แนวทางในการวางระบบความมั่นคงปลอดภัยสารสนเทศสำหรับเครือข่ายเฉพาะบริเวณแบบไร้สาย สำหรับวิสาหกิจขนาดกลางและขนาดเล็ก

INFORMATION SECURITY GUIDELINE FOR WIRELESS LOCAL AREA NETWORKS IN SMALL AND MEDIUM SIZED ENTERPRISES

ผกากรอง บ่ายสว่าง[1]

ประสงค์ ปราณีตพลกรัง[2]

พิลาศพงษ์ ทรัพย์เสริมศรี[3]

[1, 3]หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาระบบสารสนเทศคอมพิวเตอร์ มหาวิทยาลัยศรีปทุม

[2] หลักสูตรวิทยาศาสตรมหาบัณฑิต สาขาวิชาเทคโนโลยีสารสนเทศ มหาวิทยาลัยศรีปทุม

E-mail : baiswang@hotmail.com[1], prasong.pr@spu.ac.th.com[2], pilastpongs@yahoo.com[3]

บทคัดย่อ

ในงานวิจัยนี้ ผู้วิจัยได้นำเสนอแนวทางหรือกรอบความมั่นคงปลอดภัยสารสนเทศสำหรับเครือข่ายเฉพาะบริเวณแบบไร้สายสำหรับวิสาหกิจขนาดกลางและขนาดเล็ก โดยอ้างอิงกับมาตรฐาน ISO/IEC 27001 และใช้กรณีศึกษาเป็นธุรกิจร้านกาแฟที่ให้บริการเสริมด้านเครือข่ายไร้สาย โดยมีวิธีการวิจัย คือ การศึกษาถึงสภาพปัจจุบันภายในวิสาหกิจขนาดกลางและขนาดเล็ก ที่มีการใช้เครือข่ายเฉพาะบริเวณแบบไร้สาย ผู้วิจัยได้จัดทำกรอบความมั่นคงปลอดภัยสารสนเทศสำหรับเครือข่ายเฉพาะบริเวณแบบไร้สายสำหรับวิสาหกิจขนาดกลางและขนาดเล็ก ภายใต้กรอบมาตรฐาน ISO/IEC 27001 ในการวิจัยครั้งนี้มีการเก็บข้อมูลโดยการสัมภาษณ์บริษัทที่เป็นวิสาหกิจขนาดเล็ก การศึกษาเอกสารงานวิจัย ระบบมาตรฐาน ISO 17799/27001 และในการกำหนดกรอบความมั่นคงปลอดภัยสำหรับเครือข่ายเฉพาะบริเวณแบบไร้สายสำหรับวิสาหกิจขนาดกลางและขนาดเล็กนั้น ได้พิจารณา OSI Model กับ Defense Information System Agency for the Department of Defense (DISA for the DOD) และ United States Department of Homeland Security (DHS) ทั้งนี้ เพื่อให้ได้ระบบที่มีความเสถียรในการใช้งานบนระบบเครือข่าย

กรอบความมั่นคงความปลอดภัยสารสนเทศสำหรับเครือข่ายเฉพาะบริเวณแบบไร้สายสำหรับวิสาหกิจขนาดกลางและขนาดเล็กที่ผู้วิจัยได้จัดทำขึ้นนี้ สามารถใช้เป็นตัวแบบความมั่นคงปลอดภัยสารสนเทศในวิสาหกิจขนาดกลางและขนาดเล็กได้ อีกทั้งยังสามารถนำไปปรับใช้ในหน่วยงานอื่นๆ ได้

คำสำคัญ : ความมั่นคงปลอดภัย เครือข่ายเฉพาะบริเวณแบบไร้สาย วิสาหกิจขนาดกลางและขนาดเล็ก

ABSTRACT

This study presents the development of information security framework in wireless local area networks for small and medium sized enterprises according to ISO/IEC 27001. A case study is a coffee shop business providing wireless local area networks for customers.

The purpose of this paper is to determine the current condition of information security framework for wireless local area networks in small and medium sized enterprises, and creates the framework under ISO/IEC 27001 international standard. Data were collected by survey interview and data collection such as ISO 17799/27001 International standard system, study researches. The Framework of wireless network system security will be applied from OSI Model and Defense Information System Agency for the Department of Defense (DISA for the DOD) and United State Department of Homeland Security (DHS).

The information security framework for wireless local area networks that has been developed can be used in Thai SMEs and other Organizations.

KEYWORDS : Information security, Wireless local area networks, Small and medium sized enterprises

1. ความเป็นมาและความสำคัญของปัญหา

SMEs (Small and Medium Sized Enterprises) คือ วิสาหกิจขนาดกลางและขนาดเล็ก ซึ่งมีความหมายรวมถึงอุตสาหกรรมการผลิต (Manufacturing) กิจการค้าส่งและค้าปลีก (Whole sale and Retail) และกิจการบริการ (Service) ซึ่งเกณฑ์ในการจัดอุตสาหกรรม เป็นอุตสาหกรรมขนาดใหญ่ กลาง หรือ เล็กนั้นมีหลายวิธี แต่โดยทั่วไปจะใช้ จำนวนคนงาน (ขนาดการจ้างงาน) จำนวนเงินลงทุน มูลค่าทรัพย์สิน จำนวนยอดขาย หรือรายได้เป็นเกณฑ์ กิจการใดจะเข้าข่ายเป็น SMEs หรือไม่กระทรวงอุตสาหกรรมได้กำหนดเกณฑ์ การแบ่งประเภทของวิสาหกิจขนาดเล็กมีจำนวนคนงานไม่เกิน 50 คน จำนวนเงินลงทุนไม่เกิน 20 ล้านบาท และวิสาหกิจขนาดกลางจำนวนคนงานระหว่าง 50 ถึง 200 คน จำนวนเงินลงทุนระหว่าง 20 ถึง 200 ล้านบาท

เทคโนโลยีการสื่อสารแบบเครือข่ายเฉพาะบริเวณแบบไร้สาย (Wireless LAN) ที่มีการใช้งานอย่างแพร่หลาย รวมไปถึงวิสาหกิจขนาดกลางและขนาดเล็ก (SMEs) ซึ่งเป็นธุรกิจที่มีความหลากหลายและมีอัตราการเติบโตสูงขึ้นในปัจจุบัน การใช้ระบบไร้สายในองค์กรจะทำให้เพิ่มความสะดวกสบายและลดค่าใช้จ่ายในการติดตั้งเหมาะสำหรับบุคคลที่เข้ามาเชื่อมต่อข้อมูลหรือใช้งานร่วมกัน ทำให้ต้องคำนึงถึงระบบรักษาความปลอดภัยสารสนเทศสำหรับเครือข่ายเฉพาะบริเวณแบบไร้สาย เนื่องจากธุรกิจประเภท SME จะมีข้อมูลที่สำคัญเหมือนบริษัทเช่นกัน เช่น ข้อมูลทางการเงิน เป็นต้น จึงต้องการรักษาความปลอดภัยของข้อมูลในประเภทต่างๆ เช่น มีการรักษาความปลอดภัยของข้อมูลจากไวรัส การรับรองว่าจะมีการเก็บข้อมูลไว้เป็นความลับและผู้มีสิทธิเท่านั้นจึงจะเข้าถึงข้อมูลได้ การรับรองข้อมูลจะไม่ถูกเปลี่ยนแปลงหรือทำลายไม่ว่าจะเป็นอุบัติเหตุหรือโดยเจตนา การรับรองว่าข้อมูลและบริการการสื่อสารต่างๆ และพร้อมที่ใช้ได้ในเวลาที่ต้องการใช้งานเพราะธุรกิจ SME จำเป็นต้องมีการติดต่อสื่อสารโดยตรงกับลูกค้าอยู่ตลอด ดังนั้น การสร้างระบบความมั่นคงปลอดภัยจึงเป็นสิ่งจำเป็นสำหรับธุรกิจประเภท SME ด้วยเช่นกัน

ดังนั้น ในการศึกษาและวางระบบความมั่นคงปลอดภัยสำหรับระบบเครือข่ายเฉพาะบริเวณแบบไร้สายควรออกแบบให้มีความเหมาะสมกับความต้องการของธุรกิจนั้นๆ และตามลักษณะการใช้งานของผู้ใช้นั้นๆ

2. วัตถุประสงค์ของการวิจัย

ผู้วิจัยได้มีวัตถุประสงค์ของการวิจัยไว้ดังนี้

1. เพื่อศึกษาถึงสภาพปัจจุบันภายในวิสาหกิจขนาดกลางและขนาดเล็กที่มีความเกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศสำหรับเครือข่ายเฉพาะบริเวณแบบไร้สาย

2. เพื่อนำเสนอแนวทางการวางระบบความมั่นคงปลอดภัยสารสนเทศสำหรับเครือข่ายเฉพาะบริเวณแบบไร้สายในวิสาหกิจขนาดกลางและขนาดเล็กภายใต้กรอบมาตรฐาน ISO/IEC 27001

3. ขอบเขตของการวิจัย

ในการจัดทำงานวิจัยสาขาวิชาระบบสารสนเทศคอมพิวเตอร์ครั้งนี้ผู้วิจัยได้มีขอบเขตของการวิจัยโดยการศึกษามาตรฐานระบบสารสนเทศสำหรับเครือข่ายเฉพาะบริเวณแบบไร้สายสำหรับวิสาหกิจขนาดกลางและขนาดเล็กภายใต้กรอบมาตรฐาน ISO/IEC 27001 สำหรับควบคุมการทำงานของระบบธุรกิจขนาดกลางและขนาดเล็ก อาทิ ธุรกิจประเภทร้านกาแฟที่ให้บริการเสริมด้านเครือข่ายไร้สาย

4. รูปแบบการวิจัย

การวิจัยในครั้งนี้เป็นการวิจัยเชิงคุณภาพในรูปแบบของการศึกษาเฉพาะกรณี (Case Study) โดยศึกษาธุรกิจประเภท SME ที่มีการวางระบบเครือข่ายคอมพิวเตอร์และการวิจัยจะเป็นแบบประยุกต์เฉพาะกรณี โดยอ้างอิงจากมาตรฐาน ISO/IEC 27001 ซึ่งเป็นมาตรฐานในระดับสากลที่มีหลักปฏิบัติในการป้องกันและควบคุมข้อมูลที่จะสร้างความมั่นใจว่าข้อมูลและสารสนเทศยังถูกเก็บรักษาอยู่ครบถ้วนปลอดภัย โดยผู้ทำวิจัยได้ทำการศึกษาวิเคราะห์เอกสารและสอบถามความเหมาะสมต่อการวางระบบความมั่นคงปลอดภัยจากผู้เชี่ยวชาญที่เป็น CIO ของหน่วยงาน

5. แนวคิด ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

5.1 แนวคิดและทฤษฎีของไอทีต่อวิสาหกิจขนาดกลางและขนาดย่อม

ไอที และ ไอซีที (Information and Communication Technology) ประกอบด้วยเทคโนโลยีสำคัญหลายอย่าง เช่น เทคโนโลยีคอมพิวเตอร์ เทคโนโลยีการสื่อสารโทรคมนาคม เทคโนโลยีเครือข่ายคอมพิวเตอร์ เทคโนโลยีอินเทอร์เน็ต เทคโนโลยีการพิมพ์ ฯลฯ ในภาพรวมกล่าวได้ว่าการใช้ไอทีในงานธุรกิจ จะมีการใช้งานเพื่อเพิ่มความสะดวกแก่ผู้ปฏิบัติงานมากขึ้น เช่น การใช้คอมพิวเตอร์ในงานพิมพ์เอกสารที่เรียกว่างานประมวลคำ (Word Processing) หน้าเว็บในระบบอินเทอร์เน็ตยังเป็นส่วนหนึ่งของระบบสำนักงานอัตโนมัติ (Office Automation) เป็นการใช้งานคอมพิวเตอร์ในงานจัดทำและรับส่งเอกสารสำหรับบริษัทและหน่วยงาน เมื่อโลกรู้จักใช้ระบบอินเทอร์เน็ต และเทคโนโลยีเว็บแนวทางการพัฒนาระบบต่างๆ ก็เปลี่ยนไป งานประยุกต์เริ่มเปลี่ยนเป็นระบบเว็บไซต์ (Web Based System) มากขึ้น

5.2 งานวิจัยที่เกี่ยวข้อง

1. ภาคภูมิ ปรีชาพานิช (2550) ได้ทำการวิจัยเรื่องการพัฒนาตัวแบบความมั่นคงปลอดภัยของเว็บเซอร์วิสสำหรับกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร โดยงานวิจัยได้ศึกษาและพัฒนาตัวแบบความมั่นคงปลอดภัยของระบบเว็บเซอร์วิส สำหรับหน่วยงานในกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร และทำการประเมินความมั่นคงปลอดภัยของระบบเว็บเซอร์วิสภายในกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร โดยอิงตัวแบบที่ได้พัฒนาขึ้น

2. ศีลพล สุกไสว และ เกริก ภิรมย์โสภา "ระบบป้องกันการบุกรุกแบบปรับตัวได้เพื่อลดความเสียหายจากการโจมตีแบบการปฏิเสธการให้บริการ" นำเสนอแนวทางในการป้องกันและลดความเสียหายในระบบป้องกันการบุกรุก (Intrusion Prevention System) โดยใช้การปรับค่าขอบเขตสูงสุดของการติดต่อจากแต่ละหมายเลขไอพีตามช่วงเวลาที่ถูกโจมตี ซึ่งช่วยให้ระบบสามารถทนต่อการโจมตีได้นานขึ้น และยังสามารถให้บริการกับเครื่องที่มีแหล่งที่มาเดียวกันกับเครื่องที่ทำการโจมตีได้ ผลการทดลองของระบบต้นแบบที่ได้สร้างขึ้นแสดงให้เห็นว่าแนวทางที่นำเสนอนั้น สามารถที่จะลดความเสียหายจากการโจมตีได้ในขณะที่ระบบยังสามารถให้บริการกับเครื่องคอมพิวเตอร์ได้ตามปกติ

6. ผลการวิจัย

จากการดำเนินการวิจัย ผู้วิจัยได้ผลวิจัยดังต่อไปนี้

6.1 การกำหนดนโยบายด้านความมั่นคงปลอดภัยสำหรับเครือข่ายเฉพาะบริเวณแบบไร้สายสำหรับวิสาหกิจขนาดกลางและขนาดเล็ก

ในการกำหนดกรอบความมั่นคงปลอดภัยสำหรับระบบเครือข่ายไร้สายสามารถแบ่งออกเป็น 3 ส่วนมีรายละเอียดดังนี้

1. ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (Human Resources Security) การสร้างความมั่นคงปลอดภัยก่อนการจ้างงาน (Prior to Employment) การสร้างความมั่นคงปลอดภัยระหว่างการจ้างงาน (During Employment) การสิ้นสุดหรือการเปลี่ยนการจ้างงาน (Termination or Change of Employment)

2. ความมั่นคงปลอดภัยที่เกี่ยวข้องกับกระบวนการทำงาน (Process Resources Security)

- นโยบายความมั่นคงปลอดภัยของสารสนเทศ (Information Security Policy) นโยบายนี้เป็นกรอบในการกำหนดวัตถุประสงค์ มาตรการด้านความมั่นคงปลอดภัย รวมถึงแนวทางการบริหารความเสี่ยง และที่สำคัญนโยบายต้องให้ความสำคัญต่อการปฏิบัติตามกฎหมาย กฎระเบียบ สัญญาและข้อตกลงร่วมกัน
- โครงสร้างด้านความมั่นคงปลอดภัยของระบบสารสนเทศสำหรับองค์กร (Organization of Information Security)
- นโยบายการกำหนดมาตรการการป้องกันทรัพย์สินขององค์กร
- นโยบายการกำหนดหน้าที่และความรับผิดชอบและขั้นตอนการปฏิบัติงาน (Operational Procedures and Responsibilities)
- นโยบายการบริหารจัดการการให้บริการของหน่วยงานภายนอก (Third Party Service Delivery Management)

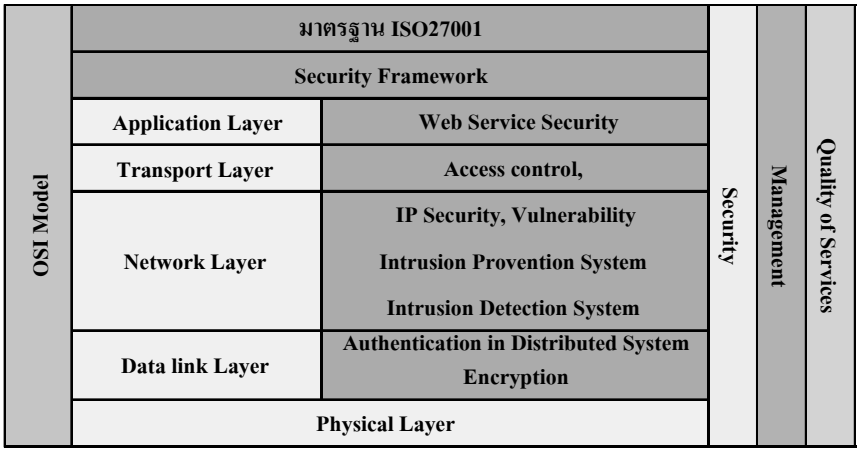
- นโยบายการควบคุมการเข้าถึง (Access Control)
- นโยบายการสร้างความมั่นคงปลอดภัยให้แก่ไฟล์ของระบบที่ให้บริการ (Security of System Files)
- นโยบายการปฏิบัติตามข้อกำหนดทางกฎหมาย (Compliance with Legal Requirements)
- นโยบายการตรวจประเมินระบบสารสนเทศ (Information Systems Audit Considerations

3. ความมั่นคงปลอดภัยที่เกี่ยวข้องกับเทคโนโลยี (Technology Resources Security)

- นโยบายความมั่นคงปลอดภัยของสารสนเทศ (Information Security Policy)
- นโยบายการสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and Environmental Security)
- นโยบายการบริหารจัดการด้านการสื่อสารและเครือข่ายสารสนเทศขององค์กร (Communicational Procedures and Responsibilities)
- นโยบายการควบคุมอุปกรณ์สื่อสารประเภทพกพา
- การปฏิบัติตามนโยบาย

6.2 การพัฒนาตัวแบบความมั่นคงความปลอดภัยสำหรับเครือข่ายเฉพาะบริเวณแบบไร้สาย สำหรับวิสาหกิจขนาดกลางและขนาดเล็ก

การพัฒนาตัวแบบความมั่นคงปลอดภัยมีฟีเจอร์และเครื่องมือต่าง ๆ ที่ช่วยในการบริหารจัดการและควบคุมระบบ จะช่วยให้การบริหารจัดการเซิร์ฟเวอร์ที่มีหลายแอพพลิเคชันและหลายยูสเซอร์ใช้งานพร้อมกัน นอกจากนี้ยังช่วยในการป้องกันข้อมูลตามนโยบายที่กำหนด ซึ่งจะติดตั้งพร้อมกับระบบเพื่อกรองข้อมูลการจราจรที่วิ่งเข้าออกบนระบบเครือข่าย ดังนั้น การศึกษาข้อมูลเกี่ยวกับกรอบความมั่นคงปลอดภัยสารสนเทศเครือข่ายเฉพาะบริเวณ แบบไร้สายสำหรับวิสาหกิจขนาดกลางและขนาดเล็กทั้งในส่วนของทฤษฎี งานวิจัยและมาตรฐาน ISO/IEC27001 ร่วมกับการวิเคราะห์ข้อมูลที่ได้จากการสัมภาษณ์ CIO จึงสามารถสร้างตัวแบบได้ดังภาพประกอบ 1



ภาพประกอบ 1 กรอบความมั่นคงปลอดภัยสารสนเทศเครือข่ายเฉพาะบริเวณแบบไร้สายสำหรับวิสาหกิจขนาดกลางและขนาดเล็ก

จากผลการกำหนดกรอบความมั่นคงปลอดภัยสารสนเทศเครือข่ายเฉพาะบริเวณแบบไร้สายสำหรับวิสาหกิจขนาดกลางและขนาดเล็กแสดงดังภาพประกอบ 1 ซึ่งแสดงถึงกรอบความมั่นคงปลอดภัยสารสนเทศเครือข่าย

เฉพาะบริเวณแบบไร้สายสำหรับวิสาหกิจขนาดกลางและขนาดเล็กที่อ้างอิงตามมาตรฐาน ISO/IEC 27001 โดยจะมีรายละเอียดในแต่ละ Layer ดังนี้

1. Application Layer เป็นจุดเชื่อมต่อระหว่างแอพพลิเคชันของผู้ใช้กับกระบวนการ การสื่อสารผ่านเครือข่าย ชั้นนี้อาจจะถือได้ว่าเป็นชั้นที่เริ่มกระบวนการติดต่อสื่อสาร คือ

- Web Services Security เป็นการรักษาความปลอดภัยสำหรับการให้บริการเว็บไซต์ โดยมีการจัดการ คือ

- Maintaining security while routing between multiple การป้องกันความปลอดภัยต้องป้องกันทุกๆ Layer เพราะผู้โจมตีอาจเลือก Layer ที่สามารถโจมตีได้ง่าย หรือมีจุดอ่อน
- Unauthorized Access ต้องจำกัดผู้ใช้งาน จำนวนผู้ใช้และการเข้าถึงข้อมูล คือกำหนดสิทธิ์ใช้งาน
- Parameter Manipulation/Malicious Input มีการส่ง Parameter หรือ Input ที่เป็นอันตรายจากผู้ไม่ประสงค์ดี เช่น SQL Injection เป็นต้น
- Network Eavesdropping and Message Replay ถ้าข้อมูลไม่ถูก Encryption ไว้ อาจถูกผู้ไม่ประสงค์ดีดักจับข้อมูลได้ง่าย ทำให้ข้อมูลไม่เป็นความลับ
- Denial of Services (DoS) ผู้โจมตีส่งคำสั่งจำนวนมากๆ (Message Bomb) ให้ Web Services ทำให้เกิดความเสียหาย
- Bypassing of Firewalls ผู้โจมตีพยายามโจมตีผ่าน port ที่ firewall เปิด คือ พยายามโจมตีผ่าน Port 80 เป็นต้น
- Immaturity of the platform Web Services มีการใช้ Platform ที่ต่างกัน ทำให้เกิดการโจมตีโดยง่าย

2. Transport Layer รับผิดชอบในการเคลื่อนย้ายข้อมูลระหว่างโพรเซสของผู้รับ และโพรเซสของผู้ส่ง ในที่นี้มีการรักษาความปลอดภัยดังนี้

- Access Control เป็นวิธีการเข้ารหัสข้อมูลที่จะนำมาใช้ในการป้องกันความลับของข้อมูลได้เป็นอย่างดี แต่ไม่สามารถที่จะป้องกันการปลอมแปลงเข้ามาในระบบได้ ส่วนวิธีที่ใช้ในการป้องกันการปลอมแปลงการเข้าระบบ การป้องกันการเรียกเข้าในระบบโดยไม่ได้รับอนุญาต เป็นการกำหนดระดับสิทธิในการเข้าถึงระบบในการเขาถึงข้อมูลต่าง ๆ กัน

3. Network Layer จะรับผิดชอบในการจัดเส้นทางให้กับข้อมูลระหว่างสถานีส่งและสถานีรับ โดยมีระบบการรักษาความปลอดภัยดังนี้

- IP Security จะมีระบบรักษาความปลอดภัยเหมือนระบบรักษาความปลอดภัยอื่นๆ คือ การใส่รหัส (Encryption) เพื่อป้องกันข้อมูลรั่วไหล ป้องกันการแอบดึงข้อมูลไปใช้

- Vulnerability การค้นหาเพื่อระบุถึง จุดอ่อนของระบบภายในองค์กรนั้น ในบางทีอาจต้องใช้วิธีทางเทคนิคเข้ามาช่วย เพื่อค้นหา จุดอ่อนในเชิง Logical ของระบบ

- Intrusion Detection System ระบบตรวจสอบการบุกรุกเข้าสู่ระบบ ตรวจสอบมักวางไว้ทั้งหน้า firewall และหลัง firewall เพื่อตรวจสอบการบุกรุก และตรวจสอบผลการใช้ firewall

- Intrusion Prevention System ระบบที่คอยตรวจจับการบุกรุกของผู้ที่ไม่ประสงค์ดี รวมไปถึงข้อมูลจำพวกไวรัสด้วย

4. Data Link Layer มีหน้าที่เหมือนกับชั้นอื่น ๆ คือรับและส่งข้อมูล ซึ่งจะรับผิดชอบในการรับส่งข้อมูลและมีการตรวจสอบความถูกต้องของข้อมูลด้วย โดยมีการรักษาความปลอดภัยดังนี้

- Authentication in Distributed System เป็นการตรวจสอบความถูกต้องระบบคอมพิวเตอร์ในเครือข่าย

- Encryption คือ การเปลี่ยนข้อความที่สามารถอ่านได้ (plain text) ไปเป็นข้อความที่ไม่สามารถอ่านได้ (cipher text) เพื่อเหตุผลด้านความปลอดภัย ปัจจุบันการเข้ารหัสมี 2 รูปแบบคือ การเข้ารหัสแบบสมมาตร เป็นการเข้ารหัสแบบใช้กุญแจตัวเดียวกันสำหรับการเข้าและถอดรหัส และการเข้ารหัสแบบอสมมาตร เป็นการเข้ารหัสที่ใช้กุญแจตัวหนึ่งสำหรับการเข้ารหัส และกุญแจอีกตัวหนึ่งสำหรับการถอดรหัส

5. Physical Layer จัดการเชื่อมต่อ และ การส่งสัญญาณทางไฟฟ้า จากผู้ส่ง ไปยังผู้รับ โดยผ่านสื่อกลาง เช่น สายทองแดง คลื่นวิทยุ สายคู่ตีเกลียว และใยแก้วนำแสงเป็นต้น

ดังนั้น พื้นฐานของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศทั่วไปเป็นฐานเนื่องจากในองค์กรส่วนใหญ่จะมีระบบสารสนเทศที่ใช้แบบมีสายและแบบไร้สาย ดังนั้นจะต้องดำเนินการรักษาความมั่นคงปลอดภัยร่วมกัน ซึ่งทุกระบบงานย่อยและระบบงานสารสนเทศต้องมี รวมถึงต้องมีการพิจารณาขั้นตอนต่างๆ การดำเนินการต่างๆ ในระดับบริหารจัดการ และเน้นไปที่การรักษาความมั่นคงปลอดภัยเพื่อให้เกิดประสิทธิภาพสูงสุด

7. สรุป

ผลที่ได้จากการวิจัยการจัดทำกรอบความมั่นคงปลอดภัยสำหรับเครือข่ายเฉพาะบริเวณแบบไร้สายในวิสาหกิจขนาดกลางและขนาดเล็ก โดยอิงมาตรฐาน ISO27001 นั้น ผู้วิจัยได้พัฒนาตัวแบบความมั่นคงปลอดภัยโดยมีวิธีการและเครื่องมือต่างๆ ช่วยในการบริหารจัดการและควบคุมระบบ ซึ่งจะติดตั้งพร้อมกับการจัดทำระบบในครั้งแรก ทั้งนี้เพื่อกรองข้อมูลการจราจรที่วิ่งเข้าออกระบบ และการที่จะรองรับกับระบบธุรกรรมต่างๆ ของ SME ได้ ระบบปฏิบัติการที่ใช้และเว็บเซอร์ฟเวอร์ต้องรองรับการสื่อสารที่ปลอดภัย จะช่วยให้การบริหารจัดการเซิร์ฟเวอร์ที่มีหลายแอพพลิเคชัน และหลายยูสเซอร์ที่ใช้งานพร้อมกันอย่างมีประสิทธิภาพมากขึ้น อย่างไรก็ดี กรอบความมั่นคงปลอดภัยที่ผู้วิจัยได้พัฒนาขึ้นยังช่วยในด้านการป้องกันความมั่นคงปลอดภัยภายในองค์กร SME ซึ่งทำให้ SME ได้ปฏิบัติตามนโยบายที่กำหนดเป็นมาตรฐานในระดับสากล

8. ข้อเสนอแนะ

จากการศึกษาวิจัยเรื่อง กรอบความมั่นคงความปลอดภัยสารสนเทศสำหรับเครือข่ายเฉพาะบริเวณแบบไร้สายสำหรับวิสาหกิจขนาดกลางและขนาดเล็ก ได้มีข้อเสนอแนะในงานวิจัยนี้แบ่งออกเป็น 2 ข้อดังนี้

1. ถ้าผู้ที่สนใจจะนำไปพัฒนาใช้จริงใน SME ควรพิจารณาด้านนโยบายขององค์กรประกอบ และกำหนดนโยบายภายใน SME ให้เหมาะสม

2. ข้อเสนอแนะสำหรับการทำวิจัยในอนาคต งานวิจัยนี้สามารถนำไปประยุกต์ใช้ในด้านระบบความมั่นคงปลอดภัยสารสนเทศสำหรับเครือข่ายเฉพาะบริเวณหรือเครือข่ายบริเวณกว้างอื่นๆ สำหรับหน่วยงานภาครัฐหรือบริษัทที่มีขนาดใหญ่ โดยเปรียบเทียบกับ Defense Information System Agency for the Department of Defense มาประกอบเป็นแนวทางในการปรับใช้

9. รายการอ้างอิง

จตุชัย แพงจันทร์, อนุโชต วุฒิพรพงษ์ , 2551. **เจาะระบบ Network.** พิมพ์ครั้งที่ 2. กรุงเทพฯ: สำนักพิมพ์ บริษัท ไอดีซี อินโฟ ดิสทริบิวเตอร์ เซ็นเซอร์ จำกัด.

ปริญญ์ เสรีพงษ์, 2551. **ISO 27001 Introduction to Information Security Management System ระบบการจัดการความมั่นคงปลอดภัยของสารสนเทศ**. พิมพ์ครั้งที่ 1. กรุงเทพฯ: บริษัท อมรินทร์พริ้นติ้งแอนด์ พับลิชชิ่ง จำกัด (มหาชน).

ภาคภูมิ ปรีชาพานิช, 2550. **"การพัฒนาตัวแบบความมั่นคงปลอดภัยของเว็บเซอร์วิสสำหรับกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร"**. บริหารธุรกิจมหาบัณฑิต สาขาวิชาพาณิชย์อิเล็กทรอนิกส์ มหาวิทยาลัยศรีปทุม.

อนันต์ ผลเพิ่ม, 2550. **แลนไร้สาย (Wireless LAN)**. กรุงเทพฯ : วี พริ้นท์ จำกัด.

International Standard ISO/IEC 27001, 2005. **Information Technology-Security Techniques-Information Security Management Systems-Requirements**. 1st . Switzerland: ISO Copyright office.

United States Defense Information System Agency for the Department of Defense, 2005. Wireless LAN Security Framework **Addendum to the Wireless Security Technical Implementation Guide**, Version 1. United States of America.

United States Department of Homeland Security Washington, D.C. 20528, 2008. **Information Technology (IT) Security Essential Body of Knowledge (EBK)**: A Competency and Functional Framework for IT Security Workforce Development.