ความรู้เบื้องต้นเกี่ยวกับ
การรักษาความปลอดภัยของระบบสารสนเทศ

วิวัฒนาการของการรักษาความปลอดภัยระบบสารสนเทศ

จำแนกตามวิวัฒนาการการพัฒนาด้านเทคโนโลยีและกาลเวลาเปลี่ยนแปลง

1. ยุคแรก (ก่อนปี ค.ศ. 1960)
2. ยุคที่สอง (ปลายปี ค.ศ. 1960 - 1970)
3. ยุคที่สาม (ปลายปี ค.ศ. 1980 - 1990)
4. ยุคที่สี่ (ปลายปี ค.ศ. 1990 ถึงปัจจุบัน)

จำแนกตามวิวัฒนาการการพัฒนาด้านเทคโนโลยี และกาลเวลาเปลี่ยนแปลง

1. ยุคแรก (ก่อนปี ค.ศ. 1960)

- คอมพิวเตอร์มีขนาดใหญ่โตและราคาแพง มีการผู้ใช้งานไม่มาก
- บุคคลหรือหน่วยงานใดมีใช้งานถือได้ว่าโชคดีเป็นอย่างมาก
- การใช้คอมคอมพิวเตอร์เป็นเรื่องที่ยุ่งยากและซับซ้อน
- ต้องใช้ผู้ที่มีความรู้โดยตรง คนทั่วไปพบเห็นได้น้อย
- การรักษาความปลอดภัยทางด้านกายภาพ (Physical Security)
- เก็บคอมพิวเตอร์ไว้ภายในอาคารหรือห้องที่มีการจัดการดูแลอย่างดี มีการตรวจตราผู้ผ่านเข้าออก ใส่กุญแจ และป้องกันไม่ให้มีการขโมยแผ่นดิสก์ ม้วนเทป และอุปกรณ์ต่างๆ

จำแนกตามวิวัฒนาการการพัฒนาด้านเทคโนโลยี และกาลเวลาเปลี่ยนแปลง

2. ยุคที่สอง (ปลายปี ค.ศ. 1960 - 1970)

- มีการพัฒนาและเปลี่ยนแปลงอย่างรวดเร็วด้านเทคโนโลยี
- คอมพิวเตอร์มีราคาถูก และขนาดเล็กลง
- บุคคลทั่วไปสามารถใช้งานได้ มีใช้งานตามห้างร้านต่างๆ
- ถูกนำไปใช้ในการกับข้อมูลหรือสารสนเทศมากขึ้น
- ทำให้เปลี่ยนแปลงรูปแบบการติดต่อสื่อสาร โดยมีการเก็บข้อมูลไว้ใน Server ส่วนกลางเพื่อให้ใช้งานข้อมูลได้ออนไลน์
- เรียกว่า ยุคของการเชื่อมต่อและแบ่งปันทรัพยากร

จำแนกตามวิวัฒนาการการพัฒนาด้านเทคโนโลยี และกาลเวลาเปลี่ยนแปลง

2. ยุคที่สอง (ปลายปี ค.ศ. 1960 - 1970) (ต่อ)

- แตกต่างจากยุคแรก เนื่องมาจากการติดต่อสื่อสาร การเก็บรวบรวมข้อมูลนั้นกระทำผ่านระบบเครือข่าย
- จากที่เคยเฝ้ารักษาความปลอดภัยไม่ให้บุคคลภายนอกเข้ามายุ่งกับคอมพิวเตอร์โดยตรง ก็ต้องปรับเปลี่ยนมาเป็นระแวดระวังภายทางสายโทรศัพท์กันแทน
- การป้องกันทำได้ยากขึ้น เนื่องจากผู้บุกรุกไม่ทิ้งร่องรอย ต่างๆ เช่น นิ้วมือ และไม่มีผู้พบเห็นได้
- ใช้วิธีการเข้ารหัสข้อมูลแทนเพื่อให้ไม่สามารถอ่านเข้าใจได้

จำแนกตามวิวัฒนาการการพัฒนาด้านเทคโนโลยี และกาลเวลาเปลี่ยนแปลง

3. ยุคที่สาม (ปลายปี ค.ศ. 1980 - 1990)

- มีการเปิดตัวคอมพิวเตอร์ส่วนบุคคล (Personal Computer : PC)
- ราคาถูกลงมาก และใช้งานง่ายขึ้น เด็กก็ยังสามารถใช้ได้
- พบเห็นคอมพิวเตอร์ได้ทุกที่ เช่น ที่ทำงาน บ้าน โรงเรียน
- ทุกคนก็สามารถใช้คอมพิวเตอร์ได้กระทั้งเด็กๆ
- มีการเริ่มใช้จดหมายอิเล็กทรอนิกส์ในการติดต่อสื่อสารกัน
- เกิดความเสียหายได้ง่ายขึ้น จาก Cracker จากการใช้ระบบเครือข่าย และสร้างความเสียหายได้ร้ายแรงกว่า

จำแนกตามวิวัฒนาการการพัฒนาด้านเทคโนโลยี และกาลเวลาเปลี่ยนแปลง

4. ยุคที่สี่ (ปลายปี ค.ศ. 1990 ถึงปัจจุบัน)

- มีความคล้ายคลึงกับยุคที่สามแตกต่างกันตรงที่ความทันสมัยและเทคโนโลยีที่ก้าวหน้าขึ้นมากทั้งระบบคอมพิวเตอร์และระบบเครือข่าย
- เป็นยุคที่มีการมีนโยบายเด่นชัดในเรื่องของการตั้งระบบรักษาความปลอดภัยอย่างมีแบบแผน มีผลิตภัณฑ์เกี่ยวกับการรักษาความปลอดภัยบนระบบเครือข่าย เช่น ซอฟต์แวร์แอนตี้ไวรัส สปายแวร์ ไฟร์วอลล์ ฯลฯ และอุปกรณ์ไบโอแมทริค เช่น การสแกนลายนิ้วมือ เป็นต้น และมีการพัฒนาให้สูงขึ้นตลอดเวลา

วิวัฒนาการของการรักษาความปลอดภัยระบบสารสนเทศ

จำแนกตามลักษณะวิธีการรักษาความปลอดภัย

1. การรักษาความปลอดภัยด้านกายภาพ (Physical Security))
2. การรักษาความปลอดภัยด้านสื่อสาร (Communication Security)
3. การรักษาความปลอดภัยการแผ่รังสี (Emissions Security)
4. การรักษาความปลอดภัยคอมพิวเตอร์ (Computer Security)
5. การรักษาความปลอดภัยเครือข่าย (Network Security)
6. การรักษาความปลอดภัยข้อมูลหรือสารสนเทศ (Information Security)

จำแนกตามลักษณะวิธีการรักษาความปลอดภัย

1. การรักษาความปลอดภัยด้านกายภาพ (Physical Security))

- เป็นการรักษาความปลอดภัยที่ใช้กันในยุคแรกๆ ใช้งานกันมานาน
- เน้นที่ทรัพย์สินที่เป็นวัตถุจับต้องได้
- ข้อมูลหรือสารสนเทศที่สำคัญก็อยู่ในรูปของวัตถุ เช่น ข้อมูลจะถูกบันทึกไว้บนแผ่นหิน แผ่นหนัง หรือกระดาษ ซึ่งอดีตนั้น
- ความรู้คืออำนาจ (Knowledge is power) ไม่นิยมถ่ายทอดให้กับคนอื่น แต่จะถ่ายทอดเฉพาะคนที่ไว้ใจเท่านั้น
- การป้องกันและรักษาความปลอดภัยจะมีลักษณะทางกายภาพ เช่น กำแพง ประสาท หรือยาม ซึ่งในการส่งข้อมูลสารสนเทศไปที่อื่นๆ จะมีผู้คุ้มกันติดตาม

จำแนกตามลักษณะวิธีการรักษาความปลอดภัย

2. การรักษาความปลอดภัยด้านสื่อสาร (Communication Security)

- การรักษาความปลอดภัยทางกายภาพอย่างเดียวยังไม่สามารถที่รักษาความปลอดภัยของข้อมูลหรือสารสนเทศได้อย่างดีที่สุด
- ข้อบกพร่องหรือจุดอ่อนอีก คือถ้าถ้ามีการโจรกรรมข้อมูลหรือสารสนเทศขึ้นทั้งที่อยู่ในสถานที่เก็บหรือระหว่างการรับส่ง ทำให้ผู้ไม่หวังดีสามารถรับรู้และเข้าใจข้อมูลหรือสารสนเทศได้
- วิธีการแก้ไขปัญหาคือใช้วิธีการเข้ารหัสข้อมูลหรือสารสนเทศ เพื่อไม่ให้สามารถอ่านและเข้าใจความหมายได้

จำแนกตามลักษณะวิธีการรักษาความปลอดภัย

2. การรักษาความปลอดภัยด้านสื่อสาร (Communication Security)

- ยุคของจูเลียส์ ซีซาส์ มีการใช้ขบวนการ “ซ่อน” ข้อมูล หรือการเข้ารหัสข้อมูล (Encryption) เพื่อเป็นการปกป้องข้อมูลระหว่างการรับส่ง ถ้าหากมีการโจรกรรมข้อมูลดังกล่าวไปก็จะไม่สามารถแปลความหมายนั้นได้ เนื่องจากไม่รู้วิธีการถอดรหัส (Decryption)
- ช่วงสงครามโลกครั้งที่ 2 ด้วย ทางกองทับเยอรมันใช้เครื่องมือที่เรียกว่า เอ็นนิกมา (Enigma) สำหรับการเข้ารหัสข้อมูลที่รับส่งระหว่างทหารด้วยกันเอง
- วิธีการนี้ก็ยังมีข้อผิดพลาดหากทราบถึงวิธีการถอดรหัสดังกล่าวก็จะสามารถแปลผลข้อมูลนั้นได้

จำแนกตามลักษณะวิธีการรักษาความปลอดภัย

2. การรักษาความปลอดภัยด้านสื่อสาร (Communication Security)

เครื่องเข้ารหัส เอ็นนิกมา (Enigma)

จำแนกตามลักษณะวิธีการรักษาความปลอดภัย

3. การรักษาความปลอดภัยการแผ่รังสี (Emissions Security)

- การเข้ารหัสที่ดีทำให้ยากต่อการถอดรหัสข้อมูล
- มีการคิดพยายามใหม่ เพื่อสามารถที่จะอ่านข้อมูลหรือสารสนเทศ
- ช่วงทศวรรษ 1950 ค้นพบว่าข้อมูลที่มีการรับส่งกันอยู่ผ่านทางโทรศัพท์ อุปกรณ์อิเล็กทรอนิกส์ทุกประเภทจะมีการแผ่รังสีออกมาเป็นสัญญาณไฟฟ้า รวมถึงเครื่องพิมพ์โทรสารและเครื่องสำหรับเข้าและถอดรหัสข้อมูลด้วย

จำแนกตามลักษณะวิธีการรักษาความปลอดภัย

3. การรักษาความปลอดภัยการแผ่รังสี (Emissions Security)

- เครื่องเข้ารหัสข้อมูลเมื่อเข้ารหัสแล้วจะส่งผ่านไปบนสายโทรศัพท์
- ค้นพบว่ามีสัญญาณไฟฟ้า 2 ชนิด คือ
  - สัญญาณไฟฟ้าของข้อมูลที่ถูกเข้ารหัสแล้ว
  - สัญญาณไฟฟ้าของข้อมูลเดิมที่ยังไม่ได้ถูกเข้ารหัส
- หากใช้เครื่องมือที่ดีเราสามารถกู้คืนข้อมูลเดิมที่ยังไม่ได้ถูกเข้ารหัสออกมาได้

จำแนกตามลักษณะวิธีการรักษาความปลอดภัย

4. การรักษาความปลอดภัยคอมพิวเตอร์ (Computer Security)

- การเข้ารหัสข้อมูลและการควบคุมการแผ่รังสีเป็นมาตรฐานความปลอดภัยที่เพียงพอ ถ้ามีการรับส่งข้อมูลเพียงการใช้โทรสารเท่านั้น
- มีการนำคอมพิวเตอร์เข้ามาใช้งานแทนเครื่องส่งโทรสาร ทำให้ข้อมูลส่วนใหญ่อยู่ในรูปแบบของดิจิตอล
- คอมพิวเตอร์ได้พัฒนาให้มีการใช้งานง่ายและสะดวกมากขึ้น ซึ่งผลให้มีผู้ใช้คอมพิวเตอร์สามารถเข้าถึงข้อมูลหรือสารสนเทศภายในเครื่องคอมพิวเตอร์นั้นได้ด้วยเช่นกัน ทำให้ไม่มีความปลอดภัยในการจัดเก็บข้อมูลในเครื่องคอมพิวเตอร์

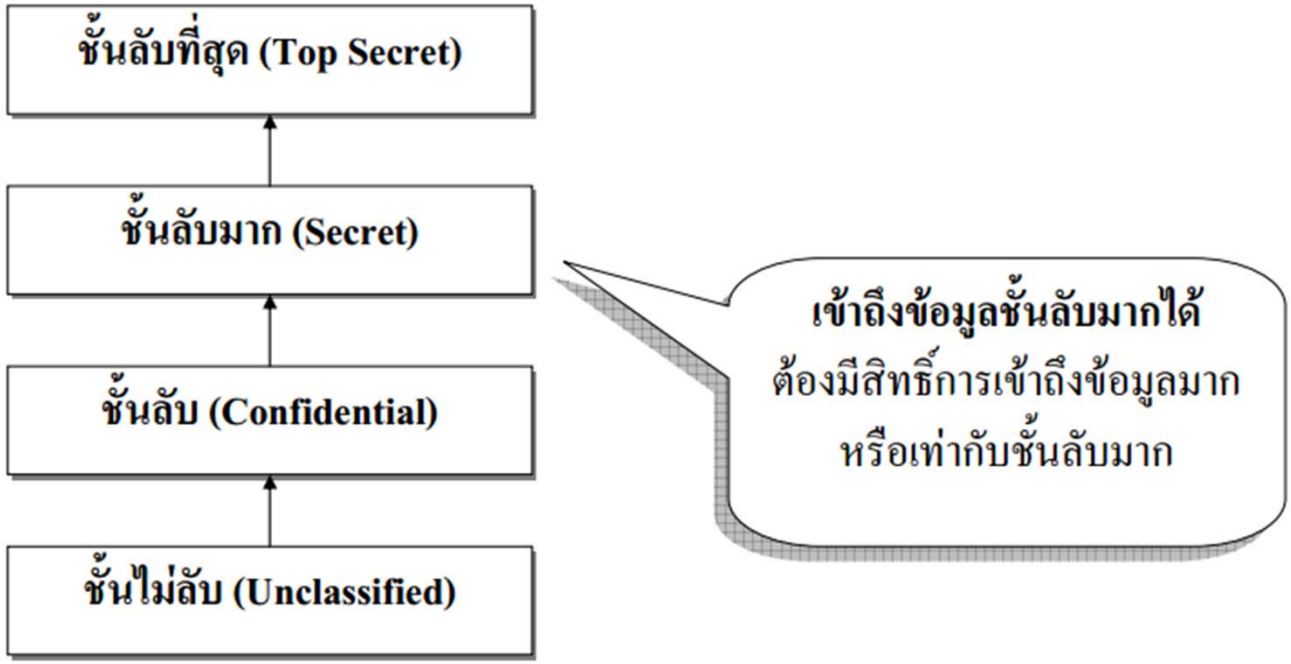
จำแนกตามลักษณะวิธีการรักษาความปลอดภัย

4. การรักษาความปลอดภัยคอมพิวเตอร์ (Computer Security)

- ช่วงปีทศวรรษ 1970 เดวิด เบลล์ และลีโอนาร์ด ลา พาดูลา มีการพัฒนาแม่แบบสำหรับการรักษาความปลอดภัยของคอมพิวเตอร์ขึ้น
- โดยอาศัยแนวคิดในการจัดระดับความปลอดภัยข้อมูลของรัฐบาลสหรัฐอเมริกา แบ่งได้ 4 ชั้น คือ ไม่ลับ ลับ ลับมาก และลับที่สุด (Unclassified , Confidential , Secret ,Top Secret) และแบ่งระดับระดับสิทธิ์ของผู้เข้าถึงข้อมูลลับนี้ (Clearance) มี 4 ระดับ เช่นกัน
- ผู้ที่สามารถเข้าถึงข้อมูลในระดับใดระดับหนึ่งได้จะต้องมีสิทธิ์ (Clearance) เท่ากันหรือสูงกว่าชั้นความลับของข้อมูลนั้น ดังนั้นผู้มีสิทธิ์น้อยกว่าชั้นความลับของไฟล์ก็ไม่สามารถเข้าถึงไฟล์นั้นได้

จำแนกตามลักษณะวิธีการรักษาความปลอดภัย

4. การรักษาความปลอดภัยคอมพิวเตอร์ (Computer Security)



การแบ่งชั้นความลับของ เดวิด เบลล์ และลีโอนาร์ด ลา พาดูลา

จำแนกตามลักษณะวิธีการรักษาความปลอดภัย

4. การรักษาความปลอดภัยคอมพิวเตอร์ (Computer Security)

- แนวคิดนี้ทางกระทรวงกลาโหมของสหรัฐอเมริกา ได้นำไปใช้โดยใช้ชื่อว่า มาตรฐาน 5200.28 หรือ TCSEC (Trusted Computing System Evaluation Criteria) หรือที่รู้จักโดยทั่วไปว่า**ออเรนจ์บุ๊ค (Orange Book)**
- มาตรฐานนี้กำหนดระดับความปลอดภัยออกเป็นระดับต่างๆ และแต่ละระดับของออเรนจ์บุ๊คนั้นมีการกำหนดฟังก์ชั่นต่าง ที่ระบบต้องมีและการประกัน ทำให้การจะได้ใบรับรองของในแต่ละระดับนั้นต้องใช้เวลาและเสียค่าใช้จ่ายสูงสำหรับผู้ผลิต

จำแนกตามลักษณะวิธีการรักษาความปลอดภัย

4. การรักษาความปลอดภัยคอมพิวเตอร์ (Computer Security)

- มีการกำหนดมาตรฐานใหม่ขึ้นมาแทนออเรนจ์บุ๊ค เพื่อแก้ไขข้อบกพร่องในเรื่องของเวลาที่ใช้ในการตรวจทดสอบเพื่อออกไปรับรอง เช่น German Green Book(1989) , Canadian Criteria (1990) , ITSEC:Information Technology Security Evaluation Criteria (1991) และ Federal Criteria (1992)
- แต่ละมาตรฐานที่กล่าวมานี้เพื่อออกใบรับรองว่าระบบคอมพิวเตอร์นั้นปลอดภัยแค่ไหน

จำแนกตามลักษณะวิธีการรักษาความปลอดภัย

4. การรักษาความปลอดภัยคอมพิวเตอร์ (Computer Security)

- แนวคิดนี้ทางกระทรวงกลาโหมของสหรัฐอเมริกา ได้นำไปใช้โดยใช้ชื่อว่า มาตรฐาน 5200.28 หรือ TCSEC (Trusted Computing System Evaluation Criteria) หรือที่รู้จักโดยทั่วไปว่าออเรนจ์บุ๊ค (Orange Book)
- มาตรฐานนี้กำหนดระดับความปลอดภัยออกเป็นระดับต่างๆ และแต่ละระดับของออเรนจ์บุ๊คนั้นมีการกำหนดฟังก์ชั่นต่าง ที่ระบบต้องมีและการประกัน ทำให้การจะได้ใบรับรองของในแต่ละระดับนั้นต้องใช้เวลาและเสียค่าใช้จ่ายสูงสำหรับผู้ผลิต

จำแนกตามลักษณะวิธีการรักษาความปลอดภัย

5. การรักษาความปลอดภัยเครือข่าย(Network Security)

- ปัญหาหนึ่งที่พบเกี่ยวกับการตรวจสอบและออกใบรับรองมาตรฐานระดับความปลอดภัยให้แก่คอมพิวเตอร์คือ ระบบมีการเชื่อมต่อกันเป็นเครือข่าย ซึ่งออเรนจ์บุ๊คไม่ได้กำหนดมาตรฐานในเรื่องเกี่ยวกับเครือข่ายคอมพิวเตอร์ไว้ ดังนั้นเมื่อเชื่อมต่อคอมพิวเตอร์เข้าสู่เครือข่ายก็จะทำให้ใบรับรองนั้นเป็นโมฆะ

จำแนกตามลักษณะวิธีการรักษาความปลอดภัย

5. การรักษาความปลอดภัยเครือข่าย(Network Security)

- แก้ไขปัญหามีการใช้มาตรฐาน TNI (Trusted Network Interpretation) ของ TCSECหรือที่รู้จักกันในเชื่อ เรดบุ๊ค (Red Book) ซึ่งออกมาในปี 1987 โดยข้อกำหนดของเรดบุ๊คเหมือนกับออเรนจ์บุ๊คทั้งหมดแตกต่างกันที่เรดบุ๊คมีการเพิ่มส่วนที่เกี่ยวข้องกับระบบเครือข่ายเข้าไป

จำแนกตามลักษณะวิธีการรักษาความปลอดภัย

6. การรักษาความปลอดภัยข้อมูลหรือสารสนเทศ (Information Security)

- ใช้วิธีการหลากหลายวิธีรวมกัน คือ
- หากเป็นปกป้องทรัพย์สินที่เป็นวัตถุวัตถุ นิยมใช้วิธีการรักษาความปลอดภัยทางด้ายกายภาพ (PHYSISEC)
- หากเป็นการปกป้องข้อมูลหรือสารสนเทศที่อยู่ระหว่างการรับส่งจะใช้วิธีการรักษาความปลอดภัยด้านการสื่อสาร (COMSEC) และถ้าฝ่ายตรงข้ามหรือผู้ไม่ประสงค์ดีมีเครื่องมือสำหรับผ่านข้อมูลจากคลื่นรังสีที่แผ่นออกมาได้ เราจะใช้วิธีการรักษาความปลอดภัยเกี่ยวกับการแผ่รังสี (EMSEC)

จำแนกตามลักษณะวิธีการรักษาความปลอดภัย

6. การรักษาความปลอดภัยข้อมูลหรือสารสนเทศ (Information Security)

- ใช้วิธีการหลากหลายวิธีรวมกัน คือ
- สำหรับการเข้าควบคุมและเข้าถึงระบบคอมพิวเตอร์ใช้วิธีการรักษาความปลอดภัยคอมพิวเตอร์ (COMPSEC) และหากคอมพิวเตอร์มีการเชื่อมต่อระบบเครือข่ายด้วยก็จำเป็นต้องใช้วิธีการรักษาความปลอดภัยระบบเครือข่าย (NETSEC)
- เมื่อเรารวมวิธีการรักษาความปลอดภัยต่างๆ ที่กล่าวมาข้างต้นทั้งหมดเข้าด้วยกันก็จะเป็นการรักษาความปลอดภัยข้อมูลหรือสารสนเทศ (INFOSEC) ได้

- การรักษาความปลอดภัยสารสนเทศนั้นเป็นทั้งศาสตร์และศิลป์
- การมีระบบรักษาความปลอดภัยที่ดีที่สุดไม่ได้หมายความว่าข้อมูลหรือสารสนเทศ ระบบคอมพิวเตอร์ และองค์กรจะปลอดภัย
- การรักษาความปลอดภัยเป็นเพียงกระบวนการ ไม่ใช่แค่การติดตั้งระบบรักษาความปลอดภัยที่ดีที่สุด แต่รวมถึงการวิเคราะห์ และบริหารความเสี่ยง (Risk) ที่เกิดจากภัยคุกคาม (Threat) และช่องโหว่หรือจุดอ่อน (Vulnerability) ขององค์กร การกำหนดและบังคับใช้นโยบายการรักษาความปลอดภัย และเฝ้าระวังเหตุการณ์อยู่ตลอด
- ยังไม่มีการรักษาความปลอดภัยวิธีการใดที่ สามารถรักษาความปลอดภัยได้ร้อยเปอร์เซ็นต์
- มีปัจจัยหลายๆอย่างมีผลต่อการรักษาความปลอดภัย เช่นบุคคลผู้ใช้งาน กระบวนการ และเทคโนโลยีที่เปลี่ยนแปลงไปอย่างรวดเร็ว

การรักษาความความปลอดภัย + สารสนเทศ

?

ความหมายของการรักษาความปลอดภัยสารสนเทศ

การรักษาความปลอดภัย (Security)

หมายถึง มาตรการที่กำหนดขึ้น ตลอดจนการดำเนินการทั้งปวงเพื่อพิทักษ์รักษา และคุ้มครองป้องกันเพื่อให้รอดพ้นจากอันตราย หรือทำให้รอดพ้นจาก ความกลัว ความทุกข์ ความกังวล

สารสนเทศ (Information)

หมายถึง ความรู้ ความคิด ข้อมูล ข่าวสาร และข้อเท็จจริง ที่เป็นประโยชน์ต่อผู้ใช้งานหรืออาจกล่าวได้ว่าสารสนเทศ เกิดจากการนำข้อมูล ผ่านระบบการประมวลผล คำนวณ วิเคราะห์และแปลความหมาย

การรักษาความปลอดภัยสารสนเทศ (Information Security)

หมายถึง การทำให้ความรู้ ความคิด ข่าวสาร และข้อเท็จจริง รอดพ้นจากอันตราย

แปลความความหมายให้เข้ากับไอที หมายถึง มาตรการที่กำหนดขึ้นตลอดจนการดำเนินการทั้งปวง เพื่อพิทักษ์รักษา และคุ้มครองป้องกัน ให้ข้อมูลหรือสารสนเทศรอดพ้นจากผู้ที่ไม่ได้รับอนุญาตในการเข้าถึง ลบ แก้ไข หรือขัดขวางไม่ให้ผู้ที่ได้รับอนุญาตใช้งานความรู้ แนวคิด และข้อเท็จจริง

รู้ไหมว่า / รู้ได้อย่างไร
ข้อมูลหรือสารสนเทศของเรานั้นยังมีความถูกต้อง
และมีความปลอดภัยอยู่

?

องค์ประกอบการรักษาความปลอดภัยระบบสารสนเทศ

พิจารณาถึงองค์ประกอบหลักๆ ของข้อมูลหรือสารสนเทศดังกล่าวว่าจะต้องประกอบไปด้วยคุณสมบัติต่างๆ ดังนี้

1. ด้านความลับ (Confidentiality)
2. ด้านความคงสภาพ (Integrity)
3. ด้านความพร้อมใช้งาน (Availability)

คุณสมบัติอื่นๆ เกี่ยวกับการรักษาความปลอดภัยของข้อมูล

1. การระบุตัวบุคคล และ อำนาจหน้าที่ (Authentication & Authorization)
2. การป้องกันการปฏิเสธ หรือ อ้างความรับผิดชอบ (Non-repudiation)

คุณสมบัติของข้อมูลหรือสารสนเทศ

1. ด้านความลับ (Confidentiality)

- ต้องมั่นใจได้ว่าสารสนเทศนั้นไม่ถูกบุคคลที่ไม่ได้รับอนุญาต (Unauthorized User) เข้าถึงแหล่งข้อมูลหรือสารสนเทศได้ และถ้าหากเข้าได้ถึงได้ก็ไม่สามารถนำไปใช้งานได้ เนื่องจากมีวิธีการปกป้องความปลอดภัยของข้อมูลหรือสารสนเทศ
- กลไกที่นิยมใช้ในปัจจุบันเรียกว่า การเข้ารหัสข้อมูล (Cryptography หรือ Encryption)
- เปรียบเทียบได้กับการส่งจดหมายที่มีการลงทะเบียนและการปิดผนึกซองจดหมาย การใช้ซองจดหมายที่ทึบแสง การเขียนหมึกที่มองไม่เห็น เป็นต้น

ต้องมั่นใจได้ว่าข้อมูลนั้นเป็นความลับจริง ๆ

คุณสมบัติของข้อมูลหรือสารสนเทศ

2. ด้านความคงสภาพ (Integrity)

- หรือ ความสมบูรณ์ของข้อมูล คือ ต้องมั่นใจว่าข้อมูลหรือสารสนเทศไม่ได้ถูกแก้ไข เปลี่ยนแปลง ด้วยวิธีการใดๆ ทั้งเจตนาและไม่เจตนา โดยที่ไม่ได้รับอนุญาต เรียกอีกอย่างว่าการทำให้ข้อมูลมีความน่าเชื่อถือ (เชื่อถือทั้งตัวข้อมูลหรือสารสนเทศ และแหล่งที่มา)
- กลไกที่นิยมใช้ในการรักษาความปลอดภัยที่นิยมกันคือ การป้องกัน (Prevention) และการตรวจสอบ (Detection) โดยกลไกการป้องกันมีอยู่ 2 ลักษณะคือ

ต้องมั่นใจว่าสารสนเทศต้องไม่มีการเปลี่ยนแปลงแก้ไข

คุณสมบัติของข้อมูลหรือสารสนเทศ

2. ด้านความคงสภาพ (Integrity)

- กลไกการป้องกันมีอยู่ 2 ลักษณะคือ
  - การป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้าไปเปลี่ยนแปลงแก้ไขข้อมูล (ป้องกันบุคคลภายนอกที่ไม่มีสิทธิ์)
  - การป้องกันไม่ให้ผู้ที่ได้รับอนุญาตเข้าไปเปลี่ยนแปลงแก้ไขข้อมูลในรูปแบบที่ไม่ถูกต้องหรือได้รับอนุญาต (ป้องกันบุคคลภายในที่มีสิทธ์)
- กลไกการตรวจสอบนั้น เป็นการวิเคราะห์ว่าข้อมูลหรือสารสนเทศยังคงสภาพเดิมอยู่หรือไม่

ต้องมั่นใจว่าสารสนเทศต้องไม่มีการเปลี่ยนแปลแก้ไข

คุณสมบัติของข้อมูลหรือสารสนเทศ

2. ด้านความคงสภาพ (Integrity)

- เปรียบเทียบได้กับ การเขียนด้วยหมึกซึ่งถ้าถูกลบแล้วจะก่อให้เกิดรอยลบขึ้น การใช้โฮโลแกรมกำกับบนบัตรเครดิต

ต้องมั่นใจว่าสารสนเทศต้องไม่มีการเปลี่ยนแปลงแก้ไข

คุณสมบัติของข้อมูลหรือสารสนเทศ

3. ด้านความพร้อมใช้งาน (Availability)

- ต้องมั่นใจว่าข้อมูลหรือสารสนเทศจะสามารถใช้งานได้ตามปกติและเต็มประสิทธิภาพ เมื่อผู้ที่ได้รับอนุญาตต้องการใช้งาน
- กลไกการป้องกันที่นิยมใช้งานคือการออกแบบระบบให้มีความมั่นคงของระบบ (Reliability)
- เปรียบเทียบได้กับร้านสะดวกซื้อ เซเวนอีเลฟเวน ซึ่งเปิดให้บริการตลอด 24 ชั่วโมงต่อวัน 7 วันต่อสัปดาห์

คำว่าความพร้อมใช้งาน (Availability) ตรงกันข้ามกับคำว่าการปฏิเสธการให้บริการ (Denial of service :DoS) คือ ภาวะที่ผู้ที่ได้รับอนุญาตให้เข้าใช้งานไม่สามารถเข้าใช้งานได้

ต้องมั่นใจได้ว่าจะสามารถใช้สารสนเทศได้ตลอดเวลาที่ต้องการ

คุณสมบัติของข้อมูลหรือสารสนเทศ

อนึ่งจะเห็นได้ว่าคุณสมบัติต่างๆของข้อมูลหรือสารสนเทศที่กล่าวมาทั้ง 3 ด้านนี้ คือ ด้านความลับ (Confidentiality) ด้านความคงสภาพ (Integrity) และด้านความพร้อมใช้งาน (Availability) จะขาดคุณสมบัติข้อใดข้อหนึ่งไปไม่ได้มิฉะนั้นจะทำให้ข้อมูลหรือสารสนเทศของเราถือว่าไม่มีความปลอดภัย

กรณีศึกษา

กรรมการบริหารบริษัท ส่งจดหมายอิเล็กทรอนิกส์ไปให้นายสมศักดิ์ ซึ่งเป็นหัวหน้าฝ่ายการเงินที่มีสิทธิ์รับจดหมายอิเล็กทรอนิกส์ได้คนเดียว โดยมีใจว่าให้ปรับขึ้นเงินเดือนของนางสาวสุดสวย จากเดิม 15,000 บาท เป็น 16,000 บาท

แต่นางสาวสุดสวยมีความสามารถด้านคอมพิวเตอร์สามารถดักรับจดหมายอิเล็กทรอนิกส์ดังกล่าวและเปิดอ่านพบเนื้อความดังกล่าว ซึ่งนางสาวสุดสวยไม่พอใจอย่างยิ่งเนื่องจากรู้สึกว่าผู้บริหารขึ้นเงินเดือนน้อยไป จึงได้ปรับแก่ไขตัวเลขจำนวนเงินเดือนใหม่ จากเดิม 16,000 บาท เป็นจำนวนเงิน 16,500 บาท แทน และส่งจดหมายอิเล็กทรอนิกส์ดังกล่าวให้หัวหน้าฝ่ายการเงิน (หัวหน้าฝ่ายการเงินไม่รู้เลยว่าเงินเดือนมีการถูกเปลี่ยนแปลงไปจากเดิม)

การวิเคราะห์

วิเคราะห์ ?

- ขาดคุณสมบัติด้านความลับ (Confidentiality)

เนื่องจากถึงแม้จะมีการรักษาความปลอดภัยโดยให้จดหมายอิเล็กทรอนิกส์นั้นรับได้เฉพาะหัวหน้าฝ่ายการเงิน แต่นางสาวสุดสวยกับสามารถใช้ความสามารถด้านคอมพิวเตอร์ ดักรับจดหมายนั้นได้

- ขาดคุณสมบัติในด้านความคงสภาพ (Integrity)

คือความถูกต้องของข้อมูลก็ผิดไปจากเดิมดังเห็นได้จากจำนวนเงินเดือนที่เปลี่ยนแปลงไป

- จะเห็นได้ว่ามีเพียงคุณสมบัติเดียวที่ยังรักษาไว้ได้ คือ ด้านความพร้อมใช้งาน (Availability)

วิธีการแก้ไข

วิเคราะห์ วิธีการแก้ไข ?

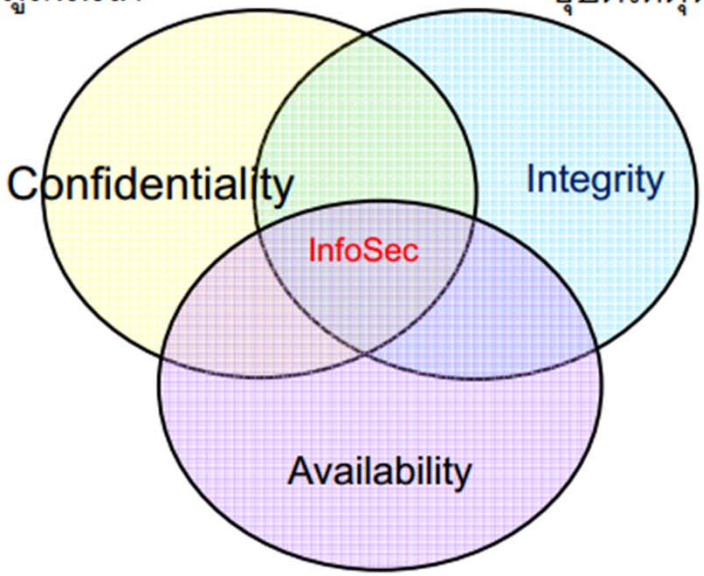
- ด้านความลับคงสภาพ (Confidentiality) ทำได้โดยการหามาตรการทำให้นางสาวสุดสวย ไม่สามารถเข้าถึงจดหมายอิเล็กทรอนิกส์ฉบับนั้นได้
- ด้านความคงสภาพ (Integrity) ทำได้โดยการเข้ารหัสใจความดังกล่าวเพื่อไม่ได้นางสาวสุดสวยอ่านได้ ถึงแม้จะสามารถดักรับข้อมูลได้ก็ตามก็ไม่สามารถอ่านได้เข้าใจ

จากตัวอย่างดังกล่าว จะเห็นได้ว่าการรักษาความปลอดภัยของข้อมูลหรือสารสนเทศเป็นสิ่งจำเป็นอย่างมาก มิฉะนั้นก็จะเกิดความเสียหายเกิดขึ้นตามมา สำหรับการพิจารณาว่าข้อมูลหรือสารสนเทศของเราปลอดภัยหรือไม่นั้น คือต้องพยายามทำให้ข้อมูลหรือสารสนเทศของเรามีคุณสมบัติยังคงรักษาคุณสมบัติด้านความลับ (Confidentiality) ด้านความคงสภาพ (Integrity) และด้านความพร้อมใช้งาน (Availability)

องค์ประกอบการรักษาความปลอดภัยระบบสารสนเทศ

Confidentiality คือการรับรองว่าจะมีการเก็บข้อมูลไว้เป็นความลับ และผู้มีสิทธิเท่านั้นจึงจะเข้าถึงข้อมูลนั้นได้

Integrity คือการรับรองว่าข้อมูลจะไม่ถูกเปลี่ยนแปลงหรือทำลายไม่ว่าจะเป็นโดยอุบัติเหตุหรือโดยเจตนา



Availability คือการรับรองว่าข้อมูลและบริการการสื่อสารต่าง ๆ พร้อมที่จะใช้งานได้เมื่อต้องการ

คุณสมบัติของข้อมูลหรือสารสนเทศ

คุณสมบัติอื่นๆ เกี่ยวกับการรักษาความปลอดภัยของข้อมูล

นอกจากคุณสมบัติทั้ง 3 ด้านที่กล่าวมาแล้วนั้น ยังมีผู้ที่ให้แนวคิดเกี่ยวกับการรักษาความปลอดภัยข้อมูลอื่นๆ อีกสรุปได้ดังนี้

1. การระบุตัวบุคคล และ อำนาจหน้าที่
   (Authentication & Authorization)

2. การป้องกันการปฏิเสธ หรือ อ้างความรับผิดชอบ
   (Non-repudiation)

คุณสมบัติอื่นๆ เกี่ยวกับการรักษาความปลอดภัยของข้อมูล

1. การระบุตัวบุคคล และ อำนาจหน้าที่ (Authentication & Authorization)

- การระบุตัวบุคคลที่ติดต่อว่าเป็นบุคคลตามที่ได้กล่าวอ้างไว้จริง และมี อำนาจหน้าที่ตามที่ได้กล่าวอ้างไว้จริง
- เปรียบเทียบได้กับการแสดงตัวด้วยบัตรประจำตัว ซึ่งมีรูปติดอยู่ด้วย
- การใช้ระบบล็อก ซึ่งผู้ที่จะเปิดได้จะต้องมีกุญแจอยู่เท่านั้น
- ถ้าเป็นด้านไอทีที่นิยมใช้กันมากที่สุดโดยการชื่อยูเซอร์เนม (User Name) เพื่อเป็นการระบุตัวตน (Authentication) และรหัสผ่าน (Password) เพื่อเป็นการระบุอำนาจหน้าที่ (Authorization)

คุณสมบัติอื่นๆ เกี่ยวกับการรักษาความปลอดภัยของข้อมูล

2. การป้องกันการปฏิเสธ หรือ อ้างความรับผิดชอบ (Non-repudiation)

- การป้องกันการปฏิเสธว่าไม่ได้มีการส่ง หรือ รับข้อมูล จากฝ่ายต่างๆ ที่เกี่ยวข้อง หรือ การป้องกันการอ้างที่เป็นเท็จว่าได้ รับหรือ ส่งข้อมูล ซึ่งระบบต้องตรวจสอบได้ เช่นการเก็บล๊อก (Logs) เกี่ยวกับกิจกรรมต่างๆที่ผู้ใช้แต่ละคนใช้งานระบบ
- เปรียบเทียบได้กับการส่งจดหมายลงทะเบียน เป็นต้น

คำถามทบทวน ?

1. อธิบายวิวัฒนาการความเป็นมาของการรักษาความปลอดภัย ?
2. อธิบายความแตกต่างระหว่างการรักษาความปลอดภัยในลักษณะทั่วไปเปรียบเทียบการรักษาความปลอดภัยของข้อมูลหรือสารสนเทศ?
3. ให้นักศึกษาค้นคว้าหาตัวอย่างปัญหาด้านการรักษาความปลอดภัยที่เกิดขึ้นและส่งผลเสียหายที่เกิดขึ้นในปัจจุบัน และอภิปรายสรุปพร้อมวิเคราะห์ตามองค์ประกอบของการรักษาความปลอดภัยของระบบสารสนเทศ (ระบุที่มาด้วยจากสื่อใดมีอ้างอิง) ?