ชื่อ-นามสกุล: _____ วันที่: _____ คะแนน: _____

การโจมตีด้วยแรนซัมแวร์และธุรกิจการกู้คืน

การรันเพย์โหลด การเข้ารหัสไฟล์ การสำรองข้อมูลออฟไลน์ ขั้นตอนการควบคุมความเสียหาย และการกู้คืนจากภัยพิบัติ

ภาพรวมการเรียนรู้เรื่องการโจมตีด้วยแรนซัมแวร์

ได้รับการรักษาความปลอดภัย
การเข้ารหัสข้อมูล
มาตรฐาน AES 256 บิต

เป็นไปตามข้อกำหนด
มาตรฐานสากล
กรอบกฎหมาย GDPR และ CCPA

ซีโร่ทรัสต์
นโยบายการเข้าถึง
การยืนยันตัวตนหลายปัจจัย

ยินดีต้อนรับ! ชุดกิจกรรมนี้จะพาคุณเรียนรู้เกี่ยวกับการโจมตีด้วยแรนซัมแวร์และการกู้คืนธุรกิจ คุณจะได้สำรวจการทำงานของเพย์โหลด การเข้ารหัสไฟล์ การสำรองข้อมูลออฟไลน์ การกักกันภัยคุกคาม การชำระเงินด้วยสกุลเงินดิจิทัล และแผนกู้คืนระบบจากภัยพิบัติ

จุดตรวจสอบของใบงาน

- [ ] **ส่วนที่ 1-4: เรียนรู้ความปลอดภัยไซเบอร์และการป้องกันภัยคุกคามให้เชี่ยวชาญ**
- [ ] **ส่วนที่ 5-7: แก้ปริศนาอักษรไขว้และค้นหาคำ**
- [ ] **ส่วนที่ 8-9: แก้กรณีศึกษาและภารกิจถอดรหัส**
- [ ] **ส่วนที่ 10: ทบทวนหน้า FAQ ระดับพื้นฐานและระดับสูง**
- [ ] **ส่วนที่ 11: สำรวจข้อเท็จจริงน่าสนใจในโลกจริง 10 ข้อ**
- [ ] **เสริม: ความท้าทายคิดเร็ว**

เปิดคู่มือความปลอดภัยไซเบอร์ของ VPN.com

URL: https://www.vpn.com/th/cybersecurity/kan-yok-ransomware/

เส้นทางการเรียนรู้การกู้คืนจากแรนซัมแวร์ของคุณ

- จำแนกความแตกต่างระหว่างเพย์โหลดของโทรจัน แรนซัมแวร์ และสปายแวร์
- วิเคราะห์ไฟล์อันตรายภายในสภาพแวดล้อมแซนด์บอกซ์ที่ปลอดภัย
- จัดทำขั้นตอนการแยกเครือข่ายและการควบคุมสถานการณ์อย่างรวดเร็ว

คำแนะนำคู่มือการโจมตีด้วยแรนซัมแวร์

ตอบคำถามแบบปรนัยและคำถามจริงหรือเท็จ เติมคำในประโยคโดยใช้คลังคำ จับคู่คำนิยาม และแก้ปริศนาอักษรไขว้และค้นหาคำ นำความรู้ของคุณไปใช้กับ การกู้คืนจากแรนซัมแวร์ ปิดท้ายด้วยกิจกรรมเสริมคิดเร็ว

การโจมตีด้วยแรนซัมแวร์และการกู้คืนจากภัยพิบัติ (บทนำ)

เพย์โหลดของแรนซัมแวร์ล็อกที่เก็บข้อมูลของระบบด้วยการเข้ารหัส และเรียกร้องเงินเป็นสกุลเงินดิจิทัลเพื่อแลกกับคีย์ถอดรหัส การลดภัยคุกคามนี้ทำได้ด้วยกฎการแยกเครือข่าย การวิเคราะห์มัลแวร์ในแซนด์บ็อกซ์ และข้อมูลสำรองแบบ air-gapped cold ที่แข็งแกร่ง

อ่านแต่ละจุดตรวจสอบอย่างระมัดระวัง แล้วเลือกหรือเขียนคำตอบที่ถูกต้อง

จุดตรวจสอบที่ 1: ความท้าทายแบบปรนัย

1. 1. กลไกหลักของการโจมตีด้วยแรนซัมแวร์คืออะไร?
   - A. การเข้ารหัสไฟล์ของผู้ใช้เพื่อปฏิเสธการเข้าถึงระบบ
   - B. การแทรกคำสั่ง SQL ที่เป็นอันตรายลงในช่องแบบฟอร์ม
   - C. ดักดูแพ็กเก็ตเครือข่ายบน Wi-Fi สาธารณะ
   - D. การปลอมส่วนหัวอีเมลเพื่อข้ามการตรวจสอบ SPF

2. 2. การสำรองข้อมูลแบบออฟไลน์ (cold) คืออะไร?
   - A. สำเนาข้อมูลที่ตัดการเชื่อมต่อจากเครือข่ายเพื่อป้องกันมัลแวร์แพร่กระจาย
   - B. สำเนาสำรองที่เก็บไว้บนฮาร์ดไดรฟ์ของเว็บเซิร์ฟเวอร์หลัก
   - C. แคชชั่วคราวของล็อกรีจิสทรีระบบ
   - D. เครื่องมือผู้ดูแลระบบที่ใช้รีเซ็ตรหัสผ่านผู้ใช้

3. 3. ทีมรักษาความปลอดภัยควรแยกระบบที่ติดเชื้อออกอย่างไรระหว่างการโจมตีด้วยแรนซัมแวร์?
   - A. ถอดสายเครือข่ายและปิดอินเทอร์เฟซไร้สายทันที
   - B. อัปเกรดฐานข้อมูลลายเซ็นแอนตี้ไวรัส
   - C. ปิดเซิร์ฟเวอร์ DNS หลัก
   - D. เปลี่ยนชื่อนามสกุลไฟล์ที่ถูกบุกรุก

4. 4. เหตุใดหน่วยงานด้านความมั่นคงจึงแนะนำไม่ให้จ่ายค่าไถ่แรนซัมแวร์?
   - A. การจ่ายเงินเป็นการสนับสนุนผู้โจมตีและไม่รับประกันว่าจะได้รับคีย์ถอดรหัส
   - B. ทำให้กรมธรรม์ประกันภัยขององค์กรทั้งหมดเป็นโมฆะโดยอัตโนมัติ
   - C. แจ้งลูกค้าทุกคนทางอีเมลโดยอัตโนมัติ
   - D. ทำให้ไฟล์สำรองระบบที่เหลือเสียหาย

5. 5. แผนกู้คืนจากภัยพิบัติ (DRP) คืออะไร?
   - A. กระบวนการที่เป็นระบบเพื่อกู้คืนการดำเนินงานและข้อมูลหลังระบบถูกบุกรุก
   - B. การกำหนดค่าไฟร์วอลล์ที่แมปพอร์ตเครือข่ายขาเข้า
   - C. สคีมาฐานข้อมูลที่แสดงรายการสิทธิ์ผู้ดูแลระบบของผู้ใช้
   - D. โปรโตคอลยืนยันตัวตนอีเมลที่ปฏิเสธโดเมนที่ปลอมแปลง

จุดตรวจสอบที่ 2: ความท้าทายจริงหรือเท็จ

6 คำถาม 6

6. เพย์โหลดของแรนซัมแวร์สามารถแพร่กระจายไปยังข้อมูลสำรองออนไลน์ที่เชื่อมต่อกับเครือข่ายได้อย่างง่ายดาย

จริง เท็จ

7 คำถาม 7

7. การจ่ายค่าไถ่เป็นคริปโตเคอร์เรนซีรับประกันว่าไฟล์จะถูกถอดรหัสสำเร็จ

จริง เท็จ

8 คำถาม 8

8. การตัดการเชื่อมต่อระบบที่ติดเชื้อจากเครือข่ายช่วยหยุดแรนซัมแวร์ไม่ให้แพร่ไปยังระบบข้างเคียง

จริง เท็จ

9 คำถาม 9

9. แรนซัมแวร์ไม่เคยใช้การเข้ารหัสแบบสมมาตรเพื่อเข้ารหัสที่เก็บข้อมูลของระบบ

จริง เท็จ

10 คำถาม 10

10. การทดสอบขั้นตอนการกู้คืนข้อมูลเป็นประจำเป็นส่วนสำคัญของการกู้คืนจากภัยพิบัติ

จริง เท็จ

จุดตรวจสอบที่ 3: การเติมคำศัพท์สำคัญ

อ่านแต่ละประโยคด้านล่างและเติมคำที่ถูกต้องจากคลังคำลงในช่องว่าง

1. การปฏิเสธการเข้าถึงไฟล์ในเครื่องใช้ _____ ด้วยวิธีเข้ารหัสลับ
2. โค้ดประสงค์ร้ายที่ทำงานอยู่บนระบบคือ _____
3. สำเนาที่จัดเก็บนอกสถานที่แบบไม่เชื่อมต่อเป็น _____ ที่ปลอดภัย
4. การหยุดมัลแวร์ไม่ให้แพร่ต้องมีการ _____ ของเครือข่ายอุปกรณ์ปลายทาง
5. การชำระเงินด้วยสกุลเงินดิจิทัลที่อาชญากรไซเบอร์เรียกร้องคือ _____
6. การคืนไฟล์ข้อมูลที่ใช้งานได้เรียกว่าการ _____ จากภัยพิบัติ

คลังคำศัพท์

การเข้ารหัส | การแยกส่วน | กู้คืน | ค่าไถ่ | โทรจัน | แบ็กอัปเย็น | เพย์โหลด | ภัยพิบัติ

เขียนคำตอบของคุณที่นี่:

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

จุดตรวจสอบที่ 4: จับคู่แนวคิดเรื่องความปลอดภัย

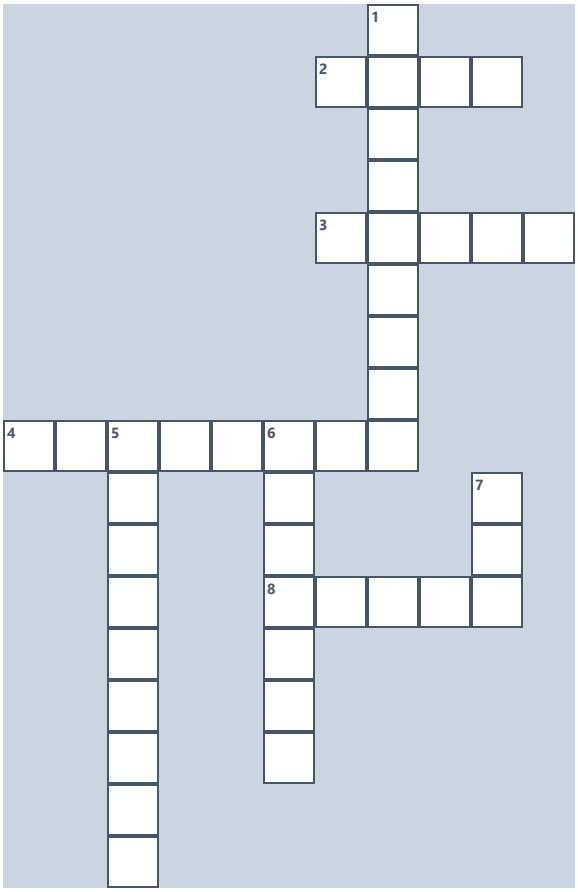
การจับคู่คำนิยาม

จับคู่ศัพท์แต่ละคำทางด้านซ้ายกับคำนิยามที่ถูกต้องทางด้านขวา โดยเขียนตัวอักษรที่ตรงกัน (A-H) ลงในช่องกรอก

☐	**1. การเข้ารหัส**	**A**	การตัดการเชื่อมต่อระบบเครือข่ายที่ติดเชื้อ
☐	**2. เพย์โหลด**	**B**	ไฟล์อันตรายที่ปลอมตัวเป็นไฟล์ปกติ
☐	**3. แบ็กอัปเย็น**	**C**	การล็อกไฟล์ด้วยการเข้ารหัส
☐	**4. การแยกส่วน**	**D**	เหตุการณ์ระบบหยุดชะงักครั้งใหญ่
☐	**5. เรียกค่าไถ่**	**E**	การรันซอฟต์แวร์อันตราย
☐	**6. การกู้คืน**	**F**	สำเนาออฟไลน์ที่ตัดการเชื่อมต่อ
☐	**7. ภัยพิบัติ**	**G**	การกู้คืนฐานข้อมูลจากข้อมูลสำรอง
☐	**8. โทรจัน**	**H**	คำขอจ่ายกุญแจเข้ารหัส

จุดตรวจสอบที่ 5: ปริศนาอักษรไขว้

แก้ปริศนาอักษรไขว้โดยพิมพ์ตัวอักษรลงในช่องสีขาวที่ใช้งานอยู่ ตัวเลขตรงกับเบาะแสด้านล่าง



แนวนอน

2. การเรียกร้องการจ่ายเพื่อแลกกุญแจเข้ารหัสลับ (4)

3. เหตุการณ์ระบบหยุดชะงักครั้งใหญ่ (5)

4. สำเนาออฟไลน์ที่ไม่ได้เชื่อมต่อ (8)

8. ไฟล์ประสงค์ร้ายที่ปลอมเป็นไฟล์ปกติ (5)

แนวตั้ง

1. การตัดการเชื่อมต่อระบบเครือข่ายที่ติดเชื้อ (9)

5. การล็อกไฟล์ด้วยวิธีเข้ารหัสลับ (9)

6. การรันซอฟต์แวร์ประสงค์ร้าย (7)

7. การคืนค่าฐานข้อมูลจากข้อมูลสำรอง (3)

จุดตรวจสอบที่ 5 แบบทางเลือก: คำใบ้ปริศนาอักษรไขว้ที่เข้าถึงได้

ผู้ใช้โปรแกรมอ่านหน้าจอและแป้นพิมพ์สามารถพิมพ์คำตอบปริศนาอักษรไขว้ลงในช่องข้อความด้านล่างได้โดยตรง

แนวนอน

2 แนวนอน: การเรียกร้องการจ่ายเพื่อแลกกุญแจเข้ารหัสลับ (4 ตัวอักษร):

3 แนวนอน: เหตุการณ์ระบบหยุดชะงักครั้งใหญ่ (5 ตัวอักษร):

4 แนวนอน: สำเนาออฟไลน์ที่ไม่ได้เชื่อมต่อ (8 ตัวอักษร):

8 แนวนอน: ไฟล์ประสงค์ร้ายที่ปลอมเป็นไฟล์ปกติ (5 ตัวอักษร):

แนวตั้ง

1 แนวตั้ง: การตัดการเชื่อมต่อระบบเครือข่ายที่ติดเชื้อ (9 ตัวอักษร):

5 แนวตั้ง: การล็อกไฟล์ด้วยวิธีเข้ารหัสลับ (9 ตัวอักษร):

6 แนวตั้ง: การรันซอฟต์แวร์ประสงค์ร้าย (7 ตัวอักษร):

7 แนวตั้ง: การคืนค่าฐานข้อมูลจากข้อมูลสำรอง (3 ตัวอักษร):

จุดตรวจสอบที่ 6: ค้นหาคำซ่อน

ค้นหาศัพท์สำคัญ 8 คำที่ซ่อนอยู่ในตารางด้านล่าง คำอาจเรียงในแนวนอน แนวตั้ง หรือแนวทแยง

ช มี ฟ บ า า ห ภั นี า ม กี จ า า
รี ต ว ย ง ก ค ย จ น โ ตี ว ร ตี
ว า ถ่ ล ล ด า พิ อ ย ท ช ฟ ก ก
น ล ไ ม า ป อ บั อ ม ร มี า ล ล
ว ป า จ า ก นี ติ กี พ จั ร ง แ า
ส่ ช ค่ า า า ลี จ ดี า น น ล ป็ ผ
ก ดี ช ก ด ร า ต เ า จ า ค ก ก
ย ดี า ช ว เ ก ด พ กี ด ท ผ อ้ ฟ
แ ช มี ม อ ข้ ต ฟ ย์ ร ดี า ท ป า
ร ส ท ข ข า กู้ า โ น ก า ล เ า
า ม ร มี า ร คื ร ห ช ก ด ง ย็ น
ก ร ต สี ย ห้ น ข ล มี ดี ด ด น ว
บ ฟ อ า ร ส ห ห ด รึ น ผ นี ม ผ
ดี ข กี ส บ ลี ง ด ร ด ค ผ ห ดี ป
ร กี นี า ต จ ห ดี ด บ ตี น สี ลี ว

รายการคำศัพท์

การเข้ารหัส | เพย์โหลด | แบ็กอัปเย็น | การแยกส่วน | ค่าไถ่ | กู้คืน | ภัยพิบัติ | โทรจัน

จุดตรวจสอบที่ 6 แบบทางเลือก: การจับคู่คำศัพท์ที่เข้าถึงได้

จับคู่ศัพท์ทั้ง 8 คำจากเกมค้นหาคำกับคำนิยามที่ถูกต้อง โดยเขียนตัวอักษร (A-H) ลงในช่องว่าง

ศัพท์สำคัญ
A. การเข้ารหัส
B. เพย์โหลด
C. แบ็กอัปเย็น
D. การแยกส่วน
E. ค่าไถ่
F. กู้คืน
G. ภัยพิบัติ
H. โทรจัน

คำนิยามและช่องจับคู่	
	1. สำเนาออฟไลน์ที่ไม่ได้เชื่อมต่อ
	2. ไฟล์ประสงค์ร้ายที่ปลอมเป็นไฟล์ปกติ
	3. การล็อกไฟล์ด้วยวิธีเข้ารหัสลับ
	4. การเรียกร้องการจ่ายเพื่อแลกกุญแจเข้ารหัสลับ
	5. การตัดการเชื่อมต่อระบบเครือข่ายที่ติดเชื้อ
	6. เหตุการณ์ระบบหยุดชะงักครั้งใหญ่
	7. การรันซอฟต์แวร์ประสงค์ร้าย
	8. การคืนค่าฐานข้อมูลจากข้อมูลสำรอง

จุดตรวจสอบที่ 7: ความท้าทายสลับตัวอักษร

เรียงตัวอักษรด้านล่างใหม่เพื่อเปิดเผยแนวคิดและศัพท์สำคัญของความปลอดภัยไซเบอร์ เขียนคำตอบของคุณในช่องกรอกที่ให้ไว้

1. า ข้ เ า ก ร หั ส ร
2. อั แ น บ็ ย์ เ ป ก
3. ถ่ ค่ ไ า
4. พิ ติ บั ภั ย
5. ห ด โ ย์ เ ล พ
6. ว แ า ส ก ก ย น ร
7. น คื กู้
8. น โ ร จั ท

กิจกรรมเสริม: คิดเร็ว

ตอบหมวดละ 3 คำตอบ ใครเติมรายการครบก่อนเป็นผู้ชนะ

1	ข้อมูลที่คุณไม่ควรแชร์เด็ดขาด			
2	อุปกรณ์ที่ถูกแฮกได้			
3	เหตุผลที่ไม่ควรจ่ายค่าไถ่			
4	นิสัยที่ปลอดภัยที่คุณเริ่มได้วันนี้			
5	เครื่องมือด้านความปลอดภัยที่คุณรู้จัก			
6	วิธีปกป้องบัญชีของคุณ			
7	สัญญาณที่บ่งบอกว่าคอมพิวเตอร์ติดเชื้อ			
8	สถานที่เก็บข้อมูลสำรอง			
9	ไฟล์ที่คุณไม่อยากสูญเสียเด็ดขาด			
10	วิธีที่แรนซัมแวร์แพร่กระจาย			
11	สิ่งที่ควรทำในชั่วโมงแรกของการโจมตี			
12	บุคคลที่ควรติดต่อระหว่างการโจมตี			
13	สิ่งที่แรนซัมแวร์ล็อกได้			
14	คำที่เกี่ยวข้องกับความปลอดภัยไซเบอร์			
15	องค์กรที่มักตกเป็นเป้าหมาย			

จุดตรวจสอบที่ 8: กรณีศึกษาความปลอดภัยไซเบอร์

นำแนวคิดที่คุณได้เรียนรู้ไปแก้สถานการณ์ในโลกจริงด้านล่าง

กรณีศึกษาที่ 1: การจำกัดเพย์โหลดแรนซัมแวร์ในองค์กร



สถานการณ์: เครือข่ายท้องถิ่นขององค์กรถูกแรนซัมแวร์ที่กำลังทำงานอยู่เจาะเข้ามา เซิร์ฟเวอร์ไฟล์สำคัญเริ่มแสดงนามสกุลไฟล์ .locked

คำถามอภิปราย: จงอธิบายขั้นตอนการจำกัดวงโดยละเอียด และสรุปโปรโตคอลการกู้คืนข้อมูล

กรณีศึกษาที่ 2: การประเมินสถาปัตยกรรมสำรองข้อมูลแบบออฟไลน์



สถานการณ์: องค์กรต้องการออกแบบกลยุทธ์การสำรองข้อมูลที่ลดความเสี่ยงที่ข้อมูลสำรองจะถูกบุกรุก แม้เครือข่ายภายในหลักจะถูกแรนซัมแวร์ยึดครองทั้งหมด

คำถามอภิปราย: ออกแบบระบบห้องนิรภัยสำหรับจัดเก็บข้อมูลสำรองออฟไลน์ที่ปลอดภัย

จุดตรวจสอบที่ 9: ถอดรหัสข้อความ

ผู้เชี่ยวชาญด้านความปลอดภัยไซเบอร์ปกป้องทรัพย์สินเครือข่ายจากผู้ก่อภัยคุกคามออนไลน์ ใช้คีย์ตัวอักษรเป็นตัวเลขด้านล่างเพื่อถอดรหัสข้อความ โดยเขียนตัวอักษรที่ตรงกันลงในช่องว่าง

คีย์เข้ารหัสตัวอักษรเป็นตัวเลข

ก=1 ข=2 ฃ=3 ค=4 ฅ=5 ฆ=6 ง=7 จ=8 ฉ=9 ช=10 ซ=11 ฌ=12
ญ=13 ฎ=14 ฏ=15 ฐ=16 ฑ=17 ฒ=18 ณ=19 ด=20 ต=21 ถ=22 ท=23 ธ=24
น=25 บ=26 ป=27 ผ=28 ฝ=29 พ=30 ฟ=31 ภ=32 ม=33 ย=34 ร=35 ฤ=36
ล=37 ฦ=38 ว=39 ศ=40 ษ=41 ส=42 ห=43 ฬ=44 อ=45 ฮ=46 ะ=47 ั=48
า=49 ำ=50 ิ=51 ี=52 ึ=53 ื=54 ุ=55 ู=56 เ=57 แ=58 โ=59 ใ=60
ไ=61 ็=62 ่=63 ้=64 ๊=65 ๋=66 ์=67

1	56	64	4	54	25		35	47	26	26		2	64	45	33	56	37

23	52	63	22	56	1		57	2	64	49	35	43	48	42

ข้อความที่ถอดรหัสแล้ว:

คำใบ้: ตัวเลขแต่ละตัวแทนตำแหน่งของตัวอักษรนั้นในตัวอักษรไทย (เช่น 1 = ก, 2 = ข, 67 = ์)

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับความปลอดภัยไซเบอร์ระดับพื้นฐาน (ส่วน A)

ทบทวนคำถามและคำตอบที่พบบ่อยเกี่ยวกับการลดภัยคุกคามออนไลน์

Q1: แรนซัมแวร์คืออะไร?

แรนซัมแวร์คือซอฟต์แวร์ที่เป็นอันตรายซึ่งออกแบบมาเพื่อบล็อกการเข้าถึงระบบคอมพิวเตอร์หรือไฟล์จนกว่าจะมีการจ่ายเงินค่าไถ่

Q2: แรนซัมแวร์แพร่กระจายอย่างไร?

ผ่านไฟล์แนบอีเมลฟิชชิง ช่องโหว่ซอฟต์แวร์ที่ไม่ได้แพตช์ และระบบเข้าถึงระยะไกลที่ถูกเจาะ [1]

Q3: เหตุใดจึงมีการขอให้ชำระเงินด้วยสกุลเงินดิจิทัล?

คริปโตเคอร์เรนซีอย่างบิตคอยน์ให้การไม่เปิดเผยตัวตนในระดับหนึ่ง ทำให้เจ้าหน้าที่บังคับใช้กฎหมายติดตามเงินได้ยาก

Q4: โปรแกรมป้องกันไวรัสบล็อกแรนซัมแวร์ได้หรือไม่?

ใช่ แต่แอนติไวรัสแบบอิงลายเซ็นอาจล้มเหลวต่อเพย์โหลดแรนซัมแวร์แบบ zero-day ที่สร้างขึ้นใหม่

Q5: การสำรองข้อมูลแบบ air-gapped คืออะไร?

สำเนาสำรองที่ไม่มีการเชื่อมต่อทางกายภาพหรือทางตรรกะกับเครือข่ายหลัก เพื่อป้องกันไม่ให้ความเสียหายลุกลาม

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับความปลอดภัยไซเบอร์ระดับพื้นฐาน (ส่วน B)

ทบทวนคำถามและคำตอบที่พบบ่อยเกี่ยวกับการลดภัยคุกคามออนไลน์

Q6: การรีดไถสองชั้น (double extortion) คืออะไร?

เมื่อผู้โจมตีไม่เพียงเข้ารหัสไฟล์ แต่ยังขโมยข้อมูลสำคัญเพื่อขู่ว่าจะเผยแพร่สู่สาธารณะหากไม่จ่ายเงิน

Q7: decryptor คืออะไร?

ยูทิลิตีซอฟต์แวร์ที่มีคีย์เข้ารหัสซึ่งจำเป็นต่อการกู้คืนไฟล์ที่ถูกล็อกให้กลับเป็นข้อความธรรมดา

Q8: คุณตรวจจับแรนซัมแวร์ได้ตั้งแต่เนิ่นๆ อย่างไร?

ด้วยการเฝ้าดูระบบไฟล์เพื่อหากิจกรรมแก้ไขและเปลี่ยนชื่อไฟล์จำนวนมากอย่างฉับพลัน

Q9: ประกันภัยมีบทบาทอะไร?

ประกันภัยไซเบอร์ช่วยครอบคลุมค่าใช้จ่ายในการกู้คืนได้ แต่เงื่อนไขความคุ้มครองและกฎเรื่องการจ่ายค่าไถ่แตกต่างกันตามกรมธรรม์

Q10: ฉันควรรีบูตระบบที่ติดเชื้อหรือไม่?

ไม่ การรีบูตอาจทำลายหลักฐานในหน่วยความจำแบบชั่วคราว ให้แยกเครื่องออกจากเครือข่ายแทน [1]

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับความปลอดภัยระดับสูง (ส่วน C)

สำรวจแง่มุมทางเทคนิคขั้นสูงของกรอบความปลอดภัย การวิเคราะห์มัลแวร์ และการปฏิบัติตามข้อกำหนดด้านข้อมูล

Q1: แรนซัมแวร์ใช้การเข้ารหัสแบบอสมมาตรอย่างไร?

ใช้คีย์สาธารณะที่ฝังในมัลแวร์เพื่อเข้ารหัสไฟล์ ต้องใช้คีย์ส่วนตัวของผู้โจมตีจึงจะถอดรหัสได้

Q2: เหตุใดจึงมีการใช้การเข้ารหัสแบบสมมาตรด้วย?

การเข้ารหัสแบบสมมาตร (เช่น AES) ทำงานเร็วและสามารถล็อกฐานข้อมูลขนาดใหญ่ได้ในไม่กี่นาที ขณะที่กุญแจอสมมาตรปกป้องกุญแจ AES

Q3: การแบ่งส่วนเชิงตรรกะ (logical segmentation) คืออะไร?

การแบ่งเครือข่ายเป็นโซนที่แยกจากกัน ป้องกันไม่ให้มัลแวร์แพร่ขยายในแนวขวางจากโหนดเวิร์กสเตชันไปยังเซิร์ฟเวอร์หลัก

Q4: ที่เก็บข้อมูลแบบ WORM คืออะไร?

สื่อแบบเขียนครั้งเดียวอ่านได้หลายครั้ง (Write-Once, Read-Many) ซึ่งป้องกันไม่ให้เพย์โหลดของแรนซัมแวร์แก้ไข เขียนทับ หรือลบข้อมูลสำรอง

Q5: shadow copy คืออะไร?

สแนปชอตสำรองข้อมูลภายในเครื่องที่ Windows สร้างขึ้น โดยปกติแรนซัมแวร์จะลบสิ่งเหล่านี้ก่อนด้วยเครื่องมือผู้ดูแลระบบ

จุดตรวจสอบที่ 10: คำถามที่พบบ่อยเกี่ยวกับความปลอดภัยระดับสูง (ส่วน D)

สำรวจแง่มุมทางเทคนิคขั้นสูงของกรอบความปลอดภัย การวิเคราะห์มัลแวร์ และการปฏิบัติตามข้อกำหนดด้านข้อมูล

Q6: การขโมยข้อมูลรับรองนำไปสู่แรนซัมแวร์ได้อย่างไร?

ผู้โจมตีซื้อข้อมูลล็อกอินผู้ดูแลระบบที่รั่วไหลเพื่อเข้าสู่ระบบผ่านริโมตเดสก์ท็อป แล้วรันแรนซัมแวร์ด้วยตนเองทั่วทั้งเครือข่าย

Q7: การทดสอบกู้คืนข้อมูลแบบ dry-run คืออะไร?

การกู้คืนฐานข้อมูลสำรองเป็นประจำในสภาพแวดล้อมทดสอบที่แยกต่างหากเพื่อตรวจสอบว่าความเร็วในการกู้คืนและความสมบูรณ์ของข้อมูลเป็นไปตามเกณฑ์การกู้คืนจากภัยพิบัติ

Q8: การตรวจจับที่อุปกรณ์ปลายทาง (EDR) หยุดแรนซัมแวร์ได้อย่างไร?

ด้วยการวิเคราะห์พฤติกรรมของกระบวนการ (เช่น การเข้ารหัสอย่างรวดเร็ว) และระงับแอปพลิเคชันที่ผิดปกติอย่างรวดเร็ว

Q9: โมเดลแรนซัมแวร์ในรูปแบบบริการ (RaaS) คืออะไร?

โมเดลแฟรนไชส์ที่นักพัฒนามัลแวร์ให้เช่าเครื่องมือสร้างแรนซัมแวร์แก่พันธมิตรเพื่อแลกกับส่วนแบ่งจากเงินที่ได้

Q10: RDP ที่ไม่ได้แพตช์กระตุ้นแรนซัมแวร์ได้อย่างไร?

เกตเวย์ Remote Desktop Protocol ที่เปิดเผยและไม่ได้แพตช์ทำให้ผู้โจมตีเดาล็อกอินแบบ brute-force และเปิดใช้มัลแวร์ด้วยตนเองได้

ส่วนที่ 11: ข้อเท็จจริงด้านความปลอดภัยไซเบอร์ในโลกจริง 10 ข้อและข้อมูลเชิงลึก

ทบทวนข้อเท็จจริงในโลกจริงเกี่ยวกับการละเมิดความปลอดภัย กลไกการป้องกัน และมาตรฐานการปฏิบัติตามข้อกำหนด

1. ข้อมูลเชิงลึกเรื่องความปลอดภัย

ผู้ก่อการแรนซัมแวร์มักใช้เครื่องมือเช่น vssadmin.exe เพื่อลบ shadow copy ของ Windows และบล็อกการกู้คืนในเครื่อง [1]

2. ข้อมูลเชิงลึกเรื่องความปลอดภัย

โดยทั่วไปใช้กุญแจสมมาตร AES-256 เข้ารหัสเพย์โหลดของไฟล์ แล้วล็อกกุญแจนั้นด้วยกุญแจสาธารณะ RSA

3. ข้อมูลเชิงลึกเรื่องความปลอดภัย

การกู้คืนจากการโจมตีด้วยแรนซัมแวร์ที่สำเร็จอาจใช้เวลาหลายสัปดาห์ ซึ่งเป็นเหตุผลที่ข้อมูลสำรองออฟไลน์ที่ผ่านการทดสอบแล้วมีความสำคัญ

4. ข้อมูลเชิงลึกเรื่องความปลอดภัย

FBI ไม่สนับสนุนการจ่ายค่าไถ่ และเตือนว่าการจ่ายไม่ได้รับประกันว่าคุณจะได้ข้อมูลคืน [2]

5. ข้อมูลเชิงลึกเรื่องความปลอดภัย

แผนกู้คืนจากภัยพิบัติ (DRP) ควรกำหนดเป้าหมายเวลากู้คืน (RTO) และเป้าหมายจุดกู้คืน (RPO)

6. ข้อมูลเชิงลึกเรื่องความปลอดภัย

FBI แนะนำให้ใช้ข้อมูลสำรองที่เข้ารหัสและเปลี่ยนแปลงไม่ได้ (immutable) หมายความว่าไม่สามารถแก้ไขหรือลบได้ [3]

7. ข้อมูลเชิงลึกด้านความปลอดภัย

ผู้พัฒนาแรนซัมแวร์ใช้เทคนิคการพรางโค้ดขั้นสูงเพื่อหลบเลี่ยงตัวสแกนของโปรแกรมป้องกันไวรัสแบบอิงลายเซ็นแบบดั้งเดิม

8. ข้อมูลเชิงลึกด้านความปลอดภัย

การแบ่งส่วนเครือข่ายจำกัดการเคลื่อนที่ในแนวขวาง ช่วยหยุดแรนซัมแวร์ไม่ให้แพร่กระจายไปไกลกว่าโฮสต์แรกที่ติดเชื้อ [3]

9. ข้อมูลเชิงลึกด้านความปลอดภัย

บริการระยะไกลที่เปิดเผยและรักษาความปลอดภัยไม่ดี เช่น Remote Desktop Protocol (RDP) เป็นช่องทางเข้าที่พบบ่อยของแรนซัมแวร์ [1]

10. ข้อมูลเชิงลึกเรื่องความปลอดภัย

CISA แนะนำให้เก็บข้อมูลสำรองที่เข้ารหัสไว้แบบออฟไลน์ เนื่องจากแรนซัมแวร์หลายรูปแบบจะค้นหาและลบข้อมูลสำรองที่เข้าถึงได้ [1]

แหล่งอ้างอิงทางเทคนิค

คู่มือการเรียนและปริศนาเซิงโต้ตอบรวบรวมจากมาตรฐานระดับโลกของ NIST, OWASP และการปฏิบัติตามข้อกำหนดด้านความเป็นส่วนตัวของข้อมูล

เอกสารอ้างอิงทางวิชาการและอุตสาหกรรม

[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

เฉลย: จุดตรวจสอบที่ 1 – แบบปรนัย

1 คำถาม 1 — คำตอบที่ถูกต้อง: A

หมายเหตุสำหรับผู้สอน

กลไกหลักของการโจมตีด้วยแรนซัมแวร์คืออะไร? → การเข้ารหัสไฟล์ของผู้ใช้เพื่อปฏิเสธการเข้าถึงระบบ

2 คำถาม 2 — คำตอบที่ถูกต้อง: A

หมายเหตุสำหรับผู้สอน

การสำรองข้อมูลแบบออฟไลน์ (cold) คืออะไร? → สำเนาข้อมูลที่ตัดการเชื่อมต่อจากเครือข่ายเพื่อป้องกันมัลแวร์แพร่กระจาย

3 คำถาม 3 — คำตอบที่ถูกต้อง: A

หมายเหตุสำหรับผู้สอน

ทีมรักษาความปลอดภัยควรแยกระบบที่ติดเชื้อออกอย่างไรระหว่างการโจมตีด้วยแรนซัมแวร์? → ถอดสายเครือข่ายและปิดอินเทอร์เฟซไร้สายทันที

4 คำถาม 4 — คำตอบที่ถูกต้อง: A

หมายเหตุสำหรับผู้สอน

เหตุใดหน่วยงานด้านความมั่นคงจึงแนะนำไม่ให้จ่ายค่าไถ่แรนซัมแวร์? → การจ่ายเงินเป็นการสนับสนุนผู้โจมตีและไม่รับประกันว่าจะได้รับคีย์ถอดรหัส

5 คำถาม 5 — คำตอบที่ถูกต้อง: A

หมายเหตุสำหรับผู้สอน

แผนกู้คืนจากภัยพิบัติ (DRP) คืออะไร? → กระบวนการที่เป็นระบบเพื่อกู้คืนการดำเนินงานและข้อมูลหลังระบบถูกบุกรุก

เฉลย: จุดตรวจสอบที่ 2 – จริงหรือเท็จ

6 **คำถาม 6** คำตอบที่ถูกต้อง: จริง

หมายเหตุสำหรับผู้สอน

เพย์โหลดของแรนซัมแวร์สามารถแพร่กระจายไปยังข้อมูลสำรองออนไลน์ที่เชื่อมต่อกับเครือข่ายได้อย่างง่ายดาย

7 **คำถาม 7** คำตอบที่ถูกต้อง: เท็จ

หมายเหตุสำหรับผู้สอน

เท็จ: FBI เตือนว่าการจ่ายเงินไม่รับประกันว่าคุณจะได้ข้อมูลคืน

8 **คำถาม 8** คำตอบที่ถูกต้อง: จริง

หมายเหตุสำหรับผู้สอน

จริง: CISA แนะนำให้ถอดปลั๊กโฮสต์ที่ติดเชื้อหรือนำเครือข่ายออฟไลน์เพื่อจำกัดการแพร่กระจาย

9 **คำถาม 9** คำตอบที่ถูกต้อง: เท็จ

หมายเหตุสำหรับผู้สอน

เท็จ: แรนซัมแวร์มักเข้ารหัสไฟล์ด้วยรหัสลับแบบสมมาตรที่รวดเร็ว เช่น AES

10 **คำถาม 10** คำตอบที่ถูกต้อง: จริง

หมายเหตุสำหรับผู้สอน

การทดสอบขั้นตอนการกู้คืนข้อมูลเป็นประจำเป็นส่วนสำคัญของการกู้คืนจากภัยพิบัติ

เฉลยคำศัพท์และเกณฑ์การให้คะแนน

เกณฑ์การให้คะแนนของผู้สอน: ให้ 1 คะแนนสำหรับการจับคู่ที่ถูกต้องแต่ละข้อ (รวม 8 คะแนน) และคำศัพท์บริบท (รวม 6 คะแนน)

จุดตรวจสอบที่ 4: เฉลย – จับคู่แนวคิด

C 1. การเข้ารหัส	E 2. เพย์โหลด	F 3. แบ็กอัปเย็น	A 4. การแยกส่วน
H 5. เรียกค่าไถ่	G 6. การกู้คืน	D 7. ภัยพิบัติ	B 8. โทรจัน

จุดตรวจสอบที่ 3: เฉลย – คำศัพท์สำคัญ

1 การเข้ารหัส	2 เพย์โหลด	3 แบ็กอัปเย็น	4 การแยกส่วน
5 ค่าไถ่	6 กู้คืน		

จุดตรวจสอบที่ 6 แบบทางเลือก: เฉลย – จับคู่คำ

1 C – แบ็กอัปเย็น	2 H – โทรจัน	3 A – การเข้ารหัส	4 E – ค่าไถ่
5 D – การแยกส่วน	6 G – ภัยพิบัติ	7 B – เพย์โหลด	8 F – กู้คืน

หมายเหตุการอภิปรายสำหรับผู้สอน

คำศัพท์สำคัญ:
ตรวจสอบว่าผู้เรียนอธิบาย การเข้ารหัส เพย์โหลด และ แบ็กอัปเย็น ด้วยคำพูดของตนเองและยกตัวอย่างแต่ละคำได้หรือไม่

กรณีศึกษา:
ให้ผู้เรียนใช้ข้อเท็จจริงจากใบงานเป็นเหตุผลประกอบข้อเสนอแนะ ไม่ใช่ความคิดเห็น

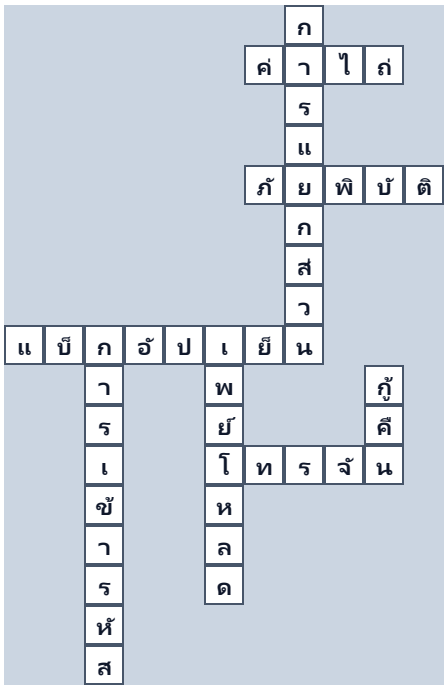
การประเมินแหล่งข้อมูล:
ให้ผู้เรียนตรวจสอบข้อความอย่างน้อยหนึ่งข้อจากแหล่งอ้างอิงของใบงาน และอภิปรายว่าเหตุใดตัวเลข ราคา และกฎเกณฑ์อาจเปลี่ยนแปลงไปตามเวลา

เฉลยปริศนาและหมายเหตุสำหรับผู้สอน

เฉลยการค้นหาคำศัพท์

ช	มี	ฟ	บ	า	า	ห	ภั	นี	า	ม	กี	จ	า	า
รี	ต	ว	ย	ง	ก	ค	ย	จ	น	โ	ตี	ว	ร	ตี
ว	า	ถ่	ล	ล	ด	า	พิ	อ	ย	ท	ซ	ฟ	ก	ก
น	ล	ไ	ม	า	ป	อ	บั	อ	ม	ร	มี	า	ล	ล
ว	ป	า	จ	า	ก	นี	ติ	กี	พ	จั	ร	ง	แ	า
ส่	ช	ค่	า	า	า	ลี	จ	ดี	า	น	น	ล	บ็	ผ
ก	ดี	ช	ก	ด	ร	า	ต	เ	า	จ	า	ค	ก	ก
ย	ดี	า	ช	ว	เ	ก	ด	พ	กี	ด	ท	ผ	อ้	ฟ
แ	ช	มี	ม	อ	ข้	ต	ฟ	ย์	ร	ดี	า	ท	ป	า
ร	ส	ท	ข	ข	า	กู้	า	โ	น	ก	า	ล	เ	า
า	ม	ร	มี	า	ร	คื	ร	ห	ช	ก	ด	ง	ย็	น
ก	ร	ต	สี	ย	ห้	น	ข	ล	มี	ดี	ด	ด	น	ว
บ	ฟ	อ	า	ร	ส	ห	ห	ด	รี	น	ผ	นี	ม	ผ
ดี	ข	กี	ส	บ	ลี	ง	ด	ร	ด	ค	ผ	ห	ดี	ป
ร	กี	นี	า	ด	จ	ห	ดี	ด	บ	ดี	น	สี	ลี	ว

เฉลยปริศนาอักษรไขว้



คู่มือผู้สอนสำหรับเฉลยอักษรไขว้

แนวนอน

2 แนวนอน: ค่าไถ่ การเรียกร้องการจ่ายเพื่อแลกกุญแจเข้ารหัสลับ (4 ตัวอักษร)

3 แนวนอน: ภัยพิบัติ เหตุการณ์ระบบหยุดชะงักครั้งใหญ่ (5 ตัวอักษร)

4 แนวนอน: แบ็กอัปเย็น สำเนาออฟไลน์ที่ไม่ได้เชื่อมต่อ (8 ตัวอักษร)

8 แนวนอน: โทรจัน ไฟล์ประสงค์ร้ายที่ปลอมเป็นไฟล์ปกติ (5 ตัวอักษร)

แนวตั้ง

1 แนวตั้ง: การแยกส่วน การตัดการเชื่อมต่อระบบเครือข่ายที่ติดเชื้อ (9 ตัวอักษร)

5 แนวตั้ง: การเข้ารหัส การล็อกไฟล์ด้วยวิธีเข้ารหัสลับ (9 ตัวอักษร)

6 แนวตั้ง: เพย์โหลด การรันซอฟต์แวร์ประสงค์ร้าย (7 ตัวอักษร)

7 แนวตั้ง: กู้คืน การคืนค่าฐานข้อมูลจากข้อมูลสำรอง (3 ตัวอักษร)

เฉลยคำสลับอักษรและรหัสลับ

เฉลยสำหรับกิจกรรมเรียงอักษรศัพท์และภารกิจรหัสลับ

เฉลยการเรียงคำที่สลับตัวอักษร

1. าข้เากรหัสร → **การเข้ารหัส**
2. อัแนบ็ย็เปก → **แบ็กอัปเย็น**
3. ถ่ค่ไา → **ค่าไถ่**
4. พิติบัภัย → **ภัยพิบัติ**
5. หดโย์เลพ → **เพย์โหลด**
6. วแาส่กกยนร → **การแยกส่วน**
7. นคืกู้ → **กู้คืน**
8. นโรจัท → **โทรจัน**

เฉลยภารกิจรหัสลับ

"กู้คืน ระบบ ข้อมูล ที่ถูก เข้ารหัส"

เฉลยกรณีศึกษา

A กรณีศึกษาที่ 1: การจำกัดเพย์โหลดแรนซัมแวร์ในองค์กร

เฉลยสำหรับผู้สอน

แนวทางการให้คะแนน

คำตอบของนักเรียนควรครอบคลุมประเด็นต่อไปนี้:

- การวิเคราะห์สถานการณ์: เครือข่ายท้องถิ่นขององค์กรถูกแรนซัมแวร์ที่กำลังทำงานเจาะเข้ามา เซิร์ฟเวอร์ไฟล์หลักเริ่มแสดงนามสกุลไฟล์ .locked
- กลยุทธ์และแนวทางแก้ไขที่แนะนำ: ตัดการเชื่อมต่อเซิร์ฟเวอร์ที่ได้รับผลกระทบทั้งหมดออกจากเครือข่ายท้องถิ่น ยุติเซสชันผู้ดูแลระบบที่ใช้งานอยู่ กู้คืนไฟล์ที่ไม่ได้รับผลกระทบจากระบบสำรองข้อมูลออฟไลน์ที่ปลอดภัยและล็อกการเขียน

B กรณีศึกษาที่ 2: การประเมินสถาปัตยกรรมสำรองข้อมูลแบบออฟไลน์

เฉลยสำหรับผู้สอน

แนวทางการให้คะแนน

คำตอบของนักเรียนควรครอบคลุมประเด็นต่อไปนี้:

- การวิเคราะห์สถานการณ์: องค์กรต้องการออกแบบกลยุทธ์การสำรองข้อมูลที่ลดความเสี่ยงที่ข้อมูลสำรองจะถูกบุกรุก แม้เครือข่ายภายในหลักจะถูกแรนซัมแวร์ยึดครองทั้งหมด
- กลยุทธ์และแนวทางแก้ไขที่แนะนำ: ใช้ที่เก็บข้อมูลแบบเขียนครั้งเดียวอ่านได้หลายครั้ง (WORM) สร้าง air-gap เชิงตรรกะ โดยตัดระบบสำรองข้อมูลออกจากเครือข่ายทั้งหมด และบังคับให้หมุนเวียนสื่อบันทึกข้อมูลจริงทุกวัน