มหาวิทยาลัยราชภัฏนครปฐม
Nakhon Pathom Rajabhat University

แนวคิดเกี่ยวกับความมั่งคงปลอดภัยในระบบคอมพิวเตอร์

เนื้อหา

- องค์ประกอบพื้นฐานของความปลอดภัยของข้อมูล
- การรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์
- สภาพแวดล้อมของความปลอดภัย
- มาตรฐานความปลอดภัย
- การบริหารและประเมินความเสี่ยงของระบบคอมพิวเตอร์และเครือข่าย
- บทสรุป

ความมั่นคงปลอดภัย (Security)

- คือ สถานะที่มีความปลอดภัย ไร้กังวล อยู่ในสถานะที่ไม่มีอันตรายและได้รับการป้องกันจากภัยอันตราย ทั้งที่เกิดขึ้นโดยตั้งใจหรือบังเอิญ เช่น ความมั่นคงปลอดภัยของประเทศ ย่อมเกิดขึ้นโดยมีระบบป้องกันหลายระดับ เพื่อปกป้องผู้นำประเทศ ทรัพย์สิน ทรัพยากร และประชาชนของประเทศ เป็นต้น

https://www.cellusys.com/services/network-security-assessment/

องค์ประกอบพื้นฐานของความปลอดภัยของข้อมูล

1. ความลับของข้อมูล (Confidentiality)
2. ความคงสภาพของข้อมูล (Integrity)
3. ความพร้อมใช้งานของข้อมูล (Availability)
4. การพิสูจน์ทราบตัวตนที่แท้จริง (Authentication)
5. การอนุญาตให้เข้าใช้งานและลำดับสิทธิในการเข้าถึง (Authorization)
6. การไม่สามารถปฏิเสธความรับผิดชอบ (Non-repudiation)

https://securityintelligence.com/data-security-goes-beyond-technology/

1. ความลับของข้อมูล (Confidentiality)

- การรักษาความลับของข้อมูล หมายถึง การปกป้องโดยมีเงื่อนไขว่าข้อมูลนั้นใครมีสิทธิ์ที่จะล่วงรู้ เข้าถึง ใช้งานได้ และการทำให้ข้อมูลสามารถเข้าถึงหรือเปิดเผยได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น
- กลไกในการควบคุมการรักษาความลับของข้อมูลสามารถทำได้โดยการควบคุมการเข้าถึงระบบ (Access Control)
- กรณีที่มีการส่งข้อมูลลับผ่านระบบเครือข่ายที่สามารถดักจับและอ่านข้อมูลได้ จะต้องมีการเข้ารหัสข้อมูล (Cryptography & Encryption)

2. ความคงสภาพของข้อมูล (Integrity)

- การรักษาความคงสภาพของข้อมูล หมายถึง การปกป้องเพื่อให้ข้อมูลไม่ถูกแก้ไข เปลี่ยนแปลง หรือถูกทำลาย ได้ (ธวัชชัย ชมศิริ, 2553, หน้า 13)

- **ตัวอย่างเช่น** นาย A ส่งไฟล์ถึงนาย B ไฟล์นั้นจะต้องไม่ถูกแก้ไขหรือเปลี่ยนแปลงโดยบุคคลอื่นในระหว่างทางที่ส่งมา เป็นต้น

3. ความพร้อมใช้งานของข้อมูล (Availability)

- ความพร้อมใช้งานของข้อมูล หมายถึง ข้อมูลจะต้องมีสภาพพร้อมใช้งานอยู่ตลอดเวลา

4. การพิสูจน์ทราบตัวตนที่แท้จริง (Authentication)

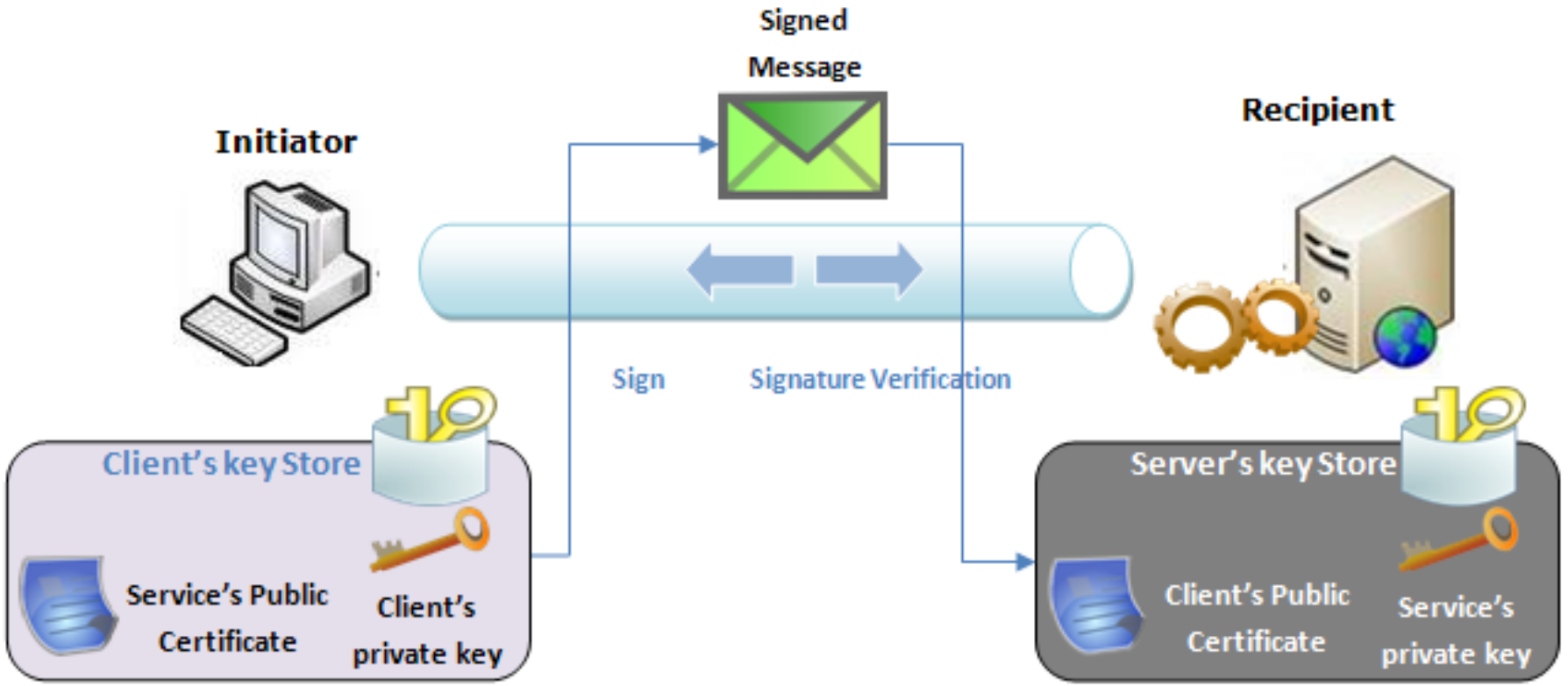
https://www.entersekt.com/images/strong-authentication-800px.png

5. การอนุญาตให้เข้าใช้งานและลำดับสิทธิในการเข้าถึง (Authorization)

- ระบบจะทำการอนุญาตให้ผู้ใช้คนนั้น ๆ เข้าใช้งานตามสิทธิของผู้ใช้งานคนนั้น ซึ่งการให้สิทธิ์สามารถแบ่งได้เป็นหลายระดับ

6. การไม่สามารถปฏิเสธความรับผิดชอบ (Non-repudiation)

- ระบบจะทำการอนุญาตให้ผู้ใช้คนนั้น ๆ เข้าใช้งานตามสิทธิของผู้ใช้งานคนนั้น ซึ่งการให้สิทธิ์สามารถแบ่งได้เป็นหลายระดับ

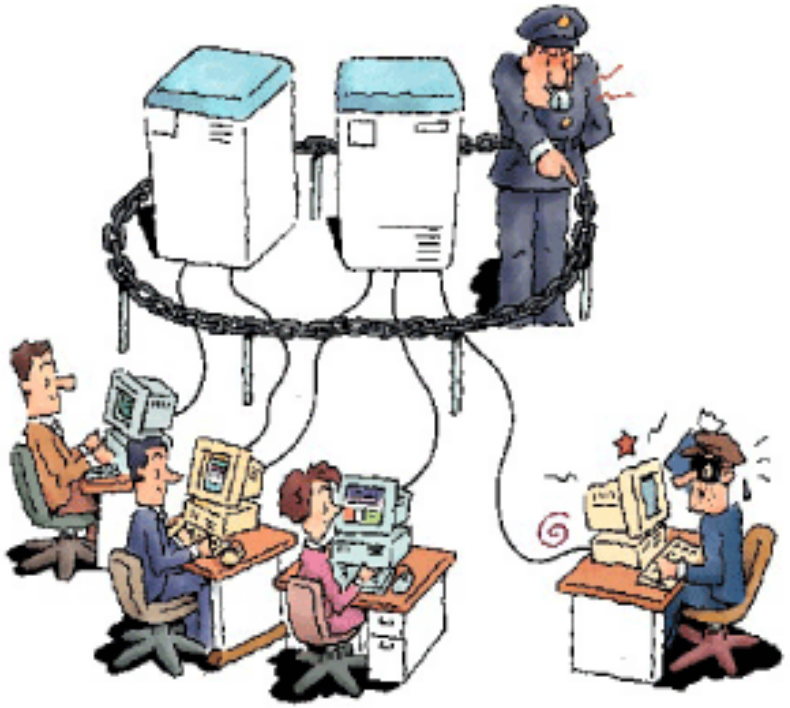


https://www.oreilly.com/library/view/wso2-developers-guide/9781787288317/assets/b2a2bfed-1d53-41cc-9f21-53249e466d0f.png

การรักษาความปลอดภัยของระบบคอมพิวเตอร์

การรักษาความปลอดภัยของระบบคอมพิวเตอร์

- การรักษาความปลอดภัยด้านกายภาพ (Physical Security)
- การรักษาความปลอดภัยส่วนบุคคล (Personal Security)
- การรักษาความปลอดภัยในการปฏิบัติงาน (Operation Security)
- การรักษาความปลอดภัยของในการติดต่อสื่อสารข้อมูล (Communication Security)
- การรักษาความปลอดภัยของเครือข่าย (Network Security)
- การรักษาความปลอดภัยของสารสนเทศ (Information Security)



การรักษาความปลอดภัยด้านกายภาพ (Physical Security)

การรักษาความปลอดภัยด้านกายภาพ หมายถึง การป้องกันการเข้าถึงสถานที่ซึ่งเป็นที่ตั้งและพื้นที่ใช้งานของระบบเทคโนโลยีสารสนเทศ ตลอดจนอุปกรณ์คอมพิวเตอร์ ข้อมูล และสารสนเทศโดยไม่ได้รับอนุญาต และป้องกันจากภัยธรรมชาติ การโจรกรรม และความเสียหายอื่น ๆ ซึ่งอาจทำให้เกิดความเสียหาย และการแทรกแซงการทำงานต่อระบบคอมพิวเตอร์

- กลุ่มที่ 1 คือ กลุ่มที่เป็นสาเหตุทำให้เครื่องสูญหาย
- กลุ่มที่ 2 คือ กลุ่มที่เป็นสาเหตุทำให้เครื่องไม่สามารถทำงานได้หรือชำรุด

การรักษาความปลอดภัยส่วนบุคคล (Personal Security)

การรักษาความปลอดภัยส่วนบุคคล เป็นการป้องกันที่เกี่ยวข้องบุคคลหรือกลุ่มบุคคล (พนิดา พานิชกุล, 2553, หน้า 4) เพื่อให้บุคคลต่าง ๆ เข้าใจในหน้าที่ความรับผิดชอบของตนเอง รวมถึงตระหนักถึงการรักษาความมั่นคงปลอดภัยในการปฏิบัติงานที่มีต่อหน่วยงาน

การรักษาความปลอดภัยในการปฏิบัติงาน (Operation Security)

การรักษาความปลอดภัยในการปฏิบัติงาน เป็นมาตรการ หรือวิธีการอย่างเป็นระบบที่ใช้ในการระบุ (identify) ควบคุม (Control) และป้องกัน (Protect) หลักฐานทั่วไปที่ไม่ระบุชั้นความลับ ที่เกี่ยวข้องหรือเชื่อมต่อกับการปฏิบัติการหรือกิจกรรมต่าง ๆ ที่สำคัญ หรือละเอียดอ่อน

การรักษาความปลอดภัยของในการติดต่อสื่อสารข้อมูล (Communication Security)

การรักษาความปลอดภัยในการติดต่อสื่อสาร เป็นการป้องกันข้อมูลในระบบเครือข่าย และป้องกันโครงสร้างพื้นฐานที่สนับสนุนระบบเครือข่าย รวมถึงเทคโนโลยีที่ใช้ในการติดต่อสื่อสาร ด้วยวิธีการซ่อนข้อมูลหรือที่เรียกว่า การเข้ารหัสข้อมูล

การรักษาความปลอดภัยของเครือข่าย (Network Security)

การรักษาความปลอดภัยของเครือข่าย เป็นการป้องกันองค์ประกอบ การเชื่อมต่อ และข้อมูลในเครือข่ายคอมพิวเตอร์ (พนิดา พานิชกุล, 2553, หน้า 4) การลักลอบเข้าถึงเครือข่ายและป้องการการลักลอบใช้งานระบบเครือข่ายอินเทอร์เน็ต นอกจากนั้นการโจมตีจากภายนอกก็ยังมีให้เห็นอยู่ เช่น เข้าถึงอุปกรณ์เครือข่ายจากระยะไกล ซึ่งทั้งหมดจำเป็นต้องวางแผนรับมือการโจมตีรูปแบบต่าง ๆ

การรักษาความปลอดภัยของสารสนเทศ (Information Security)

- ข้อมูลสำคัญที่ต้องปกป้องคือ **ข้อมูลขององค์กร** เช่น ข้อมูลรายละเอียดการสั่งซื้อสินค้า ข้อมูลรายรับรายจ่ายของบริษัท ข้อมูลเงินเดือนพนักงาน ข้อมูลรหัสผ่านของเจ้าหน้าที่ระบบเครือข่าย ซึ่งข้อมูลเหล่านี้จะอยู่ในเครื่องให้บริการฐานข้อมูล
- การป้องกันและรักษาความปลอดภัยของข้อมูลจะมีความเกี่ยวข้องกับการรักษาความปลอดภัยของเครื่องให้บริการและระบบเครือข่าย

สภาพแวดล้อมของความปลอดภัย

- ภัยคุกคาม (Threat)
- เหตุสุดวิสัย (Accidental)

ภัยคุกคาม (Threat)

- หมายถึง สิ่งที่อาจจะก่อให้เกิดความเสียหายต่อคุณสมบัติของข้อมูลด้านใดด้านหนึ่งหรือมากกว่าหนึ่งด้าน
  - การถูกคุกคามจากนักเจาะระบบ (Hacker)
  - การถูกคุกคามโดย Virus, Worm
  - การถูกคุกคามโดยพวกอยากทดลอง
  - การถูกคุกคามโดยผู้ก่อการร้าย

เหตุสุดวิสัย (Accidental)

- ปรากฏการณ์ทางธรรมชาติ
- ฮาร์ดแวร์หรือซอฟต์แวร์ชำรุดหรือทำงานผิดพลาด
- ความผิดพลาดของผู้ควบคุมระบบ

มาตรฐานความปลอดภัย

- ISO/IEC27001
- ISO/IEC TR 13335
- ISO/IEC 15408:2005/Common Criteria/ ITSEC
- ITIL
- FIPS PUB 200
- NIST 800-14
- IT BPM
- COBIT
- COSO

ISO/IEC27001

- ปัจจุบันเป็นเวอร์ชั่น ISO/ IEC27001:2013 หรือเรียกว่า ISMS (Information Security Management System) เป็นมาตรฐานการจัดการข้อมูลที่มีไว้เพื่อให้ธุรกิจดำเนินไปอย่างต่อเนื่อง ข้อกำหนดต่าง ๆ ถูกกำหนดขึ้นโดยองค์กรที่มีความน่าเชื่อถือคือ ISO (The International Organization for Standardization) และ IEC (The International Electrotechnical Commission) มาตรฐานนี้เป็นมาตรฐานสากลที่มุ่งเน้นด้านการรักษาความมั่นคงปลอดภัยให้กับระบบสารสนเทศขององค์กรและใช้เป็นมาตรฐานอ้างอิงเพื่อเป็นแนวทางในการเสริมสร้างความปลอดภัยให้กับระบบสารสนเทศอย่างแพร่หลาย สามารถนำไปประยุกต์ใช้เพื่อรักษาความมั่นคงให้กับระบบสารสนเทศขององค์กร การนำระบบ ISO27001 ให้มีประสิทธิภาพต้องวางแผนจัดทำระบบ (Establish) การนำไปปฏิบัติ (Implement) การรักษาไว้ (Maintain) การรักษามาตรฐานและปรับปรุงระบบอย่างต่อเนื่อง (Continual Improvement) จะต้องมีหลักฐานทั้งในส่วนของเอกสารและผลการปฏิบัติที่น่าเชื่อถือ สะท้อนความเป็นจริงและตรวจสอบย้อนกลับได้ (นันทนิตร์ มีพร้อม, 2560, หน้า 41)

ISO/IEC TR 13335

- มาตรฐานนี้ย่อมาจาก Guidelines for the Management of IT Security ซึ่งถูกอ้างอิงโดย ISO/IEC2007 ในเรื่องของการจัดทำ technical report เพื่อระบุภัยคุกคาม จุดอ่อนและช่องโหว่ของระบบ รวมทั้งแนวทางของการประเมินความเสี่ยงจนสามารถระบุแนวทางการลดความเสี่ยงนั้นได้

ISO/IEC 15408:2005/Common Criteria/ ITSEC

มาตรฐานนี้จัดทำขึ้นเพื่อใช้เป็นเกณฑ์กลางในการวัดระดับความมั่นคงปลอดภัยว่าอยู่ในระดับใด โดยมาตรฐานนี้เกิดจากความร่วมมือขององค์กรต่าง ๆ ซึ่งส่วนใหญ่แล้วเป็นประเทศในกลุ่มประเทศยุโรป ได้แก่องค์กร Communication Security Establishment จากประเทศแคนาดา องค์กร Central Service of the Information จากประเทศฝรั่งเศส องค์กร Federal Office for Security in Information Technology จากประเทศเยอรมนี องค์กร The Netherlands National Communications Security Agency จากประเทศเนเธอร์แลนด์ องค์กร Communications-Electronics Security Group จากประเทศสหราชอาณาจักรอังกฤษ และองค์กร National Institute of Standards and Technology and National Security Agency จากประเทศสหรัฐอเมริกา

ITIL

ITIL ย่อมาจาก Information Technology Infrastructure Library เป็นแนวทางปฏิบัติเรื่องเกี่ยวกับโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศ ได้รับการจัดทำเผยแพร่โดยหน่วยงานรัฐบาล CCTA ซึ่งขณะนี้กลายเป็นองค์กร OGC แต่ก็มิได้ประกาศบังคับว่าทุกองค์กรที่เกี่ยวข้องจะต้องปฏิบัติตาม ITIL

1. การบริหารจัดการซอฟต์แวร์และทรัพย์สินขององค์กร (Software and Asset Management)
2. การส่งมอบผลิตภัณฑ์หรือบริการที่ได้มาตรฐาน (Service Delivery)
3. คุณภาพของการบริการหลังส่งมอบ (Service Support)
4. การวางแผนสำหรับการบริหารจัดการการให้บริการ (Planning to Implement Service Management)
5. การบริหารจัดการโครงสร้างพื้นฐานด้านไอซีที (ICT Infrastructure Management)
6. การบริหารจัดการแอปพลิเคชัน (Application Management)
7. การบริหารจัดการด้านความมั่นคงปลอดภัย (Security Management)
8. มุมมองทางธุรกิจ (Business Perspective, Volume II)

FIPS PUB 200

FIPS PUB 200 ย่อมาจาก **The Federal Information Processing Standards Publication 200** กล่าวถึงเรื่องของข้อกำหนดขั้นต่ำสำหรับความต้องการด้านความมั่นคงปลอดภัย ซึ่งเป็นภาคบังคับของ องค์กรบริหารจัดการสารสนเทศและระบบสารสนเทศกลางของประเทศสหรัฐอเมริกาทุกองค์กรที่เป็นหน่วยงานภาครัฐจะต้องปฏิบัติตามข้อกำหนดด้านความมั่นคงปลอดภัยนี้เป็นอย่างน้อย โดยมาตรฐานนี้จะมีการระบุประเภทของระบบสารสนเทศต่าง ๆ และวิธีปฏิบัติที่จำเป็นสำหรับควบคุมเพื่อให้เกิดความมั่นคงปลอดภัยของสารสนเทศในระบบนั้น ๆ

1. การระบุข้อกำหนดชั้นต่ำของระบบประมวลผลสารสนเทศขององค์กรกลางในประเทศสหรัฐอเมริกา
2. การจัดทำข้อกำหนดนี้เพื่อสนับสนุนการพัฒนา
3. การลงมือปฏิบัติ
4. การดำเนินการ เพื่อสร้างความมั่นคงปลอดภัยระบบสารสนเทศ โดยหน่วยงานสามารถคัดเลือกเฉพาะส่วนที่เกี่ยวข้องกับองค์กรของตนมาปฏิบัติตามมาตรฐานนี้จึงได้มีการจัดทำแนวทางในการคัดเลือก และกำหนดมาตรการด้านความมั่นคงปลอดภัยที่จำเป็นและเหมาะสมสำหรับระบบประมวลผลสารสนเทศของแต่ละหน่วยงาน

NIST 800-14

NIST 800-14 ย่อมาจาก National Institute of Standards and Technology 800-14 เป็นมาตรฐานที่ได้รับการพิมพ์เผยแพร่จากสถาบันมาตรฐานเทคโนโลยีสารสนเทศแห่งชาติของสหรัฐอเมริกา โดยใช้ชื่อหนังสือว่า Generally Accepted Principles and Practices for Securing Information Technology Systems มาตรฐานนี้ได้รับการจัดทำและเผยแพร่ขึ้นเพื่อเสริมสร้างความมั่นคงปลอดภัยให้แก่ระบบเทคโนโลยีสารสนเทศขององค์กรหรือหน่วยงานต่าง ๆ ในประเทศสหรัฐอเมริกาให้มากที่สุด เพื่อเป็นการป้องกันภัยคุกคามด้านอาชญากรรมคอมพิวเตอร์และการละเมิดความมั่นคงปลอดภัยข้อมูลสารสนเทศ โดยเฉพาะอย่างยิ่ง สารสนเทศบนระบบโครงสร้างพื้นฐานของประเทศ

NIST 800-14

1. ในพันธกิจขององค์กรต้องให้การสนับสนุนเรื่องของความมั่นคงปลอดภัยคอมพิวเตอร์
2. ในการบริหารจัดการขององค์กรต้องผนวกเรื่องของความมั่นคงปลอดภัยคอมพิวเตอร์มีไว้เป็นสาระสำคัญด้วย
3. ควรมีการลงทุนที่เหมาะสมในเรื่องของความมั่นคงปลอดภัยคอมพิวเตอร์
4. ผู้เป็นเจ้าของระบบต้องแสดงความรับผิดชอบต่อการรักษาความมั่นคงปลอดภัยของระบบโดยตลอด
5. ความรับผิดชอบและการดูแลเอาใจใส่ในเรื่องความมั่นคงปลอดภัยคอมพิวเตอร์ ต้องได้รับการดำเนินการอย่างชัดแจ้ง
6. การรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ต้องการแนวทางที่ผสมผสานในวิธีปฏิบัติ เช่น การรักษาความมั่นคงปลอดภัยทางกายภาพทางด้านฮาร์ดแวร์ ซอฟต์แวร์ และผู้ใช้ เป็นต้น
7. ความมั่นคงปลอดภัยคอมพิวเตอร์ต้องได้รับการปรับปรุงให้ดีขึ้นอย่างต่อเนื่องและสม่ำเสมอ
8. ปัจจัยแวดล้อมสามารถส่งผลต่อการรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ได้เสมอ

IT BPM

IT BPM ย่อมาจาก Information Technology Baseline Protection Manual เป็นหนังสือคู่มือที่แนะนำการรักษาความมั่นคงปลอดภัยระบบอย่างมีมาตรฐาน แต่อาจกำหนดไว้เป็นมาตรฐานขั้นต่ำ คู่มือนี้พิมพ์เผยแพร่โดยสถาบันมาตรฐานแห่งชาติอังกฤษ BSI คู่มือนี้จะให้การแนะนำว่าระบบที่ยกตัวอย่างนี้ ควรมีเกราะป้องกัน หรือวิธีการด้านความมั่นคงปลอดภัยอย่างน้อยต้องดำเนินการอย่างไรบ้าง ซึ่งแต่ละองค์กรอาจนำไปประยุกต์ใช้ด้วยวัตถุประสงค์ที่แตกต่างกันออกไป

IT BPM

เนื้อหาประกอบด้วย

1. ระบบต้องมีการบริหารจัดการด้านความมั่นคงปลอดภัยตั้งแต่ชั้นการออกแบบ ประสานงาน และติดตามสถานะของความมั่นคงปลอดภัยของระบบที่เกี่ยวกับหน้าที่งานนั้น
2. ระบบต้องมีการวิเคราะห์และจัดทำเป็นเอกสารเกี่ยวกับโครงสร้างที่มีอยู่ของทรัพย์สินที่เป็นเทคโนโลยีสารสนเทศในองค์กร
3. ระบบต้องได้รับการประเมินถึงมาตรการและระบบบริหารจัดการด้านความมั่นคงปลอดภัยเดิมที่ได้จัดทำไว้แล้วนั้นว่า มีประสิทธิภาพเพียงพอและเหมาะสมแล้วหรือยัง
4. องค์กรต่าง ๆ สามารถนำโครงสร้างของเครือจ่ายที่มีความมั่นคงปลอดภัย ซึ่งได้ออกแบบไว้ เหมาะสมแล้วตามคู่มือนี้มาเป็นแนวทางในการจัดทำเครือข่ายขององค์กร
5. ระบบต้องได้รับการดำเนินการปรับปรุงแก้ไขกรณีที่พบว่ามาตรการหรือแนวทางการรักษาความมั่นคงปลอดภัยเหล่านั้นไม่เพียงพอ หรือมีการดำเนินบางอย่างที่ยังไม่รัดกุม

COBIT

- **กรอบวิธีปฏิบัติ COBIT (Control Objectives for Information and related Technology)** พัฒนาขึ้นโดย ISACA ใช้สำหรับการพัฒนาเพื่อให้ระบบเทคโนโลยีสารสนเทศมีความเป็น "ไอทีภิบาล" (IT Governance) เพื่อให้ระบบเทคโนโลยีสารสนเทศมีประสิทธิภาพและมีความคุ้มทุน COBIT ได้รับการใช้แพร่หลายในกลุ่มธุรกิจด้านการเงินและการธนาคาร เดิมที COBIT ได้รับการเผยแพร่ในรูปแบบของ "กระบวนการ" ด้านเทคโนโลยีสารสนเทศ ภายหลังได้มีการเพิ่มเติมแนวทางการปฏิบัติเพื่อ "การให้บริการ" ด้านเทคโนโลยีสารสนเทศที่มีประสิทธิภาพมากขึ้น อย่างไรก็ตามกรอบวิธีปฏิบัติ COBIT มุ่งเน้นไปที่การยกระดับ "ประสิทธิภาพ" ของระบบเทคโนโลยีสารสนเทศมากกว่าการมุ่งเน้นทางด้านการ "รักษาความปลอดภัย"

COSO

- COSO ย่อมาจาก The Committee of Sponsoring Organizations of the Treadway Commission เป็นกรอบปฏิบัติที่ช่วยส่งเสริมให้การตรวจสอบกิจการภายในองค์กรมีความเที่ยงตรงและโปร่งใสโดยเฉพาะองค์กรด้านการเงิน โดยเน้นไปที่การจัดทำงบการเงินเพื่อให้เกิดความน่าเชื่อถือ ความถูกต้อง เป็นไปตามหลักความจริง จริยธรรมต่อการตรวจสอบภายใน และประสิทธิภาพการรายงานตามสิ่งที่พบ เนื้อหาส่วนใหญ่ของ COSO มุ่งเน้นไปในด้านของการจัดทำรายงานงบการเงินและจรรยาบรรณในวิชาชีพผู้ตรวจสอบ

COSO

ในการทำความเข้าใจเกี่ยวกับแนวคิดของ COSO จะต้องพิจารณาในเนื้อหาอย่างลึกซึ้ง โดยองค์ประกอบทั้ง 5 มีดังนี้

1. สภาพแวดล้อมการควบคุม (Control Environment) ภาพแวดล้อมของการควบคุมเป็นองค์ประกอบที่เกี่ยวกับการสร้างจิตสำนึกและบรรยากาศของการควบคุมภายในซึ่งปัจจัยหลายๆ ปัจจัยที่นำมาพิจารณารวมกันส่งผลให้เกิดความมีประสิทธิผลของมาตรการหรือวิธีการควบคุมในองค์กร

2. การประเมินความเสี่ยง (Risk Assessment) การประเมินความเสี่ยงนั้นเป็นกระบวนการที่ทำให้กิจการขององค์กรทราบถึงความเสี่ยงที่กำลังจะเผชิญล่วงหน้าได้ เมื่อทราบถึงความเสี่ยงแล้วก็สามารถที่จะบริหารความเสี่ยงเพื่อเปลี่ยนวิกฤติให้เป็นโอกาส และเพื่อลดผลกระทบความเสียหายที่จะเกิดขึ้นได้

3. กิจกรรมการควบคุม (Control Activities) หมายถึง การกระทำที่สนับสนุนและส่งเสริมการปฏิบัติงานให้เป็นไปตามนโยบาย วิธีปฏิบัติงาน และคำสั่งต่างๆ ที่ฝ่ายบริหาร กำหนดซึ่งจะต้องเป็นการกระทำที่ถูกต้องและในเวลาที่เหมาะสม จะเพิ่มความมั่นใจในความสำเร็จตามวัตถุประสงค์ที่กำหนด

4. ข้อมูลสารสนเทศ และการสื่อสารในองค์กร (Information and Communication) ข้อมูลสารสนเทศ (Information) เป็นข้อมูลที่มีความจำเป็นสำหรับการปฏิบัติงานของบุคลากรทั้งผู้บริหารและผู้ปฏิบัติงานทุกระดับ สำหรับการสื่อสารที่มีประสิทธิภาพนั้นหมายถึง การจัดระบบการสื่อสารให้ข้อมูลส่งไปถึงผู้ที่ควรได้รับและระบบการสื่อสารที่ดีนั้น จะต้องประกอบด้วยทั้งระบบการสื่อสารภายในองค์กรหรือการสื่อสารที่เกิดขึ้นภายในองค์กรเดียวกันซึ่งควรจัดให้เป็นรูปแบบการสื่อสารสองทาง

5. การติดตามและประเมินผล (Monitoring) มาตรการและระบบการควบคุมภายในมีประสิทธิผลและได้รับการปรับปรุงให้ทันสมัยอยู่ตลอดเวลา

https://www.rama.mahidol.ac.th/risk_mgt/th/article/03092016-0912

การบริหารและประเมินความเสี่ยงของระบบคอมพิวเตอร์และเครือข่าย

ขั้นตอนที่ 1 ศึกษาโครงสร้างและความซับซ้อนของระบบเครือข่ายเป้าหมาย (ที่เราจะทำการประเมินความเสี่ยง) และศึกษาองค์ประกอบต่าง ๆ ที่เกี่ยวข้อง

ขั้นตอนที่ 2 กำหนดขอบเขตของการประเมินความเสี่ยง ว่าจะประเมินเฉพาะบางส่วนของเครือข่ายหรือทั้งหมด จะทำการประเมินแบบ Black Box หรือ White Box

ขั้นตอนที่ 3 วางแผนระยะเวลาและกำหนดตารางเวลา

ขั้นตอนที่ 4 วิเคราะห์ผลกระทบที่อาจจะเกิดขึ้นเมื่อทำการสแกนในช่วงเวลาที่ระบบกำลังให้บริการอยู่

ขั้นตอนที่ 5 วางแผนเกี่ยวกับเรื่อง Downtime (หากมี Downtime เกิดขึ้น) รวมทั้งวิธีการที่จะทำให้ระบบสามารถกลับคืนมาทำงานได้เช่นเดิมภายในเวลาอันรวดเร็ว

ขั้นตอนที่ 6 ประมาณการเกี่ยวกับกระบวนการสแกน ซึ่งขึ้นอยู่กับความซับซ้อนของเน็ตเวิร์กเป้าหมายและโฮสต์

ขั้นตอนที่ 7 กำหนดนโยบายการสแกนสำหรับแต่ละเป้าหมาย ระดับความละเอียดของการสแกนเช่น จะสแกนอะไร เช่นการสแกนเพื่อหาข้อมูลเบื้องต้น สแกนพอร์ต การวิเคราะห์รหัสผ่าน การจำลองการโจมตี และอื่น ๆ

ขั้นตอนที่ 8 ทำการสแกนเน็ตเวิร์กและโฮสเป้าหมายที่ได้วางแผนเอาไว้

ขั้นตอนที่ 9 นำผลลัพธ์จากการแสกนมาจัดหมวดหมู่ และทำการวิเคราะห์ช่องโหว่ เช่น ค่าคอนฟิกกูเรชั่นที่ผิดพลาด การใช้ค่าคอนฟิกดีฟอลต์ คุณภาพของรหัสผ่าน เวอร์ชั่นของซอฟต์แวร์และแพตช์

ขั้นตอนที่ 10 ส่งรายงานผลการประเมินความเสี่ยง และแนะนำแนวทางในการป้องกัน (ธวัชชัย ชมศิริ, 2553, หน้า 28)

บทสรุป


it's
Q&A
TIME!

คำถามทบทวนบทที่ 1