คำถามท้ายบทที่ 7.2

1. ผู้กระทำผิด มีประเภทใดบ้าง

1.แฮคเกอร์ (Hacker)

2.แครกเกอร์ (Cracker)

3.Malicious Insider

4.Industrial Spies

5.Cybercriminal

6.Cyberterrorist

2 การประเมินความเสี่ยง (Risk Assessment) คืออะไร

การพิจารณาถึงภัยคุกคาม (หรือการโจมตี) ประเภทต่าง ๆ ที่อาจเกิดขึ้นกับระบบคอมพิวเตอร์และระบบเครือข่ายขององค์กร โดยการพิจารณาถึงความเป็นไปได้ในการเกิดภัยคุกคามแต่ละประเภท

3. นโยบายความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศ (IT Security Policy) คืออะไร

คือการกำหนดข้อบังคับตามความต้องการด้านความมั่นคงปลอดภัยและการควบคุมขององค์กร ร่วมถึงกำหนดบทลงโทษสำหรับผู้ละเมิด

4. การป้องกันแบบระดับชั้น (Layered Security Solution) มีอะไรบ้าง

- ติดตั้ง Firewall
- ติดตั้ง Antivirus Software
- ป้องกันการโจมตีจากพนักงานในองค์กรเอง
- ซ่อมแซมซอฟต์แวร์อยู่เสมอ
- ตรวจสอบการสำรองข้อมูลอย่างสม่ำเสมอ
- จัดให้มีการตรวจสอบความมั่นคงปลอดภัยเป็นระยะ

5. Intrusion Detection System (IDS) และ Honey Pot คืออะไร

IDS คือ ระบบซอฟต์แวร์และ/หรือฮาร์ดแวร์ที่ ติดตามการจราจรและพฤติกรรมที่น่าสงสัยในเครือข่าย และทำการแจ้งเตือนไปยังระบบหรือผู้ดูแลระบบทันทีที่พบการ บุกรุก

Honey Pot คือ ระบบหลุมพรางที่ถูกออกแบบมาให้เป็นเหยื่อล่อผู้โจมตี ให้หันมาโจมตีเครื่อง Honey Pot แทนที่จะโจมตีระบบสำคัญหรือระบบวิกฤติขององค์กร

6. การตอบสนองการโจมตีมีขั้นตอนใดบ้าง

1. แจ้งเตือนเมื่อพบการบุกรุก/โจมตี
2. ป้องกันหลักฐานและบันทึกการบุกรุก
3. กำหนดผู้มีอำนาจตัดสินใจ
4. หยุดยั้งการโจมตี
5. การติดตามการโจมตี

คำถาม 7.2. 6016**0305** ข้อใดคือหน้าที่ของ Firewall

1. เป็นตัวกลางการกลั่นกรองข้อมูลเข้า-ออกระหว่างเครือข่ายภายใน ขององค์กร กับเครือข่ายอินเทอร์เน็ต
2. เป็นตัวดักจับการบุกรุกของข่ายภายในองค์กร
3. เป็นตัวบันทึกการใช้เครือข่ายภายในองค์
4. เป็นตัวควบคุมการทำงานของเซิฟเวอร์

เฉลย 1. เป็นตัวกลางการกลั่นกรองข้อมูลเข้า-ออกระหว่างเครือข่ายภายใน ขององค์กร กับเครือข่ายอินเทอร์เน็ต