

บทที่ 1

บทนำ

1.1 หลักการและเหตุผล

ด้วยเหตุที่การซื้อขายผ่านอินเทอร์เน็ตนั้น ได้มีการเติบโตขึ้นเรื่อย ๆ พบว่าข้อมูลต่าง ๆ ที่ส่งผ่านทางเครือข่ายอินเทอร์เน็ตที่ใช้ระหว่างจับจ่ายใช้สอยในหลาย ๆ ด้าน รวมทั้งการชำระค่าบริการต่าง ๆ หรือแม้กระทั่งการฝาก ถอน โอนเงินจากบัญชีในธนาคารได้ถูกการคุกคามโดยผู้ไม่ประสงค์ดี และได้สร้างความเสียหายอย่างมากมาเช่นเหตุการณ์ดังต่อไปนี้

การแอบขโมยข้อมูลส่วนบุคคลหรือหมายเลขบัตรเครดิตจากบริษัทเพลงทางอินเทอร์เน็ต CDUniverse เมื่อเดือนธันวาคม 2542 จำนวน 300,000 รายและเอาไปเผยแพร่ในเว็บไซต์ หลังจากบริษัทปฏิเสธที่จะจ่ายค่าไถ่จำนวน 100,000 ดอลลาร์สหรัฐ¹

นอกจากนี้ยังมีการโจมตีด้วยไวรัสเลิฟบั๊กเมื่อเดือนพฤษภาคม 2543 โดยใช้เวลาเพียงไม่กี่ชั่วโมงหลังถูกนำออกเผยแพร่ได้สร้างปัญหาให้คอมพิวเตอร์หลายสิบล้านเครื่องทั่วโลกทั้งตามบ้านและหน่วยงานต่าง ๆ สร้างความเสียหายไปแล้วถึง 10,000 ล้านดอลลาร์สหรัฐ โดยเจ้าหน้าที่ในฟิลิปปินส์แจ้งว่าการสอบสวนเรื่องนี้เจออุปสรรคและไม่มีความหมายที่ครอบคลุมเรื่องระบบคอมพิวเตอร์ อีกทั้งไม่มีหลักฐานเพียงพอที่จะระบุถึงผู้กระทำผิด จึงจำเป็นต้องปล่อยตัวผู้ต้องสงสัยเป็นอิสระ²

ด้วยเหตุผลที่ว่าหากข้อมูลที่เป็นความลับหรือข้อมูลที่สำคัญมาก ๆ นั้นได้ตกไปอยู่ในมือของผู้ไม่ประสงค์ดีหรือตกไปอยู่ในมือของฝ่ายตรงกันข้ามแล้วนั้น ก็อาจก่อให้เกิดความเสียหายอย่างมหาศาลในเชิงธุรกิจหรือแม้กระทั่งความมั่นคงของชาติได้

ดังนั้นจึงมีความสนใจที่จะศึกษาเกี่ยวกับลักษณะและประเภทของภัยคุกคามต่าง ๆ ที่จะมีย อันตรายต่อข้อมูลและระบบคอมพิวเตอร์เพื่อหาแนวทางวิธีป้องกันและรักษาความปลอดภัยให้กับระบบคอมพิวเตอร์ขององค์กรได้อย่างมีประสิทธิภาพ

¹ “อาชญากรอินเทอร์เน็ต ปัญหาใหญ่ที่ต้องเร่งรับมือ”, กรุงเทพธุรกิจ. (12 พฤษภาคม 2543) : 5

² เรื่องเดียวกัน : 5

1.2 วัตถุประสงค์ของการศึกษา

เพื่อให้ทราบถึงลักษณะของภัยคุกคามของระบบพาณิชย์อิเล็กทรอนิกส์ และวิธีการรักษาความปลอดภัย

1.3 ประโยชน์ที่คาดว่าจะได้รับ

1.3.1 เพิ่มความรู้และความเข้าใจด้านพาณิชย์อิเล็กทรอนิกส์ให้มากยิ่งขึ้น

1.3.2 ทราบถึงลักษณะและประเภทของภัยคุกคามต่าง ๆ ตลอดจนระบบรักษาความปลอดภัยของพาณิชย์อิเล็กทรอนิกส์

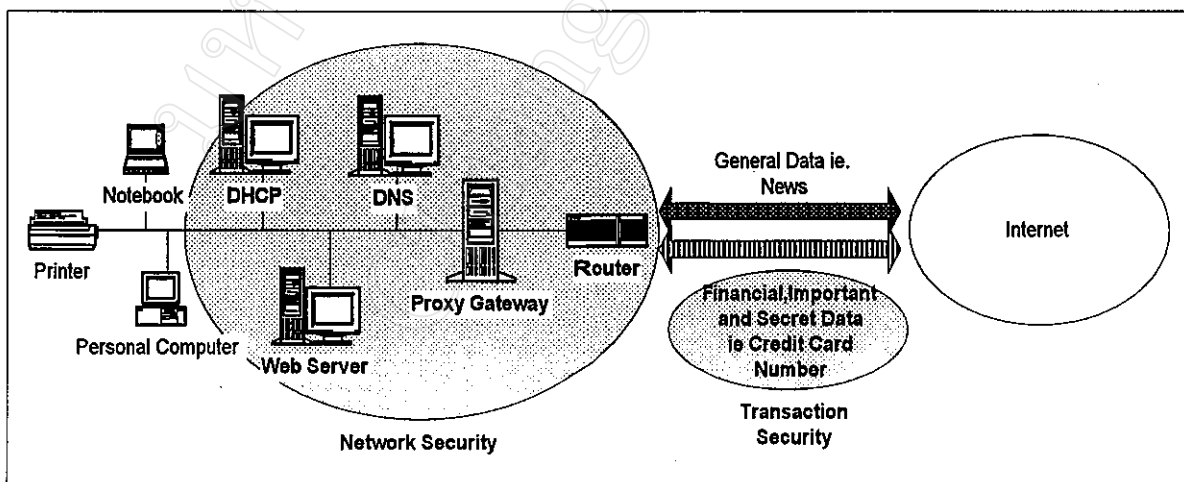
1.4 ระยะเวลาการศึกษา

ระยะเวลาการศึกษาตั้งแต่กรกฎาคม 2543 ถึงเมษายน 2546

1.5 ขอบเขตและวิธีการศึกษา

1.5.1 ขอบเขตการศึกษา

ขอบเขตของการศึกษาจะครอบคลุมถึงขบวนการต่าง ๆ ที่ใช้สำหรับการรักษาความปลอดภัยของพาณิชย์อิเล็กทรอนิกส์ โดยแบ่งเป็นการรักษาความปลอดภัยของเครือข่าย (Network Security) และการรักษาความปลอดภัยของการทำธุรกรรม(Transaction Security)



ความปลอดภัยของเครือข่าย (Network Security) ประกอบด้วยอุปกรณ์ต่าง ๆ ดังนี้
คือ

- (1) Web Server
- (2) Router
- (3) Domain Name Service(DNS)
- (4) Dynamic Host Configuration Protocol(DHCP)
- (5) Proxy Gateway

การรักษาความปลอดภัยของการทำธุรกรรม(Transaction Security) จะครอบคลุมถึงข้อมูลที่สำคัญที่มีการเข้ารหัสและส่งผ่านทางอินเทอร์เน็ต เช่น ข้อมูลบัตรเครดิต ข้อมูลด้านการเงิน โดยศึกษาถึงวิธีการเข้ารหัสข้อมูลและมาตรฐานต่าง ๆ สำหรับพาณิชย์อิเล็กทรอนิกส์ที่มีอยู่ในปัจจุบัน ข้อดีข้อเสียของวิธีการแต่ละประเภท และแนวโน้มในอนาคตว่ามีทิศทางเป็นเช่นไร

1.5.2 วิธีการศึกษา

ศึกษาค้นคว้าข้อมูลส่วนใหญ่จากแหล่งข้อมูลทุติยภูมิ เช่น หนังสือ วรรณกรรม บทความ ความพึงในประเทศและต่างประเทศและข้อมูลอินเทอร์เน็ต โดยจะทำการวิเคราะห์และสรุปเอาประเด็นที่สำคัญมาจัดทำเป็นรายงานตามขอบเขตการศึกษา พร้อมทั้งการประยุกต์ใช้

1.6 แนวคิดที่ใช้ในการศึกษา

การศึกษานี้ใช้แนวคิดเกี่ยวกับการรักษาความปลอดภัยของระบบคอมพิวเตอร์และระบบการติดต่อสื่อสาร โดยภัยคุกคามอาจเกิดขึ้นจากสิ่งต่อไปนี้

- 1.6.1 อาชญากรทางคอมพิวเตอร์
- 1.6.2 ไวรัสคอมพิวเตอร์
- 1.6.3 ข้อผิดพลาดและอุบัติเหตุ
- 1.6.4 ภัยธรรมชาติ

วิธีการที่ระบบข้อมูลหรือระบบคอมพิวเตอร์อาจถูกทำให้เสียหายจากบุคคลหรือกลุ่มบุคคล
โดย

- (1) ผู้ไม่ประสงค์ดีทำการคุกคามต่อระบบคอมพิวเตอร์ เช่น ขโมยเครื่อง โปรแกรม ข้อมูล รวมทั้งการทำลายข้อมูล
- (2) คอมพิวเตอร์อาจจะถูกใช้เป็นเครื่องมือของผู้ไม่ประสงค์ดี โดยอาจเป็นพนักงาน ผู้ใช้ระบบจากภายนอก หรือนักเจาะระบบมีอาชีพ

(3) คอมพิวเตอร์อาจถูกคุกคามโดยไวรัสคอมพิวเตอร์ เป็นต้น
 ดังนั้นการป้องกันระบบข้อมูลและระบบคอมพิวเตอร์ให้มีความปลอดภัยจากภัยคุกคาม
 สามารถดำเนินการได้โดย

- (1) การระบุถึงสิทธิ์ของผู้ที่จะใช้งาน
- (2) การเข้ารหัสข้อมูล
- (3) การป้องกันซอฟต์แวร์และข้อมูลโดยใช้ Firewall เป็นต้น
- (4) การวางแผนการกู้ข้อมูลคืนเมื่อจำเป็น

1.7 นิยามคำศัพท์

- 1.7.1 ความปลอดภัย หมายถึงการรักษาความปลอดภัยทางด้านกายภาพ ซึ่งได้แก่ทรัพย์สิน หรืออุปกรณ์ต่าง ๆ ในเครือข่าย และความปลอดภัยของข้อมูลซึ่งจะพิจารณาจากความถูกต้องของข้อมูลที่อยู่ภายในระบบเครือข่าย และข้อมูลที่ส่งออกไปนอกเครือข่าย รวมทั้งต้องรักษาข้อมูลเหล่านั้นให้เป็นความลับ
- 1.7.2 พาณิชย์อิเล็กทรอนิกส์(E-Commerce) หมายถึงการทำธุรกรรมทุกรูปแบบไม่ว่าจะผ่านทางเครือข่าย โทรศัพท์ โทรสาร หรือสื่ออื่น ๆ ที่เกี่ยวข้องกับกิจกรรมเชิงพาณิชย์ ทั้งในระดับองค์กรและส่วนบุคคล บนพื้นฐานของการประมวลผล และการส่งข้อมูลดิจิทัลที่มีทั้งข้อความ เสียงและภาพ³

³ Ahmed Sehrouchni, *Protocols for Secure Electronic Commerce*. New York, 2nd edition : Prentice-Hall, 1998 : 5