ความปลอดภัยทางสารสนเทศและโมเดลในการประกอบธุรกิจของผู้ให้บริการอินเตอร์เน็ต

Security Schemes and Business Models for Internet Service Provider

โดย

วราพร พงศ์สุวากร

รหัส 45061746

อาจารย์ที่ปรึกษา

จันทร์บูรณ์ สถิตวิริยวงศ์

รายงานนี้เป็นส่วนหนึ่งของวิชาโครงการศึกษากรณีพิเศษ
หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
ภาคเรียนที่ 1 ปีการศึกษา 2547
คณะเทคโนโลยีสารสนเทศ
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ชื่อหัวข้อ	ความปลอดภัยทางสารสนเทศและโมเดลในการประกอบธุรกิจของผู้ให้บริการอินเตอร์เน็ต
นักศึกษา	นางสาววราพร พงศ์สุวากร
อาจารย์ที่ปรึกษา	ผศ.ดร .จันทร์บูรณ์ สถิตวิริยวงศ์
ระดับการศึกษา	วิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ
แขนงวิชา	การจัดการเทคโนโลยีสารสนเทศ
ปีการศึกษา	2547

บทคัดย่อ

ปัจจุบันเครือข่ายอินเตอร์เน็ตเติบโตอย่างรวดเร็วครอบคลุมไปทั่วทุกภูมิภาคของโลก เกือบทุกองค์กรได้เชื่อมต่อเครือข่ายตนเองเข้ากับอินเตอร์เน็ตโดยผ่านผู้ให้บริการอินเตอร์เน็ต เพื่อใช้ประโยชน์จากแหล่งข้อมูลที่ใหญ่ที่สุดในโลกนี้ การทำธุรกิจให้บริการอินเตอร์เน็ตจึงเป็นอีกธุรกิจหนึ่งที่น่าจับตามอง แต่ด้วยงบประมาณการลงทุนที่สูงและระยะเวลาในการคืนทุนช้า ดังนั้นผู้ให้บริการอินเตอร์เน็ตจำเป็นต้องศึกษาและหาแนวทางในการดำเนินธุรกิจเป็นอย่างดี นอกจากนี้การรักษาความปลอดภัยของสารสนเทศในเครือข่ายจึงเป็นสิ่งที่สำคัญและจำเป็นอย่างยิ่ง โดยมีวัตถุประสงค์เพื่อรักษาบูรณภาพ ความพร้อมใช้งาน และความลับของข้อมูล มีการวางแผนจัดการและติดตั้งระบบรักษาความปลอดภัยอย่างเป็นระบบและมีประสิทธิภาพ สามารถให้บริการอินเตอร์เน็ตแก่องค์กรต่างๆ ได้เป็นอย่างดี

Title	Security Schemes and Business Models for Internet Service Provider
Student	Miss Waraporn Pongsuwagorn
Advisor	Asst. Prof. Dr. Chanboon Sathitwiriyawong
Level of Study	Master of Science in Information Technology
Major	Information Technology Management
Academic Year	2004

ABSTRACT

Nowadays, Internet system has been rapidly grow in every part of the world. Almost Organizations connect their network to internet through the Internet Service Providers (ISP) for their benefit in gathering world wide information. Internet Service Provide is the one interested business for investment. Internet Service Provider must be circumspect learn and try to get the business solution for good business process. Because internet is the non stop technology, high capital and slow to return investment. Not only that the network security is very important and necessary. Internet Service Providers (ISP) must have network security policy for data integrity, system integrity, availability and confidentiality data create planning and install network security system for the efficiency and powerful system. The security policy make the network increate their security to maintain data integrity and provide good service to every organizations.

สารบัญ

หน้า

สารบัญ(ต่อ)

หน้า

สารบัญ(ต่อ)

หน้า

สารบัญตาราง

หน้า

ตารางที่

สารบัญตาราง (ต่อ)

หน้า

ตารางที่

สารบัญรูป

หน้า

รูปที่

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

ปัจจุบันนี้เทคโนโลยีการติดต่อสื่อสารได้พัฒนาครอบคลุมไปทั่วทุกภูมิภาคของโลก โดยเฉพาะเครือข่าย อินเตอร์เน็ตได้เข้ามามีบทบาทอย่างมากในการสื่อสารและค้นหาข้อมูลได้จากทั่วโลกด้วยเหตุนี้จึงเกิดความนิยมอย่างมาก ก่อให้เกิดผู้ให้บริการอินเตอร์เน็ตขึ้นมาจำนวนมากเพื่อให้บริการรองรับความต้องการที่มากขึ้นทุกขณะ

ในการประกอบธุรกิจเกี่ยวกับการให้บริการอินเตอร์เน็ต ผู้ให้บริการจำเป็นต้องศึกษาและหาแนวทางในการดำเนินธุรกิจเป็นอย่างดี เนื่องจากเป็นธุรกิจที่ต้องใช้งบประมาณในการลงทุนสูง ระยะเวลาในการคืนทุนนาน และการให้บริการอินเตอร์เน็ต ต้องรองรับปริมาณการเชื่อมต่อของผู้ใช้บริการได้อย่างเต็มประสิทธิภาพ นอกจากนี้ความปลอดภัยของข้อมูลเป็นเรื่องที่สำคัญและขาดไม่ได้ ผู้ให้บริการอินเตอร์เน็ตมีความจำเป็นอย่างยิ่งที่ต้องมีมาตรการรักษาความปลอดภัยของระบบเครือข่ายที่อาจถูกโจมตีหรือโจรกรรมข้อมูลโดยผู้ประสงค์ร้าย ดังนั้นผู้ให้บริการอินเตอร์เน็ตควรรู้ถึงช่องทางต่างๆ ที่ผู้บุกรุกจะเข้ามาสู่ระบบเครือข่ายและวิธีป้องกันไม่ให้เข้ามายังเครือข่ายได้ อีกทั้งสามารถจัดการระบบรักษาความปลอดภัยอย่างเป็นระบบและมีประสิทธิภาพ เป็นที่รู้กันว่าระบบอินเตอร์เน็ตตั้งอยู่บนรากฐานของโปรโตคอล TCP/IP ถึงแม้ว่า TCP/IP นั้นไม่มีความปลอดภัยที่เพียงพอแต่เราก็ยังไม่มีทางเลือกอื่นที่ดีกว่ามาทดแทน การเรียนรู้ที่จะรักษาความปลอดภัยจะทำให้เราสามารถใช้ประโยชน์ได้จากเทคโนโลยีได้มากและปลอดภัยขึ้น

ระบบคอมพิวเตอร์และเน็ตเวิร์ค ได้ถูกคุกคามมากขึ้นทั้งจากไวรัสคอมพิวเตอร์หรือจากผู้ไม่ประสงค์ดี ซึ่งความมั่นคงปลอดภัยคอมพิวเตอร์และเน็ตเวิร์ค (Computer&Network Security) ช่วยปกป้องเครื่องคอมพิวเตอร์รวมไปถึงอุปกรณ์ต่างๆ ในเน็ตเวิร์คที่เกี่ยวข้อง และที่สำคัญยังสามารถช่วยปกป้องข้อมูลที่ได้จัดเก็บไว้ภายในระบบหรือใช้ในความหมายความปลอดภัยทางข้อมูลสารสนเทศ (Information Security) ก็ได้ จุดประสงค์หลักของความปลอดภัยทางข้อมูลคือ ความลับ (Confidentiality) ความสมบูรณ์ (Integrity) ความพร้อมใช้ (Availability) และการห้ามปฏิเสธความรับผิดชอบ (Non-Repudiation) ของข้อมูลต่างๆภายในองค์กร (CIA-N) ซึ่งจะกล่าวถึงในบทต่อไป

1.2 วัตถุประสงค์ของการศึกษา

ในการศึกษาเกี่ยวกับ ความปลอดภัยทางสารสนเทศและโมเดลในการประกอบธุรกิจของผู้ให้บริการอินเตอร์เน็ต มีวัตถุประสงค์ในการศึกษาดังนี้

1. เพื่อศึกษามาตรฐานการรักษาความปลอดภัยที่นิยมใช้กันในปัจจุบัน
2. เพื่อเป็นแนวทางในการสร้างความปลอดภัยของสารสนเทศอย่างเป็นระบบและมีประสิทธิภาพ
3. เพื่อเป็นแนวทางในการประกอบธุรกิจของผู้ให้บริการอินเตอร์เน็ต
4. เพื่อเป็นแนวทางในการสร้างระบบเครือข่ายของผู้ให้บริการอินเตอร์เน็ต

1.3 ขอบเขตของการศึกษา

1. ศึกษามาตรการรักษาความปลอดภัยของผู้ให้บริการอินเตอร์เน็ต
2. ศึกษาและหาแนวทางป้องกันการบุกรุกจากผู้ประสงค์ร้าย
3. ศึกษาแนวทางและทฤษฎีที่เกี่ยวข้องในการประกอบธุรกิจ
4. การวางระบบเน็ตเวิร์คและรายละเอียดอุปกรณ์ของผู้ให้บริการอินเตอร์เน็ต
5. สร้างโมเดลในการให้บริการและการประกอบธุรกิจของผู้ให้บริการอินเตอร์เน็ต

1.4 ขั้นตอนการศึกษา

1. ศึกษาความหมายและเป้าหมายของความปลอดภัย การควบคุมและภัยคุกคามต่างๆ ที่อาจเกิดขึ้นได้ในระบบ
2. ศึกษามาตรฐานการรักษาความปลอดภัยของผู้ให้บริการอินเตอร์เน็ต
3. ศึกษาการรูปแบบการโจมตีแบบต่างๆ และเทคโนโลยีเพื่อการรักษาความปลอดภัย
4. ศึกษาทฤษฎีทางธุรกิจที่เกี่ยวข้องกับการลงทุน
5. ออกแบบการวางระบบและรายละเอียดอุปกรณ์ที่ใช้ในการวางระบบของผู้ให้บริการอินเตอร์เน็ต
6. สร้างโมเดลจำลองการให้บริการและประกอบธุรกิจของผู้ให้บริการอินเตอร์เน็ต

1.5 ผลที่คาดว่าจะได้รับจากการศึกษา

1. สามารถใช้เป็นแนวทางในการสร้างระบบรักษาความปลอดภัยในองค์กรได้อย่างเป็นระบบและมีประสิทธิภาพ
2. ใช้เป็นแนวทางในประกอบธุรกิจของผู้ให้บริการอินเตอร์เน็ต

บทที่ 2
ความปลอดภัยในระบบคอมพิวเตอร์และเน็ตเวิร์ค

2.1 ความหมายของความปลอดภัย

ความปลอดภัย (Security) หมายถึง นโยบาย ขั้นตอนการปฏิบัติ และมาตรการทางเทคนิคที่นำมาใช้ป้องกัน การใช้งานจากบุคคลภายนอก การเปลี่ยนแปลง ขโมย หรือการทำความเสียหายต่อระบบสารสนเทศ องค์กรสามารถนำระบบรักษาความปลอดภัยมาใช้ร่วมกับเทคนิคและเครื่องมือต่างๆ ในการปกป้องคอมพิวเตอร์ฮาร์ดแวร์ ซอฟต์แวร์ ระบบเครือข่ายสื่อสาร และข้อมูล (สัลยุทธ์ สว่างวรรณ. 2545.)

2.2 จุดประสงค์หลักของความปลอดภัยของข้อมูล

เพื่อบำรุงรักษาหรือคงไว้ซึ่งคุณลักษณะหรือคุณภาพ 3 ประการ ดังนี้ (Whitman and Mattord. 2002.)

1. บูรณภาพ (Integrity)
2. สภาพพร้อมใช้งาน (Availability)
3. ความลับ (Confidentiality)

บูรณภาพของข้อมูล (Data Integrity)

บูรณภาพของข้อมูล หรือความครบถ้วนแท้จริงของข้อมูล (Data Integrity) หมายถึง การที่ข้อมูลมีคุณภาพ (Qualities) หรือคุณลักษณะ(Characteristics) ดังต่อไปนี้ คือมีความทันสมัยหรือทันเวลา (timeliness) ความถูกต้องหรือความแม่น (accuracy) ความสมบูรณ์ (completeness) และความสม่ำเสมอ หรือความต้องกัน (consistency) การเปลี่ยนแปลงแก้ไขข้อมูลดังกล่าวจะต้องทำตามข้อกำหนดและอำนาจโดยชอบเท่านั้น

บูรณภาพของระบบ (System Integrity)

บูรณภาพของระบบ หรือความครบถ้วนแท้จริงของระบบ (System Integrity) หมายถึง ความต้องการให้ระบบทำงานตามปกติโดยไม่มีความบกพร่อง เช่นไม่ให้ระบบถูกจับต้องโดยผู้ที่ไม่มีอำนาจ ทั้งที่กระทำโดยตั้งใจหรือพลั้งเผลอ

สภาพพร้อมใช้งาน (Availability)

สภาพพร้อมใช้งาน คือ ความต้องการให้ระบบสามารถทำงานได้ทันทีที่ต้องการ และผู้มีสิทธิโดยชอบไม่ถูกปฏิเสธการใช้งานระบบ เป้าหมายของสภาพความพร้อมใช้งานมีดังนี้

- การมีอยู่ของวัตถุ ข้อมูลและบริการที่สามารถใช้งานได้หรืออยู่ในรูปแบบที่ใช้งานได้
- มีความจุเพียงพอต่อความต้องการใช้บริการ และมีการจัดสรรทรัพยากรระบบหรือบริการที่เป็นธรรม
- เวลารอรับบริการที่มีขอบเขตเวลาแน่นอน และการตอบสนองที่ทันเวลา
- มีเวลาเพียงพอ และการให้บริการที่ทันเวลา ทันใจ ตามโอกาสและเวลาที่เหมาะสม
- มีความทนต่อความผิดพร่อง (Fault tolerance)
- ภาวะพร้อมกันที่สามารถควบคุมได้ (Controlled concurrency)

ความลับ (Confidentiality)

ความลับ คือ ความต้องการที่จะไม่เปิดเผยสารสนเทศที่เป็นส่วนตัวหรือความลับต่อบุคคลใดๆ ก็ตามที่ไม่มีสิทธิหรืออำนาจโดยชอบ

2.3 นโยบายความปลอดภัยขององค์กร (เรืองไกร รังสิพล. 2545.)

องค์ประกอบหนึ่งที่สำคัญอย่างยิ่งในการรักษาความมั่นคงของเน็ตเวิร์ค โดยที่ยังคงความสามารถในการใช้งานของผู้ใช้ในหน่วยงานต่างๆ ที่เกี่ยวข้องไว้ได้ดังเดิมนั้น จะต้องมีองค์ประกอบหลายประการที่สอดคล้องกัน หนึ่งในนั้นคือ นโยบายด้านความปลอดภัย

นโยบายด้านความปลอดภัยเป็นสิ่งสำคัญขั้นพื้นฐานขององค์กรที่มีผลต่อการป้องกันรักษาความปลอดภัยในระบบคอมพิวเตอร์และเน็ตเวิร์คที่ชัดเจนและสามารถบังคับใช้ได้ เพราะอุปกรณ์ต่างๆที่ใช้ในการรักษาความปลอดภัย เช่น ไฟร์วอลล์ หรือ IDS นั้นเป็นเพียงเครื่องมือรักษาความปลอดภัยทางเทคนิค ซึ่งสามารถกำหนดให้ทำการป้องกันได้ตามที่ผู้บริหารเน็ตเวิร์คต้องการ หากมีไฟร์วอลล์แล้วแต่การควบคุมที่กำหนดให้แก่ไฟร์วอลล์นั้นมีเพียงเล็กน้อย ไฟร์วอลล์นั้นก็สามารถช่วยป้องกันได้อย่างจำกัด ในทางกลับกันหากมีการควบคุมอย่างเคร่งครัดแล้วแน่นอนว่าจะช่วยให้เกิดความปลอดภัยสูงขึ้น แต่อาจจะส่งผลกระทบต่อผู้ใช้จนไม่สามารถใช้งานเน็ตเวิร์คได้อย่างสะดวกเช่นเดิม หากไม่มีกฎเกณฑ์ใดเป็นแนวทางสำหรับการปฏิบัติแล้วย่อมจะทำให้การดำเนินการนั้นสำเร็จได้ยากยิ่ง

สาเหตุที่ต้องมีนโยบายความปลอดภัยที่ชัดเจนเพราะ กิจกรรมหลายชนิดที่อาจจะส่งผลกระทบต่อความปลอดภัยของเครือข่ายและระบบคอมพิวเตอร์นั้นสามารถกระทำได้โดยผู้ใช้ และไม่สามารถป้องกันได้อย่างสมบูรณ์ด้วยเครื่องมือควบคุมทางเทคนิคชนิดใด เช่น การดักอ่านข้อมูล

โดยสนิฟเฟอร์ การปลอมชื่อผู้อื่นเพื่อส่งจดหมาย การเปิดดูเวปไซท์ที่ไม่เหมาะสม การส่งข้อมูลของบริษัทออกไปยังภายนอก เป็นต้น กิจกรรมต่างๆ เหล่านี้ยากต่อการป้องกันทางเทคนิค เช่น ระบบอีเมล์ทั่วไปที่ใช้ในอินเตอร์เน็ตโดยใช้โปรโตคอล SMTP ไม่มีกลไกการยืนยันตัวผู้ส่ง หากผู้ใช้จะทำการปลอมจดหมายก็มีโอกาสที่จะกระทำได้ เช่นเดียวกับการดักอ่านข้อมูลด้วยสนิฟเฟอร์ที่อาจจะสามารถกระทำได้หากมีการใช้เน็ตเวิร์คร่วมกัน ซึ่งหากไม่มีกฎเกณฑ์ที่กำกับและควบคุมไว้อย่างชัดเจนว่ากิจกรรมใดเป็นสิ่งที่อนุญาตให้กระทำและกิจกรรมใดเป็นสิ่งที่ห้ามกระทำแล้ว ย่อมจะทำให้มีการละเมิดความปลอดภัยเกิดขึ้นได้อย่างง่ายดายโดยไม่ต้องมีการรับผิด

นอกจากเป็นการระบุที่ชัดเจนถึงข้อควรปฏิบัติและข้อห้ามของการใช้งานระบบคอมพิวเตอร์และเน็ตเวิร์คแล้ว การเพิ่มมาตรการรักษาความปลอดภัยภายในเน็ตเวิร์คนั้นเป็นเสมือนหนึ่งการจำกัดสิทธิการใช้งานของผู้ใช้ในทุกระดับที่ใช้งานเน็ตเวิร์คร่วมกันอยู่นั้น ไม่ว่าจะเป็นผู้ใช้ทั่วไปหรือเป็นผู้บริหารระบบเอง (System Administrator) ย่อมจะได้รับผลกระทบจากมาตรการที่ได้กำหนดขึ้นไม่มากก็น้อย การรักษาความปลอดภัยมักจะอยู่คนละฟากกับความสะดวกสบายเสมอ หากต้องการความปลอดภัยสูงขึ้นก็ต้องยอมรับกับความสะดวกสบายที่ลดลง และหากต้องการความสะดวกสบายมากขึ้นก็จำเป็นต้องยอมรับความเสี่ยงที่อาจจะมาพร้อมกับความสะดวกสบายนั้น

นโยบายความปลอดภัยจึงต้องได้รับการพิจารณาจากผู้บริหารระดับสูงขององค์กรนั้นด้วย โดยควรจะเป็นนโยบายระดับสูงที่พิจารณาควบคู่กับวิสัยทัศน์ ภารกิจ และกลยุทธ์ขององค์กรนั้น หากเป็นหน่วยงานทางธุรกิจแล้วนโยบายความปลอดภัยจะพิจารณาให้สอดคล้องและรองรับกับแผนการดำเนินธุรกิจของบริษัท สิ่งหนึ่งที่ต้องตระหนักเสมอคือทรัพยากรในระบบสารสนเทศ อันประกอบด้วยฮาร์ดแวร์ ซอฟต์แวร์ ข้อสนเทศ และผู้ใช้นั้นมีไว้เพื่อส่งเสริมการดำเนินธุรกิจ จึงต้องดูแลให้ทำงานประสานกันอย่างมีประสิทธิภาพ และมีความปลอดภัยอย่างเพียงพอต่อธุรกิจนั้นๆ

นโยบายความปลอดภัยที่ดีควรครอบคลุมส่วนต่างๆ เหล่านี้

1. การปฏิบัติงานตามปกติของผู้ใช้ที่ทำให้ผู้ใช้ปลอดภัย เพื่อเป็นแนวทางในการปฏิบัติงานทั่วไปของผู้ใช้ที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศ เช่น การใช้ซอฟต์แวร์ การรับ-ส่งอีเมล์ การติดต่อกับบุคคลภายนอก การป้องกันการใช้งานโดยบุคคลอื่น การบราวส์เว็บ เป็นต้น

2. การปฏิบัติงานของผู้ที่มีหน้าที่รับผิดชอบทางเทคนิค เช่น ผู้บริหารระบบ (System Administrator) วิศวกรเน็ตเวิร์ค เพื่อเป็นแนวทางในการปฏิบัติงานที่สามารถวางใจได้ว่าจะทำให้ระบบสารสนเทศมีความปลอดภัย เช่น การสำรองข้อมูล การทดสอบระบบ การป้องกันสิ่งผิดปกติ การจัดเก็บบันทึก (log)

3. ข้อห้ามสำหรับกิจกรรมต่างๆ ที่ไม่พึงปรารถนาสำหรับองค์กร และไม่อนุญาตให้ผู้ใช้

ดำเนินการกิจกรรมดังกล่าวภายในระบบสารสนเทศขององค์กร เช่น การแคร็ก (Crack) รหัสผ่าน การปลอมจดหมาย การใช้งานในชื่อผู้อื่น เป็นต้น

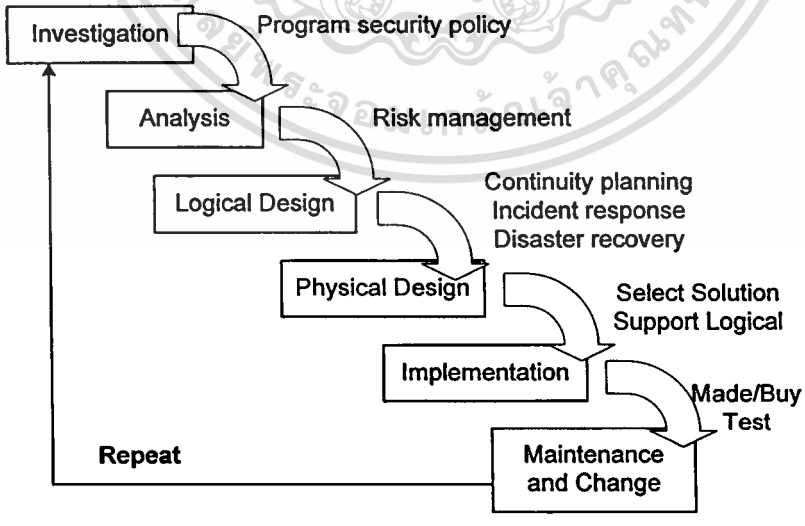
4. ข้อจำกัดในการใช้งาน เช่น ไม่อนุญาตให้ใช้โปรแกรมบางประเภทได้ ไม่อนุญาตให้เปิดดูเว็บไซท์บางประเภท เป็นต้น

5. การป้องกันทางเทคนิคขั้นต่ำที่จะต้องมี เพื่อให้สามารถมั่นใจได้ว่าสามารถควบคุมป้องกัน และตรวจจับเหตุการณ์ผิดปกติที่จะส่งผลกระทบต่อความปลอดภัยในระบบสารสนเทศได้

6. แบ่งหน้าที่และความรับผิดชอบในด้านความปลอดภัย ของผู้ที่เกี่ยวข้องกับระบบสารสนเทศไม่ว่าจะเป็นผู้บริหาร ผู้ใช้ และผู้มีหน้าที่ทางเทคนิค

2.4 กระบวนการการพัฒนาระบบรักษาความปลอดภัยของสารสนเทศ (The Security Systems Development Life Cycle :SecSDLC)

การพัฒนาระบบรักษาความปลอดภัย เช่นเดียวกับการพัฒนาระบบอื่นๆ ที่ต้องจัดทำโครงการที่มีขั้นตอนแบ่งไว้เหมือนกับ System Development Life Cycle (SDLC) ที่ใช้ในการพัฒนาระบบทางด้านเทคโนโลยีสารสนเทศทั่วไป จึงดัดแปลงมาให้เหมาะสมกับขั้นตอนของการพัฒนาระบบรักษาความปลอดภัยด้วย โดยใช้ตัวย่อว่า SecSDLC ซึ่งมีกระบวนการพื้นฐานพอสังเขปดังแสดงในรูปที่ 2.1 (Whitman and Mattord. 2002.)



รูปที่ 2.1 แสดงกระบวนการในการพัฒนาระบบรักษาความปลอดภัยของสารสนเทศ

ขั้นตอนของการพัฒนาระบบรักษาความปลอดภัย (SecSDLC) ประกอบด้วย

1. Investigation

เป็นขั้นตอนแรกที่เกี่ยวข้องกับฝ่ายบริหาร กล่าวถึงวัตถุประสงค์ หลักการและแนวความคิดเชิงนโยบาย และการทำงบประมาณต่างๆ ที่จะจัดทำขึ้นสำหรับภายในองค์กรที่เกี่ยวข้องกับด้านความปลอดภัยสารสนเทศ และรวมไปถึงการจัดตั้งคณะทำงานด้านนี้ขึ้นมาโดยเฉพาะ หรือ Program Security Policy และแม้กระทั่งการติดตาม เฝ้าระวังการตรวจสอบระบบสารสนเทศให้มีความปลอดภัยที่เชื่อถือได้เพียงพอต่อการดำเนินธุรกิจอย่างมั่นใจ

2. Analysis

คือขั้นตอน วิเคราะห์ ข้อมูล เอกสาร และผลจากการเข้าไปศึกษาในขั้นตอนแรกที่ได้มา ทำการพิจารณาเปรียบเทียบนโยบายเดิม และมาตรการต่างๆ ด้านความปลอดภัย ที่ใช้อยู่ในปัจจุบัน มีการควบคุม และให้ความสำคัญ มีการจัดการหรือข้อควรปฏิบัติที่เกิดขึ้นจริง อย่างเหมาะสมขึ้นมาใหม่ มีการรองรับให้เหมาะสมเพียงพอหรือไม่ โดยเน้นที่การทำ Risk Management ซึ่งมีผลกระทบกับสารสนเทศ และการดำเนินธุรกิจอย่างต่อเนื่องแท้จริง

3. Logical Design

การออกแบบด้านความปลอดภัยในมุมมองของ Logical ให้เป็นตามสิ่งที่ได้มาจากขั้นแรกๆ ทั้ง 2 ส่วน ให้สามารถจัดการปัญหาด้านความปลอดภัยให้ครอบคลุมและเน้นย้ำตามความสำคัญที่ให้ไว้ มักกล่าวเน้นเรื่องของการทำ Continuity Planning กับ Incident Response และการวางแผนสำหรับ Disaster Recovery เป็นสิ่งสำคัญ

4. Physical Design

ขั้นตอนนี้เป็นการออกแบบ จัดหาและเลือกใช้ เทคโนโลยีเพื่อสนับสนุนการออกแบบที่ได้จากขั้นตอนที่แล้ว และได้ทำการตกลงเป็นที่ยอมรับเรียบร้อยไปแล้ว ซึ่งอาจจะมีความเปลี่ยนแปลงด้านความต้องการที่เปลี่ยนไป เพื่อให้ได้ทางเลือกที่เหมาะสมที่สุดและเกิดประโยชน์สูงสุดกับองค์กรด้วยก่อนที่จะตัดสินใจเลือกเทคโนโลยีที่ตรงกับที่ออกแบบ

5. Implementation

ขั้นตอนนี้ก็จะเป็นการจัดทำ หรือจัดซื้อ เพื่อให้ได้มาซึ่งระบบรักษาความปลอดภัยของระบบสารสนเทศขององค์กร แล้วทำการทดสอบ การใช้ และประเมินผล รวมทั้งการจัดฝึกอบรมกับผู้เกี่ยวข้องโดยเฉพาะ

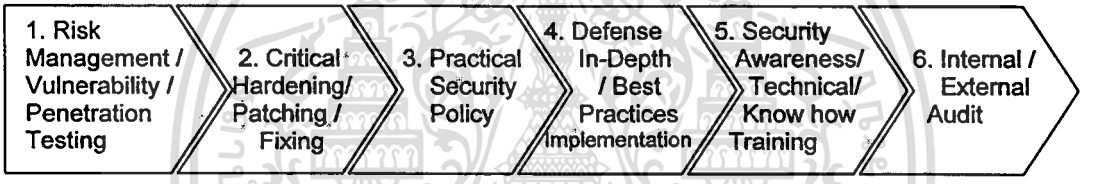
6. Maintenance and Change

กระบวนการสุดท้ายของ SecSDLC นี้มีความสำคัญที่สุดเพราะต้องมีการเฝ้าตรวจ ทดสอบ และปรับปรุงซ่อมแซมระบบรักษาความปลอดภัยสารสนเทศให้ทันสมัย และใช้งานได้ ไม่เป็น

จุดอ่อน อยู่สม่ำเสมอ การคุกคามต่อระบบสารสนเทศทีมากมาย หรือไม่เคยพบเจอมาก่อนเพิ่มขึ้นทุกๆวัน จนกว่าระบบที่ออกแบบไว้จะไม่สามารถรองรับด้านความปลอดภัยที่เปลี่ยนแปลงไปได้ จึงจำเป็นต้องย้อนกลับไปเริ่มกระบวนในขั้นตอนแรกใหม่ เพื่อให้เกิดระบบรักษาความปลอดภัยรุ่นใหม่ที่รองรับสถานการณ์นั้นได้

2.5 การจัดการระบบรักษาความปลอดภัยอย่างเป็นระบบ (Hom-anek. 2003.)

การจัดการระบบรักษาความปลอดภัยของผู้ให้บริการอินเตอร์เน็ตอย่างเป็นระบบ และมีประสิทธิภาพ โดยการนำ ISMF : Information Security Management Framework มาช่วยในการดำเนินการ ผู้ให้บริการอินเตอร์เน็ตควรทำตามขั้นตอนทั้ง 7 ขั้นตอน เป็นประจำทุกๆ 3 เดือน หรืออย่างน้อยปีละ 2 ครั้ง เพื่อให้มั่นใจถึงระบบรักษาความปลอดภัยที่ทันสมัย เหมาะกับสภาวการณ์และเทคโนโลยีที่เปลี่ยนไป ขั้นตอนทั้ง 7 ดังแสดงในรูปที่ 2.2



รูปที่ 2.2 แสดงการจัดการระบบรักษาความปลอดภัยอย่างเป็นระบบ

ขั้นตอนที่ 1 การทำ Risk Management / Vulnerability / Penetration Testing

ทำการวิเคราะห์และประเมินความเสี่ยง โดยการวิเคราะห์และตรวจหาช่องโหว่ในระบบ ที่เรียกว่า Vulnerability Assessment และการทดสอบเจาะระบบเพื่อนำเอาข้อมูลที่สำคัญออกมาจากระบบโดยการทดลอง Hack เสมือนว่ามี Hacker เข้ามาในระบบเข้ามาเจาะระบบ เรียกขั้นตอนนี้ว่า Penetration Testing การทำ Penetration Testing นั้น จะรวมไปถึงการทดสอบความแข็งแกร่งของระบบโดยการจำลอง Attack แบบ DoS Attack หรือ Denial Of Services Attack เพื่อให้ระบบใช้งานไม่ได้แบ่งออกเป็น 2 ประเภท คือ Black-Box และ White-Box

- **Black-Box Penetration Testing** เป็นการเจาะระบบโดยที่ผู้ที่รับจ้างเจาะระบบจะไม่ได้รับข้อมูลจากผู้ว่าจ้างนอกจากเป้าหมายที่เป็น Web Site หรือเป็น IP Address เท่านั้น ที่เหลือผู้รับจ้างต้องพยายามเจาะเข้ามาจาก Internet โดยใช้ความสามารถของผู้รับจ้างเอง

ข้อดี ของการเจาะระบบแบบ Black-Box Penetration Testing คือ ผู้ให้บริการอินเตอร์เน็ตสามารถประเมินความแข็งแกร่งของระบบได้ จากภายนอกก็คือจากพวก Hacker ที่เจาะเข้ามาจากทาง Internet โดยตรง

ข้อเสีย ของการเจาะระบบแบบ Black-Box Penetration Testing คือ ผู้รับจ้างอาจจะไม่สามารถเจาะเข้า มาได้เพราะข้อมูลไม่เพียงพอ หรือ ความสามารถของผู้รับจ้างมีไม่มากพอที่จะเจาะเข้าสู่ระบบได้

- **White-box Penetration Testing** เป็นการเจาะระบบที่ผู้รับจ้างจะต้องเข้ามาที่ Office และ On-line เข้าสู่ระบบ LAN หรือ Intranet ของผู้ว่าจ้าง เรียกว่าเป็นการเจาะจากข้างใน เพื่อเป็นการประเมินความเสี่ยงภายในของผู้ให้บริการอินเตอร์เน็ต

ข้อดี ของวิธีเจาะระบบแบบ White-Box Penetration Testing คือ ผู้ให้บริการอินเตอร์เน็ตสามารถประเมินความเสี่ยงได้ใกล้เคียงกับสถานการณ์จริงมากกว่าแบบ Black-Box Penetration Testing เพราะ ผู้รับจ้างเจาะระบบ จะมีข้อมูลภายในมากกว่าแบบแรก

ข้อเสีย ของวิธีเจาะระบบแบบ White-Box Penetration Testing คือ เราไม่สามารถประเมินจากภายนอกได้เหมือนแบบแรก

กล่าวโดยสรุปก็คือ เราควรทำทั้งสองแบบแล้วนำผล Summary Report จากการทำ Black-box และ White-box box Penetration Testing มาประมวลผลรวมกัน เพื่อหาแนวทางในการแก้ไขในขั้นตอนที่ 2 ของ ISMF ต่อไป

ขั้นตอนที่ 2 การทำ Critical Hardening / Patching Fixing

เมื่อระบบมีช่องโหว่เกิดขึ้นต้องทำการประเมินว่าช่องโหว่นั้น สามารถก่อให้เกิดความเสียหายกับระบบมากน้อยเพียงใด จึงจำเป็นต้องมีหลักเกณฑ์ในการประเมินผลจากรายงานช่องโหว่ที่เราตรวจพบ และทำการจัดลำดับความสำคัญของช่องโหว่ที่เราพบว่า ช่องโหว่แบบไหนมีความจำเป็นต้องแก้ไขโดยด่วน ซึ่งปกติเราจะเรียกช่องโหว่ในลักษณะนี้ว่า High Risk ซึ่งก็จะต่างกับช่องโหว่แบบ Medium Risk หรือ Low Risk ที่หมายความว่ายังไม่ก่อผลกระทบรุนแรงให้กับระบบเหมือนแบบ High Risk หลักเกณฑ์ในการประเมินความเสี่ยงที่ว่าช่องโหว่แบบใดที่เป็น High Risk ดูได้จากผลจากรายงานของ" Vulnerability Scanner" ในเบื้องต้น ซึ่ง Vulnerability Scanner ที่ใช้ควรจะใช้หลายๆ ตัวประกอบกัน ยกตัวอย่างที่นิยมใช้กันโดยทั่วไปได้แก่ Nessus (Open Source), Retina, Internet Scanner, Shadow Security Scanner เป็นต้น ประกอบกับข้อมูลเทคนิคการ Hack ระบบใหม่ๆ มาช่วยประเมินว่าเราต้องจัดการแก้ปัญหากับช่องโหว่ตัวไหนก่อนเพื่อที่จะทำให้ระบบของเรายังคงมีความปลอดภัยและมีเสถียรภาพเพียงพอที่จะต่อการโจมตีของ Hacker

เมื่อพบ Risk ต้องทำการปิดช่องโหว่หรือการ" Harden" ระบบ ซึ่งเน้นไปที่ช่องโหว่ที่เป็นแบบ High Risk ก่อน เพราะมีผลกระทบกับระบบมากที่สุด หลักการในการ Harden ระบบนั้นคือ

- ไม่เปิดใช้บริการที่ไม่มีความจำเป็นต้องใช้ เช่น ถ้าใช้เครื่องทำเป็น Web Server อย่างเดียว ก็ควรเปิดใช้บริการเฉพาะพอร์ต 80 (http) และพอร์ต 443 (https) เท่านั้น

- ปิดบริการที่เป็นค่า Default มาจากการติดตั้งระบบในตอนแรก เช่น ใน Web Server จะมีการเปิดพอร์ต TCP 135 ซึ่งเป็น RPC (Remote Procedure Call) Service เป็นผลให้ติด Virus Worm Blaster หรือ Nachi เป็นต้น นอกจากนี้ ยังเปิดพอร์ต TCP139 และ TCP/IP 445 เป็นค่าโดยกำหนด ซึ่งเป็นการให้บริการ "File & Print Sharing" เช่น การ Map Network Drive เป็นต้น

- ทำการ Stop Service ที่ไม่มีความจำเป็นต้องใช้งาน

- ใช้ TCP Filter ซึ่งเป็นความสามารถที่ Windows NT/2000/2003 Server มีมาให้ใช้งานอยู่แล้ว สามารถเป็น Firewall ให้กับเครื่องแบบไม่ต้องลงทุน

- ทำการการ Patch หรือการลง Hotfix ให้กับระบบนั้น ก็เป็นสิ่งจำเป็นที่ต้องทำนอกเหนือจากการปิดบริการหรือพอร์ตที่เราไม่ได้ใช้งานเช่นกัน ต้องมีการติดตามลง Patch หรือโปรแกรมแก้ไขช่องโหว่ที่เกิดขึ้นในระบบ ซึ่งช่องโหว่ของระบบโดยทั่วไปจะเกิดขึ้นทุกเดือน

จะเห็นได้ว่าการ Harden ระบบนั้น ไม่ใช่ทำเสร็จแล้วจะจบเลย การ Harden ครั้งแรกจนระบบปลอดจากช่องโหว่นั้นเราเรียกว่า" Get Secure" แต่ปัญหาก็คือ เราจะทำอย่างไรให้" Stay Secure" นั่นคือ ต้องคอยติดตามข่าวสารช่องโหว่ใหม่ๆ รายเดือน บางทีอาจเป็นรายสัปดาห์หรือรายวันก็มี และเราต้องคอยลง Patch, Horfix ตลอดจน Service Pack ต่างๆ ที่จะออกมาเป็นระยะๆ เพื่อให้ระบบมีความปลอดภัยอยู่เสมอ

ขั้นตอนที่ 3 การทำ Practical Information Security Policy

กำหนดนโยบายการใช้งานคอมพิวเตอร์และอินเทอร์เน็ตอย่างปลอดภัย มีการป้องกันในระดับบริหารจัดการ (Administrative Level) ซึ่งหมายถึงเรื่อง Policy , Standard, Guideline และ Procedure ที่ต้องถูกนำมาใช้เป็นนโยบายใน การปฏิบัติของผู้ใช้ IT ในองค์กร โดยปกติแล้วองค์กรมักจะนิยมเขียนนโยบายด้านความปลอดภัยข้อมูลคอมพิวเตอร์ โดยอิงจากมาตรฐาน ISO/IEC 17799:2000 ซึ่งประกอบไปด้วยหัวข้อต่างๆ 10 เรื่อง โดยเน้นในรูปของภาพรวมไม่เจาะลึกด้านปฏิบัติ

ขั้นตอนที่ 4 การทำ Defense-In-Depth และ Best Practices Implementation

คำว่า 'Defense-In-Depth" นั้นเน้นการจัดการแบบ "Layered Security" คือมีการป้องกันระบบเป็นชั้น ๆ เปรียบเสมือนมีประตูหลายชั้นก่อนจะเข้าถึงตัวระบบได้ และมีการแบ่งระบบออกเป็นหลายส่วน ในทางเทคนิคเราเรียกว่า "Compartmentalization" เช่น การทำ VLAN แยกระบบที่สำคัญออกจากกัน หรือการแบ่ง DMZ (Demilitarized Zone) ออกเป็นหลาย ๆ DMZ เช่น Web Sever ไม่ควรอยู่กับ Mail Server ใน DMZ เดียวกัน หรือ Primary DNS ไม่ควรอยู่กับ

Secondary DNS ใน DMZ เดียวกันเป็นต้น เพื่อที่จะป้องกันในกรณีที่ Hacker เจาะ Server หรือ Host ใด Host หนึ่งใน DMZ สำเร็จ Hacker ก็จะเจาะ Host ที่อยู่ในบริเวณ DMZ เดียวกันได้ง่าย แต่ถ้าแบ่งระบบออกเป็น หลายชั้น/หลายส่วน Hacker ก็ต้องใช้ความพยายามมากขึ้นที่จะ Hacked ระบบทั้งหมด ส่วนของ Best Practices นั้นเป็นส่วนหนึ่งของหลักการ IT Governance Implementation กล่าวคือ Best Practices นั้น หมายถึง การนำเอาสูตรสำเร็จ หรือตัวอย่างการ Implement ที่ดีมาจัดการกับระบบของเรา

ขั้นตอนที่ 5 การทำ Security Awareness/Technical Know-how Transfer Training

ทำการฝึกอบรมความรู้ความเข้าใจด้านการรักษาความปลอดภัยข้อมูลให้กับ ผู้บริหารตลอดจนพนักงาน ให้มีความเข้าใจและมีความตระหนักให้ระวังภัยจากการใช้งานคอมพิวเตอร์โดยเฉพาะอินเทอร์เน็ตโดยไม่ระมัดระวังเพียงพอ ซึ่งอาจก่อให้เกิดความเสียหายกับองค์กรได้โดยไม่รู้ตัว การฝึกอบรมต้องมีการแสดงกรณีตัวอย่าง หรือ Case Study ให้ผู้เข้ารับการอบรมเห็นว่า Hacker และ Virus มีวิธีการในการโจมตีเราได้อย่างไร เมื่อทุกคนได้เ ห็นตัวอย่างแล้วก็จะเกิดความตระหนักได้ด้วยตนเองว่า จากนี้ต้องใช้งานเครือข่ายและอินเทอร์เน็ตด้วยความระมัดระวังมากขึ้น ต้องมีการฝึกอบรมเป็นประจำทุกปี และควรฝึกอบรมให้ครบ 6 กลุ่ม แสดงในตารางที่ 2.1 ดังนี้

ตารางที่ 2.1 แสดงการฝึกอบรมพนักงานด้านการรักษาความปลอดภัยของข้อมูล

กลุ่มที่	การฝึกอบรม	ผลที่ได้รับ
กลุ่มที่ 1 ผู้บริหารระดับสูง) Top Management) **กลุ่มที่ 2** ผู้บริหารระดับกลาง) Middle Management)	การฝึกอบรม เรื่อง Security Awareness Training ให้กับผู้บริหารระดับสูงนั้นควรจะเป็นเรื่องความเสี่ยงที่มีอยู่ในอินเทอร์เน็ตทุกวันนี้ (Information Security Risk), โอกาสที่จะเกิดความเสียหายขึ้นจากการจู่โจมของ Hacker หรือ Virus Computer, ความจำเป็นที่ระบบต้องมีการควบคุมด้วย" Control" เช่น การติดตั้ง Enterprise Firewall และ Intrusion Detection System ตลอดจนการติดตั้ง Personal Firewall และ Anti -Virus ในทุก workstation การฝึกอบรมควรใช้ระยะเวลาสั้นๆ ไม่เกิน 3ชั่วโมงและไม่ควรใช้ศัพท์เทคนิคมากเกินไป	จะทำให้ผู้บริหารมีความเข้าใจเรื่อง Information Security มากขึ้น และมีผลอย่างมากกับองค์กร เนื่องจากผู้บริหารจะให้ความสนับสนุนฝ่าย IT มากยิ่งขึ้น หลังจากที่ได้ทำความเข้าใจกับปัญหาทางด้านความปลอดภัยคอมพิวเตอร์หลังจากการฝึกอบรมแล้ว

ตารางที่ 2.1 แสดงการฝึกอบรมพนักงานด้านการรักษาความปลอดภัยของข้อมูล (ต่อ)

กลุ่มที่	การฝึกอบรม	ผลที่ได้รับ
กลุ่มที่ 3 กลุ่มผู้ดูแลระบบ (System Administrators) **กลุ่มที่ 4** กลุ่มผู้ดูแลความปลอดภัยคอม พิวเตอร์โดยตรง (Security Administrators) **กลุ่มที่ 5** กลุ่มผู้ตรวจสอบระบบสารสนเทศ (IT Auditors)	การฝึกอบรมทั้ง 3 กลุ่มนี้ควรเน้นเนื้อหาทางด้านเทคนิคเพิ่มขึ้นจากการฝึกอบรมผู้บริหารและควรมีกรณีศึกษา(Security Incident case study) ของระบบต่างๆ และ แสดงให้เห็นถึงวิธีการ โจมตีของ Hacker และ Virus ตลอดจน วิธีการป้องกันที่ถูกต้องและมีประสิทธิภาพ โดยอาจมีรายละเอียดและระยะเวลาในแต่ละกลุ่มแตกต่างกัน ตั้งแต่ 6 ชั่วโมง จนถึง 30 ชั่วโมง ในกรณีที่ต้องการให้มีความเข้าใจมากขึ้น ควรมี" Hand-on" ให้ผู้เข้าอบรมได้ใช้คอมพิวเตอร์ฝึกปฏิบัติในห้องเรียนด้วย	เพื่อให้มีความรู้ความเข้าใจในการปฏิบัติงานและสามารถดูและระบบเน็ตเวิร์คให้มีความปลอดภัยได้
กลุ่มที่ 6 กลุ่มผู้ใช้งานคอมพิวเตอร์ทั่วไป (Users)	กลุ่มนี้เป็นกลุ่มที่มีความเสี่ยงสูงที่จะปล่อย Virus เข้าสู่ระบบโดยไม่รู้ตัว พอๆ กับกลุ่มที่ 1 และ 2 เนื่องจากไม่มีความรู้พื้นฐานทางเทคนิคเพียงพอ ดังนั้น การฝึกอบรมต้องแสดงให้เห็นถึงการใช้งานคอมพิวเตอร์รายวันที่ผู้ใช้ต้องใช้คอมพิวเตอร์ในการทำงานของตนเองเป็นประจำอยู่แล้ว เช่น การเข้าไปหาข้อมูลใน Web site และ การรับ-ส่ง e-Mail การฝึกอบรมควรจะแสดงให้เห็นถึงภัยต่าง ๆ จากการเข้า Web site ที่ไม่เหมาะสม หรือ การถูกโปรแกรม SpyWare ประเภท Key Logger มาฝังในเครื่องโดยผ่านทาง Attached file ที่มากับ e-Mail การใช้งานอินเทอร์เน็ตโดยไม่มี Personal Firewall ก็เป็นอีกปัญหาหนึ่งของผู้ใช้งานโดยทั่วไปที่ต้องเน้นในการฝึกอบรมเช่นกัน	เพื่อสามารถใช้งานคอมพิวเตอร์และอินเตอร์เน็ตได้อย่างถูกต้องและปลอดภัย ลดความเสี่ยงในการติด virus ที่มีกับการเข้าเวปหรืออีเมล์

หลังจากการฝึกอบรม Security Awareness Training และการฝึกอบรม Technical Know-how Transfer Training ในเชิงลึกด้านเทคนิคแล้ว จะทำให้ทั้ง 6 กลุ่มซึ่งก็คือพนักงานทุกคนในองค์กร มีความเข้าใจเรื่องภัยจากอินเทอร์เน็ต รวมทั้งวิธีการป้องกันตนเองและองค์กรให้พ้นภัยจากเหล่า Hacker และ Virus ได้ดียิ่งขึ้น ส่งผลให้ระบบมีความปลอดภัยและมีเสถียรภาพเพิ่มมากขึ้น ฝ่าย IT ก็ทำงานง่ายขึ้นด้วย เพราะฉะนั้นโปรแกรมนี้ควรถูกบรรจุเข้าไว้ใน IT Master Plan ขององค์กรและควรเตรียมงบประมาณไว้ให้เพียงพอ สำหรับค่าใช้จ่ายด้านการฝึกอบรมในแต่ละปีด้วย เพื่อที่องค์กรของเราจะได้ลดปัญหาทางด้านความปลอดภัยคอมพิวเตอร์ลง ไม่ให้มีผลกระทบรุนแรงอย่างเช่นในทุกวันนี้

ขั้นตอนที่ 6 การทำ Internal/ External Audit, Re-Assessment and Re-Hardening

เป็นการทำการตรวจสอบ (IT Auditing) ซึ่งเป็นส่วนหนึ่งของแนวคิด IT Governance ที่องค์กรสมัยใหม่นิยมนำมาประยุกต์ใช้ หลังจากที่ได้ทำประเมินความเสี่ยงของระบบและปิดช่องโหว่ของระบบแล้ว เพื่อจะทราบว่าช่องโหว่ที่มีผลกระทบกับระบบได้ถูกจัดการแก้ไขอย่างถูกต้อง ดังนั้น เราจึงต้องทำการตรวจสอบซ้ำเป็นครั้งที่ 2 การตรวจสอบทำโดยการทำ Re-Assessment รายละเอียดเหมือน ISMF ขั้นตอนที่ 1 แต่จะสรุปผลออกมาในภาพรวมมากขึ้น โดยมีการเปรียบเทียบกับผลจากขั้นตอนที่ 1 ก่อนที่เราจะ Hardening หรือ ปิดช่องโหว่ในขั้นตอนที่ 2 เราจะได้ความแตกต่างจาก GAP Analysis แสดงให้เห็นถึงผล ก่อน Hardening และ หลัง Hardening ว่ามีความแตกต่างกันอย่างไร ถ้าการ Hardening ยังไม่สมบูรณ์ก็ต้องมีการ Re-Hardening อีกครั้ง เพื่อให้แน่ใจว่าได้ปิดช่องโหว่จนความเสี่ยงอยู่ระดับที่ยอมรับได้ (Risk Acceptance Level) การตรวจสอบระบบนั้นผู้ตรวจสอบระบบสารสนเทศ (IT Auditor) ควรมี Compliance Checklist เพื่อนำไปตรวจสอบระบบต่างๆ และนำผลลัพธ์มาทำ GAP Analysis ว่าระบบที่ใช้อยู่นั้นได้มีการจัดการด้านระบบรักษาความปลอดภัยเป็นไปตาม IT Security Policy ขององค์กรหรือไม่ และได้ทำตาม Best Practices ที่เหมาะสมกับระบบนั้นๆ แล้วหรือไม่ สามารถแบ่งประเภทของงานตรวจสอบระบบสารสนเทศออกเป็น 7 ประเภทใหญ่ๆ ดังนี้

1. การตรวจสอบระบบปฏิบัติการ (NOS Audit) เช่น การตรวจสอบระบบ Server ที่ใช้ MS Windows เช่น Windows NT, Window 2000 Server ตลอดจน Workstation ที่ใช้ Windows XP เป็นต้น การตรวจสอบควรจะครอบคลุมถึงระบบปฏิบัติการอื่นด้วย เช่น การตรวจสอบระบบปฏิบัติการ Unix เช่น Sun Solaris, HP/UX, IBM AIX และ ระบบปฏิบัติการ Linux ที่ได้รับความนิยมเพิ่มขึ้นเรื่อยๆ

2. การตรวจสอบอุปกรณ์เครือข่าย (Network Devices Audit) เช่น การตรวจสอบ Router, การตรวจสอบ Switching และ การตรวจสอบ Remote Access Server ตลอดจน การ

ตรวจสอบโครงสร้างของเครือข่าย (Network Infrastructure Audit) และ ประสิทธิภาพของเครือข่าย (Network Performance Audit) โดยใช้โปรแกรมตรวจสอบประเภท Packet Sniffer หรือ RMON Probe เป็นต้น

3. การตรวจสอบอุปกรณ์รักษาความปลอดภัย (Security Devices Audit) เช่น การตรวจสอบ Firewall, การตรวจสอบ Intrusion Detection System (IDS), การตรวจสอบ Intrusion Prevention System (IPS), การตรวจสอบโปรแกรม Enterprise Anti-Virus, การตรวจสอบ VPN Server เป็นต้น การตรวจสอบอุปกรณ์รักษาความปลอดภัยนั้นเป็นสิ่งที่มีความจำเป็นอย่างสูง เพราะถ้าอุปกรณ์รักษาความปลอดภัยมีปัญหาเสียเอง หรือโดน Hacker เจาะเข้ามา compromised ก็จะทำให้เกิดปัญหากับความปลอดภัยของระบบโดยรวม ผู้ตรวจสอบควรเป็นผู้ชำนาญงานด้านการใช้งาน Firewall หรือ IDS/IPS มาก่อนด้วยจะช่วยได้มาก

4. การตรวจสอบโปรแกรมฐานข้อมูล (RDBMS Audit) เช่น การตรวจสอบ Oracle, IBM DB2, Microsoft SQL Server, Informix, SYBASE หรือ MySQL RDBMS การตรวจสอบโปรแกรมฐานข้อมูล ควรกระทำควบคู่ไปกับการตรวจสอบระบบปฏิบัติการที่โปรแกรมฐานข้อมูลทำงานอยู่ เช่น Oracle ทำงานบน Unix เป็นต้น เพื่อที่จะเจาะลึกลงไปในด้านความปลอดภัยของตัวโปรแกรมฐานข้อมูลเองว่ามีช่องโหว่หรือไม่ ผู้ตรวจสอบควรเป็นผู้เชี่ยวชาญการใช้งานโปรแกรมฐานข้อมูลนั้นๆมาก่อน เพราะการตรวจสอบต้องใช้ความรู้เชิงลึกทางด้าน RDBMS ด้วย

5. การตรวจสอบโปรแกรมประยุกต์และโปรแกรมที่ให้บริการในลักษณะServer (Application Specific Audit) เช่น การตรวจสอบ Web Server IIS บน Microsoft Windows Platform และ การตรวจสอบ Web Server Apache บน Unix/Linux Platform ซึ่งทั้ง 2เป็นโปรแกรม Web Server ยอดนิยมอยู่ในขณะนี้ นอกจากการตรวจสอบ Web Server แล้ว IT Auditor ควรตรวจสอบ Mail Server, FTP Server, LDAP Server, RADIUS Server ตลอดจน DNS Server ซึ่งถือเป็นหัวใจหลักของระบบ หาก DNS Server มีปัญหาจะทำให้ระบบไม่สามารถอ้างอิง Hostname ได้ ซึ่งจะก่อให้เกิดปัญหาใหญ่กับระบบโดยรวม

6. การตรวจสอบกระบวนการบริหารจัดการควบคุมด้านสารสนเทศ (Administrative Control) จากข้อ 1 ถึง ข้อ 5 เป็นการตรวจสอบในมุมมองทางด้านเทคนิค (Technical Control) การตรวจสอบในมุมมองการบริหารจัดการนั้น ได้แก่ การตรวจสอบ Policy, Standard, Guideline และ Procedure ที่องค์กรมีอยู่ว่าครอบคลุม และ มีการปฏิบัติตามหรือไม่ ในขั้นตอนนี้รวมถึงการตรวจสอบว่าองค์กรมีการจัดฝึกอบรมด้านการรักษาความปลอดภัย (Security Awareness Training) หรือไม่ ซึ่งตามปกติควรจะ มีเป็นประจำทุกปี การตรวจสอบการบริหารจัดการนั้นต้องพิจารณาจากโครงสร้างหน่วยงาน, การแบ่งแยกหน้าที่ต่างๆในหน่วยงาน, การจัดทำแผนสำรองฉุกเฉิน และแผน

รับเหตุการณ์ (Business Continuity Planning, Disaster Recovery Planning and Incident Response Procedure) ตลอดจนการควบคุมการเปลี่ยนแปลงระบบงาน (Change Control Management)

7. การตรวจสอบด้านกายภาพ (Physical Control) ได้แก่ การตรวจสอบระบบควบคุมการเข้า-ออกศูนย์คอมพิวเตอร์, การตรวจสอบ Hardware ระบบ Backup/Restore และ ระบบไฟสำรอง เช่น มี UPS เพียงพอหรือไม่ การตรวจสอบอุปกรณ์เฝ้าระวัง เช่น กล้องวงจรปิด (CCTV) เป็นต้น

บทที่ 3
มาตรฐานและทฤษฎีความปลอดภัยเกี่ยวข้อง

3.1 มาตรฐานการจัดการด้านความปลอดภัยของข้อมูล BS7799 และ ISO/IEC17799 (ISO/IEC 17799. 2002.)

BS7799 และ ISO/IEC17799 คือมาตรฐานการจัดการด้านความปลอดภัยของข้อมูล ซึ่งเป็นการรักษาความปลอดภัยของข้อมูลให้แก่องค์กรวิธีหนึ่ง ที่เน้นที่ " ระบบการบริหารจัดการ " ไม่ใช่เน้นที่การใช้เทคโนโลยี Hardware หรือ Software ต่างๆเข้ามาช่วย นั่นหมายความว่า มาตรฐานนี้จะมีข้อกำหนดต่างๆ เพื่อการรักษาความปลอดภัยของข้อมูลครอบคลุมกระบวนการทำงาน ในองค์กรในส่วนที่เกี่ยวข้องกับการนำข้อมูลมาใช้และจัดเก็บข้อมูลทั้งหมด รวมถึงการมีแผนรับมือ เมื่อเกิดเหตุฉุกเฉินขึ้นกับข้อมูล เช่น ไฟฟ้าดับ ฮาร์ดดิสก์เสีย หรือพายุ เพื่อให้องค์กรสามารถ ปฏิบัติการรับมือได้อย่างถูกต้อง เกิดความสูญเสียน้อยที่สุด และสามารถกู้ข้อมูลกลับมาดำเนินงาน ตามปกติได้เร็วที่สุด

ในปัจจุบัน มาตรฐานนี้มีการนำไปใช้งานกันอย่างแพร่หลายทั่วโลก โดยเฉพาะในประเทศอังกฤษ และแถบยุโรปและเป็นที่น่าสนใจว่า ในอนาคตมาตรฐานด้านความปลอดภัยของข้อมูลนี้อาจได้รับการยอมรับและนำไปใช้งานกันอย่างแพร่หลายในประเทศไทย ไม่แพ้ระบบการบริหารจัดการคุณภาพ (ISO9001) ก็เป็นได้ เพราะการพัฒนา IT ที่เจริญรุดหน้าอย่างรวดเร็วและ การดำเนินธุรกิจแบบดิจิตอลที่แพร่หลายอยู่ในประเทศไทย

จุดเด่นที่สำคัญอีกอย่างหนึ่งสำหรับมาตรฐานการจัดการด้านความปลอดภัยของข้อมูลนี้ก็คือ มาตรฐาน BS7799 นี้ได้ถูกปรับปรุงขึ้นเพื่อให้สามารถเข้ากันได้กับมาตรฐาน ISO9001 และ ISO14001 ซึ่งจะทำให้องค์กรที่มี ISO9001 หรือ ISO14001 อยู่แล้ว สามารถใช้ระบบ เอกสารที่องค์กรคุ้นเคยอยู่แล้วนั้นกับมาตรฐาน BS7799 ได้ และยังมีระบบในด้านของการทบทวน โดยผู้บริหาร (Management review) และการตรวจติดตามระบบภายใน (Internal audit) ที่มีแนวปฏิบัติคล้ายคลึงกันอีกด้วย

ความแตกต่างระหว่างมาตรฐาน ISO/IEC17799:2000 และ BS7799-2:2002

ISO/IEC17799:2000 – Code of practice for information security management หรือก็คือ BS7799 part 1 นั้นจะประกอบไปด้วยหัวข้อของการควบคุม ทางด้านการจัดการความปลอดภัยของ

ข้อมูลที่ควรปฏิบัติเพื่อให้เกิดความปลอดภัยต่อข้อมูล ขององค์กรซึ่งจะมีทั้งหมด 127 หัวข้อการควบคุมใน 10 หมวดหลัก

BS7799-2:2002 Information security management systems -- Specification with guidance for use ก็คือ BS7799 part 2 มีเนื้อหา ว่าด้วยการจัดตั้ง " ระบบการจัดการด้านความปลอดภัยของข้อมูล " ขึ้นในองค์กร โดยเริ่มตั้งแต่การริเริ่มทำระบบ การนำไปใช้ การทบทวน การปรับปรุงอย่างสม่ำเสมอ ซึ่งในส่วนนี้จะมีการประยุกต์เพื่อนำแนวคิดของวงล้อ PDCA (Plan-Do-Check-Act) เข้าใช้ในการจัดตั้งและพัฒนาระบบด้วย ในส่วนของเนื้อหาของระบบ ISMS ที่จะจัดตั้ง ขึ้นนั้นก็จะต้องอ้างอิงตามหัวข้อของการควบคุมทั้ง 127 หัวข้อในมาตรฐาน ISO/IEC17799

มาตรฐาน ISO/IEC17799:2000 Code of practice for information security management หัวข้อต่อไปนี้คือ 10 หมวดหมู่หลักที่ครอบคลุมโดยมาตรฐาน ISO/IEC17799

1. Security policy ครอบคลุมถึงเรื่องของนโยบายการจัดการด้านความปลอดภัยของข้อมูลในองค์กร การเล็งเห็น ถึงความสำคัญของนโยบายฯ และการให้การสนับสนุนจากผู้บริหารระดับสูงเพื่อให้มีการนำ นโยบายฯไปใช้อย่างมีประสิทธิภาพ

2. Organizational security ครอบคลุมถึงเรื่องการจัดตั้งหน่วยงานขึ้นเพื่อประสานงานและดำเนินงานด้านการดูแลรักษาความปลอดภัยของข้อมูล

3. Asset classification and control ครอบคลุมถึงเรื่องของการจัดจำแนกประเภทของข้อมูลตามระดับความสำคัญ ควบคุมการเข้าถึง ข้อมูลแต่ละประเภท รวมถึงการควบคุมทรัพย์สินต่างๆขององค์กรที่เกี่ยวกับงานด้าน IT

4. Personnel security ครอบคลุมถึงเรื่องของการให้ความรู้แก่พนักงานถึงภัยคุกคามต่างๆ และแนะนำวิธีการปฏิบัติงานที่ถูกต้องและเหมาะสม เช่น การตั้ง password และใช้งาน password อย่างปลอดภัย การปฏิบัติเมื่อพบสิ่งผิดปกติในระบบ

5. Physical and Environmental security ครอบคลุมถึงการรักษาความปลอดภัยของพื้นที่ทำงาน การควบคุมการเข้า-ออก และการนำสิ่งของ เข้า-ออก เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาตและป้องกันการเสียหาย / สูญหายของทรัพย์สิน

6. Communications and Operations management ครอบคลุมถึงการรักษาความปลอดภัยให้แก่คอมพิวเตอร์ ระบบเครือข่ายและการประมวลผลข้อมูล เช่น การป้องกันไวรัสคอมพิวเตอร์ การทำ Back-up ข้อมูล การจัดการเมื่อเกิดเหตุการณ์ฉุกเฉิน การควบคุมความปลอดภัยของระบบเครือข่าย การกำจัดสื่อบันทึกข้อมูล การควบคุมความปลอดภัยในการใช้งาน E-mail ฯลฯ

7. Access control ครอบคลุมถึงการควบคุมการเข้าถึงข้อมูลและป้องกันการเข้าถึงข้อมูลโดยผู้ไม่ได้รับอนุญาตทั้งจาก การเข้าใช้งานทางคอมพิวเตอร์ภายในบริษัท ทางระบบเครือข่ายและทางระบบการเข้าถึงทางไกล (Remote access)

8. Systems development and maintenance ครอบคลุมถึงการพัฒนาระบบคอมพิวเตอร์ ระบบเครือข่าย Software และ Hardware เริ่มตั้งแต่การจัดซื้อ / จัดจ้าง ติดตั้งระบบ การใช้งานจริง และการบำรุงรักษาอย่างสม่ำเสมอ รวมถึงการควบคุมการใช้รหัสลับ (Cryptographic control)

9. Business continuity management ค รอบคลุมถึงการจัดทำแผนการจัดการให้ธุรกิจดำเนินได้อย่างต่อเนื่อง (Business continuity Plan-BCP) ซึ่งก็คือวิธีปฏิบัติในการรับมือในกรณีที่เกิดความผิดพลาดขึ้นกับระบบ หรือภัยธรรมชาติ เพื่อให้เกิดความเสียหายน้อยที่สุด และเพื่อให้ธุรกิจสามารถฟื้นตัวกลับมา ดำเนินงานตามปกติได้เร็วที่สุด

10. Compliance ครอบคลุมถึงการปฏิบัติงานที่ถูกต้องตามกฎหมาย เช่นการใช้ Software ที่มีลิขสิทธิ์ (License)

มาตรฐาน BS7799-2:2002 Information security management systems

เนื้อหาของมาตรฐาน BS7799-2:2002 จะเกี่ยวข้องกับวิธีการปฏิบัติเพื่อให้เกิด "ระบบการจัดการด้านความปลอดภัยของข้อมูล " (Information security management systems - ISMS) ขึ้นในองค์กร ซึ่งแนวคิดของมาตรฐานส่วนนี้จะเป็นแนวทางสำคัญ สำหรับองค์กรที่ต้องการนำระบบ ISMS ไปปรับใช้เพื่อป้องกันความปลอดภัยให้แก่ข้อมูล ขององค์กร เนื้อหาของมาตรฐาน BS7799-2:2002 แบ่งออกเป็น 7 ส่วนดังนี้

0 Introduction

1. Scope

2. Normative reference

3. Terms and definitions

4. Information security management system

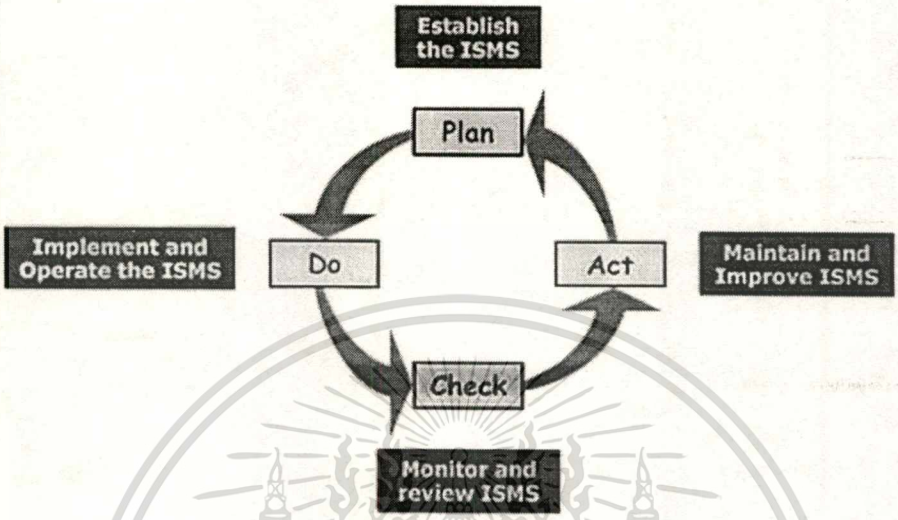
5. Management responsibility

6. Management review of the ISMS

7. ISMS improvement

มาตรฐานนี้ได้ถูกจัดทำขึ้นโดยยึดตามแนวคิดของวงล้อ PDCA (Plan-Do-Check-Act) เพื่อให้เกิดวิธีการปฏิบัติงานที่เป็นระบบ และมีการพัฒนาขึ้นอย่างต่อเนื่อง (Continuous improvement) เริ่มต้นตั้งแต่การจัดตั้ง (Establish) การนำระบบไปใช้ (Implement), การดำเนินงาน

(Operate) การวัดผล (Monitor) การทบทวน (Review) การบำรุงรักษา ระบบ (Maintain) และการปรับปรุงพัฒนาระบบ (Improve) ซึ่งสามารถอธิบายได้ดังรูปที่ 3.1



รูปที่ 3.1 แสดงวงล้อ PDCA

หัวใจสำคัญของการริเริ่มจัดตั้งและการพัฒนาระบบ ISMS อย่างต่อเนื่องที่สำคัญก็คือ การทำการ ตรวจประเมินความเสี่ยง (Risk assessment) และการเลือกวิธีการควบคุม ให้เหมาะสมกับการปฏิบัติงานและระดับความปลอดภัยที่ยอมรับได้ ขององค์กร

3.2 ภัยคุกคาม (Threat) (เรืองไกร รังสิพล. 2544.)

ภัยคุกคาม คือ เหตุการณ์หรือกรณีที่มีโอกาสก่อความเสียหายต่อระบบในรูปแบบการทำลาย การเปิดเผย การเปลี่ยนแปลงข้อมูลและการปฏิเสธการให้บริการของระบบ ผลต่อระบบคอมพิวเตอร์และเน็ตเวิร์คนั้นแบ่งระดับของภัยคุกคามออกไปตามลักษณะของการเข้าถึงและการใช้งานเน็ตเวิร์คออกได้เป็น 4 ระดับ คือ

1. ระดับกายภาพ

คือระดับที่ภัยคุกคามนั้นจะต้องอาศัยการเข้าถึงระบบคอมพิวเตอร์และเน็ตเวิร์คในระดับกายภาพ และทำลายให้เสียหาย เช่น การขโมยเซิร์ฟเวอร์ การตัดสายเคเบิล การลัดวงจร รวมถึงภัยคุกคามที่มาจากธรรมชาติ เช่น น้ำท่วม แผ่นดินไหว ความเสียหายของภัยประเภทนี้จะส่งผลเสียหายต่อระดับกายภาพจริงๆ เช่น เซิร์ฟเวอร์หายไปจริง สายเคเบิลขาดจริง ส่วนใหญ่จะมองเห็นหรือสัมผัสได้ด้วยตาเปล่า

2. ระดับเน็ตเวิร์ค

คือภัยคุกคามที่มีจากการสามารถเข้าถึงเน็ตเวิร์คได้โดยอาศัยช่องทางการสื่อสารที่มีอยู่และใช้การสื่อสารนั้นไปเพื่อทำให้เน็ตเวิร์คเสียหายให้ใช้การไม่ได้ หรือใช้เน็ตเวิร์คไปเพื่อวัตถุประสงค์ในการบุกรุก โดยการกระทำดังกล่าวใช้เทคนิคในระดับเน็ตเวิร์คอาศัยข้อบกพร่องของโปรโตคอล ภัยคุกคามชนิดนี้ไม่จำเป็นต้องเข้าถึงเป้าหมายในระดับกายภาพ ขอให้สามารถเข้าถึงเป้าหมายในแบบลอจิคอลก็เพียงพอ และภัยคุกคามก็จะไม่ผูกติดกับแอพพลิเคชันใดแอพพลิเคชันหนึ่งโดยเฉพาะแต่จะผูกติดกับโปรโตคอลและวิธีการสื่อสารเป็นหลัก

3. ระดับแอพพลิเคชัน

เป็นภัยคุกคามที่เกิดขึ้นโดยตรงต่อแอพพลิเคชันหรือระบบปฏิบัติการ โดยอาศัยความไม่สมบูรณ์ของแอพพลิเคชันใดแอพพลิเคชันหนึ่งโดยเฉพาะมาใช้เป็นช่องทางในการบุกรุกก่อกวนหรือทำให้แอพพลิเคชันนั้นเสียหายไม่สามารถให้บริการได้ เช่น แอพพลิเคชันที่มีการตรวจสอบผู้ใช้ไม่รัดกุมพอ (Weak Authentication) ทำให้แพ็กเกตสามารถเล็ดรอดเข้าไปในระบบได้โดยไม่ต้องป้อนรหัสผ่าน, แอพพลิเคชันที่ตรวจสอบการรับข้อมูลจากผู้ใช้ไม่รัดกุมก็อาจจะถูกผู้ใช้ป้อนข้อมูลที่อยู่นอกเงื่อนไขการตรวจสอบเข้าไป ทำให้แอพพลิเคชันทำงานผิดพลาดหรือหยุดทำงาน (Buffer Overflow Technique) หรือแอพพลิเคชันตัวใดตัวหนึ่งอาจจะซ่อนประตูหลัง (Back Door) ไว้เพื่อให้ผู้อื่นสามารถเข้ามาควบคุมโฮสต์ได้โดยไม่ต้องผ่านการตรวจสอบความปลอดภัย เป็นต้น ภัยคุกคามในระดับแอพพลิเคชันนั้นมีมากมายพอๆกับจำนวนแอพพลิเคชันที่มีให้บริการอยู่ การมีแอพพลิเคชันที่มีระบบรักษาความปลอดภัยบกพร่องให้บริการอยู่ไม่ว่าผู้ใช้จะสามารถเข้าถึงแอพพลิเคชันด้วยวิธีใดเน็ตเวิร์กแบบใด โปรโตคอลใด ก็สามารถเป็นภัยคุกคามต่อระบบได้โดยไม่แตกต่างกัน

4. ระดับผู้ใช้

โดยทั่วไปอาจไม่นึกว่าจะมีภัยคุกคามต่อผู้ใช้ที่ส่งผลกระทบต่อการทำงานของเน็ตเวิร์คได้ แต่จริงๆแล้วในตัวผู้ใช้เองก็มีความเสี่ยงอยู่มากที่ส่งผลต่อการทำงานของเน็ตเวิร์ค เพราะอย่าลืมว่าทุกๆระบบต่างถูกออกแบบมาเพื่อรับใช้มนุษย์อย่างสุดความสามารถ นั่นหมายถึงไม่ว่าระบบที่มีความปลอดภัยสูงสุดอย่างไรก็จะต้องมีผู้ใช้ที่เป็นเจ้าของและสามารถใช้งานได้เสมอ

ภัยคุกคามในระดับผู้ใช้ได้แก่การเปิดเผยความลับของผู้ใช้เอง เช่น การเปิดเผยรหัสผ่านให้แก่ผู้อื่นเข้าไปใช้งาน การไม่รักษาความลับ การจัดเก็บรหัสผ่านไว้อย่างไม่ปลอดภัย หรือการที่ผู้ใช้ไม่ได้บังคับใช้การรักษาความปลอดภัยที่เหมาะสม ผู้ใช้มีความรู้ไม่เพียงพอ ประมาทเลินเล่อ ในกรณีของการบุกรุกจำนวนมากพบว่าเน็ตเวิร์คสามารถบุกรุกได้อย่างง่ายดายเพราะผู้ใช้มีความรู้ไม่เพียงพอ ประมาทเลินเล่อ ในกรณีของการบุกรุกจำนวนมากจะพบว่าเน็ตเวิร์คสามารถบุกรุกได้อย่าง

ง่ายดายเพราะผู้ใช้ไม่รู้ว่าจะจำกัดสิทธิ์การใช้งานอย่างไร จึงเปิดโอกาสให้แพ็กเกตสามารถเข้ามาในระบบและมีสิทธิ์สูงสุดโดยไม่ต้องออกแรง

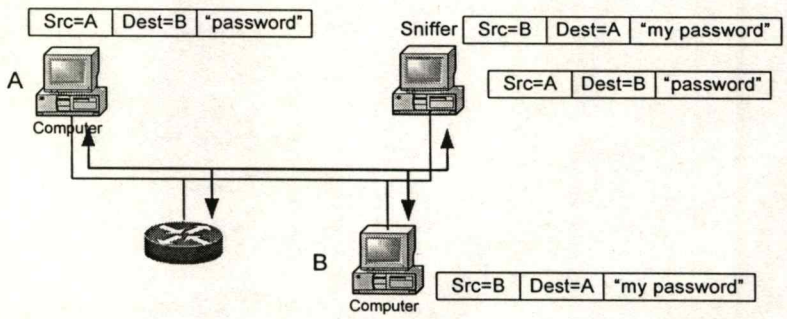
นอกจากตัวผู้ใช้เองแล้วอาจจะมาจากผู้อื่นที่ใช้เทคนิคทางจิตวิทยาหลอกลวงผู้ใช้เพื่อให้ผู้ใช้เปิดเผยความลับ (Social Engineer Technique) เช่น การแสร้งว่าตนเองเป็นเจ้าหน้าที่ของศูนย์คอมพิวเตอร์และทำการหลอกขอรหัสผ่านจากผู้ใช้ หรือหลอกถามข้อมูลจากผู้ใช้โดยทำให้เชื่อว่าเป็นผู้มีอำนาจ เป็นต้น รวมทั้งวิธีการใดๆ ก็ตามที่มีเป้าหมายไปยังผู้ใช้เพื่อให้ได้มาซึ่งสิทธิ์ในการใช้งานของผู้ใช้คนนั้นๆ ภัยในระดับนี้ห่างไกลกับเรื่องเทคนิคทางคอมพิวเตอร์แต่เป็นเรื่องเล่ห์กลเสียมากกว่า

3.3 รูปแบบการโจมตีเครือข่าย (จตุชัย แพงจันทร์ และ อนุโชต วุฒิพรพงษ์. 2546.)

เครือข่ายเป็นเทคโนโลยีที่น่าอัศจรรย์ แต่ก็ยังคงมีความเสี่ยงอยู่มากมายถ้าไม่มีการควบคุมหรือป้องกันที่ดี การโจมตีหรือการบุกรุกเครือข่ายหมายถึงความพยายามที่จะเข้าใช้ระบบ (Access Attack) การแก้ไขข้อมูลหรือระบบ (Modification Attack) การทำให้ระบบไม่สามารถใช้งานได้ (Deny of Service Attack) และการทำให้ข้อมูลเป็นเท็จ (Repudiation Attack) ซึ่งจะกระทำโดยผู้ประสงค์ร้าย ผู้ที่ไม่มีสิทธิ์ หรืออาจเกิดจากความไม่ตั้งใจของผู้ใช้เอง ต่อไปนี้เป็นรูปแบบต่างๆ ที่ผู้ไม่ประสงค์ดีพยายามที่จะบุกรุกเครือข่ายเพื่อลักลอบข้อมูลที่สำคัญหรือเข้าใช้ระบบโดยไม่ได้รับอนุญาต

3.3.1 แพ็กเกตสนิฟเฟอร์

ข้อมูลที่คอมพิวเตอร์ส่งผ่านเครือข่ายนั้นจะถูกแบ่งย่อยเป็นก้อนเล็กๆ ซึ่งจะเรียกว่า แพ็กเกต (Packet) แอพพลิเคชันหลายชนิดจะส่งข้อมูลโดยที่ไม่ได้เข้ารหัส (Encryption) หรือในรูปแบบเคลียร์เท็กซ์ (Clear Text) ดังนั้นข้อมูลอาจถูกคัดลอกและโพรเซสโดยแอพพลิเคชันอื่นก็ได้ ดังแสดงในรูปที่ 3.2



รูปที่ 3.2 แสดงการบุกรุกแบบ Packet Sniffing

เน็ตเวิร์คโปรโตคอลเป็นตัวกำหนดหมายเลขของแต่ละแพ็กเกต ซึ่งเป็นสิ่งที่คอมพิวเตอร์ใช้สำหรับบ่งบอกว่าแพ็กเกตนั้นส่งไปไหนหรือมาจากไหน เนื่องจากโปรโตคอลที่ใช้ส่วนใหญ่ เช่น TCP/IP เป็นโปรโตคอลมาตรฐานและเป็นที่รู้จักกันโดยทั่วไป ทำให้บางกลุ่มพัฒนาแอพพลิเคชันที่สามารถตรวจจับแพ็กเกตที่วิ่งบนเครือข่ายได้ ซึ่งเทคนิคนี้เรียกว่า "แพ็กเกตสนิฟเฟอร์ (Packet Sniffer)" สิ่งที่น่ากลัวจริงๆ ในปัจจุบันนี้คือ โปรแกรมแพ็กเกตสนิฟเฟอร์มีให้ดาวน์โหลดบนอินเตอร์เน็ตมากมาย และผู้ที่ใช้งานไม่จำเป็นต้องมีความรู้เกี่ยวกับคอมพิวเตอร์มากก็สามารถใช้ซอฟต์แวร์เหล่านี้ได้ แพ็กเกตสนิฟเฟอร์เป็นโปรแกรมใช้เน็ตเวิร์คการ์ดในโหมดโพรมิสเชียส์ (Promiscuous mode) ซึ่งในโหมดนี้เน็ตเวิร์คการ์ดจะรับทุกๆ แพ็กเกตที่วิ่งบนสายสัญญาณและส่งต่อไปให้ยังแอพพลิเคชันเพื่อโพรเซสต่อไป

เนื่องจากแอพพลิเคชันส่วนใหญ่จะส่งแพ็กเกตแบบเคลียร์เท็กซ์ แพ็กเกตสนิฟเฟอร์สามารถตรวจจับข้อมูลที่อาจเป็นประโยชน์ได้ เช่น ชื่อผู้ใช้และรหัสผ่าน เป็นต้น ถ้าหากมีการใช้ฐานข้อมูลผ่านเครือข่ายแพ็กเกตสนิฟเฟอร์อาจโจมตีโดยชื่อผู้ใช้และรหัสผ่านที่ตรวจจับได้ก็ได้ สิ่งที่น่ากลัวมากกว่าคือผู้ใช้มักจะใช้ชื่อผู้ใช้ และรหัสผ่านเดิมกับทุกๆ แอพพลิเคชัน ทำให้ผู้บุกรุกสามารถโจมตีแอพพลิเคชันต่างๆ ได้อย่างง่ายดายและอาจทำให้เครือข่ายเกิดความเสียหายมากกว่าที่คิด

3.3.2 ไอพีสปูฟิง

ไอพีสปูฟิง (IP Spoofing) หมายถึง การที่ผู้บุกรุกอยู่นอกเครือข่ายแล้วแกล้งทำเป็นว่าเป็นคอมพิวเตอร์ที่เชื่อถือได้ (Trusted) โดยอาจจะใช้ไอพีแอดเดรสเหมือนกับที่ใช้ในเครือข่าย หรืออาจจะใช้ไอพีแอดเดรสข้างนอกที่เครือข่ายเชื่อว่าเป็นคอมพิวเตอร์ที่เชื่อถือได้หรืออนุญาตให้เข้าใช้ทรัพยากรในเครือข่ายได้ โดยปกติแล้วการโจมตีแบบไอพีสปูฟิงเป็นการเปลี่ยนแปลง หรือเพิ่มข้อมูลเข้าไปในแพ็กเกตที่รับส่งระหว่างไคลเอนท์และเซิร์ฟเวอร์ หรือคอมพิวเตอร์สื่อสารกันในเครือข่าย การที่จะทำอย่างนี้ได้ผู้บุกรุกจะต้องปรับเราท์ติ้งเทเบิ้ลของเราท์เตอร์เพื่อให้ส่งต่อแพ็กเกตไปที่เครื่องของผู้บุกรุก หรืออีกวิธีหนึ่งคือการที่ผู้บุกรุกสามารถแก้ไขให้แอพพลิเคชันส่งข้อมูลที่เป็นประโยชน์ต่อการเข้าถึงแอพพลิเคชันนั้นผ่านทางอีเมล หลังจากนั้นผู้บุกรุกก็สามารถเข้าใช้แอพพลิเคชันได้โดยใช้ข้อมูลดังกล่าว

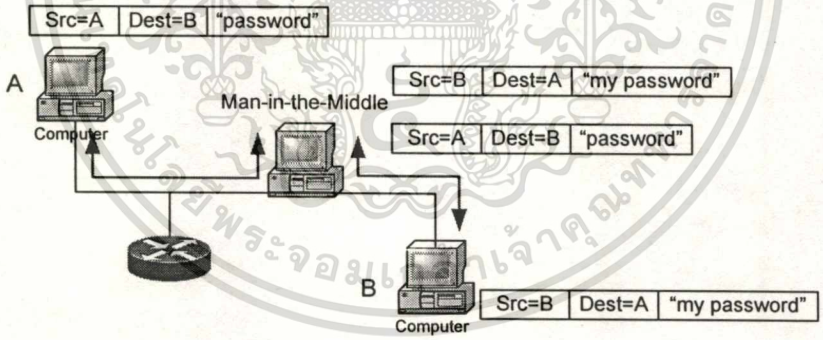
อย่างไรก็ตาม ถ้าผู้บุกรุกสามารถปรับเปลี่ยนเราท์ติ้งเทเบิ้ลเพื่อให้ส่งข้อมูลไปยังเครื่องปลอมได้ผู้บุกรุกสามารถรับส่งข้อมูลกับแอพพลิเคชันนั้นเสมือนเป็นหนึ่งในผู้ใช้ทั่วๆ ไปได้ ไอพีสปูฟิงไม่จำเป็นต้องเป็นคอมพิวเตอร์ที่อยู่นอกเครือข่ายเท่านั้น แต่อาจจะเป็นผู้ใช้ที่อยู่ข้างในที่ไม่มีสิทธิ์ก็ได้ ซึ่งอย่างที่เป็นที่ทราบกันดีว่า การโจมตีเครือข่ายนั้น 90% จะเป็นการโจมตีที่เกิดจากภายในเครือข่ายเอง

3.3.3 การโจมตีรหัสผ่าน

การโจมตีรหัสผ่าน (Password Attacks) หมายถึง การโจมตีที่ผู้บุกรุกพยายามเดารหัสผ่านของผู้ใช้คนใดคนหนึ่ง ซึ่งวิธีการเดานั้นก็มีหลายวิธี เช่น บรู๊ทฟอร์ซ (Brute-Force) โทรจันฮอร์ส (Trojan Horse) ไอพีสปูฟิง แพ็กเกตสนิฟเฟอร์ เป็นต้น การเดาแบบบรู๊ทฟอร์ซ หมายถึง การลองผิดลองถูกรหัสผ่านเรื่อยๆ จนกว่าจะถูก บ่อยครั้งที่การโจมตีแบบบรู๊ทฟอร์ซใช้การพยายามล็อกอินเข้าใช้รีซอร์สของเครือข่าย โดยการทำสำเร็จผู้บุกรุกก็จะมีสิทธิ์เหมือนกับเจ้าของแอ็คเคาท์นั้นๆ ถ้าหากแอ็คเคาท์นี้มีสิทธิ์เพียงพอผู้บุกรุกอาจสร้างแอ็คเค้าท์ใหม่เพื่อเป็นประตูหลัง (Back Door) และใช้สำหรับการเข้าระบบในอนาคตได้

3.3.4 การโจมตีแบบ Man-in-the-Middle

การโจมตีแบบ Man-in-the-Middle นั้นผู้โจมตีต้องสามารถเข้าถึงแพ็กเกตที่ส่งระหว่างเครือข่ายได้ เช่น ผู้โจมตีอาจอยู่ที่ ISP ซึ่งสามารถตรวจจับแพ็กเกตที่รับส่งระหว่างเครือข่ายภายในและเครือข่ายอื่นๆ โดยผ่าน ISP การโจมตีนี้ใช้แพ็กเกตสนิฟเฟอร์เป็นเครื่องมือเพื่อขโมยข้อมูล หรือใช้เซสชั่นเพื่อแอ็กเซสเครือข่ายภายใน หรือวิเคราะห์การจราจรของเครือข่ายผู้ใช้ ดังแสดงในรูปที่ 3.3



รูปที่ 3.3 แสดงการบุกรุกแบบ Man-in-the-Middle Attack

3.3.5 การโจมตีแบบ DOS

การโจมตีแบบดีไนล์ออฟเซอร์วิส หรือ DOS (Denial-of-Service) หมายถึง การโจมตีเซิร์ฟเวอร์โดยการทำให้เซิร์ฟเวอร์นั้นไม่สามารถให้บริการได้ ซึ่งโดยปกติจะทำโดยการใช้รีซอร์ของเซิร์ฟเวอร์จนหมด หรือถึงขีดจำกัดของเซิร์ฟเวอร์ ตัวอย่างเช่น เว็บเซิร์ฟเวอร์ และเอฟทีพีเซิร์ฟเวอร์ การโจมตีจะทำได้โดยการเปิดการเชื่อมต่อ (Connection) กับเซิร์ฟเวอร์จนถึงขีดจำกัดของเซิร์ฟเวอร์ ทำให้ผู้ใช้คนอื่นๆ ไม่สามารถเข้ามาใช้บริการได้ การโจมตีแบบนี้อาจใช้โปรโตคอล

ที่ใช้บนอินเตอร์เน็ตทั่วๆ ไป เช่น TCP (Transmission Control Protocol) หรือ ICMP (Internet Control Message Protocol) การโจมตีแบบดีไนล์ออฟเซอร์วิส เป็นการโจมตีจุดอ่อนของระบบหรือเซิร์ฟเวอร์มากกว่าการโจมตีจุดบกพร่อง (Bug) หรือช่องโหว่ของระบบการรักษาความปลอดภัย อย่างไรก็ตาม การโจมตีอาจทำให้ประสิทธิภาพของเครือข่ายลดลงโดยการส่งแพ็กเกตจำนวนมากเข้าไปในเครือข่าย ซึ่งแพ็กเกตอาจเป็นข้อมูลที่เป็นขยะ

3.3.6 โทรจันฮอร์ส เวิร์ม และไวรัส

คำว่า โทรจันฮอร์ส (Trojan Horse) ในความหมายของคอมพิวเตอร์แล้ว หมายถึงโปรแกรมที่ทำลายระบบคอมพิวเตอร์โดยแฝงมากับโปรแกรมอื่นๆ เช่น เกม สกรีนเซฟเวอร์ เป็นต้น ซึ่งผู้ใช้อาจจะดาวน์โหลดโปรแกรมต่างๆ เหล่านี้มา แต่เมื่อติดตั้งแล้วรันโปรแกรมโทรจันฮอร์สที่แฝงมาด้วยก็จะทำลายระบบคอมพิวเตอร์ เช่น ลงไฟล์ต่างๆ หรืออาจสร้างแบ็คดอร์ให้กับโปรแกรมอื่นเข้ามาทำลายระบบได้

เวิร์ม (Worm) หมายถึง โปรแกรมที่เป็นอันตรายต่อระบบคอมพิวเตอร์ โดยจะแพร่กระจายตัวเองไปยังคอมพิวเตอร์เครื่องอื่นๆ ที่อยู่ในเครือข่าย เวิร์มจะใช้ประโยชน์จากแอพพลิเคชันที่รับส่งไฟล์โดยอัตโนมัติ ส่วนไวรัส (Virus) หมายถึง โปรแกรมที่ทำลายระบบคอมพิวเตอร์ โดยจะแพร่กระจายไปยังโปรแกรมอื่นๆ ที่อยู่ในเครื่องเดียวกัน ไวรัสสามารถทำลายเครื่องได้ตั้งแต่ลงไฟล์ทั้งหมดที่อยู่ในฮาร์ดดิสก์ไปจนถึงแค่เป็นโปรแกรมที่สร้างความรำคาญให้กับผู้ใช้ในเครือข่าย เช่น แค่เปิดวินโดวส์แล้วแสดงข้อความบางอย่าง ไวรัสจริงๆ ไม่สามารถที่จะแพร่กระจายไปยังเครื่องอื่นๆ ด้วยตัวเองได้ แต่การแพร่กระจายไปยังเครื่องอื่นต้องอาศัยโปรแกรมอื่นหรือมนุษย์ เช่น การแชร์ไฟล์โดยใช้แผ่นดิสก์ เป็นต้น

จากคำจำกัดความข้างต้น โทรจันฮอร์ส เวิร์ม และไวรัส จะมีความหมายคล้ายๆ กัน ซึ่งบางคนอาจใช้คำทั้งสามนี้แทนกันก็ได้ แต่จริงๆแล้วทั้งสามคำมีความหมายต่างกัน อย่างไรก็ตาม โปรแกรมทำลายคอมพิวเตอร์ในปัจจุบันอาจเป็นได้ทั้งสามชนิดก็ได้

3.3.7 การบุกรุกแบบอื่นๆ

การแกะรอย (Foot Printing)

วัตถุประสงค์ของการแกะรอย เพื่อที่จะทำให้การบุกรุกของผู้ไม่ประสงค์ดี ได้มาซึ่งข้อมูลที่จำเป็นต่อการบุกรุก เช่น ข้อมูลของเน็ตเวิร์คบล็อก, หมายเลข IP Address และ ชื่อโดเมน ผู้บุกรุกจะค้นหาข้อมูลที่เกี่ยวข้องกับระบบที่เป็นเป้าหมายเพื่อกำหนดขอบเขตของการบุกรุก โดยการระบุรูปแบบของการแกะรอยที่กระทำโดยผู้บุกรุกนั้น เป็นสิ่งที่ยากในการทำการตรวจสอบโดยผู้ดูแลระบบ เทคโนโลยีและข้อมูลสำคัญที่ผู้บุกรุกต้องการค้นหา

การสแกนเพื่อตรวจสอบ (Scanning)

วัตถุประสงค์ของการทำการสแกน เพื่อที่จะค้นหาเครื่องคอมพิวเตอร์ที่เปิดให้บริการอยู่ในระบบ นอกจากนี้ยังรวมไปถึงการค้นหาพอร์ตที่เครื่องคอมพิวเตอร์เปิดใช้งานอยู่ ผู้บุกรุกจะอาศัยข้อมูลที่ได้สแกน มาวิเคราะห์เพื่อหาช่องโหว่ของระบบที่อาจจะเปิดไว้

การรวบรวมรายละเอียด (Enumeration)

วัตถุประสงค์ของการรวบรวมรายละเอียด ก็เพื่อที่จะเก็บรายละเอียดของระบบคอมพิวเตอร์เป้าหมาย เพื่อที่จะช่วยทำให้ผู้บุกรุกเพิ่มโอกาสในการทำการบุกรุกได้สำเร็จ จากข้อมูลของช่องโหว่ต่างๆ ที่อาจจะถูกเปิดอยู่ โดยสามารถแบ่งข้อมูลที่ผู้บุกรุกส่วนใหญ่ต้องการเป็นกลุ่มๆ ดังนี้ รายชื่อทรัพยากรในเน็ตเวิร์ค รายชื่อแอคเคานต์ของผู้ใช้งาน และชื่อกลุ่มต่างๆ รายชื่อแอปพลิเคชั่นและแบนเนอร์ของแอปพลิเคชั่น

การยกระดับให้มีสิทธิเท่าเทียมกับผู้ดูแลระบบ (Escalating Privilege)

จุดประสงค์ที่ผู้บุกรุกต้องการคือต้องการที่จะยกระดับตัวเองให้มีสิทธิเท่าเทียมกับผู้ดูแลระบบ เพราะในบางครั้งระบบปฏิบัติการที่มีการรักษาความปลอดภัยที่ดี จะมีการกำหนดสิทธิในการเข้าถึงข้อมูลของผู้ใช้งานแต่ละคนให้อยู่ในระดับที่แตกต่างกัน การที่จะสามารถเข้าถึงข้อมูลทุกส่วนได้ จะมีเพียงผู้ดูแลระบบเท่านั้น และในบางระบบ เช่น ระบบฐานข้อมูล จะมีการรักษาความปลอดภัยของตัวเองโดยผู้ใช้งานที่สามารถเข้าถึงฐานข้อมูลทั้งหมดได้ก็คือ Database Administrator ของระบบฐานข้อมูลนั้น ในขณะที่ผู้ใช้งานอื่นจะได้รับอนุญาตให้ใช้งานตามที่ถูกกำหนดไว้เท่านั้น ดังนั้นสิทธิในการเข้าถึงข้อมูลในระดับผู้ดูแลระบบ จึงเป็นสิ่งที่ผู้บุกรุกปรารถนามาก

วิธีการที่ผู้บุกรุกใช้ในการได้มาซึ่งสิทธิของผู้ดูแลระบบ ผู้บุกรุกจะใช้ช่องโหว่ของระบบปฏิบัติการแอปพลิเคชั่น โดยใช้เทคนิคการทำให้ Buffer ของโปรแกรมล้นและทำงานผิดพลาด แล้วอาศัยชุดคำสั่งเพื่อทำงานด้วยสิทธิของผู้ดูแลระบบ เหตุการณ์ที่ทำให้เกิดการล้นของข้อมูลเกิดจากขนาดของ Buffer ถูกเรียกว่าการทำ Buffer Over Flow

การวางกับดักเพื่อดักจับรหัสผ่าน (Password Trojan) เป็นการสร้างโปรแกรมที่รอให้ผู้ดูแลระบบมา Execute และหลอกถามรหัสผ่าน ผู้ดูแลระบบที่ขาดประสบการณ์อาจหลงกลไป Execute เข้า โปรแกรมจะทำงานโดยสร้าง Prompt ของการใส่รหัสผ่าน หากผู้ดูแลระบบหลงกลใส่รหัสของตนไป โปรแกรมที่ผู้บุกรุกสร้างไว้ก็จะส่งรหัสผ่านไปยังปลายทางที่ผู้บุกรุกต้องการ เช่น ส่ง Email ไปยัง Email ของผู้บุกรุก เป็นต้น

การถอดรหัสข้อมูลเพื่อหารหัสผ่าน (Password Cracking) เป็นการใช้โปรแกรมถอดรหัสเพื่อถอดรหัสของแฟ้มข้อมูลสำคัญที่เก็บรหัสผ่านของผู้ดูแลระบบ

การขโมยข้อมูลเพิ่มเติม (Pilfering)

เมื่อผู้บุกรุกสามารถยกระดับของตนเองให้ได้รับสิทธิในการเข้าถึงข้อมูลที่มีความสำคัญแล้ว นั่นก็หมายความว่าเกราะป้องกันข้อมูลที่ถูกป้องกันไว้ได้ถูกทำลายลง ผู้บุกรุกก็อาจจะมองหาช่องทาง เพื่อจะบุกรุกไปยังระบบอื่นต่อไป โดยใช้สิทธิในการเข้าถึงแฟ้มข้อมูลสำคัญ ซึ่งผู้บุกรุกสามารถค้นหาข้อมูลได้ไม่ยาก ยกตัวอย่างเช่น การดูข้อมูลใน Registry, การสำรวจ Configuration Files ต่างๆ

การปิดบัง อำพรางตัว (Covering Tracks)

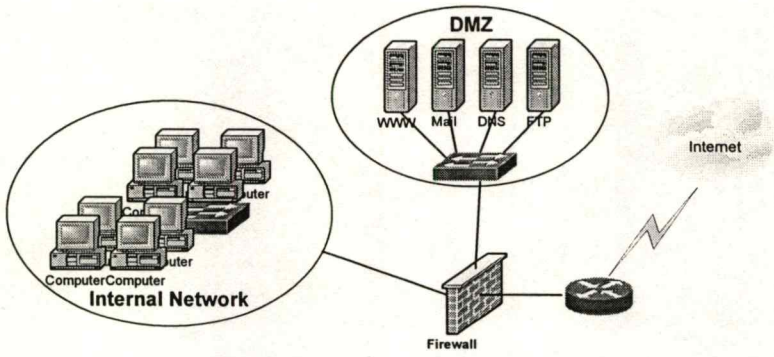
เป็นวิธีการซ่อนตัวที่ทำโดยผู้บุกรุกทำเพื่อหลีกเลี่ยงการตรวจพบจากผู้ดูแลระบบตัวจริง ทำให้ผู้ดูแลระบบที่ขาดประสบการณ์ ไม่ทราบถึงการบุกรุกที่ถูกกระทำไปแล้ว โดยผู้บุกรุกจะใช้การลบ แก้ไข เปลี่ยนแปลง ข้อมูลที่บ่งบอกถึงการบุกรุก เช่น Log Files ต่างๆ

3.4 เทคโนโลยีการรักษาความปลอดภัย (เรืองไกร รังสิพล. 2545.)

ถึงแม้ว่าการปกป้องข้อมูลเป็นสิ่งที่มีลำดับความสำคัญสูงสุด แต่การรักษาเครือข่ายให้ทำงานอย่างถูกต้องก็เป็นปัจจัยที่สำคัญในการปกป้องข้อมูลที่อยู่ในเครือข่ายนั้น ถ้ามีช่องโหว่ของระบบเครือข่ายที่อนุญาตให้โจมตีได้ ความเสียหายที่เกิดขึ้นอาจใช้ทั้งเวลาและความพยายามอย่างมากที่จะทำให้ระบบกลับมาทำงานได้เหมือนเดิม ในหัวข้อต่อไปนี้จะแสดงเทคโนโลยีที่ใช้สำหรับการป้องกันและรักษาความปลอดภัยทั้งระบบเครือข่ายเอง และข้อมูลที่จัดเก็บและรับส่งผ่านเครือข่าย

3.4.1 ไฟร์วอลล์

เหตุผลหลักที่มีการใช้ไฟร์วอลล์ (Firewall) ก็เพื่อให้ผู้ใช้ที่อยู่ภายในสามารถใช้บริการเครือข่ายภายในได้อย่างเต็มที่ และใช้บริการเครือข่ายภายนอก เช่น อินเตอร์เน็ต ในขณะที่ไฟร์วอลล์จะป้องกันไม่ให้ผู้ใช้ภายนอกเข้ามาใช้บริการเครือข่ายที่อยู่ข้างในได้ รูปที่ 3.3 แสดงการติดตั้งไฟร์วอลล์เพื่อเชื่อมต่อเครือข่ายส่วนบุคคลกับเครือข่ายอินเตอร์เน็ต จากรูปจะเห็นได้ว่าแพ็กเกตที่วิ่งระหว่างเครือข่ายภายในและอินเตอร์เน็ตต้องผ่านไฟร์วอลล์เท่านั้น ดังนั้นไฟร์วอลล์จึงสามารถควบคุมการใช้เครือข่ายได้โดยอนุญาตหรือไม่อนุญาตให้แพ็กเกตผ่านได้ ซึ่งแพ็กเกตที่อนุญาตให้ผ่านหรือไม่นี้จะขึ้นอยู่กับนโยบายการรักษาความปลอดภัย (Security Policy) ของเครือข่าย ไฟร์วอลล์เป็นระบบที่บังคับใช้นโยบายการรักษาความปลอดภัยระหว่างเครือข่าย โดยหลักการแล้วไฟร์วอลล์จะทำงานอยู่ 2 กลไก คืออนุญาตหรือไม่อนุญาตให้แพ็กเกตผ่าน การติดตั้ง Firewall ในเน็ตเวิร์ค ดังแสดงในรูปที่ 3.4



รูปที่ 3.4 แสดงการใช้ไฟร์วอลล์ในระบบเน็ตเวิร์ค

ถ้าเครือข่ายองค์กรเชื่อมต่อโดยตรงกับอินเตอร์เน็ตโดยที่ไม่มีไฟร์วอลล์ เป็นการเปิดช่องโหว่ให้เครือข่ายสามารถถูกโจมตีหรือบุกรุกได้อย่างง่ายดาย ตัวอย่างเช่น สมมติว่าเครือข่ายมีโฮสต์หรือเซิร์ฟเวอร์เป็นร้อยๆ เครื่อง ถ้าผู้บุกรุกเครือข่ายสามารถบุกรุกเข้าเครื่องใดเครื่องหนึ่งได้ ต่อไปก็ไม่เป็นการยากที่จะบุกรุกเข้าไปยังเครื่องอื่นๆ การติดตั้งไฟร์วอลล์จะเป็นการป้องกันผู้บุกรุกได้ในระดับหนึ่ง

ประเภทของไฟร์วอลล์

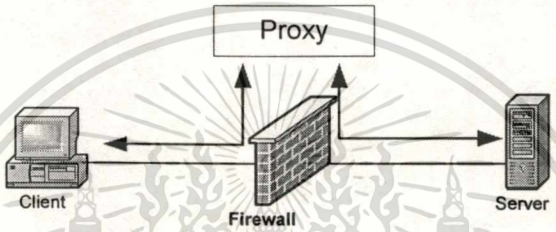
หากจะทำการจำแนกไฟร์วอลล์โดยการใช้ลักษณะการทำงานเป็นเกณฑ์แล้ว สามารถแบ่งไฟร์วอลล์ได้เป็น 3 ประเภท คือ

1. Application Layer Firewall (Proxy)
2. Packet Filtering Firewall
3. Circuit Level Firewall (Stateful Inspection Firewall)

แอพพลิเคชันเลเยอร์ไฟร์วอลล์ (Application Layer Firewall)

ไฟร์วอลล์ที่ทำงานในระดับแอพพลิเคชันเลเยอร์ (Application Layer Firewall) นั้นบางทีก็เรียกว่า พร็อกซี่ (Proxy Firewall) คือโปรแกรมที่รันบนระบบปฏิบัติการทั่วๆไป เช่น วินโดวส์เซิร์ฟเวอร์หรือยูนิกซ์ หรืออาจจะเป็นฮาร์ดแวร์ที่ติดตั้งซอฟต์แวร์พร้อมใช้งานแล้วก็ได้ ไฟร์วอลล์จะมีเน็ตเวิร์คการ์ดหลายการ์ดเพื่อสำหรับเชื่อมต่อกับเครือข่ายต่างๆ นโยบายการรักษาความปลอดภัยจะเป็นสิ่งที่กำหนดว่าทราฟิกใดสามารถถ่ายโอนระหว่างเครือข่ายใดได้บ้าง ถ้านโยบายนั้นจะถูกบังคับใช้โดยพร็อกซี่ในระดับแอพพลิเคชั่นนั้นทุกๆ โปรโตคอลที่อนุญาตให้ผ่านได้จะต้องมีพร็อกซี่สำหรับโปรโตคอลนั้น พร็อกซี่ที่ดีที่สุดนั้นจะเป็นพร็อกซี่ที่ออกแบบมาสำหรับจัดการกับโปรโตคอลนั้นโดยเฉพาะ

สำหรับไฟร์วอลล์ที่ทำงานในระดับแอพพลิเคชันนั้น ทุกๆการเชื่อมต่อจะสิ้นสุดที่ไฟร์วอล์ จากรูปที่ 3.5 การเชื่อมต่อจะเริ่มจากไคลเอนท์การส่งการร้องขอไปยังไฟร์วอลล์ หลังจากนั้นไฟร์วอลล์ก็จะตรวจสอบกับนโยบายรักษาความปลอดภัยว่าจะให้อนุญาตทราพิกนี้หรือไม่ ถ้าอนุญาตไฟร์วอลล์จะสร้างการเชื่อมต่อกับเซิร์ฟเวอร์แทนไคนเอนท์เอง นอกจากไฟร์วอลล์สามารถควบคุมการเชื่อมต่อจากภายในไปภายนอกได้แล้ว ไฟร์วอลล์ยังสามารถควบคุมการเชื่อมต่อจากภายนอกมาภายในได้เช่นกัน ดังนั้นไฟร์วอลล์จึงสามาถป้องกันการโจมตีเครือข่ายในระดับแอพพลิเคชันได้ อย่างไรก็ตามตัวไฟร์วอลล์เองจะต้องมีความปลอดภัยจากการโจมตีด้วย



รูปที่ 3.5 แสดงไฟร์วอลล์ระดับแอพพลิเคชัน

ไฟร์วอลล์ที่ทำงานในระดับแอพพลิเคชันปัจจุบันส่วนใหญ่จะมีพร็อกซี่สำหรับโปรโตคอลที่นิยมใช้ เช่น HTTP SMTP FTP และ Telnet เป็นต้น ถ้าโปรโตคอลไหนไม่มีพร็อกซี่ก็ไม่สามารถผ่านไฟร์วอลล์ได้ นอกจากนี้ไฟร์วอลล์ประเภทนี้ยังสามารถซ่อนแอดเดรสหรือหมายเลขไอพีของระบบภายในได้ เนื่องจากการเชื่อมต่อทั้งหมดจะสิ้นสุดที่ไฟร์วอลล์ ดังนั้นเครื่องที่อยู่ภายนอกจะมองเห็นเฉพาะหมายเลขไอพีของไฟร์วอลล์เท่านั้น ถ้าผู้บุกรุกไม่รู้โครงสร้างภายในโอกาสที่จะเจาะระบบได้ก็น้อยลง

ข้อดีของการใช้งานพร็อกซี่

1. สามารถควบคุมการติดต่อสื่อสารระหว่างอินเตอร์เน็ตกับเน็ตเวิร์คภายในให้อยู่ในระดับแอพพลิเคชันเท่านั้น ตัดขาดการติดต่อโดยตรงในระดับเน็ตเวิร์คเลเยอร์ระหว่างอินเตอร์เน็ตกับเน็ตเวิร์คภายในออกจากกันอย่างเด็ดขาด ทำให้ลดความเสี่ยงต่อการถูกคุกคามจากการสแกน การเจาะระบบ การก่อกวนโดยใช้เทคนิคในระดับเน็ตเวิร์คเลเยอร์ที่จะเข้ามายังเน็ตเวิร์คภายในได้อย่างเด็ดขาด

2. สามารถเพิ่มเติมหน้าที่การทำงานอย่างอื่นเข้าไปในพร็อกซี่ได้ เช่นการทำเว็บพร็อกซี่นอกจากจะเป็นตัวกลางในการติดต่อแล้ว ยังสามารถควบคุมไม่ให้เว็บบราวเซอร์ติดต่อกับเว็บไซต์ที่ไม่ต้องการได้อีกด้วย โดยการกำหนดรายชื่อเว็บไซต์เหล่านั้นไว้ในพร็อกซี่

3. สามารถทำการแคชข้อมูลเก็บไว้ในตัวพร็อกซี่ สำหรับข้อมูลใดที่มีการเรียกใช้ซ้ำบ่อยๆ ก็ไม่จำเป็นต้องไปอ่านจากเซิร์ฟเวอร์ใหม่ทุกครั้ง แต่ส่วนนี้จะใช้งานกับข้อมูลที่เป็นสแตติคเท่านั้น ข้อมูลที่มีการเปลี่ยนแปลงตลอดเวลาเป็นไดนามิคอาจจะไม่สามารถแคชได้

4. ทำให้ผู้ใช้มีการใช้แบนด์วิดธ์ร่วมกันได้อย่างมีประสิทธิภาพ โดยเฉพาะเมื่อใช้ร่วมกับการแคชที่มีอยู่ในพร็อกซี่ ทำให้ช่วยประหยัดการใช้งานแบนด์วิดธ์ไปได้มาก

5. สามารถเพิ่มเติมการตรวจสอบผู้ใช้ (Authenticate) เข้าไปเป็นหน้าที่หนึ่งของพร็อกซี่ได้ โดยการอนุญาตให้สามารถใช้งานพร็อกซี่นั้นจะขึ้นอยู่กับสิทธิ์การใช้งานที่ผู้ใช้มีอยู่ ทำให้สามารถควบคุมการใช้งานได้ใกล้ชิดมากขึ้นกว่าการควบคุมโดยพิจารณาจาก IP Address ของโฮสต์เพียงอย่างเดียว

6. สามารถทำการกลั่นกรองเนื้อหาของข้อมูลได้ (Content Filtering) ทำให้สามารถนำมาเป็นเงื่อนไขในการอนุญาตให้ข้อมูลเหล่านั้นผ่านเข้าออกได้ เช่น เว็บพร็อกซี่สามารถตรวจสอบเนื้อหาของเว็บไซต์ที่ผู้ใช้เข้าไปดู หากปรากฏว่ามีข้อความที่ไม่เหมาะสมพร็อกซี่ก็จะสามารถดร็อปเซสชั่นที่ผู้ใช้ขอมาได้ หรือกรณีที่เป็นอีเมล์พร็อกซี่ก็จะสามารถตรวจสอบเนื้อหาในอีเมล์ได้ว่ามีข้อความใดที่ไม่เหมาะสมหรือไม่ และอาจจะครอบคลุมถึงการตรวจสอบหาไวรัสที่แนบมากับจดหมายได้อีกด้วย

ข้อเสียของการใช้งานพร็อกซี่

1. ขึ้นอยู่กับแอพพลิเคชัน หาแอพพลิเคชันไม่รองรับการสื่อสารโดยผ่านพร็อกซี่ก็ไม่สามารถใช้งานได้

2. ไม่สามารถใช้งานกับแอพพลิเคชันที่ต้องการการสื่อสารโดยตรงแบบ end-to-end ซึ่งแพ็คเก็ตจะต้องมาจากโฮสต์ปลายทางทั้งคู่เท่านั้น ผ่านตัวกลางไม่ได้

3. เสี่ยงต่อการละเมิดความเป็นส่วนบุคคล (Privacy) เนื่องจากข้อมูลทั้งหมดที่สื่อสารจะต้องผ่านพร็อกซี่ก่อนเสมอ และพร็อกซี่ก็มีความสามารถที่จะเก็บข้อมูลเหล่านั้นไว้ตรวจสอบได้ หากมีผู้นำข้อมูลเหล่านั้นไปวิเคราะห์จะสามารถทราบการใช้งานหรืออาจจะทราบข้อมูลทั้งหมดของผู้ใช้ได้

4. เนื่องจากลักษณะของแต่ละแอพพลิเคชันนั้นจะแตกต่างออกไป ดังนั้นพร็อกซี่ของแต่ละแอพพลิเคชันจึงมีหน้าที่เฉพาะแอพพลิเคชันนั้นๆ ไม่สามารถใช้ร่วมกันได้ หากโฮสต์ที่อยู่หลังพร็อกซี่มีการใช้งานหลายแอพพลิเคชัน ก็จะต้องมีพร็อกซี่จำนวนมากเปิดให้บริการตามจำนวนแอพพลิเคชันนั้นๆ

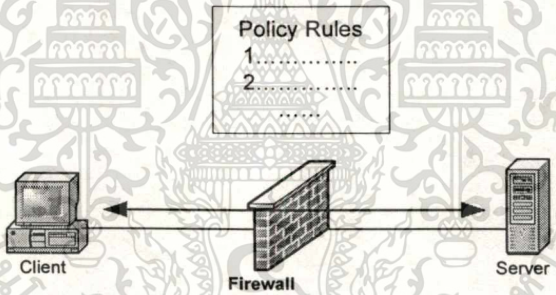
5. ความสามารถในการประมวลผลของโฮสต์ที่ทำหน้าที่พร็อกซี่อาจจะเป็นคอขวดของระบบได้เพราะการสื่อสารทั้งหมดของไคลเอนต์และเซิร์ฟเวอร์จะถูกรวมศูนย์ที่พร็อกซี่ก่อนเสมอ

แทนที่จะกระจายไปยังไคลเอนต์และเซิร์ฟเวอร์ ปัญหาลักษณะนี้จะสามารถพบได้เมื่อมีไคลเอนต์จำนวนมากๆ

6. เนื่องจากพร็อกซี่เป็นแอพพลิเคชันชนิดหนึ่งเช่นกัน การติดต่อกับในเน็ตเวิร์คจะอาศัยระบบปฏิบัติการเป็นหลัก จึงมีความสามารถในการป้องกันตัวเองต่ำกว่าไฟร์วอลล์ทั่วไป ตัวพร็อกซี่เองจึงมีความเสี่ยงต่อการถูกโจมตีได้มาก และเปราะบางต่อการ DoS ด้วยเทคนิคในระดับเน็ตเวิร์ค ซึ่งอาจจะส่งผลให้พร็อกซี่อาจจะหยุดทำงานลงได้โดยง่าย

แพ็กเกตฟิลเตอร์ริ่งไฟร์วอลล์ (Packet Filtering Firewall)

แพ็ตเก็ตฟิลเตอร์ริ่งไฟร์วอลล์ (Packet Filtering Firewall) อาจเป็นได้ทั้งซอฟต์แวร์หรือฮาร์ดแวร์ที่ทำหน้าที่กรองแพ็กเกตที่ผ่านไฟร์วอลล์โดยใช้นโยบายการรักษาความปลอดภัยที่กำหนดไว้ แพ็กเกตฟิลเตอร์ริ่งไฟร์วอลล์นั้นจะอนุญาตให้มีการเชื่อมต่อโดยตรงระหว่างไคลเอนท์และเซิร์ฟเวอร์ ดังนั้นไฟร์วอลล์ประเภทนี้จะทำงานค่อนข้างเร็วกว่าแบบแอพพลิเคชันไฟร์วอลล์ เนื่องจากไม่ต้องสร้างคอนเน็กชันใหม่ ดังแสดงในรูปที่ 3.6



รูปที่ 3.6 แสดงแพ็กเกตฟิลเตอร์ริ่งไฟร์วอลล์

ไฟร์วอลล์ชนิดนี้โดยทั่วไปจะเรียกว่า Screening Router เพราะว่าเป็นการนำเราท์เตอร์ทั่วไปที่มีความสามารถกำหนดแอคเซสรูลได้มาดัดแปลงใช้ในการควบคุมทราฟฟิค ซึ่งการกำหนดแอคเซสรูลของทราฟฟิคทำได้โดยพิจารณาจากข้อมูลแต่ละแพ็คเก็ต แต่เนื่องจากเราท์เตอร์เป็นอุปกรณ์พื้นฐานจากการทำงานอินเตอร์เน็ตเลเยอร์ ทำหน้าที่เราท์แพ็กเกตเป็นหลักโดยพิจารณาจาก IP Address และทำการเราท์ไปทีละแพ็กเกต ดังนั้นจึงสามารถควบคุมทราฟฟิคได้ดีในระดับ IP คือดูจาก IP Address ทั้งต้นทางและปลายทางเท่านั้น สำหรับข้อมูลในส่วนของโปรโตคอลในเลเยอร์สูงขึ้นไป เนื่องจากเราท์เตอร์มีขีดจำกัดในการรับรู้ข้อมูลในเลเยอร์สูงขึ้นไปจึงทำให้สามารถควบคุมทราฟฟิคโดยระบุเงื่อนไขของโปรโตคอลในทรานสปอร์ตเลเยอร์ได้อย่างจำกัด คือจะสามารถทำการควบคุมทราฟฟิคได้เฉพาะเมื่อข้อมูลในทรานสปอร์ตเลเยอร์นั้นสามารถบรรจุได้ใน

แพ็กเกตเดียว หากมีการแฟรกเมนต์และต้องเชื่อมโยงกันระหว่างหลายแพ็กเกตแล้ว เราท์เตอร์จะไม่สามารถรับรู้การเชื่อมโยงนั้นได้

เราท์เตอร์โดยทั่วไปจะมีหลักการทำงานคือ เมื่อได้รับแพ็กเกตมาก็จะตรวจสอบหมายเลขไอพีของเครื่องปลายทาง หลังจากนั้นเราท์เตอร์ก็จะตรวจเช็คเราท์ติ้งเทเบิ้ล (Routing Table) เพื่อค้นหาเราท์เตอร์หรือโฮสต์ปลายทางที่จะส่งต่อไป ส่วนขั้นตอนการกรองแพ็กเกตของไฟร์วอลล์นั้นจะทำก่อนที่จะส่งผ่านแพ็กเกตนี้ แพ็กเกตจะถูกกรองตามรายการควบคุมการเข้าถึง (Access Control List หรือ ACL) แต่ละรายการของ ACL จะประกอบด้วยฟิลด์ของเฮดเดอร์ของไอพีแพ็กเกตและการอนุญาตหรือไม่อนุญาตให้ผ่าน

หากแพ็กเกตที่เข้ามาไม่ตรงกับกฎข้อใดเลย ไฟร์วอลล์จะทำอย่างไรกับแพ็กเกตนี้ มีอยู่ 2 ประเด็นที่ไฟร์วอลล์จะทำคือ

- ถ้าไม่มีกฎข้อไหนที่ไม่ได้เขียนว่าอนุญาตให้ถือว่าห้าม
- ถ้าไม่มีกฎข้อไหนที่ไม่ได้เขียนว่าห้ามให้ถือว่าอนุญาต

โดยส่วนใหญ่แล้วไฟร์วอลล์จะใช้หลักการในข้อแรกคือ ถ้าไม่ได้ระบุอย่างชัดว่าอนุญาตให้ถือว่าห้าม ข้อมูลที่ใช้สำหรับการพิจารณาว่าจะให้แพ็กเกตผ่านหรือไม่นั้น มาจากข้อมูลในส่วนหัวของแพ็กเกต IP ภายในของแต่ละแพ็กเกตนั้นจะประกอบไปด้วยข้อมูลสำคัญซึ่งสามารถนำมาใช้เพื่อเป็นเงื่อนไขสำหรับการควบคุมทราฟฟิคโดยไฟร์วอลล์ดังนี้

1. หมายเลขไอพีต้นทาง (Source IP Address) เพื่อใช้ในการพิจารณาต้นทางของข้อมูลว่าอยู่ในเงื่อนไขที่อนุญาตหรือไม่
2. หมายเลขไอพีปลายทาง (Destination IP Address) เพื่อใช้ในการพิจารณาปลายทางของข้อมูลว่าอยู่ในเงื่อนไขที่อนุญาตหรือไม่
3. ประเภทของโปรโตคอล เช่น TCP UDP ICMP เป็นต้น ระบุโปรโตคอลที่อาศัยอยู่ใน IP Datagram ที่กำลังพิจารณา
4. หมายเลขพอร์ตต้นทาง (Source Port) ระบุพอร์ตต้นทางสำหรับโปรโตคอลที่ใช้พอร์ต คือ TCP และ UDP ซึ่งข้อมูลพอร์ตต้นทางนี้ส่วนใหญ่มักจะมีความสำคัญในลำดับรองลงไป และไม่ถูกนำมาใช้ควบคุมทราฟฟิคมากนัก
5. หมายเลขพอร์ตปลายทาง (Destination Port) ระบุพอร์ตปลายทางที่แพ็กเกตนี้ต้องการติดต่อด้วยสำหรับโปรโตคอลที่ใช้พอร์ต คือ TCP และ UDP
6. ข้อมูลสำคัญอื่นๆ ตามลักษณะของโปรโตคอล เช่น TCP Flag, ICMP Massage เป็นต้น

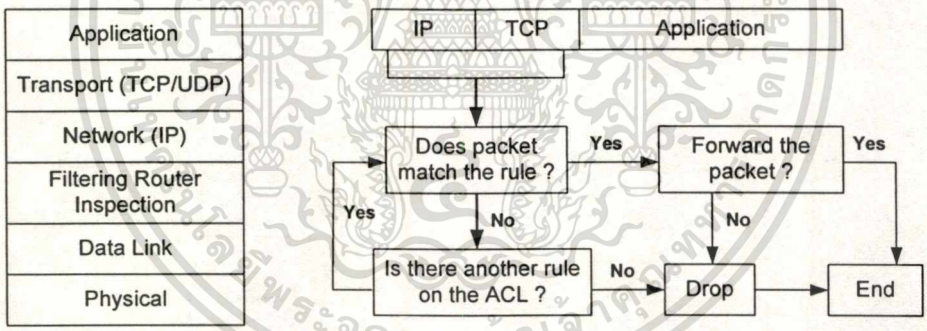
ข้อมูลทั้ง 6 ส่วนนี้จะมีได้อย่างครบถ้วนสมบูรณ์ก็ต่อเมื่อแพ็กเกตนั้นมีข้อมูลครบถ้วนทั้งหมดของ IP Datagram หากข้อมูลแพ็กเกตนั้นเป็นแฟรกเมนต์อาจจะทำให้ข้อมูลในส่วนที่ 3 เป็น

ต้นไป ซึ่งอยู่ในโปรโตคอลที่อยู่เลเยอร์สูงกว่า IP ไม่สมบูรณ์ อย่างไรก็ตามไฟร์วอลล์ส่วนใหญ่ทำการติดตั้งใช้งานใน LAN ซึ่งมีขนาดของแพ็คเก็ตที่ใหญ่พอสำหรับรองรับ IP ดาต้าแกรมได้ทั้งหมด จึงมักไม่ค่อยพบปัญหาแต่อย่างใดยกเว้นมีการแฟรกเมนต์โดยความประสงค์ของ IP เอง

นโยบายการรักษาความปลอดภัยของไฟร์วอลล์

สิ่งสำคัญที่สุดสำหรับการใช้งานไฟร์วอลล์คือ การกำหนดนโยบายการรักษาความปลอดภัย (Network Security Policy) ถึงแม้ว่าไฟร์วอลล์จะมีประสิทธิภาพและมีความปลอดภัยมากแค่ไหนก็ตาม แต่ถ้ามีนโยบายการรักษาความปลอดภัยที่หละหลวมไฟร์วอลล์ก็ไม่มีประโยชน์มากนัก ดังนั้นก่อนที่จะติดตั้งไฟร์วอลล์ควรกำหนดนโยบายการรักษาความปลอดภัยที่สามารถควบคุมหรือป้องกันทราฟิกที่อาจมีผลกระทบต่อการใช้งานเครือข่ายให้มากที่สุด เมื่อกำหนดนโยบายแล้ว ขั้นตอนต่อไปคือ นำนโยบายนี้ไปบังคับใช้ในไฟร์วอลล์กฎที่บังคับใช้นโยบายการรักษาความปลอดภัยในไฟร์วอลล์นั้นจะเรียกว่า ACL (Access Control List)

การตรวจสอบกฎใน ACL นั้นส่วนใหญ่เป็นแบบ First Match โดยไฟร์วอลล์จะตรวจสอบกฎทีละข้อตามลำดับจนกระทั่งพบกับกฎที่ตรงกัน ดังแสดงในรูปที่ 3.7



รูปที่ 3.7 แสดงขั้นตอนการตรวจสอบแพ็กเกตก่อนส่งต่อของแพ็กเกตฟิลเตอร์ริ่งไฟร์วอลล์

ข้อดีของ Screening Router

1. ราคาถูกเพราะเป็นคุณสมบัติที่มักจะมีในเราท์เตอร์อยู่แล้ว อาศัยเพียงการกำหนดแอคเซสรูลที่เหมาะสมเท่านั้น หากยังไม่มีไฟร์วอลล์อยู่เลย ก็สามารถใช้เพื่อช่วยป้องกันเน็ตเวิร์คภายในได้ดีพอสมควรในระดับหนึ่ง

2. หากเน็ตเวิร์คภายในไม่ใหญ่มาก และมีการใช้งานอินเตอร์เน็ตอย่างจำกัด ก็สามารถใช้ทดแทนไฟร์วอลล์ได้ทันที

3. การใช้ Screening Router ควบคู่กับไฟร์วอลล์จะเป็นการแบ่งเบาภาระของไฟร์วอลล์ได้

มากหากทำการกำหนดแอคเซสรูลได้อย่างสอดคล้องแล้ว จะทำให้มีการป้องกันที่เข้มแข็ง

4. การป้องกันบางประเภทไม่สามารถป้องกันได้โดยไฟร์วอลล์ จะต้องทำโดยการกำหนดที่ Router เท่านั้น

ข้อเสียของ Screening Router

1. การกำหนดแอคเซสรูลทำได้ยาก ไม่มีระบบยูสเซอร์อินเตอร์เฟสเพื่อช่วยในการทำงาน

2. คำสั่งในการทำงานจะผูกติดกับยี่ห้อของเราท์เตอร์ ไม่มีมาตรฐานของคำสั่ง

3. ไม่สามารถกำหนดกฎที่ซับซ้อนได้ เนื่องจากขีดจำกัดของเราท์เตอร์ที่ทำงานโดยพิจารณาครั้งลงแพ็กเกตเท่านั้น

4. มีความสามารถจำกัด เช่นไม่สามารถบันทึก log ของแพ็กเกตที่ต้องสงสัยไว้ตรวจสอบภายหลังได้

5. เราท์เตอร์มีกำลังในการประมวลผลจำกัด หากเน็ตเวิร์คมีขนาดใหญ่และมีการสื่อสารข้อมูลหนาแน่น เราท์เตอร์จะทำงานหนักอยู่แล้ว เมื่อต้องทำการประมวลผลแอคเซสรูลด้วยก็จะทำให้ประสิทธิภาพการเราท์แพ็กเกตต่ำลงไปมาก

Circuit Level Firewall

เป็นไฟร์วอลล์ที่ทำงานโดยที่สามารถเข้าใจสถานะการสื่อสารทั้งกระบวนการ เพราะว่าการสื่อสารข้อมูลจะสมบูรณ์ได้นั้นจะต้องมีทั้งการส่งและการรับอย่างสอดคล้องสัมพันธ์กันนั้นเอง Stateful Inspection Firewall หรือ Stateful Firewall เป็นไฟล์วอลที่ทำการควบคุมทราฟฟิคโดยใช้หลักการของแพ็คเก็ตฟิลเตอริ่งและการกำหนดแอคเซสรูลเช่นเดียวกับสกรีนนิ่งเราท์เตอร์ แต่สเตทฟูลไฟร์วอลล์จะมีความสามารถในการวิเคราะห์และรับรู้ความต่อเนื่องของแพ็กเกตในโปรโตคอลระดับสูงขึ้นไปมากกว่า ไม่ว่าจะเป็น TCP, FTP, HTTP หรือแม้กระทั่งโปรโตคอลในระดับแอพพลิเคชันเลเยอร์ที่มีลักษณะเฉพาะของแอพพลิเคชันนั้น ที่จะมีวิธีการกำหนดเสตทของตนเอง

สเตทฟูลไฟร์วอลล์เป็นเครื่องมือที่ถูกออกแบบมาเพื่อทำหน้าที่ในการควบคุมทราฟฟิคโดยเฉพาะ ไม่ได้เป็นการดัดแปลงการทำงานมาจากเราท์เตอร์จึงมีความสามารถในการควบคุมทราฟฟิค การกำหนดแอคเซสรูล การบริหาร รวมไปถึงความยืดหยุ่นของการควบคุมทราฟฟิค และประสิทธิภาพการทำงานที่สูงกว่าสกรีนนิงเราท์เตอร์เป็นอย่างมาก เนื่องจากสเตทฟูลไฟร์วอลล์มีความสามารถในการประกอบรวมแฟรกเมนต์เข้าด้วยกันเป็นดาต้าแกรมที่สมบูรณ์ก่อน หลังจากนั้นจึงนำดาต้าแกรมนั้นมาทำการตรวจสอบเปรียบเทียบกับแอคเซสรูล

ข้อดีของสเตทฟูลไฟร์วอลล์

1. ใช้งานง่ายเพราะถูกออกแบบมาทำหน้าที่ของไฟร์วอลล์โดยเฉพาะ ตรวจสอบแก้ไขแอคเซสรูลได้ง่าย ทำให้ผู้ใช้ไม่ต้องคอยกังวลถึงคำสั่ง และรูปแบบคำสั่ง

2. ประสิทธิภาพการทำงานสูง เนื่องจากออกแบบมาเพื่อทำหน้าที่ไฟร์วอลล์โดยเฉพาะ สามารถรองรับแอคเซสรูลที่ซับซ้อนได้ โดยที่ความสามารถในการทำงานไม่ตกลง

3. มีคุณสมบัติเพิ่มเติมให้ใช้ได้มากนอกเหนือจากการควบคุมทราฟฟิค เช่น สามารถนำไปใช้ร่วมกับระบบตรวจจับการบุกรุก (IDS) เพื่อป้องกันการโจมตีได้อัตโนมัติ สามารถบันทึกข้อมูลเอาไว้กลับมาดูในภายหลังได้ สามารถใช้งานร่วมกับระบบ Anti Virus ได้ เป็นต้น

4. การกำหนดแอคเซสรูลทำได้ง่าย เพราะไฟร์วอลล์มีความเข้าใจในโปรโตคอลระดับสูง ผู้ใช้สามารถกำหนดกฎบนพื้นฐานของแอพพลิเคชันที่ผู้ใช้รู้จัก

5. สามารถเพิ่มเติมความปลอดภัยโดยระบบตรวจสอบผู้ใช้ (Authenticate) ได้

6. สามารถเพิ่มเติมบริการอื่นๆได้ เช่น Virtual Private Network, Tunneling

7. การสื่อสารระหว่างไฟร์วอลล์กับแอดมินคอนโซล จะมีความปลอดภัยสูง มีการเข้ารหัสเพื่อป้องกันการดักอ่านข้อมูล

ข้อเสียของสเตทฟูลไฟร์วอลล์

1. มีราคาแพง

2. ในกรณีที่เป็นไฟร์วอลล์แบบซอฟต์แวร์ที่ทำงานอยู่บนระบบปฏิบัติการทั่วไป เช่น Solaris, Window NT, Windows2000 ต่างก็มีความเสี่ยงที่จะถูกเจาะได้เนื่องจากปัญหาของแต่ละระบบปฏิบัติการเอง

3. ในกรณีที่ไฟร์วอลล์เป็นประเภท Network Appliance คือ ออกแบบทั้งซอฟต์แวร์และฮาร์ดแวร์เป็นเครื่องเดียวกันเพื่อทำหน้าที่เป็นไฟร์วอลล์โดยเฉพาะผู้ใช้จำเป็นต้องพึ่งพาผู้ผลิตค่อนข้างมาก หากมีปัญหาอาจจะไม่สามารถแก้ไขโดยการใช้อะไหล่ทดแทนจากที่อื่นได้

3.4.2 ไฟร์วอลล์แบบซอฟต์แวร์ที่นิยมใช้

แพ็กเกตฟิลเตอร์ IPCHAINS

แพ็กเกตฟิลเตอร์ IPCHAINS คือ ซอฟต์แวร์ที่ใช้สำหรับอ่านข้อมูลของเฮดเดอร์แล้วทำการตัดสินว่าจะทำการอนุญาตหรือปฏิเสธแพ็กเกตที่ถูกส่งมา การตัดสินแพ็กเกตจะมีอยู่ 3 กรณี

1. แพ็กเกตจะถูกปฏิเสธเสมือนหนึ่งคอมพิวเตอร์ปลายทางไม่เคยได้รับแพ็กเกตนั้นมาก่อน

2. แพ็กเกตฟิลเตอร์จะอนุญาตให้แพ็กเกตผ่านเข้ามาในระบบได้และ

3. แพ็กเกตจะถูกปฏิเสธเหมือนกรณีแรกแต่จะทำการส่งข้อมูลตอบกลับไปยังแหล่งต้นทางเพื่อบอกถึงการปฏิเสธแพ็กเกตนั้นๆ

ภายใต้ระบบปฏิบัติการลีนุกซ์ แพ็กเกตฟิลเตอร์จะถูกสร้างอยู่ในส่วนของเคอร์เนล และทำการประมวลผลข้อมูลบางอย่างได้มากกว่าระบบปฏิบัติการอื่นๆ แต่หลักการในการตัดสินแพ็กเกตยังคงยึดหลักการที่ได้กล่าวมาแล้วข้างต้น

หลักการพื้นฐานของการส่งข้อมูลในระบบเน็ตเวิร์คจะอยู่ในรูปแบบของแพ็กเกต ซึ่งแต่ละแพ็กเกตจะประกอบไปด้วยส่วนที่เรียกว่าเฮดเดอร์และบอดี้ เฮดเดอร์จะเก็บข้อมูลที่เกี่ยวกับคอมพิวเตอร์ต้นทางและปลายทางที่แพ็กเกตจะถูกจัดส่งไป รวมถึงรายละเอียดการจัดการอื่นๆ ส่วนบอดี้จะบรรจุข้อมูลแท้จริงที่ใช้ส่ง การดาวโหลดแพ็กเกตแต่ละแพ็กเกต ไม่สามารถทำได้ภายในครั้งเดียว ตัวอย่างเช่น แพ็กเกตที่มีความยาว 50 k อาจต้องดาวโหลดครั้งละ 1460 ไบต์ ต่อเนื่องกันไป 36 ครั้ง เพื่อจะได้ข้อมูลทั้งหมดโปรโตคอลบางประเภท เช่น TCP ซึ่งถูกใช้สำหรับการส่งข้อมูลในเว็บไซต์ ส่งเมล์ หรือ Remote Login ใช้หลักการที่เรียกว่า คอนเนคชั่น นั่นคือก่อนที่จะมีการส่งผ่านข้อมูลแต่ละครั้ง แต่ละแพ็กเกตจะต้องมีการแลกเปลี่ยนข้อมูลในส่วนของเฮดเดอร์เพื่อบอกถึงความพร้อมในการส่งจากต้นทางและรับข้อมูลจากปลายทางเสียก่อน การรับส่งแพ็กเกตถึงจะเริ่มขึ้นได้

การใช้งาน IPCHAINS เพื่อควบคุมแพ็กเกต

ถ้าผู้ใช้เลือกใช้ระบบปฏิบัติการลีนุกซ์สำหรับทำการติดต่อระหว่างเนตเวิร์คภายในกับเน็ตเวิร์คภายนอก เช่น อินเตอร์เน็ต ผู้ใช้สามารถที่จะกำหนดเงื่อนไขในการควบคุมการส่งข้อมูลได้ ยกตัวอย่างเช่น สามารถป้องกันไม่ให้แพ็กเกตถูกส่งไปยังเส้นทางที่กำหนดไว้ หรือจำกัดโปรโตคอลที่ใช้ในการส่ง นั่นหมายถึง แพ็กเกตที่จะถูกจัดส่งออกไปทั้งหมดต้องผ่านเงื่อนไขที่ถูกกำหนดไว้ในส่วนของลีนุกซ์ก่อน หรือในกรณีการควบคุมการรับข้อมูลจากภายนอกเข้ามายังเน็ตเวิร์คภายใน เช่น ใช้เบราเซอร์เนตสเคปเพื่อที่จะเข้าไปอ่านข้อมูลของคอมพิวเตอร์เครื่องหนึ่งนอกระบบ แต่ทุกครั้งก่อนที่จะอ่านข้อมูลได้ คอมพิวเตอร์เครื่องนั้นได้กำหนดให้มีการดาวโหลดข้อมูลจากอีกเว็บไซต์หนึ่งเสียก่อน ซึ่งเราสามารถหลีกเลี่ยงการดาวโหลดนี้ได้โดยการกำหนดให้แพ็กเกตฟิลเตอร์ไม่อนุญาตให้มีการรับข้อมูลที่มาจากเว็บไซต์นั้น

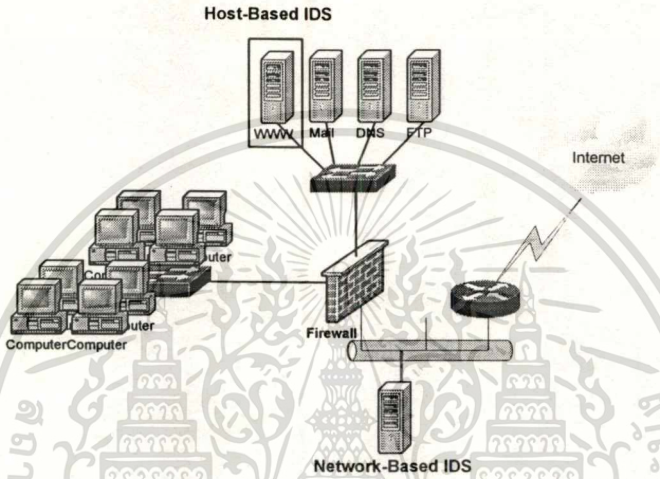
3.4.3 ระบบตรวจจับการบุกรุก (Intrusion Detection System)

ระบบตรวจจับการบุกรุก หรือ IDS (Intrusion Detection System) เป็นเครื่องมือสำหรับการรักษาความปลอดภัยอีกประเภทหนึ่งที่ใช้สำหรับตรวจจับความพยายามที่จะบุกรุกเครือข่าย โดยระบบจะแจ้งเตือนผู้ดูแลระบบเมื่อการบุกรุกหรือพยายามที่จะบุกรุกเครือข่าย IDS นั้นไม่ใช่ระบบที่ใช้ป้องกันการบุกรุกแต่เป็นระบบที่คอยแจ้งเตือนภัยเท่านั้น

หน้าที่หลักของ IDS คือ แจ้งเตือนการเข้าใช้เครือข่ายผิดปกติ สิ่งที่เป็นประเด็นสำคัญในการออกแบบระบบ IDS ก็คือ เหตุการณ์ใดคือสิ่งที่ถือว่าผิดปกติ ดังนั้นการใช้ IDS นั้นก็ขึ้นกับว่าอะไรที่จะแจ้งเตือนให้ทราบ คำตอบนั้นไม่ใช่แค่ถูกหรือผิด แต่จะขึ้นอยู่กับสภาวะของระบบในขณะนั้น

ประเภทของ IDS

IDS แบ่งออกเป็น 2 ประเภทคือ Host-Bases IDS และ Network-Based IDS โดยโฮสต์เบสไอดีเอส นั้นคือ ระบบที่ติดตั้งที่โฮสต์และเฝ้าระวังและตรวจจับความพยายามที่จะบุกรุกโฮสต์นั้น ส่วนเน็ตเวิร์คเบสไอดีเอสนั้นคือ ระบบที่ตรวจดูแพ็กเกตที่วิ่งอยู่ในเครือข่าย และแจ้งเตือนถ้าพบหลักฐานที่คาดว่าจะเป็นการบุกรุกเครือข่าย



รูปที่ 3.8 แสดงการติดตั้ง Intrusion Detection System

จากรูปที่ 3.8 โฮสต์เบสไอดีเอสจะติดตั้งที่เครื่องเว็บเซิร์ฟเวอร์เพื่อตรวจจับความพยายามที่จะแฮ็กเว็บเซิร์ฟเวอร์เอง ส่วนเน็ตเวิร์คไอดีเอสนั้นจากรูปจะติดตั้งระหว่างเราท์เตอร์และไฟร์วอลล์ เพื่อที่จะตรวจทราฟิกที่วิ่งเข้าออกระหว่างเครือข่ายและอินเตอร์เน็ต

Host-Based IDS

โฮสต์เบสไอดีเอสเป็นซอฟต์แวร์ที่รันบนโฮสต์ โดยปกติแล้ว IDS ประเภทนี้จะวิเคราะห์ล็อก (Log) เพื่อค้นหาข้อมูลเกี่ยวกับการบุกรุก ในระบบยูนิกซ์นั้นล็อกที่ IDS จะตรวจสอบ เช่น Syslog Messages Lastlog และ Wtmp เป็นต้น ส่วนในวินโดว์นั้น IDS ก็จะตรวจสอบอีเวนต์ล็อกต่างๆ เช่น System Application และ Security เป็นต้น โดยปกติ IDS จะอ่านเหตุการณ์ใหม่ที่เกิดขึ้นในล็อกและเปรียบเทียบกับกฎที่ตั้งไว้ก่อนหน้า ถ้าตรงก็จะแจ้งเตือนทันที ดังนั้นการที่ IDS จะตรวจจับการบุกรุกได้ระบบจะต้องบันทึกเหตุการณ์ต่างๆ ที่สำคัญที่เกิดขึ้นกับระบบในล็อกไฟล์ ถ้าไม่เช่นนั้น IDS ก็ไม่มีข้อมูลที่จะใช้วิเคราะห์ว่ามีการบุกรุกหรือไม่

นอกจากการตรวจสอบล็อกไฟล์แล้ว IDS บางชนิดอาจสามารถตรวจสอบการเรียกใช้ฟังก์ชันของระบบปฏิบัติการ (System Call) ซึ่งถ้าเหตุการณ์คล้ายหรือตรงกับการบุกรุก IDS ก็

จะแจ้งเตือนทันที นอกจากนี้ IDS ยังสามารถตรวจสอบการแก้ไขไฟล์ในระบบได้ด้วย ซึ่งอาจทำได้โดยการตรวจสอบวันที่ที่แก้ไขครั้งสุดท้ายและขนาดของไฟล์ เป็นต้น วิธีที่แน่นอนกว่าก็จะคำนวณเช็คซัม (Checksum) ของไฟล์แล้วเก็บไว้เพื่อเปรียบเทียบเมื่อมีการตรวจสอบความคงสภาพของไฟล์ในระบบ โดยเมื่อมีการคำนวณเช็คซัมใหม่แล้วค่าที่ได้ไม่ตรงกับค่าเดิมก็แสดงว่าไฟล์ถูกแก้ไข

ข้อได้เปรียบของโฮสต์เบสไอดีเอส

1. โฮสต์เบสไอดีเอสสามารถตรวจพบทุกการบุกรุกกับโฮสต์นั้นๆ ได้เสมอถ้าระบบสามารถบันทึกเหตุการณ์ดังกล่าวในล็อกได้ หรือการบุกรุกมีการเรียกใช้ซิสเต็มคอลล์

2. โฮสต์เบสไอดีเอสสามารถบอกได้ว่าการบุกรุกนั้นสำเร็จหรือไม่ โดยการวิเคราะห์ข้อความในล็อกหรือจากหลักฐานอื่นๆ เช่น มีการแก้ไขไฟล์ที่สำคัญของระบบ เป็นต้น

3. โฮสต์เบสไอดีเอสสามารถบ่งชี้ได้ว่ามีการเข้าใช้ระบบอย่างผิดปกติโดยผู้ใช้ของระบบเอง

ข้อเสียเปรียบของโฮสต์เบสไอดีเอส

1. โพรเซสของ IDS อาจถูกโจมตีเองจนอาจไม่สามารถแจ้งเตือนได้

2. โฮสต์เบสไอดีเอสจะแจ้งเตือนก็ต่อเมื่อเหตุการณ์ที่เกิดขึ้นนั้นตรงกับที่กำหนดไว้ก่อนหน้า ถ้าแฮ็กเกอร์มีเทคนิคใหม่ๆ IDS อาจไม่แจ้งเตือนการบุกรุกได้

3. การทำงานของโฮสต์ไอดีเอสอาจมีผลกระทบต่อประสิทธิภาพของโฮสต์เองเนื่องจากต้องตรวจสอบล็อกไฟล์และซิสเต็มคอลล์

Network-Based IDS

เน็ตเวิร์คเบสไอดีเอส คือ ซอฟต์แวร์พิเศษที่รันบนคอมพิวเตอร์เครื่องหนึ่งต่างหาก IDS ประเภทนี้จะมีเน็ตเวิร์คการ์ดที่ทำงานในโหมดที่เรียกว่า โพรมิสเซียส (Promiscuous Mode) ซึ่งในโหมดนี้เน็ตเวิร์คการ์ดจะส่งต่อทุกๆ แพ็กเกตที่วิ่งอยู่บนเครือข่ายไปให้แอพพลิเคชันโพรเซส ในขณะที่เน็ตเวิร์คการ์ดที่รันโหมดธรรมดานั้นจะรับเอาเฉพาะแพ็กเกตที่มีที่อยู่ปลายทางตรงกับของเครื่องนั้นเท่านั้น เมื่อทุกๆ แพ็กเกตส่งผ่านไปให้แอพพลิเคชัน IDS จะวิเคราะห์ข้อมูลในแพ็กเกตเหล่านั้นกับกฎที่ได้ตั้งไว้ก่อนหน้า ถ้าตรงกับกฎก็จะแจ้งเตือนทันที

ในแต่ละ IDS จะมีข้อมูลที่ใช้สำหรับเปรียบเทียบเพื่อบอกว่ามีการพยายามที่จะบุกรุกเครือข่ายหรือไม่ ซึ่งข้อมูลนี้จะเรียกว่า ซิกเนเจอร์ (Signature) IDS จะใช้ซิกเนเจอร์ที่เก็บไว้เปรียบเทียบกับข้อมูลที่ได้จากการวิเคราะห์แพ็กเกตที่วิ่งในเครือข่าย ดังนั้นถ้าแฮ็กเกอร์มีเทคนิคใหม่ๆ และ IDS ไม่รู้จักเทคนิคนี้หรือมีซิกเนเจอร์นี้ IDS ก็จะไม่สามารถตรวจจับการบุกรุกประเภทนี้ได้

โดยส่วนใหญ่แล้ว IDS ประเภทนี้จะมี 2 เน็ตเวิร์คการ์ด โดยเน็ตเวิร์คการ์ดแรกจะเชื่อมต่อเข้ากับเครือข่ายที่ต้องการเฝ้าระวังหรือตรวจจับการบุกรุก โดยเน็ตเวิร์คการ์ดนี้จะไม่มีหมายเลขไอพี ดังนั้นเครื่องอื่นๆ ที่อยู่ในเครือข่ายจะมองไม่เห็นเครื่องนี้ ส่วนเน็ตเวิร์คการ์ดอีกอันหนึ่งจะเชื่อมต่อเข้าอีกเครือข่ายหนึ่งเพื่อใช้สำหรับส่งการแจ้งเตือนภัยไปยังเซิร์ฟเวอร์ โดยเครือข่ายนี้จะต้องไม่ถูกเชื่อมต่อกับเครือข่ายหลักที่ IDS จะตรวจจับการบุกรุก

ข้อได้เปรียบของเน็ตเวิร์คเบสไอดีเอส

1. เน็ตเวิร์คเบสไอดีเอสจะแอบซ่อนในเครือข่าย ทำให้ผู้บุกรุกไม่รู้ว่ากำลังถูกเฝ้ามอง

2. เน็ตเวิร์คเบสไอดีเอสหนึ่งเครื่องสามารถใช้เฝ้าระวังการบุกรุกได้กับหลายระบบหรือโฮสต์

3. เน็ตเวิร์คเบสไอดีเอสสามารถตรวจจับทุกๆ แพ็กเกตที่วิ่งไปยังระบบที่ถูกเฝ้าระวังภัยอยู่

ข้อเสียเปรียบของเน็ตเวิร์คเบสไอดีเอส

1. เน็ตเวิร์คเบสไอดีเอสจะแจ้งเตือนภัยก็ต่อเมื่อตรวจพบแพ็กเกตที่ตรงกับซิกเนเจอร์ที่กำหนดไว้ก่อนหน้าเท่านั้น

2. เน็ตเวิร์คเบสไอดีเอสอาจพลาดที่จะตรวจจับแพ็กเกตได้ในกรณีที่มีการใช้เครือข่ายมากจนทำให้ IDS วิเคราะห์แพ็กเกตที่วิ่งอยู่บนเครือข่ายไม่ทัน หรือมีเส้นทางข้อมูลอื่นที่ไม่ต้องผ่าน IDS

3. เน็ตเวิร์คเบสไอดีเอสไม่สามารถสรุปได้ว่าการบุกรุกนั้นสำเร็จหรือไม่

4. เน็ตเวิร์คเบสไอดีเอสไม่สามารถตรวจวิเคราะห์แพ็กเกตที่ถูกเข้ารหัสไว้ได้

5. เครือข่ายที่ใช้สวิตช์นั้นต้องเซตเพื่อให้พอร์ตที่เชื่อมต่อกับ IDS นั้นสามารถมองเห็นทุกแพ็กเกตที่วิ่งผ่านสวิตช์นั้น

ทั้งโฮสต์เบสไอดีเอส และเน็ตเวิร์คเบสไอดีเอสมีทั้งข้อดีและข้อเสียที่แตกต่างกัน ในขณะที่เน็ตเวิร์คเบสนั้นสามารถใช้เฝ้าระวังได้ครอบคลุมส่วนของเครือข่ายได้มากกว่า ดังนั้นจึงเป็นทางเลือกที่ประหยัดกว่าแต่โฮสต์เบสไอดีเอสจะเหมาะสำหรับการเฝ้าระวังภัยที่อาจจะสร้างโดยผู้ใช้ของเครือข่ายเอง ดังนั้นการเลือกประเภทของ IDS ให้เหมาะสมนั้นก็ขึ้นอยู่กับภัยที่คุกคามเครือข่ายขององค์กร

การแจ้งเตือนภัยของ IDS

IDS จะรายงานเฉพาะสิ่งที่กำหนดให้รายงานเท่านั้น มีอยู่สองสิ่งที่ผู้ดูแลระบบจะต้องคอนฟิกให้กับ IDS สิ่งแรกคือ ซิกเนเจอร์ของการบุกรุก สิ่งที่สองคือเหตุการณ์ที่ผู้ดูแลระบบให้ความสำคัญหรือเหตุการณ์ที่คาดว่าจะเป็นผลไปสู่การบุกรุกในภายหน้า ซึ่งเหตุการณ์ต่างๆ เหล่านี้อาจเป็นกราฟิกที่ไม่ปกติหรืออาจเป็นบางข้อความในล็อก การคอนฟิกซิกเนเจอร์ให้กับ IDS ของแต่ละองค์กรนั้นอาจจะไม่เหมือนกัน ซึ่งจะขึ้นอยู่กับว่าองค์กรนั้นจะให้ความสนใจกับการบุกรุก

ประเภทใด เมื่อ IDS ได้ถูกคอนฟิกอย่างถูกต้องแล้ว เหตุการณ์ที่ IDS จะรายงานให้ทราบนั้น สามารถแบ่งออกได้เป็น 3 ประเภท คือ

1. การสำรวจเครือข่าย
2. การโจมตี
3. เหตุการณ์ที่น่าสงสัยหรือผิดปกติ

การสำรวจเครือข่าย

เหตุการณ์ที่เป็นการสำรวจเครือข่ายเป็นการพยายามของผู้บุกรุกที่จะรวบรวมข้อมูลเกี่ยวกับระบบเครือข่ายก่อนที่จะโจมตีจริงๆ เช่น

- **IP Scans** ไอพีสแกนเป็นความพยายามของผู้บุกรุกที่ทราบเกี่ยวกับโฮสต์ต่างๆ ที่อยู่ในเครือข่ายซึ่งระบบที่สแกนนั้นอาจใช้การปิง (ping) ช่วงของหมายเลขไอพีของเครือข่าย

- **Port Scans** หลังจากที่ผู้บุกรุกพอได้ข้อมูลเกี่ยวกับว่าเครือข่ายมีโฮสต์ใดอยู่บ้าง ข้อมูลต่อมาที่ผู้บุกรุกต้องการคือ บริการใดบ้างที่แต่ละโฮสต์ให้บริการอยู่ ซึ่งหมายเลขพอร์ตนั้นจะเป็นสิ่งที่บ่งบอกว่ามีแอพพลิเคชันใดบ้างที่ให้บริการอยู่

- **Trojan Scans** การสแกนโทรจันนั้นเป็นความพยายามของผู้บุกรุกที่จะตรวจเช็คว่ามีพอร์ตของโทรจันใดบ้างที่เปิดอยู่

- **Vulnerability Scans** การสแกนหาจุดอ่อนของระบบ เป็นความพยายามที่จะใช้การโจมตีหลายๆ แบบกับระบบใดระบบหนึ่งเพื่อตรวจเช็คดูระบบนี้ว่ามีจุดอ่อนอย่างไร

- **File Snooping** ไฟล์สนูปิงเป็นการตรวจเช็คว่ายูสเซอร์มีสิทธิ์อย่างไรกับไฟล์นั้น ซึ่งระบบไฟล์ส่วนใหญ่จะมีการกำหนดสิทธิ์ของผู้ใช้ในการเข้าใช้แต่ละไฟล์

การโจมตี

การโจมตีเครือข่ายหรือระบบนั้นควรให้ลำดับความสำคัญสูงสุด เมื่อ IDS รายงานเหตุการณ์นี้ผู้ดูแลระบบตอบสนองกับเหตุการณ์นี้ทันทีเพื่อป้องกันการสูญเสียมากกว่านี้ บางครั้ง IDS อาจแยกแยะระหว่างการโจมตีจริงๆ กับการสแกนหาจุดอ่อน เนื่องจากเหตุการณ์ทั้งสองนั้น IDS จะตรวจพบซิกเนเจอร์ของการโจมตีเหมือนกัน ผู้ดูแลระบบอาจต้องวิเคราะห์ข้อมูลเพิ่มเติม การสแกนหาจุดอ่อนนั้น IDS จะรายงานการโจมตีหลายๆ รูปแบบในช่วงเวลาสั้นๆ กับระบบใดระบบหนึ่ง ส่วนการโจมตีจริงนั้นอาจมีการรายงานการโจมตีแค่รูปแบบเดียวกับระบบใดระบบหนึ่ง

เหตุการณ์ที่น่าสงสัยหรือผิดปกติ

เหตุการณ์อื่นๆ ที่ผิดปกติและไม่ได้จัดอยู่ในประเภทต่างๆ ที่กล่าวมาข้างต้นถือว่าเป็นเหตุการณ์ที่น่าสงสัยว่าอาจมีการโจมตีเครือข่ายเกิดขึ้น ซึ่งผู้ดูแลระบบต้องวิเคราะห์และสืบหาสาเหตุของเหตุการณ์ที่ว่านี้ต่อ ตัวอย่างเช่น บางโฮสต์อาจส่งแพ็กเกตที่มีข้อมูลส่วนหัวผิดไปจากที่

กำหนดในมาตรฐาน ซึ่งเหตุการณ์นี้อาจเกิดขึ้นเนื่องจากการโจมตีแบบใหม่ หรือเน็ตเวิร์คการ์ดเครื่องส่งอาจเสีย หรือข้อมูลอาจเกิดผิดพลาดในระหว่างการส่งผ่านสายสัญญาณ IDS จะไม่มีข้อมูลเพียงพอที่จะบอกได้ว่าเหตุการณ์นี้เกิดขึ้นเพราะอะไร แต่จะแจ้งเตือนให้ผู้ดูแลระบบทราบเพื่อสืบค้นหาสาเหตุที่แท้จริงต่อไป

3.4.4 IDS แบบซอฟต์แวร์ที่นิยมใช้

Snort IDS

Snort เป็นเครื่องมือที่ใช้ตรวจจักการบุกรุกทางเครือข่าย (Network Intrusion Detection) โดย Martin Roesch (http://www.snort.org) การทำงานของ Snort จะใช้ไลบรารี (Library) พื้นฐานชื่อ libpcab ซึ่งใช้กันโดยทั่วไปในบรรดา Network Sniffer และ Network Analyzer ทั้งหลาย สำหรับ Snort นั้นสามารถทำ Protocol Analysis Content Searching/Matching ตรวจจับการบุกรุกและ Probe เช่น Buffer Overflow Stealth port Scan CGI Attack SMB Probe OS Fingerprint และอื่นๆ นอกจากนี้ยังมีคุณสมบัติในการทำ Real-time Alerting อีกด้วย นอกเหนือจากการเก็บล็อกไปที่ syslog หรือเก็บแยกไฟล์ต่างหาก และยังสามารถ alert ผ่าน winpopup ผ่าน ทาง Samba's client ได้อีกด้วย Snort สนับสนุนฐานข้อมูล MySQL, Postgresql, unixODBC และ Oracle ในกรณีที่ใช้ฐานข้อมูลอื่น เช่น DB2, Informix หรืออื่นๆ ท่านสามารถใช้ unixODBC เป็นตัวกลางในการเชื่อมต่อได้

3.5 นโยบายความปลอดภัยบนอุปกรณ์ควบคุมเครือข่าย

นโยบายความปลอดภัยบนอุปกรณ์ควบคุมเครือข่ายจะครอบคลุมถึงการกลั่นกรองจราจรของแพ็กเกตที่อยู่บนเครือข่ายข้อมูล

3.5.1 Access Control List

หรือที่เรียกอย่างสั้นว่า ACL นั้นเป็นบริการหนึ่งของซอฟต์แวร์ที่ควบคุมและดูแลการทำงานของเราท์เตอร์ด้านการกรองจราจรในเครือข่ายข้อมูล ส่วนกฎที่ใช้ในไฟร์วอลล์นั้นแม้จะต่างกันแต่ก็มีหลักการในการทำงานแบบเดียวกันกับ ACL

ACL กลั่นกรองการจราจรที่เข้าหรือออกเครือข่ายโดยการตรวจสอบแพ็กเกตข้อมูลที่ขาเชื่อมต่อหรืออินเตอร์เฟส (interface) ระหว่างเราท์เตอร์กับเครือข่ายนั้นว่าจะกั้น (block) ด้วยการปล่อยแพ็กเกตเหล่านั้นทิ้งไป หรือปล่อยผ่านให้ไป (forward) ตามเงื่อนไขที่กำหนดไว้ใน ACL ที่กำหนดโดยผู้ควบคุมระบบตามนโยบายความปลอดภัย ซึ่งสามารถระบุจากหมายเลขหรือแอดเดรส (address) ของต้นทาง ปลายทาง และโปรโตคอลที่อยู่ระดับเหนือขึ้นไป รวมทั้งข้อมูลอื่นๆ ซึ่งบางโปรโตคอลนั้นจะใช้คำว่า filter แทนคำว่า Access-list

การกรองแพ็กเกตโดยใช้เราท์เตอร์

นอกจากจะควบคุมการสื่อสารโดยข้อมูลโดยใช้ไฟร์วอลล์แล้ว เราท์เตอร์ซึ่งมีหน้าที่หลักในการเราท์แพ็กเกตได้มีความสามารถเพิ่มขึ้นจนสามารถนำมาใช้เพื่อการรักษาความปลอดภัยได้ นั้นคือความสามารถในการกรองแพ็กเกต (Packet Filtering) ซึ่งเป็นการกรองแพ็กเกตในระดับพื้นฐานโดยอาศัยการพิจารณาองค์ประกอบของแพ็กเกตเช่นเดียวกับไฟร์วอลล์ คือดูที่แอดเดรสและพอร์ตเป็นหลัก แต่เป็นการดูในระดับพื้นฐานเท่านั้น ไม่สามารถทำการกำหนดเงื่อนไขได้อย่างกฎของไฟร์วอลล์ แต่ก็ยังสามารถช่วยในการรักษาความปลอดภัยได้ในระดับหนึ่ง

อย่างไรก็ตาม ยังมีการควบคุมบางประเภทที่เหมาะสำหรับบนเราท์เตอร์เท่านั้น ไม่เหมาะสำหรับกำหนดเป็นกฎของไฟร์วอลล์ เช่น การป้องกันการบรอดคาสต์ การป้องกันแฟรกเมนต์ เป็นต้น ซึ่งการควบคุมแพ็กเกตประเภทนี้บนเราท์เตอร์จะช่วยแบ่งเบาภาระของไฟร์วอลล์ลงไปได้มาก ถึงแม้จะมีการควบคุมบางประเภทที่สามารถกำหนดได้ทั้งบนเราท์เตอร์และไฟร์วอลล์ แต่โดยพื้นฐานแล้วหากการควบคุมการสื่อสารชนิดใดที่สามารถกำหนดเป็นกฎบนไฟร์วอลล์ได้ก็ควรจะกำหนดไว้บนไฟร์วอลล์ ควรหลีกเลี่ยงการนำเราท์เตอร์มาทำหน้าที่แทนไฟร์วอลล์ เพราะไม่สามารถแทนกันได้เนื่องจากหน้าที่หลักแตกต่างกัน และจะส่งผลเสียต่อความปลอดภัยที่อาจไม่สามารถป้องกันได้จริง รวมถึงประสิทธิภาพการสื่อสารข้อมูล เพราะเราท์เตอร์ต้องเสียเวลาในการตรวจสอบแพ็กเกตมากเกินไปจนประสิทธิภาพในการเราท์ข้อมูลซึ่งเป็นหน้าที่หลักลดต่ำลง

สาเหตุที่ต้องมีการนำ ACL มาใช้นั้นก็เกิดจากความจำเป็นหลายประการ ไม่ว่าจะเป็นการควบคุมการเปลี่ยนแปลงข้อมูลเส้นทาง ระหว่างเราท์เตอร์หรือควบคุมการไหลของจราจร แต่ที่สำคัญที่สุดนั่นคือการนำมาใช้เพื่อรักษาความปลอดภัยภายในเครือข่ายในระดับหนึ่ง วิธีการเบื้องต้นก็คือการใช้ ACL กลั่นกรองแพ็กเกตที่ผ่านเข้าออกแต่ละอินเตอร์เฟส โดยปกติถ้าไม่มีการกำหนด ACL แล้ว แพ็กเกตที่ผ่านเข้ามายังเราท์เตอร์นั้นได้รับการอนุญาตให้ไปยังส่วนใดๆ ของเครือข่ายก็ได้ นอกจากนี้ยังสามารถระบุตามประเภทของโปรโตคอลว่าจะให้ผ่านหรือกันไว้ได้อีกด้วย เช่นอนุญาตให้ email ผ่านได้แต่กันการ Telnet ไว้เป็นต้น โดยการตรวจสอบจากหมายเลขพอร์ตซึ่งต่างกัน

หลักการของการกำหนด ACL

เราท์เตอร์จะทำการตรวจสอบแพ็กเกตกับ ACL ตามลำดับ และทิศทางที่กำหนดไว้สำหรับอินเตอร์เฟส บางโปรโตคอลอย่างเช่น IP นั้นสามารถระบุได้สอง ACL สำหรับแพ็กเกตที่ผ่านเข้ามา (inbound) และออกไปจากอินเตอร์เฟสนั้น (outbound) โดยแต่ละ ACL นั้นจะต้องมีหมายเลขกำกับไว้ในการกำหนดให้กับอินเตอร์เฟสที่ต้องการ ซึ่งหมายเลขนี้จะใช้บอกประเภทและโปรโตคอลด้วย สำหรับ IP นั้นจะมีอยู่สองช่วงคือ 1-99 กับ 1300-1999 และ 100-199 กับ 2000-2999 สำหรับแบบ

Extended ซึ่งเป็น ACL ของ IP แบบที่มีการระบุถึงพอร์ตของโปรโตคอลด้วย กฎที่ประกอบกันเป็น ACL นั้นจะทำงานตามลำดับ การเพิ่มกฎใหม่เข้าไปจะต่อท้ายเสมอ ดังนั้นถ้าต้องการแทรกจะต้องทำการลบ ACL ออกทั้งกลุ่มแล้วจึงป้อนเข้าไปใหม่ทั้งหมด ถ้าไม่ระบุไว้ กฎสุดท้ายใน ACL นั้นคือไม่ให้แพ็กเกตผ่านไป (deny all traffic)

ตารางที่ 3.1 แสดงช่วงของ Port ในการใช้กำหนด Access Rule ของ Cisco

Protocol	Access list Number
IP	1-99 and 1300-1999
Extended IP	100-199 and 1200-2999
Ethernet type code	200-299
Ethernet address	700-799
Transparent bridging (protocol type)	200-299
Transparent bridging (vender code)	700-799
Extended transparent bridging	1100-1199
DECnet and extended DECnet	300-399
XNS	400-499
Extended XNS	500-599
Apple Talk	600-699
Source-route bridging (protocol type)	200-299
Source-route bridging (vendor code)	700-799
IPX	800-899
Extended IPX	900-999
IPX SAP	1000-1099
Standard VINES	1-100
Extended VINES	101-200
Simple VINES	201-300

รูปแบบของการกำหนด ACL

Standard IP Access List มีรูปแบบดังนี้

access-list <number 1-99> <deny | permit> <source address> <wildcard mask>

ตัวอย่าง *access-list 1 permit 172.30.16.100 0.0.0.0*

หมายความว่า จะอนุญาตเฉพาะแพ็กเกตที่มาจากโฮสต์ 172.30.16.100 เท่านั้น

Extended IP Access List เป็น ACL แบบ Extended ตามเงื่อนไข ประกอบด้วย Source Address, Destination Address, IP Protocol (TCP, UTP, ICMP etc..), Port Information (FTP, WWW, DNS etc..) มีรูปแบบดังนี้

access-list <number 100-199> <deny | permit> <protocol> <source address> <source wildcard mask> <destination address> <destination wildcard mask> <operator> <port>

ตัวอย่าง *access-list 100 deny tcp 172.18.16.0 0.0.0.255 any eq ftp*

หมายความว่า ไม่อนุญาตการทำ FTP จากทุกๆ โฮสต์ ที่มี IP 172.18.16.x ไปยังทุกๆ ปลายทาง

ขั้นตอนการกำหนด ACL

ออกแบบและเขียน ACL ตามนโยบายความปลอดภัยของระบบที่อยู่ในการพิจารณา

1. นำ ACL สู่เราท์เตอร์ สามารถทำได้หลายวิธีคือ การป้อนผ่านบรรทัดคำสั่ง และการใช้ TFTP

2. นำ ACL ที่กำหนดขึ้นนั้นไปใช้กับอินเตอร์เฟสของเราท์เตอร์ที่ต้องการ

3.5.2 รูปแบบของกฎตามแบบ SNORT

โปรแกรม IDS ชื่อ SNORT เป็นระบบที่ใช้ตรวจสอบการรุกราน (Intrusion Detection System) ขนาดย่อมซึ่งมีความสามารถในการวิเคราะห์การจราจรในเครือข่ายแบบ real-time ภาษาในการอธิบายนโยบายที่ SNORT ใช้นั้นอยู่ในรูปแบบของกฎ (rule-based) ที่มีความยืดหยุ่นสูงและมีกฎที่กำหนดไว้แล้วสามารถนำมาใช้งานได้ทันที

รูปแบบของการกำหนดกฎของ SNORT

รูปแบบข้อกำหนดสำคัญของกฎแต่ละข้อที่ใช้ใน SNORT นั้นคือต้องจบภายในบรรทัดเดียว ประกอบไปด้วยรูปแบบดังนี้

[rule action] [protocol] [ip address/mask] [port] [direction operator] [ip address/mask] [port] ([rule options])

ส่วนที่อยู่ด้านหน้าวงเล็บที่เป็นส่วนที่เรียกว่า Rule header ซึ่งประกอบไปด้วย Rule Action, Protocol และหมายเลข IP กับพอร์ตของต้นทางและปลายทาง

Rule Action ประกอบไปด้วยการกระทำสามแบบคือ alert ซึ่งเป็นการเตือนตามรูปแบบที่ได้กำหนดไว้พร้อมกับบันทึกแพ็กเกตนั้นไว้ log เพื่อบันทึกแพ็กเกตนั้น และ pass คือทิ้งแพ็กเกตนั้นไป

Protocol สนับสนุนโปรโตคอล TCP, UDP และ ICMP

IP Address และ Port ส่วนนี้สามารถใช้คำว่า any เพื่อกำหนดว่าเป็น IP address อะไรก็ได้ สำหรับ IP address นั้นจะต้องมีการระบุ netmask ในรูปจำนวนบิตด้วย เครื่องหมาย ! นั้นใช้บอกว่าเป็น IP address ที่ยกเว้น ส่วน port นั้นสามารถใช้เครื่องหมาย : บอกช่วงได้

Direction Operation ใช้เครื่องหมาย -> บอกทิศทางของแพ็กเกต โดยด้านซ้ายแสดงถึงต้นทางและด้านขวาเป็น ปลายทาง ส่วนเครื่องหมาย < > ใช้บอกว่าเป็นการพิจารณาแบบสองทิศทาง

Rule options แต่ละ rule option ในวงเล็บจะต้องลงท้ายด้วยเครื่องหมาย ; และใช้เครื่องหมาย : คั่นระหว่าง Rule option keyword กับ argument ของมัน

ตัวอย่างกฎตามแบบ SNORT

Log udp any any -> 192.168.1.0/24 1:1024

หมายความว่า บันทึก UDP traffic ที่มาจาก port ใดๆ ไปยัง port 1 ถึง 1024 ในเครือข่าย 192.168.1.0

Alert tcp any any -> 192.168.1.0/24 111 (content : "|00 01 86 a5|"; msg: "mountd access";)

หมายความว่า เตือนเมื่อมี TCP traffic จาก port ใดๆ ไปยัง port 111 ในเครือข่าย 192.168.1.0 โดยประกอบไปด้วยข้อมูลตามรูปแบบที่กำหนด โดยให้มีการบันทึกข้อความว่า mountd access ลงไปด้วย

บทที่ 4
ทฤษฎีเกี่ยวกับการประกอบธุรกิจ

โดยที่การดำเนินโครงการทุกประเภทย่อมต้องเกี่ยวพันกับเงินเสมอ โดยเงินจะเป็นตัวหล่อเลี้ยงและหล่อลื่นโครงการตราบที่โครงการนั้นยังดำเนินการอยู่ การหมุนเวียนของเงินในโครงการจึงเปรียบเสมือนการหมุนเวียนของโลหิตในร่างกายมนุษย์ เมื่อไหร่ที่การหมุนเวียนของเงินหยุดชะงัก การดำเนินงานของโครงการก็ย่อมสิ้นสุดลงตามไปด้วย (ฐาปนา ฉิ่นไพศาล และ อัจฉรา ชีวะตระกูลกิจ. 2542.)

หน้าที่ทางการจัดการการเงินสำหรับโครงการ จะครอบคลุม ใน 2 ประเด็นใหญ่ๆ ดังนี้

1. หน้าที่ในการจัดหาเงินทุนมาใช้ในโครงการ (Acquisition)
2. หน้าที่ในการจัดสรรเงินทุนของโครงการ (Allocation)

ในการจัดหาเงินทุนมาใช้ในธุรกิจ ผู้บริหารโครงการจะต้องพยากรณ์ความต้องการเงินทุนของโครงการ ทั้งในแง่จำนวนเงินและเวลาที่ต้องการใช้เงินทุนนั้นๆ ซึ่งอาจแบ่งเป็นระยะสั้นและระยะยาว จากนั้นผู้บริหารโครงการก็จะต้องตัดสินใจเกี่ยวกับการเลือกแหล่งเงินทุนซึ่งแบ่งออกเป็น 2 ประเภทใหญ่ๆ คือ แหล่งเงินทุนจากหนี้สิน และแหล่งเงินทุนจากส่วนของเจ้าของ

แหล่งเงินทุนจากหนี้สินอาจจัดหาจากแหล่งหนี้สินระยะสั้น หรือที่เรียกว่าหนี้สินหมุนเวียน ตัวอย่างเช่น เจ้าหนี้การค้า ตั๋วเงินจ่าย ส่วนแหล่งหนี้สินระยะยาว เช่น การออกหุ้นกู้ หรือการกู้เงินระยะยาวจากสถาบันการเงิน เป็นต้น

แหล่งเงินทุนจากส่วนของเจ้าของ จัดเป็นแหล่งเงินทุนระยะยาว ซึ่งอาจหาได้จากการออกหุ้นทุน ได้แก่ หุ้นบุริมสิทธิ์ หรือหุ้นสามัญจำหน่าย

เนื่องจากโครงการที่จะลงทุน อาจจัดตั้งได้หลายรูปแบบ ซึ่งอาจเป็นกิจการเจ้าของคนเดียว ห้างหุ้นส่วนหรือบริษัทจำกัด ซึ่งในแต่ละรูปแบบจะทำให้กิจการมีโอกาสในการจัดหาเงินทุนต่างกันออกไป โดยรูปแบบของบริษัทจำกัดจะเป็นรูปแบบที่มีโอกาสจัดหาเงินทุนจากแหล่งต่างๆ ได้มากที่สุด เพราะสถาบันการเงินที่จะให้กู้ยืมจะให้ความเชื่อถือมากกว่ารูปแบบอื่นๆ เนื่องจากการบริหารในรูปบริษัททำโดยคณะบุคคลในรูปของคณะกรรมการบริษัท ส่วนรูปแบบเจ้าของคนเดียวและห้างหุ้นส่วนจำกัดนั้น การบริหารจะจำกัดอยู่ที่ตัวบุคคลไม่กี่ราย

สำหรับข้อควรพิจารณาในการจัดหาเงินทุนมาใช้นั้น ผู้บริหารโครงการควรพิจารณาที่ต้นทุน เงินทุน ความเสี่ยงทางการเงิน ระยะเวลาครบกำหนด ภาระผูกพัน ความยากง่ายในการจัดหาตลอดจนเงื่อนไขที่เจ้าของเงินทุนกำหนด ดังนั้นในการจัดหาเงินทุนมาใช้ในโครงการ ผู้บริหาร

จะต้องทำหน้าที่ตัดสินใจว่าควรจะจัดหาเงินทุนจากแหล่งใด และเป็นสัดส่วนอย่างไร ระหว่างเงินทุนจากแหล่งหนี้สินและส่วนของเจ้าของ จึงจะทำให้ต้นทุนของเงินทุนเฉลี่ยของโครง การต่ำที่สุด โดยไม่เกิดความเสี่ยงทางการเงินมากเกินไป

ส่วนหน้าที่การจัดสรรเงินทุนที่โครงการจัดหามาให้นั้น ผู้บริหารโครงการจะต้องรู้จักจัดสรรเงินทุนเพื่อการลงทุนในสินทรัพย์ของโครงการอย่างมีประสิทธิภาพ ทั้งนี้เพื่อให้เกิดประโยชน์ต่อโครงการให้มากที่สุด การจัดสรรเงินทุนหรือการใช้เงินทุนนี้สามารถแบ่งได้เป็น 2 ประเภทใหญ่ๆ คือ การลงทุนในสินทรัพย์หมุนเวียน และการลงทุนในสินทรัพย์ถาวร

การลงทุนในสินทรัพย์หมุนเวียน ได้แก่ การลงทุนในรูปของเงินสด หลักทรัพย์ในความต้องการของตลาด ลูกหนี้การค้า สินค้าคงเหลือ ฯลฯ โดยผู้บริหารโครงการจะต้องตัดสินใจว่าควรจะลงทุนในสินทรัพย์หมุนเวียนแต่ละประเภท ในระดับที่ก่อให้เกิดความสามารถในการทำกำไรให้แก่โครงการสูงสุดเท่าที่เป็นไปได้ โดยมีสภาพคล่องในระดับที่เหมาะสมด้วย

การลงทุนในสินทรัพย์ถาวรส่วนใหญ่เป็นเรื่องของงบประมาณลงทุน (Capital Budgeting) กล่าวคือ เป็นการตัดสินใจจัดสรรเงินทุนเพื่อลงทุนในสินทรัพย์ที่ก่อให้เกิดผลตอบแทนในอนาคต เช่น การลงทุนในอุปกรณ์ อาคาร หรือที่ดิน เป็นต้น ในการตัดสินใจของผู้บริหารโครงการจะพิจารณาที่องค์ประกอบและคุณภาพของสินทรัพย์ และความเสี่ยงที่จะเกิดขึ้นจากการลงทุนนั้นๆ โดยผู้บริหารโครงการจะตัดสินใจลงทุนในสินทรัพย์ใดหรือไม่นั้น จะขึ้นอยู่กับผลตอบแทนที่คาดว่าจะได้รับเปรียบเทียบกับต้นทุนที่ต้องจ่ายว่าคุ้มค่ากันหรือไม่

อย่างไรก็ตาม หน้าที่ในการจัดหาเงินทุนกับหน้าที่ในการจัดหาเงินทุนของโครงการก็มีความสัมพันธ์กันเป็นอย่างยิ่ง กล่าวคือในการตัดสินใจจัดหาเงินทุน ผู้จัดหาจำเป็นต้องทราบต้นทุนเงินทุนจากแต่ละแห่งและในกรณีที่โครงการใช้เงินทุนจากหลายแหล่งก็จำเป็นต้องคำนวณหาต้นทุนเงินทุนถัวเฉลี่ยด้วย ทั้งนี้เพราะการทราบต้นเงินทุนถัวเฉลี่ยจะนำไปใช้เปรียบเทียบกับผลตอบแทนของโครงการ นั่นเอง

4.1 แหล่งเงินทุนของโครงการ (ฐาปนา ฉิ่นไพศาล และ อัจฉรา ชีวะตระกูลกิจ. 2542.)

4.1.1 แหล่งเงินทุนระยะสั้น

เงินทุนระยะสั้น หมายถึง เงินทุนที่มีระยะเวลาในการชำระคืนภายในระยะเวลา 1 ปี เงินทุนระยะสั้นนี้จะนำมาใช้เป็นเงินทุนหมุนเวียนในโครงการ เช่น ใช้ลงทุนในลูกหนี้การค้า สินค้าคงเหลือ หรือ เพื่อจ่ายค่าใช้จ่ายล่วงหน้าต่างๆ

แหล่งเงินทุนระยะสั้นสามารถ จำแนกได้เป็น 3 แหล่ง ดังนี้

1.1 สินเชื่อทางการค้า (Trade credit)

1.2 ตราสารพาณิชย์ หรือเอกสารการค้า (Commercial paper)

1.3 เงินกู้ระยะสั้น (Short term loans)

สินเชื่อทางการค้า

สินเชื่อทางการค้า หมายถึงสินเชื่อที่ได้จากการซื้อวัตถุดิบเป็นเงินเชื่อ ซึ่งนับว่าเป็นแหล่งเงินทุนที่สำคัญของธุรกิจในทางปฏิบัติ โดยปกติผู้ขายสินค้ามักยินดีที่จะให้สินเชื่อแก่ผู้ซื้อตามประเพณีทางการค้าหรือเนื่องจากการแข่งขัน สินเชื่อทางการค้าจึงเป็นแหล่งเงินที่โครงการมักจะได้รับมาโดยอัตโนมัติ (Spontaneous source of funds) ซึ่งเรียกได้อีกอย่างหนึ่งว่าเจ้าหนี้การค้า เจ้าหนี้การค้าจะไม่มีค่าใช้จ่ายหรือต้นทุนของเงินทุน ทั้งนี้เพราะในการขายสินค้าเป็นเงินเชื่อนั้น ผู้ขายไม่ได้เพิ่มราคาให้สูงกว่าการขายเป็นเงินสด)ยกเว้นในกรณีที่มีการเสนอส่วนลดเงินสดและโครงการไม่รับก็จะเกิดต้นทุนของเงินทุนขึ้น ซึ่งก็คือต้นทุนค่าเสียโอกาสนั่นเอง (ดังนั้น สินเชื่อทางการค้าจึงเป็นแหล่งเงินทุนแหล่งแรกที่ทุก โครงการควรจัดหามาด้วยการซื้อสินค้าเป็นเงินเชื่อให้มากที่สุด นอกจากนี้ยังควรต้องต่อรองให้ผู้ขายกำหนดระยะเวลาชำระหนี้ให้ยาวนานด้วย ซึ่งอย่างน้อยระยะเวลาชำระหนี้ควรยาวกว่าหรือเท่ากับระยะเวลาที่โครงการให้สินเชื่อแก่ลูกหนี้ของโครงการเอง

ตราสารพาณิชย์หรือเอกสารการค้า

แหล่งเงินทุนระยะสั้นอีกแหล่งหนึ่งของโครงการ ก็คือการออกตราสารพาณิชย์ชนิดที่ไม่มีหลักทรัพย์ค้ำประกันจำหน่ายในตลาดเงิน ซึ่งอาจจะออกมาในรูปตั๋วสัญญาใช้เงินที่ไม่มีหลักทรัพย์ค้ำประกัน หรือตั๋วเงินกู้ที่ไม่มีหลักทรัพย์ค้ำประกัน โดยจะนำออกจำหน่ายให้กับผู้สนใจซึ่งอาจจะเป็นบุคคลธรรมดาทั่วไป ธุรกิจหรือสถาบันการเงินที่ต้องการจะลงทุนระยะสั้นจากการที่มีเงินสดเหลืออยู่ในมือเป็นการชั่วคราว

ตราสารพาณิชย์มักมีอายุสั้น ซึ่งอาจมีอายุไม่ถึงสัปดาห์ และอย่างมากที่สุดไม่เกิน 12 เดือน และเนื่องจากเป็นตราสารที่ไม่มีหลักทรัพย์ค้ำประกันดังกล่าว โครงการที่จะสามารถจัดหาเงินทุนโดยวิธีนี้ จึงต้องเป็นโครงการขนาดใหญ่ที่เจ้าของโครงการมีชื่อเสียงทางการค้าดี และมีฐานะทางการเงินที่น่าเชื่อถือ

เงินกู้ระยะสั้น

เงินกู้ระยะสั้น สามารถแบ่งได้เป็น 2 ชนิด ดังนี้

1. เงินกู้ชนิดไม่มีหลักทรัพย์ค้ำประกัน (Unsecured loans)
2. เงินกู้ชนิดมีหลักทรัพย์ค้ำประกัน (Secured loans)

4.1.2 แหล่งเงินทุนระยะยาว

เงินทุนระยะยาว หมายถึง เงินทุนที่มีระยะเวลาในการชำระคืนเกินกว่า 1 ปี ขึ้นไป โครงการควรนำเงินทุนระยะยาวนี้ไปลงทุนในสินทรัพย์ถาวรซึ่งมีอายุการใช้งานยาวนา และยังรวมไปถึงการลงทุนในสินทรัพย์หมุนเวียนในส่วนที่เป็นสินทรัพย์หมุนเวียนถาวรอีกด้วย

หนี้สินระยะยาว คือ เงินทุนที่หามาโดยการก่อหนี้ที่มีระยะเวลาชำระคืนเกินกว่า 1 ปีขึ้นไป การจัดหาเงินทุนระยะยาวโดยการก่อหนี้ อาจทำได้ดังนี้

1. การกู้ยืมระยะยาว
2. การออกหุ้นกู้หรือพันธบัตร

การกู้ยืมระยะยาว (Long term debt) เป็นการหาเงินทุนจากการกู้ยืมจากธนาคารพาณิชย์หรือสถาบันการเงินอื่นๆ ต้นทุนของการกู้ยืมระยะยาวโดยทั่วไปจะเท่ากับดอกเบี้ยที่กำหนด อย่างไรก็ตามการกู้ยืมจากธนาคารพาณิชย์อาจมีการกำหนดเงินฝากขั้นต่ำ (Compensation balance) หรือคิดค่าธรรมเนียมเงินกู้ หรือกำหนดให้จ่ายดอกเบี้ยล่วงหน้า ซึ่งสิ่งเหล่านี้จะทำให้ต้นทุนสูงขึ้นเป็นเหตุให้ผู้บริหารต้องคำนวณหาต้นทุนของการกู้ยืมที่แท้จริง (Effective rate) ต่อไป

หุ้นกู้หรือพันธบัตร (Bond) เป็นตราสารที่กิจการผู้ออกซึ่งมีฐานะเป็นผู้กู้จะมอบให้แก่ผู้ซื้อตราสารนั้นไว้เป็นหลักฐานในการกู้เงิน โดยที่ใบหุ้นกู้แต่ละฉบับจะระบุมูลค่าที่ตราไว้ (Face value) ชื่อบริษัทผู้ออก อัตราดอกเบี้ย (Coupon rate) วันที่ออกหุ้น (Issued date) และวันที่ถึงกำหนดไถ่ถอน (Maturity) ไว้บนใบหุ้นนั้น

ส่วนของเจ้าของ

เงินทุนส่วนของเจ้าของคือ เงินทุนที่ได้จากการจำหน่ายหุ้นทุน ซึ่งแยกได้เป็น 2 แหล่งใหญ่ๆ คือ

1. การออกหุ้นบุริมสิทธิ
2. การออกหุ้นสามัญ

หุ้นบุริมสิทธิ (Preferred stock) เป็นแหล่งเงินทุนที่มีลักษณะกึ่งหนี้สินและกึ่งเจ้าของ กล่าวคือ เหมือนหุ้นสามัญตรงที่มีการจ่ายเงินปันผล และยังถูกจัดรวมอยู่ในส่วนทุน (Capital) ของกิจการ แต่ก็มีลักษณะเหมือนหุ้นระยะยาวตรงที่ระบุจ่ายเงินปันผลในอัตราคงที่เหมือนหุ้นกู้ หุ้นบุริมสิทธิไม่มีการกำหนดอายุไถ่ถอน จึงนับเป็นเงินลงทุนระยะยาว ในกรณีที่เลิกกิจการ ผู้ถือหุ้นบุริมสิทธิแม้จะได้สิทธิในการเรียกร้องสินทรัพย์ก่อนหุ้นสามัญแต่ก็หลังเจ้าหนี้ ดังนั้นถ้าหลังจากชำระหนี้สินแล้วไม่มีทรัพย์สินเหลืออยู่ ทั้งหุ้นบุริมสิทธิและหุ้นสามัญก็จะต้องรับส่วนที่ขาดทุนนั้นไป นอกจากนี้ การจ่ายเงินปันผลสำหรับหุ้นบุริมสิทธิบางประเภทยังอาจระงับไม่จ่ายเงินปันผลได้

หากบริษัทขาดทุนหรืออยู่ในสภาวะการเงินที่ไม่ค่อยดี ซึ่งต่างจากหนี้สินที่บริษัทมีภาระผูกพันที่จะต้องจ่ายดอกเบี้ยอย่างแน่นอน ไม่ว่าฐานะการเงินของบริษัทจะเป็นอย่างไร

หุ้นสามัญ (Common stock) ถือว่าเป็นส่วนทุนของเจ้าของอย่างแท้จริง ซึ่งผู้ลงทุนในหุ้นชนิดนี้จะมีสิทธิในการควบคุมการดำเนินงานของกิจการ และถ้ากิจการประสบความสำเร็จในการดำเนินงานผลตอบแทนที่ผู้ถือหุ้นจะได้รับก็จะสูงตามไปด้วย แต่ในขณะเดียวกันผู้ถือหุ้นสามัญก็ต้องรับความเสี่ยงในการดำเนินงานของกิจการอย่างเต็มที่เช่นกัน กล่าวคือ ถ้าบริษัทขาดทุน ผู้ถือหุ้นสามัญจะต้องรับส่วนของการขาดทุนนั้นด้วย

4.2 ต้นทุนเงินทุนของโครงการ

เงินทุนระยะยาวที่โครงการต้องการจัดหาเพื่อนำมาลงทุนในสินทรัพย์ โครงการอาจจัดหามาจากแหล่งเงินทุนเพียงแหล่งเดียวหรือจากหลายแหล่ง ซึ่งเงินทุนที่ได้จากแต่ละแหล่งจะต้องเสียต้นทุนหรือค่าใช้จ่ายในรูปแบบที่แตกต่างกัน เช่น เงินทุนที่ได้จากการก่อหนี้ระยะยาว จะต้องเสียค่าใช้จ่ายในรูปของดอกเบี้ย ซึ่งเรียกว่า ต้นทุนเงินทุนของหนี้ (Cost of debt) ส่วนเงินทุนที่ได้มาจากการออกหุ้นบุริมสิทธิหรือหุ้นสามัญ โครงการจะต้องจ่ายผลตอบแทนให้แก่ผู้ถือหุ้นบุริมสิทธิและหุ้นสามัญในรูปของเงินปันผล ต้นทุนที่เกิดขึ้นจึงเรียกว่า ต้นทุนเงินทุนของหุ้นบุริมสิทธิ (Cost of preferred stock) และต้นทุนเงินทุนของหุ้นสามัญ (Cost of common stock)

4.2.1 ต้นทุนเงินทุนของหนี้

ต้นทุนเงินทุนของเงินกู้ยืมระยะยาว

ในการกู้ยืมเงินโดยทั่วไปผู้กู้จะต้องมีการตกลงเรื่องอัตราดอกเบี้ยกัน ซึ่งอัตราดอกเบี้ยดังกล่าวมักจะเป็นอัตราดอกเบี้ยลอยตัว (Floating rate) ซึ่งขึ้นลงได้ตามสภาวะการในตลาด ซึ่งผู้วิเคราะห์โครงการจำเป็นที่จะต้องคาดคะเนอัตราดอกเบี้ยล่วงหน้า ตลอดระยะเวลาการกู้ยืม ไว้ที่อัตราดอกเบี้ยหนึ่งๆ ที่คิดว่าเป็นอัตราดอกเบี้ยที่คาดว่าจะจ่ายมากที่สุด ซึ่งโดยทั่วไปก็มักยึดที่อัตราดอกเบี้ยในขณะที่จะเริ่มทำโครงการ ซึ่งได้จากการสอบถามผู้ให้กู้ที่หมายตาไว้นั่นเอง

ต้นทุนเงินทุนของหุ้นกู้

โดยปกติอัตราดอกเบี้ยของหุ้นกู้ที่กำหนดไว้บนใบหุ้นกู้จะเป็นอัตราคงที่ ไม่ขึ้นลงตามภาวะตลาด แต่ราคาที่จำหน่ายของหุ้นกู้จะขึ้นอยู่กับภาวะตลาดในขณะนั้นที่ออกหุ้นกู้จำหน่าย ซึ่งมีผลให้ราคาหุ้นกู้ที่จำหน่ายได้ อาจสูงหรือต่ำกว่าราคาที่ตราไว้หน้าหุ้นกู้ (Face value) ก็ได้ นอกจากนี้ในการจำหน่ายหุ้นกู้ยังอาจมีค่าใช้จ่ายในการจำหน่ายอื่นๆ เกิดขึ้นด้วย ซึ่งมีผลให้ราคาขายสุทธิของหุ้นกู้ที่จำหน่ายได้น้อยลงไป

4.3 ผลของภาษีที่มีต่อต้นทุนเงินทุนของหนี้

โดยที่ดอกเบี้ยจ่ายที่เกิดจากการจัดหาเงินทุนโดยการก่อหนี้ ไม่ว่าจะเป็นวิธีกู้ยืมเงินจากสถาบันการเงินหรือการออกหุ้นกู้ก็ตาม ถือเป็นค่าใช้จ่ายของกิจการที่สามารถนำไปหักออกจากกำไรจากการดำเนินงานได้เป็นผลให้ภาษีที่ต้องจ่ายในปีนั้นๆ ลดลง ดังนั้นการหาต้นทุนของหนี้ จึงควรคำนึงถึงผลดีในแง่ภาษีจ่ายที่ลดลงนี้ด้วย หรืออีกนัยหนึ่งก็คือ ต้นทุนของหนี้สินจะลดลงเท่ากับภาษีที่ประหยัดได้ ดังนั้น ในการคำนวณหาต้นทุนของหนี้จึงควรหาต้นทุนของหนี้จึงควรหาเป็นต้นทุนหลังภาษี

4.4 การประมาณการด้านการเงินของโครงการ

โดยที่โครงการเป็นกิจกรรมที่เกี่ยวกับการใช้ทรัพยากรต่างๆ เพื่อหวังผลประโยชน์ตอบแทนในอนาคต ดังนั้นจึงอาจเปรียบโครงกาเป็นเสมือนหน่วยผลิตที่ทำการแปลงสภาพทรัพยากรหรือปัจจัยการผลิต (Inputs) ให้กลายเป็นผลผลิต (Outputs) ซึ่งปัจจัยการผลิตที่ใส่เข้าไปนี้เมื่อทำการคิดเป็นมูลค่าหรือตัวเงินแล้ว ก็คือต้นทุน หรือค่าใช้จ่าย (Cost) ของโครงการ ในขณะที่ผลผลิตที่ออกมาจากโครงการเมื่อคิดเป็นมูลค่าหรือตัวเงินก็คือผลตอบแทน (Benefit) ของโครงการ นั่นเอง

จากการศึกษาความเป็นไปได้ ของโครงการเป็นกิจกรรมที่จะต้องกระทำล่วงหน้าก่อนที่โครงการจะเกิดขึ้นจริง ดังนั้นจึงต้องมีประมาณการด้านการเงินของโครงการ ซึ่งก็คือการประมาณการค่าใช้จ่ายและผลตอบแทนที่จะได้รับจากการทำโครงการนั้นๆ ว่าจะเป็นจำนวนเงินเท่าใดและเป็นระยะเวลากี่ปี การประมาณการค่าใช้จ่ายและผลตอบแทนของโครงการนี้จะเป็นข้อมูลสำคัญที่จะนำไปใช้ในการวิเคราะห์ด้านการเงิน ซึ่งจะช่วยในการตัดสินใจของผู้บริหารว่า โครงการดังกล่าวว่าควรจะลงทุนหรือไม่ ดังนั้น ถ้าการประมาณค่าใช้จ่ายต่ำกว่าที่ควรจะเป็น ซึ่งพอดำเนินการจริงก็จะเกิดความเสียหายขึ้น ดังนั้นผู้วิเคราะห์จึงควรต้องใช้ความระมัดระวังในการประมาณการด้านการเงินดังกล่าว เป็นอย่างยิ่ง

ค่าใช้จ่ายของโครงการ

ค่าใช้จ่ายของโครงการ อาจแบ่งได้เป็น 2 ลักษณะคือ ค่าใช้จ่ายที่มีตัวตน (Tangible costs) และค่าใช้จ่ายที่ไม่มีตัวตน (Intangible costs) ค่าใช้จ่ายที่มีตัวตน หมายถึง ค่าใช้จ่ายที่สามารถคิดเป็นมูลค่าหรือตัวเงินได้ ขณะที่ค่าใช้จ่ายที่ไม่มีตัวตน จะหมายถึงค่าใช้จ่ายที่ไม่สามารถคิดออกมาเป็นมูลค่าหรือตัวเงินได้

ค่าใช้จ่ายที่มีตัวตน ยังสามารถแบ่งตามหน้าที่ออกได้เป็น 2 ประเภท คือ ค่าใช้จ่ายลงทุน (Investment costs) และค่าใช้จ่ายในการดำเนินงาน (Operating costs)

ค่าใช้จ่ายทุน

ค่าใช้จ่ายลงทุน หมายถึง มูลค่าของทรัพยากรที่ใช้ไปเพื่อเป็นฐานหรือสร้างสิ่งอำนวยความสะดวกในการผลิตหรือให้บริการ ค่าใช้จ่ายลงทุน หรือเรียกอีกอย่างหนึ่งว่า เงินลงทุนในโครงการ โดยทั่วไปจะประกอบด้วย

1. เงินลงทุนในสินทรัพย์ถาวร หมายถึง เงินลงทุนในสินทรัพย์ที่มีอายุการใช้งานมากกว่า 1 ปี และโครงการจำเป็นต้องใช้ในการดำเนินงาน ซึ่งได้แก่

1.1 ที่ดินและค่าพัฒนาที่ดิน เช่น ค่าถมดิน ค่าทำถนน ค่าติดตั้งเสาไฟฟ้าและค่าทำรั้ว

1.2 อาคารและสิ่งก่อสร้างอื่นๆ เช่น ค่าอาคารโรงงาน ค่าก่อสร้างบ้านพักคนงาน ค่าก่อสร้างโกดังเก็บวัตถุดิบ ซึ่งจะรวมถึง ค่าติดตั้งระบบไฟฟ้า น้ำประปาและระบบโทรศัพท์

1.3 เครื่องจักรและอุปกรณ์ เช่น ค่าเครื่องจักร เครื่องมือและอุปกรณ์ในการผลิต ค่าอุปกรณ์การขนถ่ายวัสดุ ค่าเครื่องมือต่างๆ ในโรงงาน อุปกรณ์และเครื่องใช้ในสำนักงาน

2. ค่าใช้จ่ายก่อนการดำเนินงาน หมายถึง ค่าใช้จ่ายที่เกิดขึ้นนับตั้งแต่เริ่มโครงการจนถึงวันที่เริ่มดำเนินการผลิตหรือให้บริการ แต่ถ้าเป็นกรณีโครงการขยายกิจการ จะหมายถึงค่าใช้จ่ายที่เกิดขึ้นตั้งแต่เริ่มโครงการจนถึงวันที่มีรายได้ส่วนเพิ่มจากการขยายกิจการ ค่าใช้จ่ายก่อนการดำเนินงานโดยทั่วไป ได้แก่ เงินเดือนผู้บริหารและเจ้าหน้าที่ของโครง ค่าเดินทาง ค่าเช่าสำนักงาน ค่าธรรมเนียมในการขออนุญาตตั้งกิจการ ค่าใช้จ่ายในการติดต่อขอกู้เงิน ค่าฝึกอบรมพนักงาน ค่าใช้จ่ายในการทดลองเครื่อง ค่าดอกเบี้ยเงินกู้ระหว่างก่อสร้าง ค่าโฆษณาประชาสัมพันธ์ก่อนเริ่มโครงการ เป็นต้น

3. เงินทุนหมุนเวียน หมายถึง เงินทุนหมุนเวียนสุทธิที่จำเป็นต้องใช้ในการดำเนินงานโครงการ ซึ่งหาได้จากสินทรัพย์หมุนเวียน ซึ่งโดยปกติโครงการจะต้องเตรียมเงินทุนหมุนเวียนนี้ไว้นอกเหนือจากค่าใช้จ่ายลงทุนประเภทอื่น ทั้งนี้เพื่อความราบรื่นในการดำเนินงาน อย่างไรก็ตามเมื่อโครงการสิ้นสุดลง เงินทุนหมุนเวียนนี้ก็จะกลับคืนมาเป็นผลตอบแทนในปีสุดท้ายของโครงการ เนื่องจากเงินทุนที่ลงทุนเป็นเงินทุนหมุนเวียนไม่ได้จ่ายแล้วจ่ายเลย แต่ใช้หมุนเวียนอยู่ในโครงการ ดังนั้นเมื่อสิ้นสุดโครงการจึงได้รับกลับคืนมา

ค่าใช้จ่ายในการดำเนินงาน

ค่าใช้จ่ายในการดำเนินงาน หมายถึง มูลค่าของทรัพยากรที่ใช้ไปเพื่อการดำเนินงานของโครงการ หรืออีกนัยหนึ่งก็คือจำนวนเงินที่โครงการจ่ายออกไปเพื่อการดำเนินงานตามปกติของโครงการนั่นเอง ค่าใช้จ่ายในการดำเนินงานโดยทั่วไปประกอบด้วย 2 ประเภทคือ

1. ค่าใช้จ่ายในการผลิตหรือต้นทุนผลิต หมายถึง ค่าใช้จ่ายทั้งหมดที่เกี่ยวกับการผลิตสินค้าหรือการให้บริการประกอบด้วย

1.1 ค่าวัตถุดิบทางตรง ได้แก่ ต้นทุนวัตถุดิบที่ใช้เป็นส่วนสำคัญของการผลิตสินค้า หรือการให้บริการ

1.2 ค่าแรงทางตรง ได้แก่ ต้นทุนแรงงานที่ใช้โดยตรงในการผลิสินค้าหรือให้บริการ

1.3 ค่าใช้จ่ายการผลิต ได้แก่ ต้นทุนการผลิตทั้งหมดที่จำเป็นต้องใช้ นอกเหนือจากวัตถุดิบทางตรง และค่าแรงทางตรง ตัวอย่างเช่น ค่าวัตถุดิบทางอ้อม ค่าแรงทางอ้อม ค่าน้ำ-ไฟ ค่าเสื่อมราคาและค่าประกันภัยเครื่องจักร ของใช้สิ้นเปลือง

2. ค่าใช้จ่ายในการขายและบริหาร หมายถึง ค่าใช้จ่ายทั้งหมดที่เกี่ยวกับการขายและบริหารซึ่งเป็นค่าใช้จ่ายที่ไม่เกี่ยวข้องกับการผลิตสินค้าหรือให้บริหารโดยตรง เช่น เงินเดือนผู้บริหาร ค่านายหน้าพนักงาน ค่าเช่าสำนักงาน ค่าน้ำ-ไฟ ในสำนักงาน ค่าเสื่อมราคาอุปกรณ์ในสำนักงาน ค่าประกันภัยสำนักงาน

ค่าใช้จ่ายที่ไม่มีตัวตน

ค่าใช้จ่ายที่ไม่มีตัวตน หมายถึง ค่าใช้จ่ายที่ไม่สามารถคำนวณออกมาเป็นตัวเงินได้ เช่น โครงการที่จะทำอาจมีผลกระทบต่อสังคม หรือ ศิลปวัฒนธรรม

4.5 ขั้นตอนการประมาณค่าใช้จ่ายของโครงการ

1. ระบุรายการและปริมาณค่าใช้จ่าย
2. ตีราคาค่าใช้จ่าย
3. รวมค่าใช้จ่ายเป็นรายปี

ขั้นตอนที่ 1 ระบุรายการและปริมาณค่าใช้จ่าย

ค่าใช้จ่ายโครงการ คือมูลค่าของปัจจัยการผลิตหรือทรัพยากรที่โครงการใช้ไป ดังนั้นการประมาณการค่าใช้จ่ายต่างๆ ของโครงการ จึงควรเริ่มต้นจากการระบุว่าถ้ามีการลงทุนก่อสร้างตามแผนงานโครงการแล้ว จะต้องมีการใช้ปัจจัยการผลิตหรือทรัพยากรอะไรบ้างและปริมาณมากน้อยเพียงใดและหลังจากพยายามระบุค่าใช้จ่ายที่เกี่ยวของในทุกประเภทออกมาได้แล้ว จากนั้นก็ให้การจัดประเภทค่าใช้จ่ายออกเป็นหมวดหมู่ต่างๆ เช่น ค่าที่ดิน ค่าอาคารและสิ่งก่อสร้าง ค่าเครื่องจักรและอุปกรณ์เป็นต้น

ขั้นตอนที่ 2 ตีราคาค่าใช้จ่าย

การตีราคาค่าใช้จ่าย คือการนำราคาที่เหมาะสมมาตีค่ารายการค่าใช้จ่ายที่ระบุไว้แล้วในขั้นตอนที่ 1 ทั้งนี้ เพื่อจะได้ประมาณการรายการค่าใช้จ่ายที่ระบุให้เป็นตัวเงิน เนื่องจากปัจจัยการผลิตหรือทรัพยากรที่ใช้ในโครงการมีหน่วยไม่เหมือนกัน การตีราคาค่าใช้จ่ายจะต้องมีการกำหนด

ราคาที่ใช้ในการตีราคาที่เหมาะสม เพราะหากมีการใช้ราคาที่ไม่เหมาะสม อาจนำไปสู่ความผิดพลาดในการประเมินค่าโครงการในที่สุด อย่างไรก็ตาม ราคาที่อาจนำมาใช้ได้มี 2 ชนิด คือ ราคาตลาด (Market price) และราคาเงา (Shadow price)

ราคาตลาด หมายถึง ราคาที่กำหนดขึ้นโดยเปิดเผย ซึ่งสามารถสังเกตได้จากการซื้อขายจริงในตลาด ราคาตลาดจะเป็นราคาจริง (Actual price) ของปัจจัยการผลิตที่มีการซื้อขายกันภายใต้ระบบการแลกเปลี่ยนตามปกติ ราคาตลาดจึงสามารถนำมาใช้ในการตีราคาปัจจัยการผลิตของโครงการได้ และเพื่อให้ได้มาซึ่งราคาตลาด ผู้วิเคราะห์โครงการอาจใช้วิธีสอบถามราคาปัจจัยการผลิตที่ต้องการจากแหล่งข้อมูลต่างๆ ซึ่งอาจจะเป็นผู้ค้าส่งหรือผู้ค้าปลีกหรือผู้ขายปัจจัยการผลิตนั้นๆ ส่วนถ้าเป็นประเภทค่าก่อสร้าง ก็อาจสอบถามจากผู้รับเหมา หรือราคาที่วิศวกรประมาณการไว้ เป็นต้น

ราคาเงา หมายถึง ราคาที่ควรจะเป็นในระบบเศรษฐกิจที่มีดุลยภาพ ภายใต้เงื่อนไขของการแข่งขันที่สมบูรณ์ ราคาเงาเป็นราคาสมมติที่จะสะท้อนถึงค่าเสียโอกาสที่แท้จริงของปัจจัยการผลิต ราคาเงาจึงเป็นแนวคิดในทางเศรษฐศาสตร์

ขั้นตอนที่ 3 รวมค่าใช้จ่ายเป็นรายปี

การรวมค่าใช้จ่ายเป็นรายปี เป็นขั้นตอนสุดท้ายของการประมาณการค่าใช้จ่ายของโครงการ ทั้งนี้เพื่อให้ผู้วิเคราะห์โครงการได้มองเห็นภาพรวมของค่าใช้จ่ายทั้งหมดของโครงการ ตลอดอายุของโครงการ ซึ่งตามปกติโครงการทุกประเภทส่วนใหญ่มักจะมีการลงทุนมาก ในระยะแรกเนื่องจากมี ค่าที่ดิน ค่าก่อสร้าง ค่าเครื่องจักรและอุปกรณ์การผลิต อย่างไรก็ตาม ยังมีค่าใช้จ่ายเกี่ยวกับการดำเนินงานที่เกิดขึ้นในแต่ละปีเมื่อโครงการก่อสร้างเสร็จแล้วและเริ่มเปิดดำเนินการอีกด้วย เช่น ค่าวัตถุดิบ ค่าแรงงาน ค่าน้ำประปา ค่าไฟฟ้า ค่ากระกันภัย ค่าซ่อมแซมและบำรุงรักษา เงินเดือนผู้บริหาร ฯลฯ ซึ่งประมาณการค่าใช้จ่ายในการดำเนินงานนี้ควรทำการประมาณการเป็นรายปีในแต่ละรายการของค่าใช้จ่าย เช่น เงินเดือนผู้บริหารใช้วิธีประมาณการตามที่คาดว่าจะจ่ายจริง ขณะที่ค่าวัตถุดิบจะประมาณการตามความต้องการใช้วัตถุดิบเพื่อการผลิตในแต่ละปี เป็นต้น

การประเมินค่าโครงการลงทุน

1.การประเมินค่าโครงการลงทุนที่ไม่คำนึงถึงค่าของเงินกับเวลา

2. การประเมินค่าโครงการลงทุนที่คำนึงถึงค่าของเงินกับเวลา

การประเมินค่าโครงการลงทุนที่ไม่คำนึงถึงค่าของเงินกับเวลา

วิธีการประเมินค่าแบบนี้เป็นวิธีที่ง่าย โดยถือว่าเงินจำนวนที่เท่ากันในเวลาที่ต่างกันมีค่าเท่ากัน เช่น เงิน 100 บาท ในปีที่ 1 มีค่าเท่ากับ เงิน 100 บาท ในปีที่ 5 เป็นต้น ดังนั้น การคำนวณหากระแสเงินสดสุทธิจึงนำเงินในแต่ละปีมาบวกหรือลบกันได้เลย

วิธีการประเมินค่าโครงการลงทุนที่ไม่คำนึงถึงค่าของเงินสามารถจำแนกออกเป็น 2 วิธี คือ

1. วิธีอัตราผลตอบแทนถัวเฉลี่ย (Average rate of return) เป็นการคำนวณหาผลตอบแทนจากเงินที่ลงทุนไป โดยการนำกำไรสุทธิถัวเฉลี่ยหารเงินลงทุนเฉลี่ย

2. ระยะเวลาคืนทุน (Payback period) คือระยะเวลาที่กระแสเงินสดรับสุทธิเท่ากับเงินสดจ่ายลงทุนของโครงการ หรือระยะเวลาที่ผลตอบแทนจากการดำเนินโครงการเท่ากับเงินลงทุนของโครงการ วิธีนี้นิยมใช้มากในทางธุรกิจ

การประเมินค่าโครงการลงทุนที่คำนึงถึงค่าของเงินกับเวลา

การประเมินค่าโครงการลงทุนวิธีนี้ มีแนวความคิดว่าเงินในแต่ละปีถึงจะมีจำนวนเดียวกันก็จะมีมูลค่าไม่เท่ากัน นั่นก็คือ เงินมีค่าตามเวลา หรือเวลาเป็นปัจจัยที่มีค่าสำหรับค่าของเงิน (Time value of money) ซึ่งเป็นที่ยอมรับกันมานานแล้ว ถ้าต้องการที่จะได้รับเงินในอนาคตจำนวนเงินในอนาคตจะต้องมากขึ้นด้วยเท่ากับว่าเรานำเงินจำนวนนั้นไปลงทุนหาผลประโยชน์ ซึ่งอย่างน้อยควรจะได้รับผลตอบแทนจากอัตราดอกเบี้ยของหลักทรัพย์ที่ไม่มีความเสี่ยง (Risk free rate) ราคาหรือมูลค่าของเงินจะขึ้นอยู่กับอัตราดอกเบี้ย (Interest rate) เป็นตัวกำหนด

วิธีประเมินค่าโครงการลงทุนที่คำนึงถึงค่าของเงินกับเวลาสามารถจำแนกได้เป็น 3 วิธี คือ

1. วิธีมูลค่าปัจจุบันสุทธิ (Net present value หรือ NPV) หมายถึง ผลต่างของมูลค่าปัจจุบันของกระแสเงินสดรับสุทธิแต่ละปีตลอดอายุของโครงการกับเงินสดจ่ายลงทุน อัตราค่าของทุน (Cost of capital)

NPV = 0 แสดงว่าผลตอบแทนเท่ากับต้นทุน หรือจุดคุ้มทุน กล่าวคือโครงการไม่มีกำไร ไม่ขาดทุน

NPV > 0 แสดงว่าผลตอบแทนมากกว่าต้นทุนโครงการมีกำไร

NPV < 0 แสดงว่าผลตอบแทนน้อยกว่าต้นทุนโครงการนั้นขาดทุน

2. วิธีอัตราผลตอบแทนของโครงการ (Internal rate of return หรือ IRR) เป็นการคำนวณหาอัตราส่วนลด หรืออัตราดอกเบี้ยที่ทำให้มูลค่าปัจจุบันของกระแสเงินสดรับสุทธิตลอดอายุของโครงการเท่ากับเงินสดจ่ายลงทุน

หากค่าของ r ใดๆ มาแทนค่าในสูตรแล้วทำให้อัตราผลตอบแทนโครงการมากกว่าค่าของทุน (Cost of capital) แสดงว่าโครงการมีกำไรสมควรลงทุน

หากค่าของ r ใดๆ มาแทนแล้วทำให้อัตราผลตอบแทนของโครงการเท่ากับค่าของทุน แสดงว่าโครงการนี้ไม่มีกำไรไม่ขาดทุนคือ เสมอตัว

หากค่าของ r ใดๆ มาแทนแล้วทำให้อัตราผลตอบแทนของโครงการน้อยกว่าค่าของทุน แสดงว่าโครงการนี้ขาดทุนไม่น่าลงทุน

3. อัตราส่วนผลตอบแทนต่อต้นทุน (Benefit/Cost ratio) หมายถึง อัตราส่วนระหว่างมูลค่าปัจจุบันของผลตอบแทน กับมูลค่าปัจจุบันของต้นทุนที่จ่ายไปในการดำเนินโครงการ ในทางธุรกิจเรียกอัตราส่วนนี้ว่าดัชนีทำกำไร (Profitability index)

หากเท่ากับ 1 แสดงว่าผลตอบแทนเท่ากับต้นทุน แสดงว่าคุ้มทุน ธุรกิจดำเนินงานแล้วไม่มีกำไร ไม่ขาดทุน

หากมากกว่า 1 แสดงว่าผลตอบแทนมากกว่าต้นทุน ธุรกิจจะมีกำไร

หากน้อยกว่า 1 แสดงว่าผลตอบแทนน้อยกว่าต้นทุน ธุรกิจจะประสบการขาดทุน

4.6 การวิเคราะห์จุดคุ้มทุน (Break-even analysis)

การวิเคราะห์จุดคุ้มทุนเป็นเทคนิคที่ใช้ศึกษาความสัมพันธ์ระหว่างค่าใช้จ่ายคงที่ ค่าใช้จ่ายผันแปรได้และกำไร ถ้าค่าใช้จ่ายของธุรกิจเป็นค่าใช้จ่ายผันแปรได้ทั้งหมด ปัญหาเรื่องปริมาณคุ้มทุนคงไม่เกิดขึ้น แต่เนื่องจากธุรกิจเป็นค่าใช้จ่ายบางส่วนเป็นค่าใช้จ่ายผันแปรได้ และบางส่วนเป็นค่าใช้จ่ายคงที่ ธุรกิจจะพบกับการขาดทุนจนกว่ายอดขายจะสูงขึ้นถึงระดับหนึ่ง

การวิเคราะห์จุดคุ้มเป็นวิธีการหนึ่งของรูปแบบของการวางแผนกำไร โดยอาศัยหลักเกี่ยวกับความสัมพันธ์ระหว่างต้นทุนและรายได้ การวิเคราะห์จุดคุ้มทุนเป็นเครื่องมือสำหรับกำหนดจุดที่ยอดขายธุรกิจจะต้องคุ้มค่าใช้จ่ายทั้งหมด ได้แก่ ค่าใช้จ่ายผันแปรโดยตรงกับการผลิตและไม่เปลี่ยนแปลงไปตามระดับการผลิต ค่าใช้จ่ายแต่ละประเภทสามารถแสดงรายละเอียด ดังนี้

ค่าใช้จ่ายคงที่	ค่าใช้จ่ายผันแปร
-ค่าเสื่อมราคาเครื่องจักรและโรงงาน	-ค่าแรงงาน
-ค่าเช่าโรงงานและสำนักงาน	-ค่าวัตถุดิบ
-ดอกเบี้ยเงินกู้	-ค่านายหน้าพนักงานขาย
-เงินเดือนผู้บริหาร	
-เงินเดือนพนักงานวิจัย	
-เงินเดือนพนักงานบัญชี	
-ค่าใช้จ่ายสำนักงาน	

โดยทั่วไปค่าใช้จ่ายรวมทั้งสิ้นประกอบด้วยค่าใช้จ่ายผันแปรและค่าใช้จ่ายคงที่ ค่าใช้จ่ายผันแปร หมายถึง ค่าใช้จ่ายที่ผันแปรไปตามปริมาณการผลิตและการขาย ถ้าปริมาณการผลิตและการขายสูงขึ้น ค่าใช้จ่ายผันแปรรวมจะสูงขึ้นตามไปด้วย แต่ค่าใช้จ่ายผันแปรต่อหน่วยจะคงที่หรือเท่ากันทุกๆหน่วย ส่วนค่าใช้จ่ายคงที่ หมายถึงค่าใช้จ่ายที่ไม่เปลี่ยนแปลงไปตามระดับการดำเนินงานของธุรกิจ กล่าวคือไม่ว่าธุรกิจจะมีปริมาณการผลิตมากหรือน้อยก็ตาม ก็จะต้องเสีย

ค่าใช้จ่ายคงที่เท่าเดิมเสมอ โดยปกติค่าใช้จ่ายคงที่จะคงที่หรือไม่เปลี่ยนแปลงภายในช่วงระยะเวลาของการดำเนินงานหนึ่ง ถ้าพิจารณาต้นทุนคงที่ต่อหน่วย ณ ระดับการขายและผลิตต่างกัน ต้นทุนคงที่ต่อหน่วยจะต่างกัน ถ้ากิจการผลิตสินค้ามากขึ้น ต้นทุนคงที่ต่อหน่วยจะถูกเฉลี่ยไปยังหน่วยที่ผลิตเพิ่มขึ้น ดังนั้นต้นทุนคงที่จะถูกเฉลี่ยไปยังสินค้าที่ผลิตน้อยชิ้นลง ดังนั้น ต้นทุนคงที่ต่อหน่วยก็จะสูงขึ้น

กล่าวคือ จุดคุ้มทุนหมายถึง จุด ณ ระดับการดำเนินงานของธุรกิจที่ปริมาณการผลิตและขายมีผลทำให้ธุรกิจมีรายได้เท่ากับค่าใช้จ่ายรวม หรือหมายถึงจุด ณ ระดับการดำเนินงานของธุรกิจที่ไม่กำไรหรือขาดทุน

ประโยชน์ของการวิเคราะห์จุดคุ้มทุน

. 1. ช่วยในการตัดสินใจของผู้บริหาร ในกรณีที่ผู้บริหารต้องการการผลิตผลิตภัณฑ์ใหม่จำหน่าย การวิเคราะห์จุดคุ้มทุนจะบอกให้ทราบว่ากิจจะต้องขายสินค้ากี่หน่วยจึงเริ่มมีกำไร

2. การวิเคราะห์จุดคุ้มทุนจะช่วยในการกำหนดราคาสินค้า การวางแผนกำไรและการควบคุมค่าใช้จ่าย หรือต้นทุนของกิจการ

3. ช่วยในการบริหารสินทรัพย์ถาวรให้เป็นไปอย่างมีประสิทธิภาพ ซึ่งการวิเคราะห์จุดคุ้มทุนจะบอกให้ทราบว่าการใช้สินทรัพย์ถาวร เช่น เครื่องจักรและอุปกรณ์ใช้เต็มประสิทธิภาพหรือไม่ หากมีการใช้สินทรัพย์ถาวรไม่เต็มประสิทธิภาพจะมีผลทำให้ต้นทุนสูงขึ้น

ข้อจำกัดของการวิเคราะห์จุดคุ้มทุน

การวิเคราะห์จุดคุ้มทุนถึงแม้ว่าจะมีประโยชน์แล้ว แต่ก็มีข้อจำกัดบางอย่างที่ผู้ใช้จำเป็นต้องทราบ ดังนี้

1. ราคาขายต่อหน่วยของสินค้าจะคงที่เสมอ ไม่ว่าจะผลิตมากหรือน้อยก็ตาม ซึ่งในทางปฏิบัติราคาขายต่อหน่วยจะไม่คงที่ เพราะถ้าผู้ซื้อสินค้าจำนวนมาก ผู้ขายก็จะลดราคาสินค้าให้เพื่อจูงใจลูกค้า

2. ต้นทุนผันแปร ได้มีค่าคงที่ตลอดไม่ว่าจะผลิตมาหรือน้อย ซึ่งในทางปฏิบัติจะไม่เป็นจริงเพราะถ้าธุรกิจมียอดขายสูงขึ้นก็จะต้องผลิตสินค้ามากขึ้นเต็มกำลังการผลิต ต้องจ้างคนงานและจ่ายค่าช่วงเวลาเพิ่มขึ้น ทำให้ค่าใช้จ่ายผันแปรสูงขึ้น

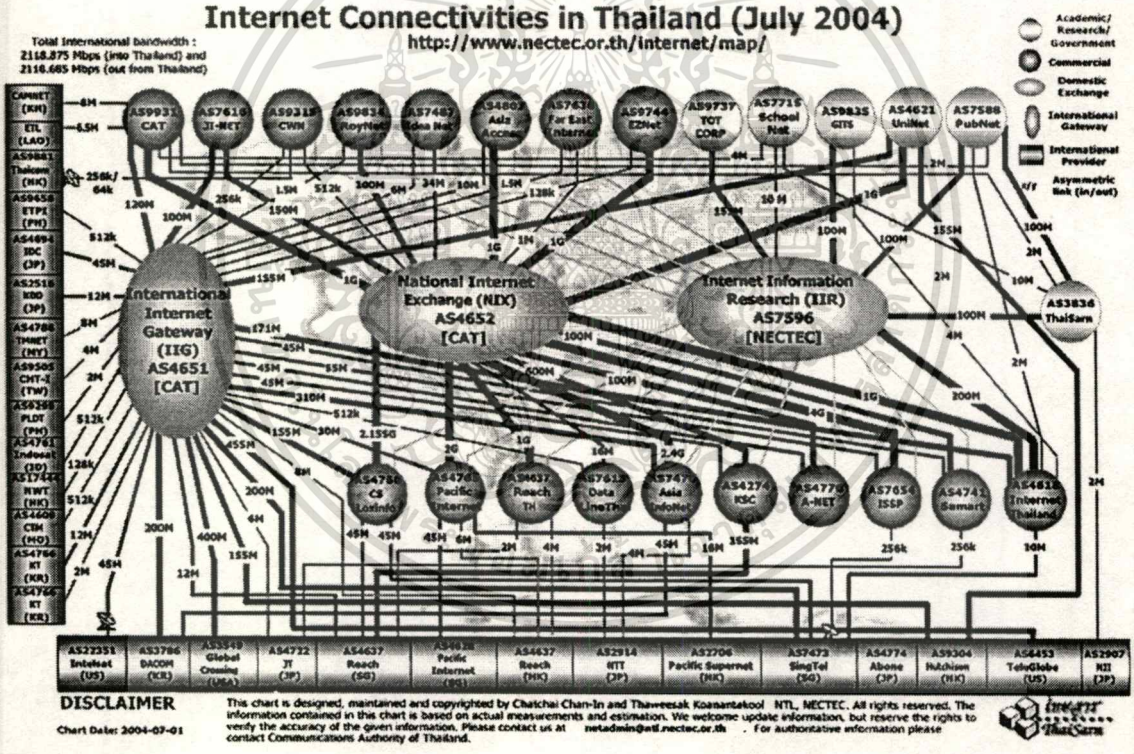
3. ต้นทุนคงที่ไม่เปลี่ยนแปลงไปตามปริมาณการขาย จะคงที่จนถึงปริมาณการขายระดับหนึ่งเท่านั้น เมื่อเกินระดับนี้แล้วก็จะเพิ่มขึ้น

บทที่ 5

โมเดลของผู้ให้บริการอินเตอร์เน็ต

5.1 ความหมายของผู้ให้บริการอินเตอร์เน็ต (การสื่อสารแห่งประเทศไทย. 2547.)

ผู้ให้บริการอินเตอร์เน็ต หมายถึง บริษัทหรือหน่วยงานที่ตั้งขึ้นมาเพื่อให้บริการติดต่อเชื่อมโยงกับเครือข่ายอินเตอร์เน็ตโดยอาจจะคิดค่าบริการหรือไม่ก็แล้วแต่บริษัทหรือหน่วยงานนั้นๆ ยกตัวอย่างเช่น ผู้ให้บริการอินเตอร์เน็ต(ISP) ในเมืองไทย loxinfo KSC Internet Thailand เป็นต้น



รูปที่ 5.1 แผนที่แสดงการเชื่อมต่ออินเตอร์เน็ตของประเทศไทย (ปี 2004)

NIX (National Internet Exchange) เป็นศูนย์กลางการติดต่อเครือข่ายภายในประเทศของ ISP ด้วย NIX ทำให้ ISP ในประเทศไทยสามารถติดต่อระหว่างกันได้โดยไม่ต้องอาศัยเครือข่ายของต่างประเทศ

IIG (International Internet Gateway) เป็นบริการของกสท.ในฐานะเป็น Carrier ที่ทำหน้าที่เชื่อมโยงกับเครือข่ายต่างประเทศโดยตรง เพื่อเป็นgateway สำหรับผู้ให้บริการอินเตอร์เน็ตออกสู่อินเตอร์เน็ตต่างประเทศ โดยไม่ต้องเชื่อมต่อวงจรอินเตอร์เน็ตกับต่างประเทศโดยตรง (IPLC) ซึ่งทำให้ผู้ให้บริการอินเตอร์เน็ตลดค่าใช้จ่ายในการเชื่อมต่ออินเตอร์เน็ตกับต่างประเทศอย่างมาก

IIR (Internet Information Research) ให้บริการอินเตอร์เน็ตเกี่ยวกับการศึกษาวิจัยผู้ให้บริการอินเตอร์เน็ต จากรูปที่ 5.1 แสดงถึงการเชื่อมต่อเครือข่ายอินเตอร์เน็ตของประเทศไทยซึ่งประกอบด้วย ผู้ให้บริการอินเตอร์เน็ตเชิงพาณิชย์ จำนวน 19 ราย ได้แก่ CAT JI-NET CWN RoyNet Idea Net Asia Access Far East Internet EZNet CS Loxinfo Pacific Internet Reach TH Data LineThai Asia InfoNet KSC A-NET ISSP Samart Internet Thailand และศูนย์บริการอินเตอร์เน็ตเพื่อการศึกษาและวิจัยจำนวน 6 ศูนย์ ได้แก่ SchoolNet UniNet Pubnet ThaiSarn TOT CORP และ GITS

การแลกเปลี่ยนข้อมูลภายในประเทศ ผู้ให้บริการอินเตอร์เน็ตทั้งหมดนี้จะเชื่อมต่อกันเพื่อแลกเปลี่ยนข้อมูลกันภายในประเทศโดยเชื่อมโยงผ่าน ศูนย์กลางอินเตอร์เน็ตเพื่อแลกเปลี่ยนข้อมูลภายในประเทศ (Domestic Internet Exchange) ซึ่งมี 2 แห่ง คือ National Internet Exchange (NIX) เพื่อให้บริการเชิงพาณิชย์ซึ่งดูแลโดย กสท. และ Internet Information Research (IIR) เพื่อการศึกษาวิจัย ได้แก่ การจัดทำเส้นทางการเชื่อมโยงข้อมูลและนักสถิติไหลเวียนของข้อมูลเสนอเป็นรายงานสาธารณะซึ่งดูแลโดยเนคเทค

การเชื่อมโยงกับต่างประเทศ มี 2 ทางเลือกคือเชื่อมต่อกับ International Internet Gateway (IIG) แล้วออกไปยังวงจรอินเตอร์เน็ตต่างประเทศอีกทีหนึ่ง หรือเชื่อมต่อวงจรอินเตอร์เน็ตต่างประเทศโดยตรง ซึ่งมีความสามารถในการดึงข้อมูลมายังประเทศไทยได้สูงสุด 2118.875 Mbps และมีความสามารถในการดึงข้อมูลออกจากประเทศไทยได้สูงสุด 2118.685 Mbps

ตารางที่ 5.1 แสดงขนาดแบนวิธในการเชื่อมโยงทั้งภายในและภายนอกประเทศของผู้ให้บริการอินเตอร์เน็ต ปี 2547 (การสื่อสารแห่งประเทศไทย. 2547.)

ISP	IIG (CAT)	NIX (CAT)	Internet Gateway
CAT	120M	1G	Camnet(KH) 8M ETL (LAO) 6.5M
JINET	100M	150M	
CSloxinfo	155M	2.155G	Reach (SG) 45M Singtel (SG) 45M
Asia Infonet	310M	2.4G	Dacom(KR) 45M NTT(JP) 4M
Internet Thailand	171M	1G	Singtel(SG)10M
KSC	45M	600M	Reach(SG) 155M
Asia Access	10M	1G	
Pacific	30M	2G	Pacific int.(SG) 45M Pacific supernet(HK) 16M
A Net	45M	100M	
ISSP	55M	100M	Singtel(SG) 256K
Samart	45M	100M	Singtel(SG) 256K
CWN	256K	512K	Thaicom(HK) 256K/64K
Roynet	1.5M	100M	
Ideanet	6M	34M	
Far East Int.	1.5M	1M	
EZ net	128K	1G	
Reach TH		1G	Reach(SG) 2M Reach(HK) 4M
Datalinethai	512K	16M	NTT(JP) 2M

5.2 โมเดลของผู้ให้บริการอินเตอร์เน็ต ผู้ให้บริการเชื่อมต่ออินเตอร์เน็ตแบ่งตามประเภทและขนาดของการให้บริการ สามารถแบ่งเป็น 3 ขนาด คือ

1. ผู้ให้บริการอินเตอร์เน็ตโมเดลที่ 1

คือ ผู้ให้บริการอินเตอร์เน็ตที่มีการให้บริการเน้นไปในการให้บริการอินเตอร์เน็ตแก่ผู้ใช้บริการรายย่อย (Individual Access) ได้แก่ บุคคลทั่วไป (Home Use) และ องค์กรขนาดเล็ก (Small Business Use) โดยวิธีเชื่อมต่อแบบ Dial up ให้บริการ แบ่งเป็น 2 รูปแบบ คือ Internet Card/Kit และ Member

Internet Card/Kit โดยให้บริการอินเตอร์เน็ตแก่ผู้ใช้ทั่วไป (Home Use) จะขาย card หรือชุด kit ที่มี Username และ Password ในการ login เข้าสู่อินเตอร์เน็ต ผู้ใช้สามารถเลือกซื้อชั่วโมงอินเตอร์เน็ตได้ตามความต้องการเหมาะสำหรับผู้เริ่มใช้อินเตอร์เน็ต หรือผู้ที่ใช้อินเตอร์เน็ตเป็นครั้งคราว

ชุดInternet Kit เป็นชุดอินเตอร์เน็ต สำเร็จรูปที่ ภายในชุดของ internet kit จะประกอบด้วยแผ่น CD Rom จำนวน 1 แผ่น ซึ่งได้บรรจุ Software ที่จำเป็นในการใช้งานทางอินเตอร์เน็ต อยู่มากมาย และมีคู่มือในการติดตั้งใช้งานอินเตอร์เน็ตเหมาะสำหรับผู้ใช้งานอินเตอร์เน็ตเป็นครั้งแรก

<u>การให้บริการ</u>

- บริการในการ access เข้าสู่อินเตอร์เน็ตเพียงอย่างเดียว
- ผู้ใช้บริการสามารถ check ชั่วโมงในการใช้งานอินเตอร์เน็ต และเปลี่ยน Username และ Password ได้

Member โดยให้บริการอินเตอร์เน็ตแก่องค์กรขนาดเล็ก (Small Business Use) ผู้ใช้บริการต้องสมัครเป็นสมาชิกรายเดือนของผู้ให้บริการอินเตอร์เน็ตก่อน และจ่ายค่าบริการเป็นรายเดือน สามารถเติมชั่วโมงอินเตอร์เน็ตได้ เหมาะสำหรับองค์กรที่ไม่ได้ใช้อินเตอร์เน็ตตลอดเวลา ไม่ต้องการติดตั้งเซิร์ฟเวอร์ ไม่มีผู้เชี่ยวชาญดูแลระบบ ไม่ต้องการเสียค่าใช้จ่ายมาก แต่ต้องการใช้อินเตอร์เน็ตเต็มรูปแบบ เหมือนองค์กรขนาดใหญ่

<u>การให้บริการ</u>

- บริการในการ access เข้าสู่อินเตอร์เน็ต
- สามารถ Login ใช้งานได้ทีละหลายคนแล้วแต่ package ที่ซื้อ
- บริการใช้ Mail Box ฟรี มีพื้นที่ให้รวม 15 MB โดยจำนวน User ขึ้นกับ Package ที่ซื้อ สามารถใช้ E-mail Account เป็น Username@ISPname.com หรือ Username@CompanyName.ISPname.com
- ไม่จำเป็นต้องมีระบบ Lan แต่สามารถขยายการเชื่อมต่อโดยใช้อุปกรณ์ IPSharing ได้

การให้บริการเพิ่มเติมพิเศษ (ต้องเสียค่าบริการพิเศษ)

- ให้บริการจด Domain Name เพื่อให้บริการเมื่อลูกค้าต้องการ E-mail Account ที่อยู่ภายใต้ Domain Name ที่ต้องการ และบริการ DNS Server เพื่อชี้ไปยัง Domain Name ที่ตั้งขึ้นมา
- ให้บริการรับฝาก Web Server (Web Hosting) โดยพื้นที่ให้บริการเริ่มต้นที่ 10 MB

2. ผู้ให้บริการอินเตอร์เน็ตโมเดลที่ 2

คือ ผู้ให้บริการอินเตอร์เน็ตที่มีการให้บริการอินเตอร์เน็ตแก่ผู้ใช้บริการรายย่อย (Individual Access) ได้แก่ บุคคลทั่วไป (Home Use) และองค์กรทุกขนาด (Business Use) ให้บริการโดยวิธีเชื่อมต่อแบบ Dial up, Always on (ADSL) และผู้ใช้บริการที่เป็นองค์กร (Corporate Access) ที่ต้องการความเป็นส่วนตัวในการจัดการ Sever และมีการให้บริการโดยวิธีเชื่อมต่อแบบ Lease Line, ISDN และ DSL

Individual Access แบ่งเป็น 2 รูปแบบ คือ Internet Card/Kit และ Member

Internet Card/Kit โดยให้บริการอินเตอร์เน็ตจะขาย card หรือชุด kit ที่มี Username และ Password ในการ login เข้าสู่อินเตอร์เน็ต ผู้ใช้สามารถเลือกซื้อชั่วโมงอินเตอร์เน็ตได้ตามความต้องการเหมาะสำหรับผู้เริ่มใช้อินเตอร์เน็ต หรือผู้ที่ใช้อินเตอร์เน็ตเป็นครั้งคราว

ชุดInternet Kit เป็นชุดอินเตอร์เน็ต สำเร็จรูปที่ ภายในชุดของ internet kit จะประกอบด้วย แผ่น CD Rom จำนวน 1 แผ่น ซึ่งได้บรรจุ Software ที่จำเป็นในการใช้งานทางอินเตอร์เน็ต อยู่มากมาย และมีคู่มือในการติดตั้งใช้งานอินเตอร์เน็ตเหมาะสำหรับผู้ใช้งานอินเตอร์เน็ตเป็นครั้งแรก

การให้บริการ

- บริการในการ access เข้าสู่อินเตอร์เน็ต
- มีบริการใช้ Mail Box ฟรี มีพื้นที่ให้รวม 10 MB โดยจำนวน User ขึ้นกับ Package ที่ซื้อ สามารถใช้ E-mail Account เป็น Username@ISPname.com
- ผู้ใช้บริการสามารถ check ชั่วโมงในการใช้งานอินเตอร์เน็ต และเปลี่ยน Username และ Password ได้

Member โดยให้บริการอินเตอร์เน็ตแก่องค์กรทุกขนาด (Business Use) ผู้ใช้บริการต้องสมัครเป็นสมาชิกรายเดือนของผู้ให้บริการอินเตอร์เน็ตก่อน และจ่ายค่าบริการเป็นรายเดือน สามารถเติมชั่วโมงอินเตอร์เน็ตได้ เหมาะสำหรับองค์กรที่ไม่ได้ใช้อินเตอร์เน็ตตลอดเวลา ไม่ต้องการติดตั้งเซิร์ฟเวอร์ ไม่มีผู้เชี่ยวชาญดูแลระบบ ไม่ต้องการเสียค่าใช้จ่ายมาก แต่ต้องการใช้อินเตอร์เน็ตเต็มรูปแบบ เหมือนองค์กรขนาดใหญ่

การให้บริการ

- บริการในการ access เข้าสู่อินเตอร์เน็ต
- สามารถ Login ใช้งานได้ทีละหลายคนแล้วแต่ package ที่ซื้อ
- บริการใช้ Mail Box ฟรี มีพื้นที่ให้รวม 15 MB โดยจำนวน User ขึ้นกับ Package ที่ซื้อ สามารถใช้ E-mail Account เป็น Username@ISPname.com หรือ Username@CompanyName.ISPname.com
- ไม่จำเป็นต้องมีระบบ Lan แต่สามารถขยายการเชื่อมต่อโดยใช้อุปกรณ์ IPSharing ได้

Member (DSL) ให้บริการเชื่อมต่ออินเตอร์เน็ตความเร็วสูง ผู้ใช้บริการต้องสมัครเป็นสมาชิกรายเดือนของผู้ให้บริการอินเตอร์เน็ตก่อน และจ่ายค่าบริการ ค่าเช่าอุปกรณ์ เป็นรายเดือน เหมาะสำหรับบุคคลทั่วไป องค์กรทุกขนาดที่ต้องการเชื่อมต่ออินเตอร์เน็ตตลอดเวลา ไม่ต้องการติดตั้งเซิร์ฟเวอร์ ไม่มีผู้เชี่ยวชาญดูแลระบบ ไม่ต้องการเสียค่าใช้จ่ายมาก แต่ต้องการใช้อินเตอร์เน็ตความเร็วสูงเต็มรูปแบบ เหมือนองค์กรขนาดใหญ่

การให้บริการ

- บริการในการ access เข้าสู่อินเตอร์เน็ต โดยการใช้งานอินเตอร์เน็ตไม่จำกัดเวลาในการเชื่อมต่อ (Unlimited)
- บริการใช้ Mail Box ฟรี มีพื้นที่ให้รวม 15 MB โดยจำนวน User ขึ้นกับ Package ที่ซื้อ สามารถใช้ E-mail Account เป็น Username@ISPname.com หรือ Username@CompanyName.ISPname.com
- ผู้ใช้บริการต้องเสียค่าติดตั้งอุปกรณ์ในครั้งแรก ค่าเช่าคู่สายและอุปกรณ์ Modem DSL

Corporate Access เหมาะสำหรับลูกค้าที่เป็นองค์กรทุกขนาด ที่มีความต้องการมี E-mail ภายใต้ Domain Name ของบริษัท และสามารถจัดการบริหาร Server ได้เอง ต้องการใช้อินเตอร์เน็ตเชื่อมต่อตลอดเวลา และมี Public IP Address เพื่อใช้งานในองค์กร การเชื่อมต่อเป็นได้ทั้ง ISDN DSL หรือ Lease Line ซึ่งเสียค่าบริการเป็นรายเดือน สามารถใช้งานอินเตอร์เน็ตได้ไม่จำกัด (Unlimited)

การให้บริการ

- บริการในการ access เข้าสู่อินเตอร์เน็ต โดยการใช้งานอินเตอร์เน็ตไม่จำกัดเวลาในการเชื่อมต่อ (Unlimited)
- ผู้ใช้บริการต้องเสียค่าเช่าคู่สายและอุปกรณ์ Router หรือ Modem DSL ที่ใช้ในการเชื่อมต่อ

- ลูกค้าสามารถมี Mail Server ส่วนตัว โดยสามารถรับและส่งเมล์ได้จาก Mail Server ที่มีอยู่โดยมี Mail Server ของผู้ให้บริการอินเตอร์เน็ตเป็น Backup เมื่อ Mail Server ส่วนตัวมีปัญหา
- ลูกค้าสามารถสร้าง Server ที่ต้องการได้เองโดยมี Public IP Address ให้ตามที่ร้องขอ

<u>การให้บริการเพิ่มเติมพิเศษ</u> (ต้องเสียค่าบริการพิเศษ)

- ให้บริการจด Domain Name เพื่อให้บริการเมื่อลูกค้าต้องการ E-mail Account ที่อยู่ภายใต้ Domain Name ที่ต้องการ และบริการ DNS Server เพื่อชี้ไปยัง Domain Name ที่ตั้งขึ้นมา
- ให้บริการรับฝาก Web Server (Web Hosting) โดยพื้นที่ให้บริการเริ่มต้นที่ 10 MB
- ให้บริการรับฝาก Server ของลูกค้า (Co-Location) และ ดูแล Server ให้ เรียกว่า Internet Data Center (IDC)
- การให้บริการเชื่อมต่อ Virtual Private Network (VPN)

3. ผู้ให้บริการอินเตอร์เน็ตโมเดลที่ 3

คือ ผู้ให้บริการอินเตอร์เน็ตที่มีการให้บริการอินเตอร์เน็ตแก่ผู้ใช้บริการรายย่อย (Individual Access) ได้แก่ บุคคลทั่วไป (Home Use) และองค์กรทุกขนาด (Business Use) ให้บริการ โดยวิธีเชื่อมต่อแบบ Dial up, Always on (ADSL) และผู้ใช้บริการที่เป็นองค์กร (Corporate Access) ที่ต้องการความเป็นส่วนตัวในการจัดการ Sever และมีการให้บริการโดยวิธีเชื่อมต่อแบบ Lease Line, ISDN และ DSL

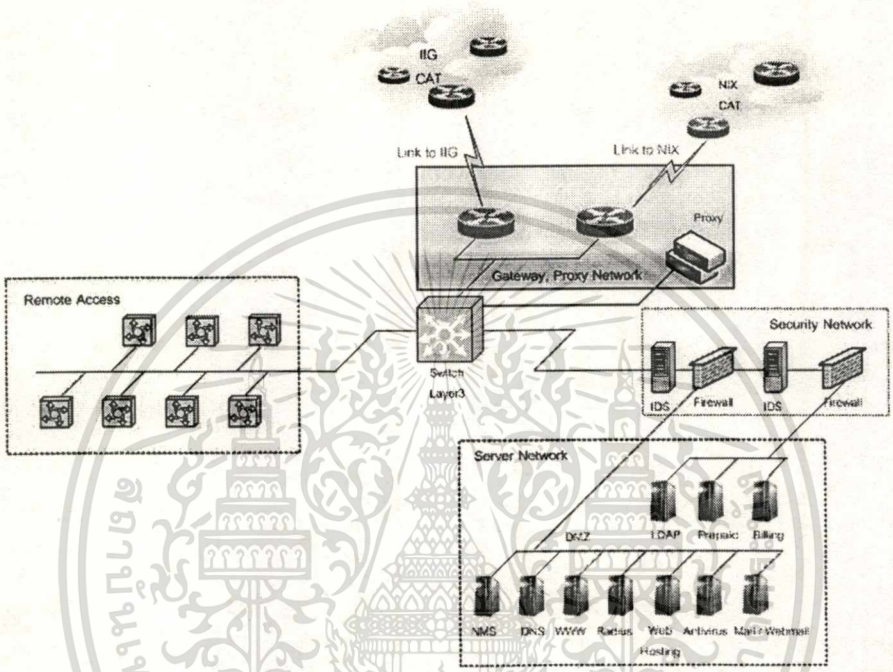
การให้บริการคล้ายกับผู้ให้บริการอินเตอร์เน็ตประเภทที่ 2 แต่มีการเพิ่มระดับการรักษาความปลอดภัย ระบบ Backup Link และ Backup อุปกรณ์ เพื่อสามารถให้บริการได้ต่อเนื่องไม่หยุดชะงักเมื่ออุปกรณ์หรือ Link มีปัญหา

5.3 การวางระบบเครือข่ายของผู้ให้บริการอินเตอร์เน็ต

รูปแบบในการเชื่อมต่อระบบเครือข่ายของผู้ให้บริการอินเตอร์เน็ต ต้องคำนึงถึงการรักษาความปลอดภัยทางสารสนเทศ การเชื่อมต่อระบบเครือข่ายของผู้ให้บริการอินเตอร์เน็ตคล้ายกับการเชื่อมต่อเพื่อความปลอดภัยขององค์กรทั่วไป แต่ต้องมีระดับการรักษาความปลอดภัยที่เหมาะสมไม่มากและไม่น้อยจนเกินไป เนื่องจากต้องให้บริการแก่ลูกค้าหลากหลายชนิด ต้องเชื่อมต่อเพื่อเป็น Gateway ออกสู่ระบบอินเตอร์เน็ต ของหลายๆองค์กรและอาจมีการเชื่อมต่อกับ Backbone Internet ที่ให้บริการ ISP ทั่วโลก การวางระบบเครือข่ายของผู้ให้บริการอินเตอร์เน็ต แบ่งตามขนาด

และลักษณะการให้บริการได้เป็น 3 ประเภท คือผู้ให้บริการอินเตอร์เน็ตโมเดลที่ 1, ผู้ให้บริการอินเตอร์เน็ตโมเดลที่ 2 และผู้ให้บริการอินเตอร์เน็ตโมเดลที่ 3 ดังนี้

1. การวางระบบเครือข่ายผู้ให้บริการอินเตอร์เน็ตโมเดลที่ 1 มีการวางระบบเครือข่ายดังรูปที่ 5.2



รูปที่ 5.2 แสดงระบบการเชื่อมต่อของผู้ให้บริการอินเตอร์เน็ตโมเดลที่ 1

การวางระบบเครือข่ายของผู้ให้บริการอินเตอร์เน็ตโมเดลที่ 1ประกอบด้วยอุปกรณ์ต่างๆ ดังนี้

Backbone Network แบ่งเป็น 4 กลุ่มหลัก คือ

1. Gateway, Proxy Network
2. Access Server Network
3. Server Network
4. Security Network

แต่ละ Network เชื่อมต่อกันผ่าน Catalyst 6500 (L3 Switch)

Internet Gateway

1. International Link

   - IIG 1.5 Mbps Leased Line

2. Domestic Link

- NIX 100 Mbps Leased Line

การให้บริการ

1. Dial up Telephone Lines = 2880 Lines

Digital Lines

- xxx-xxx 96 E1 (2880 Lines)

หมายเหตุ ใช้พร้อมกันได้ 1563 Lines / Domestic Link และ 23 Lines / International Link หาก การใช้มากกว่านี้จะ Share Bandwidth กัน

2. Web Hosting สามารถเพิ่มปริมาณตามจำนวนลูกค้า

Gateway / Proxy Network

มี IP ในช่วง xxx.xxx.xxx.xxx /xx ประกอบด้วยอุปกรณ์ทั้งหมด 8 units คือ

1. Border Router (Link to IIG)
   - Specification
     - Cisco 7206
     - NPE-G1 includes 3GigE/FE/E Ports and IP SW1 Gigabit Ethernet Port
2. Border Router (Link to NIX)
   - Specification
     - Cisco 7206
     - NPE-G1 includes 3GigE/FE/E Ports and IP SW1 Gigabit Ethernet Port
3. Switch Layer 3
   - Specification
     - Cisco Catalyst 6500
     - 24-port GigE Mod: fabric-enabled
4. Switch Layer 2 @ 3 units
   - Specification
     - Cisco Catalyst 5000
     - 1 Fast-Ethernet Port
5. Proxy (Caching Server) @ 2 units
   - Specification
     - Netapp C1200

Access Server Network

ประกอบด้วยอุปกรณ์ทั้งหมด 6 units คือ

RAS Router (Digital Line) @ 6 units = 2880 Line

- Specification
  - Cisco 5350
  - 16 Channelized E1/PRI port
  - 1 Ethernet Port
  - 1 Fast-Ethernet Port

Server Network

ประกอบด้วยอุปกรณ์ทั้งหมด 9 units คือ

1. WWW Server

   Hardware : Compaq DL380R03

   OS : Fedora Core1 / Snort

   Service : ISP Homepage

2. DNS Server

   Hardware : Compaq DL380R03

   OS : Fedora Core1 / Snort

   Service : DNS Server

3. Network Management Server

   Hardware : Compaq DL380R03

   OS : Fedora Core1 / Snort

   Service : Network Management via web interface

4. Mail Server / Web mail

   Hardware : Compaq DL380R03

   OS : Fedora Core1 / Snort

   Service : Mail Relay SMTP Service

   : POP3 / SMTP / IMAP4

   : Mail-Monitor, Admin Tools

5. Authentication Authorization and Accounting (AAA) Radius Server

   Hardware : Compaq DL380R03

OS : Fedora Core1

Service : Radius for Authentication

6. Antivirus Server

Hardware : Compaq DL380R03

OS : Fedora Core1

Service : Trend Micro Antivirus for Mail Server

7. Billing & CRM

Hardware : Compaq DL380R03

OS : Fedora Core1 / Snort

Service : Oracle

: CRM

: Statement

8. Prepaid

Hardware : Compaq DL380R03

OS : Fedora Core1 / Snort

Service : Prepaid Database

: Oracle

9. LDAP Server

Hardware : Compaq DL380R03

OS : Fedora Core1 / Snort

Service : Directory Access Database

: LDAP

Security Network

ประกอบด้วยอุปกรณ์ทั้งหมด 4 units คือ

1. IDS Server @ 2 units

Hardware : Compaq DL380R03

OS : Fedora Core1 / Snort

Service : IDS Server for Server farm / Billing, Prepaid &LDAP Server

2. Firewall (for Billing Server)

Hardware : Compaq DL380R03

OS : Linux Slackware 7.1

Service : Firewall for Billing, Prepaid &LDAP

3. Firewall (for Server)

Hardware : Netscreen 208

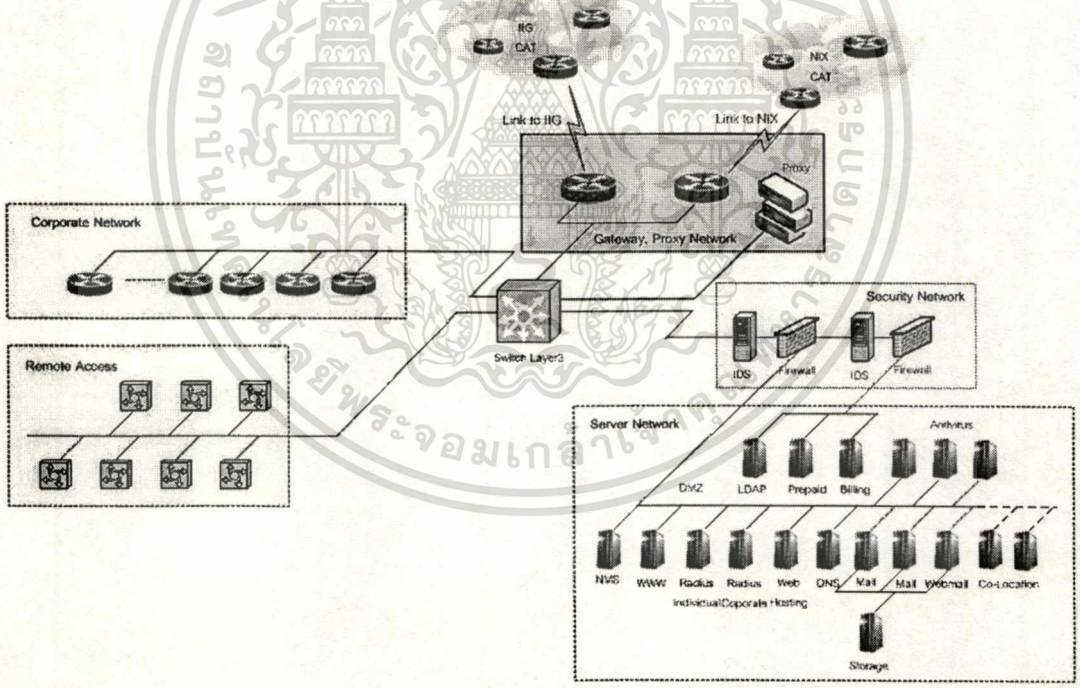
: Performance 550 MBps

: Concurrent Connection 128,000

: 8 port 10/100 Base-T

Service : Firewall for Server

2. การวางระบบเครือข่ายผู้ให้บริการอินเตอร์เน็ตโมเดลที่ 2 มีการวางระบบเครือข่ายดังรูปที่ 5.3



รูปที่ 5.3 แสดงระบบการเชื่อมต่อของผู้ให้บริการอินเตอร์เน็ตโมเดลที่ 2

การวางระบบเครือข่ายของผู้ให้บริการอินเตอร์เน็ตโมเดลที่ 2 ประกอบด้วยอุปกรณ์ต่างๆ ดังนี้

Backbone Network แบ่งเป็น 5 กลุ่มหลัก คือ

1. Gateway, Proxy Network
2. Access Server Network
3. Corporate Network
4. Server Network
5. Security Network

แต่ละ Network เชื่อมต่อกันผ่าน Catalyst 6500 (L3 Switch)

Internet Gateway

1. International Link

- IIG 45 Mbps Leased Line

2. Domestic Link

- NIX 1 Gbps Leased Line

การให้บริการ

1. Dial up Telephone Lines /ISDN = 3840 Lines

จำกัดการใช้งาน 20 % = 200 Mbps for Domestic Link

Digital Lines

- xxx-xxx 64 E1 (1920 lines)
- xxx-xxx 64 E1 (1920 lines) type ISDN

<u>หมายเหตุ</u> ใช้งานที่ Line ละ 64 Kbps พร้อมกันได้ 3125 Lines / Domestic Link หากการใช้มากกว่านี้จะทำให้ลด Speed ลงเพราะมีการ Share Bandwidth กัน

2. DSL

จำกัดการใช้งาน 15 % = 150 Mbps for Domestic Link

-1 STM1 155 Mbps รองรับได้ 2000 users (มี License)

<u>หมายเหตุ</u> ใช้งานพร้อมกันได้ไม่เกิน 2000 users สามารถกำหนด Bandwidth แต่ละ user ได้ โดยการ Authorization ที่ BRAS (Board Band Remote Access Server)

3. Lease Line

จำกัดการใช้งาน 50 % = 500 Mbps for Domestic Link

- Serial 112 ports 224 Mbps

- E1 Channel 64 E1 (128 Mbps)
- ATM port 155 Mbps

4. Co-Location/Web Hosting

จำกัดการใช้งาน 15 % = 150 Mbps for Domestic Link

***** สำหรับ International Link 45 Mbps เนื่องจากมี Bandwidth น้อยจึง Share ใช้งานร่วมกัน**

Gateway, Proxy Network

มี IP ในช่วง xxx.xxx.xxx.xxx/xx ประกอบด้วยอุปกรณ์ทั้งหมด 11 units คือ

1. Border Router (Link to IIG)

- Specification
  - Cisco 7206
  - NPE-G1 includes 3GigE/FE/E Ports and IP SW1 Gigabit Ethernet Port

2. Border Router (Link to NIX)

- Specification
  - Cisco 7200
  - NPE-G1 includes 3GigE/FE/E Ports and IP SW1 Gigabit Ethernet Port

3. Switch Layer 3

- Specification
  - Cisco Catalyst 6500
  - 24-port GigE Mod: fabric-enabled

4. Switch Layer 2 @ 5 units

- Specification
  - Cisco Catalyst 5000
  - 1 Fast-Ethernet Port

5. Proxy (Caching Server) @ 3 units

- Specification
  - Netapp C1200

Access Server Network

ประกอบด้วยอุปกรณ์ทั้งหมด 8 units คือ

1. RAS Router (Digital Line) @ 4 units = 1920 Line

- Specification

- Cisco 5350
- 16 Channelized E1/PRI port
- 1 Ethernet Port
- 1 Fast-Ethernet Port

2. RAS Router (Digital Line) @ 4 units = 1920 Line (for ISDN)

- Specification
  - Cisco 5350
  - 16 Channelized E1/PRI port
  - 1 Ethernet Port
  - 1 Fast-Ethernet Port

3. BRAS (Broadband Remote Access Server)

- Specification
  - Nortel Shasta 500BSN
  - STM1
  - 2000 Users (License)

Corporate Network

ประกอบด้วยอุปกรณ์ทั้งหมด 5 units

1. Router Cisco 7513 @ 4 units

- Specification
  - Cisco 7513
  - 28 Fast Serial Port
  - 4 Ethernet Port
  - 2 Fast Ethernet Port
  - 16 E1 Port

2. Router Cisco MGX8850

- Specification
  - Cisco MGX8850
  - 2 Fast Ethernet Port
  - Double-height ATM VS/VD*SM

Server Network / Firewall

ประกอบด้วยอุปกรณ์ทั้งหมด 15 units คือ

1. WWW Server

Hardware : Sun Sparc 20

OS : Solaris 9

Service : ISP Homepage

: Secondary DNS

2. DNS Server

Hardware : Sun E250

OS : Solaris 9

Service : Primary DNS

3. Network Management Server

Hardware : Sun Ultra 5

OS : Solaris 9

Service : Network Management via web interface

4. Mail Server @ 2 units

Hardware : Sun E220

OS : Solaris 9

Service : Mail Relay SMTP Service

: POP3 / SMTP / IMAP4

: Mail-Monitor, Admin Tools

5. Web Mail Server

Hardware : Sun E220

OS : Solaris 9

Service : Mail Relay SMTP Service

: POP3 / SMTP / IMAP4

: Mail-Monitor, Admin Tools

6. Authentication Authorization and Accounting (AAA) Radius Server @ 2 units

Hardware : Sun E220

OS : Solaris 9

Service : Radius for Authentication

7. Antivirus Server @ 3 units

Hardware : Compaq DL380R03

OS : Fedora Core1

Service : Trend Micro Antivirus for Mail Server

8. Storage Server

Hardware : NetApp

OS : Fedora Core1

Service : Storage Mail

9. Billing & CRM

Hardware : Sun E250

OS : Solaris 9

Service : Oracle

: CRM

: Statement

10. Prepaid

Hardware : Sun E250

OS : Solaris 9

Service : Prepaid Database

: Oracle

11. LDAP Server

Hardware : Sun E250

OS : Solaris 9

Service : Directory Access Database

: LDAP

Security Network

ประกอบด้วยอุปกรณ์จำนวน 4 units

1. IDS Server @ 2 units

Hardware : Compaq DL380R03

OS : Fedora Core1 / Snort

Service : IDS Server for Server farm / Billing, Prepaid &LDAP Server

2. Firewall @ 2 units

Hardware : Netscreen 208

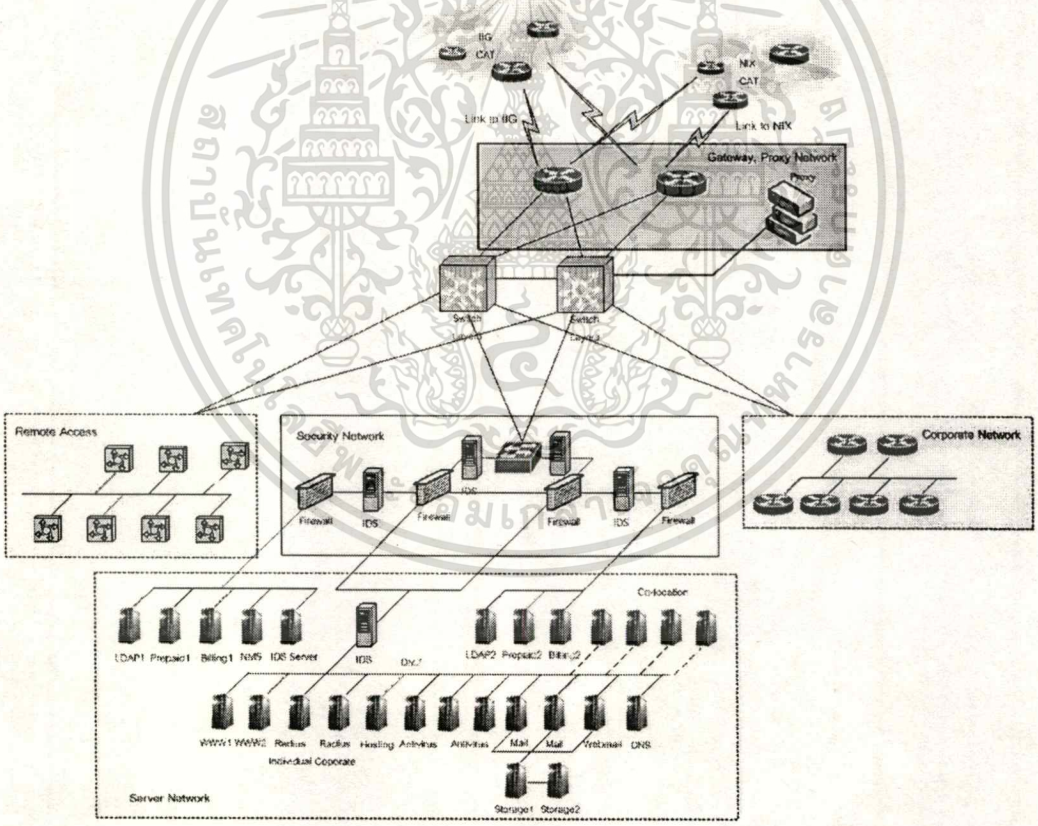
: Performance 550 Mbps

: Concurrent Connection 128,000

: 8 port 10/100 Base-T

Service : Firewall for Server farm / Billing, Prepaid &LDAP Server

3. การวางระบบเครือข่ายผู้ให้บริการอินเตอร์เน็ตโมเดลที่ 3 มีการวางระบบเครือข่ายดังรูปที่ 5.4



รูปที่ 5.4 แสดงระบบการเชื่อมต่อของผู้ให้บริการอินเตอร์เน็ตโมเดลที่ 3

การวางระบบเครือข่ายของผู้ให้บริการอินเตอร์เน็ตโมเดลที่ 3ประกอบด้วยอุปกรณ์ต่างๆ ดังนี้

Backbone Network แบ่งเป็น 5 กลุ่มหลัก คือ

1. Gateway, Proxy Network
2. Access Server Network
3. Corporate Network
4. Server Network
5. Security Network

แต่ละ Network เชื่อมต่อกันผ่าน Catalyst 6500 (L3 Switch)

Internet Gateway

1. International Link
   - IIG 155 Mbps Leased Line
2. Domestic Link
   - NIX 2 Gbps Leased Line

การให้บริการ

1. Dial up Telephone Lines /ISDN = 7680 Lines

จำกัดการใช้งาน 20 % = 400 Mbps for Domestic Link

Digital Lines

- xxx-xxx 128 E1 (3840 lines)
- xxx-xxx 128 E1 (3840 lines) type ISDN

<u>หมายเหตุ</u> ใช้งานที่ Line ละ 64 Kbps พร้อมกันได้ 6250 Lines / Domestic Link หากการใช้มากกว่านี้จะทำให้ลด Speed ลงเพราะมีการ Share Bandwidth กัน

2. DSL

จำกัดการใช้งาน 15 % = 300 Mbps for Domestic Link

-2 STM1 310 Mbps รองรับได้ 4000 users (มี License)

<u>หมายเหตุ</u> ใช้งานพร้อมกันได้ไม่เกิน 4000 users สามารถกำหนด Bandwidth แต่ละ user ได้ โดยการ Authorization ที่ BRAS (Board Band Remote Access Server)

3. Lease Line

จำกัดการใช้งาน 50 % = 1 Gbps for Domestic Link

- Serial 224 ports 448 Mbps

- E1 Channel 128 E1 (256 Mbps)
- 2 ATM port 310 Mbps

4. Co-Location/Web Hosting

จำกัดการใช้งาน 15 % = 300 Mbps for Domestic Link

***** สำหรับ International Link 155 Mbps Share ใช้งานร่วมกัน**

Gateway, Proxy Network

มี IP ในช่วง xxx.xxx.xxx.xxx/xx ประกอบด้วยอุปกรณ์ทั้งหมด 13 units คือ

1. Border Router (Link to IIG)
   - Specification
     - Cisco 7206
     - NPE-G1 includes 3GigE/FE/E Ports and IP SW1 Gigabit Ethernet Port
2. Border Router (Link to NIX)
   - Specification
     - Cisco 7206
     - NPE-G1 includes 3GigE/FE/E Ports and IP SW1 Gigabit Ethernet Port
3. Switch Layer 3 @ 2 units
   - Specification
     - Cisco Catalyst 6500
     - 24-port GigE Mod: fabric-enabled
4. Switch Layer 2 @ 6 units
   - Specification
     - Cisco Catalyst 5000
     - 1 Fast-Ethernet Port
5. Proxy (Caching Server) @ 3 units
   - Specification
     - Netapp C1200

Access Server Network

ประกอบด้วยอุปกรณ์ทั้งหมด 17 units คือ

1. RAS Router (Digital Line) @ 8 units = 3840 Line
   - Specification

- Cisco 5350
- 16 Channelized E1/PRI port
- 1 Ethernet Port
- 1 Fast-Ethernet Port

2. RAS Router (Digital Line) @ 8 units = 3840 Line (for ISDN)

- Specification
  - Cisco 5350
  - 16 Channelized E1/PRI port
  - 1 Ethernet Port
  - 1 Fast-Ethernet Port

3. BRAS (Broadband Remote Access Server)

- Specification
  - Nortel Shasta 500BSN
  - 2 STM1
  - 4000 Users (License)

Corporate Network

ประกอบด้วยอุปกรณ์ทั้งหมด 9 units คือ

1. Router Cisco 7513 @ 8 units

- Specification
  - Cisco 7513
  - 28 Fast Serial Port
  - 4 Ethernet Port
  - 2 Fast Ethernet Port
  - 8 E1 Port @ 2 units

2. Router Cisco MGX8850

- Specification
  - Cisco MGX8850
  - 2 Fast Ethernet Port
  - Double-height ATM VS/VD SM, 16 T3s or E3s

Server Network

ประกอบด้วยอุปกรณ์ทั้งหมด 20 units คือ

1. WWW Server @ 2 units

Hardware : Sun Sparc 20

OS : Solaris 9

Service : ISP Homepage

: Secondary DNS

2. DNS Server

Hardware : Sun E250

OS : Solaris 9

Service : Primary DNS

3. Network Management Server

Hardware : Sun Ultra 5

OS : Solaris 9

Service : Network Management via web interface

4. Mail Server @ 2 units

Hardware : Sun E220

OS : Solaris 9

Service : Mail Relay SMTP Service

: POP3 / SMTP / IMAP4

: Mail-Monitor, Admin Tools

5. Web Mail Server

Hardware : Sun E220

OS : Solaris 9

Service : Mail Relay SMTP Service

: POP3 / SMTP / IMAP4

: Mail-Monitor, Admin Tools

6. Authentication Authorization and Accounting (AAA) Radius Server @ 2 units

Hardware : Sun E220

OS : Solaris 9

Service : Radius for Authentication Individual / Corporate

7. Antivirus Server @ 3 units

Hardware : Compaq DL380R03

OS : Fedora Core1

Service : Trend Micro Antivirus for Mail Server

8. Storage Server @ 2 units

Hardware : NetApp

OS : Fedora Core1

Service : Storage Mail

9. Billing & CRM @ 2 units

Hardware : Sun E250

OS : Solaris 9

Service : Oracle

: CRM

: Statement

10. Prepaid @ 2 units

Hardware : Sun E250

OS : Solaris 9

Service : Prepaid Database

: Oracle

11. LDAP Server @ 2 units

Hardware : Sun E250

OS : Solaris 9

Service : Directory Access Database

: LDAP

Security Network

ประกอบด้วยอุปกรณ์ทั้งหมด 9 units คือ

1. IDS Server @ 5 units

Hardware : Compaq DL380R03

OS : Fedora Core1 / Snort

Service : IDS Server for Server farm / Billing, Prepaid &LDAP Server

2. Firewall @ 4 units

Hardware : Netscreen 500

: Performance 700 Mbps

: Concurrent Connection 250,000

: 8 port 10/100 Base-T

Service : Firewall for Server farm / Billing, Prepaid &LDAP Server

5.4 การเลือกใช้อุปกรณ์รักษาความปลอดภัย

5.4.1 Firewall

ใช้ในการรักษาความปลอดภัยของอุปกรณ์เครือข่าย สิ่งที่ผู้ให้บริการอินเตอร์เน็ตจะต้องคำนึงถึงในการเลือกใช้ Firewall มีดังนี้

- ประสิทธิภาพในเรื่องความเร็วในการส่งผ่านแพ็กเกต (Firewall Performance)
- จำนวนการสร้าง Connection (Concurrent Session)
- ความเร็วในการสร้าง Connection (New Session/Second)
- จำนวน Policy ที่สามารถ set ได้
- ชนิดและจำนวน interface
- รองรับการเชื่อมต่อแบบ VPN
- สะดวกในการ Monitoring และ Management

ผู้ให้บริการอินเตอร์เน็ตสามารถเลือกใช้ Firewall ได้ตามความเหมาะสมของขนาดการให้บริการและงบประมาณการลงทุน ชนิดของ Firewall ที่เลือกใช้ มีทั้งชนิดแพ็กเกตฟิลเตอร์ริ่งไฟร์วอลล์ (Packer Filtering Firewall), สเตทฟูลไฟร์วอลล์ (Stateful Firewall) ซึ่งแพ็ตเก็ตฟิลเตอร์ริ่งไฟร์วอลล์จะดูเฉพาะส่วนที่เป็นแฮดเดอร์เท่านั้น และไม่สามารถฟิลเตอร์แพ็กเกตที่ถูกแฟรกเมนต์ได้ เป็นคุณสมบัติที่มีอยู่แล้วบนเราท์เตอร์ควรตั้งค่าเพื่อลดภาระการทำงานของไฟร์วอลล์ได้ แต่ไม่ควรมีกฎที่เยอะเกินไปเพราะจะทำให้ประสิทธิภาพการทำงานของเราท์เตอร์ต่ำลง

นอกจากแพ็กเกตฟิลเตอร์ริ่งไฟร์วอลล์ ผู้ให้บริการอินเตอร์เน็ตทุกโมเดลควรใช้สเตทฟูลไฟร์วอลล์ซึ่งเป็นฮาร์ดแวร์ที่มีหน้าที่เป็นไฟร์วอลล์โดยเฉพาะ มีประสิทธิภาพในการรักษาความปลอดภัยมากกว่า เพื่อรักษาความปลอดภัยให้แก่เซอร์ฟเวอร์ที่ให้บริการลูกค้าและเซอร์เวอร์ของลูกค้าที่มาฝากไว้

5.4.2 ระบบตรวจจับการบุกรุก (Intrusion Detection System)

ระบบตรวจจับการบุกรุก หรือ IDS (Intrusion Detection System) เป็นเครื่องมือสำหรับการรักษาความปลอดภัยอีกประเภทหนึ่งที่ใช้สำหรับตรวจจับความพยายามที่จะบุกรุกเครือข่าย โดยระบบจะแจ้งเตือนผู้ดูแลระบบเมื่อการบุกรุกหรือพยายามที่จะบุกรุกเครือข่าย IDS นั้นไม่ใช่ระบบที่ใช้ป้องกันการบุกรุกแต่เป็นระบบที่คอยแจ้งเตือนภัยเท่านั้น

IDS ที่ผู้ให้บริการอินเตอร์เน็ตใช้นั้นแบ่งออกเป็น 2 ประเภทคือ Host-Bases IDS และ Network-Based IDS โดยโฮสต์เบสไอดีเอส นั้นคือ ระบบที่ติดตั้งที่เครื่องเว็บเซิร์ฟเวอร์เพื่อตรวจจับความพยายามที่จะแฮ็กเว็บเซิร์ฟเวอร์เอง ส่วนเน็ตเวิร์คไอดีเอสนั้นจากรูปจะติดตั้งระหว่างเราท์เตอร์และไฟร์วอลล์เพื่อที่จะตรวจทราฟิกที่วิ่งเข้าออกระหว่างเครือข่ายและอินเตอร์เน็ต และแจ้งเตือนถ้าพบหลักฐานที่คาดว่าจะเป็นการบุกรุกเครือข่าย ในการติดตั้งระบบเตือนภัยของควรมีทั้ง 2 ประเภทเพื่อการแจ้งเตือนที่มีประสิทธิภาพ ผู้ดูแลสามารถรับรู้ได้อย่างรวดเร็ว เพื่อเตรียมการรับมือกับเหตุการณ์ที่เกิดขึ้นได้อย่างทันท่วงที

บทที่ 6
วิเคราะห์ความเป็นไปได้ทางธุรกิจ

โมเดลของผู้ให้บริการอินเตอร์เน็ตทั้ง 3 โมเดล นำมาวิเคราะห์ความเป็นไปได้ในการทำธุรกิจ โดยประเมินผลการประกอบการในระยะเวลา 10 ปี โดยใช้ระยะเวลาการคืนทุน (Payback Period), Net Present Value, Internal Rate of Return เปรียบเทียบการทำธุรกิจในแต่ละโมเดล เพื่อเป็นแนวทางในการตัดสินใจในการประกอบธุรกิจต่อไป

6.1 ค่าใช้จ่ายทั้งหมดในการทำกิจการ

ค่าใช้จ่ายในการประกอบกิจการทั้งหมดเป็นระยะเวลา 10 ปี ประกอบด้วย

1. ค่าอุปกรณ์ (Asset Cost)

ผู้ให้บริการอินเตอร์เน็ต ทั้ง 3 ประเภท ใช้ชนิดและจำนวนของอุปกรณ์แตกต่างกันแล้วแต่ลักษณะการให้บริการ, ปริมาณผู้ใช้บริการอินเตอร์เน็ต และระดับความปลอดภัยที่ต้องการ ดังแสดงในตารางที่ 6.1

ตารางที่ 6.1 แสดงรายการอุปกรณ์เครือข่ายของผู้ให้บริการอินเตอร์เน็ตทั้ง 3 โมเดล

Network Equipment	Model 1	Model 2	Model 3
Border Router / Cisco 7200 @ 1,517,000	1	1	1
Border Router / Cisco 7200 @ 1,517,000	1	1	1
Switch Layer 3 / Catalyst 6500 @ 840,500	1	1	2
Switch Layer 2 / Catalyst 5000 @ 20,500	3	5	6
RAS Router / Cisco 5350 @ 2,200,000	6	8	16
BRAS / Nortel Shasta 500BSC/1STM1 @ 800,000	-	1	-
BRAS / Nortel Shasta 500BSC/2STM1 @ 1,000,000	-	-	1
Corporate / Cisco 7513 @ 2,500,000	-	4	8
Corporate / Cisco MGX8850 @ 2,300,000	-	1	1
Web Server / Compaq DL380 @ 150,000	1	1	1
DNS Server / Sun E250 @ 200,000	-	1	1
DNS Server / Compaq DL380 @ 150,000	1	-	-
NMS Server / Sun Ultra5 @ 250,000	-	1	1
NMS Server / Compaq DL380 @ 150,000	1	-	-
Mail Server / Sun E220 @ 205,000	-	3	3
Mail Server / Compaq DL380 @ 150,000	1	-	-
Storage Server / NetApp @ 880,000	-	1	1
Radius Server / Sun E220 @ 205,000	-	2	2
Radius Server / Compaq DL380 @ 150,000	1	-	-

ตารางที่ 6.1 แสดงรายการอุปกรณ์เครือข่ายของผู้ให้บริการอินเตอร์เน็ตทั้ง 3 โมเดล (ต่อ)

Network Equipment	Model 1	Model 2	Model 3
Prepaid Server / Compaq DL380 @ 150,000	1	-	-
Billing Server / Sun E250 @ 200,000	-	1	1
Billing Server / Compaq DL380 @ 150,000	1	-	-
LDAP Server / Sun E250 @ 200,000	-	1	1
LDAP Server / Compaq DL380 @ 150,000	1	-	-
Proxy / NetApp @ 380,000	2	3	3
Hosting Server / Compaq DL380 @ 150,000	-	1	1
Security / Back up System Equipment	**Model 1**	**Model 2**	**Model 3**
Antivirus Server / Compaq DL380 @ 150,000	1	3	3
Firewall (software) / IBM Notfinity @ 70,000	1	-	-
Firewall / Netscreen 208 @ 430,000	1	-	-
Firewall / Netscreen 500 @ 650,000	-	2	3
IDS Server / Compaq DL380 @ 150,000	2	2	5
Web Server / Compaq DL380 @ 150,000	1	1	1
Storage Server / NetApp @ 880,000	-	-	1
Prepaid Server / Sun E250 @ 200,000	-	-	1
Billing Server / Sun E250 @ 200,000	-	-	1
LDAP Server / Sun E250 @ 200,000	-	-	1

สรุปราคาค่าอุปกรณ์ทั้งหมดที่ผู้ใช้บริการอินเตอร์เน็ต โดยแยกเป็นราคาอุปกรณ์ที่เกี่ยวกับการเชื่อมต่อรวมถึง server ต่างๆ และอุปกรณ์ที่เกี่ยวกับการรักษาความปลอดภัยเครือข่าย ดังแสดงในตารางที่ 6.2

ตารางที่ 6.2 แสดงค่าใช้จ่ายโดยประมาณของอุปกรณ์ในการติดตั้งระบบ

System Equipment	Model 1	Model 2	Model 3
Network System Cost	18,500,000	38,100,000	66,700,000
Security System Cost	1,100,000	2,200,000	4,800,000
Total System Cost	**19,600,000**	**40,300,000**	**71,500,000**

2. ค่าเช่า Link Internet

ตารางที่ 6.3 แสดงค่าใช้จ่ายเช่า Link Internet ต่อเดือน

Description	Model 1	Model 2	Model 3
ค่าเช่า Link Domestic 100 Mbps	3,000	-	-
ค่าเช่า Link Inter. 1.5 Mbps	140,500	-	-
ค่าเช่า Link Domestic 1 Gbps	-	7,500	-
ค่าเช่า Link Inter. 45 Mbps	-	1,900,000	-
ค่าเช่า Link Domestic 2 Gbps	-	-	13,000
ค่าเช่า Link Inter. 155 Mbps	-	-	3,800,000
Total	**143,500**	**1,907,500**	**3,813,000**

3. เงินเดือนพนักงาน

เงินเดือนพนักงาน คิดที่ 15,000 บาท ผู้จัดการ 30,000 บาท

- ผู้ให้บริการอินเตอร์เน็ตโมเดลที่ 1 พนักงาน 6 คน ผู้จัดการ 1 คน
- ผู้ให้บริการอินเตอร์เน็ตโมเดลที่ 2 พนักงาน 15 คน ผู้จัดการ 1 คน
- ผู้ให้บริการอินเตอร์เน็ตโมเดลที่ 3 พนักงาน 25 คน ผู้จัดการ 1 คน

4. ค่าสาธารณูปโภค

5. ค่าติดตั้งและซ่อมบำรุงอุปกรณ์

6. ค่าเช่าออฟฟิศ ในอัตรา 160 บาท/ ตร.ม.

7. ดอกเบี้ยเงินกู้ระยะยาว MLR 6% ชำระภายใน 10 ปี

8. ภาษีเงินได้ 30% กิจการได้รับการยกเว้นภาษีเงินได้ 5 ปี

6.2 การประเมิน Cost-Benefit

Cash flow forecasting

ตารางที่ 6.4 แสดงค่า Net Profit ในระยะเวลา 10 ปี

Year	Model 1	Model 2	Model 3
0	-19,972,000	-40,960,000	-72,530,000
1	1,598,400	8,942,400	17,055,000
2	1,571,634	8,887,365	16,957,358
3	1,543,262	8,829,029	16,853,857
4	1,513,187	8,767,192	16,744,147
5	1,496,308	9,001,645	17,227,853
6	1,013,261	6,042,515	11,553,208
7	988,188	5,990,961	11,461,741
8	961,610	5,936,314	11,364,786
9	933,438	5,878,388	11,262,014
10	914,075	6,026,986	11,573,075
Net Profit	12,533,362	74,302,794	142,053,039

ตารางที่ 6.5 แสดงการประมาณการเงินสดจ่ายต่อปี: ผู้ให้บริการอินเตอร์เน็ตโมเดลที่ 1

ปีที่	0	1	2	3	4	5	6	7	8	9	10
ค่าอุปกรณ์	19,600,000	0	0	0	0	0	0	0	0	0	0
ค่าติดตั้ง	180,000	0	0	0	0	0	0	0	0	0	0
ค่าเช่าลิงค์	0	1,722,000	1,722,000	1,722,000	1,722,000	1,722,000	1,722,000	1,722,000	1,722,000	1,722,000	1,722,000
เงินเดือนพนักงาน	0	1,440,000	1,440,000	1,440,000	1,440,000	1,440,000	1,440,000	1,440,000	1,440,000	1,440,000	1,440,000
ค่าซ่อมบำรุง	0	0	0	0	0	50,000	0	0	0	0	50,000
ค่าสาธารณูปโภค	0	798,000	798,000	798,000	798,000	798,000	798,000	798,000	798,000	798,000	798,000
ค่าเช่าออฟฟิศ	192,000	192,000	192,000	192,000	192,000	192,000	192,000	192,000	192,000	192,000	192,000
ดอกเบี้ยเงินกู้ 6%	0	1,176,000	1,086,779	992,205	891,957	785,694	673,055	553,657	427,096	292,941	150,737
เงินสดจ่าย	19,972,000	5,328,000	5,238,779	5,144,205	5,043,957	4,987,694	4,825,055	4,705,657	4,579,096	4,444,941	4,352,737

ตารางที่ 6.6 แสดงการประมาณการงบประมาณเงินสดของโครงการ: ผู้ให้บริการอินเตอร์เน็ตโมเดลที่ 1

ปีที่	0	1	2	3	4	5	6	7	8	9	10
ประมาณการเงินสดจ่าย	-19,972,000	-5,328,000	-5,238,779	-5,144,205	-5,043,957	-4,987,694	-4,825,055	-4,705,657	-4,579,096	-4,444,941	-4,352,737
ประมาณการเงินสดรับ	0	6,926,400	6,810,413	6,687,467	6,557,144	6,484,002	6,272,571	6,117,354	5,952,824	5,778,423	5,658,557
กำไรก่อนหักภาษี	0	1,598,400	1,571,634	1,543,262	1,513,187	1,496,308	1,447,516	1,411,697	1,373,729	1,333,482	1,305,821
ภาษีเงินได้ 30%	0	0	0	0	0	0	-434,255	-423,509	-412,119	-400,045	-391,746
กำไรสุทธิ	0	1,598,400	1,571,634	1,543,262	1,513,187	1,496,308	1,013,261	988,188	961,610	933,438	914,075

หมายเหตุ กิจการได้รับการยกเว้นการเสียภาษีเงินได้ เป็นเวลา 5 ปี และกำไรก่อนหักภาษีคิดที่ 30% ของรายจ่าย

ผู้ให้บริการอินเตอร์เน็ตโมเดลที่ 1

Payback Period คือ การหาจุดคุ้มทุนในการลงทุน

ตารางที่ 6.7 แสดง Payback Period ของผู้ให้บริการอินเตอร์เน็ตโมเดลที่ 1

Year	Cash flow	Payback Period
0	-19,972,000	-19,972,000
1	1,598,400	-18,373,600
2	1,571,634	-16,801,966
3	1,543,262	-15,258,705
4	1,513,187	-13,745,518
5	1,496,308	-12,249,209
6	1,013,261	-11,235,948
7	988,188	-10,247,760
8	961,610	-9,286,150
9	933,438	-8,352,712
10	914,075	-7,438,638

** พบว่าระยะเวลาในการคืนทุนนาน มากกว่า 10 ปี จึงไม่เหมาะแก่การลงทุน

ตารางที่ 6.8 แสดงการหาค่า NPV ที่ Discount rate 10 %

Year	Cash flow	Discount factor 10 %	Discount Cash flow
0	19,972,000	1.0000	19,972,000.0000
1	1,598,400	0.9091	1,453,090.9091
2	1,571,634	0.8264	1,298,870.8959
3	1,543,262	0.7513	1,159,475.2780
4	1,513,187	0.6830	1,033,527.1325
5	1,496,308	0.6209	929,089.5947
6	1,013,261	0.5645	571,959.6709
7	988,188	0.5132	507,096.6854
8	961,610	0.4665	448,598.2131
9	933,438	0.4241	395,868.6483
10	914,075	0.3855	352,415.3543
NPV			**-11,822,007.6177**

Discount factor ในปี year คำนวณได้จาก $1/(1+r)^{year}$

** พบว่าค่า NPV ที่ Discount rate 10% ในระยะ 10 ปี มีค่าติดลบ โมเดลนี้ไม่สมควรลงทุน

ตารางที่ 6.9 แสดงการประมาณการเงินสดจ่ายต่อปี: ผู้ให้บริการอินเตอร์เน็ตโมเดลที่ 2

ปีที่	0	1	2	3	4	5	6	7	8	9	10
ค่าอุปกรณ์	40,300,000	0	0	0	0	0	0	0	0	0	0
ค่าติดตั้ง	300,000	0	0	0	0	0	0	0	0	0	0
ค่าเช่าลิงค์	0	22,890,000	22,890,000	22,890,000	22,890,000	22,890,000	22,890,000	22,890,000	22,890,000	22,890,000	22,890,000
เงินเดือนพนักงาน	0	3,060,000	3,060,000	3,060,000	3,060,000	3,060,000	3,060,000	3,060,000	3,060,000	3,060,000	3,060,000
ค่าซ่อมบำรุง	0	0	0	0	0	1,000,000	0	0	0	0	1,000,000
ค่าสาธารณูปโภค	0	1,080,000	1,080,000	1,080,000	1,080,000	1,080,000	1,080,000	1,080,000	1,080,000	1,080,000	1,080,000
ค่าเช่าออฟฟิศ	360,000	360,000	360,000	360,000	360,000	360,000	360,000	360,000	360,000	360,000	360,000
ดอกเบี้ยเงินกู้ 6 %	0	2,418,000	2,234,551	2,040,096	1,833,973	1,615,482	1,383,883	1,138,387	878,161	602,322	309,933
เงินสดจ่าย	40,960,000	29,808,000	29,624,551	29,430,096	29,223,973	30,005,482	28,773,883	28,528,387	28,268,161	27,992,322	28,699,933

ตารางที่ 6.10 แสดงการประมาณการงบประมาณเงินสดของโครงการ: ผู้ให้บริการอินเตอร์เน็ตโมเดลที่ 2

ปีที่	0	1	2	3	4	5	6	7	8	9	10
ประมาณการเงินสดจ่าย	-40,960,000	-29,808,000	-29,624,551	-29,430,096	-29,223,973	-30,005,482	-28,773,883	-28,528,387	-28,268,161	-27,992,322	-28,699,933
ประมาณการเงินสดรับ	0	38,750,400	38,511,917	38,259,124	37,991,164	39,007,127	37,406,047	37,086,903	36,748,610	36,390,019	37,309,913
กำไรก่อนหักภาษี	0	8,942,400	8,887,365	8,829,029	8,767,192	9,001,645	8,632,165	8,558,516	8,480,448	8,397,697	8,609,980
ภาษีเงินได้ 30%	0	0	0	0	0	0	-2,589,649	-2,567,555	-2,544,135	-2,519,309	-2,582,994
กำไรสุทธิ	0	8,942,400	8,887,365	8,829,029	8,767,192	9,001,645	6,042,515	5,990,961	5,936,314	5,878,388	6,026,986

หมายเหตุ กิจการได้รับการยกเว้นการเสียภาษีเงินได้ เป็นเวลา 5 ปี และกำไรก่อนหักภาษี คิดที่ 30% ของรายจ่าย

ผู้ให้บริการอินเตอร์เน็ตโมเดลที่ 2

Payback Period คือ การหาจุดคุ้มทุนในการลงทุน

ตารางที่ 6.11 แสดง Payback Period ของผู้ให้บริการอินเตอร์เน็ตโมเดลที่ 2

Year	Cash flow	Payback Period
0	-40,960,000	-40,960,000
1	8,942,400	-32,017,600
2	8,887,365	-23,130,235
3	8,829,029	-14,301,206
4	8,767,192	-5,534,014
5	9,001,645	3,467,631

** พบว่าระยะเวลาในการคืนทุนปีที่ 5

Return on Investment (ROI) or Accounting rate of return (ARR)

คำนวณหาเปอร์เซ็นต์เพื่อเปรียบเทียบผลกำไรที่เกิดขึ้นต่อการลงทุนทั้งหมด

$$\text{ROI} = \frac{\text{average annual profit}}{\text{Total investment}} \times 100$$

** พบว่า **ROI = 18.14 %**

Net Present Value (NPV)

คำนวณหาค่า NPV ด้วย Discount rate 10 %

ตารางที่ 6.12 แสดงการหาค่า NPV ที่ Discount rate 10 %

Year	Cash flow	Discount factor 10 %	Discount Cash flow
0	40,960,000	1.0000	40,960,000.0000
1	8,942,400	0.9091	8,129,454.5455
2	8,887,365	0.8264	7,344,930.0689
3	8,829,029	0.7513	6,633,379.9322
4	8,767,192	0.6830	5,988,109.9615
5	9,001,645	0.6209	5,589,313.1279
6	6,042,515	0.5645	3,410,842.3730
7	5,990,961	0.5132	3,074,310.3825
8	5,936,314	0.4665	2,769,334.2242
9	5,878,388	0.4241	2,493,010.2039
10	6,026,986	0.3855	2,323,663.9621
NPV			**6,796,348.7816**

Internal rate of return (IRR)

หาค่า IRR โดย ค่า NPV ต้องเข้าใกล้ศูนย์ที่สุด

ตารางที่ 6.13 แสดงการหาค่า IRR

Year	Cash flow	Discount factor 14.145 %	Discount Cash flow
0	40,960,000	1.0000	40,960,000.0000
1	8,942,400	0.8761	7,834,245.9153
2	8,887,365	0.7675	6,821,175.9266
3	8,829,029	0.6724	5,936,661.0075
4	8,767,192	0.5891	5,164,555.3675
5	9,001,645	0.5161	4,645,552.8397
6	6,042,515	0.4521	2,731,973.0190
7	5,990,961	0.3961	2,373,002.8555
8	5,936,314	0.3470	2,059,973.8847
9	5,878,388	0.3040	1,787,089.0368
10	6,026,986	0.2663	1,605,207.7570
NPV			-562.3905

** พบว่า **IRR = 14.145 %**

ตารางที่ 6.14 แสดงการประมาณการเงินสดจ่ายต่อปี: ผู้ให้บริการอินเตอร์เน็ตโมเดลที่ 3

ปีที่	0	1	2	3	4	5	6	7	8	9	10
ค่าอุปกรณ์	71,500,000	0	0	0	0	0	0	0	0	0	0
ค่าติดตั้ง	550,000	0	0	0	0	0	0	0	0	0	0
ค่าเช่าลิงค์	0	45,756,000	45,756,000	45,756,000	45,756,000	45,756,000	45,756,000	45,756,000	45,756,000	45,756,000	45,756,000
เงินเดือนพนักงาน	0	4,860,000	4,860,000	4,860,000	4,860,000	4,860,000	4,860,000	4,860,000	4,860,000	4,860,000	4,860,000
ค่าซ่อมบำรุง	0	0	0	0	0	2,000,000	0	0	0	0	2,000,000
ค่าสาธารณูปโภค	0	1,464,000	1,464,000	1,464,000	1,464,000	1,464,000	1,464,000	1,464,000	1,464,000	1,464,000	1,464,000
ค่าเช่าออฟฟิศ	480,000	480,000	480,000	480,000	480,000	480,000	480,000	480,000	480,000	480,000	480,000
ดอกเบี้ยเงินกู้ 6 %	0	4,290,000	3,964,526	3,619,524	3,253,822	2,866,178	2,455,275	2,019,718	1,558,028	1,068,636	549,881
เงินสดจ่าย	72,530,000	56,850,000	56,524,526	56,179,524	55,813,822	57,426,178	55,015,275	54,579,718	54,118,028	53,628,636	55,109,881

ตารางที่ 6.15 แสดงการประมาณการงบประมาณเงินสดของโครงการ: ผู้ให้บริการอินเตอร์เน็ตโมเดลที่ 3

ปีที่	0	1	2	3	4	5	6	7	8	9	10
ประมาณการเงินสดจ่าย	-72,530,000	-56,850,000	-56,524,526	-56,179,524	-55,813,822	-57,426,178	-55,015,275	-54,579,718	-54,118,028	-53,628,636	-55,109,881
ประมาณการเงินสดรับ	0	73,905,000	73,481,884	73,033,382	72,557,969	74,654,032	71,519,858	70,953,634	70,353,436	69,717,227	71,642,845
กำไรก่อนหักภาษี	0	17,055,000	16,957,358	16,853,857	16,744,147	17,227,853	16,504,583	16,373,916	16,235,408	16,088,591	16,532,964
ภาษีเงินได้ 30%	0	0	0	0	0	0	-4,951,375	-4,912,175	-4,870,623	-4,826,577	-4,959,889
กำไรสุทธิ	0	17,055,000	16,957,358	16,853,857	16,744,147	17,227,853	11,553,208	11,461,741	11,364,786	11,262,014	11,573,075

หมายเหตุ กิจการได้รับการยกเว้นการเสียภาษีเงินได้ เป็นเวลา 5 ปี และกำไรก่อนหักภาษี คิดที่ 30% ของรายจ่าย

ผู้ให้บริการอินเตอร์เน็ตโมเดลที่ 3

Payback Period คือ การหาจุดคุ้มทุนในการลงทุน

ตารางที่ 6.16 แสดง Payback Period ของผู้ให้บริการอินเตอร์เน็ตโมเดลที่ 3

Year	Cash flow	Payback Period
0	-72,530,000	-72,530,000
1	17,055,000	-55,475,000
2	16,957,358	-38,517,642
3	16,853,857	-21,663,785
4	16,744,147	-4,919,638
5	17,227,853	12,308,215

** พบว่าระยะเวลาในการคืนทุนปีที่ 5

Return on Investment (ROI) or Accounting rate of return (ARR)

คำนวณหาเปอร์เซ็นต์เพื่อเปรียบเทียบผลกำไรที่เกิดขึ้นต่อการลงทุนทั้งหมด

$$ROI = \frac{\text{average annual profit}}{\text{Total investment}} \times 100$$

** พบว่า **ROI = 19.59 %**

Net Present Value (NPV)

คำนวณหาค่า NPV ด้วย Discount rate 10 %

ตารางที่ 6.17 แสดงการหาค่า NPV ที่ Discount rate 10 %

Year	Cash flow	Discount factor 10 %	Discount Cash flow
0	72,530,000	1.0000	72,530,000.0000
1	17,055,000	0.9091	15,504,545.4545
2	16,957,358	0.8264	14,014,345.4016
3	16,853,857	0.7513	12,662,552.4779
4	16,744,147	0.6830	11,436,477.5118
5	17,227,853	0.6209	10,697,141.5666
6	11,553,208	0.5645	6,521,484.6262
7	11,461,741	0.5132	5,881,685.3665
8	11,364,786	0.4665	5,301,756.4767
9	11,262,014	0.4241	4,776,193.1303
10	11,573,075	0.3855	4,461,921.3783
NPV			**18,728,103.3905**

Internal rate of return (IRR)

หาค่า IRR โดย ค่า NPV ต้องเข้าใกล้ศูนย์ที่สุด

ตารางที่ 6.18 แสดงการหาค่า IRR

Year	Cash flow	Discount factor 16.355 %	Discount Cash flow
0	72,530,000	1.0000	72,530,000.0000
1	17,055,000	0.8594	14,657,728.5033
2	16,957,358	0.7386	12,525,298.5487
3	16,853,857	0.6348	10,699,024.0119
4	16,744,147	0.5456	9,135,300.1045
5	17,227,853	0.4689	8,078,038.4614
6	11,553,208	0.4030	4,655,778.2031
7	11,461,741	0.3463	3,969,677.5513
8	11,364,786	0.2977	3,382,835.2925
9	11,262,014	0.2558	2,881,048.6475
10	11,573,075	0.2199	2,544,475.4211
NPV			-795.2547

** พบว่า IRR = 16.355 %

6.3 สรุปผลโมเดลการประกอบธุรกิจของผู้ให้บริการอินเตอร์เน็ต

ตารางที่ 6.19 สรุปผลโมเดลการประกอบธุรกิจของผู้ให้บริการอินเตอร์เน็ตทั้ง 3 โมเดล

ISP	Payback Period	ROI (%)	IRR (%)
ISP Model 1	>10	-	-
ISP Model 2	5	18.14	14.145
ISP Model 3	5	19.59	16.355

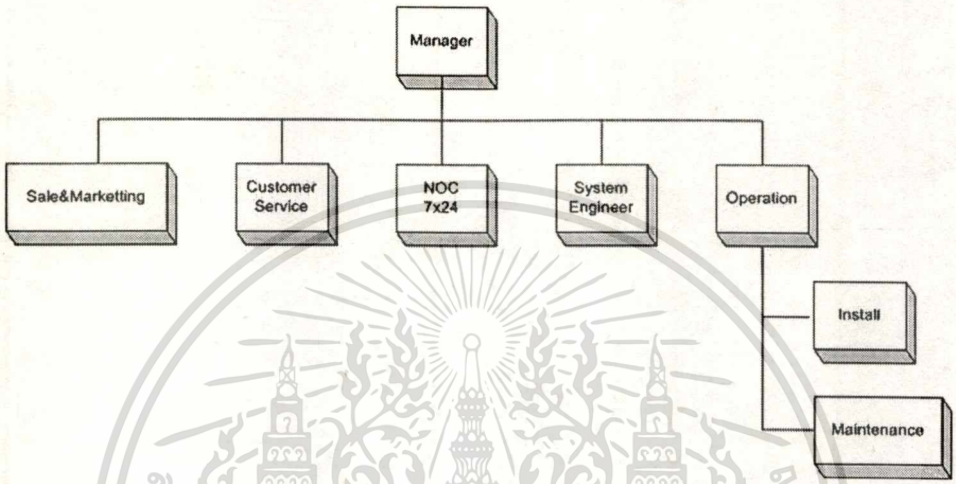
วิเคราะห์ข้อมูล จากตารางจะเห็นได้ว่า

1. ผู้ให้บริการอินเตอร์เน็ตโมเดลที่ 1 คืนทุนช้ามาก กลุ่มลูกค้าน้อยเนื่องจากประเภทของการให้บริการน้อยทำกำไรได้ยาก และค่า NPV ติดลบ สรุปได้ว่าไม่เหมาะสมแก่การลงทุน

2. ผู้ให้บริการอินเตอร์เน็ตโมเดลที่ 2 ระยะเวลาในการคืนทุนประมาณ 5 ปี ค่า ROI 18.14 % และ IRR 14.145 % พบว่าเหมาะสมแก่การลงทุนมากกว่าโมเดลที่ 1

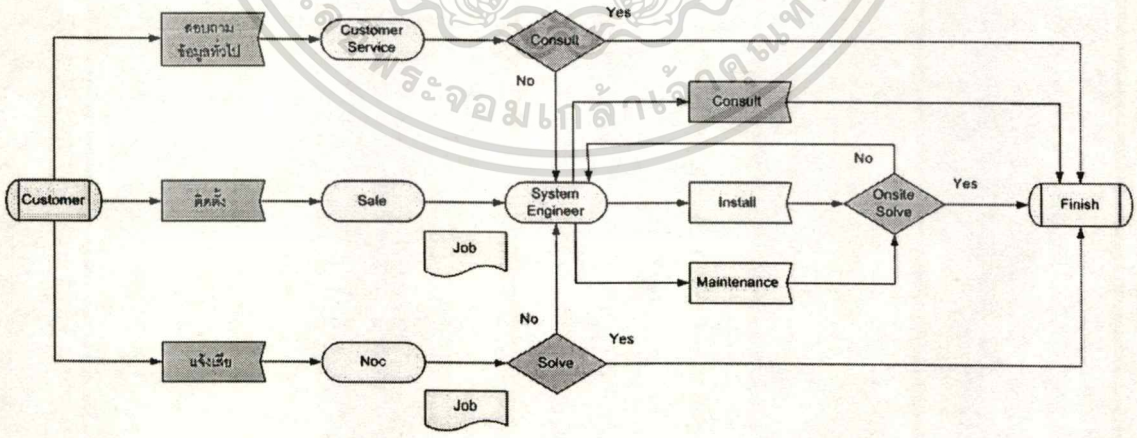
3. ผู้ให้บริการอินเตอร์เน็ตโมเดลที่ 3 ระยะเวลาในการคืนทุนประมาณ 5 ปี ค่า ROI 19.59 % และ IRR 16.355 % พบว่ามีค่า ROI และ IRR มากที่สุด เหมาะสมแก่การลงทุนมากที่สุด

6.4 การจัดแบ่งองค์กรและขั้นตอนการให้บริการลูกค้า



รูปที่ 6.1 การจัดแบ่งองค์กรของผู้ให้บริการอินเตอร์เน็ต

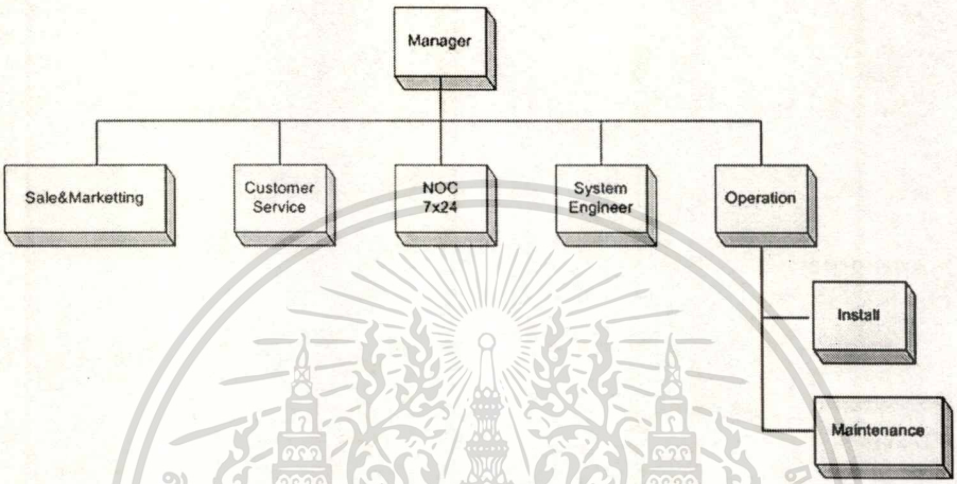
ขั้นตอนการให้บริการและหน่วยงานที่เกี่ยวข้อง



รูปที่ 6.2 แสดงขั้นตอนการให้บริการลูกค้า

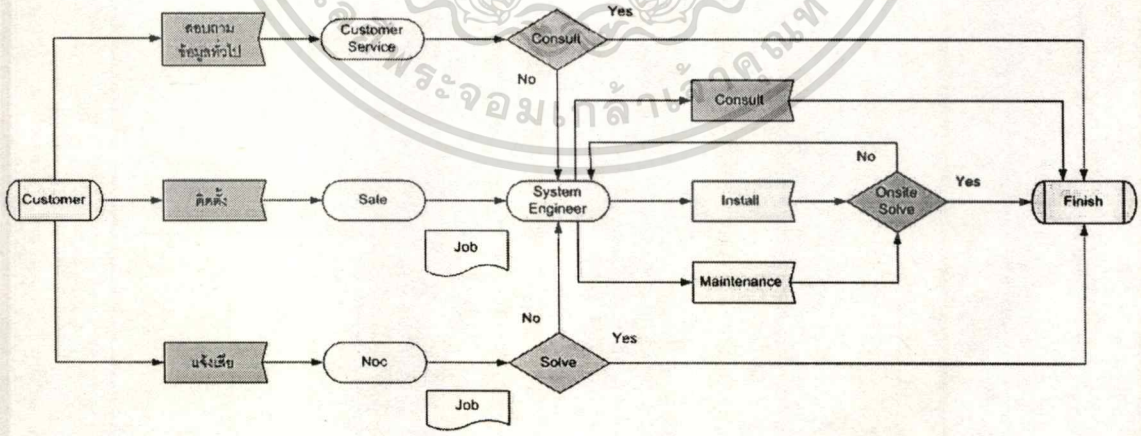
3. ผู้ให้บริการอินเตอร์เน็ตโมเดลที่ 3 ระยะเวลาในการคืนทุนประมาณ 5 ปี ค่า ROI 19.59 % และ IRR 16.355 % พบว่ามีค่า ROI และ IRR มากที่สุด เหมาะสมแก่การลงทุนมากที่สุด

6.4 การจัดแบ่งองค์กรและขั้นตอนการให้บริการลูกค้า



รูปที่ 6.1 การจัดแบ่งองค์กรของผู้ให้บริการอินเตอร์เน็ต

ขั้นตอนการให้บริการและหน่วยงานที่เกี่ยวข้อง



รูปที่ 6.2 แสดงขั้นตอนการให้บริการลูกค้า

หน่วยงานที่เกี่ยวข้องในการให้บริการลูกค้า มีดังนี้

1. **Customer Service**

หน้าที่ - ให้คำปรึกษาแก่ลูกค้าในเรื่องทั่วไป เช่น อัตราค่าบริการ, ปัญหาทางเทคนิคทั่วไป, สอบถามเวลาและค่าบริการ เป็นต้น โดยใช้ระบบ CRM (Customer Relationship Management) ในการให้บริการลูกค้า หากตอบคำถามทางเทคนิคไม่ได้ให้ลูกค้าปรึกษาทาง System Engineer ต่อไป

2. **Sale**

หน้าที่ - ให้ข้อมูลเกี่ยวกับงานขายและสอบถามความต้องการของลูกค้า

- ออกเอกสาร Job Request ให้ System Engineer เพื่อเตรียม Configuration และระบบให้พร้อมก่อนการติดตั้ง
- ออกเอกสารหนังสือสัญญาการและเก็บค่าใช้จ่ายในการใช้บริการแก่ลูกค้า
- ดูแลและสร้างความพึงพอใจแก่ลูกค้าหลังการขาย
- ประสานงานระหว่างลูกค้าและ System Engineer

3. **Network Operation Center**

หน้าที่ - รับงานแจ้งเสียตลอด 24 ชม. เปิดงานเสีย และแก้ไขปัญหาเบื้องต้น (First Level) ทางโทรศัพท์ หากแก้ไขไม่ได้ส่งใบงานต่อไปยัง System Engineer (2 Level)

- Monitoring ตรวจเช็คการทำงานของระบบให้อยู่ในสภาพปกติตลอดเวลา
- จัดทำรายงานสรุปการแจ้งเสียเป็นประจำทุกเดือน โดยแยกเป็นประเภทและราย ชื่อลูกค้าเพื่อเป็นข้อมูลในการวิเคราะห์หาแนวทางในการป้องกันและแก้ไขปัญหา

4. **System Engineer**

หน้าที่ - ให้คำปรึกษาแก่ลูกค้าและหน่วยงานที่เกี่ยวข้อง (Second Level)

- วิเคราะห์และสรุปสาเหตุของปัญหา
- จัดเตรียม Configuration และระบบให้พร้อมก่อนการติดตั้ง
- หากแก้ไขปัญหาไม่ได้ทางโทรศัพท์ทำการส่งงานต่อไปยังแผนก Maintenance และให้คำปรึกษาในการแก้ปัญหาต่อไป
- วิเคราะห์และตรวจสอบพฤติกรรมการใช้งาน และขนาด Bandwidth ที่ใช้
- เพิ่ม, ลบ และแก้ไข ข้อมูล Username/Password และการให้บริการในการตรวจสอบ AAA (Authentication, Authorization, Accounting) ของลูกค้า Individual
- หาเทคโนโลยีใหม่ๆ เพื่อความทันสมัยอยู่เสมอ

5. Installation

หน้าที่ - จัดเตรียมอุปกรณ์และ Configuration ทำการ Onsite Service ติดตั้งอุปกรณ์ที่ site ลูกค้า

- สรุปงานข้อมูลลูกค้าเก็บใน Database
- แนะนำการใช้งานและแก้ไขปัญหาเบื้องต้นเพื่อลดอัตราการแจ้งเสียที่จะเกิดขึ้น

6. Maintenance

หน้าที่ - Onsite Service แก้ไขปัญหาที่หน้า site งาน

- สรุปและรวบรวมผลการแก้ปัญหาเพื่อเป็นข้อมูลในการแก้ไขครั้งต่อไป
- ทำการตรวจเช็คระบบและอุปกรณ์ประจำปี (Preventive Maintenance)

บทที่ 7
สรุปผลและข้อเสนอแนะ

7.1 สรุปผล

เมื่ออินเตอร์เน็ตเป็นสิ่งที่ขาดไม่ได้ในยุคปัจจุบันนี้ แทบทุกองค์กรมีการเชื่อมต่อกับอินเตอร์เน็ตโดยผ่านผู้ให้บริการอินเตอร์เน็ต ธุรกิจการให้บริการอินเตอร์เน็ตจึงเป็นธุรกิจที่น่าจับตามอง และการรักษาความปลอดภัยของผู้ให้บริการอินเตอร์เน็ตเป็นสิ่งสำคัญและขาดไม่ได้ ปัจจุบันอินเตอร์เน็ตได้แพร่หลายไปทั่วโลก ดังนั้นผู้ให้บริการอินเตอร์เน็ตจึงต้องมีระบบรักษาความปลอดภัยของข้อมูลและสารสนเทศอย่างเข้มงวดเพื่อการสื่อสารของข้อมูลที่ราบรื่น

การทำธุรกิจการให้บริการอินเตอร์เน็ตสิ่งที่ต้องคำนึงถึงคือ การเลือกใช้อุปกรณ์, การวางระบบเน็ตเวิร์ค, การประมาณการค่าใช้จ่ายและผลกำไร เพื่อวิเคราะห์ว่าเหมาะสมสำหรับการลงทุนหรือไม่ ในการศึกษานี้ใช้การวิเคราะห์จากระยะเวลาในการคืนทุน (Payback Period), Net Present Value, Internal Rate of Return ในการประเมินหาความเหมาะสมและประกอบการตัดสินใจในการเริ่มทำธุรกิจ เนื่องจากเป็นการลงทุนที่สูงและใช้ระยะเวลาในการคืนทุนนาน ผู้ประกอบธุรกิจให้บริการอินเตอร์เน็ตต้องวางแผนในการวางระบบเป็นอย่างดี

ในการศึกษานี้นอกจากในแง่มุมการลงทุนทางธุรกิจจะกล่าวถึงความหมาย วัตถุประสงค์ของความปลอดภัย การพัฒนาระบบรักษาความปลอดภัย มาตรฐานด้านความปลอดภัยของข้อมูล (ISO/IEC17799) การจัดการความเสี่ยง และวิธีการโจมตีต่างๆ ของผู้ไม่ประสงค์ดีที่ใช้ทำการโจมตีหรือบุกรุกเครือข่าย เช่น แพ็ตเก็ตสนิฟเฟอร์ แมนอินเดอะมิดเดิล และดีไนล์ออฟเซอร์วิส เป็นต้น ซึ่งเป็นเครื่องมือหรือโปรแกรมสำหรับการโจมตีแบบต่างๆ ซึ่งค้นหาและดาวน์โหลดจากอินเตอร์เน็ตมาใช้งานได้ง่าย ดังนั้นการเชื่อมต่อกับอินเตอร์เน็ตจึงต้องมีระบบรักษาความปลอดภัยภายในเครือข่ายด้วย

การรักษาความปลอดภัยภายในเครือข่ายนั้นสิ่งแรกที่ต้องนึกถึงคือ ไฟร์วอลล์ ซึ่งเป็นระบบที่ควบคุมการใช้งานระหว่างเครือข่าย โดยเปรียบเสมือนยามที่คอยตรวจตราการเข้าออกจากสถานที่ต่างๆ และ IDS เป็นเครื่องมือรักษาความปลอดภัยในเครือข่ายอีกประเภทหนึ่ง ที่ใช้สำหรับตรวจจับการโจมตีหรือความพยายามที่จะโจมตีเครือข่าย

7.2 ข้อเสนอแนะ

เมื่อตัดสินใจประกอบธุรกิจให้บริการอินเตอร์เน็ตแล้วนอกจากการมีระบบและอุปกรณ์รักษาความปลอดภัยที่ดีแล้ว สิ่งสำคัญคือต้องมีนโยบายและมาตรการรักษาความปลอดภัย ทั้งทางด้าน การบริหารจัดการ การปฏิบัติการ การดำเนินการด้านเทคนิค นอกจากนั้นผู้บริหารระดับสูงควรจะต้องวางนโยบายควบคุมจากเพื่อใช้เป็นข้อบังคับให้พนักงานที่รับผิดชอบและพนักงานทั่วไปปฏิบัติตามอย่างเคร่งครัด

การในการรักษาความปลอดภัยของผู้ให้บริการอินเตอร์เน็ตต้องมีความเหมาะสม ไม่มากและไม่น้อยจนเกินไป เนื่องจากมีข้อจำกัดในการเชื่อมต่อกับผู้ใช้และเครือข่ายอินเตอร์เน็ต เพราะผู้ใช้ต้องใช้บริการจากอินเตอร์เน็ตได้อย่างเต็มที่หากมีการป้องกันที่แน่นหนาเกินไปอาจทำให้ผู้ใช้ไม่สามารถใช้บางแอพพลิเคชั่นที่ต้องการได้ ผู้ให้บริการส่วนมากเปิดการให้บริการทุกแอพพลิเคชันสามารถวิ่งผ่านได้ และทำการควบคุมความปลอดภัยโดยการใช้ไฟร์วอลล์ที่สามารถรองรับปริมาณทราฟฟิคที่มากมายมหาศาลจากการเชื่อมต่อ เพื่อป้องกัน Server ที่ให้บริการ และผู้ให้บริการอินเตอร์เน็ตต้องทันต่อเหตุการณ์เพื่อสามารถรับมือและแก้ไขกับปัญหาได้อย่างรวดเร็วและถูกต้องที่สุด

7.3 สรุป

ในปัจจุบันโลกอินเตอร์เน็ตได้เปิดกว้างขยายไปทั่วทุกภูมิภาคในโลก ให้ประโยชน์มหาศาลแต่ในขณะเดียวกันก็อาจมีโทษอย่างที่คาดคิด ผู้ให้บริการอินเตอร์เน็ตจำเป็นต้องมีนโยบายและมาตรการรักษาความปลอดภัยแก่ทั้งองค์กรตัวเอง และผู้ที่มาใช้บริการเชื่อมต่ออินเตอร์เน็ต ซึ่งเป็นไปตามมาตรฐานด้านความปลอดภัยของข้อมูล ISO/IEC 17799 ซึ่งเนื้อหาชัดเจนครบถ้วนสำหรับการปกป้องสารสนเทศโดยทั่วไป ไม่เฉพาะธุรกิจใดๆ

จากการศึกษาชี้ให้เห็นถึงการประเมินและวิเคราะห์หาความเหมาะสมในการดำเนินธุรกิจของผู้ให้บริการอินเตอร์เน็ตเพื่อใช้เป็นแนวทางในการประกอบธุรกิจ นอกจากนี้สามารถใช้เป็นแนวคิดในการพิจารณาสร้างระบบรักษาความปลอดภัยและการเลือกใช้อุปกรณ์รักษาความปลอดภัยภายในองค์กร เพราะปัจจุบันนี้ข้อมูลซึ่งอยู่ในรูปแบบดิจิตอลมีความสำคัญมากเพราะมีความสะดวกและรวดเร็วแต่ในขณะเดียวกันก็ถูกโจรกรรมและโจมตีได้ง่ายจึงสมควรอย่างยิ่งที่ทุกองค์กรต้องมีระบบรักษาความปลอดภัยที่ดีและเหมาะสมกับองค์กรนั้นๆ

บรรณานุกรม

การสื่อสารแห่งประเทศไทย. 2547. **ศูนย์แลกเปลี่ยนข้อมูลอินเตอร์เน็ตระหว่างประเทศ.** [Online]. เข้าถึงได้จาก: http://www.cat.net.th/thix/iig_thai.html

การสื่อสารแห่งประเทศไทย. 2547. **ศูนย์แลกเปลี่ยนข้อมูลอินเตอร์เน็ตภายในประเทศ.** [Online]. เข้าถึงได้จาก: http://www.cat.net.th/thix/nix_thai.html

จตุชัย แพงจันทร์ และ อนุโชต วุฒิพรพงษ์. 2546. **เจาะระบบเน็ตเวิร์ค.** นนทบุรี: ไอดีซี อินโฟ ดิสทริบิวเตอร์ เซ็นเตอร์.

ฐาปนา ฉิ่นไพศาล และ อัจฉรา ชีวะตระกูลกิจ. 2542. **การบริหารโครงการและการศึกษาความเป็นไปได้.** กรุงเทพฯ: ธีระฟิล์มและไซเท็กซ์.

เรืองไกร รังสิพล. 2544. **เจาะระบบ TCP/IP จุดอ่อนของโปรโตคอลและวิธีป้องกัน.** กรุงเทพฯ: โปรวิชัน.

เรืองไกร รังสิพล. 2545. **เปิดโลก Firewall และ Internet Security.** กรุงเทพฯ: โปรวิชัน.

สาธิต รังคสิริ และ จรัญญา แสงสุขดี. 2545. **ประมวลรัษฎากร 2545.** หมวด 3 ภาษีเงินได้ หน้า 55. กรุงเทพฯ: บางกอกเทรนนิ่งเซ็นเตอร์.

สัลยุทธ์ สว่างวรรณ. 2545. **ระบบสารสนเทศเพื่อการจัดการ.** กรุงเทพฯ: เพียร์สัน เอ็ดดูเคชั่น.

Bace, Rebecca and Mell, Peter. 2001. **Intrusion Detection Systems.** [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-31/sp800-31.pdf

ISO/IEC 17799. 2002. **Information Technology-Code of Practice for Information Security Management**. [Online]. Available: http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=33441&ICS1=35&ICS2=40&ICS3=

Nectec. 2004. **The Internet Index of Thailand.** [Online]. Available: http://iir.ngi.nectec.or.th/internet/map/current.html

Pinya Hom-anek. 2003. **Information Security Management Framework.** [Online]. Available : http://www.acisonline.net/article_prinya_ismf1.htm

Scambray, Joel. 2001. **Hacking Exposed.** Second Edition. Berkeley: McGraw-Hill.

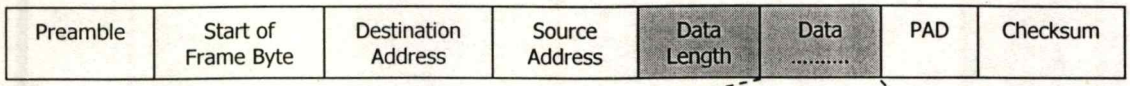
Whitman, M. and Mattord. H. 2002. **Principles of Information Security.** Massachusetts: Thomson Course Technology.

ภาคผนวก

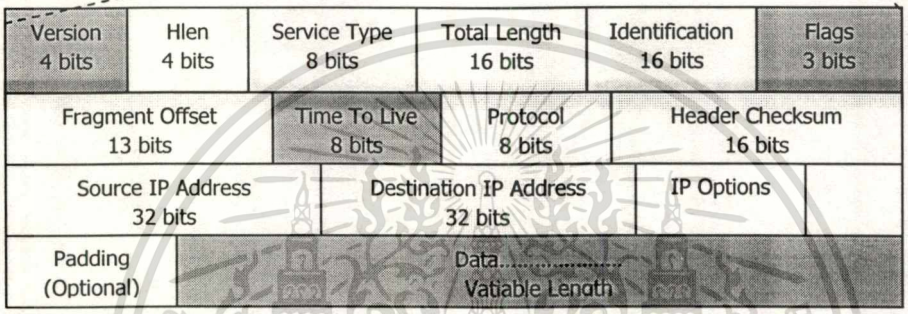
ภาคผนวก ก.

Frame Format IEEE 802.3

CSMA/CD : Layer 2



IP Datagram : Layer 3



รูปที่ ก.1 แสดงแฟรมฟอร์เมตของ IEEE 802.3

ภาคผนวก ข.

ตารางแสดงหมายเลข Port และ Application

ตารางที่ ข.1 แสดง TCP/UDP service ที่ควรปิดกั้นที่ไฟร์วอลล์

Port (Transport)	Server	Port(s) (Transport)	Server
1 (TCP & UDP)	tcpmux	1981 (TCP)	Shockrave
7 (TCP & UDP)	echo	1999 (TCP)	BackDoor
9 (TCP & UDP)	discard	2001 (TCP)	Trojan Cow
11 (TCP & UDP)	systat	2023 (TCP)	Ripper
13 (TCP & UDP)	daytime	2049 (TCP & UDP)	nfs
15 (TCP & UDP)	netstat	2115 (TCP)	Bugs
17 (TCP & UDP)	qotd	2140 (TCP)	Deep Throat
19 (TCP & UDP)	chargen	2222 (TCP)	Subseven21
37 (TCP & UDP)	time	2301 (TCP & UDP)	compaqdiag
43 (TCP & UDP)	whois	2565 (TCP)	Striker
67 (TCP & UDP)	bootps	2583 (TCP)	WinCrash

ตารางที่ ข.1 แสดง TCP/UDP service ที่ควรปิดกั้นที่ไฟร์วอลล์ (ต่อ)

68 (TCP & UDP)	bootpc	2701 (TCP & UDP)	sms-rcinfo
69 (UDP)	tftp	2702 (TCP & UDP)	sms-remctrl
93 (TCP)	supdup	2703 (TCP & UDP)	sms-chat
111 (TCP & UDP)	sunrpc	2704 (TCP & UDP)	sms-xfer
135 (TCP & UDP)	loc-srv	2801 (TCP)	Phineas P.
137 (TCP & UDP)	netbios-ns	4045 (TCP)	lockd
138 (TCP & UDP)	netbios-dgm	5800 - 5899 (TCP)	winvnc web server
139 (TCP & UDP)	netbios-ssn	5900 - 5999 (TCP)	winvnc
177 (TCP & UDP)	xdmcp	6000 - 6063 (TCP)	X11 Window System
445 (TCP & UDP)	microsoft-ds	6665 - 6669 (TCP)	irc
512 (TCP)	rexec	6711 - 6712 (TCP)	Subseven
513 (TCP)	rlogin	6776 (TCP)	Subseven
513 (UDP)	who	7000 (TCP)	Subseven21
514 (TCP)	rsh, rcp, rdist, rdump, rrestore	12345 - 12346 (TCP)	NetBus
515 (TCP)	lpr	16660 (TCP)	Stacheldraht
517 (UCP)	talk	27444 (UCP)	Trinoo
518 (UCP)	ntalk	27666 (TCP)	Trinoo
540 (TCP)	uucp	31335 (UCP)	Trinoo
1024 (TCP)	NetSpy	31337 -31338 (TCP & UDP)	Back Orifice
1045 (TCP)	Rasmin	32700 - 32900 (TCP & UDP)	RPC services
1090 (TCP)	Xtreme	32720 (TCP)	Trinity V3
1170 (TCP)	Psyber S.S	39168 (TCP)	Trinity V3
1234 (TCP)	Ultors Trojan	65000 (TCP)	Stacheldraht
1243 (TCP)	Backdoor-G		
1245 (TCP)	VooDoo Doll		
1349 (UCP)	Back Orifice DLL		
1492 (TCP)	FTP99CMP		
1600 (TCP)	Shivka-Burka		
1761 - 1764 (TCP & UDP)	sms-helpdesk		
1807 (TCP)	SpySender		

ตารางที่ ข.2 แสดง TCP/UDP service ที่ควรปิดกั้นไม่ให้เข้ามาจากภายนอก

Port(s) (Transport)	Server
79 (TCP)	finger
161 (TCP & UDP)	snmp
162 (TCP & UDP)	snmp trap
514 (UDP)	syslog
550 (TCP & UDP)	new who

ตารางที่ ข.3 แสดง TCP/UDP service ที่อาจเปิดให้บริการใน DMZ (ในทางปฏิบัติให้เปิดเฉพาะ service ที่มีการให้บริการจริงเท่านั้น)

Port(s) (Transport)	Server
20 (TCP)	ftpdata
21 (TCP)	ftp
22 (TCP)	ssh
23 (TCP)	telnet
25 (TCP)	smtp
53 (TCP & UDP)	domain
80 (TCP)	http
110 (TCP)	pop3
119 (TCP)	nntp
123 (TCP)	ntp
143 (TCP)	imap
179 (TCP)	bgp
389 (TCP & UDP)	ldap
443 (TCP)	ssl
1080 (TCP)	socks
3128 (TCP)	squid
8000 (TCP)	http (alternate)
8080 (TCP)	http-alt
8888 (TCP)	http (alternate)

ตารางที่ ข.4 แสดง ICMP message ที่ควรอนุญาตให้ออกไปจากเครือข่ายภายในได้

Message Type	
Number	**Name**
4	source quench
8	echo request (ping)
12	parameter problem

ตารางที่ ข.5 แสดง ICMP message ที่ควรอนุญาตให้เข้ามายังเครือข่ายภายในได้

Message Type	
Number	**Name**
0	echo reply
3	destination unreachable
4	source quench
11	time exceeded
12	parameter problem

ประวัติผู้เขียน

นางสาว วราพร พงศ์สุวากร

17 เมษายน พ.ศ. 2519

กรุงเทพมหานคร

กำลังศึกษา วิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ

คณะเทคโนโลยีสารสนเทศ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง