06016405,06016309 CYBERSECURITY FUNDAMENTAL (2/2024)

Started on	Wednesday, 18 December 2024, 9:13 AM
State	Finished
Completed on	Wednesday, 18 December 2024, 9:59 AM
Time taken	46 mins 11 secs
Grade	Not yet graded

Question **1**

Complete

Marked out of 1.00

CIA Triad ซึ่งเป็นส่วนหนึ่งที่เป็นของ Basic Security Principles มีด้านใดบ้าง จงอธิบาย

1. Data Confidentiality (ข้อมูลมีความเป็นความลับ)
- ป้องกันไม่ให้บุคคลที่ไม่มีสิทธิ์เข้าถึงได้โดยไม่ได้รับอนุญาต

2. Data Integrity (ความเป็นต้นฉบับของข้อมูล)
- ปกป้องข้อมูลจากการแก้ไขโดยไม่ได้รับอนุญาต
- ข้อมูลต้องถูกต้องและเชื่อถือได้

3. Data Availability (ความพร้อมใช้งานของข้อมูล)
- การทำให้ข้อมูลและระบบพร้อมใช้งานตลอดเวลา

Question **2**

Complete

Marked out of 1.00

นอกเหนือจาก CIA Triad แล้ว Security Principles มีด้านใดอีกบ้าง จงอธิบาย

- ยืนยันว่าข้อมูลหรือการสื่อสารมาจากแหล่งที่ถูกต้องและน่าเชื่อถือ

Accountability (ความรับผิดชอบ)
- สามารถติดตาม บันทึกการกระทำและตรวจสอบกิจกรรมต่าง ๆ ที่เกิดขึ้นในระบบได้
- ช่วยให้สามารถระบุและตรวจสอบการกระทำของผู้ใช้หรือระบบได้

Resilience (ความยืดหยุ่น)
- ความสามารถของระบบในการตอบสนองต่อการโจมตีหรือความเสียหายและสามารถกลับมาทำงานได้อย่างรวดเร็ว
- เพื่อให้ระบบยังคงพร้อมใช้งานแม้ในสภาวะฉุกเฉิน

Privacy (ความเป็นส่วนตัว)
- การรักษาความเป็นส่วนตัวของข้อมูลส่วนบุคคลและข้อมูลสำคัญ

Auditability (การตรวจสอบได้)
- ความสามารถในการตรวจสอบและยืนยันว่าระบบมีการทำงานตามที่กำหนดไว้จริง

Question **3**

Complete

Marked out of 1.00

จากที่ได้เรียนไปแล้ว Data มีกี่ States อะไรบ้าง พร้อมกับยกตัวอย่าง Threats ที่มีผลกระทบต่อ Data แต่ละ State

1. Data at Rest (ข้อมูลที่พักอยู่)
- ข้อมูลที่ไม่ได้ถูกส่งผ่านหรือประมวลผล เช่น ข้อมูลที่เก็บอยู่ในฮาร์ดไดรฟ์หรือเซิร์ฟเวอร์
- ตัวอย่าง threat -> การโจมตีทางกายภาพ คือ การเข้าถึงอุปกรณ์จัดเก็บข้อมูลโดยไม่ได้รับอนุญาต

2. Data in Transit (ข้อมูลที่กำลังส่ง)
- ข้อมูลที่กำลังถูกส่งจากที่หนึ่งไปยังอีกที่หนึ่ง เช่น ข้อมูลที่ส่งผ่านเครือข่ายอินเทอร์เน็ต
- ตัวอย่าง threat -> การดักฟังข้อมูลที่กำลังส่งผ่านเครือข่าย

3. Data in Process (ข้อมูลที่กำลังประมวลผล)
- ข้อมูลที่กำลังถูกใช้งานหรือประมวลผล เช่น ข้อมูลที่ถูกแก้ไขหรือคำนวณในระบบ
- ตัวอย่าง threat -> การโจมตีแบบ Data Tampering คือ การแก้ไขหรือเปลี่ยนแปลงข้อมูลในระหว่างการประมวลผล

Question **4**

Complete

Marked out of 1.00

Threats สามารถถูกจัดเป็นกลุ่มตามนิยาม Threat Consequence ใน RFC 2828 ได้กี่กลุ่ม แต่ละกลุ่มมีลักษณะเฉพาะอย่างไร

1. Unauthorized Disclosure (การเผยแพร่โดยไม่ได้รับอนุญาต)
   - Exposure: การเผยแพร่ข้อมูลลับโดยตรงให้กับองค์กรที่ไม่ได้รับอนุญาต
   - Interception: การดักจับข้อมูลขณะเคลื่อนที่โดยองค์กรที่ไม่ได้รับอนุญาต
   - Inference: การเข้าถึงข้อมูลลับโดยองค์กรที่ไม่ได้รับอนุญาตโดยการอธิบายจากลักษณะหรือผลของการสื่อสาร
   - Intrusion: การเข้าถึงข้อมูลลับโดยองค์กรที่ไม่ได้รับอนุญาตโดยการละเอียดระบบความปลอดภัย

2. Deception (การล่วงหลบ)
   - Masquerade: การเข้าถึงระบบหรือการกระทำความผิดโดยการแสดงตัวเป็นผู้ที่ได้รับอนุญาต
   - Falsification: การใช้ข้อมูลที่ไม่ถูกต้องเพื่อล่วงหลบผู้ที่ได้รับอนุญาต
   - Repudiation: การปฏิเสธความรับผิดชอบโดยการโจมตีหรือการกระทำความผิด

3. Disruption (การขัดขวาง)
   - Incapacitation: การขัดขวางการทำงานของระบบโดยการทำให้ส่วนประกอบของระบบหยุดทำงาน
   - Corruption: การปรับแก้ข้อมูลหรือการทำงานของระบบให้ผิดพลาด
   - Obstruction: การขัดขวางการส่งข้อมูลหรือบริการของระบบ

Question **5**

Complete

Marked out of 1.00

จงอธิบายบทบาทของ Security Controls หรือ Countermeasures ที่มีต่อ Asset ในบริบทของเรื่อง Cybersecurity

Countermeasures ในด้าน cybersecurity คือ การใช้เทคโนโลยีและนโยบายต่าง ๆ เพื่อป้องกันและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

Question **6**

Complete

Marked out of 1.00

Security Controls สามารถแบ่งกลุ่มได้กี่กลุ่ม อะไรบ้าง จงอธิบายลักษณะเฉพาะของแต่ละกลุ่ม

1. Preventive Controls (การควบคุมเชิงป้องกัน)
- มาตรการที่ใช้เพื่อป้องกันการเกิดเหตุการณ์ที่ไม่พึงประสงค์ เช่น การใช้ไฟร์วอลล์ การเข้ารหัสข้อมูล และการควบคุมการเข้าถึง

2. Detective Controls (การควบคุมเชิงตรวจจับ)
- มาตรการที่ใช้เพื่อตรวจจับเหตุการณ์ที่ไม่พึงประสงค์ที่เกิดขึ้นแล้ว เช่น การตรวจสอบบันทึกเหตุการณ์ การตรวจจับการบุกรุก และการตรวจสอบความปลอดภัย

3. Corrective Controls (การควบคุมเชิงแก้ไข)
- มาตรการที่ใช้เพื่อแก้ไขผลกระทบจากเหตุการณ์ที่ไม่พึงประสงค์ เช่น การกู้คืนข้อมูล การแก้ไขช่องโหว่ และการปรับปรุงระบบความปลอดภัย

Question **7**

Complete

Marked out of 1.00

ก่อนที่จะตัดสินใจเลือก Security Control มาใช้งาน นศ ต้องทำสิ่งใดก่อน และใช้เงื่อนไขใดในการตัดสินใจเลือกดังกล่าว

1. การประเมินความเสี่ยง: นักศึกษาควรทำการประเมินความเสี่ยงเพื่อระบุภัยคุกคามและช่องโหว่ที่อาจเกิดขึ้นกับระบบและข้อมูลขององค์กร การประเมินความเสี่ยงนี้จะช่วยให้นักศึกษาทราบถึงความเสี่ยงที่ต้องการการควบคุมและการป้องกัน.

2. การวิเคราะห์ความต้องการ: นักศึกษาควรทำการวิเคราะห์ความต้องการขององค์กรเพื่อระบุว่ามีข้อมูลหรือระบบใดที่ต้องการการป้องกันเป็นพิเศษ การวิเคราะห์นี้จะช่วยให้นักศึกษาทราบถึงความต้องการที่แท้จริงขององค์กร.

3. การศึกษาและเปรียบเทียบ Security Control: นักศึกษาควรศึกษาและเปรียบเทียบ Security Control ที่มีอยู่ในตลาด เพื่อหาตัวเลือกที่เหมาะสมที่สุดสำหรับองค์กร การเปรียบเทียบนี้ควรพิจารณาถึงประสิทธิภาพ ความสามารถในการป้องกัน และค่าใช้จ่าย.

เงื่อนไขในการตัดสินใจเลือก Security Control ได้แก่

1. ความเหมาะสมกับความต้องการขององค์กร: Security Control ที่เลือกควรสามารถตอบสนองความต้องการขององค์กรได้อย่างมีประสิทธิภาพ

2. ความสามารถในการป้องกัน: Security Control ควรมีความสามารถในการป้องกันภัยคุกคามและช่องโหว่ที่ระบุในการประเมินความเสี่ยง

Question **8**

Not answered

Marked out of 1.00

Risk Treatments **คืออะไร มีกี่รูปแบบ แต่ละรูปแบบเกี่ยวอย่างไรกับการเลือก** Security Controls

Question **9**

Not answered

Marked out of 1.00

จงอธิบายคำจำกัดความของคำต่อไปนี้
1. Attack Vector
2. Attack Surface
3. IOC

Question **10**

Not answered

Marked out of 1.00

Pillars หลักทั้ง 3 ที่สำคัญของ Security Controls หรือ Countermeasure หรือ Safeguards มีอะไรบ้าง และจงอธิบายลักษณะเฉพาะของแต่ละ Pillar

Previous Activity

Jump to...

Next Activity