บทที่ 2

กรอบแนวคิดทางทฤษฎีและงานวิจัยที่เกี่ยวข้อง

2.1 กรอบแนวคิดทางทฤษฎี

การศึกษาความเป็นไปได้ในการให้บริการอินเตอร์เน็ตปลอดไวรัสผ่านโครงข่าย Broadband ADSL ของ บมจ.ทีโอที ในครั้งนี้ ได้ใช้กรอบแนวคิดและทฤษฎีที่เกี่ยวข้องกับไวรัสคอมพิวเตอร์ เทคโนโลยีในการป้องกันและกำจัดไวรัสคอมพิวเตอร์ รวมถึงทฤษฎีทางธุรกิจในด้านต่างๆมาได้แก่ การบริหารการตลาด การวางกลยุทธ์ธุรกิจ รวมถึงทฤษฎีเกี่ยวกับการจัดทำแผนธุรกิจ ด้วยการใช้หลักสถิติจากแหล่งข้อมูลทุติยภูมิต่างๆ รวมถึงการศึกษางานวิจัยที่เกี่ยวข้องที่ได้มีการดำเนินการไปแล้ว

2.1.1 ไวรัสคอมพิวเตอร์และเทคโนโลยีในการจัดการกับความปลอดภัยจากไวรัส

2.1.1.1 ไวรัสคอมพิวเตอร์

การใช้งานอินเตอร์เน็ตในปัจจุบัน นับว่าเป็นเรื่องที่ผู้ใช้บริการจะต้องมีความระมัดระวังเพิ่มขึ้นเป็นอย่างมาก เนื่องจากภัยคุกคามในปัจจุบันอาจจะเข้ามาจากช่องทางการสื่อสารผ่านระบบอินเตอร์เน็ตนั่นเอง ที่ปัจจุบันได้มีการพัฒนารูปแบบการการโจมตีที่แปลกใหม่และหลากหลายมากขึ้น อันได้แก่ภัยจากมัลแวร์ (Malware : Malicious Software) ซึ่งเป็นโปรแกรมที่มีประสงค์ร้าย ภัยจากมัลแวร์นี้ส่วนใหญ่ผู้ใช้งานทั่วๆไปอาจจะเรียกและรู้จักกันกว้างๆว่าไวรัสคอมพิวเตอร์นั่นเอง โดยหากเมื่อผู้ใช้งานอินเตอร์เน็ตเปิดอ่านอีเมล์ จากบุคคลที่ไม่รู้จักมาก่อน หรืออาจจะเป็นไฟล์ที่ติดไวรัสที่ส่งมาจากคนที่รู้จักก็ตาม หรือว่าจากการนำใช้โปรแกรมเถื่อนที่มีขายทั่วไปตามท้องตลาดมาใช้งานก็อาจติดไวรัสคอมพิวเตอร์ได้เช่นกัน ทั้งนี้การเข้าเวปไซด์ที่มีการแพร่ของไวรัส ก็สามารถทำให้ผู้ใช้งานอินเตอร์เน็ตถูกไวรัสโจมตีได้อีกเช่นกัน โดยไฟล์ไวรัสที่

พบในปัจจุบันนั้นจะฝังตัวอยู่กับแฟ้มข้อมูลที่ส่วนใหญ่จะเป็นไฟล์นามสกุล[1] .HTA, .PIF, .SCR, .EXE, .COM, .BAT, .CMD, และ .VBS หรือไฟล์ที่แสดงตามตารางที่ 2.1

ตารางที่ 2.1

ไฟล์นามสกุลส่วนใหญ่ที่ต้องสงสัยอาจเป็นไวรัสคอมพิวเตอร์ได้

File Extension	Description	File Extension	Description
ADE	Microsoft Access Project Extension	MDB	Microsoft Access Application
ADP	Microsoft Access Project	MDE	Microsoft Access MDE Database
BAS	Visual Basic® Class Module	MSC	Microsoft Common Console Document
BAT	Batch File	MSI	Windows Installer Package
CHM	Compiled HTML Help File	MSP	Windows Installer Patch
CMD	Windows NT® Command Script	MST	Visual Test Source File
COM	MS-DOS® Application	PCD	Photo CD Image
CPL	Control Panel Extension	PIF	Shortcut to MS-DOS Program
CRT	Security Certificate	REG	Registration Entries
EXE	Application	SCR	Screen Saver
HLP	Windows® Help File	SCT	Windows Script Component
HTA	HTML Applications	SHS	Shell Scrap Object
INF	Setup Information File	URL	Internet Shortcut (Uniform Resource Locator)
INS	Internet Communication Settings	VB	VBScript File
ISP	Internet Communication Settings	VBE	VBScript Encoded Script File
JS	JScript® File	VBS	VBScript Script File
JSE	JScript Encoded Script File	WSC	Windows Script Component
LNK	Shortcut	WSF	Windows Script File
		WSH	Windows Scripting Host Settings File

ที่มา : www.acisonline.net

2.1.1.1.1 ประเภทของไวรัส สำหรับในประเทศไทยคนส่วนใหญ่จะเรียกกว้างๆ รวมกันว่า ไวรัส หรือไวรัสคอมพิวเตอร์นั่นเอง แต่ศัพท์สากลจะเรียกกันว่า มัลแวร์ หมายถึง โปรแกรมประสงค์ร้ายที่สร้างความเสียหายหรือรบกวนให้กับระบบอินเตอร์เน็ตและคอมพิวเตอร์

[1] ปริญญา หอมอเนก, “Dangerous File Extensions”, <www.acisonline.net/article_prinya_eleader_1148.htm>, 2548.

ซึ่งทางศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ประเทศไทย (ThaiCERT:Thai Computer Emergency Response Team) ได้แบ่งประเภทมัลแวร์[2] ได้ดังนี้

1.ไวรัสคอมพิวเตอร์แบบธรรมดา ที่มีลักษณะเป็นโปรแกรมคอมพิวเตอร์ประเภทหนึ่งที่ถูกออกแบบมาให้แพร่กระจายตัวเองจากไฟล์หนึ่งไปยังไฟล์อื่นๆ ภายในเครื่องคอมพิวเตอร์ ไวรัสจะแพร่กระจายตัวเองอย่างรวดเร็วไปยังทุกไฟล์ภายในคอมพิวเตอร์ หรืออาจจะทำให้ไฟล์เอกสารติดเชื้ออย่างช้าๆ แต่ไวรัสจะไม่สามารถแพร่กระจายจากเครื่องหนึ่งไปยังอีกเครื่องหนึ่งได้ด้วยตัวมันเอง โดยทั่วไปเกิดจากการที่ผู้ใช้เป็นพาหะ โดยสามารถเรียกชื่อได้ในลักษณะดังต่อไปนี้

- บูตไวรัส (boot virus) คือ ไวรัสคอมพิวเตอร์ที่แพร่เข้าสู่เป้าหมายในระหว่างเริ่มทำการบูตเครื่อง ส่วนมาก มันจะติดต่อเข้าสู่แผ่นฟลอปปี้ดิสก์ระหว่างกำลังสั่งปิดเครื่อง เมื่อนำแผ่นที่ติดไวรัสนี้ไปใช้กับเครื่องคอมพิวเตอร์เครื่องอื่น ๆ ไวรัสก็จะเข้าสู่เครื่องคอมพิวเตอร์ตอนเริ่มทำงานทันที บูตไวรัสจะติดต่อเข้าไปอยู่ส่วนหัวสุดของฮาร์ดดิสก์ ที่มาสเตอร์บูตเรคคอร์ด (master boot record) และมันจะโหลดตัวเองเข้าไปสู่หน่วยความจำก่อนที่ระบบปฏิบัติการจะเริ่มทำงาน ทำให้เหมือนไม่มีอะไรเกิดขึ้น

- ไฟล์ไวรัส (file virus) ใช้เรียกไวรัสที่ติดไฟล์โปรแกรม

- มาโครไวรัส (macro virus) คือไวรัสที่ติดไฟล์เอกสารชนิดต่าง ๆ ซึ่งมีความสามารถในการใส่คำสั่งมาโครสำหรับทำงานอัตโนมัติในไฟล์เอกสารด้วย ตัวอย่างเอกสารที่สามารถติดไวรัสได้เช่น ไฟล์ไมโครซอฟท์เวิร์ด ไมโครซอฟท์เอ็กเซล เป็นต้น

2. หนอน (Worm) เป็นรูปแบบหนึ่งของไวรัส มีความสามารถในการทำลายระบบในเครื่องคอมพิวเตอร์สูงที่สุดในบรรดาไวรัสทั้งหมด สามารถกระจายตัวได้รวดเร็ว ผ่านทางระบบอินเทอร์เน็ต ซึ่งสาเหตุที่เรียกว่าหนอนนั้น คงจะเป็นลักษณะของการกระจายและทำลาย ที่คล้ายกันหนอนกินผลไม้ ที่สามารถกระจายตัวได้มากมาย รวดเร็ว และเมื่อยิ่งเพิ่มจำนวนมากขึ้นระดับการทำลายล้างยิ่งสูงขึ้น

3. โทรจัน (Trojan) คือโปรแกรมจำพวกหนึ่งที่ถูกออกแบบขึ้นมาเพื่อแอบแฝง กระทำการบางอย่าง ในเครื่องของเรา จากผู้ที่ไม่หวังดี หากเคยดูภาพยนตร์เรื่องทรอย ก็คงจะพอนึกออกเกี่ยวกับโปรแกรมจำพวกนี้ ที่มีตำนานมาจากม้าไม้แห่งเมืองทรอยนั่นเอง ซึ่งการติดนั้น ไม่

---

[2] สัญญา คล่องในวัย, “ทำความรู้จักกับไวรัส หนอน โทรจันและ Hoax”, <http://www.thaicert.nectec.or.th/paper/virus/virus2.php>, 2544.

เหมือนกับไวรัส และหนอน ที่จะกระจายตัวได้ด้วยตัวมันเอง แต่โทรจันจะถูกแนบมากับ อีการ์ด อีเมล์หรือโปรแกรมที่มีให้โหลดตามอินเทอร์เน็ตในเว็บไซต์ใต้ดินทั้งหลาย และสุดท้ายที่มันต่างกับไวรัสและเวิร์ม คือ ผู้ใช้จะเป็นผู้ที่อ้าแขนรับ มันเข้ามาในเครื่องเอง โดยคิดไม่ถึง หรือไม่คาดคิดนั่นเอง

4.ข่าวไวรัสหลอกลวง[3](Hoax) เป็นรูปแบบหนึ่งที่มีผลต่อผู้ใช้คอมพิวเตอร์จำนวนมาก โดยไวรัสหลอกลวงพวกนี้จะมาในรูปของจดหมายอิเล็กทรอนิกส์ การส่งข้อความต่อๆกันไปผ่านทางโปรแกรมรับส่งข้อความ หรือห้องสนทนาต่างๆ ซึ่งสามารถสร้างความวุ่นวายให้เกิดขึ้นได้มากหรือน้อยเพียงใด ก็ขึ้นกับเทคนิค และการใช้จิตวิทยาของผู้สร้างข่าวขึ้นมา โดยส่วนใหญ่ จดหมายประเภทนี้จะมีหัวข้อที่ชวนเชื่อ อ้างแหล่งข้อมูล และบริษัทใหญ่ๆเป็นการสร้างความเชื่อมั่น และเมื่อผู้รับส่งต่อไปยังเพื่อนสนิท และคนคุ้นเคย ก็ยิ่งสร้างความเชื่อมั่นมากขึ้น จากนั้นผู้รับก็จะทำตัวเป็นผู้ส่งต่อๆ ไปอีกหลายๆทอด ซึ่งเป็นลักษณะเด่นของไวรัสหลอกลวง

เมื่อกล่าวถึง hoax ลักษณะของ hoax อีกรูปแบบหนึ่งที่ไม่ใช่ไวรัสคอมพิวเตอร์ แต่จะเป็นอาชญากรรมทางคอมพิวเตอร์รูปแบบหนึ่งที่กำลังเป็นที่พบเห็นได้มากขึ้นเรื่อยๆ ในปัจจุบัน นั่นคือ "Phishing" ซึ่งเป็นการปลอมแปลงอีเมลล์ (E-mail Spoofing) และทำการสร้างเว็บไซต์ปลอมที่มีเนื้อหาเหมือนกับเว็บไซต์ของจริงและมี Address ใกล้เคียงกับเว็บไซต์จริง เพื่อทำการหลอกลวงให้เหยื่อหรือผู้รับอีเมลล์เปิดเผยข้อมูลทางด้านการเงินหรือข้อมูลส่วนบุคคลอื่นๆ อาทิ ข้อมูลของหมายเลขบัตรเครดิต บัญชีผู้ใช้ (Username) และ รหัสผ่าน (Password) หมายเลขบัตรประจำตัวประชาชน หรือข้อมูลส่วนบุคคลอื่นๆ

4. สปายแวร์ [4](Spyware) คือโปรแกรมแฝงที่ส่วนใหญ่จะมาจากการใช้โฆษณา หรือจะเรียกอีกชื่อหนึ่งได้ว่าแอดแวร์ ที่หมายความว่าเป็นโปรแกรมที่อาจเข้ามาติดตั้งในเครื่องคอมพิวเตอร์โดยที่ผู้ใช้ไม่ได้เจตนา โดยผลที่เกิดขึ้นกับเครื่องคอมพิวเตอร์คือ

- อาจส่งหน้าต่างโฆษณาเล็กๆ ปรากฏขึ้นมา(ป๊อบอัพ) ขณะที่ใช้งานเครื่องคอมพิวเตอร์อยู่

---

[3] ศิวรักษ์ ศิวโมกษธรรม, “สาระน่ารู้สู่ความปลอดภัยจากไวรัสคอมพิวเตอร์”, <http://www.thaicert.nectec.or.th/paper/virus/virus_knowledge.php>, 2547.

[4] ดวงกมล ทรัพย์พิทยากร, “สปายแวร์และวิธีการป้องกัน”, <http://www.thaicert.nectec.or.th/paper/spyware>, 2547.

- เมื่อเปิดเว็บบราวเซอร์ เว็บบราวเซอร์จะทำการต่อตรงไปยังเว็บไซต์หลักของตัวสปายแวร์ที่ถูกตั้งค่าให้ลิ้งค์ไป

- สปายแวร์อาจทำการติดตามเว็บไซต์ที่เข้าไปเยี่ยมชมบ่อยๆ

- สปายแวร์บางเวอร์ชั่นที่มีลักษณะรุกรานระบบจะทำการติดตามค้นหา คีย์ หรือรหัสผ่าน ที่พิมพ์ลงไปเมื่อทำการ log in เข้าแอคเคาน์ต่างๆ

ในที่สุดเมื่อสปายแวร์ได้ถูกติดตั้งอยู่ในคอมพิวเตอร์ มันจะพยายาม Run Process ที่จะทำให้เครื่องคอมพิวเตอร์ทำงานช้าลงรวมถึงทำให้การเข้าสู่เว็บไซด์ต่างๆได้ช้าลง หรืออาจส่งผลให้เข้าเว็บไซต์ที่ต้องการไม่ได้เลย และยังส่งผลร้ายกับเรื่องความเป็นส่วนตัวของข้อมูลส่วนบุคคลด้วย (privacy) ดังประเด็นต่อไปนี้

- ไม่ทราบได้เลยว่าข้อมูลที่ถูกนำไปมีอะไรบ้าง

- ไม่ทราบเลยว่าใครเป็นผู้นำข้อมูลเหล่านั้นไป

- ไม่ทราบว่า ข้อมูลเหล่านั้นจะถูกนำไปใช้อย่างไร

2.1.1.1.2 <u>ประวัติของไวรัส</u> การเกิดขึ้นของไวรัสนั้นมีมากว่า 40 ปีแล้ว และจากการบันทึกจุดเริ่มต้นที่สำคัญเกี่ยวกับประวัติ[5] และวิวัฒนาที่สำคัญของไวรัสได้ดังนี้คือในปี

- พ.ศ. 2505 (ค.ศ. 1962) ทีมวิศวกรของ Bell Telephone Laboratories ได้สร้างเกมชื่อว่า "Darwin" ถือเป็นโปรแกรมคอมพิวเตอร์ตัวแรกที่มีรูปแบบของไวรัส โดยฝังตัวอยู่ในหน่วยความจำ เกมนี้ใช้คำศัพท์บางอย่างที่มีคำว่า "supervisor" มีลักษณะที่กำหนดกฎเกณฑ์การต่อสู้ระหว่างผู้เข้าแข่งขัน โปรแกรม Darwin นี้มีความสามารถที่จะวิจัยสภาพแวดล้อมของมัน ทำสำเนา และทำลายตัวเองได้ จุดประสงค์หลักของเกมนี้ก็คือลบโปรแกรมทั้งหมดที่คู่แข่งเขียนและครอบครองสนามรบ

- ต้นปี พ.ศ. 2513 (ค.ศ. 1970) มีการตรวจพบไวรัส Creeper ในเครือข่าย APRANET ของทหารอเมริกา ถือเป็นต้นแบบไวรัสคอมพิวเตอร์ในปัจจุบัน โปรแกรม Creeper สามารถเข้าครอบครองเครือข่ายผ่านโมเด็มและส่งสำเนาตัวเองไปที่ฝั่ง remote ไวรัส นี้ทำให้คนรู้ว่าติดไวรัสด้วยการ broadcast ข้อความ "I'M THE CREEPER ... CATCH ME IF YOU CAN"

- ปี พ.ศ. 2517 (ค.ศ. 1974) โปรแกรมชื่อ "Rabbit" โผล่ขึ้นมาบนเครื่องเมนเฟรมที่เรื่องชื่อนี้เพราะมันไม่ได้ทำอะไรนอกจากสำเนาตัวเองอย่างรวดเร็วไปในระบบเก็บข้อมูลชนิดต่างๆ

---

[5] วิกิพีเดีย สารานุกรมเสรี, “ไวรัสคอมพิวเตอร์”, <http://th.wikipedia.org/wiki>, 2549.

Rabbit นี้ได้ดึงทรัพยากรของระบบมาใช้อย่างมาก ทำให้การทำงานกระทบอย่างรุนแรงจนอาจทำให้ระบบทำงานผิดพลาดได้

- ปี พ.ศ. 2525 (ค.ศ. 1982) มีการตรวจพบไวรัสชื่อ "Elk Cloner" นั้นเป็นคอมพิวเตอร์ไวรัสบนเครื่องคอมพิวเตอร์ส่วนบุคคลตัวแรก ซึ่งแพร่กระจาย คือในวงที่กว้างออกไปกว่าภายในห้องทดลองที่สร้างโปรแกรม โปรแกรมนี้ถูกเขียนขึ้นโดย Rich Skrenta โดยไวรัสนี้จะติดไปกับระบบปฏิบัติการ Apple DOS 3.3 ผ่านทาง boot sector ของฟล็อปปี้ดิสก์ ณ เวลานั้นผลของมันทำให้ผู้ใช้คอมพิวเตอร์บางคนนึกว่าไวรัสคอมพิวเตอร์เกิดจากมนุษย์ต่างดาว เพราะทำให้การแสดงภาพที่จอกลับหัว, ทำตัวอักษรกระพริบ, ขึ้นข้อความต่างๆออกมา

- ปี พ.ศ. 2526 (ค.ศ. 1983) Len Adleman แห่งมหาวิทยาลัย Lehigh ตั้งคำว่า "Virus" ว่าเป็นโปรแกรมคอมพิวเตอร์ที่ทำสำเนาตัวเองได้ และในปีถัดมาใน Information security conference ครั้งที่ 7 Fred Cohen ได้ให้คำจำกัดความของคำ "computer virus" ว่าเป็นโปรแกรมที่สามารถติดต่อไปยังโปรแกรมอื่นโดยการแก้ไขโปรแกรมเดิมเพื่อแพร่ขยายตัวเอง

- เดือนพฤศจิกายน พ.ศ. 2526 (ค.ศ. 1983) Fred Cohen บิดาแห่งไวรัสศาสตร์ (Virology) ได้ใช้คอมพิวเตอร์ VAX 11/750 สาธิตว่าโปรแกรมไวรัสสามารถฝังตัวเข้าไปใน object อื่นได้

- ปี พ.ศ. 2529 (ค.ศ. 1986) ไวรัสตัวคอมพิวเตอร์รุ่นแรกๆ สร้างโดยโปรแกรมเมอร์อายุ 19 ปี ชาวปากีสถาน ชื่อ Basit Farooq และพี่ชายชื่อ Amjad เรียกชื่อ "Brain" ที่มีเป้าไปที่เครื่องคอมพิวเตอร์ IBM Compatible ด้วยเหตุผลที่ว่าต้องการรู้ระดับของซอฟต์แวร์เถื่อนในประเทศตัวเอง แต่โชคไม่ดีที่การทดลองนี้หลุดออกมานอกประเทศ

- ปี พ.ศ. 2529 (ค.ศ. 1986) โปรแกรมเมอร์ชาวเยอรมันชื่อ Ralf Burger พบวิธีตรวจจับโปรแกรมที่ copy ตัวเองโดยการเพิ่ม code บางตัวเข้าไปใน ไฟล์ COM version ที่ใช้ทดลองชื่อ Virdem ถูกนำมาแสดงในเดือนธันวาคม ที่ Hamburg เป็น forum ที่เหล่า hacker ที่ชำนาญในการ crack ระบบ VAX/VMS มารวมตัวกันชื่อ "Chaos Computer Club"

- ปี พ.ศ. 2530 (ค.ศ. 1987) เกิดไวรัสระบาดที่ เวียนนา เป็นไวรัสที่ทำลายคอมพิวเตอร์ส่วนบุคคลตัวแรกที่ทำงานเต็มระบบ ส่งผลกระทบไปเกือบทั่วโลก ที่มาของไวรัสนี้เป็นประเด็นถกเถียงกันมาก เพราะคนที่อ้างว่าเป็นคนเขียนคือ Franz Svoboda แต่เมื่อสืบไปจึงพบว่าเขารับมาจาก Ralf Burger ซึ่งก็อ้างว่ารับมาจาก Svoboda เดิมชื่อไวรัสคือ "lovechild" แต่เพราะไม่สามารถหาคนให้กำเนิดได้จึงถูกเรียกอย่างเป็นทางการว่า "orphan" (ลูกกำพร้า)

- ปี พ.ศ. 2530 (ค.ศ. 1987) เดือนธันวาคม เกิดการระบาดใต้ดินครั้งแรกในเครือข่ายคอมพิวเตอร์ ชื่อ "Christmas Three" วันที่ 9 ไวรัสหลุดมาจาก เครือข่าย Bitnet ของมหาวิทยาลัย Western University ประเทศเยอรมนี ทะลุเขาไปใน European Acadamic Research Network (EARN) และเข้าไป เครือข่าย IBM-Vnet เป็นเวลา 4 วัน เครื่องที่ติดไวรัสจะแสดงผลที่หน้าจอเป็นรูปต้นคริสมาสต์ และส่งไปให้ผู้ใช้อื่นๆในเครือข่าย

- ปี พ.ศ. 2531 (ค.ศ. 1988) Peter Norton programmer ที่มีชื่อเสียง ผู้ซึ่งเป็นผู้ก่อตั้งบริษัท Symantec ได้ออกมาประกาศว่าไวรัสคอมพิวเตอร์เป็นเรื่องไร้สาระ โดยเปรียบว่าเป็นแค่จระเข้ที่อยู่ในท่อระบายน้ำเสียในนิวยอร์ก แต่ในที่สุดเขาเป็นผู้ที่ได้เริ่มต้น project Norton AntiVirus

- ปี พ.ศ. 2531 (ค.ศ. 1988) วันที่ 22 เดือนเมษายน เกิด forum ที่ถกกันเรื่อง security threat เป็นครั้งแรก ชื่อ Virus-L host ไว้ที่ Usebet สร้างโดย Ken Van Wyk เพื่อร่วมงานของ Fred Cohen ที่มหาวิทยาลัย Lehigh

- ปี พ.ศ. 2531 (ค.ศ. 1988) เดือนตุลาคม มีการแพร่ข่าวไวรัสชื่อ Mr. "Rochenle" อย่างมากเป็นไวรัสประเภทหลอกลวง (HOAX) เป็นตัวแรก อ้างถึงชื่อบุคคลที่ไม่มีตัวตนชื่อ Mike RoChenle ("Microchannel") อ้างว่าไวรัสนี้สามารถส่งตัวเองไประหว่างโมเด็มด้วยความเร็ว 2400 bps ทำให้ความเร็วโมเด็มลดลงเหลือ 1200 bps และได้อธิบายวิธีการแก้ไขที่ไม่ได้มีผลอะไร แต่มีคนหลงเชื่อทำตามกันอย่างมากมาย

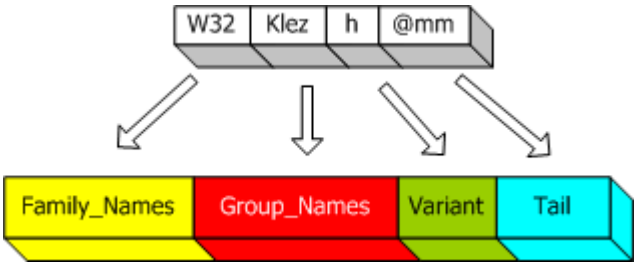
- ปี พ.ศ. 2531 (ค.ศ. 1988) เดือนพฤศจิกายน มีหนอนเครือข่ายชื่อ "Morris" ระบาดอย่างหนักทำให้คอมพิวเตอร์กว่า 6000 เครื่องในอเมริการวมทั้งใน ศูนย์วิจัยของ NASA ติดไปด้วย ส่งผลกระทบให้การปฏิบัติงานหยุดโดยสิ้นเชิง เหตุเนื่องจากมี error ใน code ของ Morris ทำให้มัน copy ตัวเองไปที่เครือข่ายอื่นอย่างไม่จำกัดทำให้เครือข่ายรับไม่ไหว การระบาดครั้งทำทำให้สูญเสียเป็นมูลค่ากว่า 96 ล้านเหรียญสหรัฐ

ในปัจจุบันจากความก้าวหน้าของเทคโนโลยีและการเรียนรู้ใหม่ๆทางด้านโปรแกรมก็ได้ทำให้เกิดไวรัสสายพันธุ์ใหม่ๆเกิดขึ้นแทบทุกวัน และสามารถขยายตัวผ่านระบบอินเตอร์เน็ตมากขึ้น อีกทั้งยังมีความสามารถที่จะสร้างความเสียหายให้กับระบบคอมพิวเตอร์มากขึ้นด้วย โดยพบว่าจนถึงสิ้นปี 2544 ได้เกิดไวรัสขึ้นมามากกว่า 46,000 ชนิดแล้ว ในปัจจุบันจะพบว่ามีอัตราการเกิดใหม่ของไวรัสเฉลี่ยวันละ 2 ถึง 3 ตัว

2.1.1.1.3 การเรียกชื่อของไวรัส ชื่อของไวรัส[6] ที่เห็นทั่วไปนั้นมีความหมายว่าแตกต่างกันไป ทั้งๆ ที่ไวรัสที่ค้นพบนั้นเป็นตัวเดียวกัน อย่างไรก็ตามแม้ว่าชื่อจะเขียนไม่เหมือนกันทุกตัวอักษร แต่ความหมายที่แปลได้จากชื่อนั้นเหมือนกัน ตัวอย่างเช่น W32.Klez.h@mm W32/Klez.h@MM WORM_KLEZ.H I-Worm.Klez.h เป็นต้น โดยจะอธิบายถึงส่วนต่างๆ ของชื่อไวรัส เพื่อทำให้สามารถจำแนกแยกแยะประเภทของไวรัสจากชื่อของไวรัส ความสามารถเด่นๆ ตลอดจนวิธีการแพร่กระจายตัวของไวรัส โดยมีส่วนประกอบของชื่อไวรัสนั้นแบ่งได้เป็นส่วนๆ ดังนี้

ภาพที่ 2.1

ส่วนประกอบของชื่อไวรัส



ที่มา : www.thaicert.nectec.or.th

ชื่อตระกูลของไวรัส (Family Names) จะแสดงเป็นส่วนแรก ชื่อส่วนใหญ่จะตั้งตามชนิดของปัญหาที่ไวรัสก่อขึ้น หรือภาษาที่ใช้ในการพัฒนา เช่น เป็นม้าโทรจัน ถูกพัฒนาด้วย Visual Basic scripts หรือเป็นไวรัสที่รันบนระบบปฏิบัติการวินโดวส์ 32 บิต เป็นต้น ซึ่งชื่อของตระกูลของไวรัสที่ค้นพบในปัจจุบัน ดังตารางที่ 2.2

[6] กิติศักดิ์ จิรวรรณกูล และมนัชยา ชมธวัช , “ชื่อไวรัสบอกอะไรได้บ้าง”, <http://www.thaicert.nectec.or.th/paper/virus/virusname.php>, 2546.

ตารางที่ 2.2

รายชื่อตระกูลของไวรัส

Family Names	ความหมาย
WM	ไวรัสที่เป็นมาโครของโปรแกรม Word
W97M	ไวรัสที่เป็นมาโครของโปรแกรม Word 97
XM	ไวรัสที่เป็นมาโครของโปรแกรม Excel
X97M	ไวรัสที่เป็นมาโครของโปรแกรม Excel 97
W95	ไวรัสที่มีผลกระทบกับระบบปฏิบัติการวินโดวส์ 95
W32/Win32	ไวรัสที่มีผลกระทบกับระบบปฏิบัติการวินโดวส์ 32 บิต
WNT	ไวรัสที่มีผลกระทบกับระบบปฏิบัติการวินโดวส์ NT 32 บิต
I-Worm/Worm	หนอนอินเทอร์เน็ต
Trojan/Troj	ม้าโทรจัน
VBS	ไวรัสที่ถูกพัฒนาด้วย Visual Basic Script
AOL	ม้าโทรจัน America Online
PWSTEAL	ม้าโทรจันที่มีความสามารถในการขโมยรหัสผ่าน
Java	ไวรัสที่ถูกพัฒนาด้วยภาษาจาวา
Linux	ไวรัสที่มีผลกระทบกับระบบปฏิบัติการลินุกซ์
Palm	ไวรัสที่มีผลกระทบกับระบบปฏิบัติการ Palm OS
Backdoor	เปิดช่องให้ผู้บุกรุกเข้าถึงเครื่องได้
HILLW	บ่งบอกว่าไวรัสถูกคอมไพล์ด้วยภาษาระดับสูง

ที่มา : www.thaicert.nectec.or.th

1. <u>ชื่อของไวรัส (Group Name)</u> เป็นชื่อดั้งเดิมที่ผู้เขียนไวรัสเป็นคนตั้ง โดยปกติจะถูกแทรกไว้อยู่ในโค้ดของไวรัส และในส่วนนี้เองจะเอามาเรียกชื่อไวรัสเปรียบเสมือนเรียกชื่อเล่น ตัวอย่างเช่นชื่อของไวรัสคือ W32.Klez.h@mm และจะถูกเรียกว่า Klez.h เพื่อให้สั้นและกระชับขึ้น

2. <u>ส่วนของรายละเอียด (Variant)</u> ส่วนนี้จะบอกว่าสายพันธุ์ของไวรัสชนิดนั้นๆ มีการปรับปรุงสายพันธุ์จนมีความสามารถต่างจากสายพันธุ์เดิมที่มีอยู่ variant มี 2 ลักษณะคือ

- Major Variants จะตามหลังส่วนชื่อของไวรัส เพื่อบ่งบอกว่ามีความแตกต่างกันอย่างชัดเจน เช่นหนอนชื่อ VBS.LoveLetter.A (A เป็น Major Variant) แตกต่างจาก VBS.LoveLetter อย่างชัดเจน

- Minor Variants ใช้บ่งบอกในกรณีที่แตกต่างกันนิดหน่อย ในบางครั้ง Minor Variant เป็นตัวเลขที่บอกขนาดไฟล์ของไวรัส ตัวอย่างเช่น W32.Funlove.4099 หนอนชนิดนี้มีขนาด 4,099 KB

3. <u>ส่วนท้าย (Tail)</u> เป็นส่วนที่จะบอกว่าวิธีการแพร่กระจาย ประกอบด้วย

- @M หรือ @m บอกให้รู้ว่าไวรัสหรือหนอนชนิดนี้เป็น "Mailer" ที่จะส่งตัวเองผ่านทางอี-เมล์เมื่อผู้ใช้ส่งอี-เมล์เท่านั้น

- @MM หรือ @mm บอกให้รู้ว่าไวรัสหรือหนอนชนิดนี้เป็น "Mass Mailer" ที่จะส่งตัวเองผ่านทุกอีเมลล์แอดเดรสที่อยู่ในเมล์บอกซ์

<u>ตัวอย่าง</u> W32.HILLW.Lovgate.C@mm แสดงได้ว่า

1. Family Names อยู่ในตระกูลที่มีผลต่อระบบปฏิบัติการวินโดวส์ 32 บิต และถูกคอมไพล์ด้วยภาษาระดับสูง
2. Group Name ชื่อของไวรัสคือ Lovgate
3. ที่มี variant คือ C
4. มีความสามารถในการแพร่กระจายผ่านทางอี-เมล์โดยส่งไปยังทุกอีเมลล์แอดเดรสที่อยู่ในเมล์บอกซ์

จากส่วนประกอบของชื่อไวรัสที่ได้อธิบายไว้ข้างต้น จะเห็นได้ว่าชื่อของไวรัสนั้นสามารถบอกถึงประเภทของไวรัส ชื่อดั้งเดิมของไวรัสที่ผู้เขียนไวรัสเป็นคนตั้ง สายพันธุ์ต่างๆ ของไวรัสที่ถูกพัฒนาต่อไป และวิธีการแพร่กระจายตัวของไวรัสเองด้วย

2.1.1.1.4 <u>การโจมตีของไวรัส</u> จากการศึกษาทางเทคนิคพบว่าเส้นทาง[7] ในการโจมตีระบบของไวรัส หรือมัลแวร์นั้นมีอยู่ทั้งหมด 6 เส้นทาง ได้แก่

1. การโจมตีผ่านทางจดหมายอิเล็กทรอนิกส์ (Email Attack)

การโจมตีผ่านทางอีเมลล์นั้น เป็นวิธีการโจมตีที่มัลแวร์นิยมใช้มากที่สุด เนื่องจากทุกวันนี้ผู้ใช้คอมพิวเตอร์ทุกคนต้องอ่านอีเมลล์เป็นประจำ โอกาสที่ผู้ใช้จะเปิด Email ที่ไม่หวังดีจึงมีความเป็นไปได้สูง การโจมตีมักจะมาในรูปแบบของไฟล์แนบ (Attached File) หรือ มาในรูปของ Hyperlink หลอกให้ผู้ใช้คลิ๊กเพื่อไปดาวน์โหลดมัลแวร์ลงมาในเครื่องคอมพิวเตอร์โดยปกติแล้วไฟล์แนบดังกล่าวจะใช้นามสกุลที่เราไม่ค่อยคุ้น เช่น *.VBS, *.HTA, *.CMD, *.PIF และมักจะมาในรูป executable file เช่น *.EXE หรือ .*.COM หากเราพบไฟล์แนบนามสกุลดังกล่าว ให้สงสัยว่าเป็นมัลแวร์ไว้ก่อน เพราะคนปกติส่วนใหญ่จะไม่ส่งไฟล์แนบโดยใช้นามสกุลไฟล์ดังกล่าว ในปัจจุบันผู้สร้างมัลแวร์หันมานิยมใช้ไฟล์แนบนามสกุล *.ZIP ที่เรานิยมใช้กันทั่วไป ทำให้ผู้ใช้งานโดยหลอกง่ายขึ้นโดยการแต่งข้อความใน Email ให้ดูน่าเชื่อถือ วิธีการนี้เรียกว่า Social Engineering เพื่อหลอกผู้อ่าน Email ให้ตายใจนึกว่าเป็น Email จากคนรู้จักก็มักจะเปิดโดยไม่ระวังทำให้ถูกมัลแวร์โจมตี ได้อย่างง่ายดาย

2. การโจมตีผ่านทางการดาวน์โหลดไฟล์หรือจากการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม (Web Attack)

มัลแวร์สามารถถูกดาวน์โหลดโดยอัตโนมัติจากการที่เราใช้ IE หรือ Firefox Browser เข้าสู่เว็บไซต์ที่ไม่เหมาะสม โดยเว็บไซต์ดังกล่าวมักจะมีการตกลงธุรกิจร่วมกันกับผู้ผลิตมัลแวร์เรียกว่ามีผลประโยชน์ร่วมกันอยู่ ทำให้มัลแวร์สามารถถูกดาวน์โหลดโดยที่เราเองยังไม่ได้สั่งดาวน์โหลดเลยด้วยซ้ำ (ในกรณีที่ Browser มีช่องโหว่) หรือ บางครั้งเราเองก็เผลอดาวน์โหลดไฟล์มัลแวร์โดยไม่ทราบว่าโปรแกรมดังกล่าวนั้นเป็นมัลแวร์ บางทีก็หลอกมาว่าเป็น โปรแกรมที่มีอรรถประโยชน์ (Utility Program) ในกรณีนี้จะเรียกโปรแกรมเหล่านี้ว่า "ม้าโทรจัน" (Trojan Horse) ซึ่งดูเหมือนจะเป็นโปรแกรมที่ดีแต่จริง ๆ แล้วเป็นโปรแกรมมัลแวร์ที่ไม่ประสงค์ดี

3. การโจมตีผ่านทาง เครือข่ายโปรแกรมประเภท Instant Messaging (IM attack)

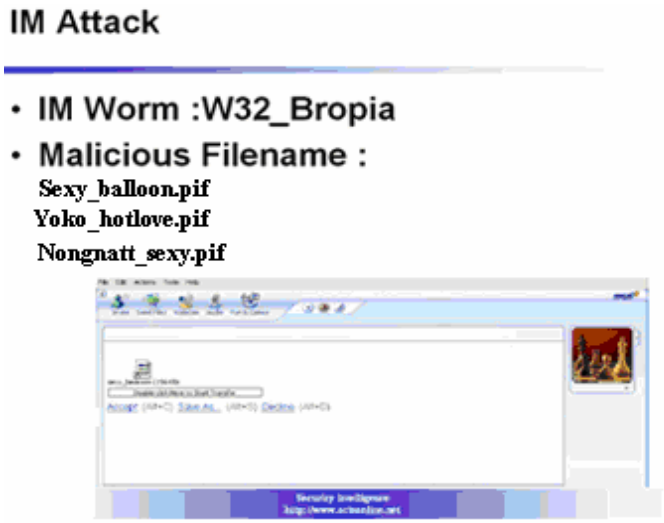
ปัจจุบันผู้ใช้คอมพิวเตอร์ทั่วไปนิยมใช้โปรแกรม IM (Instant Messaging) เช่น MSN หรือ Yahoo Messaging ในการติดต่อ "chat" ที่ได้รับความนิยมกันมาก โปรแกรมประเภท IM ทำให้ผู้ไม่หวังดี

---

[7] ปริญญา หอมอเนก, “เส้นทางในการโจมตีระบบของมัลแวร์”, <http://www.acisonline.net/article_prinya_eweek_011249.htm>, 2549.

เห็นช่องทางใหม่ในการโจมตีคอมพิวเตอร์และระบบเครือข่ายผ่านทางผู้ใช้ IM ที่ไม่ทราบถึงภัยจากมัลแวร์ผ่านทาง IM เช่น ผู้ผลิตมัลแวร์ หรือไวรัสคอมพิวเตอร์ทำออกแบบโปรแกรมไวรัสโดยตั้งชื่อไฟล์ให้ดูน่าสนใจ เช่น Sexy_Balloon.pif หรือ Nongnatt_sexy.pif เพื่อหลอกให้ผู้ใช้ IM เช่น MSN ที่มักจะอยากรู้อยากเห็นไฟล์ชื่อที่น่าสนใจนั้นและคิดว่าเพื่อนส่งมาให้ จึงเผลอเปิดไฟล์โดยไม่รู้ตัว โดยไฟล์ดังกล่าวคือ ไวรัสที่ทำงานในลักษณะหนอนอินเตอร์เน็ตที่มีชื่อว่า "Bropia Worm" ดังตัวอย่างเช่นภาพที่ 2.2

ภาพที่ 2.2
การส่งไฟล์ไวรัสที่ชื่อ Sexy_Balloon.pif ซึ่งชื่อทำให้ดูน่าสนใจ
แต่เป็นโปรแกรมหนอนอินเตอร์เน็ตผ่านทางโปรแกรม IM หรือ Yahoo Messaging



ที่มา : www.acisonline.net

เมื่อผู้ใช้เปิดไฟล์ดังกล่าวจะมีผลกระทบต่อระบบเครือข่ายภายในขององค์กร และเครื่องคอมพิวเตอร์ที่ตกเป็นเหยื่อตลอดจน โปรแกรมหนอน Bropia จะส่งไฟล์ไวรัสกระจายไปยังผู้ใช้ MSN ที่อยู่ใน Contact List ทุกคน ปัญหาของการใช้โปรแกรม IM อย่างไม่ระมัดระวังก็คือโปรแกรมหนอนดังกล่าวสามารถทำให้ระบบเครือข่ายใช้งานไม่ได้ หรือทำให้เกิดข้อมูลจราจรมาหาศาลซึ่งมีผลถึงจุดที่ทำให้ระบบล่มได้ในไม่กี่นาที

4. การโจมตีผ่านทางเครือข่ายโปรแกรมประเภท P2P (Peer-To-Peer) (P2P Attack)

การใช้เทคโนโลยีอินเตอร์เน็ต Broadband ADSL ทำให้แบนด์วิธ (Bandwidth) ในการใช้งานเพิ่มมากขึ้นหลายเท่าตัวจากระบบโมเด็ม 56K เดิมมาเป็นระบบ ADSL ที่มีการเชื่อมต่ออินเตอร์เน็ตในลักษณะ "Always On" ได้ตลอด 24 ชั่วโมง ทำให้การดาวน์โหลดข้อมูลและโปรแกรมต่าง ๆ ในอินเทอร์เน็ตมีความรวดเร็วมากขึ้นจากพฤติกรรมการใช้งานอินเตอร์เน็ตที่เปลี่ยนไปดังกล่าวทำให้ผู้ไม่หวังดีเช่น บรรดาเหล่าแฮ็คเกอร์ "Black Hat" ได้อาศัยช่องโหว่ของเครื่องคอมพิวเตอร์ผู้ใช้งานอินเตอร์เน็ตบรอดแบนด์โดยเฉพาะผู้ใช้งานอินเตอร์เน็ตตามบ้าน เข้ามาโจมตีและยึดเครื่องคอมพิวเตอร์เหล่านั้น เพื่อประโยชน์ของแฮ็คเกอร์ โดยเราเรียกกลุ่มเครื่องที่ตกเป็นเหยื่อว่า "Botnet" หรือ "Robot Network" ที่แฮ็คเกอร์สามารถควบคุมได้ แต่ถ้าหากผู้ใช้ตามบ้านติดตั้งโปรแกรม Personal Firewall ก็สามารถป้องกันการโจมตีแบบ Remote Exploint ดังกล่าวได้ แฮ็คเกอร์จึงเปลี่ยนวิธีในการโจมตีโดยการสร้างโปรแกรมประเภท P2P ขึ้นมาเพื่อให้ผู้ใช้สามารถดาวน์โหลดข้อมูลระหว่างผู้ใช้อินเตอร์เน็ตด้วยกันได้ง่ายยิ่งขึ้น ขณะเดียวกันก็แอบแฝงติดตั้งโปรแกรมมัลแวร์นำพวกสปายแวร์เข้ามาด้วย โปรแกรม P2P หลายโปรแกรมมาพร้อมกับสปายแวร์ในตัว ขณะเดียวกันก็สร้างไฟล์โดยตั้งชื่อไฟล์หลอกผู้ใช้ให้ดาวน์โหลดไฟล์โดยคิดว่าเป็นไฟล์ที่ผู้ใช้ต้องการ แต่แท้จริงแล้วเป็นโปรแกรมมุ่งร้ายหรือมัลแวร์ในลักษณะของม้าโทรจัน (Trojan Horse) หลังจากผู้ใช้ดาวน์โหลดและติดตั้งโปรแกรมดังกล่าวผู้ใช้อาจถูกขโมยข้อมูลส่วนตัวเช่น ชื่อผู้ใช้และรหัสผ่านโดยโปรแกรมประเภท "Key Logger" จะคอยดักข้อมูลผู้ใช้โดยไม่รู้ตัวจากนั้นแฮ็คเกอร์ก็สามารถนำชื่อและรหัสผ่าน ไปใช้งานแทนตัวผู้ใช้โดยที่ผู้ใช้กว่าจะรู้ตัวก็เกิดความเสียหายไปเรียบร้อยแล้ว เช่น ถูกขโมยเงินจากการใช้งานบริการธนาคารทางอินเตอร์เน็ตได้

ภัยจากโปรแกรม P2P นอกจากจะทำให้เราติดไวรัสหรือมัลแวร์ได้ง่าย และ ขโมยข้อมูลส่วนตัวของเราแล้ว ยังมีภัยอีกรูปแบบหนึ่งที่ถือได้ว่า เป็นภัยระดับองค์กร ได้แก่ ภัยมืดจากการใช้แบนด์วิธจำนวนมากของโปรแกรม P2P ขณะที่ผู้ใช้ดาวน์โหลดข้อมูลระหว่างโปรแกรม P2P ด้วยกันจะทำให้มีการใช้งานแบนด์วิธของเครือข่ายที่เชื่อมต่อกับระบบอินเตอร์เน็ตซึ่งมีปริมาณข้อมูลจราจรจำนวนมาก ทำให้เกิดความล่าช้าต่อผู้ใช้บริการอินเตอร์เน็ตในองค์กรคนอื่น ๆ ไม่สามารถใช้งานอินเตอร์เน็ตได้ตามปกติ ในบางรายโปรแกรม ANTI-VIRUS ทำงานผิดพลาดเพราะไม่สามารถอัพเดต VIRUS Signature ได้เพราะแบนด์วิธไม่เพียงพอในการดาวน์โหลด จะเห็นได้ว่าการใช้งานโปรแกรม P2P ทั้งโดยที่ตั้งใจและไม่ตั้งใจของผู้ใช้อินเตอร์เน็ตนั้น ก่อให้เกิดภัยมืดกับตนเองหรือกับองค์กรได้โดยไม่รู้ตัว

5. การโจมตีผ่านทางเครือข่ายในขณะที่เครื่องออนไลน์ (Network Attack)

การที่เปิดเครื่องคอมพิวเตอร์และต่อออนไลน์กับระบบอินเตอร์เน็ตแล้ว ถึงจะยังไม่ได้ใช้โปรแกรม email หรือ Internet Browser ตลอดจนโปรแกรม IM หรือ P2P ก็ตาม ก็มีโอกาสถูกโจมตีได้ภายในไม่กี่นาที เคยมีงานวิจัยเรื่องภัยอินเตอร์เน็ตได้สรุปว่า แค่เพียงเราต่อเชื่อมกับระบบอินเตอร์เน็ตโดยไม่ได้มีการป้องกันเครื่องคอมพิวเตอร์โดยใช้โปรแกรมประเภท Personal Firewall เครื่องคอมพิวเตอร์อาจถูกโจมตีโดยไวรัส, วอร์ม หรือ แฮ็คเกอร์ภายในเวลาที่ต่ำสุดไม่ถึง 5 นาที สาเหตุมาจากเครื่องคอมพิวเตอร์ที่ถูกโจมตีนั้นไม่ได้ติดตั้ง Service Pack หรือ Hotfix ที่มีความจำเป็น (Critical Patch/Hofix) และไม่ได้เปิดใช้งาน Personal Firewall ทำให้ตกเป็นเหยื่อการโจมตีได้ง่าย

6. การโจมตีที่ไม่ได้ผ่านทางระบบเครือข่าย (Physical Security Attack)

ผู้ใช้คอมพิวเตอร์อาจติดไวรัส หรือตกเป็นเหยื่อมัลแวร์ได้จากการโจมตีทางกายภาพ (Physical Security Attack) ทั้งตั้งใจและไม่ได้ตั้งใจ ได้แก่ การที่ผู้ใช้คอมพิวเตอร์เปิดเครื่องคอมพิวเตอร์ทิ้งไว้ไม่ได้ "Lock" หน้าจอไว้ทำให้ผู้ไม่หวังดีสามารถนำโปรแกรมมัลแวร์ประเภท "Key Logger" แอบเข้ามาติดตั้งดักจับข้อมูลส่วนตัว ละเมิด "Privacy" ก็คือการขโมยความเป็นตัวตนของเราจากโปรแกรมสปายแวร์ได้อย่างง่ายดาย หรืออาจเกิดจากผู้ใช้คอมพิวเตอร์นำโปรแกรมที่อยู่ใน CD หรือ DVD มาใช้งานโดยไม่ได้ตั้งใจแต่โปรแกรมเหล่านั้นติดไวรัส หรือเป็นมัลแวร์ที่อาจแฝงมาในรูปของโปรแกรมอรรถประโยชน์ (Ultility) ที่เป็นโปรแกรมไม่ถูกลิขสิทธิ์ ก็ทำให้ตกเป็นเหยื่อของมัลแวร์ ได้เช่นกัน

2.1.1.1.5 <u>อาการของเครื่องที่ติดไวรัส</u>

- ใช้เวลานานผิดปกติในการเรียกโปรแกรมขึ้นมาทำงาน
- ขนาดของโปรแกรมใหญ่ขึ้น (เพิ่มจากปกติอย่างผิดสังเกต)
- วันเวลาของโปรแกรมหรือไฟล์ข้อมูลเปลี่ยนไป(โดยไม่ได้มีการแก้ไขหรือใช้งาน)
- ขนาดของหน่วยความจำที่เหลือลดน้อยลงกว่าปกติ โดยไม่ทราบสาเหตุ
- ไฟแสดงสถานการณ์ทำงานของฮาร์ดดิสก์ติดค้างนานกว่าที่เคยเป็น(แม้จะไม่เรียกโปรแกรมทำงานก็กระพริบตลอด)
- แป้นพิมพ์หรือเม้าท์ทำงานผิดปกติหรือไม่ทำงานเลย
- เครื่องทำงานช้าลงหรือหยุดทำงานโดยไม่ทราบสาเหตุ รวมทั้งเกิดการรีบูตตัวเองโดยไม่ได้สั่ง

- เซกเตอร์ที่เสียมีจำนวนเพิ่มขึ้น โดยมีการรายงานว่ามีจำนวนเซกเตอร์ที่เสียเพิ่มขึ้นทั้งๆ ที่ยังไม่ได้ใช้โปรแกรมใดๆ เข้าไปตรวจหาเลย

- ไฟล์ข้อมูลหรือโปรแกรมที่เคยใช้อยู่ๆ ก็หายไป

2.1.1.2 เทคนิคในการป้องกันและกำจัดไวรัสคอมพิวเตอร์

ในการป้องกันและกำจัดไวรัสคอมพิวเตอร์สามารถแบ่งรูปแบบของเทคนิคในการทำงานได้เป็น 3 ลักษณะดังนี้คือ

2.1.1.2.1 การป้องกันและกำจัดไวรัสคอมพิวเตอร์ด้วยโปรแกรมคอมพิวเตอร์

โปรแกรมป้องกันไวรัสและกำจัดไวรัสคอมพิวเตอร์เป็นปัจจัยที่สำคัญมากที่จะช่วยให้เครื่องคอมพิวเตอร์ปลอดภัยจากการคุกคามของไวรัสคอมพิวเตอร์ ซึ่งปัจจุบันโปรแกรมนั้นป้องกันไวรัสก็มีมากขึ้น ซึ่งเทคนิคในการตรวจจับไวรัส[8] ได้ถูกพัฒนาขึ้น เพื่อตรวจจับไวรัสแตกต่างกันออกไป ซึ่งเทคนิคในการตรวจจับไวรัสโดยทั่วไป แบ่งได้ 4 เทคนิคคือ

1. การตรวจหา (Scanning) เป็นเทคนิคที่ใช้ตัวตรวจหา (Scanner) เข้าไปค้นหาไฟล์ที่ถูกบ่งบอกว่าถูกไวรัสแฝงตัวอยู่ ในหน่วยความจำ ส่วนเริ่มต้นในการบูต (Boot sector) และไฟล์ที่ถูกเก็บอยู่ในฮาร์ดดิสก์ โดยใช้หลักการ Checksum ซึ่งมีวิธีการทำงานคือ ในไฟล์ทุกไฟล์จะมีส่วนที่เก็บข้อมูลว่ามีจุดเริ่มต้น จุดสิ้นสุดของไฟล์ที่ตำแหน่งใด ตามด้วยข้อมูลของไฟล์และปิดท้ายด้วยค่า Checksum ตัวตรวจหาจะคำนวณหาค่า Checksum ของแต่ละไฟล์แล้วนำไปทำการเปรียบเทียบกับค่า Checksum ของไฟล์นั้นๆ ดังนั้นถ้าไฟล์ใดถูกไวรัสแฝงตัวก็จะทำให้ค่า Checksum ที่คำนวณได้จะไม่เท่ากับค่า Checksum ที่เป็นข้อมูลของไฟล์ดังกล่าว โปรแกรมป้องกันไวรัสทั่วๆไป โดยจะมีวิธีการตรวจหา 2 ชนิดคือ

- การตรวจหาชนิด On - access เป็นวิธีการตรวจหาไฟล์ก่อนที่จะถูกโหลดเข้าหน่วยความจำ เพื่อทำการเอ็กซิคิวต์

---

[8] กิติศักดิ์ จิรวรรณกูล, “โปรแกรมป้องกันไวรัสทำงานกันอย่างไร”, <http://www.thaicert.org/paper/virus/antivirus1.php>, 2546.

- การตรวจหาชนิด On - demand เป็นวิธีการตรวจหาในหน่วยความจำหลัก ส่วนเริ่มต้นในการบูต และฮาร์ดดิสก์ ผู้ใช้งานยังสามารถเรียกใช้งานวิธีการตรวจหาชนิดนี้ตามความต้องการได้

ข้อดีของเทคนิคนี้คือตัวตรวจหาสามารถพบไวรัสก่อนที่จะทำการเอ็กซิคิวต์

2. <u>การตรวจสอบความคงอยู่ (Integrity Checking)</u> เทคนิคนี้อาศัยตัวตรวจสอบความคงอยู่ (Integrity Checker) ที่เก็บข้อมูลความคงอยู่ (Integrity Information) ของไฟล์สำคัญไว้สำหรับเปรียบเทียบ ตัวอย่างข้อมูลเช่น ขนาดไฟล์ เวลาแก้ไขครั้งล่าสุด และค่า Checksum เป็นต้น ส่วนมากจะใช้ค่าของ Checksum ในการเปรียบเทียบ เมื่อมีไฟล์เปลี่ยนแปลงที่มีสาเหตุอันเนื่องจากไวรัสหรือความผิดพลาดใดๆ จนทำให้ข้อมูลความคงอยู่ต่างจากข้อมูลเดิมที่เคยเก็บไว้ ระบบก็จะแจ้งให้ผู้ใช้งานทราบถึงความผิดปกติและยังสามารถมีทางเลือกให้ผู้ใช้สามารถกู้ไฟล์ข้อมูลดังกล่าวคืนไปเป็นไฟล์ก่อนที่จะติดไวรัสได้

ข้อดีของเทคนิคนี้คือ เป็นเทคนิคเดียวที่จะตรวจสอบว่ามีไวรัสทำลายไฟล์หรือไม่ และเกิดความผิดพลาดน้อย ตัวตรวจสอบความคงอยู่ในปัจจุบันมีความสามารถที่จะตรวจจับการทำลายข้อมูลชนิดต่างๆ ได้ เช่นไฟล์ไม่สมบูรณ์ (Corruption) และยังสามารถกู้ไฟล์คืนได้

3. <u>การตรวจจับไวรัสโดยใช้การวิเคราะห์พฤติกรรม (Heuristic)</u> เป็นเทคนิคทั่วไปที่นิยมใช้ในการตรวจจับไวรัส โดยจะเปรียบเทียบการทำงานของไวรัสกับกฎ Heuristic (Rules Based System) และชุดกฎ Heuristic ถูกพัฒนาให้สามารถแยกแยะพฤติกรรมการทำงานว่าเป็นการทำงานของไวรัสหรือไม่ มีการเก็บข้อมูลของไวรัสที่รู้จักเพื่อใช้ในการจับคู่แพตเทิร์น และชุดกฎนี้ถูกพัฒนาโดยผู้พัฒนาโปรแกรมป้องกันไวรัส ยกตัวอย่างวิธีการตรวจจับไวรัสชนิดนี้เช่น โปรแกรมป้องกันไวรัสรู้จักพฤติกรรมการทำงานของไวรัสทั่วไป (เช่น การอ่าน/เขียนลงใน Master Boot Record ซึ่งโปรแกรมทั่วๆ ไปจะไม่ทำเช่นนี้) เมื่อโปรแกรมป้องกันไวรัสตรวจพบว่ามีการทำงานที่ผิดปกติขึ้นในเครื่อง โปรแกรมป้องกันไวรัสจะใช้กฎ Heuristic เปรียบเทียบกับลักษณะดังกล่าว เพื่อที่จะระบุว่าเป็นพฤติกรรมการทำงานของไวรัสชนิดใด

ข้อดีของเทคนิคนี้คือมีความยืดหยุ่นในการตรวจจับ และสามารถรู้จักไวรัสชนิดใหม่ๆ ได้เอง

4. <u>การตรวจจับไวรัสโดยการดักจับ (Interception)</u> เทคนิคนี้จะเริ่มต้นด้วยการที่โปรแกรมป้องกันไวรัสจะสร้าง virtual machine ที่มีความอ่อนแอมากไว้ภายในเครื่อง คอยล่อให้โปรแกรมประเภทไวรัสโจมตี และยังมีหน้าที่เฝ้าดูว่ามีไวรัสหรือโปรแกรมใดบ้างที่มีพฤติกรรมผิดปกติน่าสงสัยเข้ามาทำงานใน virtual machine ตัวอย่างเช่น มีโปรแกรมที่ทำการติดตั้งตัวเอง

รวมทั้งมีการส่ง Request ผิดปกติออกมาเพื่อทำให้เครื่องทำงานผิดพลาด เป็นต้น โปรแกรมที่ผิดปกติหรือน่าสงสัยนี้อาจจะเป็นไวรัสก็ได้

ข้อดีของการใช้เทคนิคนี้คือจะหยุดการทำงานของโปรแกรมไวรัสที่พยายามที่จะฝังตัวในหน่วยความจำได้ดี

เทคนิคในการตรวจจับไวรัสทั้ง 4 เทคนิค เป็นเทคนิคพื้นฐานที่พัฒนาขึ้นเพื่อใช้ในการตรวจจับไวรัส โดยโปรแกรมป้องกันไวรัสทั่วไป จะอาศัยเทคนิคที่กล่าวมา โดยอาจรวบรวมเอาจุดเด่นของแต่ละเทคนิคมาพัฒนาจนเป็นเทคนิคใหม่ๆ เพื่อใช้กำจัดไวรัสในยุคใหม่ๆ

2.1.1.2.2 <u>การป้องกันด้วยไฟร์วอลล์ส่วนตัว (Personal Firewall)</u>

ไฟร์วอลล์ส่วนตัว[9] คือซอฟต์แวร์ที่ติดตั้งในเครื่องคอมพิวเตอร์ส่วนตัวมีหน้าที่ช่วยป้องกันผู้บุกรุกหรือผู้ไม่ประสงค์ดีเข้ามาในเครื่องคอมพิวเตอร์ และช่วยป้องกันโปรแกรมที่ไม่ประสงค์ดีทั้งหลาย เช่น ไวรัส โทรจัน สปายแวร์ ถูกติดตั้งลงไปในเครื่องคอมพิวเตอร์ส่วนตัวโดยที่ผู้ใช้งานอาจไม่ทราบหรือไม่รู้ตัว

ไฟร์วอลล์ทำงานโดยทำการตรวจสอบข้อมูลทั้งหมด (ไวรัส โทรจัน สปาย-แวร์ ก็ถือเป็นข้อมูลด้วย) ที่เข้าหรือออกจากเครื่องคอมพิวเตอร์ส่วนตัว และจะอนุญาตให้ผ่านไปได้ก็ต่อเมื่อตรวจสอบแล้วและพบว่าไม่ละเมิดกับกฎเกณฑ์ของไฟร์วอลล์ที่กำหนดไว้ และในทางตรงกันข้ามหากมีการละเมิด ไฟร์วอลล์ก็จะไม่อนุญาตให้ผ่านไป

ทั้งนี้มาตรฐานในการอนุญาตที่จะให้แพ็คเกจผ่านเข้าและผ่านออกได้นั้น ก็จะขึ้นอยู่กับ มาตรฐานการกำหนดกฎ จากผู้ผลิต Personal Firewall ด้วยนั่นเอง

2.1.1.2.3 <u>การป้องกันไวรัสและกำจัดไวรัสคอมคอมพิวเตอร์ด้วย Firewall Application ชนิด UTM (Unified Threat Management) บริเวณ Internet Gateway</u>

เทคโนโลยีอุปกรณ์[10] UTM (Unified Threat Management) เป็นอุปกรณ์ไฟร์วอลล์ที่เป็นทั้งฮาร์ดแวร์และซอฟต์แวร์ภายในตัวเดียวกัน เป็นอุปกรณ์ที่เป็นเทคโนโลยีอัจฉริยะเพราะเพียง

---

[9] คณะอนุกรรมการด้านความมั่นคง ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ, “ไฟล์วอลล์ส่วนตัว”, 2548.

[10] บริษัท แอสทาโร่ ประเทศไทย (จำกัด), “การป้องกันภัยจาก Network”, <www.astaro.co.th>, 2550.

อุปกรณ์ UTM ตัวเดียวก็มีความสามารถที่ป้องกันภัยคุกคามจาก Network ได้หมด ไม่ว่าเป็นการทำ Firewall ในระดับ Stateful Inspection Technology ที่เป็นการออกแบบมาเพื่อปกป้องการโจมตีจากเครือข่ายต่างๆ โดยสามารถใช้ได้หลายรูปแบบในการปกป้อง อันได้แก่ VPN , Load Balancing, Network Shaping , DNS Server , DHCP Server , LAN Autentication รวมถึงความสามารถที่สำคัญที่มีเทคโนโลยีระบบตรวจจับผู้บุกรุก IDS/IPS และ Proxy Anti virus/spam/spyware ได้ในตัว โดยการปกป้องรูปแบบต่างๆ นี้จะทำงานร่วมกันเพื่อป้องกันภัยคุกคามข้อมูลจากเครือข่ายทั้งที่เหนือกว่าเทคโนโลยีไฟล์วอลล์ชนิดดั้งเดิมที่ไม่เคยปรากฏมาก่อน

การติดตั้งอุปกรณ์ UTM จะกระทำบริเวณเกตเวย์ระหว่างเครือข่ายองค์กรและอินเทอร์เน็ตหรือเครือข่ายอื่นๆ เช่นเดียวกับไฟร์วอลล์ โดยจะมีการบริหารจัดการผ่านหน้าจอควบคุมแบบเว็บเพียงจุดเดียว โดยสามารถสแกนข้อมูลในเครือข่ายองค์กรได้ทั้งขาเข้าและขาออกเพื่อปกป้องที่สมบูรณ์แบบในทุกวงเครือข่ายและไม่รบกวนประสิทธิภาพในการเชื่อมต่อ โดยยังมีระบบที่จะอัพเดตไวรัสซิกเนเจอร์แบบอัตโนมัติในตัวด้วย สำหรับการบริหารจัดการความปลอดภัยขององค์กรจากระยะไกลโดยผ่านทางอินเทอร์เน็ต ไม่เพียงป้องกันไวรัส เวิร์ม และโทรจันได้เท่านั้น แต่ยังป้องกันภัยคุกคามอื่นๆ ได้อีกด้วย เช่น สปายแวร์ แอดแวร์ โปรแกรมต่อโทรศัพท์ หรือโปรแกรมเจาะระบบโดยสามารถสรุปความสามารถต่างๆของ UTM ได้ดังนี้

- <u>การป้องกันภัยจากเวปไซด์ (Web Security)</u>
    - โดยสามารถบล็อกการเข้ามาของสปายแวร์/ป้องกันการส่งข้อมูลลับออกนอกระบบ (Spyware Protection)
    - สามารถป้องกันการติดไวรัสจากการดาวน์โหลดจากเว็ปไซด์และเวปอีเมลล์ (Virus Protection for Website)
    - สามารถป้องกันการเข้าเวปไซด์ที่มีความเสี่ยง และเวปไซด์ที่ไม่พึงประสงค์ได้ (Content Filtering)
- <u>การป้องการภัยจากทางอีเมลล์ (E-mail Security)</u>
    - สามารถตรวจจับอีเมลล์ตามโปรโตรคอล SMTP และ POP3 เพื่อตรวจหาไฟล์แนบ ตลอดจนไฟล์บีบอัดได้ (Virus Protection for E-mail)

- สามารถกรองจดหมายสแปม และอีเมลล์ที่ไม่ถูกต้องได้ (Virus Protection for E-mail)
- สามารถบล็อกอีเมลล์ที่พยายามหลอกลวงให้ผู้ใช้งานเปิดเผยความลับได้ (Phishing Protection)

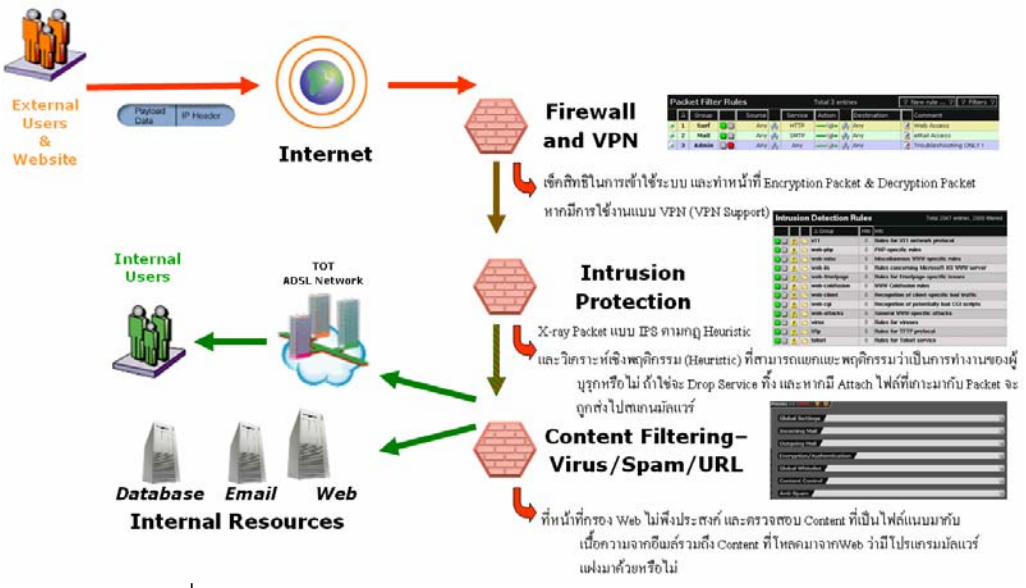
- <u>การป้องกันภัยจากโครงข่าย (Network Security)</u>

- สามารถตรวจจับและบล็อกการโจมตีโดยใช้เทคนิค Heristics ,Anomaly Detection และ Pattern –Based (Intrusion Protection)
- สามารถตรวจจับป้องกัน Packet และ Application Proxy ช่วยกรองการเข้าของอินเตอร์เน็ตได้ (Firewall)
- สามารถรองรับการใช้งานแบบเชื่อมต่อแบบเสมือน VPN ได้อย่างปลอดภัยจากไวรัส (Vertual Private Gateway)

การทำงานของ UTM นั้นจะป้องกันภัยจากภายนอก และภายในโครงข่ายได้โดยเริ่มจากการเช็คสิทธิ์ในการเข้าใช้ระบบและทำหน้าที่ Encryption Packet และ Decryption Packet หากมีการใช้งานแบบ VPN จากนั้นหากการ Access เข้า Network ถูกต้องก็จะถูกส่งผ่านเข้าไปยังกระบวนการ Intrusion Protection เพื่อตรวจลักษณะของ Packet (X-ray) ตามแบบของ IPS ให้เป็นไปตามกฎ Heuristic ที่จะแยกแยะพฤติกรรมว่าเป็นการทำงานของไวรัสหรือไม่โดยถ้าเป็นก็จะมีการ Drop Service ทิ้ง จากนั้นหาก Packet ที่มาเป็นปกติก็จะผ่านเข้าไปสู่ขั้นตอน กรองเวปไซด์ที่ไม่พึงประสงค์ (Content Filtering) และหากเป็น Content ที่มาจากอีเมลล์ก็จะส่งไปตรวจหามัลแวร์ต่อไป หรือเมื่อหากเป็น Content โหลดมาจากเวปไซด์ก็จะตรวจว่ามีมัลแวร์แฝงมาด้วยหรือไม่ ดังแสดงตามภาพที่ 2.3

ภาพที่ 2.3

ลักษณะการทำงานของ UTM บนโครงข่ายอินเตอร์เน็ต



แหล่งที่มา : www.astraro.co.th

ในอนาคตคาดว่าจะมีแนวโน้มนิยมการนำเทคโนโลยี Firewall ประเภท UTM นี้มาใช้กันมากขึ้น โดยเฉพาะอย่างยิ่งในประเทศไทย และเมื่อหากต้องการนำ UTM มาวางบนเครือข่ายระดับใหญ่แล้ว จะต้องทำการบริหารจัดการแยกส่วนอุปกรณ์ให้ดี เพื่อสร้างเสถียรภาพในการทำงานให้กับระบบ UTM เอง รวมถึงประสิทธิภาพจากการใช้งานของโครงข่าย

สำหรับการจัดการเพื่อนำ UTM มาติดตั้งบนโครงข่ายนั้น จะต้องใช้เทคโนโลยีในการการจำลองเพื่อสร้างเครือข่าย[11] โดยส่วนใหญ่จะใช้การแบ่ง VLAN (Virtual LAN) ที่เป็นเทคโนโลยีที่ใช้ในการจำลองสร้างเครือข่าย LAN แต่ไม่ขึ้นอยู่กับการต่อทางกายภาพเช่น สวิตช์หนึ่งตัวสามารถใช้จำลองเครือข่าย LAN ได้ห้าเครือข่าย หรือสามารถใช้สวิตช์สามตัวจำลองเครือข่าย LAN เพียงหนึ่งเครือข่ายก็ได้เช่นกัน ในการสร้าง VLAN โดยใช้อุปกรณ์เครือข่ายหลายตัว จะมีพอร์ตที่ทำหน้าที่เชื่อมต่อระหว่างอุปกรณ์เครือข่ายแต่ละตัว เรียก Trunk port ซึ่งเสมือนมีท่อเชื่อมหรือ Trunk เป็นตัวเชื่อมด้วยเนื่องมาจาก VLAN เป็น LAN แบบจำลอง แม้ว่าจะต่อทางกายภาพ

---

[11] กิติศักดิ์ จิรวรรณกูล, “ทำความรู้จักกับ VLAN”, <http://thaicert.nectec.or.th/paper/basic/vlan.php>, 2545.

อยู่บนอุปกรณ์เครือข่ายตัวเดียวกัน แต่การติดต่อกันนั้นจำเป็นต้องใช้อุปกรณ์ที่มีความสามารถในการค้นหาเส้นทาง เช่น เราท์เตอร์ หรือสวิตช์เลเยอร์สาม

ลักษณะพิเศษของ VLAN ทั่วๆ ไปคือ

- VLAN แต่ละเครือข่ายที่ติดต่อกันนั้นจะมีลักษณะเหมือนกับต่อแยกกันด้วยบริดจ์
- VLAN สามารถต่อข้ามสวิตช์หลายตัวได้
- ท่อเชื่อม (Trunks) ต่างๆ จะรองรับทราฟฟิคที่คับคั่งของแต่ละ VLAN ได้

ชนิดของ VLAN

1. Layer 1 VLAN : Membership by ports

ในการแบ่ง VLAN จะใช้พอร์ตบอกว่าเป็นของ VLAN ใด เช่นสมมุติว่าในสวิตช์ที่มี 4 พอร์ต กำหนดให้ พอร์ต 1, 2 และ 4 เป็นของ VLAN เบอร์ 1 และพอร์ตที่ 3 เป็นของ VLAN เบอร์ 2 ดังตารางที่ 2.3

ตารางที่ 2.3

การกำหนดพอร์ตให้กับ VLAN

Port	VLAN
1	1
2	1
3	2
4	1

ที่มา : http://www.thaicert.nectec.or.th

2. Layer 2 VLAN : Membership by MAC Address

ใช้ MAC Address ในการแบ่ง VLAN โดยให้สวิตช์ตรวจหา MAC Address จากแต่ละ VLAN ดูตารางที่ 2.4

ตารางที่ 2.4

การกำหนด MAC Address ให้กับ VLAN ต่างๆ

MAC Address	VLAN
1212354145121	1
2389234873743	2
3045834758445	2
5483573475843	1

ที่มา : http://www.thaicert.nectec.or.th

3. Layer 2 VLAN : Membership by Protocol types

แบ่ง VLAN โดยใช้ชนิดของ protocol ที่ปรากฏอยู่ในส่วนของ Layer 2 Header ดูตารางที่ 2.5

ตารางที่ 2.5

การแบ่ง VLAN โดยใช้ชนิดของ protocol กำหนด

Protocol	VLAN
IP	1
IPX	2

ที่มา : http://www.thaicert.nectec.or.th

4. Layer 3 VLAN : Membership by IP subnet Address

แบ่ง VLAN โดยใช้ Layer 3 Header นั่นก็คือใช้ IP Subnet เป็นตัวแบ่ง เช่นดังตารางที่ 2.6

ตารางที่ 2.6

การแบ่ง VLAN โดยใช้ IP Subnet

IP Subnet	VLAN
23.2.24.0	1
26.21.35.0	2

ที่มา : http://www.thaicert.nectec.or.th

5. Higher Layer VLAN's

VLAN ทำได้โดยใช้โปรแกรมประยุกต์หรือ service แบ่ง VLAN เช่นการใช้โปรแกรม FTP สามารถใช้ได้ใน VLAN 1 เท่านั้น และถ้าจะใช้ Telnet สามารถเรียกใช้ได้ใน VLAN 2 เท่านั้น เป็นต้น

<u>จุดประสงค์ในการใช้ VLAN</u>

1. เพิ่มประสิทธิภาพของเครือข่าย

ในระบบเครือข่ายทั่วไปจะมีการส่งข้อมูล Broadcast จำนวนมาก ทำให้เกิดความคับคั่ง (Congestion) และ VLAN มีความสามารถช่วยเพิ่มประสิทธิภาพของเครือข่ายได้เนื่องจาก VLAN จะจำกัดให้ส่งข้อมูล Broadcast ไปยังผู้ที่อยู่ใน VLAN เดียวกันเท่านั้น

2. ง่ายต่อการบริหารการใช้งาน

VLAN อำนวยความสะดวกในการบริหารจัดการโครงสร้างของระบบเครือข่ายให้ง่าย มีความยืดหยุ่น และเสียค่าใช้จ่ายน้อย โดยเพียงเปลี่ยนโครงสร้างทางตรรกะ (Logical) เท่านั้น ไม่จำเป็นต้องเปลี่ยนโครงสร้างทางกายภาพ กล่าวคือ ถ้าต้องการเปลี่ยนโครงสร้างของ VLAN ก็ทำโดยการคอนฟิกที่อุปกรณ์เครือข่ายใหม่ ไม่จำเป็นเปลี่ยนรูปแบบทางกายภาพของการเชื่อมต่อเครือข่ายที่มีอยู่เดิม

3. เพิ่มการรักษาความปลอดภัยมากขึ้น

เนื่องจากการติดต่อระหว่างอุปกรณ์เครือข่ายจะสามารถทำได้ภายใน VLAN เดียวกันเท่านั้น ถ้าต้องการที่จะติดต่อข้าม VLAN ต้องติดต่อผ่านอุปกรณ์ค้นหาเส้นทางหรือสวิตช์เลเยอร์สาม

มาตรฐานของ VLAN

มาตรฐาน IEEE 802.1Q นั้นเป็นมาตรฐานในการนำข้อมูลของ VLAN membership ใส่เข้าไปใน Ethernet Frame หรือที่เรียกว่า การ Tagging และโปรโตคอล 802.1Q นี้ถูกพัฒนาเพื่อแก้ปัญหาเรื่องการบริหารจัดการด้านเครือข่ายที่เพิ่มขึ้น เช่น การกระจายเครือข่ายใหญ่ๆ ให้เป็นส่วนย่อยๆ (Segment) ทำให้ไม่สูญเสียแบนวิธให้กับการ broadcast และ multicast มากเกินไป และยังเป็นการรักษาความปลอดภัยระหว่างส่วนย่อยต่างๆ ภายในเครือข่ายให้สูงขึ้นด้วย

การต่อเติมเฟรม (tagging Frame) ด้วยมาตรฐาน 802.1Q นั้นจะทำในระดับ Data-Link layer และการทำ VLAN Tagging นั้นจะเป็นการเปลี่ยนรูปแบบของ Ethernet Frame มาตรฐาน 802.3 ให้เป็นรูปแบบใหม่ที่เป็นมาตรฐาน 802.3 ac ซึ่งมีไดอะแกรมของเฟรมมาตรฐาน 802.3 ดังรูปที่ 2.4 และไดอะแกรมของมาตรฐาน 802.3 ac ดังภาพที่ 2.5 (ส่วนที่อยู่ในปีกกาส่วนกลางจะแทนส่วนของ tag 802.1Q)

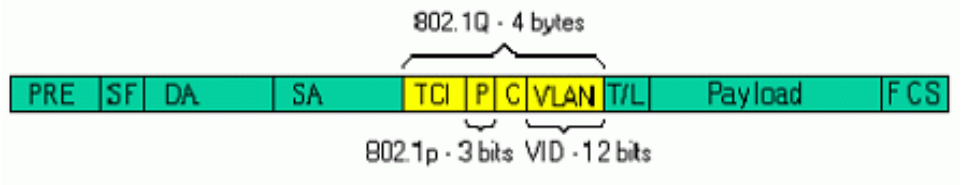
ภาพที่ 2.4

รูปแบบของเฟรม 802.3 ก่อนที่จะทำ VLAN Tagging

ที่มา : http://www.thaicert.nectec.or.th

ภาพที่ 2.5

รูปแบบของเฟรม 802.3 ที่มีการ tagging 802.1Q แล้ว



ที่มา : http://www.thaicert.nectec.or.th

ตารางที่ 2.7

คำอธิบายส่วนต่างๆ ของมาตรฐาน 802.3

Label	Field Name	Size	Description
PRE	Preamble	7 bytes	Used to synchronize traffic between nodes
SF	Start Frame Delimiter	1 bytes	Marks the beginning of the header
DA	Destination Address	6 bytes	The MAC address of the next/final hop
SA	Source Address	6 bytes	The MAC address of the source
TCI	Tag Control Info	2 bytes	When set to '8100', indicates this frame uses 802.1p and Q tags
P	Priority	3 bits	Indicates 802.1p priority level 0-7
C	Canonical Indicator	1 bit	Indicates if the MAC addresses are in canonical format – Ethernet uses "0"
VLAN	VLAN Identifier (VID)	12 bits	Indicates which VLAN this frame belongs to (0-4095)
T/L	Type/Length Field	2 bytes	Ethernet II "type" or 802.3 "length" information
Payload	Payload	≤1500 bytes	User data or higher layer protocol information
FCS	Frame Check Sequence	4 bytes	Error checking on the frame's contents – also known as "CRC" (Cyclical Redundancy Check)

ที่มา : http://www.thaicert.nectec.or.th

2.1.2 ทฤษฎีทางการตลาดสำหรับวางกลยุทธ์ในการดำเนินธุรกิจ

สำหรับการนำทฤษฎีที่จะมาทำการวิเคราะห์สำหรับการวางแผนกลยุทธ์ในการศึกษาความเป็นไปได้ในการให้บริการอินเตอร์เน็ตปลอดไวรัสครั้งนี้ จะศึกษาความเป็นไปได้จากทฤษฎีการศึกษาความเป็นไปได้ทางการตลาด รวมถึงการวิเคราะห์ด้วยทฤษฎี SWOT และวิเคราะห์ด้วยทฤษฎีของโมเดลผลกระทบจากแรงกดดัน 5 ประการ (Five Forces Model of Competition ; Michael E. Porter) รวมถึงทฤษฎีการวิเคราะห์ส่วนประสมทางการตลาด (4P : Market MIX) มาทำการวิเคราะห์การวางกลยุทธ์ดังกล่าว

2.1.2.1 ทฤษฎีการศึกษาความเป็นไปได้ทางการตลาด

การศึกษาความเป็นไปได้ทางการตลาด[12] แบ่งเป็นขั้นตอนต่างๆ ได้ 4 ขั้นตอนดังนี้

2.1.2.1.1 การวิเคราะห์สภาวะตลาดโดยการศึกษา โดยจะศึกษาตามหัวข้อดังต่อไปนี้

1) ขนาดของตลาด(Market Size)

คือการคาดคะเนความต้องการของตลาดโดยรวม ซึ่งต้องคำนึงถึงปัจจัยอื่น ๆ เพิ่มเติม เช่น อำนาจการซื้อ อัตราการบริโภค

2) แนวโน้มของตลาด (Market Trend)

คือการหาทิศทางความต้องการของผู้บริโภคที่มีต่อผลิตภัณฑ์หนึ่ง ๆ ว่าจะมีมากขึ้นหรือน้อยลงเพียงใดเมื่อเวลาผ่านไป นิยมวัดเป็นอัตราการขยายตัว (Growth Rate) มีหน่วยเป็นเปอร์เซ็นต์

3) ส่วนแบ่งของตลาด (Market Share)

คือความสามารถของธุรกิจ หรืออาจเป็นโครงการที่ทำแล้วจะได้ส่วนแบ่งของตลาดส่วนหนึ่งจากตลาดทั้งหมดที่คาดคะเนไว้ ซึ่งปัจจัยที่มีผลต่อความสามารถในการครองตลาดมี 2 ประการ คือ

1. ความเข้มข้นของการแข่งขัน (Competition)

---

[12] ศิริวรรณ เสรีรัตน์ และคณะ , “หลักการตลาด”, 2543.

2. ความสามารถตอบสนองความต้องการของผู้บริโภค(Customer Satisfaction)

2.1.2.1.2 <u>การพยากรณ์ความต้องการของตลาด</u>

เมื่อทำการวิเคราะห์สภาวะตลาดแล้ว จะต้องทำการพยากรณ์ปริมาณความต้องการของตลาด ในรูปของจำนวนเงิน หรือจำนวนหน่วยสำหรับผลิตภัณฑ์ชนิดใดชนิดหนึ่ง ของกลุ่มผู้บริโภคภายในขอบเขตพื้นที่หนึ่ง และระยะเวลาที่กำหนดให้ โดยพิจารณาถึง ผลิตภัณฑ์ที่จะพยากรณ์ ตลาดของผลิตภัณฑ์ กลุ่มผู้บริโภค ขอบเขตพื้นที่ ระยะเวลา โปรแกรมทางการตลาด และสภาวะแวดล้อมทางการตลาด

2.1.2.1.3 <u>การประมาณการยอดขายสินค้า</u>

วิธีการพื้นฐานที่นิยมใช้ในการพยากรณ์ยอดขาย คือการคาดคะเนส่วนแบ่งตลาดที่โครง การนั้นจะได้รับว่าเป็นร้อยละเท่าใดของตลาดรวม โดยพิจารณาถึงสภาวะเศรษฐกิจ การแข่งขัน ระดับของกลยุทธ์ทางการตลาดที่ใช้ การโฆษณาและการส่งเสริมการขาย

2.1.2.1.4 <u>การสรุปผลการศึกษาทางการตลาด</u>

เป็นขั้นตอนสุดท้ายของการศึกษาความเป็นไปได้ทางตลาดที่จะให้คำตอบว่า ควรทำการ ศึกษาความเป็นไปได้ทางด้านอื่นๆ ของโครงการหรือไม่ กล่าวคือ ถ้าผลการศึกษาทางการตลาดออกมาน่าพอใจ ซึ่งนั่นคืออุปสงค์หรือความต้องการของตลาดในผลิตภัณฑ์ของโครงการมีมากพอ แต่ถ้าผลการศึกษาทางการตลาดพบว่าความต้องการของตลาดไม่มากพอ ก็อาจตัดสินใจยกเลิกโครงการได้

2.1.2.2 <u>การวิเคราะห์สภาพแวดล้อมองค์กร (SWOT Analysis)</u>

การวิเคราะห์ SWOT จะช่วยให้ผู้บริหารทราบถึงจุดแข็ง จุดอ่อนในธุรกิจของตนจากการวิเคราะห์สภาพแวดล้อมภายในองค์กรของตน (Internal environment) โดยหลักแล้วจะเป็นการศึกษาวิเคราะห์เพื่อหาข้อได้เปรียบหรือเสียเปรียบเชิงกลยุทธ์ของภายในองค์กรนั่นของ ซึ่งโดยทั่วไปแล้วนักบริหารจะทำการสำรวจปัจจัยภายในขององค์กรของตนในทุกๆ ด้านเพื่อหาจุดแข็งและจุดอ่อนขององค์กร ซึ่งอาจยกตัวอย่างได้ เช่น สำรวจวิเคราะห์ช่องทางการตลาดรวมถึงช่องทางการจัดจำหน่าย ว่ามีจุดแข็งจุดอ่อนอย่างไร และควรปรับปรุงแก้ไขอย่างไรเป็นต้น ซึ่งโดยทั่วไปแล้วในแต่ละองค์กรก็จะมีจุดอ่อนและจุดแข็งของตนที่แตกต่างกันไป

จากสภาพแวดล้อมของธุรกิจ ผู้บริหารยังต้องเฝ้าติดตามสภาพแวดล้อมภายนอกองค์กร (External environment) ที่อาจจะส่งผลดีเป็นโอกาสในการดำเนินธุรกิจ หรืออาจส่งผลร้ายกลายเป็นอุปสรรค์ในการดำเนินธุรกิจขององค์กรได้เช่นกัน เนื่องจากปัจจัยภายนอกองค์กรนั้นมีความสัมพันธ์ต่อการดำเนินงานขององค์กร ตัวอย่างเช่น การเฝ้าติดตามสถานการณ์อัตราแลกเปลี่ยนเงินตราต่างประเทศ หากผู้บริหารมิได้ใส่ใจและสำรองเงินตราต่างประเทศไว้และเป็นธุรกิจที่ต้องซื้อขายกับต่างประเทศ ก็อาจจะทำให้ประสบกับสภาวะขาดทุนได้

การวิเคราะห์ SWOT สามารถแบ่งได้เป็น 4 หัวข้อหลักๆ ได้ดังนี้คือ

1. <u>จุดแข็ง (S : Strengths)</u>

จุดแข็งหรือจุดได้เปรียบที่เกิดจาก สภาพแวดล้อมภายในที่สามารถแข่งขันได้โดยที่แต่ละองค์กรจะมีจุดแข็งของตนและแตกต่างกันไป เช่น จุดแข็งด้านส่วนประสมการตลาด จุดแข็งด้านการเงิน จุดแข็งด้านการผลิต จุดแข็งในการบริหารงาน ทรัพยากรมนุษย์ และการจัดองค์กร จากจุดแข็งขององค์กรจะนำมาใช้ในการกำหนดกลยุทธ์การตลาด

2. <u>จุดอ่อน (W : Weaknesses)</u>

จุดอ่อนหรือจุดเสียเปรียบอันที่เกิดจาก สภาพแวดล้อมภายในด้านต่างๆ ขององค์กร ซึ่งจะเป็นอุปสรรคต่อการดำเนินงานซึ่งอาจเกิดได้ในหลายๆ ด้าน

3. <u>โอกาส (O : Opportunities)</u>

โอกาสหรือช่องทางที่สามารถจะนำมาใช้ให้เป็นประโยชน์กับธุรกิจของเราได้ ซึ่งเป็นการนำข้อได้เปรียบซึ่งวิเคราะห์จากสิ่งแวดล้อมภายนอกที่บริษัทอาจแสวง หาโอกาสจากสิ่งแวดล้อมด้านใดด้านหนึ่งมากำหนดกลยุทธ์การตลาดที่เหมาะสมกับสิ่งแวดล้อมนั้น เช่น ส่วนแบ่งการตลาดที่ยังพอมีที่ว่างให้เราแทรกเข้าไปได้ ตัวผลิตภัณฑ์ยังมีช่องทางการพัฒนารูปแบบให้แตกต่างออกไปได้อีก การเพิ่มสายการผลิตประกอบชิ้นส่วนใหม่ๆ เพื่อโอกาสขยายตลาด โอกาสขยายตลาดโดยอาศัยการสนับสนุนจากบริษัทแม่

4. <u>อุปสรรค์ (T : Threats)</u>

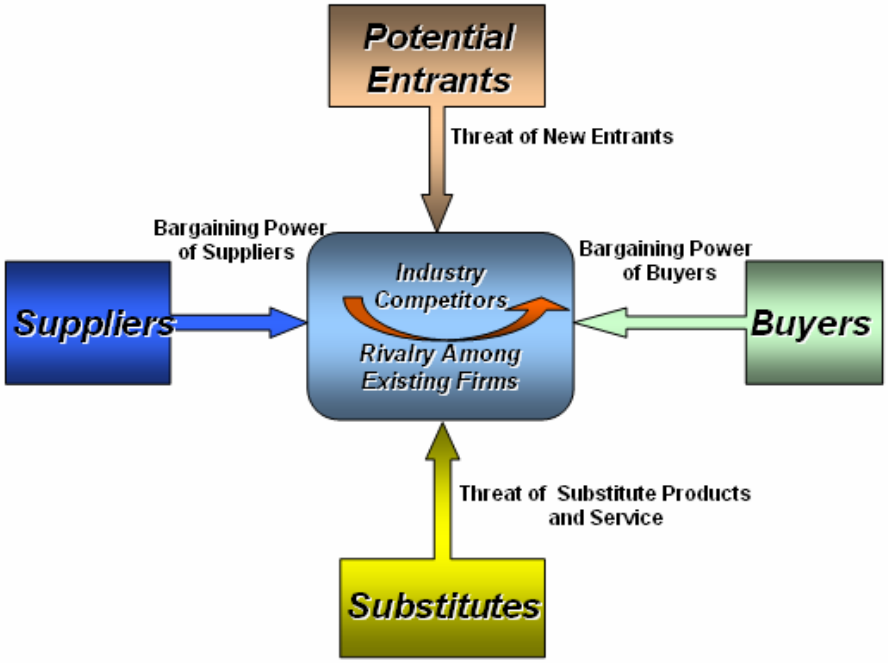
ภัยคุกคามเป็นข้อจำกัดที่เกิดจากสิ่งแวดล้อม ภายนอกองค์กร ซึ่งจำเป็นที่จะต้องปรับกลยุทธ์การตลาดให้เหมาะสม เช่น ภาวะถดถอยทางเศรษฐกิจ การเข้าตลาดของคู่แข่งรายใหม่ กฎหมาย หรือระเบียบใหม่ๆ ที่ทางราชการกำหนด รวมไปถึงเทคโนโลยีใหม่ๆที่จะมาทดแทนเทคโนโลยีในตลาดเก่าได้เช่นกัน

2.1.2.3 การวิเคราะห์ผลกระทบจากแรงกดดัน 5 ประการ (Five Force Model of Competition)

Michael E. Porter ได้พัฒนาเครื่องมือในการวิเคราะห์ ที่มีประโยชน์ในการสำรวจสภาพแวดล้อมทางการแข่งขัน อิทธิพลเหล่านี้จะพิจารณาถึงลักษณะ และขอบเขตในการแข่งขัน เช่น ศักยภาพการสร้างกำไรของอุตสาหกรรม ดังภาพที่ 2.6 แสดงถึงโมเดลผลกระทบจากแรงทั้ง 5 ประการ จากสภาพแวดล้อมทางการแข่งขันของอุตสาหกรรมของธุรกิจ ดังนั้นความเข้าใจอิทธิพลทั้ง 5 ประการจะช่วยให้ผู้บริหารพิจารณาถึงการบริหารเชิงกลยุทธ์ที่เหมาะสมที่สุด

ภาพที่ 2.6

โมเดลผลกระทบจากแรงกดดัน 5 ประการ (The five forces model of competition)



1. อุปสรรคจากคู่แข่งขันที่เข้ามาใหม่ในตลาด (Threat of New Entrants)

คู่แข่งขันใหม่ในอุตสาหกรรม จะเป็นอุปสรรคทางการแข่งขันสำหรับธุรกิจเดิม การเพิ่มขึ้นของสมรรถภาพ และศักยภาพที่จะแย่งส่วนครองตลาดของคู่แข่งขันเดิม คู่แข่งขันใหม่จะทำให้เกิดการใช้ทรัพยากรมากขึ้น ซึ่งเกิดจากความสัมพันธ์ระหว่างอุปสรรคจากการเลิกกิจการ (Exit barriers) และอุปสรรคจากการเข้ามาแข่งขัน (Entry barriers) 4 กรณี ดังนี้

1) ผลตอบแทนต่ำและคงที่ (Low and stable returns) เกิดขึ้นในกรณีที่อุปสรรคจากการเลิกกิจการต่ำและอุปสรรคจากการเข้ามาแข่งขันต่ำด้วย

2) ผลตอบแทนสูงและคงที่ (High and stable returns) เกิดขึ้นในกรณีที่อุปสรรคจากการเลิกกิจการต่ำและอุปสรรคจากการเข้ามาแข่งขันสูงด้วย

3) ผลตอบแทนต่ำและมีความเสี่ยงสูง (Low and risky returns) เกิดขึ้นในกรณีที่อุปสรรคจากการเลิกกิจการสูงและอุปสรรคจากการเข้ามาแข่งขันต่ำ

4) ผลตอบแทนสูงและมีความเสี่ยงสูง (High and risky returns) เกิดขึ้นในกรณีที่อุปสรรคจากการเลิกกิจการสูงและอุปสรรคจากการเข้ามาแข่งขันสูง

2. อำนาจการต่อรองของผู้ขายปัจจัยผลิต (Bargaining Power of Suppliers)

ผู้ขายปัจจัยการผลิตจะมีผลกระทบต่อศักยภาพด้านกำไรของอุตสาหกรรม ทำให้ราคาปัจจัยการผลิต และราคาสินค้าสูงขึ้น หรือลดคุณภาพสินค้า และลดบริการ

3. อำนาจการต่อรองของผู้ซื้อ (Bargaining Power of Buyers)

ผู้ซื้อผลิตภัณฑ์ของอุตสาหกรรมจะสร้างอำนาจการต่อรองด้านราคาหรือต้องการคุณภาพที่ดีขึ้นสำหรับราคาเดิม

4. อุปสรรคจากผลิตภัณฑ์ที่ทดแทนกันได้ (Threat of Substitute Products or Service)

ความสามารถในการหาผลิตภัณฑ์ที่ทดแทนกัน จะทำให้เกิดข้อจำกัดด้านราคาของผลิตภัณฑ์ในอุตสาหกรรมเมื่อราคาของผลิตภัณฑ์ที่มีอยู่สูงขึ้นเหนือกว่าผลิตภัณฑ์ที่ทดแทนกันได้ ลูกค้าจะเปลี่ยนแปลงไปใช้สินค้าทดแทนกันได้ทันทีธุรกิจที่มีการผลิตสินค้าที่ทดแทนกันได้ต้องพยายามสร้างความแตกต่างทางการแข่งขัน ทางเลือกก็คือ ธุรกิจที่ต้องการเพิ่มต้นทุนของผู้ซื้อของการเปลี่ยนระหว่างผลิตภัณฑ์ของบริษัทของคู่แข่งขันซึ่งผลิตภัณฑ์ที่ทดแทนกันได้ เราจะต้องติดตามอย่างใกล้ชิด ประกอบด้วยลักษณะการพัฒนาการปรับปรุงผลิตภัณฑ์ในรูปของการบริหารและการลดราคาลง

5. การแข่งขันที่ในอุตสาหกรรม (Rivalry Among Existing Firms)

อุตสาหกรรมในระบบเศรษฐกิจเสรีนิยมส่วนใหญ่จะมีระดับการแข่งขันที่รุนแรงมากขึ้น การแข่งขันนี้โดยทั่วไปจะเป็นการทำโปรโมรชั่นมาแข่งขันกันด้วยราคา ความแตกต่างด้านผลิตภัณฑ์ หรือความแปลกใหม่ของนวัตกรรมด้านผลิตภัณฑ์นั่นเอง โดยผู้บริหารจะต้องระลึก

เสมอว่าธุรกิจในรูปแบบของการแข่งขันเหล่านี้จะไม่สามารถแยกจากกันได้ จึงต้องจำเป็นที่จะต้องจับตาในสถานการณ์การแข่งขันในตลาดอยู่เสมอ

การแข่งขันระหว่างคู่แข่งขันในอุตสาหกรรมระบบเศรษฐกิจนิยม(หรือทุนนิยม) สามารถแบ่งได้ 3 รูปแบบ คือ

1) การแข่งขันด้านราคา (Price Competition)
2) นวัตกรรมผลิตภัณฑ์ (Product Innovation)
3) ความแตกต่างด้านผลิตภัณฑ์ (Product Differentiation)

2.1.2.4 <u>การวิเคราะห์ทางการตลาด (4P : Market MIX)</u>

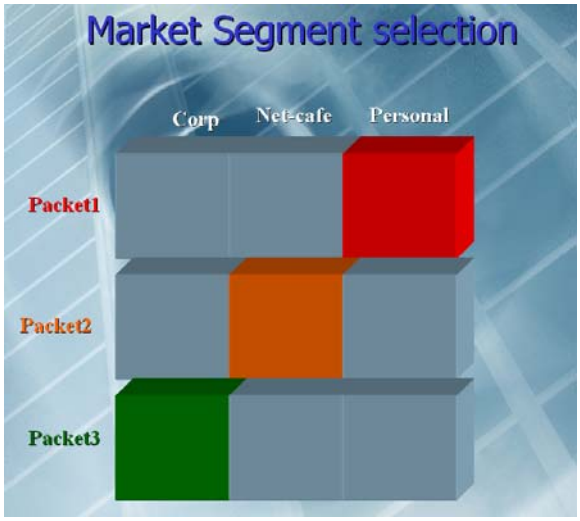
การวางแผนการตลาดด้วยการนำ 4P (Product Price Place Promotion) มาใช้ทำกลยุทธ์ทางการตลาดนั้น เป็นการนำเอาหลักการวางแผนขององค์ประกอบในขั้นตอนทางการตลาดมาทำการบริหารจัดการให้เหมาะสม เพื่อให้บรรลุวัตถุประสงค์ทางการตลาด (Marketing objectives) โดยเป็นการกำหนดจุดมุ่งหมายของแผนการตลาดที่จะประกอบไปด้วยวัตถุประสงค์ทางการเงิน และวัตถุประสงค์ทางการตลาด โดยการจัดการส่วนประสมทางการตลาด (Marketing Mix) ที่เป็นตัวแปรทางการตลาดที่ควบคุมได้ ซึ่งบริษัทรวมถึงพนักงานในส่วนต่างๆ ต้องร่วมกันเพื่อใช้ความคิดริเริ่มสร้างสรรค์มาทำการบริหารจัดการในการตอบสนองความพึงพอใจแก่กลุ่มเป้าหมายโดยผ่านเครื่องมือทางการตลาดที่สามารถแบ่งออกได้เป็น 4 ประเภทหลักๆได้แก่

1. <u>ผลิตภัณฑ์ (P1 : Product)</u> ได้แก่สิ่งที่เสนอขายโดยธุรกิจเพื่อสนองความต้องการของลูกค้าให้พึงพอใจผลิตภัณฑ์ที่เสนอขายนี้ อาจจะมีตัวตนหรือไม่มีตัวตนก็ได้ ผลิตภัณฑ์จึงประกอบด้วยสินค้า บริการ ความคิด สถานที่องค์กรหรือบุคคล ผลิตภัณฑ์ต้องมีอรรถประโยชน์ (Utility) มีคุณค่า (Value) ในสายตาของลูกค้า จึงจะมีผลทำให้ผลิตภัณฑ์สามารถขายได้ การกำหนดกลยุทธ์ด้านผลิตภัณฑ์ต้องพยายามคำนึงถึงปัจจัยต่อไปนี้ ความแตกต่างของผลิตภัณฑ์ (Product Differentiation) พิจารณาจากองค์ประกอบของผลิตภัณฑ์ (Product Component) การกำหนดตำแหน่งผลิตภัณฑ์(Product Positioning) การพัฒนาผลิตภัณฑ์(Product Development) กลยุทธ์เกี่ยวกับส่วนประสมผลิตภัณฑ์ (Product Mix) และสายผลิตภัณฑ์ (Product Line) อีกทั้งการจัดแพ็คเก็จหรือลักษณะของผลิตภัณฑ์ ให้เหมาะสมตามลักษณะการจัดแบ่งลักษณะ

(Segmentation) ในการใช้บริการตาม Life Style ของลูกค้าด้วย รวมถึงยังต้องคำนึงถึงรูปแบบในการใช้งานของลูกค้าเป็นสำคัญด้วย ดังตัวอย่างภาพที่ 2.7

ภาพที่ 2.7

ตัวอย่างการจัดวาง Segment ของการบริการตามลักษณะประเภทของลูกค้า



2. <u>ราคา (P2 : Price)</u> หมายถึง คุณค่าผลิตภัณฑ์ในรูปตัวเงินเป็นต้นทุน (Cost) ของลูกค้า ผู้บริโภคจะเปรียบเทียบระหว่างลูกค้า (Value) ผลิตภัณฑ์กับราคา (Price) ผลิตภัณฑ์นั้นถ้าคุณค่าสูงกว่าราคาลูกค้าก็จะตัดสินใจซื้อ ดังนั้นผู้กำหนดกลยุทธ์ด้านราคาต้องคำนึงถึง คุณค่าที่รับรู้ (Perceived Value) ในสายตาลูกค้าซึ่งต้องพิจารณาว่าการยอมรับของลูกค้าในคุณค่าของผลิตภัณฑ์ว่าสูงกว่าราคาผลิตภัณฑ์นั้น ต้นทุนสินค้าและค่าใช้จ่ายที่เกี่ยวข้อง การ แข่งขันและปัจจัยอื่นๆ

3. <u>การจัดจำหน่าย (P3 : Place หรือ Distribution)</u>หมายถึง โครงสร้างของช่องทางการจำหน่าย ซึ่งประกอบด้วยสถาบันและกิจกรรม ใช้เพื่อเคลื่อนย้ายผลิตภัณฑ์และบริการจากองค์กรไปยังตลาด สถาบันที่นำผลิตภัณฑ์ออกสู่ตลาดเป้าหมาย คือ สถาบันการตลาด ส่วนกิจกรรมที่ช่วยในการกระจายสินค้าประกอบด้วย การขนส่ง การคลังสินค้า และการเก็บรักษาสินค้าคงคลัง ประกอบด้วย 2 ส่วนคือ

- ช่องทางการจัดจำหน่าย (Channel of Distribution) หมายถึงเส้นทางที่ผลิตภัณฑ์และกรรมสิทธิ์ที่ผลิตภัณฑ์ถูกเปลี่ยนมือไปยังตลาด ในระบบช่องทางการจำหน่ายจึงประกอบด้วย ผู้ผลิต คนกลาง ผู้บริโภคหรือผู้ใช้ทางอุตสาหกรรม

- การสนับสนุนการกระจายตัวสินค้าสู่ตลาด (Market Logistics) หมายถึงกิจกรรมที่เกี่ยวข้องกับการเคลื่อนย้ายผลิตภัณฑ์จากผู้ผลิตไปยังผู้บริโภคหรือผู้ใช้ทางอุตสาหกรรม ประกอบด้วยงาน คือ การขนส่ง (Transportation) การเก็บรักษาสินค้า (Storage) และการคลังสินค้า (Warehousing) และการบริหารสินค้าคงเหลือ (Inventory Management)

4. <u>การส่งเสริมการขาย (P4 : Promotion)</u> เป็นการติดต่อสื่อสารเกี่ยวกับข้อมูลระหว่างผู้ซื้อกับผู้ขาย เพื่อสร้างทัศนคติและพฤติกรรมการซื้อ การติดต่อ สื่อสารอาจใช้พนักงานขายทำการขาย (Personal Selling) และการติดต่อสื่อสารโดยไม่ใช้คน (Nonpersonal Selling) เครื่องมือในการติดต่อสื่อสารมีหลายประการซึ่งอาจเลือกใช้หนึ่งหรือหลายเครื่องมือต้องใช้หลักการเลือกเครื่องมือสื่อสารแบบประสมประสานกัน (Integrated Marketing Communication; IMC) โดยพิจารณาถึงความเหมาะสมกับลูกค้า ผลิตภัณฑ์ คู่แข่งขัน โดยบรรลุ จุดมุ่งหมายร่วมกันได้ เครื่องมือส่งเสริมการขายที่สำคัญมีดังนี้

- การโฆษณา (Advertising) เป็นกิจกรรมในการเสนอข่าวสารเกี่ยวกับองค์กรและผลิตภัณฑ์ บริการ หรือความคิด ที่ต้องมีการจ่ายเงินโดยผู้อุปถัมภ์รายการ กลยุทธ์ในการโฆษณาจะเกี่ยวข้องกับ กลยุทธ์การสร้างสรรค์งานโฆษณา (Creative Strategy) ยุทธวิธีการโฆษณา (Advertising Tactics) และกลยุทธ์สื่อ (Media Strategy)

- การขายโดยใช้พนักงานขาย (Personal Selling) เป็นกิจกรรมการแจ้งข่าวสารและจูงใจตลาดโดยใช้บุคคล

- การส่งเสริมการขาย (Sales Promotion) หมายถึง กิจกรรมการส่งเสริมที่นอกเหนือจากการโฆษณาการขายโดยใช้พนักงานขาย และการให้ข่าวและการประชาสัมพันธ์ ซึ่งสามารถกระตุ้นความสนใจ ทดลองใช้ หรือการซื้อโดยลูกค้าขั้นสุดท้ายหรือบุคคลอื่นในช่องทาง การส่งเสริมการขายมี 3 รูปแบบ คือ การกระตุ้นผู้บริโภค การกระตุ้นคนกลาง และการกระตุ้นพนักงานขาย

- การให้ข่าวและการประชาสัมพันธ์ (Publicity and Public Relations) การให้ข่าวเป็นการเสนอความคิดเกี่ยวกับสินค้าหรือบริการที่ไม่ต้องมีการจ่ายเงิน ส่วนการประชาสัมพันธ์

หมายถึง ความพยายามที่มีการวางแผนโดยองค์กรหนึ่งเพื่อสร้างทัศนคติที่ดีต่อองค์กรให้เกิดกับกลุ่มใดกลุ่มหนึ่ง การให้ข่าวเป็นกิจกรรมหนึ่งของการประชาสัมพันธ์

- การตลาดทางตรง (Direct Marketing หรือ Direct Response Marketing) และการตลาดเชื่อมตรง (Online Marketing) เป็นการติดต่อสื่อสารกับกลุ่ม เป้าหมายเพื่อให้เกิดการตอบสนอง (Response) โดยตรง หรือหมายถึงวิธีการต่างๆ ที่นักการตลาดใช้ส่งเสริมผลิตภัณฑ์โดยตรงกับผู้ซื้อและทำให้เกิดการตอบสนองในทันทีประกอบด้วย การขายทางโทรศัพท์ การขายโดยใช้จดหมายตรง การขายโดยใช้แคตตาล็อค การขายทางโทรทัศน์ วิทยุหรือหนังสือพิมพ์ ซึ่งจูงใจให้ลูกค้ามีกิจกรรมการตอบสนอง

2.1.3 ทฤษฎีทางการเงินในการจัดทำแผนธุรกิจ

การใช้เกณฑ์สำหรับการพิจารณา การลงทุนหมายถึง ต้นทุนที่ต่ำสุด หรือการทำกำไรหรืออัตรากำไรที่สูงสุดนั่นเอง การคัดเลือกจะเริ่มต้นจากการกำหนดวัตถุประสงค์หรือเป้าหมายในการลงทุนแล้วจึงพิจารณาโครงการและแนวทางเลือกทั้งหมดที่สามารถดำเนินการ เพื่อบรรลุวัตถุประสงค์ที่กำหนดไว้[13] หลังจากนั้นจึงจะพิจารณาเปรียบเทียบผลตอบแทนหรือผลประโยชน์ที่จะได้รับจากโครงการ แล้วจึงตัดสินใจเลือกโครงการหรือทางเลือกที่ให้ผลตอบแทนสูงสุด ซึ่งการพิจารณาเพื่อการตัดสินใจนี้ สามารถทำได้หลายวิธี ได้แก่

1. วิธีวัดมูลค่าปัจจุบันสุทธิ (NPV : Net Present Value)
2. วิธีคิดอัตราผลตอบแทนแบบคิดลด (IRR : Internal Rate of Return)
3. วิธีการคิดระยะเวลาคืนทุน (PB : Payback Period Method)
4. วิธีระยะเวลาคืนทุนแบบคิดลด (DPB : Discount Payback Period Method)
5. วิธีวัดดัชนีในการทำกำไร (PI : Profitability Index Method)
6. วิธีวัดอัตราผลตอบแทนเฉลี่ยทางบัญชี (ARR : Average rate of return Method)

[13] MC Graw Hill, “Finance Fundamental”, 2006.

โดยการที่จะเลือกลงทุนในโครงการใดโครงการหนึ่งนั้นจะต้องมีสิ่งสำคัญที่ต้องพิจารณาควบคู่กันไปได้แก่ ลักษณะของของโครงการลงทุน เพื่อพิจาณาว่าโครงการที่เราจะลงทุนนั้นมีลักษณะเป็นอย่างไร ซึ่งสามารถจำแนกโครงการลงทุนออกเป็น 3 ลักษณะคือ

1. โครงการที่เป็นอิสระต่อกัน (Dependent project) หมายถึง โครงการลงทุนที่ไม่ขึ้นอยู่กับโครงการใดโครงการหนึ่ง ซึ่งเมื่อรับหรือปฏิเสธโครงการหนึ่งแล้วไม่มีผลต่อโครงการอื่น

2. โครงการที่ขึ้นต่อกัน (Contingent project) หมายถึง โครงการลงทุนที่เกี่ยวข้องกัน เมื่อรับโครงการหนึ่งแล้ว ก็ต้องรับอีกโครงการหนึ่งด้วย เช่น โครงการสร้างรถไฟฟ้า เมื่อรับโครงการสร้างรถไฟฟ้าแล้วก็ต้องรับโครงการสร้างอาคารสถานีรถไฟฟ้ารวมถึงอาคารผู้โดยสารด้วย

3. โครงการที่มีวัตถุประสงค์อย่างเดียวกัน (Mutually exclusive project) หมายถึง เมื่อเลือกโครงการใดโครงการหนึ่งแล้ว โครงการอื่นที่วัตถุประสงค์เดียวกันก็ต้องยกเลิกไป เช่น กิจการต้องการขยายกำลังการผลิต จึงพิจารณาซื้อเครื่องจักร A และ B เมื่อเลือกซื้อเครื่องจักร A แล้ว เครื่องจักร B ก็ยกเลิกไป

2.1.3.1 <u>วิธีวัดมูลค่าปัจจุบันสุทธิ (NPV : The net present Value)</u>

เป็นการวัดผลต่างระหว่างมูลค่าปัจจุบันของกระแสเงินสดรับสุทธิแต่ละปี ตลอดอายุโครงการกับมูลค่าปัจจุบันของเงินสดจ่ายลงทุน ณ อัตราค่าของทุน (Cost of Capital) โดยมีวิธีในการคำนวณดังนี้

$$NPV = \sum_{t=1}^{n} \frac{X_t}{(1+r_p)^t} - I \quad \text{.....(2.1)}$$

กำหนดให้

NPV คือ มูลค่าปัจจุบันสุทธิ

X คือ กระแสเงินสด (Cash flow) รับสุทธิแต่ละปีตั้งแต่ปีที่ 1- ปีที่ n

r_p คือ อัตราผลตอบแทนที่ต้องการหรือค่าของทุน (required Rate of return or cost of capital)

I คือเงินสดจ่ายสุทธิของโครงการ (Investment)

n คือ อายุของโครงการ หรือ อายุการใช้งานของสินทรัพย์ถาวร มีหน่วยเป็น ปี

โดยในการตัดสินใจลงทุนในโครงการ จะมีเกณฑ์การพิจารณาอยู่สามทางเลือก คือ

1. มูลค่าปัจจุบันสุทธิ มากกว่าศูนย์ (NPV > 0) ยอมรับโครงการ

2. มูลค่าปัจจุบันสุทธิ มากกว่าศูนย์ (NPV < 0) ปฏิเสธโครงการ

3. มูลค่าปัจจุบันสุทธิ เท่ากับศูนย์ (NPV < 0) อาจจะยอมรับหรือเพิกเฉยต่อโครงการ

จุดเด่น จุดด้อยของวิธีการมูลค่าปัจจุบัน

จุดเด่น

1. คำนึงถึงมูลค่าของเงินตามเวลา
2. คำนึงถึงกระแสเงินสดตลอดโครงการ
3. สมมติว่ากระแสเงินสดที่ได้รับจะนำไปลงทุนต่อในอัตราเดียวกับต้นทุนส่วนเพิ่มของเงินทุน

จุดด้อย

1. อาจตัดสินผิดหากโครงการนั้นแยกกันอย่างเด็ดขาด และมีอายุไม่เท่ากัน

2.1.3.2 วิธีคิดอัตราผลตอบแทนแบบคิดลด (IRR : Internal Rate of Return Method)

เป็นการคิดแบบอัตราคิดลด (Discount Rate) ที่ทำให้มูลค่าปัจจุบันของกระแสเงินสดรับสุทธิที่ได้รับในอนาคตเท่ากับเงินสดจ่ายลงทุนสุทธิ หรืออาจจะเรียกว่าเป็นการคำนวณหาอัตราผลตอบแทนที่แท้จริงของโครงการลงทุน หรือ อัตราผลตอบแทนที่ทำให้ PVCI = PVCO หรือ NPV = 0 ใช้สำหรับวัดประสิทธิผลของการลงทุน โดยมีวิธีในการคำนวณดังนี้

$$PV = \sum_{t=1}^{n} \frac{CFt}{(1+r)^t} \quad \text{.....(2.2)}$$

โดยกำหนดให้

PV คือ มูลค่าปัจจุบันหรือเงินสดจ่ายลงทุนสุทธิ

CFt คือ กระแสเงินสดรับสุทธิแต่ละปีของโครงการ

r คือ อัตราผลตอบแทนคิดลด(IRR)

n คือ อายุของโครงการหรืออายุการใช้งานของทรัพย์สินถาวร

โดยการจะยอมรับโครงการหรือไม่ จะพิจารณาจาก ค่า r

จุดเด่นและจุดด้อย ของวิธีคิดอัตราผลตอบแทนคิดลด (IRR Method)

จุดเด่น

1. คำนึงถึงมูลค่าของเงินตามระยะเวลา
2. คำนึงถึงกระแสเงินสดตลอดโครงการ

<u>จุดด้อย</u>

1. มีปัญหาในการจัดอันดับของโครงการ
2. อาจสับสนจากการมี IRR หลายค่า

2.1.3.3 <u>วิธีการคิดระยะเวลาคืนทุน (PB : Payback Period Method)</u>

การดูระยะคืนทุน จะเป็นการคำนวณหาจำนวนปีที่กิจการจะได้รับเงินที่ลงทุนเริ่มแรกของโครงการกลับคืนมา หรือเป็นการคิดระยะเวลาที่กระแสเงินสดสะสมของโครงการมีค่าเท่ากับศูนย์ เพื่อใช้สำหรับการตัดสินใจพิจารณาโครงการ โดยโครงการที่มีระยะเวลาคืนทุนยิ่งสั้นก็จะยิ่งดี กล่าวได้คือหากคืนทุนยิ่งเร็วก็ควรจะพิจารณาลงทุน ตัวอย่างเช่น การลงทุนที่ต้องลงเงินทุนทั้งสิ้น 1,000,000 บาท สามารถทำกำไรหลังหักภาษีได้ปีละ 200,000 บาทจะมีระยะเวลาคืนทุนเท่ากับ $\frac{1,000,000}{200,000}$ = 5 ก็คือโครงการนี้มีระยะเวลาคืนทุน คือ 5 ปี เป็นต้นนั่นเอง

<u>จุดเด่นและจุดด้อย ของวิธีระยะเวลาคืนทุน (Payback Period Method)</u>

<u>จุดเด่น</u>

1. คำนวณและเข้าใจง่าย
2. ใช้เป็นเครื่องมือวัดสภาพคล่องได้ (Biased towards liquidity)

<u>จุดด้อย</u>

1. ไม่ได้พิจารณาผลกำไรรวม และมูลค่าเงินที่เปลี่ยนตามเวลา
2. ไม่ได้คำนึงถึงกระแสเงินสดภายหลังระยะเวลาคืนทุน
3. ไม่เหมาะที่จะนำมาคิดกับงานโครงการที่มีระยะการคืนทุนที่นาน ได้แก่ประเภทการลงทุนในงานวิจัยพัฒนา หรือการลงทุนในโปรเจคใหม่ เนื่องจากการลงทุนในด้านนี้อาจมีความเสี่ยงในการใช้เวลาคืนทุนนาน หรืออาจจะไม่ได้ทุนคืนเลย ซึ่งผลของการคืนทุนก็อาจเปลี่ยนไปในรูปแบบอื่นได้

2.1.3.4 วิธีคิดระยะเวลาคืนทุนแบบคิดลด (DPB : Discount Payback Period Method)

เป็นการคิดระยะเวลาคืนทุนคิดลด คือ จำนวนปีที่กระแสเงินสดรับคิดลดของโครงการเท่ากับเงินลงทุนเริ่มแรก หรือ ระยะเวลาที่กระแสเงินสดคิดลดสะสม ของโครงการมีค่าเท่ากับศูนย์ ซึ่งในการคำนวณจะเหมือนกับวิธีระยะเวลาการคืนทุน (PB) แต่จะนำมูลค่าของเงินที่เปลี่ยนตามเวลา มาคิดด้วย

จุดเด่นและจุดด้อย ของวิธีระยะเวลาคืนทุนแบบคิดลด (Discount Payback Period Method)

จุดเด่น

1. คำนวณและเข้าใจง่าย
2. คำนึงถึงมูลค่าเงินที่เปลี่ยนไปตามเวลา (time value of money)
3. สามารถใช้เป็นเครื่องมือวัดสภาพคล่อง (Biased towards liquidity)
4. จะไม่ยอมรับโครงการที่มี ค่า NPV เป็นลบ

จุดด้อย

1. อาจจะปฏิเสธโครงการที่มีค่า NPV เป็นบวกได้
2. ไม่ได้พิจารณาผลกำไรรวมและมูลค่าเงินที่เปลี่ยนตามเวลา
3. ไม่ได้คำนึงถึงกระแสเงินสดภายหลังระยะเวลาคืนทุน
4. อาจจะมีผลลบกับตัวโครงการที่มีระยะการคืนทุนที่นาน เช่น การลงทุนในด้านการวิจัยและพัฒนาหรือการลงทุนในโปรเจคใหม่ เนื่องจากการลงทุนในด้านนี้ย่อมใช้เวลาคืนทุนนาน และผลของการคืนทุนอาจจะเปลี่ยนไปในรูปแบบอื่น

2.1.3.5 วิธีวัดดัชนีในการทำกำไร (PI : Profitability Index Method)

เป็นการคำนวณหาอัตราส่วนระหว่างมูลค่าปัจจุบันของกระแสเงินสดรับสุทธิที่คาดว่าจะได้รับ กับ มูลค่าปัจจุบันของกระแสเงินสดจ่ายลงทุนสุทธิของโครงการนั้น

$$PI = \frac{NPV}{I} \quad \text{.....(2.3)}$$

โดยจะพิจารณาเลือกลงทุนในโครงการที่มีค่า PI มากกว่า 1 สูงสุด

<u>จุดเด่น และจุดด้อย ของวิธีดัชนีกำไร (Profitability Index Method)</u>

<u>จุดเด่น</u>

1. เหมือน NPV
2. สื่อให้เห็นภาพและเข้าใจได้ง่าย
3. ใช้ในกรณีจัดสรรเงินทุนที่มีจำกัดอย่างเหมาะสม โดยเลือกโครงการทั้งหมดที่จะทำให้โครงการโดยรวมเกิดประโยชน์สูงสุด

<u>จุดด้อย</u>

1. อาจมีปัญหาในการจัดอันดับของโครงการ

2.1.3.6 <u>วิธีวัดอัตราผลตอบแทนเฉลี่ยทางบัญชี (ARR : Average Rate of Return Method)</u>

การเปรียบเทียบกำไรสุทธิหลังภาษีถัวเฉลี่ยกับเงินลงทุนเฉลี่ย หรือเรียกว่าอัตราผลตอบแทนทางบัญชี หรือผลตอบแทนเฉลี่ยของมูลค่าตามบัญชี คิดได้จากการนำกำไรสุทธิหลังภาษีถัวเฉลี่ยมาหารด้วยมูลค่าตามบัญชีถัวเฉลี่ย

$$\text{อัตราตอบแทนถัวเฉลี่ย} = \frac{\text{กำไรสุทธิหลังภาษีถัวเฉลี่ย}}{\text{มูลค่าตามบัญชีถัวเฉลี่ย}}$$

เราจะพิจารณาโครงการโดยการดูผลอัตราตอบแทนถัวเฉลี่ยที่คิดเป็นเปอร์เซ็นต์ โดยหากค่าของอัตราตอบแทนถัวเฉลี่ยมากกว่าที่ตั้งไว้ ก็จะยอมรับโครงการนั้นได้

<u>ตัวอย่างการหาอัตราตอบแทนถัวเฉลี่ยที่คิดเป็นเปอร์เซ็นต์</u>

กำไรสุทธิหลังหักภาษีถัวเฉลี่ยของโครงการหนึ่งที่มีอายุโครงการ 5 ปี โดยแต่ละปีมีค่าดังนี้ (เมื่อโครงการนี้มีมูลค่าการลงทุนเริ่มต้น ฿500,000)

ปีที่ 1	ปีที่ 2	ปีที่ 3	ปีที่ 4	ปีที่ 5
฿100,000	฿150,000	฿50,000	฿0	-฿50,000

กำไรสุทธิหลังหักภาษีถัวเฉลี่ย $= \frac{100,000+150,000+50,000+0+(-50,000)}{5}$

$= ฿50,000$

มูลค่าตามบัญชีถัวเฉลี่ย $= \frac{500,000+0}{2} = ฿\ 250,000$

อัตราตอบแทนถัวเฉลี่ย(ARR) $= \frac{50,000}{250,000} \times 100 = 20\ \%$

โดยถ้าผู้ลงทุนตั้งเป้าหมาย ARR ไว้ต่ำกว่า 20 % ก็ควรจะเลือกลงทุนโครงการนี้

<u>จุดเด่นและจุดด้อย ของ ARR</u>

<u>จุดเด่น</u>

1. ผู้บริการส่วนใหญ่ชอบวิธีนี้เนื่องจากผู้บริการมักประเมินค่าโครงการโดยใช้อัตราส่วนกำไรสุทธิต่อสินทรัพย์รวม
2. คำนวณง่าย

<u>จุดด้อย</u>

1. ไม่คำนึงถึงมูลค่าของเงินตามระยะเวลา
2. ใช้กำไรสุทธิทางบัญชีไม่ใช่กระแสเงินสด

2.2 <u>งานวิจัยที่เกี่ยวข้อง</u>

จากการทบทวนงานวิจัยที่เกี่ยวข้องกับการศึกษาความเป็นไปได้ในการให้บริการอินเตอร์เน็ตปลอดไวรัสผ่านโครงข่าย Broadband ADSL ของ บริษัท ทีโอที จำกัด (มหาชน) ผู้วิจัยได้ศึกษารายงาน รวมถึงงานวิจัยที่เกี่ยวข้องและสามารถใช้เป็นแนวทางเป็นประโยชน์ในการจัดทำได้ดังนี้

1. <u>รายงานสำรวจกลุ่มผู้ใช้อินเตอร์เน็ตในประเทศไทย (ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ , 2548)</u>

รายงานผลการสำรวจพฤติกรรมการใช้อินเตอร์เน็ตของปี พ.ศ.2548 จากหัวข้อในการสำรวจปัญหาสำคัญที่พบจากการใช้อินเตอร์เน็ต ที่ผู้ตอบคำถามสามารถตอบได้มากกว่าหนึ่งข้อจากคำถามปัญหาที่ตั้งไว้ 30 คำถาม โดยมีผู้ตอบคำถามหมดทั้งสิ้น 20,067 คน พบว่าปัญหา

เกี่ยวกับไวรัสเป็นปัญหาที่ผู้ตอบแบบสอบถามเห็นว่าสำคัญที่สุดอันดับหนึ่งถึงร้อยละ 66.3 ที่โดยเห็นได้ว่ามีแนวโน้มเพิ่มขึ้นจากการสำรวจในปี 2547 โดยในปีก่อนนั้นจัดอันดับปัญหาไวรัสคอมพิวเตอร์ได้เป็นอันดับที่สอง อยู่ที่ร้อยละ 55.3 และปี พ.ศ. 2546 อยู่ที่ร้อยละ 45.1 ส่วนปัญหารองลงมาของปี พ.ศ.2548 นั้นพบว่าเป็นปัญหาจากความล่าช้าคิดเป็นร้อยละ 54.9 และอีเมล์ขยะร้อยละ 42.5 ตามลำดับ โดยจะเห็นได้ว่าปัญหาไวรัสคอมพิวเตอร์ดังกล่าวนั้น มีแนวโน้มที่จะเพิ่มขึ้นเมื่อเทียบกับรายงานในปีก่อนนั่นเอง

2. <u>งานวิจัยเรื่อง การบริการและกลยุทธ์ด้านการตลาดอินเตอร์เน็ตความเร็วสูง กรณีศึกษา บริษัท ทรู คอร์ปอเรชั่น จำกัด (มหาชน) (จิตติมา ห้วยหงษ์ทอง, 2548)</u>

บรอดแบนด์ (Broadband) หรืออินเตอร์เน็ตความเร็วสูงเป็นเทคโนโลยีการสื่อสารที่เป็นที่นิยมในหลายประเทศทั่วโลก และในประเทศที่มีจำนวนผู้ใช้บรอดแบนด์จำนวนมากอย่างเช่นในเกาหลี ญี่ปุ่น และสหรัฐอเมริกา มีแนวโน้มว่าจำนวนผู้ให้บริการด้านข้อมูลหรือคอนเทนต์โพรไวเดอร์ เช่น ผู้ผลิตเกมออนไลน์ โปรแกรมสำหรับดิจิตอล ทีวี ภาพยนตร์ รวมทั้งเพลงออนไลน์ ก็จะเพิ่มขึ้นด้วย นั่นคือ การที่มีเครือข่ายบรอดแบนด์ที่ดี ส่งผลให้ธุรกิจอีกหลาย ๆ ด้านเติบโตขึ้นตามไปด้วย

หลังจาก ทรู ได้เปิดให้บริการ Hi-Speed Internet ในอัตราการบริการที่ต่ำลง ส่งผลให้ผู้บริโภคมีความตื่นตัว และในปัจจุบัน ทรู มียอดผู้ใช้บริการเพิ่มขึ้นอย่างมากด้วยนโยบายที่ชัดเจนของรัฐบาลที่ประกาศออกมาเมื่อต้นปี 2547 ว่าต้องการให้คนไทยทั่วประเทศเข้าถึงบรอดแบนด์ได้โดยไม่ยาก อินเตอร์เน็ตความเร็วสูงจึงได้รับความสนใจสูงทำให้ผู้ให้บริการอินเตอร์เน็ตหันมาใช้กลยุทธ์แข่งขันด้านราคากันมากขึ้น โดยให้บริการอินเตอร์เน็ตความเร็วสูงในราคาที่ถูกลง เช่น Samart, ADC, TOT, TT&T, CS Loxinfo และ ISSP เป็นต้น

ผู้วิจัยนั้นมีความสนใจที่จะศึกษาแนวความคิดและกลยุทธ์การให้บริการ ไฮ-สปีด อินเตอร์เน็ต และศึกษาความพึงพอใจของผู้ใช้บริการ ไฮ-สปีด อินเตอร์เน็ต ของบริษัท ทรู คอร์ปอเรชั่น จำกัด (มหาชน) ในปัจจุบัน เพื่อทราบความพึงพอใจและปัญหาของการให้บริการ เพื่อประโยชน์ในการสร้างกลยุทธ์ด้านการตลาดที่สามารถแข่งขันในตลาด และยังคงรักษาความเป็นผู้นำของตลาดอินเตอร์เน็ตความเร็วสูงไว้ได้ นอกจากนั้น ยังใช้เป็นแนวทางสำหรับการปรับปรุงการให้บริการอินเตอร์เน็ตความเร็วสูงสำหรับผู้ให้บริการรายอื่น ๆ เพื่อส่งเสริม และกระตุ้นให้อัตรา

ผู้ใช้บริการอินเตอร์เน็ตในประเทศไทยเพิ่มสูงขึ้น ซึ่งจะส่งผลดีต่อการขยายตัวของอีกหลายธุรกิจตามไปด้วย

3. งานวิจัยเรื่องการบูรณาการ “การสร้างสรรค์มูลค่า” ในกระบวนการพัฒนาผลิตภัณฑ์ใหม่ (จุฬาพรรณ บรรจงสัตย์, 2546)

หัวใจสำคัญของการตลาดมุ่งเน้นยุทธศาสตร์ (Strategic Marketing) ในการพัฒนาผลิตภัณฑ์ใหม่ที่นำไปสู่ความสำเร็จในยุคของการการมุ่งเน้นการตลาดองค์รวม (Holistic Marketing Concept) คือ การสร้างความโดดเด่นด้วยความแตกต่างที่เหนือกว่าบนความแตกต่างให้กับผลิตภัณฑ์ใหม่พร้อมการส่งมอบมูลค่าที่เหนือกว่าผ่านกระบวนการสร้างมูลค่าเพิ่มอย่างต่อเนื่อง (Value Creation) โดยจะต้องพิจารณาถึงคุณค่าที่แท้จริงที่ตรงกับความต้องการและเหนือความคาดหมายของลูกค้า อันจะนำไปสู่การจูงใจและการสร้างความจงรักภักดีของลูกค้า (Customer Loyalty) ที่มีต่อองค์กร เพื่อที่จะสามารถรักษาลูกค้ารายเก่า (Retention) และ ขยายตลาดไปยังลูกค้ารายใหม่ (Acquisition) นำไปสู่การเพิ่มส่วนครองตลาดทางใจของผู้บริโภค (Mind Share) ให้กับองค์กรอย่างยั่งยืน

ปัจจัยที่นำไปสู่ความสำเร็จในการสร้างมูลค่าเพิ่ม (Value Creation) ให้กับการพัฒนาผลิตภัณฑ์ใหม่มิใช่การมองเพียงแค่ลูกค้าเพียงด้านเดียว แต่จะต้องมองประกอบกันทั้งด้านผู้ผลิตและลูกค้า ซึ่งเป็นการตลาดยุทธศาสตร์ (Strategic Marketing) ในลักษณะ Prosumer (Producer +Consumer) การบริหารจัดการประกอบไปด้วย 3 ด้าน คือ ประการแรก ด้านลูกค้า (Demand Management) โดยการค้นหาและทำความเข้าใจถึงคุณค่าและความต้องการที่แท้จริงของลูกค้าเพื่อออกแบบและสร้างความแตกต่างที่สามารถครองใจลูกค้าได้ ประการที่สอง ด้านทรัพยากร(Resource Management) คือ การบริหารกระบวนการพัฒนาผลิตภัณฑ์ใหม่ให้มีประสิทธิภาพสูงสุดและให้สามารถส่งมอบผลิตภัณฑ์ใหม่ได้อย่างสัมฤทธิ์ผล ประการที่สาม ด้านการบริหารเครือข่าย (Network Management) การสร้างเครือข่ายสัมพันธ์กับพันธมิตร ทางธุรกิจที่มีส่วนร่วมเพื่อช่วยให้เกิดการสร้างมูลค่าเพิ่มที่มีประสิทธิภาพมากขึ้น

<u>จากการทบทวนงานวิจัยที่เกี่ยวข้องกับการศึกษาความเป็นไปได้ในการให้บริการอินเตอร์เน็ตปลอดไวรัสสามารถสรุปได้ดังนี้</u>

ผู้จัดทำมีแนวความคิดหลังจากได้ศึกษารายงานสำรวจกลุ่มผู้ใช้อินเตอร์เน็ตของประเทศไทย ปี พ.ศ.2548 พบว่าปัจจุบันปัญหาของผู้ใช้บริการอินเตอร์เน็ตในการสำรวจพบว่าปัญหาที่พบมากที่สุดได้แก่ การถูกโจมตีด้วยไวรัสคอมพิวเตอร์ผ่านโครงข่ายอินเตอร์เน็ต ประกอบกับการศึกษาถึงกลยุทธ์เกี่ยวกับตลาดพบว่าราคาของอัตราการบริการที่มีแนวโน้มที่จะต่ำลง โดยเป็นผลจากกลยุทธ์ที่ต้องการเพิ่มยอดผู้ใช้บริการให้มีการเพิ่มขึ้น ตามนโยบายของรัฐบาล ต้นปี 2547 ที่ต้องการให้คนไทยทั่วประเทศเข้าถึงบรอดแบนด์ได้โดยไม่ยาก อินเตอร์เน็ตความเร็วสูงจึงได้รับความสนใจสูง จนทำให้ผู้ให้บริการอินเตอร์เน็ตหันมาใช้กลยุทธ์แข่งขันด้านราคากันมากขึ้น และทำให้การบริการอินเตอร์เน็ตความเร็วสูงนั้นมีราคาที่ถูกลง และจากการศึกษากระบวนการพัฒนาผลิตภัณฑ์ใหม่ ที่ผู้จัดทำยังคิดสอดคล้องกับ คุณจุฬาพรรณ บรรจงสัตย์ ที่เห็นว่าหัวใจสำคัญของการตลาดที่มุ่งเน้นยุทธศาสตร์ นั้นก็คือการพัฒนาผลิตภัณฑ์ใหม่ ที่นำพาองค์กรไปสู่ความสำเร็จในยุคของการการมุ่งเน้นการตลาดองค์รวม รวมถึงที่จะการสร้างความโดดเด่นด้วยความแตกต่างที่เหนือกว่าบนความแตกต่างให้กับผลิตภัณฑ์ ซึ่งผู้จัดทำคาดว่าจะก่อให้เกิดประโยชน์และความสมบูรณ์ในการศึกษาความเป็นไปได้ในการให้บริการอินเตอร์เน็ตปลอดไวรัสของ บมจ.ทีโอที ในครั้งนี้ได้เป็นอย่างมาก