บทที่ 1

บทนำ

1.1 ความสำคัญและความเป็นมาของปัญหา

ในปัจจุบันนี้เป็นยุคของการสื่อสารข้อมูลผ่านทางเครือข่ายอินเตอร์เน็ต (Internet) เนื่องจากระบบอินเตอร์เน็ตเป็นระบบเครือข่ายขนาดใหญ่ที่เชื่อมต่อถึงกันทั่วโลก โดยมีมาตรฐานในการรับส่งข้อมูลที่ชัดเจนเป็นหนึ่งเดียว ทำให้การเชื่อมต่อคอมพิวเตอร์ต่างชนิดต่างแบบกันเป็นไปได้อย่างง่ายดาย ไม่ว่าจะเป็นเมนเฟรมคอมพิวเตอร์ มินิคอมพิวเตอร์ คอมพิวเตอร์ส่วนบุคคลชนิดต่าง ๆ สามารถต่อเชื่อมถึงกันได้ทำให้คอมพิวเตอร์แต่ละเครื่องสามารถรับส่งข้อมูลในรูปแบบต่าง ๆ เช่น ตัวอักษร ภาพและเสียง สามารถค้นหาข้อมูลจากที่ต่าง ๆ ได้อย่างรวดเร็วสามารถรับรู้ข่าวสารข้อมูลทันสมัยได้ตลอดเวลาและสามารถใช้บริการต่าง ๆ เช่น การรับส่งไปรษณีย์อิเล็กทรอนิคส์ (E-mail) การสืบค้นข้อมูลในเวิลด์ไวด์เว็บ (World Wide Web) หรือโกเฟอร์ (Gopher) การโอนย้ายข้อมูล (File Transfer) การเทลเน็ต (Telnet) ฯลฯ จากความนิยมที่แพร่หลายของการใช้งานระบบเครือขายอินเตอร์เน็ตในด้านต่าง ๆ มีผลทำให้มีเกิดความเสี่ยงในด้านการจัดการระบบการรักษาความปลอดภัยของข้อมูล โดยเฉพาะกับองค์กรที่มีการต่อเชื่อมระบบเครือข่ายท้องถิ่นเข้ากับระบบเครือข่ายอินเตอร์เน็ต

ระบบรักษาความปลอดภัยของข้อมูลสำหรับองค์กรที่ได้มีการต่อเชื่อมระบบเครือข่ายท้องถิ่นเข้ากับระบบเครือข่ายอินเตอร์เน็ตสามารถแบ่งออกได้เป็น 2 ชนิดคือ การรักษาความปลอดภัยทางกายภาพและการรักษาความปลอดภัยทางระบบเครือข่ายคอมพิวเตอร์

การรักษาความปลอดภัยทางกายภาพ เป็นการป้องกันที่สามารถสังเกตได้ด้วยตาเปล่าจากพฤติกรรมของผู้บุกรุกเพื่อป้องกันไม่ให้สามารถเข้าใช้อุปกรณ์ทางเครือข่ายได้ เช่น การมีประตูหรือกำแพงไว้ป้องกันบุคคลภายนอกที่ไม่เกี่ยวข้องไม่ให้เข้ามาใช้งาน การวางอุปกรณ์ทางเครือข่ายไว้ในที่ปลอดภัย ฯลฯ

การรักษาความปลอดภัยทางระบบเครือข่ายคอมพิวเตอร์ เป็นการป้องกันที่ไม่สามารถสังเกตได้ด้วยตาเปล่าจากพฤติกรรมของผู้บุกรุก ซึ่งพฤติกรรมในการบุกรุกส่วนใหญ่จะมาในรูปของการ เทลเน็ต หรือเป็นการบุกรุกระบบเครือข่ายท้องถิ่นโดยที่เราไม่สามารถที่จะล่วงรู้ได้ว่าผู้บุกรุกนั้นเป็นใคร อย่างไรก็ตามการติดตั้งอุปกรณ์ทางระบบเครือข่ายที่เรียกว่า "เร้าเตอร์" (Router) และ "ไฟร์วอลล์" (Firewall) เป็นตัวกลั่นกรองผู้ที่ต้องการติดต่อกับระบบเครือข่ายท้องถิ่นเพื่อป้องกันการบุกรุกการเข้าสู่ระบบเครือข่ายได้

ในทางปฏิบัติ ผู้ที่มีหน้าที่ในการดูแลระบบรักษาความปลอดภัยบนเครือข่ายอินเตอร์เน็ตสำหรับองค์กร คือ ผู้ควบคุมระบบเครือข่าย (Network Administrator) โดยที่ผู้ควบคุมระบบเครือข่ายจะคำนึงถึงระบบการรักษาความปลอดภัยเมื่อมีการต่อเชื่อมระบบเครือข่ายท้องถิ่นเข้าเครือข่ายอินเตอร์เน็ต โดยจะวาง

แผนและประชุมกับผู้ที่เกี่ยวข้อง เพื่อกำหนดแบบแผนในการป้องกันและระดับในการป้องกัน บุคคลภายนอก เพื่อไม่ให้สามารถเข้าใช้ข้อมูลได้

1.2 วัตถุประสงค์ของการวิจัย

เพื่อวัดประสิทธิภาพของเครื่องมือที่ใช้ในระบบรักษาความปลอดภัยบนเครือข่ายอินเตอร์เน็ต ซึ่งจะไปใช้ในการตัดสินใจในการออกแบบระบบรักษาความปลอดภัยบนเครือข่ายอินเตอร์เน็ตที่สมบูรณ์ของจุฬาลงกรณ์มหาวิทยาลัย

1.3 ขอบเขตของการวิจัย

ขอบเขตของการวิจัยแบ่งได้ดังต่อไปนี้

1.3.1 ทดสอบประสิทธิภาพของอุปกรณ์ไฟร์วอลล์ โดยใช้ พีไอเอ็กซ์ไฟร์วอลล์ (PIX Firewall) รุ่น 4.0 ของบริษัท ซิสโกซิสเต็ม จำกัด (Cisco System Inc.) และ เร้าเตอร์ รุ่น 2514 เป็นกรณีศึกษา

1.3.2 การทำงานของ โปรแกรมประยุกต์ (Application Program) ที่ใช้ในการทดสอบจะทำงานบนระบบยูนิกซ์ ซึ่งใช้ระบบยูนิกซ์บนลินุกส์ (Linux) เป็นกรณีศึกษา

1.3.3 กรณีศึกษาที่ใช้ทดสอบนี้ จะศึกษาเฉพาะประสิทธิภาพในการทำงานของอุปกรณ์ไฟร์วอลล์เท่านั้นมิได้รวมถึงกรณีของการรักษาความปลอดภัยบนเครือข่ายอินเตอร์เน็ต

1.4 ขั้นตอนและวิธีดำเนินการวิจัย

1.4.1 ศึกษาการทำงานของ

- 1.4.1.1 เลเยอร์ทั้ง 7 ของไอเอสโอ และ โพรโทคอล ทีซีพี/ไอพี
- 1.4.1.2 พีไอเอ็กซ์ไฟร์วอลล์
- 1.4.1.3 เร้าเตอร์

1.4.2 ออกแบบและกำหนดโครงแบบ

- 1.4.2.1 พีไอเอ็กซ์ไฟร์วอลล์
- 1.4.2.1 เร้าเตอร์

1.4.3 จัดหาอุปกรณ์ที่เกี่ยวข้องและติดต่อหน่วยงานที่เกี่ยวข้อง

- 1.4.3.1 ติดต่อบริษัท ซิสโกซิสเต็ม (ประเทศไทย) จำกัด เพื่อจัดเตรียมอุปกรณ์ พีไอเอ็กซ์ไฟร์วอลล์
- 1.4.3.2 ติดต่อบริษัท เดอะคอมมิวนิเคชั่นโซลูชั่น จำกัด เพื่อจัดเตรียมอุปกรณ์เร้าเตอร์

1.4.4 เขียนโปรแกรมเพื่อใช้สำหรับทดสอบโดยแบ่งการทดสอบเป็น 3 วิธีการ ได้แก่

1.4.4.1 วิธีการที่ 1 ระบบที่ไม่มีอุปกรณ์ไฟร์วอลล์

1.4.4.2 วิธีการที่ 2 ระบบที่มีพีไอเอ็กซ์ไฟร์วอลล์

1.4.4.3 วิธีการที่ 3 ระบบที่มีเร้าเตอร์

1.4.5 ทดสอบระบบงาน

1.4.6 วิเคราะห์ผลที่ได้ทางสถิติจากการทดสอบ

1.4.7 สรุปผลจากการวิจัยและเรียบเรียงวิทยานิพนธ์

1.5 ประโยชน์ที่คาดว่าจะได้รับจากการวิจัย

1.5.1 เพื่อเป็นแนวทางในการกำหนดนโยบาย รักษาความปลอดภัยบนเครือข่ายอินเตอร์เน็ตของจุฬาลงกรณ์มหาวิทยาลัย

1.5.2 เพื่อเป็นแนวทางในการเลือกอุปกรณ์ สำหรับการออกแบบระบบรักษาความปลอดภัยเครือข่ายอินเตอร์เน็ตของจุฬาลงกรณ์มหาวิทยาลัย

1.5.3 เพื่อเป็นกรณีศึกษาระบบรักษาความปลอดภัยบนเครือข่ายอินเตอร์เน็ตสำหรับมหาวิทยาลัยอื่น ที่มีลักษณะและองค์ประกอบทางกายภาพที่คล้ายคลึงกับจุฬาลงกรณ์มหาวิทยาลัย