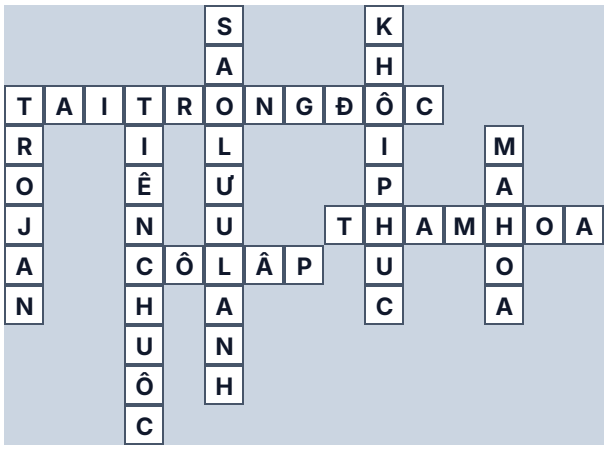
Đánh giá nguồn:
Yêu cầu học sinh kiểm chứng ít nhất một nhận định trong các nguồn của phiếu và thảo luận vì sao số liệu, giá cả và quy định có thể thay đổi theo thời gian.

Đáp án câu đố và ghi chú cho giáo viên

ĐÁP ÁN TÌM TỪ

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

ĐÁP ÁN Ô CHỮ



HƯỚNG DẪN CHO GIÁO VIÊN VỀ ĐÁP ÁN Ô CHỮ

HÀNG NGANG

3 hàng ngang: TAITRONGĐÔC Phần mềm độc hại được thực thi (11 chữ cái)

6 hàng ngang: THAMHOA Sự kiện gián đoạn hệ thống nghiêm trọng (7 chữ cái)

7 hàng ngang: CÔLÂP Ngắt kết nối các hệ thống mạng bị nhiễm (5 chữ cái)

HÀNG DỌC

1 hàng dọc: SAOLƯULANH Bản sao ngoại tuyến, đã ngắt kết nối (10 chữ cái)

2 hàng dọc: KHÔIPHUC Phục hồi cơ sở dữ liệu từ bản sao lưu (8 chữ cái)

3 hàng dọc: TROJAN Tệp độc hại ngụy trang thành tệp sạch (6 chữ cái)

4 hàng dọc: TIÊNCHUÔC Yêu cầu trả tiền để lấy khóa mật mã (9 chữ cái)

5 hàng dọc: MAHOA Khóa tệp bằng mật mã (5 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	5. ĐAGNICROTÔT	TAITRONGĐÔC
2. NLSAƯHLAUO	SAOLƯULANH	6. ÂCLPÔ	CÔLÂP
3. THCIUCNÔÊ	TIÊNCHUÔC	7. KCPHUHIÔ	KHÔIPHUC
4. AHHMOTA	THAMHOA	8. ONTAJR	TROJAN

KHÓA THỬ THÁCH MẬT THƯ BÍ MẬT

"KHÔI PHUC HÊ THÔNG MA HOA TƯ BAN SAO LƯU LANH"

Đáp án nghiên cứu tình huống

A Nghiên cứu tình huống 1: Ngăn chặn mã độc tống tiền trong doanh nghiệp

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: Mạng cục bộ của một doanh nghiệp đã bị ransomware đang hoạt động xâm nhập. Các máy chủ tệp quan trọng bắt đầu hiển thị phần mở rộng tệp .locked.
- Chiến lược và giải pháp đề xuất: Ngắt kết nối tất cả máy chủ bị ảnh hưởng khỏi mạng cục bộ. Chấm dứt các phiên quản trị đang hoạt động. Khôi phục các tệp chưa bị xâm phạm từ hệ thống sao lưu ngoại tuyến an toàn, bị khóa ghi.

B Nghiên cứu tình huống 2: Đánh giá các kiến trúc sao lưu ngoại tuyến

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 doanh nghiệp muốn thiết kế chiến lược sao lưu dữ liệu giúp giảm rủi ro bản sao lưu bị xâm phạm ngay cả khi mạng cục bộ chính bị ransomware chiếm quyền hoàn toàn.
- Chiến lược và giải pháp đề xuất: Triển khai lưu trữ ghi một lần đọc nhiều lần (WORM). Tạo khoảng cách ly logic bằng cách ngắt hệ thống sao lưu khỏi mọi mạng, và áp dụng việc luân chuyển phương tiện vật lý hằng ngày.