หลักการพื้นฐานด้านความมั่นคงปลอดภัยสารสนเทศ
Information Security Fundamentals

สารบัญ

บทที่ 1

จุดประสงค์ของบทเรียน

1.1 อธิบายนิยามและแนวคิดเกี่ยวกับหลักการด้านความมั่นคงปลอดภัย สารสนเทศและความมั่นคงปลอดภัยไซเบอร์

1.2 อภิปรายคุณสมบัติและองค์ประกอบต่าง ๆที่เกี่ยวกับความมั่นคง ปลอดภัยสารสนเทศ

1.3 เรียนรู้เกี่ยวกับแนวคิดความสัมพันธ์ของสามเหลี่ยมด้านความมั่นคง ปลอดภัย การท างานและการใช้งาน

1.4 อภิปรายประเภท รูปแบบของภัยคุกคามและการโจมตีด้านความมั่นคง ปลอดภัยสารสนเทศ

1.5 อภิปรายแนวโน้มด้านความมั่นคงปลอดภัยสารสนเทศ

1.6 ท าความเข้าใจความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

บทที่ 2

คำอธิบายเกี่ยวกับบทเรียน

ความรู้พื้นฐานด้านการรักษาความมั่นคงปลอดภัยสารสนเทศเกี่ยวข้องกับการสร้างความมั่นคงปลอดภัยให้กับข้อมูล สารสนเทศ และระบบสารสนเทศ องค์ประกอบคุณสมบัติหลักด้านความมั่นคงปลอดภัยสารสนเทศ 3 ด้าน **(การรักษาความลับ ความถูกต้อง และความพร้อมใช้)** และองค์ประกอบส าคัญอื่นที่เกี่ยวข้อง แนวคิดความสัมพันธ์ของสามเหลี่ยมด้านความมั่นคงปลอดภัย ฟังก์ชันการทำงาน และการใช้งาน **(theSecurity,FunctionalityandUsabilityTriangle)** สำหรับการกำหนดระดับความมั่นคงปลอดภัยสารสนเทศ รูปแบบการโจมตีด้านความมั่นคงปลอดภัยสารสนเทศ ประเภทภัยคุกคามและช่องโหว่ ลักษณะภัยคุกคามทางไซเบอร์ แนวโน้มด้านความมั่นคงปลอดภัย การบริหารความเสี่ยงและมาตรการจัดการความเสี่ยง

บทที่ 3

กลุ่มสาระบทเรียน

3.1 แนวคิดด้านความมั่นคงปลอดภัยสารสนเทศ/ไซเบอร์

3.2 องค์ประกอบและคุณสมบัติด้านความมั่นคงปลอดภัยสารสนเทศ

3.3 ภัยคุกคามด้านความมั่นคงปลอดภัยสารสนเทศ

3.4 ประเภทการโจมตีด้านความมั่นคงปลอดภัยสารสนเทศ

3.5 แนวโน้มด้านความมั่นคงปลอดภัยสารสนเทศ

3.6 ความเสี่ยงด้านความมั่นคงปลอดภัยและมาตรการจัดการ

บทที่ 4

นิยามภายในบทเรียน

4.1 Information Security

“ความมั่นคงปลอดภัยสารสนเทศ”

(1) “ความมั่นคงปลอดภัยด้านสารสนเทศ” หมายความว่า การธำรงไว้ซึ่ง

- ความลับ **(Confidentiality)**
- ความถูกต้องครบถ้วน **(Integrity)**
- สภาพพร้อมใช้งาน **(Availability)**

รวมทั้งคุณสมบัติอื่น ได้แก่

- ความถูกต้องแท้จริง **(Authenticity)**
- ความรับผิด **(Accountability)**
- การห้ามปฏิเสธความรับผิด **(Non-repudiation)**
- ความน่าเชื่อถือ **(Reliability)**

(2) “ความมั่นคงปลอดภัยของระบบสารสนเทศ” หมายความว่า การป้องกันทรัพย์สินสารสนเทศจากการเข้าถึงใช้เปิดเผยขัดขวางเปลี่ยนแปลงแก้ไขทำให้สูญหายทำให้เสียหายถูกทำลายหรือล่วงรู้โดยมิชอบ

4.2 Confidentiality

“การรักษาความลับ” หมายความว่า การรักษาหรือสงวนไว้เพื่อป้องกันระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์หรือข้อมูลคอมพิวเตอร์ จากการเข้าถึงใช้หรือเปิดเผยโดยบุคคลซึ่งไม่ได้รับอนุญาต

4.3 Integrity

“การรักษาความครบถ้วน” หมายความว่า การดำเนินการเพื่อให้ข้อมูลสารสนเทศข้อมูลอิเล็กทรอนิกส์หรือข้อมูลคอมพิวเตอร์อยู่ในสภาพสมบูรณ์ขณะที่มีการใช้งานประมวลผล โอนหรือเก็บรักษาเพื่อมิให้มีการเปลี่ยนแปลงแก้ไขทำให้สูญเสียทำให้เสียหายหรือถูกทำลายโดยไม่ได้รับอนุญาตหรือโดยมิชอบ

4.4 Availability

“การรักษาสภาพพร้อมใช้งาน” หมายความว่า การจัดทำให้ทรัพย์สินสารสนเทศสามารถทำงานเข้าถึงหรือใช้งานได้ในเวลาที่ต้องการ

4.5 Cybersecurity

“การรักษาความมั่นคงปลอดภัยไซเบอร์” หมายความว่า มาตรการหรือการดำเนินการที่กำหนดขึ้น เพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ทั้งจากภายในและภายนอกประเทศ อันกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ

4.6 Cyber

“ไซเบอร์” หมายความรวมถึง ข้อมูลและการสื่อสารที่เกิดจากการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต หรือโครงข่ายโทรคมนาคม รวมทั้งการให้บริการโดยปกติของดาวเทียมและระบบเครือข่ายที่คล้ายคลึงกันที่เชื่อมต่อกันเป็นการทั่วไป

4.7 CyberThreats

“ภัยคุกคามทางไซเบอร์” หมายความว่า การกระทำหรือการดำเนินการใดๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์หรือข้อมูลอื่นที่เกี่ยวข้องและเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์หรือข้อมูลอื่นที่เกี่ยวข้อง

ลักษณะของภัยคุกคามทางไซเบอร์ แบ่งออกเป็น 3 ระดับ ได้แก่ ภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรงภัยคุกคามทางไซเบอร์ในระดับร้ายแรง ภัยคุกคามทางไซเบอร์ในระดับวิกฤติ

บทที่ 5

เนื้อหาในบทเรียน

5.1 แนวคิดด้านความมั่นคงปลอดภัยสารสนเทศ

5.2 หลักการสำคัญของการรักษาความมั่นคงปลอดภัยสารสนเทศ

5.3 คุณสมบัติและองค์ประกอบหลักด้านความมั่นคงปลอดภัยฯ

5.4 คุณสมบัติและองค์ประกอบอื่นที่เกี่ยวข้องด้านความมั่นคงฯ

5.5 ความสัมพันธ์ของสามเหลี่ยมด้านความมั่นคงปลอดภัยฯ

5.6 การรักษาความมั่นคงปลอดภัยไซเบอร์

5.7 การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

5.8 ความท้าทายด้านความมั่นคงปลอดภัยสารสนเทศ

5.9 กลุ่มภัยคุกคามด้านความมั่นคงปลอดภัยสารสนเทศ

5.10 ลักษณะของภัยคุกคามทางไซเบอร์

5.11 รูปแบบการโจมตีด้านความมั่นคงปลอดภัยสารสนเทศ

5.12 ประเภทการโจมตีระบบสารสนเทศ

5.13 แนวโน้มด้านความมั่นคงปลอดภัยสารสนเทศ

5.14 การบริหารความเสี่ยงและมาตรการจัดการ

5.1 แนวคิดด้านความมั่นคงปลอดภัยสารสนเทศ

ความมั่นคงปลอดภัยสารสนเทศ

“การรักษาความมั่นคงปลอดภัยสารสนเทศ” คือ การสร้างความมั่นใจในการรักษาความลับ ความถูกต้องสมบูรณ์ และสภาพความพร้อมใช้ของสารสนเทศ ตลอดจนข้อมูล ระบบสารสนเทศ และทรัพย์สินสารสนเทศ ซึ่งครอบคลุมถึงข้อมูลที่จัดเก็บ ประมวลผล และรับส่งผ่านเครือข่าย จากการเข้าถึงโดยไม่ได้รับอนุญาต การใช้งานโดยไม่ได้รับอนุญาต การใช้ในทางที่ผิด การทำลายหรือการเปลี่ยนแปลง โดยมีการบริหารจัดการความเสี่ยง และนำมาตรการต่าง ๆ ด้านบริหารจัดการ ด้านเทคนิคด้านกายภาพที่เหมาะสมมาใช้จัดการภัยคุกคามต่าง ๆ

Information Security Risk Concepts

“การรักษาความมั่นคงปลอดภัยสารสนเทศและการบริหารความเสี่ยง” จุดมุ่งหมายเพื่อสร้างความมั่นใจต่อการดำเนินธุรกิจได้อย่างต่อเนื่องและยั่งยืน ลดผลกระทบที่เกิดขึ้นจากเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ ตลอดจนการปฏิบัติตามข้อกำหนดของกฎหมายและกฎเกณฑ์ที่มีผลใช้บังคับ ภายใต้สภาพความเสี่ยงที่ยอมรับได้ขององค์กร

5.2 หลักการสำคัญของการรักษาความมั่นคงปลอดภัยสารสนเทศ

“หลักการสำคัญของการรักษาความมั่นคงปลอดภัยสารสนเทศ” คือ การปกป้องทรัพย์สินสารสนเทศตามสภาพความเสี่ยงขององค์กร การสร้างความตระหนักรู้เกี่ยวกับความจำเป็นและความสำคัญในการรักษาความมั่นคงปลอดภัยสารสนเทศ การกำหนดความรับผิดชอบและนโยบายสำหรับการรักษาความมั่นคงปลอดภัยสารสนเทศ ความต่อเนื่องในการให้บริการข้อมูล สารสนเทศ ระบบ และทรัพย์สินสารสนเทศ

โดยดำเนินการในเชิงกระบวนการอย่างเป็นระบบและต่อเนื่องพร้อมทั้งประสิทธิผลของมาตรการควบคุมทั้งมาตรการด้านบริหารจัดการ **(Administrative)** มาตรการด้านเทคนิค **(Technical)** และมาตรการทางกายภาพ **(Physicalsecurity)** ตอบสนองความต้องการทางธุรกิจและกลุ่มผู้มีส่วนได้เสีย และภายใต้การบริหารจัดการความเสี่ยงตามระดับความเสี่ยงที่ยอมรับได้ขององค์กร

5.3 คุณสมบัติและองค์ประกอบหลักด้านความมั่นคงปลอดภัยฯ

Information Security Triad

- **การรักษาความลับ (Confidentiality)** ข้อมูล สารสนเทศ เข้าถึงได้เฉพาะผู้ที่มีสิทธิ์หรือได้รับอนุญาตเท่านั้น จะต้องไม่มีการเปิดเผยโดยมิชอบ หรือโดยบุคคลที่ไม่มีสิทธิ์หรือไม่ได้รับอนุญาต
- **การรักษาความถูกต้องครบถ้วน (Integrity)** ข้อมูล สารสนเทศ มีความถูกต้อง จะมีการแก้ไข เปลี่ยนแปลง ได้เฉพาะผู้ที่มีสิทธิ์หรือได้รับอนุญาตเท่านั้น
- **สภาพความพร้อมใช้ (Availability)** ข้อมูล สารสนเทศ มีความพร้อมในการใช้งานอยู่เสมอผู้มีสิทธิ์หรือได้รับอนุญาต สามารถเข้าถึงได้เมื่อต้องการ

5.4 คุณสมบัติและองค์ประกอบอื่นที่เกี่ยวข้องด้านความมั่นคงฯ

Other Information Security Properties

- **ความถูกต้องแท้จริง (Authenticity)** คุณลักษณะเฉพาะเพื่อยืนยันความถูกต้องแท้จริงถึงตัวตนผู้ใช้งาน
- **ความรับผิด (Accountability)** ความรับผิดชอบที่สามารถตรวจสอบได้
- **การห้ามปฏิเสธความรับผิด (Non-repudiation)** วิธีการที่ผู้ส่งและผู้รับข้อความจะไม่สามารถปฏิเสธการส่งหรือการรับข้อความนั้นได้ หากได้ดำเนินการนั้นไปแล้ว
- **ความน่าเชื่อถือ (Reliability)** ความสามารถในการให้บริการได้ตามที่กำหนดไว้

5.5 ความสัมพันธ์ของสามเหลี่ยมด้านความมั่นคงปลอดภัยฯ

(The Security, Functionality, and Usability Triangle)

การกำหนด **“ระดับความมั่นคงปลอดภัยของสารสนเทศ”** ต้องพิจารณาการรักษาความสมดุลขององค์ประกอบ 3 ด้าน ที่เรียกว่า **“ความสัมพันธ์ของสามเหลี่ยมด้านความมั่นคงปลอดภัย ด้านฟังก์ชั่นการทำงาน และด้านการใช้งาน”** ซึ่งจะต้องยืดหยุ่นหรือปรับไปตามจุดประสงค์ที่ต้องการ จากข้อกำหนดด้านความมั่นคงปลอดภัย **(Requirements)** คุณลักษณะ **(Features)** และความต้องการใช้งาน **(GUI)** ตัวอย่างเช่น ในบางครั้งเพื่อตอบสนองความสะดวกในการใช้งาน ก็อาจจำเป็นต้องลดระดับมาตรการด้านความมั่นคงปลอดภัย

5.6 การรักษาความมั่นคงปลอดภัยไซเบอร์

Cybersecurity

การรักษาความมั่นคงปลอดภัยไซเบอร์เป็นการปกป้องด้านความมั่นคงปลอดภัยจากภัยคุกคามต่าง ๆ ตามเป้าหมายของการรักษาความมั่นคงปลอดภัยสารสนเทศ ในการรักษาความลับ ความถูกต้องสมบูรณ์ และสภาพความพร้อมใช้ สำหรับข้อมูล สารสนเทศ และระบบสารเทศ ในสภาพแวดล้อมไซเบอร์ที่มีการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต หรือโครงข่ายโทรคมนาคม รวมทั้งการให้บริการโดยปกติของดาวเทียมและระบบเครือข่ายที่คล้ายคลึงกัน ที่เชื่อมต่อกันเป็นการทั่วไป ทั้งนี้ เพื่อดำเนินการมาตรการจัดการภัยคุกคามทางไซเบอร์

Cybersecurityfor CII

หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical information infrastructure: CII) จะต้องมีการประเมินและตรวจสอบว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้นหรือคาดว่าจะเกิดขึ้นหรือไม่ โดยให้ดำเนินการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ตาม ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน

ประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

- แผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
- แผนการรับมือภัยคุกคามทางไซเบอร์

กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

- ระบุความเสี่ยง
- มาตรการป้องกันความเสี่ยง
- มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์
- มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์
- มาตรการรักษาและฟื้นฟูความเสียหาย

5.7 การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคล

Data Security vs. Data Privacy and Data Protection

การรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลคือ การธำรงไว้ซึ่งความลับ ความถูกต้องครบถ้วน และสภาพพร้อมใช้งานของข้อมูลส่วนบุคคลทั้งนี้ เพื่อป้องกันการสูญหาย เข้าถึงใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยมิชอบ โดยต้องมีมาตรการป้องกันด้านการบริหารจัดการด้านเทคนิคและด้านกายภาพอย่างน้อยครอบคลุมในเรื่องการเข้าถึงหรือควบคุมการใช้งานข้อมูลส่วนบุคคล
(AccessControl)

Data Breach

การรั่วไหลของข้อมูล และเหตุละเมิดที่เกี่ยวข้องกับข้อมูล ซึ่งมีสถิติสูงเพิ่มขึ้นเรื่อย ๆ ได้กลายเป็นภัยคุกคามร้ายแรงต่อองค์กร ทั้งกรณีข้อมูลเสียหาย สูญหาย รวมถึงประเด็นด้านชื่อเสียงและภาพลักษณ์องค์กร อันเนื่องมาจากเหตุละเมิดหรือเหตุการณ์ที่เกี่ยวข้องด้านความมั่นคงปลอดภัยไซเบอร์

5.8 ความท้าทายด้านความมั่นคงปลอดภัยสารสนเทศ

Security Challenges

- ความก้าวหน้าและการเปลี่ยนแปลงด้านเทคโนโลยี
- การเพิ่มมากขึ้นของระบบงานผ่านเครือข่าย
- ความซับซ้อนของการบริหารจัดการเทคโนโลยีระบบคอมพิวเตอร์ และโครงสร้างพื้นฐาน
- ความยุ่งยากในการจัดการสภาพแวดล้อมระบบที่กระจายภายใต้การจัดการแบบรวมศูนย์
- เหตุละเมิดด้านความมั่นคงปลอดภัยและการรั่วไหลของข้อมูลที่ส่งผลกระทบต่อองค์กร
- ความสามารถในการปฏิบัติตามกฎหมายและข้อกำหนดของหน่วยงานกำกับดูแล
- การรักษาความต่อเนื่องและความพร้อมรับมือต่อภัยคุกคามในการให้บริการระบบและข้อมูล

5.9 กลุ่มภัยคุกคามด้านความมั่นคงปลอดภัยสารสนเทศ

Network Threats

(1) ภัยคุกคามระบบเครือข่าย (Network Threats)

ภัยคุกคามที่มีต่อชุดระบบคอมพิวเตอร์และอุปกรณ์ต่างๆ ที่เชื่อมต่อกันด้วยช่องทางเครือข่ายสื่อสารเพื่อแบ่งปันทรัพยากรและข้อมูล โดยที่ผู้ไม่ประสงค์ดีอาจเจาะเข้าไปในช่องทางเครือข่ายสื่อสาร เพื่อขโมยข้อมูล ที่ส่งผ่านเครือข่าย หรือกระทำใด ๆ ที่ส่งผลต่อข้อมูล สารสนเทศ และระบบสารสนเทศ

Network Threats

Information Gathering	• การลาดตระเวน หรือเก็บรวบรวมข้อมูลของเป้าหมาย
Sniffing and Eavesdropping	• การดักจับข้อมูลและการลักลอบดักฟัง
Spoofing	• การปลอมตัวเพื่อโจมตีระบบหรือควบคุมระบบ
Session Hijacking, Man-in-the-Middle Attack	• การขโมยเซสชั่นและปลอมแทรกระหว่างกลาง
DNS and ARP Poisoning	• การเปลี่ยนข้อมูลโดเมนเว็บไปยังปลายทางอื่น
Password-based Attacks	• การโจมตีรหัสผ่าน
Denial-of-Service Attack	• การโจมตีระบบให้บริการหยุดชะงัก
Compromised-key Attack	• การโจมตีเจาะกุญแจรหัส
Firewall and IDS Attacks	• การโจมตีอุปกรณ์ความปลอดภัยเครือข่าย

Host Threats

(2) ภัยคุกคามระบบโฮสต์ (Host Threats)

ภัยคุกคามที่มุ่งเป้าระบบโฮสต์เฉพาะที่มีข้อมูลที่มีค่าหรือความสำคัญ ผู้ไม่ประสงค์ดีพยายามละเมิดความปลอดภัยของทรัพยากรระบบข้อมูล ซึ่งส่งผลต่อการใช้งาน

Host Threats

Malware Attacks	• การโจมตีด้วยมัลแวร์
Footprinting	• การสำรวจร่องรอยและรวบรวมข้อมูลระบบ
Password Attacks	• การโจมตีรหัสผ่าน
Denial-of-Service Attack	• การโจมตีระบบให้บริการหยุดชะงัก
Arbitrary Code Execution	• การสั่งดำเนินการด้วยคำสั่งแปลกปลอม
Unauthorized Access	• การเข้าถึงโดยไม่ได้รับอนุญาต
Privilege Escalation	• การยกระดับสิทธิ์ของผู้ไม่ประสงค์ดีเพื่อควบคุมระบบ
Backdoor Attacks	• การโจมตีผ่านเส้นทางลับที่เป็นรูรั่วของระบบ
Physical Security Threats	• ภัยคุกคามด้านความมั่นคงปลอดภัยทางกายภาพ

Application Threats

(3) ภัยคุกคามระบบงาน (Application Threats)

ภัยคุกคามที่มีต่อช่องโหว่ของระบบงานหรือระบบสารสนเทศ อันเนื่องมาจากมาตรการด้านความมั่นคงปลอดภัยที่ไม่เหมาะสมในระหว่างการพัฒนาหรือการบำรุงรักษาระบบ

Application Threats

Improper Data/Input Validation	• การตรวจสอบข้อมูลหรือการนำเข้าสู่ระบบที่ไม่เหมาะสม
Authentication and Authorization Attacks	• การโจมตีต่อการยืนยันตัวตนและการพิสูจน์ตัวตน
Security Misconfiguration	• การตั้งค่าผิดพลาดด้านความมั่นคงปลอดภัย
Information Disclosure	• การเปิดเผยข้อมูล
Broken Session Management	• การจัดการเซสชั่นที่บกพร่อง
Buffer Overflow Issues	• ปัญหาจากข้อมูลไม่ประสงค์ดีที่เกินขนาดความจุหน่วยความจำชั่วคราว
Cryptography Attacks	• การโจมตีด้านการเข้ารหัสลับ
SQL Injection	• การใช้คำสั่ง SQL เพื่อทำความเสียหายต่อระบบฐานข้อมูล
Improper Error Handling and Exception Management)	• ความบกพร่องในการจัดการข้อผิดพลาด

5.10 ลักษณะของภัยคุกคามทางไซเบอร์

Cybersecurity / Cyber Threats

ภัยคุกคามด้านความมั่นคงปลอดภัยไซเบอร์หรือ ภัยคุกคามทางไซเบอร์หมายถึง การกระทำหรือการดำเนินการใด ๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์ โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึง

ลักษณะของภัยคุกคามทางไซเบอร์แบ่งออกเป็น 3 ระดับ

- **ภัยคุกคามทางไซเบอร์ในระดับวิกฤติ**

ภัยคุกคามทางไซเบอร์ที่มีความเสี่ยงอย่างมีนัยสำคัญถึงระดับที่ทำให้ระบบคอมพิวเตอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศ หรือการให้บริการของรัฐด้อยประสิทธิภาพลง

- **ภัยคุกคามทางไซเบอร์ในระดับร้ายแรง**

การเพิ่มขึ้นอย่างมีนัยสำคัญ เพื่อโจมตีโครงสร้างพื้นฐานสำคัญของประเทศ จนไม่สามารถทำงานหรือให้บริการได้

- **ภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง**

การโจมตีในระดับที่สูงขึ้นส่งผลกระทบรุนแรงเป็นวงกว้าง ล้มเหลวทั้งระบบในระดับประเทศ ไม่สามารถควบคุมการทำงานส่วนกลางของระบบคอมพิวเตอร์ของรัฐ บุคคลจำนวนมากเสียชีวิต

5.11 รูปแบบการโจมตีด้านความมั่นคงปลอดภัยสารสนเทศ

Information Security Attack Vectors

- ภัยคุกคามทางไซเบอร์ระดับสูง **(Advanced Persistent Threats: APT)**
- ภัยคุกคามต่ออุปกรณ์พกพา **(Mobile Threats)**
- ภัยคุกคามจากการประมวลผลแบบคลาวด์ **(Cloud Computing Threats)**
- มัลแวร์ ไวรัสคอมพิวเตอร์ และหนอนคอมพิวเตอร์ **(Malware, Virus and Worms)**
- บอตเน็ต **(Botnet)**
- การโจมตีที่เกิดขึ้นจากภายในองค์กร **(Insider Attack)**

5.12 ประเภทการโจมตีระบบสารสนเทศ

Types of Attacks on a System

ระบบที่มีจุดบกพร่องหรือช่องโหว่ด้านความมั่นคงปลอดภัย อันเนื่องมาจากการพัฒนาและบำรุงรักษาระบบที่ไม่ดีหรือไม่เหมาะสม การทดสอบที่ไม่เพียงพอ รวมถึงการกำหนดค่าความปลอดภัยของระบบอย่างผิดพลาดหรือไม่ถูกต้อง เป็นช่องโหว่ให้ผู้โจมตีสามารถเข้าถึงข้อมูลหรือระบบหรืออาจใช้ประโยชน์โดยมิชอบ

ผู้ดูแลระบบควรจะต้องตรวจสอบและปรับปรุงแก้ไขช่องโหว่ระบบอย่างสม่ำเสมอ รวมทั้งเปลี่ยนการใช้ค่าเริ่มต้นของอุปกรณ์และระบบ ปิดใช้งานพอร์ตและบริการที่ไม่จำเป็น เพื่อลดความเสี่ยงจากการโจมตีระบบสารสนเทศ โดยจำแนกประเภทการโจมตีเป็น 4 ระดับ

- ระดับระบบปฏิบัติการ **Operating System Attacks**
- ระดับค่าการติดตั้งระบบ **Mis-configuration Attacks**
- ระดับระบบงาน **Application-Level Attacks**
- ระดับชุดคำสั่งระบบ **Shrink-Wrap Code Attacks**

Information Security Attack Vectors

(1) การโจมตีระบบปฏิบัติการ (Operating System Attacks)

ช่องโหว่บางอย่างของระบบปฏิบัติการ ตัวอย่าง ได้แก่

- ช่องโหว่ในพื้นที่หน่วยความจำชั่วคราว **(Buffer overflow vulnerabilities)**
- จุดบกพร่องในระบบปฏิบัติการ **(Bugs in the operating system)**
- ระบบปฏิบัติการที่ไม่มีการแก้ไขปรับปรุง **(An unpatched operating system)**

การโจมตีในระดับระบบปฏิบัติการ ตัวอย่าง ได้แก่

- การใช้ประโยชน์จากการใช้งานโปรโตคอลเครือข่ายที่เฉพาะเจาะจง **(Exploiting specific network protocol implementations)**
- การโจมตีผ่านระบบพิสูจน์ตัวตนที่ติดตั้งในระบบ **(Attacking built-in authentication systems)**
- การทำลายความมั่นคงปลอดภัยของระบบแฟ้มข้อมูล **(Breaking file-system security)**
- การเจาะรหัสผ่านและกลไกการเข้ารหัส **(Cracking passwords and encryption mechanisms)**

(2) การโจมตีที่มีต่อการกำหนดค่าติดตั้งระบบที่ไม่ถูกต้อง (Mis-configuration Attacks)

การตั้งค่าความปลอดภัยของระบบที่ผิดพลาดหรือไม่ถูกต้อง เป็นช่องโหว่ที่มีผลต่อเครื่องแม่ข่ายระบบเว็บ แพลตฟอร์มระบบงาน ฐานข้อมูล เครือข่าย หรือกรอบการทำงาน ซึ่งอาจมีการเข้าถึงโดยมิชอบ ดังนั้น จึงควรต้องมีการตรวจหาช่องโหว่อย่างสม่ำเสมอ และปิดใช้บริการที่ไม่จำเป็น

Information Security Attack Vectors

(3) การโจมตีในระดับระบบงาน (Application-Level Attacks)

การพัฒนาและทดสอบที่ไม่สมบูรณ์เพียงพอ หรืออาจมาจากขาดความตระหนักด้านความมั่นคงปลอดภัย ทำให้เกิดช่องโหว่และเป็นเป้าหมายการโจมตีระบบ ตัวอย่างได้แก่

- การโจมตีช่องโหว่ในพื้นที่หน่วยความจำชั่วคราว **(Buffer Overflow Attacks)**
- การเปิดเผยข้อมูลที่ละเอียดอ่อน **(Sensitive Information Disclosure)**
- การฝังชุดคำสั่งเพื่อขโมยข้อมูล **(Cross-site Scripting)**
- การขโมยเซสชั่นการทำงานระบบ **(Session Hijacking)**
- การโจมตีโดยการปลอมแทรกระหว่างกลาง **(Man-in-the-middle Attacks)**
- การโจมตีระบบให้บริการหยุดชะงัก **(Denial-of-service Attacks)**
- การโจมตีโดยการใช้คำสั่ง **SQL** เพื่อให้เกิดความเสี่ยหายต่อระบบฐานข้อมูล **(SQL Injection Attacks)**
- การหลอกลวงผ่านอีเมลหรือข้อความอิเล็กทรอนิกส์ **(Phishing)**
- การแทรกแซงเพื่อควบคุมพารามิเตอร์หรือเปลี่ยนข้อมูล **(Parameter / Form Tampering)**
- การโจมตีช่องโหว่ที่เข้าถึงระบบไฟล์ **(Android)(Directory Traversal Attacks)**

(4) การโจมตีผ่านชุดคำสั่งสาธารณะ (Shrink-Wrap Code Attacks)

นักพัฒนาซอฟต์แวร์มักจะใช้ชุดคำสั่ง **(Libraries and Code)** ที่ได้รับอนุญาตจากแหล่งอื่น เพื่อลดเวลาและค่าใช้จ่ายในการพัฒนา ซึ่งเป็นความเสี่ยงหากผู้ไม่ประสงค์ดีค้นพบช่องโหว่ในชุดค าสั่งนั้น ดังนั้น จึงจำเป็นต้องมีการปรับแต่งชุดคำสั่ง หรือเพิ่มค่าความมั่นคงปลอดภัย

5.13 แนวโน้มด้านความมั่นคงปลอดภัยสารสนเทศ

Trends in Security

- เทคโนโลยีใหม่ ๆ อาจยังไม่มีความมั่นคงปลอดภัยได้ทันที หรือไม่เพียงพอ
- การโจมตีข้อมูลขององค์กร และข้อมูลส่วนบุคคลในระบบคลาวด์เพิ่มขึ้น
- มัลแวร์ผ่าน **SMS** แพร่หลายมากขึ้นบนโทรศัพท์มือถือ และอุปกรณ์พกพา
- การยึดบัญชีผู้ใช้งานที่เป็นเหยื่อจากสื่อสังคมออนไลน์ หรือโปรแกรมต่าง ๆ ทำให้ผู้ไม่ประสงค์ดีสามารถเข้าถึงโทรศัพท์มือถือ หรืออุปกรณ์พกพาของเหยื่อ เพื่อเข้าถึงข้อมูลและบัญชีอื่นได้
- ผู้ไม่ประสงค์ดีใช้เทคนิคในการล่อลวงระดับผู้บริหาร ให้เปิดเผยข้อมูลมากยิ่งขึ้น เพื่อรวบรวมและเข้าถึงข้อมูลในองค์กร โดยใช้สื่อสังคมออนไลน์ เช่น **LinkedIn** หรือกระบวนการหลอกลวงทางไซเบอร์/วิศวกรรมสังคม **(Social Engineering)**
- หน่วยงานของรัฐ/หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ **(CII)** เป็นกลุ่มเป้าหมายการโจมตีจากผู้ไม่ประสงค์ดี/อาชญากรไซเบอร์ที่เพิ่มมากขึ้น
- อาชญากรไซเบอร์มุ่งเป้าหมายไปที่ลิงก์ที่อ่อนแอที่สุดในห่วงโซ่การแลกเปลี่ยนข้อมูล ได้แก่ การแบ่งปันข้อมูลกับผู้ให้บริการภายนอก ที่ปรึกษา และการแลกเปลี่ยนข้อมูลระหว่างองค์กร
- การเผยแพร่หรือแบ่งปันชุดคำสั่ง **(Source Code)** สู่สาธารณะ หรือชุดคำสั่งรั่วไหลเป็นการเร่งให้มัลแวร์เพิ่มมากขึ้นอย่างรวดเร็ว ทำให้อาชญากรไซเบอร์ศึกษาและสร้างมัลแวร์รูปแบบใหม่ ๆ ซึ่งอาจมีคุณสมบัติหลบเลี่ยงจากการตรวจพบทั่วไป
- มัลแวร์สำเร็จรูปหรือชุดคำสั่งเพื่อเจาะระบบ หาได้ง่ายมากขึ้นในอินเทอร์เน็ต ทำให้มีอาชญากรไซเบอร์หน้าใหม่หรือมือสมัครเล่นมากยิ่งขึ้น ที่จะลองทดสอบโจมตีระบบความมั่นคงปลอดภัยของเป้าหมาย
- **Exploit kits** ยังคงเป็นภัยคุกคามหลักสำหรับ **Windows XP** ซึ่ง **Microsoft** หยุดสนับสนุน ผู้ไม่ประสงค์ดีจึงสามารถกำหนดเป้าหมายได้ เนื่องจากผู้ใช้จำนวนมากอาจไม่ได้ย้ายไปยัง **Windows** เวอร์ชันล่าสุด ที่มีคุณลักษณะด้านความปลอดภัยขั้นสูง

5.14 การบริหารความเสี่ยงและมาตรการจัดการ

Information Security Risk Management

การบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศเป็นการประสานกิจกรรมเพื่อสั่งการและควบคุมองค์กรเกี่ยวกับความเสี่ยง เพื่อดำเนินการจัดการผลของความไม่แน่นอนต่อวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศ ในการรักษาความลับ ความถูกต้อง สภาพพร้อมใช้ของข้อมูล สารสนเทศ ระบบสารสนเทศ ทรัพย์สินสารสนเทศ โดยมี กรอบการบริหารความเสี่ยง **(RiskManagementFramework)** และ กระบวนการบริหารความเสี่ยง **(RiskManagementProcess)**เพื่อพิจารณาดำเนินการมาตรการควบคุมที่เหมาะสมสำหรับจัดการด้านความมั่นคงปลอดภัยสารสนเทศ ตามสภาพความเสี่ยงที่ยอมรับได้ขององค์กร

- กรอบการบริหารความเสี่ยง **(Risk Management Framework)**

กลุ่มขององค์ประกอบที่ระบุรากฐานและการจัดการองค์กรสำหรับการออบแบบ การนำไปปฏิบัติ การติดตามตรวจสอบ การทบทวน และการปรับปรุงการบริหารความเสี่ยงอย่างต่อเนื่องทั่วทั้งองค์กร

- กระบวนการบริหารความเสี่ยง **(Risk Management Process)**

การใช้นโยบายทางการบริหาร ขั้นตอนการดำเนินงาน และการปฏิบัติในกิจกรรมของการสื่อสาร การปรึกษา การจัดทำบริบท รวมถึงการชี้บ่ง การวิเคราะห์ การประเมินผล การแก้ไข การเฝ้าติดตาม และการทบทวนความเสี่ยงอย่างเป็นระบบ

The Three States of Data

การจัดการข้อมูลในองค์กรเพื่อตอบสนองตามวัตถุประสงค์และลักษณะของธุรกิจ จำแนกตามสถานะของข้อมูลเป็น 3 รูปแบบ โดยต้องมีการปกป้องข้อมูลและมาตรการควบคุม

- **Data at Rest :** ข้อมูลที่ถูกจัดเก็บอยู่ในสื่อบันทึกหรือ **Storage** ขององค์กร **(Storage Server, Files Server, Database, Backup Image, ฯลฯ)** ทั้งในส่วนกลางและเครื่องผู้ใช้งาน
- **Data in Transit :** ข้อมูลที่มีการรับส่ง โอนย้ายระหว่างอุปกรณ์หรือระบบคอมพิวเตอร์ การส่งข้อมูลจากคอมพิวเตอร์เครื่องหนึ่งไปยังอีกเครื่องหนึ่ง
- **Data in Use :** ข้อมูลที่ใช้งานอยู่ในเครื่องคอมพิวเตอร์ของผู้ใช้งาน **(Client/Endpoint)**

สรุปท้ายบท

ความมั่นคงปลอดภัยสารสนเทศเกี่ยวข้องกับการสร้างความมั่นคงปลอดภัยให้กับข้อมูล สารสนเทศ ระบบสารสนเทศ ทรัพย์สินสารสนเทศ จากการเข้าถึงโดยมิชอบ การใช้โดยมิชอบ การนำไปใช้ในทางผิด การทำลายทำให้เสียหาย หรือการเปลี่ยนแปลงแก้ไขโดยมิชอบ

คุณสมบัติสำคัญด้านความมั่นคงปลอดภัยสารสนเทศ : องค์ประกอบหลัก 3 ด้าน ได้แก่

- การรักษาความลับ **(Confidentiality)**
- ความถูกต้องครบถ้วน **(Integrity)**
- สภาพความพร้อมใช้งาน **(Availability)**

องค์ประกอบอื่น ได้แก่

- ความถูกต้องแท้จริง **(Authenticity)**
- ความรับผิดที่ตรวจสอบได้ **(Accountability)**
- การห้ามปฏิเสธความรับผิด **(Non-repudiation)**
- ความน่าเชื่อถือ **(Reliability)**

ระดับความมั่นคงปลอดภัยในระดับใด ๆ จะกำหนดขึ้นได้โดยการรักษาความสมดุลความสัมพันธ์ขององค์ประกอบ 3 ด้าน ได้แก่

- ความมั่นคงปลอดภัย **(Security)**
- ฟังก์ชั่นการทำงาน **(Functionality)**
- การใช้งาน **(Usability)**

ภัยคุกคามด้านความมั่นคงปลอดภัยสารสนเทศ จำแนกเป็น 3 กลุ่ม ได้แก่

- กลุ่มภัยคุกคามระบบเครือข่าย **(Network Threats)**
- กลุ่มภัยคุกคามระบบโฮสต์ **(Host Threats)**
- กลุ่มภัยคุกคามระบบงาน **(Application Threats)**

รูปแบบการโจมตีที่สำคัญ ๆ ด้านความมั่นคงปลอดภัยสารสนเทศและความมั่นคงปลอดภัยไซเบอร์ ได้แก่ ภัยคุกคามระดับสูง **(APT)** ภัยคุกคามต่ออุปกรณ์พกพาภัยคุกคามจากการประมวลผลแบบคลาวด์ มัลแวร์ บอตเน็ต และการโจมตีที่เกิดขึ้นจากภายในองค์กร

ภัยคุกคามทางไซเบอร์ หมายถึง การกระทำหรือการดำเนินการใด ๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์ ลักษณะของภัยคุกคามทางไซเบอร์ แบ่งออกเป็น 3 ระดับ ได้แก่

คุณสมบัติสำคัญด้านความมั่นคงปลอดภัยสารสนเทศ : องค์ประกอบหลัก 3 ด้าน ได้แก่

- ภัยคุกคามทางไซเบอร์ในระดับวิกฤติ
- ภัยคุกคามทางไซเบอร์ในระดับร้ายแรง
- ภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง

ประเภทการโจมตีระบบสารสนเทศ จำแนก 4 ระดับ ได้แก่

- ระดับระบบปฏิบัติการ **Operating System Attacks**
- ระดับค่าการติดตั้งระบบ **Mis-configuration Attacks**
- ระดับระบบงาน **Application-level Attacks**
- ระดับชุดคำสั่งระบบ Shrink-Wrap Code Attacks

แนวโน้มด้านความมั่นคงปลอดภัย (Trends in Security) ได้แก่ เทคโนโลยีใหม่ ๆ อาจยังไม่มีความมั่นคงปลอดภัยได้ทันทีหรือไม่เพียงพอ การโจมตีข้อมูลขององค์กรและข้อมูลส่วนบุคคลในระบบคลาวด์เพิ่มขึ้นการโจมตีผ่านโทรศัพท์มือถือและอุปกรณ์พกพา วิธีการหลอกลวงทางไซเบอร์ และมัลแวร์ใหม่ ๆ ที่หลบเลี่ยงการตรวจพบโดยโปรแกรมป้องกันไวรัสโดยทั่วไป