แนวทางในการวางนโยบายความมั่นคงปลอดภัยทางสารสนเทศสำหรับวิสาหกิจขนาดกลางและขนาดเล็ก ด้านระบบเครือข่ายไร้สาย
Guidelines for Information Security Management Policy for Small and Medium Sized Enterprises about Wireless LAN

ไกรลาศ สิทธิยะ*

บทคัดย่อ

ปัจจุบันเทคโนโลยีการสื่อสารแบบเครือข่ายเฉพาะบริเวณแบบไร้สาย (Wireless LAN) มีการใช้งานอย่างแพร่หลาย รวมไปถึงวิสาหกิจขนาดกลางและขนาดเล็ก (SMEs) ซึ่งเป็นธุรกิจที่มีความหลากหลายและมีอัตราการเติบโตสูงขึ้นในปัจจุบัน การใช้ระบบไร้สายในองค์กรจะทำให้เพิ่มความสะดวกสบายและลดค่าใช้จ่ายในการติดตั้ง เหมาะสำหรับบุคคลที่เข้ามาเชื่อมต่อข้อมูลหรือใช้งานร่วมกัน ทำให้ต้องคำนึงถึงระบบรักษาความปลอดภัยสารสนเทศสำหรับเครือข่ายเฉพาะบริเวณแบบไร้สาย เนื่องจากธุรกิจประเภท SMEs มักจะมีข้อมูลที่สำคัญเหมือนบริษัทขนาดใหญ่ ซึ่งมีโอกาสเสี่ยงต่อผู้ไม่หวังดีที่ต้องการทำลายให้ข้อมูลเกิดความเสียหายผ่านระบบเครือข่ายไร้สาย ซึ่งแนวทางในการกำหนดนโยบายเพื่อใช้สำหรับวางระบบความมั่นคงปลอดภัยสารสนเทศ คือ มีการกำหนดนโยบายด้านความมั่นคงปลอดภัยสำหรับเครือข่ายเฉพาะบริเวณแบบไร้สายสำหรับวิสาหกิจขนาดกลางและขนาดเล็ก โดยกำหนดกรอบความมั่นคงปลอดภัยสำหรับระบบเครือข่ายไร้สาย การพัฒนาตัวแบบความมั่นคงความปลอดภัยสำหรับเครือข่ายเฉพาะบริเวณแบบไร้สาย โดยพิจารณาตามกรอบมาตรฐาน ISO/IEC 27001 ซึ่งเป็นมาตรฐานที่กำลังได้รับความนิยมอย่างแพร่หลายในปัจจุบัน และกล่าวถึงข้อกำหนดในการจัดทำระบบบริหารจัดการความมั่นคงปลอดภัยหรือ ISMS (Information Security Management System) ให้กับองค์กร

คำสำคัญ

นโยบายความมั่นคงปลอดภัยทางสารสนเทศ วิสาหกิจขนาดกลางและขนาดเล็ก ระบบเครือข่ายไร้สาย

Abstract

Nowadays, the Wireless LAN communication technology has been widely used among small and medium sized enterprises (SMEs) - the varied and high growth firms. The use of Wireless LAN system in the organization is more convenient and suitable for people to link the information and work together as

* อาจารย์ประจำสาขาวิชาคอมพิวเตอร์ธุรกิจ คณะบริหารธุรกิจ มหาวิทยาลัยฟาร์อีสเทอร์น
E-mail: krailas@feu.edu

well as decreases the installation payment. The Information Security Management System for Wireless LAN is considered because most of SMEs business often has the crucial information like the big business that is very risky to others who want to damage the information via Wireless LAN. The policy making for the information security management system is to set the information security management system for Wireless LAN of SMEs. Development network security according to standard ISO/IEC 27001 is very popular and refers to the regulation of information Security Management System (ISMS) for the organization.

Keywords

Information Security Management Policy, Small and Medium Sized Enterprises, Wireless LAN

บทนำ

วิสาหกิจขนาดกลางและขนาดเล็ก (Small and Medium Sized Enterprises: SMEs) มีความหมายรวมถึงอุตสาหกรรมการผลิต กิจการค้าส่งและค้าปลีก และกิจการการบริการ ซึ่งเกณฑ์ในการจัดอุตสาหกรรม เป็นอุตสาหกรรมขนาดใหญ่ กลาง หรือ เล็กนั้น มีหลายวิธี แต่โดยทั่วไปจะใช้ จำนวนคนงาน (ขนาดการจ้างงาน) จำนวนเงินลงทุน มูลค่าทรัพย์สิน จำนวนยอดขาย หรือรายได้เป็นเกณฑ์ ว่ากิจการใดจะเข้าข่ายเป็น SMEs หรือไม่ กระทรวงอุตสาหกรรมได้กำหนดเกณฑ์การแบ่งประเภทของวิสาหกิจขนาดกลางและขนาดเล็ก คือ มีจำนวนคนงานไม่เกิน 50 คน จำนวนเงินลงทุนไม่เกิน 20 ล้านบาท ส่วนวิสาหกิจขนาดกลาง คือ มีจำนวนคนงานระหว่าง 50 ถึง 200 คน จำนวนเงินลงทุนระหว่าง 20 ถึง 200 ล้านบาท (กระทรวงอุตสาหกรรม, ม.ป.ป.)

ไอที และ ไอซีที (Information and Communication Technology) ประกอบด้วยเทคโนโลยีสำคัญหลายอย่าง เช่น เทคโนโลยีคอมพิวเตอร์ เทคโนโลยีการสื่อสารโทรคมนาคม เทคโนโลยีเครือข่ายคอมพิวเตอร์ เทคโนโลยีอินเทอร์เน็ต เทคโนโลยีการพิมพ์ ฯลฯ ในภาพรวมกล่าวได้ว่าการใช้ไอทีในงานธุรกิจ จะมีการใช้งานเพื่อเพิ่มความสะดวกแก่ผู้ปฏิบัติงาน (สานนท์ ฉิมมณี และ ภส จันทรศิริ, 2553) เช่น การใช้คอมพิวเตอร์ในงานพิมพ์เอกสารที่เรียกว่างานประมวลคำ (Word Processing) เพื่อการทำงานด้านเอกสาร หน้าเว็บไซต์บนระบบอินเทอร์เน็ต และยังเป็นส่วนหนึ่งของระบบสำนักงานอัตโนมัติ (Office Automation) เป็นการใช้งานคอมพิวเตอร์ในงานจัดทำและรับส่งเอกสารสำหรับบริษัทและหน่วยงาน เมื่อโลกรู้จักใช้ระบบอินเทอร์เน็ตและเทคโนโลยีเว็บไซต์ แนวทางการพัฒนาระบบต่างๆ ก็เปลี่ยนไป งานประยุกต์เริ่มเปลี่ยนเป็นระบบเว็บไซต์ (Web Based System) มากขึ้น ดังนั้น การคำนึงถึงระบบรักษาความปลอดภัยสารสนเทศสำหรับเครือข่ายเฉพาะบริเวณแบบไร้สายจึงมีความสำคัญ เนื่องจากธุรกิจขนาดเล็กมักมีข้อมูลสำคัญเช่นเดียวกับบริษัทขนาดใหญ่ อาทิ ข้อมูลทางการเงินและบัญชี ข้อมูลลูกค้า เป็นต้น จึงต้องการการรักษาความปลอดภัยของข้อมูลในประเภทต่างๆ เช่น มีการรักษาความปลอดภัยของข้อมูลจากไวรัสหรือภัยคุกคาม การรับรองว่าจะมีการเก็บข้อมูลไว้เป็นความลับและผู้มีสิทธิเท่านั้นจึงจะเข้าถึงข้อมูลได้ การรับรองว่าข้อมูลจะไม่ถูกเปลี่ยนแปลงหรือทำลายไม่ว่าจะเป็นอุบัติเหตุหรือโดยเจตนา การรับรองว่าข้อมูลและบริการการสื่อสารมีความพร้อมใช้งานในเวลาที่ต้องการ เพราะธุรกิจขนาดเล็กจำเป็นต้องติดต่อสื่อสารกับลูกค้าโดยตรงอย่างสม่ำเสมอ (เศรษฐพงศ์ มะลิสุวรรณ, ม.ป.ป.) ดังนั้น การสร้างระบบความมั่นคงปลอดภัยให้แก่สารสนเทศ

จึงเป็นสิ่งจำเป็นสำหรับธุรกิจขนาดเล็กด้วยเช่นกัน โดยบทความนี้ได้ทำการศึกษาและนำเสนอนโยบายความมั่นคงปลอดภัยสำหรับระบบเครือข่ายเฉพาะบริเวณแบบไร้สายว่าควรออกแบบให้มีความเหมาะสมกับความต้องการของธุรกิจและตามลักษณะการใช้งานของผู้ใช้ได้อย่างไร

ระบบเครือข่ายไร้สายและเสาอากาศส่งสัญญาณ

อรรณพ สุวัฒนพิเศษ (ม.ป.ป.) กล่าวว่า ระบบเครือข่ายไร้สาย (WLAN = Wireless Local Area Network) คือ ระบบการสื่อสารข้อมูลที่มีความคล่องตัวมาก ซึ่งอาจนำมาใช้ทดแทนหรือเพิ่มเติมจากระบบเครือข่าย LAN (Local Area Network) ที่ใช้สายแบบดั้งเดิม โดยใช้การส่งคลื่นความถี่วิทยุ (Radio Frequency: RF) และคลื่นอินฟราเรด (Infrared) ในการรับและส่งข้อมูลระหว่างคอมพิวเตอร์แต่ละเครื่อง ผ่านอากาศ ทะลุกำแพง เพดาน หรือสิ่งก่อสร้างอื่นๆ โดยปราศจากความต้องการของการเดินสาย นอกจากนั้นระบบเครือข่ายไร้สายก็ยังมีคุณสมบัติครอบคลุมทุกอย่างเช่นเดียวกับระบบ LAN แบบใช้สาย ที่สำคัญ คือ การที่ไม่ต้องใช้สายทำให้การเคลื่อนย้ายการใช้งานทำได้โดยสะดวก ไม่เหมือนระบบ LAN แบบใช้สาย ที่ต้องใช้เวลาและการลงทุนในการปรับเปลี่ยนตำแหน่งการใช้งานเครื่องคอมพิวเตอร์

ปัจจุบันเราเข้าสู่ยุคแห่งการติดต่อสื่อสารแบบไร้สายด้วยเทคโนโลยีต่างๆ เช่น โทรศัพท์เคลื่อนที่กลายเป็นสิ่งจำเป็นต่อการดำเนินธุรกิจและการใช้ชีวิตประจำวัน ความต้องการรับรู้ข้อมูลและการรับบริการต่างๆ มีความจำเป็นสำหรับนักธุรกิจ เทคโนโลยีที่สนองต่อความต้องการเหล่านั้น มีมากมาย ยกตัวอย่าง นักธุรกิจที่มีความจำเป็นต้องใช้งานเครื่องคอมพิวเตอร์นอกสถานที่ที่ทำงานปกติ ทั้งการนำเสนองานยังบริษัทลูกค้า หรือการนำเครื่องคอมพิวเตอร์พกพาไปงานประชุมสัมมนาต่างๆ มีความจำเป็นที่จะต้องเชื่อมต่อเข้ากับเครือข่ายคอมพิวเตอร์ไม่ว่าจะเป็นเครือข่ายคอมพิวเตอร์ขององค์กรซึ่งอยู่ห่างออกไปหรือเครือข่ายคอมพิวเตอร์สาธารณะ ซึ่งเทคโนโลยีเครือข่ายไร้สายสามารถอำนวยความสะดวกให้กับบุคคลเหล่านี้ได้ ซึ่งในปัจจุบันได้มีการเปิดให้บริการเชื่อมต่อเครือข่ายอินเตอร์เน็ตแบบไร้สายตามสนามบินใหญ่ทั่วโลก และนำมาใช้งานแพร่หลายในห้างสรรพสินค้า และโรงแรมต่างๆ แล้ว (เศรษฐพงค์ มะลิสุวรรณ, ม.ป.ป.)

1. **ระบบเครือข่ายไร้สาย**

1.1 ประโยชน์ของระบบเครือข่ายไร้สาย มีดังนี้ (Gary, Alice & Alexis, 2002)

1) Mobility Improves Productivity & Service: มีความคล่องตัวสูง ดังนั้นไม่ว่าเราจะเคลื่อนที่ไปที่ไหน หรือเคลื่อนย้ายคอมพิวเตอร์ไปตำแหน่งใด ก็ยังมีการเชื่อมต่อกับเครือข่ายตลอดเวลา ตราบใดที่ยังอยู่ในระยะการส่งข้อมูล

2 Installation Speed and Simplicity: สามารถติดตั้งได้ง่ายและรวดเร็ว เพราะไม่ต้องเสียเวลาติดตั้งสายเคเบิล

3) Installation Flexibility: สามารถขยายระบบเครือข่ายได้ง่าย โดยใช้พีซีการ์ด (PC Card) มาต่อเข้ากับคอมพิวเตอร์โน๊ตบุ๊ค หรือ ใช้ PC Card ต่อเข้าสู่เครือข่ายได้ทันที

4) Reduced Cost- of-Ownership: ลดค่าใช้จ่ายโดยรวมที่ผู้ลงทุนต้องลงทุน เพราะในระยะยาวแล้วระบบเครือข่ายไร้สายไม่จำเป็นต้องเสียค่าบำรุงรักษา และด้วยการติดตั้งที่ง่ายจึงทำให้การลงทุนเพื่อการขยายเครือข่ายใช้เงินลงทุนต่ำกว่าการลงทุนเพื่อการติดตั้งเครือข่ายแบบใช้สาย

5) Scalability: เครือข่ายไร้สายทำให้องค์กรสามารถปรับขนาดและความเหมาะสมได้ง่าย เพราะสามารถโยกย้ายตำแหน่งการใช้งาน โดยเฉพาะระบบที่มีการเชื่อมระหว่างจุดต่อจุด เช่น ระหว่างอาคารกับอาคาร

1.2 รูปแบบการเชื่อมต่อของระบบเครือข่ายไร้สาย มีดังนี้ (Gary, Alice & Alexis, 2002)

1) Peer-to-Peer (Ad Hoc Mode) : รูปแบบการเชื่อมต่อระบบ LAN ไร้สายแบบ Peer to Peer เป็นลักษณะการเชื่อมต่อแบบโครงข่ายโดยตรงระหว่างเครื่องคอมพิวเตอร์ จำนวน 2 เครื่องหรือมากกว่า เป็นการใช้งานร่วมกันของ Wireless Adapter Cards โดยไม่จำเป็นต้องเชื่อมต่อกับเครือข่ายแบบใช้สาย เครื่องคอมพิวเตอร์แต่ละเครื่องจะมีความเท่าเทียมกัน สามารถทำงานของตนเองได้และขอใช้บริการเครื่องอื่นได้ เหมาะสำหรับการนำมาใช้งานเพื่อจุดประสงค์ในด้านความรวดเร็วหรือติดตั้งได้โดยง่ายเมื่อไม่มีโครงสร้างพื้นฐานที่จะรองรับ เช่น ในศูนย์ประชุม หรือ การประชุมที่จัดขึ้นนอกสถานที่ เป็นต้น

2) Client/server (Infrastructure Mode): ระบบเครือข่ายไร้สายแบบ Client / Server หรือ Infrastructure Mode เป็นการรับส่งข้อมูลโดยอาศัย Access Point (AP) หรือเรียกว่า “Hot Spot” ทำหน้าที่เป็นสะพานเชื่อมต่อระหว่างระบบเครือข่ายแบบใช้สายกับเครื่องคอมพิวเตอร์ลูกข่าย (Client) โดยกระจายสัญญาณคลื่นวิทยุเพื่อ รับ-ส่งข้อมูลเป็นรัศมีโดยรอบ เครื่องคอมพิวเตอร์ที่อยู่ในรัศมีของ AP จะกลายเป็นเครือข่ายกลุ่มเดียวกันทันที เครื่องคอมพิวเตอร์สามารถติดต่อกัน หรือ ติดต่อกับ Server เพื่อแลกเปลี่ยนและค้นหาข้อมูลได้ โดยไม่ต้องติดต่อผ่าน AP เท่านั้น ซึ่ง AP 1 จุด สามารถให้บริการเครื่องลูกข่ายได้ตั้งแต่ 15 - 50 เครื่อง เหมาะสำหรับการนำไปขยายเครือข่ายหรือใช้ร่วมกับระบบเครือข่ายแบบใช้สาย เช่น ในสำนักงาน ห้องสมุด หรือในห้องประชุม เพื่อช่วยเพิ่มประสิทธิภาพในการทำงานให้มากขึ้น

3) Multiple Access Points and Roaming: โดยทั่วไปแล้วการเชื่อมต่อสัญญาณระหว่างเครื่องคอมพิวเตอร์ กับ Access Point ของเครือข่ายไร้สายจะอยู่ในรัศมีประมาณ 500 ฟุต ภายในอาคาร และ 1,000 ฟุต ภายนอกอาคาร หากสถานที่ที่ติดตั้งมีขนาดกว้างมากๆ เช่น คลังสินค้า บริเวณภายในมหาวิทยาลัย สนามบิน จะต้องมีการเพิ่มจุดการติดตั้ง AP ให้มากขึ้น เพื่อให้การรับส่งสัญญาณในบริเวณเครือข่ายขนาดใหญ่เป็นไปอย่างครอบคลุมทั่วถึง

4) Use of an Extension Point: กรณีที่โครงสร้างของสถานที่ติดตั้งเครือข่ายแบบไร้สายมีปัญหา ผู้ออกแบบระบบ อาจจะใช้ Extension Points ที่มีคุณสมบัติเหมือนกับ Access Point แต่ไม่ต้องผูกติดไว้กับเครือข่ายไร้สาย แต่เป็นส่วนที่ใช้เพิ่มเติมในการรับส่งสัญญาณ

5) The Use of Directional Antennas: ระบบเครือข่ายไร้สายแบบนี้เป็นแบบใช้เสาอากาศในการรับส่งสัญญาณระหว่างอาคารที่อยู่ห่างกัน โดยการติดตั้งเสาอากาศในแต่ละอาคารเพื่อส่งและรับสัญญาณระหว่างกัน

2. **เสาอากาศ** (Antenna)

อรรณพ สุวัฒนพิเศษ (ม.ป.ป.) กล่าวถึงหน้าที่หลักของเสาอากาศ คือ การแปลงสัญญาณวิทยุไปเป็นคลื่นแม่เหล็กไฟฟ้าเพื่อส่งสัญญาณออกอากาศไปยังภาคส่งคลื่นวิทยุ และทำหน้าที่ในการแปลงคลื่นแม่เหล็กไฟฟ้าที่อยู่ในอากาศไปเป็นสัญญาณวิทยุเพื่อส่งให้ภาครับคลื่นวิทยุทำการดีโมดูเลท (Demodulate) ข้อมูลออกจากสัญญาณวิทยุต่อไป เสาอากาศจัดเป็นอุปกรณ์ที่มีความสำคัญมาก ถ้าเสาอากาศไม่มีคุณภาพอาจจะส่งสัญญาณไม่ออกหรือ ไม่สามารถรับสัญญาณได้ซึ่งมีตัวแปรหลายๆ ค่าที่ใช้บอกคุณสมบัติของเสาอากาศ เช่น เกน (Gain) หรือ อัตราขยายเป็นตัวบอกว่าเสาอากาศนี้มีคุณสมบัติในการแปลงคลื่นแม่เหล็กไฟฟ้ามาเป็นสัญญาณไฟฟ้าได้ดีเพียงใด ค่าบีมวิธ (Beam Width) ซึ่งบอกรูปร่างลักษณะการกระจายคลื่นว่า เป็น รูปแบบไหน การเลือกใช้เสาอากาศที่มีทิศทางจะช่วยกำหนดรูปแบบการกระจายคลื่นได้ดีกว่า และการอ่านค่าจากเครื่องวัดเสาอากาศ (SWR Metter) ซึ่งมีตัวเลขที่บอกถึงคลื่นที่สะท้อนกลับมาเมื่อเราส่งสัญญานออกอากาศไป สำหรับประเภทเสามีอยู่ 5 ประเภท ได้แก่

2.1 เสาอากาศแบบ Omni ใช้สำหรับเชื่อมต่อระบบเครือข่ายไร้สายภายนอกอาคาร แบบ Point to Multi-Point เหมาะสำหรับการกระจายสัญญาณรอบทิศทาง หรือการทำจุดกระจายสัญญาณไร้สายสาธารณะ (Wi-Fi Hot Spot)

2.2 เสาอากาศแบบ Panel ใช้สำหรับเชื่อมต่อระบบเครือข่ายไร้สายภายนอกอาคาร แบบ Point to Multi-Point เหมาะสำหรับการเชื่อมต่อระหว่างอาคารที่ตั้งกระจายตัวอยู่ในบริเวณเดียวกัน แต่มีระยะไม่ห่างกันมาก และต้องการควบคุมทิศทางของสัญญาณไร้สาย

2.3 เสาอากาศแบบ Sector ใช้สำหรับเชื่อมต่อระบบเครือข่ายไร้สายภายนอกอาคาร แบบ Point to Multi-Point และต้องการควบคุมทิศทางสัญญาณในแนวระนาบ เหมาะสำหรับการเชื่อมต่ออาคารที่กระจายตัวอยู่ในบริเวณเดียวกันและอาคารมีความสูงใกล้เคียงกัน

2.4 เสาอากาศแบบ Grid ใช้สำหรับเชื่อมต่อระบบเครือข่ายไร้สายภายนอกอาคาร แบบ Point to Point เหมาะสำหรับการเชื่อมต่อระบบเครือข่ายไร้สายจากอาคารสู่อาคารและต้องการควบคุมทิศทางของสัญญาณ

2.5 เสาอากาศแบบ Yagi ใช้สำหรับเชื่อมต่อระบบเครือข่ายไร้สายภายนอกอาคาร แบบ Point to Point เหมาะสำหรับการใช้งานกับ Client ที่ต้องการเชื่อมต่อกับ Access Point ในระยะไกลโดยเน้นการกระจายสัญญาณเป็นเส้นตรง

หลักการพื้นฐานการรักษาความปลอดภัยในองค์กร

ในการรักษาความมั่นคงปลอดภัย ประกอบด้วยการรักษาคุณสมบัติพื้นฐาน 3 ประการ ได้แก่ ความลับ (Confidentiality) บูรณภาพ (Integrity) และความพร้อมใช้งาน (Availability) ซึ่งมีคำจำกัดความที่สำคัญ ดังนี้ (มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ ประจำปี 2555, 2555)

1. เทคโนโลยีสารสนเทศ (IT) หมายถึง เทคโนโลยีสำหรับการประมวลผล ครอบคลุมถึงการรับส่ง แปลง ประมวลผล และสืบค้นสารสนเทศ โดยมีองค์ประกอบ 3 ส่วน คือ คอมพิวเตอร์ การสื่อสารและสารสนเทศ ซึ่งต้องอาศัยการทำงานร่วมกัน

2. ความลับ (Confidentiality) คือ การรับรองว่าจะมีการเก็บรักษาข้อมูลไว้เป็นความลับและจะมีเพียงผู้มีสิทธิเท่านั้นที่จะสามารถเข้าถึงข้อมูลเหล่านั้นได้

3. บูรณภาพ (Integrity) คือ การรับรองว่าข้อมูลจะไม่ถูกกระทำการใดๆ อันมีผลให้เกิดการเปลี่ยนแปลงหรือแก้ไขจากผู้ซึ่งไม่มีสิทธิ ไม่ว่าการกระทำนั้นจะมีเจตนาหรือไม่

4. ความพร้อมใช้งาน (Availability) คือ การรับรองว่าข้อมูลหรือระบบเทคโนโลยีสารสนเทศทั้งหลายพร้อมที่จะให้บริการในเวลาที่ต้องการใช้งาน

5. การพิสูจน์ฝ่าย (Authentication) คือ การตรวจสอบและการพิสูจน์สิทธิ์การขอเข้าใช้ระบบของผู้ใช้บริการจากรายชื่อผู้มีสิทธิสำหรับอุปกรณ์ไอที รวมถึงแอพพลิเคชัน

6. การพิสูจน์สิทธิ์ (Authorization) คือ การตรวจสอบว่า บุคคล อุปกรณ์ หรือแอพพลิเคชัน ได้รับอนุญาตให้ดำเนินการอย่างหนึ่งอย่างใดต่อระบบสารสนเทศหรือไม่

7. การเก็บสำรองข้อมูล (Data Backup) คือ ในระหว่างการเก็บสำรอง สำเนาของชุดข้อมูลปัจจุบันจะถูกสร้างขึ้นมา เพื่อป้องกันการสูญหาย

8. การปกป้องข้อมูล (Data Protection) คือ การป้องกันข้อมูลส่วนบุคคลต่อการประสงค์ร้ายของบุคคลที่สาม

9. การรักษาความมั่นคงปลอดภัยของข้อมูล (Data Security) คือ การป้องกันข้อมูลในบริบทของการรักษาความลับ บูรณภาพ และความพร้อมใช้งานของข้อมูล ซึ่งสามารถใช้แทนการรักษาความมั่นคงปลอดภัยของสารสนเทศได้

10. การประเมินความเสี่ยง หรือการวิเคราะห์ความเสี่ยง (Risk Assessment or Analysis) ของระบบสารสนเทศ คือ การตรวจสอบโอกาสของผลลัพธ์ใดๆ ที่ไม่พึงประสงค์ต่อระบบสารสนเทศ และผลเสียที่อาจจะเกิดขึ้นตามมาได้

11. นโยบายด้านความมั่นคงปลอดภัย (Security Policy) คือ นโยบายที่แสดงเป้าหมายที่จะต้องปกป้องและขั้นตอนทั่วไปของกระบวนการรักษาความมั่นคงปลอดภัยในบริบทของความต้องการอย่างเป็นทางการขององค์กร

แนวทางการกำหนดนโยบายความมั่นคงปลอดภัยสารสนเทศสำหรับเครือข่าย

มาตรฐาน ISO/IEC 27001 เป็นมาตรฐานสากลที่ได้รับการยอมรับและนำไปใช้อย่างแพร่หลายในระดับนานาชาติรวมถึงประเทศไทย ซึ่งกล่าวถึงข้อกำหนดในการจัดทำระบบบริหารจัดการความมั่นคงปลอดภัยหรือ (Information Security Management System: ISMS) ให้กับองค์กร (มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ ประจำปี, 2555) มีวัตถุประสงค์เพื่อให้องค์กรสามารถบริหารจัดการความมั่นคงปลอดภัยได้อย่างมีระบบเพียงพอเหมาะสมต่อการดำเนินธุรกิจขององค์กร โดยมีสาระสำคัญอยู่ 4 ประเด็น ได้แก่ (1) ขอบเขต (Scope) (2) ศัพท์เทคนิคและนิยาม (Terms and Definitions) (3) โครงสร้างของมาตรฐาน (Structure of This Standard) (4) การประเมินความเสี่ยงและการจัดการกับความเสี่ยง ลด/ โอนย้าย/ ยอมรับความเสี่ยง (Risk Assessment and Treatment) (Gary, Alice & Alexis, 2002) นอกจากนี้ ยังประกอบไปด้วยวงจรบริหารจัดการความมั่นคงปลอดภัยตามขั้นตอน Plan-Do-Check-Act (P-C-D-A) และใช้แนวทางการประเมินความเสี่ยงมาประกอบการพิจารณาหาวิธีการหรือมาตรการเพื่อป้องกัน ลดความเสี่ยง และรักษาสารสนเทศที่มีค่าขององค์กรให้มีความมั่นคงปลอดภัยที่เหมาะสม จากการศึกษารวบรวมข้อมูล สามารถสรุปแนวทางในการกำหนดนโยบาย ได้ 2 ประเด็น ดังนี้

1. การกำหนดนโยบายด้านความมั่นคงปลอดภัยสำหรับเครือข่ายเฉพาะบริเวณแบบไร้สาย สำหรับวิสาหกิจขนาดกลางและขนาดเล็กด้านกรอบความมั่นคงปลอดภัยสำหรับระบบเครือข่ายไร้สาย

2. การพัฒนาตัวแบบความมั่นคงความปลอดภัยสำหรับเครือข่ายเฉพาะบริเวณแบบไร้สายสำหรับวิสาหกิจขนาดกลางและขนาดเล็ก การพัฒนาตัวแบบความมั่นคงปลอดภัยซึ่งมีคุณสมบัติและเครื่องมือต่าง ๆ ที่ช่วยในการบริหารจัดการและควบคุมระบบ จะช่วยให้การบริหารจัดการเซิร์ฟเวอร์ที่มีหลายแอพพลิเคชันและหลายยูสเซอร์ใช้งานพร้อมกัน นอกจากนี้ยังช่วยในการป้องกันข้อมูลตามนโยบายที่กำหนด ซึ่งจะติดตั้งพร้อมกับระบบเพื่อกรองข้อมูลการจราจรที่วิ่งเข้าออกบนระบบเครือข่าย (สานนท์ ฉิมมณี และ ภส จันทรศิริ, 2553)

กรอบความมั่นคงปลอดภัยสารสนเทศเครือข่ายเฉพาะบริเวณแบบไร้สายสำหรับวิสาหกิจขนาดกลางและขนาดเล็กที่อ้างอิงตามมาตรฐาน ISO/IEC 27001 มีรายละเอียดในแต่ละชั้น ดังนี้ (ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย, ม.ป.ป.)

ตารางที่ 1

สรุปแนวทางการวางนโยบายสำหรับเครือข่ายเฉพาะบริเวณแบบไร้สาย และการพัฒนาตัวแบบความมั่นคงความปลอดภัย สำหรับวิสาหกิจขนาดกลางและขนาดเล็ก

หัวข้อหลัก	หัวข้อย่อย	คำอธิบาย
1. การกำหนดนโยบายด้านความมั่นคงปลอดภัยสำหรับเครือข่ายเฉพาะบริเวณแบบไร้สายสำหรับวิสาหกิจขนาดกลางและขนาดเล็ก	1.1 ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (Human Resources Security)	- การสร้างความมั่นคงปลอดภัยก่อนการจ้างงาน (Prior to Employment) - การสร้างความมั่นคงปลอดภัยระหว่างการจ้างงาน (During Employment) ควรจะให้ความสำคัญจุดนี้ให้มากโดยมีการจำกัดการเข้าถึงของแต่ละคน - การสิ้นสุดหรือการเปลี่ยนการจ้างงาน (Termination or Change of Employment) เมื่อมีการเลิกจ้างควรมีระบบลบข้อมูล หรือ รหัสเพื่อป้องกันการเข้าถึงระบบ
	1.2 ความมั่นคงปลอดภัยที่เกี่ยวข้องกับกระบวนการทำงาน (Process Resources Security)	- นโยบายความมั่นคงปลอดภัยของสารสนเทศ (Information Security Policy) นโยบายนี้เป็นกรอบในการกำหนดวัตถุประสงค์ มาตรการด้านความมั่นคงปลอดภัย รวมถึงแนวทางการบริหารความเสี่ยง และที่สำคัญนโยบายต้องให้ความสำคัญต่อการปฏิบัติตามกฎหมาย กฎระเบียบ สัญญาและข้อตกลงร่วมกัน - โครงสร้างด้านความมั่นคงปลอดภัยของระบบสารสนเทศสำหรับองค์กร (Organization of Information Security) ควรมีการวางโครงสร้างชัดเจนในการทำงาน - นโยบายการกำหนดมาตรการการป้องกันทรัพย์สินขององค์กร

หัวข้อหลัก	หัวข้อย่อย	คำอธิบาย
1. การกำหนดนโยบายด้านความมั่นคงปลอดภัยสำหรับเครือข่ายเฉพาะบริเวณแบบไร้สายสำหรับวิสาหกิจขนาดกลางและขนาดเล็ก	1.3 ความมั่นคงปลอดภัยที่เกี่ยวข้องกับเทคโนโลยี (Technology Resources Security)	- 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
2. การพัฒนาตัวแบบความมั่นคงปลอดภัยสำหรับเครือข่ายเฉพาะบริเวณแบบไร้สาย สำหรับวิสาหกิจขนาดกลางและขนาดเล็ก การพัฒนาตัวแบบความมั่นคงปลอดภัยมีคุณสมบัติและเครื่องมือต่าง ๆ	2.1 Application Layer เป็นจุดเชื่อมต่อระหว่างแอพพลิเคชันของผู้ใช้กับกระบวนการการสื่อสารผ่านเครือข่าย Layer นี้อาจจะถือได้ว่าเป็น Layer ที่เริ่มกระบวนการติดต่อสื่อสาร	- นโยบายความมั่นคงปลอดภัยของสารสนเทศ (Information Security Policy) - นโยบายการสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม (Physical and Environmental Security) - นโยบายการบริหารจัดการด้านการสื่อสารและเครือข่ายสารสนเทศขององค์กร (Communicational Procedures and Responsibilities) - นโยบายการควบคุมอุปกรณ์สื่อสารประเภทพกพา ปัจจุบันมีอุปกรณ์พกพาที่สามารถเชื่อมต่อไร้สายเพิ่มมากขึ้น ต้องมีการควบคุมการจำกัดการเข้าถึงมากขึ้น - การปฏิบัติตามนโยบาย - Maintaining Security While Routing Between Multiple การป้องกันความปลอดภัยต้องป้องกันทุกๆ Layer เพราะผู้โจมตีอาจเลือก Layer ที่สามารถโจมตีได้ง่ายหรือมีจุดอ่อน - Unauthorized Access ต้องจำกัดผู้ใช้งาน จำนวนผู้ใช้และการเข้าถึงข้อมูล คือ กำหนดสิทธิ์ใช้งาน - Parameter Manipulation/Malicious Input มีการส่ง Parameter หรือ Input ที่เป็นอันตรายจากผู้ไม่ประสงค์ดี เช่น SQL Injection เป็นต้น - Network Eavesdropping and Message Replay ถ้าข้อมูลไม่ถูกใส่รหัส 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

หัวข้อหลัก	หัวข้อย่อย	คำอธิบาย
2. การพัฒนาตัวแบบความมั่นคงปลอดภัยสำหรับเครือข่ายเฉพาะบริเวณแบบไร้สาย สำหรับวิสาหกิจขนาดกลางและขนาดเล็ก การพัฒนาตัวแบบความมั่นคงปลอดภัยมีคุณสมบัติและเครื่องมือต่าง ๆ	2.2. Transport Layer รับผิดชอบในการเคลื่อนย้ายข้อมูลระหว่างขั้นตอนของผู้รับ และขั้นตอนของผู้ส่ง ในที่นี้มีการรักษาความปลอดภัย	- Access Control เป็นวิธีการเข้ารหัสข้อมูลที่จะนำมาใช้ในการป้องกันความลับของข้อมูลได้เป็นอย่างดี แต่ไม่สามารถที่จะป้องกันการปลอมแปลงเข้ามาในระบบได้ ส่วนวิธีที่ใช้ในการป้องกันการปลอมแปลงการเข้าระบบ การป้องกันการเรียกเข้าในระบบโดยไม่ได้รับอนุญาต เป็นการกำหนดระดับสิทธิในการเข้าถึงระบบในการเข้าถึงข้อมูลต่าง ๆ กัน
	2.3 Network Layer จะรับผิดชอบในการจัดเส้นทางให้กับข้อมูลระหว่างสถานีส่งและสถานีรับ โดยมีระบบการรักษาความปลอดภัย	- IP Security จะมีระบบรักษาความปลอดภัยเหมือนระบบรักษาความปลอดภัยอื่นๆ คือ การใส่รหัสเพื่อป้องกันข้อมูลรั่วไหล ป้องกันการแอบดึงข้อมูลไปใช้ - Vulnerability การค้นหาเพื่อระบุถึงจุดอ่อนของระบบภายในองค์กรนั้น ในบางทีอาจต้องใช้วิธีทางเทคนิคเข้ามาช่วยเพื่อค้นหาจุดอ่อนในเชิง Logical ของระบบ - Intrusion Detection System ระบบตรวจสอบการบุกรุกเข้าสู่ระบบ ตรวจสอบมักวางไว้ทั้งหน้า Firewall และหลัง Firewall เพื่อตรวจสอบการบุกรุกและตรวจสอบผลการใช้ Firewall - Intrusion Prevention System : IPS หมายถึง ระบบที่ใช้ป้องกันการบุกรุก เป็นอุปกรณ์ที่อยู่ใน Network เพื่อทำหน้าที่ป้องกันการบุกรุก หรือโจมตีทางระบบเครือข่ายต่างๆ เช่น พวกการโจมตีระบบฐานข้อมูล (Database Attack) หรือโจมตีตัวเว็บเซิฟเวอร์ (Web Server Attack)

สรุป

ปัจจุบันเทคโนโลยีสารสนเทศและการสื่อสารได้เข้ามามีบทบาทสำคัญต่อการดำเนินชีวิตของมนุษย์และก่อให้เกิดการเปลี่ยนแปลงกับสังคมมนุษย์อย่างมากมายไม่ว่าจะเป็นการเปลี่ยนแปลงในการดำเนินชีวิตประจำวัน โดยมีการใช้ระบบสารสนเทศผ่านเครือข่ายไร้สายซึ่งมีความคล่องตัวสูง ติดตั้งง่าย ขยายเครือข่ายง่าย ลดค่าใช้จ่าย และสามารถปรับขนาดความเหมาะสมให้เข้ากับองค์กร สามารถเลือกอุปกรณ์เสาสัญญาณที่เหมาะสมกับสถานที่ติดตั้ง รวมทั้งคำนึงถึงรูปแบบการเชื่อมต่อของระบบเครือข่ายไร้สายในแบบต่างๆ แต่ในขณะเดียวกันการใช้ระบบไร้สายจำเป็นต้องคำนึงถึงเรื่องระบบความปลอดภัยของเครือข่ายเป็นอย่างมาก โดยเฉพาะวิสาหกิจขนาดกลางและขนาดเล็ก ควรมีการวางนโยบายและกรอบความมั่นคงปลอดภัยสารสนเทศเครือข่ายเฉพาะบริเวณแบบไร้สายโดยอ้างอิงตามมาตรฐาน ISO / IEC 27001

เอกสารอ้างอิง

กระทรวงอุตสาหกรรม. (ม.ป.ป.). **การจำแนกประเภทของวิสาหกิจขนาดย่อมและขนาดกลาง**. สืบค้นเมื่อวันที่ 10 มกราคม 2558, จาก http://www. Industry.go.th/industry/index.php?option=com_k2 &view=item &layout=item&id=737 &site = psd& cat_id=282.

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ ประจำปี 2555. (2555). กรุงเทพฯ: ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ.

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย. (ม.ป.ป.). **บทความ Cyber Threats 2013**. สืบค้นเมื่อวันที่ 10 มกราคม 2558, จาก https://www.thaicert.or.th/downloads/files /Cyber_Security Threats _2013.pdf.

เศรษฐพงค์ มะลิสุวรรณ. (ม.ป.ป.). **การจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ**. สืบค้นเมื่อ 22 พฤศจิกายน 2553, จาก http://www.our-teacher.com/our-teacher/Military% 20Men torship/20-IT%20 Risk%20 Management.pdf.

สานนท์ ฉิมมณี และ ภส จันทรศิริ. (2553). **เอกสารประกอบการฝึกอบรมโครงการเสริมสร้างศักยภาพบุคลากร ICT ไทยระยะที่ 1 หลักสูตรผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยของระบบเครือข่ายและคอมพิวเตอร์ ระดับที่ 3**. กรุงเทพฯ: สำนักส่งเสริมอุตสาหกรรมเทคโนโลยีสารสนเทศ กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร.

อรรณพ สุวัฒนพิเศษ. (ม.ป.ป.). **ระบบเครือข่ายไร้สาย (Wireless LAN)**. สืบค้นเมื่อวันที่ 10 มกราคม 2558, จาก https://www.thaicyberpoint.com/ford/blog/id/194/

Gary, S.; Alice, G. & Alexis, F. (2002). **Risk Management Guide for Information Technology Systems**. n.p.: National Institute of Standards and Technology.