Information and Computer Security

Course Outline

ผศ.ดร. ธนัญชัย ตรีภาค

ระดับพฤติกรรมด้านความรู้ ความคิด

- รู้ : คืออะไร มีอะไรบ้าง
- เข้าใจ : ทำอย่างไร ยกตัวอย่าง อธิบายโดยใช้สำนวนของตนเอง
- ประยุกต์ : นำไปใช้กับอะไรได้บ้าง จงออกแบบ
- วิเคราะห์ : ข้อดีข้อเสียคืออะไร แล้วจะเกิดอะไรขึ้นถ้า
- สังเคราะห์ : องค์ประกอบของระบบมีอะไรบ้าง กระทบกับใครบ้าง อย่างไร
- ประเมิน/สร้างสรรค์ : อะไรดีกว่ากัน เลือกทางไหนดี สร้างอะไรใหม่ได้

มุ่งเน้นความรู้ให้นักศึกษามีความรู้ระดับ เข้าใจ ประยุกต์ และ วิเคราะห์

เกณฑ์คะแนน

- Assignment / การบ้าน / quiz / กิจกรรมในห้องเรียน 30 คะแนน
- Midterm 30 คะแนน
- Final 40 คะแนน

Output / Outcome ที่ต้องการ

- นักศึกษาสามารถอธิบายคำศัพท์ พร้อมยกตัวอย่างการทำงาน เครื่องมือ มาตรฐาน หรือวิธีการที่เกี่ยวข้องกับคำศัพท์นั้นๆ ได้
- เมื่อกำหนดรายละเอียดของระบบสารสนเทศให้ นักศึกษาสามารถระบุปัญหาความปลอดภัยที่อาจจะเกิดขึ้นในระบบดังกล่าวได้
- เมื่อกำหนดรายละเอียดปัญหาความปลอดภัยระบบสารสนเทศ นักศึกษาสามารถกำหนดวิธีการ หรือเครื่องมือที่ใช้ในการตรวจสอบ ป้องกัน และแก้ไขปัญหาดังกล่าวได้
- นักศึกษาสามารถประยุกต์ใช้หลักการด้านการรักษาความปลอดภัย เพื่อกำหนดกระบวนการในการจัดการกับปัญหา Security ในระบบเครือข่ายได้อย่างเหมาะสม
- นักศึกษาสามารถระบุเครื่องมือ อุปกรณ์ ซอฟต์แวร์ ที่จำเป็นในการจัดการกับปัญหาด้าน Security ในระบบเครือข่ายได้

#1 :หลักการด้านการรักษาความปลอดภัย และการประยุกต์ใช้

- ทำความเข้าใจหลักการ CIA / AAA / PDR
- การประยุกต์ใช้หลักการต่างๆ ในปัญหา Security ต่างๆ ได้

- **คำถามหลัก**
  - **จากปัญหา ... หมายถึงระบบขาดหลักการข้อใด และควรดำเนินการอย่างไร**

#2 : Computer Networking

- ทบทวนพื้นฐานทางด้านเครือข่าย
- สามารถวาด Network Diagram ที่เหมาะสม
- สามารถระบุปัญหาด้านความปลอดภัยจากข้อมูลใน Network Diagram และข้อเสนอแนะที่เหมาะสมได้

- **คำถามหลัก**
  - **จาก Network Diagram ที่ระบุ นักศึกษาคิดว่าจะมีปัญหาด้านความปลอดภัยอะไรบ้าง และควรมีการปรับปรุงอย่างไร**

#3,#4 : Firewall

- ทราบทฤษฎีพื้นฐานของ Firewall
- สามารถกำหนดตำแหน่งติดตั้ง และระบุข้อดีข้อเสียของตำแหน่งติดตั้งได้
- สามารถกำหนดนโยบายในการคัดกรองและป้องกันปัญหาความปลอดภัยในเครือข่ายได้

- **คำถามหลัก**
  - **เพื่อป้องกันปัญหา ... ควรใช้ Firewall ชนิดใด**
  - **เพื่อป้องกันปัญหา DoS ในที่ใช้โพรโตคอล ICMP ควรกำหนดกฎอย่างไร**

#5 : เครื่องมือช่วยรักษาความปลอดภัยเครือข่าย

- ทราบเครื่องมือ อุปกรณ์ และซอฟต์แวร์ที่ช่วยในการรักษาความปลอดภัยระบบเครือข่าย

- **คำถามหลัก**
  - อยากตรวจสอบ Virus ที่มากับ E-mail ใช้โปรแกรมอะไรช่วยได้บ้าง
  - โปรแกรมอะไรบอก Utilization ของ Network ได้
  - โปรแกรมอะไรที่สามารถบอกได้ว่าขณะนี้เครื่องเซิร์ฟเวอร์กำลังทำงานหนักเกินไปแล้ว
  - โปรแกรม ... ทำงานอย่างไร
  - จากปัญหา ... เครือข่ายที่มีโปรแกรมใด จะช่วยให้พบปัญหาได้เร็วขึ้น

#6 : Incident & Response

- นักศึกษาทราบรายละเอียดของ Incident ต่างๆ
- นักศึกษาสามารถเลือกใช้เครื่องมือและกำหนดกระบวนการที่เหมาะสมเพื่อจัดการกับ Incident ได้

- **คำถามหลัก**
  - **ปัญหาไวรัสในองค์กร ควรมีกระบวนการรับมืออย่างไร**
  - **ปัญหาที่เกิดจากความไม่รู้ของ User ควรมีกระบวนการจัดการอย่างไร**

#7 : การรักษาความปลอดภัยใน Web Technology

- การทำงานของ HTTP Protocol
- เทคโนโลยีที่เกี่ยวข้องใน Web Technology
- ช่องโหว่สำคัญใน OWASP Top 10

- **คำถามหลัก**
  - **การโจมตีแบบ XSS มีการทำงานอย่างไร จะตรวจสอบและแก้ไขอย่างไร**
  - **จะทราบได้อย่างไรว่า web application มีช่องโหว่ที่ทำให้โดนโจมตีแบบ SQL Injection ได้**

#8 : การรักษาความปลอดภัยใน Wireless LAN

- ทราบการทำงานตามมาตรฐาน IEEE 802.11
- ทราบปัญหาความปลอดภัยพื้นฐานของ IEEE 802.11
- สามารถกำหนดวิธีการจัดการกับปัญหาความปลอดภัยใน IEEE 802.11 ได้

- **คำถามหลัก**
  - **องค์กรขนาด 10 users ,50 users และ มากกว่า 300 users ควรกำหนดกระบวนการรักษาความปลอดภัยเครือข่ายไร้สายอย่างไร**

#9 : การบริหารความเสี่ยงระบบสารสนเทศ

- ทราบขั้นตอนการบริหารความเสี่ยง
- สามารถกำหนดกิจกรรมเพื่อลดความเสี่ยงระบบสารสนเทศได้

- **คำถามหลัก**
  - **ขั้นตอนทั้งหมดในการบริหารความเสี่ยงมีอะไรบ้าง**
  - **ถ้าความเสี่ยงของระบบอยู่ที่... ควรมีการกำหนด Action Plan อย่างไรบ้าง**

#10 : กระบวนการและมาตรฐานด้านการรักษาความปลอดภัย

- ทราบรายละเอียดสำคัญในมาตรฐาน ISO 27001

- **คำถามหลัก**
  - **KMITL จะต้องทำอย่างไรบ้างเพื่อให้สอดคล้องกับมาตรฐาน ISO 27001**

#11 : กฎหมายที่เกี่ยวข้องกับการรักษาความปลอดภัยระบบสารสนเทศ

- ทราบรายละเอียดของกฎหมายเกี่ยวกับการรักษาความปลอดภัยระบบสารสนเทศ
- ทราบข้อกำหนดของกฎหมายที่ส่งผลกระทบต่องานด้าน IT ต่างๆ

- **คำถามหลัก**
  - **โรงเรียนมัธยม ที่ให้นักเรียนสามารถเชื่อมต่ออินเตอร์เน็ตได้ จะต้องทำอย่างไรเพื่อให้สอดคล้องกับ พรบ.คอมพิวเตอร์ 2550**

#12 : กระบวนการและเทคนิคในการทำ BCM ในระบบสารสนเทศ

- ทราบว่าภัยพิบัติ และภัยคุกคามที่ทำให้ระบบไม่สามารถทำงานได้อย่างต่อเนื่องมีอะไรบ้าง
- ควรดำเนินการทางเทคนิคอย่างไรบ้างเพื่อให้ระบบสามารถทำงานอย่างต่อเนื่องแม้จะเผชิญภัยพิบัติ

- **คำถามหลัก**
  - **มีวิธีการ replicate ข้อมูลไปยัง DR Site ได้อย่างไรบ้าง**

#13 : สรุป / บทเรียน

- ให้ตั้งคำถามของเนื้อหาวิชาตามระดับพฤติกรรมด้านความรู้ความคิด ทั้ง 6 ระดับ

- Facebook (discussion & notes)
  - 2565/2 Information and Computer Security

- Google Classroom (Assignment / ส่งงาน)
  - http://classroom.google.com
  - Classname : 2565/2 Information and Computer Security
  - Class Code : yrg4hmy

Web รายวิชา

- https://sites.google.com/kmitl.ac.th/ics/home
  - Slide
  - Clip
  - Share Doc
  - Answer Sheet

Assignment