วิชา พื้นฐานทางธุรกิจดิจิทัล (30204 -2001)

หน่วยที่ 7 ความมั่นคงปลอดภัยในการทำธุรกรรมดิจิทัล

Asst. Prof. Juthawut Chantharamalee

Assistant Professor in Computer Science

(Chairperson of B.Sc. Program in Computer Science)

Office. Suan Dusit University, Phone. (+66) 2244-5691

Email. juthawut_cha@dusit.ac.th, jchantharamalee@gmail.com

หน่วยที่ 7 ความมั่นคงปลอดภัยในการทำธุรกรรมดิจิทัล

1. ความหมายของความมั่นคงปลอดภัยทางไซเบอร์
2. ระบบ Cyber Security
3. ความมั่นคงปลอดภัยในการำธุรกรรมดิจิทัล
4. การรักษาความมั่นคงปลอดภัยโครงสร้างพื้นฐาน

หน่วยที่ 7 ความมั่นคงปลอดภัยในการทำธุรกรรมดิจิทัล

5. หลักการรักษาความมั่นคงปลอดภัยในการทำธุรกรรมดิจิทัล
6. ภัยคุกคามด้านความมั่นคงปลอดภัย
7. เทคโนโลยีที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยในการทำธุรกรรมดิจิทัล
8. ข้อควรระวังในการทำธุรกรรมดิจิทัล

จุดประสงค์การเรียนรู้

1. ขอกความหมายของความมั่นคงปลอดภัยทางไซเบอร์ได้
2. อธิบายระบบ Cyber Security ได้
3. อธิบายหลักการรักษาความมั่นคงปลอดภัยในการทำธุรกรรมดิจิทัลได้
4. ประยุกต์การใช้เทคโนโลยีที่เกี่ยวข้องในการรักษาความมั่นคงปลอดภัยในการทำธุรกรรมดิจิทัลได้
5. มีเจตคติและกิจนิสัยที่ดีในการปฏิบัติงานด้วยความรับผิดชอบ ซื่อสัตย์ ละเอียดรอบคอบ

สมรรถนะประจำหน่วย

1. แสดงความรู้เกี่ยวกับความหมายของความมั่นคงปลอดภัยทางไซเบอร์
2. แสดงความรู้เกี่ยวกับความมั่นคงปลอดภัยธุรกิจดิจิทัล
3. แสดงความรู้เกี่ยวกับหลักการรักษาความมั่นคงปลอดภัยในการทำธุรกรรมดิจิทัล
4. แสดงความรู้เกี่ยวกับภัยคุกคามด้านความปลอดภัย
5. ปฏิบัติการใช้เทคโนโลยีที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยในการทำธุรกรรมดิจิทัล

ความนำ

การดำเนินธุรกิจทุกประเภทย่อมมีความเสี่ยง ในการถูกลักลอบขโมยข้อมูลหรือการลอกเลียนแบบ โดยเฉพาะอย่างยิ่ง ในปัจจุบันมีการดำเนินการทำธุรกรรมดิจิทัลในโลกออนไลน์มากขึ้น ก็จะเกิดความเสี่ยงในเรื่องความปลอดภัยในการทำธุรกรรมดิจิทัลมากยิ่งขึ้น จึงต้องมีความจำเป็นในการจัดระบบการควบคุมและป้องกันความเสี่ยงหรือความปลอดภัย

ความหมายของความมั่นคงปลอดภัยทางไซเบอร์

ในโลกยุคปัจจุบัน ปัจจุบันผู้ใช้งานสามารถเข้าถึงและใช้บริการด้านข้อมูลผ่านระบบเทคโนโลยีสารสนเทศได้อย่างสะดวก รวดเร็ว ไม่จำกัดเวลาและสถานที่ ในขณะเดียวกัน ข้อมูลขนาดใหญ่ของผู้ใช้งานที่อยู่ในระบบมีความเสี่ยงต่อการถูกโจมตี ขโมย หรือถูกทำลายได้ เช่น การขโมยข้อมูลธุรกรรมทางการเงิน การสร้างไวรัสโจมตีระบบปฏิบัติการ เป็นต้น หากไม่มีระบบการรักษาความมั่นคงปลอดภัยที่ดีเพียงพอ ซึ่งภัยคุกคามทางไซเบอร์เหล่านี้สามารถสร้างความเสียหายแก่ตัวผู้ใช้งานได้ แนวคิดเรื่องการรักษาความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) จึงต้องถูกพัฒนาไปพร้อมกับความก้าวหน้าของระบบเทคโนโลยี

ระบบ CYBER SECURITY

ระบบ Cyber Security จำเป็นต่อทุกอุตสาหกรรม แต่เนื่องด้วยความจำเป็นเร่งด่วนและผลกระทบที่รุนแรง ได้ถูกนำมาใช้อย่างมากในอุตสาหกรรมการเงินและการธนาคาร เนื่องจากในโลกยุคปัจจุบัน ในหลาย ๆ ประเทศมีการเปิดเสรีทางการเงินการธนาคารเพื่อดึงดูดนักลงทุนต่างชาติให้เข้ามาลงทุนในอุตสาหกรรมทางการเงิน รวมถึงการซื้อขายแลกเปลี่ยน และการทำธุรกรรมทางการเงินสามารถทำได้ผ่านระบบอินเทอร์เน็ตที่ใช้งานบนสมาร์ทโฟน สถาบันการเงินจึงเห็นความจำเป็นในการพัฒนาระบบการทำธุรกรรมทางการเงินควบคู่ไปกับระบบรักษาความมั่นคงปลอดภัยเพื่อให้ผู้ใช้งานเกิดความมั่นใจ อันจะส่งผลให้ e-commerce และ e-banking เติบโตในภาพรวม

ความมั่นคงปลอดภัยในการทำธุรกรรมดิจิทัล (DIGITAL SECURITY)

Digital Security ระบบความปลอดภัยในการทำธุรกรรมดิจิทัล เป็นทักษะหนึ่งที่ต้องตระหนัก รู้วิธีป้องกันและหลีกเลี่ยง เพราะในโลกธุรกิจดิจิทัลแฝงไปด้วยภัยอันตรายต่าง ๆ มากมาย ที่อาจจะทำให้องค์กรหรือธุรกิจได้รับความเสียหายได้ ไม่ว่าจะเป็นการถูกแฮกบัญชี การถูกโจรกรรมข้อมูลสำคัญ ๆ การถูกขโมยรหัสผ่าน การถูกละเมิดทรัพย์สินทางปัญญา การถูกโจรกรรมทรัพย์สิน หรือการติดไวรัส และการโจมตีเฟิร์มแวร์ ซึ่งล้วนแต่เป็นภัยร้ายต่อองค์กรหรือธุรกิจแทบทั้งสิ้น

ปัจจัยที่สำคัญของ DIGITAL SECURITY

1. บุคลากร (Personal) องค์กรจะต้องมีบุคลากรที่มีประสบการณ์และมีความเชี่ยวชาญ มีความสามารถในด้านความปลอดภัยสูงโดยต้องอยู่ภายใต้การรับรองของหน่วยงานสากลหรือ Certificate

2. เครื่องมือ (Tool) การเลือกใช้อุปกรณ์ดิจิทัลและซอฟต์แวร์ที่ทันสมัยได้รับการยอมรับแล้วว่าสามารถป้องกันและมีความแม่นยำในการวิเคราะห์ภัยคุกคาม สามารถป้องกันการโจมตีเฟิร์มแวร์ ซึ่งเป็นภัยใหญ่ที่สุดในองค์กรได้อย่างมีประสิทธิภาพ

การรักษาความมั่นคงปลอดภัยโครงสร้างพื้นฐาน

1. ฮาร์ดแวร์และอุปกรณ์เชื่อมต่อต่าง ๆ (Hardware and its peripheral)
2. ซอฟต์แวร์ (Software)
3. โครงสร้างพื้นฐานระบบเครือข่าย (Network)
4. ขั้นตอนระเบียบปฏิบัติ (Procedure)
5. ผู้ใช้งาน (User)

หลักการรักษาความมั่นคงปลอดภัยในการทำธุรกรรมดิจิทัล

1. การรักษาความลับ (Confidentiality)
2. การรักษาความครบถ้วนสมบูรณ์ (Integrity)
3. การรักษาความพร้อมใช้ (Availability)

การรักษาความปลอดภัยของข้อมูลในการทำธุรกิจดิจิทัล

1. การระบุตัวตน (Identification)
2. การพิสูจน์ทราบตัวตน (Authentication)
3. การอนุญาตใช้งาน (Authorization)
4. การตรวจสอบได้ (Accountability)

ภัยคุกคามด้านความมั่นคงปลอดภัย

ภัยคุกคาม (Threat) หมายถึง สิ่งที่ทำให้เกิดความเสียหายของข้อมูล ไม่ว่าจะเป็นส่วนใดส่วนหนึ่งของข้อมูล เมื่อข้อมูลนั้นการคุกคามโดยภัยคุกคามนี้ถ้าไม่ได้มีการป้องกันที่รัดกุมแล้วนั้นก็จะเป็นสาเหตุที่จะทำให้ข้อมูลนั้นเกิดการเสียหายได้ โดยการโจมตีของกลุ่มที่ไม่หวังดีเช่น จากบุคคลภายในองค์กรเอง หรือกลุ่มเจาะระบบ (Hacker) แต่อย่างไรก็ดี ถ้ามีการจัดการที่ดีต่อข้อมูลทำให้ข้อมูลนั้นปลอดภัยรัดกุมอยู่เสมอ ภัยต่าง ๆ ก็ไม่สามารถที่จะทำให้ข้อมูลเสียหายได้

ภัยคุกคามต่อทรัพยากรสารสนเทศจำแนกได้ 4 ลักษณะ คือ

1. การดักรับ (Interception)
2. การขัดจังหวะ (Interruption)
3. การดัดแปลงแก้ไข (Modification)
4. การปลอมแปลง (Fabrication)

ไฟร์วอลล์ (FIREWALL)

ไฟร์วอลล์ (Firewall) เป็นเทคโนโลยีที่ถูกสร้างขึ้นเพื่อป้องกันภัยคุกคามและการโจมตีทางเครือข่าย หลักทั่วไปของการใช้งานไฟร์วอลล์คือ การป้องกันภัยคุกคามที่มาจากภายนอก (ซึ่งอาจหมายถึงเครือข่ายภายนอก หรือเครือข่ายที่เครื่องคอมพิวเตอร์ส่วนบุคคลเครื่องหนึ่งเชื่อมต่อด้วยก็ได้)

จำแนกชนิดของไฟร์วอลล์ตามลักษณะการใช้งานได้สองลักษณะ คือ

1. ไฟร์วอลล์สำหรับเครือข่าย (Network Firewall)
2. ไฟล์วอลล์ส่วนบุคคล (Personal Firewall)

ข้อควรระวังในการทำธุรกรรมดิจิทัล

1. ความมั่นคงปลอดภัยออนไลน์ (Online Security)
2. ความน่าเชื่อถือของระบบ (System Reliability)
3. ประเด็นเรื่องความเป็นส่วนตัว
4. ข้อพิพาทหรือร้องเรียนของลูกค้า
5. การฉ้อโกงบัตรเครดิต

ข้อควรระวังในการทำธุรกรรมดิจิทัล

6. ทรัพย์สินทางปัญญา รูปภาพ คำอธิบายผลิตภัณฑ์ต่าง
7. SEO (Search Engine Optimization)
8. ภาษีอากร
9. การคืนสินค้าและการรับประกัน
10 ระบบคลังสินค้าและโลจิสติกส์

สรุปประเด็นสำคัญ

ระบบ Cyber Security จำเป็นต่อทุกอุตสาหกรรม แต่เนื่องด้วยความจำเป็นเร่งด่วนและผลกระทบที่รุนแรง ได้ถูกนำมาใช้อย่างมากในอุตสาหกรรมการเงินและการธนาคาร เนื่องจากในโลกยุคปัจจุบัน ในหลาย ประเทศมีการเปิดเสรีทางการเงินการธนาคารเพื่อดึงดูดนักลงทุนต่างชาติให้เข้ามาลงทุนในอุตสาหกรรมทางการเงิน รวมถึงการซื้อขายแลกเปลี่ยน และการทำธุรกรรมทางการเงินสามารถทำได้ผ่านระบบอินเทอร์เน็ตที่ใช้งานบนสมาร์ทโฟน

สรุปประเด็นสำคัญ

เทคโนโลยีที่เกี่ยวกับข้องกับการรักษาความมั่นคงปลอดภัยในการทำธุรกรรมดิจิทัล ได้แก่ เทคโนโลยีที่เกี่ยวข้องกับการรักษาความปลอดภัยทางกายภาพ วิทยาการรหัสลับ (Cryptography) ไฟร์วอลล์ (Firewall) เป็นเทคโนโลยีที่ถูกสร้างขึ้นเพื่อป้องกันภัยคุกคามและการโจมตีทางเครือข่าย หลักทั่วไปของการใช้งานไฟร์วอลล์ระบบตรวจจับผู้บุกรุก (Intrusion Detection System) และแอนตี้ไวรัสซอฟต์แวร์ (Anti-Virus Software)