การจัดการความปลอดภัยภายในองค์กร

สมหมาย แม้นมณี[1]

การทำงานภายในองค์กรย่อมเกี่ยวข้องกับข้อมูลข่าวสาร ซึ่งต้องทำงานผ่านระบบเครือข่าย และมีซอฟต์แวร์ไว้ใช้งาน ดังนั้นข้อมูลในองค์กรจึงมีความสำคัญ ข้อมูล (Data) เป็นข้อเท็จจริงที่เกิดขึ้น เมื่อนำมาผ่านกระบวนการอย่างใดอย่างหนึ่งแล้วทำให้ได้สารสนเทศ (Information) ที่เป็นประโยชน์ ความปลอดภัยภายในองค์กรเพื่อรักษาข้อมูลข่าวสารที่สำคัญและเป็นประโยชน์ขององค์กรจึงเป็นเรื่องที่ต้องคำนึงถึงเป็นอย่างมาก

รูปที่ 1. การทำงานภายในองค์กร

ที่มา : http://courseware.payap.ac.th/docu/sc312/slide/lesson3.ppt

การควบคุมความปลอดภัยของข้อมูลสารสนเทศ (Information Security) มีองค์ประกอบดังนี้

1. การกำหนดนโยบายในองค์กร (Policies)

ผู้บริหารองค์กรควรมีการกำหนดนโยบายเพื่อรักษาความปลอดภัยภายในองค์กรของตนเอง จะออกเป็นกฎหรือระเบียบปฏิบัติอะไรก็ได้ เพื่อให้ผู้ปฏิบัติงานได้ระมัดระวังและกระทำไปในทิศทางเดียวกัน นโยบายควรแบ่งออกเป็นด้านต่างๆดังนี้

1.1.นโยบายในการจัดการข้อมูลข่าวสาร (Information Policy)

1.2.นโยบายในการรักษาความปลอดภัยในระบบเครือข่าย (Network Policy)

1.3.นโยบายการใช้งานบนระบบเครือข่าย (Usage Policy)

[1]สาขาวิชาวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยราชภัฏพิบูลสงคราม พิษณุโลก 65000

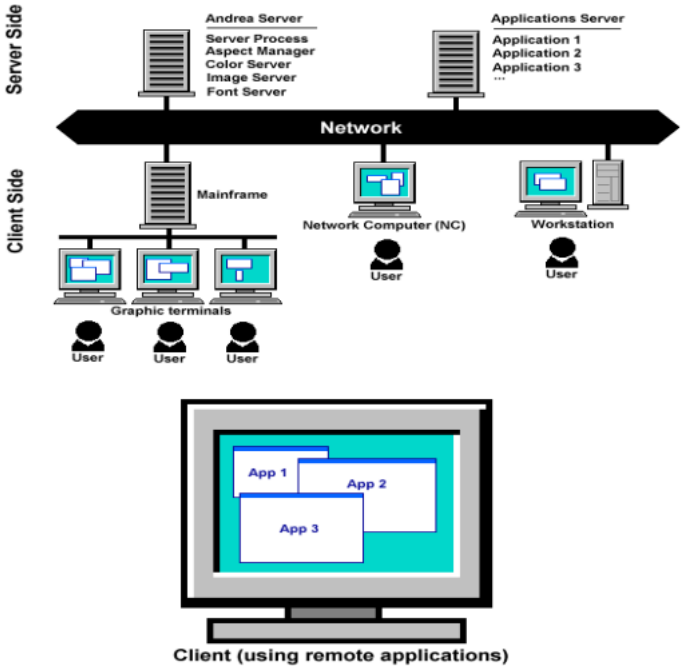
รูปที่ 2. ความเกี่ยวข้องกันของนโยบายในด้านต่างๆ

2. การควบคุมความปลอดภัยของระบบโดยฮาร์ดแวร์ (Hardware Control)

ภายในองค์กรจะต้องมีระบบเครือข่ายที่ใช้อุปกรณ์ที่ได้มาตรฐานมีคุณภาพเพียงพอ เพื่อก่อให้เกิดเสถียรภาพและความปลอดภัย การลงทุนในด้านเครื่องมือจะมากหรือน้อยขึ้นอยู่กับขนาดขององค์กรและขึ้นอยู่กับระดับความปลอดภัยที่เลือกใช้เช่นกัน

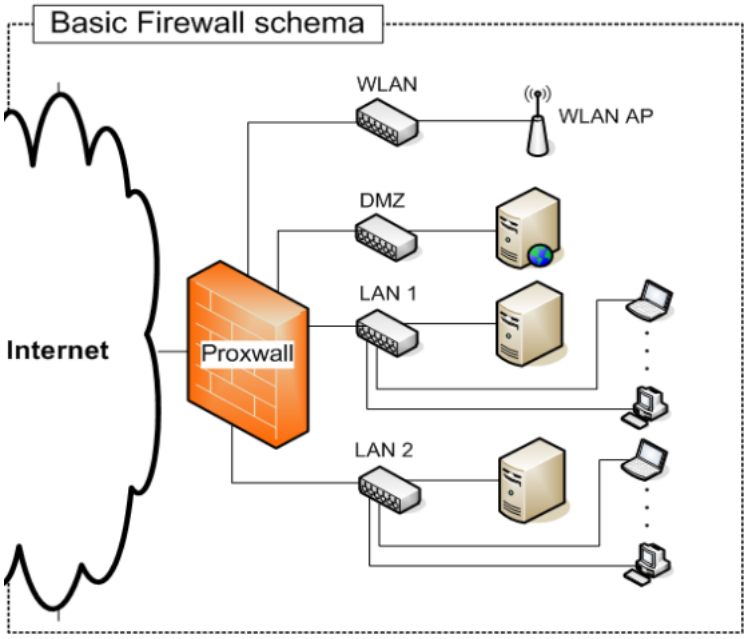
รูปที่ 3. ตัวอย่างเครื่องคอมพิวเตอร์ที่มีระบบความปลอดภัย

ที่มา : http://www.cyfence.com/it-security/services/smart_log.html



รูปที่ 4. ตัวอย่างการวางระบบเครือข่ายในองค์กร

ที่มา : http://courseware.payap.ac.th/docu/sc312/lesson4/lesson04.html



รูปที่ 5. การป้องกันระบบเครือข่ายในองค์กรด้วยอุปกรณ์

ที่มา : http://courseware.payap.ac.th/docu/sc312/lesson4/lesson04.html

3. การควบคุมรักษาความปลอดภัยโดยตัวซอฟต์แวร์ (Software Control)

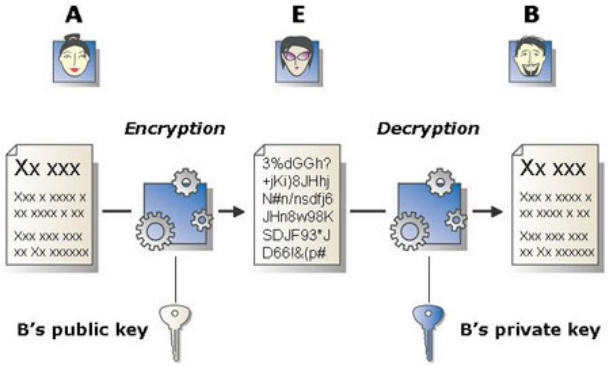
การรักษาความปลอดภัยด้วยซอฟต์แวร์สามารถแบ่งได้เป็น 3 แบบดังนี้

3.1. การควบคุมความปลอดภัยโดยระบบปฏิบัติการ (Operating System Control) ควรเลือกใช้ระบบปฏิบัติการที่มีระบบความปลอดภัย ระบบปฏิบัติการที่ใช้กันโดยทั่วไปเช่น Windows, UNIX, LINUX ฯลฯ

3.2. การควบคุมความปลอดภัยด้วยซอฟต์แวร์(Internal Program Control) ปัจจุบันในองค์กรต่าง ๆ ต้องปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ซึ่งจะต้องจัดเก็บรายการทำงานของผู้ใช้งานตลอดเวลา เพื่อจะได้ติดตามและตรวจสอบได้ในภายหลัง

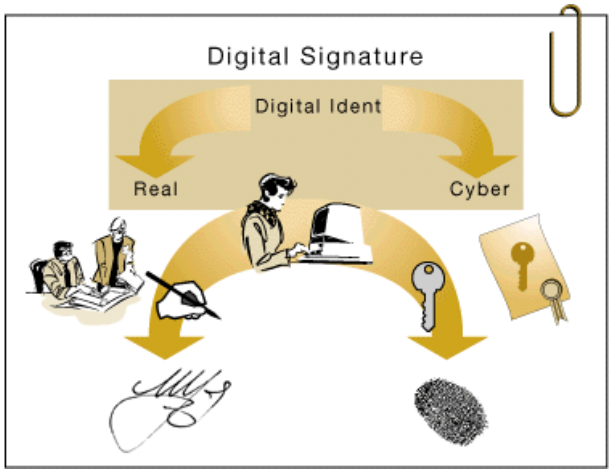
รูปที่ 6. ตัวอย่างโปรแกรมที่มีการจัดเก็บรายการใช้งานของผู้ใช้งาน

ที่มา : http://www.cyfence.com/it-security/services/secure_log_management.html



รูปที่ 7. การเข้ารหัส/ถอดรหัสข้อมูลด้วยกุญแจส่วนตัวและกุญแจสาธารณะในระบบเครือข่าย

ที่มา : http://courseware.payap.ac.th/docu/sc312/lesson4/lesson04.html



รูปที่ 8. การเข้ารหัส/ถอดรหัสข้อมูลด้วยเทคนิคลายเซ็นต์อิเล็กทรอนิกส์

ที่มา : http://courseware.payap.ac.th/docu/sc312/lesson4/lesson04.html

4. การป้องกันทางกายภาพ (Physical Control)

เป็นการระวังป้องกันในสถานที่ต่างๆ ด้วยการเฝ้าดูพฤติกรรมของบุคลากรในองค์กร อาจจะมีการจ้างพนักงานรักษาความปลอดภัย หรือติดตั้งกล้องวงจรปิดไว้ตามสถานที่ต่างๆ อาจจะพัฒนาและออกแบบให้ระบบมีการเชื่อมต่อกับระบบกล้องวงจรปิด **Closed-Circuit Television (CCTV)** โดยผ่านเครือข่ายอินเทอร์เน็ต ทำให้สามารถติดตามตรวจสอบได้ทุกที่ทุกเวลา

สรุป การรักษาความปลอดภัยในองค์กรจึงเป็นเรื่องที่สำคัญมากในยุคปัจจุบัน ประกอบกับรัฐบาลได้ออกพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ทำให้ทุกองค์กรต้องปฏิบัติตาม ดังนั้นจึงเป็นหน้าที่ของผู้รับผิดชอบในแต่ละองค์กร ที่จะต้องเริ่มกำหนดนโยบายความปลอดภัยภายในองค์กร และลงมือกระทำตามนโยบายกำหนดไว้ เพื่อความมั่นคงปลอดภัยขององค์กรต่อไป