การพัฒนาระบบการจัดการความมั่นคงปลอดภัยบนระบบเครือข่ายคอมพิวเตอร์สำหรับมหาวิทยาลัยราชภัฏสวนดุสิต

The Development of a Computer Network Security Management System for Suan Dusit Rajabhat University, Thailand.

จิตติมา เทียมบุญประเสริฐ[1]และ กว้าน สีตะธนี[2]

[1]บัณฑิตวิทยาลัย มหาวิทยาลัยราชภัฏสวนดุสิต

[2]ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ

E-Mail : jittima_tia@dusit.ac.th

บทคัดย่อ

การวิจัยนี้มีวัตถุประสงค์เพื่อการพัฒนาระบบการจัดการความมั่นคงปลอดภัยบนระบบเครือข่ายคอมพิวเตอร์สำหรับมหาวิทยาลัยราชภัฏสวนดุสิต การศึกษางานวิจัยครั้งนี้แบ่งเป็น 6 ขั้นตอน คือ ขั้นตอนที่ 1 ศึกษามาตรฐานความมั่นคงปลอดภัยของระบบเครือข่ายโดยศึกษามาตรฐาน ISO/ IEC 17799: 2005 (Second Edition) และมาตรฐานความมั่นคงปลอดภัยของ ThaiCERT, NECTEC & NSTDA ขั้นตอนที่ 2 ตรวจสอบสภาพระบบเครือข่ายคอมพิวเตอร์ของมหาวิทยาลัยราชภัฏสวนดุสิต ขั้นตอนที่ 3 การศึกษาพฤติกรรมการใช้ระบบอินเทอร์เน็ตจากผู้ใช้ ขั้นตอนที่ 4 การสัมภาษณ์เชิงลึกผู้บริหารไอซีที (ICT) ของมหาวิทยาลัยราชภัฏสวนดุสิต ขั้นตอนที่ 5 จัดการเข้าร่วมสนทนากลุ่ม (Focus Group) กับผู้เชี่ยวชาญทางด้านไอซีที เพื่อพัฒนาระบบการจัดการความมั่นคงปลอดภัยบนระบบเครือข่ายคอมพิวเตอร์สำหรับมหาวิทยาลัยราชภัฏสวนดุสิต ขั้นตอนที่ 6 ให้ผู้เชี่ยวชาญตรวจสอบระบบการจัดการความมั่นคงปลอดภัยบนระบบเครือข่ายคอมพิวเตอร์ที่เหมาะสมสำหรับมหาวิทยาลัยราชภัฏสวนดุสิต ผลการศึกษา 1) จากการตรวจสอบสภาพระบบเครือข่ายคอมพิวเตอร์ของมหาวิทยาลัยพบว่า มีการบุกรุกเข้าสู่ระบบเครือข่ายบางส่วนที่มีความเสี่ยงสูงและพบว่ามีช่องโหว่เกิดขึ้นกับเซิร์ฟเวอร์ทุกเครื่อง ซึ่งช่องโหว่ที่มีความเสี่ยงสูงอาจเป็นจุดอ่อนต่อภัยคุกคามที่เข้ามาทำลายระบบเครือข่าย ผู้วิจัยจึงได้ทำการแก้ปัญหาโดยการปิดช่องโหว่ของระบบปฏิบัติการและซอฟต์แวร์ที่เกี่ยวข้อง ส่วนพอร์ตสำคัญที่ต้องเปิดให้บริการตลอดเวลาจะไม่สามารถปิดช่องโหว่ได้และก็ยังปรากฏว่ามีความเสี่ยงสูงคงเดิม 2) ผลการสอบถามพฤติกรรมผู้ใช้ระบบอินเทอร์เน็ตพบว่าผู้ใช้บางส่วนยังมีพฤติกรรมการใช้งานไม่ถูกต้อง เนื่องจากไม่เข้าใจและไม่มีความตระหนักในการใช้งานซึ่งมีผลกระทบต่อความมั่นคงปลอดภัยบนระบบเครือข่าย ผู้วิจัยจึงได้พัฒนาระบบการจัดการความมั่นคงปลอดภัยบนระบบเครือข่ายคอมพิวเตอร์สำหรับมหาวิทยาลัยราชภัฏสวนดุสิตโดยนำโมเดล

PDCA มาเป็นแนวทางในการพัฒนาซึ่งระบบประกอบด้วย คู่มือสำหรับผู้ดูแลระบบและคู่มือสำหรับผู้ใช้ระบบ โดยคู่มือจะประกอบด้วยกฎระเบียบและแนวทางในการปฏิบัติงาน ระบบนี้จะช่วยลดความเสี่ยงที่เป็นภัยคุกคามที่เกิดขึ้นกับระบบเครือข่ายได้อีกทางหนึ่งนอกเหนือจากการจัดหาอุปกรณ์ฮาร์ดแวร์และซอฟต์แวร์ในการรักษาความมั่นคงปลอดภัยเครือข่ายเพิ่มเติม

Abstract

The main objective of this research is to develop a computer network security management system for Suan Dusit Rajabhat University. This research is divided into six steps. The first step is to study ISO/ IEC 17799 : 2005 (Second Edition), ThaiCERT, NECTEC & NSTDA standards. The second step is the assessment of Suan Dusit Rajabhat University's network system. The third step is an investigation of users' behavior. The fourth step is conducting in-depth interviews with the ICT administrators at Suan Dusit Rajabhat University. The fifth step is to hold a focus group with the ICT experts who responsible for development of a computer network security management system in Suan Dusit Rajabhat University. The sixth step is to have experts assess a network security management system which should be appropriate for Suan Dusit Rajabhat University. Findings are as follows : 1) the security audit of Suan Dusit's network is found at high risk for intrusion and vulnerabilities in every server. Server vulnerabilities could be solved by patching the operating system and other software, but some essential ports that have to provide services at all times could not be patched. So risk is still high; 2) users' behavior on using the internet is found to be inappropriate by some users for lack of understanding or not aware of the appropriate use of the internet, which is impacted network security. The researcher has developed a new computer network security management system for Suan Dusit Rajabhat University in accordance to the university network security policies by applying the PDCA Model. The system is comprised of manuals for administrators and users. The manuals are contained regulations and guidelines for using the network. This system is one way to reduce the risk of threats on the network apart from obtaining additional software and hardware to provide for network security.

บทนำ

ปัจจุบันเทคโนโลยีสารสนเทศและการสื่อสาร (ICT: Information and Communication Technology) ได้เจริญก้าวหน้าไปอย่างรวดเร็ว โดยเฉพาะระบบอินเทอร์เน็ต (Internet) เข้ามามีส่วนสำคัญในชีวิตประจำวันมากขึ้น เช่น มีการแลกเปลี่ยนข้อมูลข่าวสารทางอินเทอร์เน็ต การค้นหาข้อมูล สารสนเทศทางอินเทอร์เน็ตและการทำธุรกิจซื้อขายสินค้าทางอินเทอร์เน็ต เป็นต้น จนเป็นที่ยอมรับกันว่าอินเทอร์เน็ตมีประโยชน์มหาศาลและมีอัตราการขยายตัวของผู้ใช้อินเทอร์เน็ตเพิ่มมากขึ้นทุกปี การที่มีผู้นิยมใช้อินเทอร์เน็ตเพิ่มขึ้นอย่างรวดเร็ว ทำให้เกิดอาชญากรรมบนเครือข่ายอินเทอร์เน็ต เช่น การบุกรุก ก่อกวน ลักลอบใช้และการทำลายระบบทำให้เกิดความเสียหาย โดยมีการโจรกรรมข้อมูล การลักลอบเปลี่ยนแปลงข้อมูล การละเมิดสิทธิส่วนบุคคล การรบกวนหรือขัดขวางการให้บริการการทำลายข้อมูลและระบบเครือข่าย เป็นต้น ซึ่งสร้างความเสียหายเกิดขึ้นเป็นจำนวนมาก ปัญหาที่เกิดจากการบุกรุกและการโจรกรรมข้อมูลมีแนวโน้มมากขึ้นและมีความรุนแรงขึ้น เพราะระบบเครือข่ายอินเทอร์เน็ตเชื่อมโยงถึงกันและมีผู้ใช้เพิ่มมากขึ้น ซึ่งมีทั้งผู้ประสงค์ดีและผู้ประสงค์ร้ายประกอบกับข้อมูลหลายอย่างบนอินเทอร์เน็ตมีความสำคัญเป็นที่ต้องการของผู้บุกรุก จะเห็นได้ว่าความเสียหายที่อาจเกิดขึ้นกับระบบเครือข่ายเนื่องจากการรักษาความมั่นคงปลอดภัยไม่ดีนั้น สามารถสร้างความเสียหายทั้งระดับบุคคล องค์กรและประเทศชาติได้ ซึ่งปัจจุบันระบบเครือข่ายยากต่อการควบคุมและรักษาความปลอดภัยเนื่องจากเทคโนโลยีเจริญไปอย่างรวดเร็ว ในสถานศึกษาก็เช่นเดียวกัน ถ้าไม่มีระบบความมั่นคงปลอดภัยของระบบเครือข่ายที่ดีพออาจถูกโจมตีจากแฮกเกอร์ ไวรัสคอมพิวเตอร์และเมล์ขยะเข้ามาสร้างความเสียหายกับระบบหรือเปลี่ยนแปลงแก้ไขข้อมูลสารสนเทศในระบบ เช่น คะแนน หรือ เกรดของนักศึกษา ข้อมูลทางด้านการเงินหรือข้อมูลของบุคลากรในสถาบันการศึกษา เป็นต้น

มหาวิทยาลัยราชภัฏสวนดุสิตเป็นมหาวิทยาลัยที่จัดการศึกษาในระดับอุดมศึกษาซึ่งมีการผลิตบัณฑิตทั้งในระดับปริญญาตรี ปริญญาโทและปริญญาเอก ปัจจุบันมหาวิทยาลัยมีนักศึกษาเป็นจำนวนมากจึงจำเป็นต้องมีระบบเทคโนโลยีสารสนเทศที่มีประสิทธิภาพเข้ามาช่วยสนับสนุนการจัดการเรียนการสอนและการบริหารจัดการ มหาวิทยาลัยได้ลงทุนกับระบบเทคโนโลยีสารสนเทศค่อนข้างสูงแต่สภาพปัจจุบันระบบเครือข่ายก็ยังมีปัญหา เนื่องจากการที่มีผู้ใช้ระบบเครือข่ายเป็นจำนวนมากแต่ผู้ใช้ยังขาดความรู้ความเข้าใจและความตระหนักในการใช้งาน และยังไม่มีระบบการจัดการความมั่นคงปลอดภัยบนระบบเครือข่ายทั้งระบบ ดังนั้นมหาวิทยาลัยควรต้องรีบดำเนินการอย่างเร่งด่วน

ความมั่นคงปลอดภัยบนระบบเครือข่ายจึงเป็นสิ่งสำคัญและจำเป็นมากสำหรับมหาวิทยาลัย ที่ผู้บริหารต้องให้ความสำคัญและสร้างความตระหนักให้เกิดกับบุคลากรของมหาวิทยาลัย ซึ่งนับวันอาชญากรรมทางคอมพิวเตอร์ก็ยิ่งทวีความรุนแรงมากขึ้น "ความมั่นคงปลอดภัยบนระบบเครือข่ายจึงไม่ใช่แต่เพียงอาศัยขีดความสามารถของระบบปฏิบัติการเท่านั้น แต่ยังต้องการนโยบายความมั่นคงปลอดภัย (Security Policy) ซึ่งเป็นตัวกำหนดขอบเขตการใช้งานและมาตรการดำเนินการเพื่อความมั่นคงปลอดภัยโดยรวมทั้งระบบ" (ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ, 2547: 9)

วัตถุประสงค์

1. เพื่อพัฒนาระบบการจัดการ ความมั่นคงปลอดภัยบนระบบเครือข่ายคอมพิวเตอร์สำหรับมหาวิทยาลัยราชภัฏสวนดุสิต

วิธีการศึกษา

วิธีการศึกษาแบ่งออกเป็น 6 ขั้นตอน ดังนี้

ขั้นตอนที่ 1 ศึกษามาตรฐานความมั่นคงปลอดภัยของระบบเครือข่าย ผู้วิจัยได้ศึกษามาตรฐาน ISO/IEC 17799 : 2005 (Second Edition) เป็นมาตรฐานที่ช่วยสร้างกระบวนการในการรักษาความมั่นคงปลอดภัยให้กับองค์กรซึ่งเป็นมาตรฐานสากลที่นิยมใช้กันทั่วโลก และมาตรฐานความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ของ ThaiCERT, NECTEC and NSTDA ประจำปี 2547 ซึ่งเป็นองค์กรที่ทำหน้าที่จัดทำมาตรฐานความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์สำหรับประเทศไทย

ขั้นตอนที่ 2 ตรวจสอบสภาพปัจจุบันของระบบเครือข่ายคอมพิวเตอร์ของมหาวิทยาลัยราชภัฏสวนดุสิต

การตรวจสอบสภาพปัจจุบันของระบบเครือข่าย เพื่อดักจับการบุกรุกระบบเครือข่ายและการสแกนหาช่องโหว่ของเซิร์ฟเวอร์ที่เป็นจุดอ่อนต่อการถูกบุกรุกหรือเจาะเข้าสู่ระบบ การตรวจสอบ มีขั้นตอนดังนี้

2.1 การดักจับการบุกรุกเข้าสู่ระบบเครือข่ายของมหาวิทยาลัย ผู้วิจัยได้ติดตั้งเครื่องคอมพิวเตอร์ไว้ที่เครือข่ายหลัก (Core Network) 2 จุด โดยจุดที่ 1 ดักจับการบุกรุกจากเครือข่ายภายนอกเข้าสู่เครือข่ายภายในของมหาวิทยาลัยโดยผ่านทาง Dusit Gate Router และจุดที่ 2 เพื่อดักจับการบุกรุกจากเครือข่ายศูนย์การศึกษาเข้ามายังเครือข่ายภายในมหาวิทยาลัย ทั้ง 2 จุดใช้โปรแกรม Snort สำหรับตรวจจับการบุกรุกระบบเครือข่ายโดยทำการตรวจสอบตลอดเวลา 24 ชั่วโมง ระยะเวลาประมาณ 2 สัปดาห์

2.2 การสแกน (Scan) เซิร์ฟเวอร์ เพื่อหาช่องโหว่ต่างๆ ที่เป็นจุดอ่อนต่อภัยคุกคามที่เข้ามาทำลายระบบเครือข่ายโดยทำการสแกนเซิร์ฟเวอร์ฟาร์มทั้ง 3 กลุ่ม ตลอดเวลา 24 ชั่วโมง ระยะเวลาประมาณ 2 สัปดาห์ ได้แก่ เซิร์ฟเวอร์ฟาร์มที่ห้องควบคุม เซิร์ฟเวอร์ฟาร์มที่ศูนย์ข้อมูลกลางและเซิร์ฟเวอร์ฟาร์มที่สำนักวิทยบริการและเทคโนโลยีสารสนเทศ โดยใช้โปรแกรม Nessus ตรวจสอบช่องโหว่เพื่อประเมินความเสี่ยงของระบบเครือข่ายว่ามีความเสี่ยงต่อการถูกบุกรุกโจมตีมากน้อยเพียงใด

2.3 การเก็บรวบรวมข้อมูล เก็บข้อมูลที่ผ่านเข้ามาในระบบจากจุดที่ตั้งเครื่องคอมพิวเตอร์ทั้ง 2 จุดและข้อมูลที่ได้จากการสแกนเซิร์ฟเวอร์ฟาร์มทั้ง 3 กลุ่มโดยเก็บบันทึกข้อมูล (Log File) ไว้

2.4 การวิเคราะห์ข้อมูล นำข้อมูลที่บันทึกไว้ มาวิเคราะห์ดังนี้

ข้อมูลที่ได้จากการใช้โปรแกรม Snort เป็นข้อมูลที่เกิดจากการบุกรุกเครือข่ายหรือข้อมูลที่ผ่านเข้าระบบเครือข่ายแบบผิดปกติ โดยโปรแกรมจะประเมินความผิดปกติเป็นร้อยละและสรุปความเสี่ยงแบ่งเป็น 3 ระดับ ดังนี้

ความเสี่ยงระดับสูง เป็นระดับที่สามารถเข้าสู่ระบบเครือข่ายและสร้างความเสียหายให้เกิดกับระบบได้ ต้องแก้ไขปัญหาอย่างเร่งด่วน

ความเสี่ยงระดับกลาง เป็นระดับที่ต้องเตรียมวิเคราะห์ปัญหาเพื่อหาวิธีป้องกัน

ความเสี่ยงระดับต่ำ เป็นระดับที่ต้องมีการเตรียมการเฝ้าระวัง

ข้อมูลที่ได้จากการใช้โปรแกรม Nessus เป็นช่องโหว่ที่พบในพอร์ต (Port) ต่างๆ จากการสแกนเซิร์ฟเวอร์โดยโปรแกรมจะประเมินค่าเป็นร้อยละและสรุปความเสี่ยงแบ่งเป็น 3 ระดับเช่นเดียวกัน

2.5 ปิดช่องโหว่ (Patch) ที่พบในพอร์ตต่างๆ ที่สามารถปิดได้และไม่มีผลกระทบต่อการให้บริการระบบเครือข่าย

2.6 สแกนเซิร์ฟเวอร์ด้วยโปรแกรม Nessus อีกครั้งแล้วสรุปผลความแตกต่างของระบบเครือข่ายก่อนและหลังจากการแก้ปัญหาโดยการปิดช่องโหว่แล้ว

ขั้นตอนที่ 3 ศึกษาพฤติกรรมการใช้ระบบเครือข่ายอินเทอร์เน็ตจากผู้ใช้

3.1 ประชากรและกลุ่มตัวอย่าง

3.1.1 ประชากร ได้แก่ อาจารย์ เจ้าหน้าที่และนักศึกษาของมหาวิทยาลัยราชภัฏสวนดุสิตซึ่งมีทั้งหมด 44,209 คนในปีการศึกษา 2549 โดยจำแนกเป็นอาจารย์ 926 คน เจ้าหน้าที่ 783 คน นักศึกษา 42,500 คน

3.1.2 กลุ่มตัวอย่าง การดำเนินการสุ่มกลุ่มตัวอย่างที่ใช้ในการวิจัยนี้ ขนาดของกลุ่มตัวอย่างคำนวณจากสูตรของ ยามาเน่ (Yamane, 1970: 580-581) โดยกำหนดที่ระดับนัยสำคัญ .01 ขนาดของความคลาดเคลื่อน $\pm$ ร้อยละ 5 ดังนี้

$$n = \frac{2.25\ N}{2.25 + Ne^2}$$

เมื่อแทนค่าสูตร ได้กลุ่มตัวอย่าง (n) เท่ากับ 883 คน จากกลุ่มตัวอย่างนี้ ผู้วิจัยได้สุ่มแบบแบ่งชั้น (Stratified Random Sampling) ตามสัดส่วนของประชากรซึ่งจำแนกเป็นอาจารย์ 18 คน เจ้าหน้าที่ 16 คนและนักศึกษา 849 คน

3.2 การสร้างเครื่องมือ เครื่องมือที่ใช้ในการเก็บรวบรวมข้อมูล ได้แก่ แบบสอบถามและตั้งประเด็นคำถามบนกระดานข่าว

3.2.1 สร้างแบบสอบถาม ซึ่งเป็นแบบสอบถามแบบตรวจสอบรายการ (Checklist) ถามพฤติกรรมการใช้ระบบเครือข่ายอินเทอร์เน็ตของผู้ใช้ทุกระดับ ได้แก่ อาจารย์ เจ้าหน้าที่และนักศึกษาของมหาวิทยาลัยราชภัฏสวนดุสิตแล้วตรวจสอบคุณภาพของแบบสอบถามโดยผู้เชี่ยวชาญจำนวน 5 ท่าน เพื่อนำมาหาความเที่ยงตรงเชิงโครงสร้าง (Construct Validity) และดูความชัดเจนรายข้อ (Objectivity) แล้วปรับปรุงแก้ไข จากนั้นนำไปทดลองใช้กับกลุ่มตัวอย่างจำนวน 30 คน เพื่อดูความชัดเจนรายข้อและความเหมาะสมด้านการใช้ภาษาแล้วนำมาปรับปรุงแก้ไขก่อนนำไปใช้กับกลุ่มตัวอย่างจริง

3.2.2 ตั้งประเด็นคำถามเกี่ยวกับพฤติกรรมการใช้ระบบเครือข่ายในอินทราเน็ตของมหาวิทยาลัยราชภัฏสวนดุสิตและตรวจสอบคุณภาพของประเด็นคำถามโดยผู้เชี่ยวชาญ

3.3 การศึกษาพฤติกรรมการใช้งานระบบเครือข่าย ผู้วิจัยได้สอบถามพฤติกรรมจากผู้ใช้ทุกระดับ ได้แก่ อาจารย์ เจ้าหน้าที่และนักศึกษาโดยใช้แบบสอบถามและสอบถามทางกระดานข่าวในอินทราเน็ต

3.4 การเก็บรวบรวมข้อมูลจากกลุ่มตัวอย่าง 883 คน โดยใช้วิธีการสุ่มแบบแบ่งชั้น (Stratified Random Sampling) และ เก็บรวบรวมข้อมูลบนกระดานข่าวในอินทราเน็ตโดยให้ผู้ใช้แสดงความคิดเห็นและให้ข้อเสนอแนะเกี่ยวกับการใช้บริการระบบเครือข่ายอินเทอร์เน็ต

3.5 การวิเคราะห์ข้อมูลเชิงปริมาณจากแบบสอบถามโดยใช้สถิติที่เกี่ยวข้องได้แก่ ค่าความถี่ (Frequency) และค่าร้อยละ (%)

3.6 สรุปพฤติกรรมในการใช้ระบบเครือข่ายอินเทอร์เน็ตของมหาวิทยาลัย รวมทั้งข้อคิดเห็นและข้อเสนอแนะต่างๆ เพื่อเป็นข้อมูลส่วนหนึ่งในการออกแบบระบบการจัดการความมั่นคงปลอดภัยบนระบบเครือข่ายคอมพิวเตอร์สำหรับมหาวิทยาลัยราชภัฏสวนดุสิต

ขั้นตอนที่ 4 สัมภาษณ์ผู้บริหารไอซีทีของมหาวิทยาลัยราชภัฏสวนดุสิต

4.1 สร้างแบบสัมภาษณ์เชิงลึกแบบมีโครงสร้าง (Structure Form In-depth Interview) โดยกำหนดประเด็นคำถามตามหน้าที่ที่ผู้ถูกสัมภาษณ์รับผิดชอบและตามมาตรฐานที่ ThaiCERT, NECTEC and NSTDA ประจำปี 2547 กำหนดไว้ แล้วตรวจสอบคุณภาพของแบบสัมภาษณ์โดยผู้เชี่ยวชาญ

4.2 สัมภาษณ์ผู้บริหารไอซีทีของมหาวิทยาลัยราชภัฏสวนดุสิต ได้แก่ อธิการบดี ผู้ช่วยอธิการบดีฝ่าย ICT/ CIO ผู้อำนวยการสำนักวิทยบริการฯ รองผู้อำนวยการสำนักวิทยบริการฯ ผู้ช่วยผู้อำนวยการสำนักวิทยบริการฯ หัวหน้ากองเทคนิคและเครือข่ายและผู้ดูแลระบบเครือข่ายเพื่อหาข้อสรุปและข้อเสนอแนะ

4.3 วิเคราะห์ข้อมูลเชิงคุณภาพจากการสัมภาษณ์ สรุปผลสัมภาษณ์และข้อเสนอแนะเพื่อนำมาใช้เป็นส่วนหนึ่งในการพัฒนาระบบการจัดการ ความมั่นคงปลอดภัยบนระบบเครือข่ายคอมพิวเตอร์สำหรับมหาวิทยาลัยราชภัฏสวนดุสิต

ขั้นตอนที่ 5 จัดการสนทนากลุ่ม (Focus Group) กับผู้เชี่ยวชาญทางด้านไอซีที

ผู้วิจัยนำผลการศึกษาในขั้นตอนที่ 1 - 4 มาสร้างรูปแบบระบบการจัดการ ความมั่นคงปลอดภัยบนระบบเครือข่ายคอมพิวเตอร์สำหรับมหาวิทยาลัยและจัดการสนทนากลุ่มโดยเชิญผู้เชี่ยวชาญทางด้านไอซีทีร่วมแสดงความคิดเห็นพิจารณารูปแบบระบบการจัดการ ความมั่นคงปลอดภัยบนระบบเครือข่ายคอมพิวเตอร์ที่เหมาะสมสำหรับมหาวิทยาลัยราชภัฏสวนดุสิต

ขั้นตอนที่ 6 ผู้เชี่ยวชาญตรวจสอบ

นำระบบการจัดการ ความมั่นคงปลอดภัยบนระบบเครือข่ายคอมพิวเตอร์ที่ปรับปรุงแก้ไขแล้วจากการสนทนากลุ่ม มาให้ผู้เชี่ยวชาญตรวจสอบเพื่อปรับให้เหมาะสมสำหรับมหาวิทยาลัยราชภัฏสวนดุสิต

ผลการศึกษา

จากการศึกษาผู้วิจัยได้ตอบคำถาม 3 ประเด็นดังนี้

1. สภาพปัจจุบันของระบบเครือข่ายของมหาวิทยาลัยราชภัฏสวนดุสิตมีการบุกรุกจากภายนอกและภายในอย่างไร

การวิเคราะห์สภาพปัจจุบันของระบบเครือข่ายของมหาวิทยาลัย ผู้วิจัยได้ทำการตรวจสอบข้อมูลเพื่อดักจับการบุกรุกระบบเครือข่ายจากภายนอกและภายในโดยใช้โปรแกรม Snort และตรวจสอบช่องโหว่ของเซิร์ฟเวอร์ฟาร์มทั้ง 3 กลุ่ม เพื่อประเมินความเสี่ยงโดยใช้โปรแกรม Nessus

สรุปผลการวิเคราะห์สภาพปัจจุบันของระบบเครือข่ายของมหาวิทยาลัย โดยแบ่งเป็น 2 ขั้นดังนี้

ขั้นที่ 1 ผู้วิจัยได้ตรวจจับการบุกรุกระบบเครือข่ายจากภายนอกเข้าสู่เครือข่ายภายในของมหาวิทยาลัยและตรวจจับการบุกรุกระบบเครือข่ายจากเครือข่ายศูนย์การศึกษาเข้าสู่เครือข่ายภายในของมหาวิทยาลัย โดยใช้โปรแกรม Snort ผลการวิเคราะห์สรุปได้ดังนี้

1.1 ผลการวิเคราะห์การบุกรุกระบบเครือข่ายจากภายนอกเข้าสู่เครือข่ายภายในของมหาวิทยาลัยพบว่า มีความพยายามจากภายนอกที่จะบุกรุกเข้ามาในระบบเครือข่ายของมหาวิทยาลัยโดยการบุกรุกผ่านทางเว็บ ความพยายามบุกรุกเพื่อให้ได้สิทธิ์ของผู้ใช้ระบบและผู้ดูแลระบบซึ่งถ้าบุกรุกผ่านเข้ามาในระบบเครือข่ายได้สำเร็จสามารถสร้างความเสียหายให้เกิดกับระบบเครือข่ายของมหาวิทยาลัยได้

1.2 ผลการวิเคราะห์การบุกรุกระบบเครือข่ายภายในจากเครือข่ายศูนย์การศึกษาเข้าสู่เครือข่ายภายในของมหาวิทยาลัยพบว่ามีความพยายามบุกรุกจากภายในระบบเครือข่ายโดยบุกรุกจากศูนย์การศึกษาเข้ามายังเครือข่ายภายในมหาวิทยาลัย มีกลุ่มที่พยายามหาข้อมูลที่รั่วไหลเพื่อนำมาใช้ในการบุกรุกและพยายามกำหนดค่าระบบใหม่มีความเสี่ยงระดับปานกลางซึ่งเป็นระดับที่ยังไม่ก่อให้เกิดความเสียหายแต่ต้องเตรียมวิเคราะห์ปัญหาเพื่อหาวิธีป้องกันและกลุ่มการส่งข้อมูลที่ไม่ตรงตามโปรโตคอล มีความเสี่ยงในระดับต่ำซึ่งเป็นระดับที่ต้องมีการเฝ้าระวัง

ขั้นที่ 2 ตรวจสอบช่องโหว่ของเซิร์ฟเวอร์ฟาร์มโดยใช้โปรแกรม Nessus สแกนเซิร์ฟเวอร์ฟาร์มทั้ง 3 กลุ่ม ได้แก่ เซิร์ฟเวอร์ฟาร์มที่ห้องควบคุม เซิร์ฟเวอร์ฟาร์มที่ศูนย์ข้อมูลกลางและเซิร์ฟเวอร์ฟาร์มที่สำนักวิทยบริการ ผลการวิเคราะห์สรุปได้ดังนี้

จากผลการสแกนเซิร์ฟเวอร์ฟาร์มทั้ง 3 กลุ่มพบว่าเซิร์ฟเวอร์ทุกเครื่องมีช่องโหว่เกิดขึ้นในระดับความเสี่ยงสูงหลายพอร์ตซึ่งเป็นระดับที่เป็นอันตรายที่ผู้บุกรุกสามารถเข้าสู่ระบบและสร้างความเสียหายให้เกิดกับระบบเครือข่ายได้ต้องแก้ไขปัญหาอย่างเร่งด่วน ผู้วิจัยจึงทำการปิดช่องโหว่ที่เซิร์ฟเวอร์ฟาร์มทั้ง 3 กลุ่ม เฉพาะพอร์ตที่สามารถปิดช่องโหว่ได้และไม่มีผลกระทบต่อการให้บริการ หลังจากปิดช่องโหว่ในบางพอร์ตแล้วทำการสแกนเซิร์ฟเวอร์ใหม่อีกครั้งปรากฏผลว่า ความเสี่ยงเป็น 0 % ส่วนพอร์ตสำคัญที่ต้องให้บริการที่ไม่สามารถปิดช่องโหว่ได้ก็ยังปรากฏว่ามีความเสี่ยงสูงคงเดิม ซึ่งการแก้ปัญหาควรนำวิธีการอื่นมาใช้

2. จากการถูกบุกรุกทั้งภายนอกและภายในระบบเครือข่าย มีความเสี่ยงหรือเกิดผลกระทบอย่างไรบ้าง

จากผลการตรวจสอบสภาพปัจจุบันของระบบเครือข่ายของมหาวิทยาลัยปรากฏว่ามีการบุกรุกทั้งภายนอกและภายในระบบเครือข่าย มีความเสี่ยงเกิดขึ้นทั้งในระดับสูง ปานกลางและต่ำ และเมื่อทำการสแกนเซิร์ฟเวอร์ก็พบว่ามีช่องโหว่เกิดขึ้นในระดับความเสี่ยงสูง ปานกลางและต่ำ

เช่นเดียวกัน ซึ่งถ้ามีการบุกรุกที่มีความเสี่ยงสูงแล้วมาพบช่องโหว่ที่มีความเสี่ยงต่ำก็จะไม่เกิดปัญหาหรือผลกระทบต่อระบบ แต่ถ้ามีการบุกรุกที่มีความเสี่ยงสูงแล้วมาพบช่องโหว่ที่มีความเสี่ยงสูงด้วยแล้วก็จะเกิดผลกระทบอย่างสูงต่อระบบเป็นอันตรายต่อระบบในการแก้ปัญหาต้องมีการเตรียมการทั้ง ฮาร์ดแวร์ ซอฟต์แวร์และพีเพิลแวร์ ซึ่งเกี่ยวข้องในการสร้างความมั่นคงปลอดภัยให้เกิดกับระบบเครือข่าย ดังนี้

ในการสร้างความมั่นคงปลอดภัยให้กับระบบเครือข่าย ถึงแม้มหาวิทยาลัยจะลงทุนกับฮาร์ดแวร์และซอฟต์แวร์แล้วก็ตาม แต่ก็ยังไม่สามารถสร้างระบบให้เกิดความมั่นคงปลอดภัยได้ถ้าผู้ใช้ไม่ให้ความร่วมมือ ในการใช้งานระบบเครือข่ายให้ถูกต้องเหมาะสม ดังนั้น ผู้วิจัยจึงได้ทำการศึกษาพฤติกรรมการใช้งานระบบเครือข่ายอินเทอร์เน็ตและสัมภาษณ์แนวนโยบายจากผู้บริหารไอซีที เพื่อนำมาเป็นแนวทางในการพัฒนาระบบการจัดการ ความมั่นคงปลอดภัยบนระบบเครือข่ายคอมพิวเตอร์สำหรับมหาวิทยาลัยราชภัฏสวนดุสิตต่อไป

การศึกษาพฤติกรรมการใช้ระบบเครือข่ายอินเทอร์เน็ตจากผู้ใช้โดยใช้แบบสอบถาม สรุปพฤติกรรมได้ดังนี้

1) เกี่ยวกับสภาพการใช้บริการระบบอินเทอร์เน็ต ผู้ใช้ใช้บริการระบบอินเทอร์เน็ตในวันธรรมดา (จันทร์ – ศุกร์) ช่วงเวลา 08.01 – 16.00 น. มากที่สุด ส่วนวันหยุด (เสาร์ – อาทิตย์และวันนักขัตฤกษ์) ใช้ช่วงเวลา 16.01 – 22.00 น. มากที่สุด จากผลการวิจัยทำให้ทราบช่วงเวลาที่มีผู้ใช้ใช้บริการระบบอินเทอร์เน็ตมาก ซึ่งสามารถนำข้อมูลที่ได้ไปใช้บริหารจัดการระบบเครือข่ายอินเทอร์เน็ตเพื่อให้บริการกับผู้ใช้ให้เกิดประโยชน์สูงสุด

2) เกี่ยวกับพฤติกรรมในการใช้บริการระบบอินเทอร์เน็ตนอกจากการศึกษาแล้วส่วนใหญ่ผู้ใช้ใช้ระบบอินเทอร์เน็ตในการส่งอีเมล์ (E-Mail) มากที่สุด รองลงมาใช้ในการดูหนัง ฟังเพลงและเล่นเกมส์ การใช้อีเมล์ผู้ใช้ ใช้ Dusit Mail น้อยกว่าเมล์ฟรีอื่นๆ ส่วนการเข้าใช้ระบบบริหารการศึกษาของมหาวิทยาลัยผู้ใช้บางส่วนให้ผู้อื่นทำให้ สำหรับการใช้รหัสผ่าน ผู้ใช้เคยใช้รหัสผ่าน (Password) ของผู้อื่นเกือบ 50 % ในการเปลี่ยนรหัสผ่านส่วนใหญ่ผู้ใช้เปลี่ยนรหัสผ่านไม่บ่อยนักและการที่ผู้ใช้มีบัญชีชื่อผู้ใช้ (User Account) หลายชุดในการเข้าใช้บริการต่างๆ ในระบบอินเทอร์เน็ต เช่น การใช้ระบบบริหารการศึกษา การใช้บทเรียนออนไลน์ การเข้าใช้ระบบอินเทอร์เน็ต การใช้ระบบบุคลากร เป็นต้น ทำให้ผู้ใช้เกิดความสับสนต่อการใช้งาน

ส่วนปัญหาที่ผู้ใช้พบบ่อยๆ ในการใช้ระบบอินเทอร์เน็ตของมหาวิทยาลัย คือ ปัญหาไวรัส การเข้าใช้ระบบบริหารการศึกษาไม่ได้และเชื่อมต่อระบบอินเทอร์เน็ตไม่ได้ ทุกครั้งที่ผู้ใช้เปิดพบเมล์ขยะ (Spam mail) หรือเมล์ที่ไม่รู้จักผู้ใช้เปิดดูแล้วจึงลบทิ้ง ส่วนการดาวน์โหลดข้อมูลผู้ใช้ส่วนใหญ่ดาวน์โหลดข้อมูลประเภท เพลง/ภาพยนตร์ รองลงมาเป็นเกมส์ โดยทุกครั้งที่ดาวน์โหลดผู้ใช้ไม่ได้ทำการตรวจสอบไวรัสก่อน ผู้ใช้ส่วนใหญ่ติดตั้งโปรแกรม Antivirus ที่เครื่องคอมพิวเตอร์

ของตนเองแต่นานๆ ครั้งจึงทำการตรวจสอบและอัพเดท (update) โปรแกรม Antivirus สำหรับการรับทราบข้อมูลข่าวสารต่างๆ เกี่ยวกับการแพร่ระบาดของไวรัส ผู้ใช้รับทราบจากเว็บ http://www.dusit.ac.th น้อยมาก ผู้ใช้ส่วนใหญ่ไม่ทราบว่ามหาวิทยาลัยมีบริการให้ความรู้เกี่ยวกับการใช้บริการระบบเครือข่ายที่เว็บ http://www.arit.dusit.ac.th/ask ผู้ใช้เกือบครึ่งเคยใช้ระบบอินเทอร์เน็ตในทางผิดกฎหมายหรือขัดต่อศีลธรรมอันดีโดยเผยแพร่หรือเข้าถึงสื่อลามกอนาจารที่ขัดต่อศีลธรรม รองลงมาคือการส่งข้อความที่ไม่สุภาพ หยาบคาย หรือก่อกวนผู้อื่นและส่งเมล์ที่เป็นจดหมายลูกโซ่ ผู้ใช้ส่วนใหญ่เห็นด้วยว่าควรมีการกำหนดกฎระเบียบ เพื่อเป็นนโยบายในการใช้งานระบบอินเทอร์เน็ตของมหาวิทยาลัย โดยผู้ใช้และผู้ดูแลระบบควรเป็นผู้รับผิดชอบในการรักษาความมั่นคงปลอดภัยบนระบบเครือข่ายของมหาวิทยาลัย จากพฤติกรรมต่างๆ ที่ได้จากการวิจัยสามารถนำไปใช้ในการออกแบบระบบการจัดการความมั่นคงปลอดภัยบนระบบเครือข่ายคอมพิวเตอร์ของมหาวิทยาลัย

3) การสอบถามความคิดเห็นต่อการใช้บริการระบบอินเทอร์เน็ต ผู้วิจัยได้สอบถามผู้ใช้โดยใช้แบบสอบถามให้ผู้ใช้แสดงความคิดเห็นเป็นคำถามปลายเปิดและให้แสดงความคิดเห็นทางกระดานข่าวในอินทราเน็ต เกี่ยวกับจริยธรรมในการใช้ระบบอินเทอร์เน็ตควรเป็นอย่างไร ผลสรุปส่วนใหญ่ผู้ใช้จะเน้นในเรื่องการใช้งานใช้ให้ถูกกาลเทศะ เปิดเว็บไซต์ที่เหมาะสม ไม่ผิดศีลธรรม รักษากฎระเบียบในการใช้งานอย่างเคร่งครัดไม่ละเมิดสิทธิผู้อื่นและไม่ทำผิดกฎหมาย สำหรับปัญหาระบบอินเทอร์เน็ตช้า ล่ม หรือ ไวรัสคอมพิวเตอร์ ส่วนใหญ่ผู้ใช้จะเน้นการแก้ปัญหาด้วยตนเองก่อนโดยการสแกนไวรัส ถ้าฆ่าไวรัสไม่ได้ก็ปรึกษาผู้เชี่ยวชาญหรือติดต่อเจ้าหน้าที่เพื่อแก้ปัญหา และถ้าจะพัฒนาระบบการจัดการเพื่อรักษาความมั่นคงปลอดภัยบนระบบเครือข่ายคอมพิวเตอร์ของมหาวิทยาลัย ผู้ใช้ส่วนใหญ่มีความเห็นว่า มหาวิทยาลัยควรเน้นเรื่องการรักษาความลับของข้อมูลโดยให้มีการสำรองข้อมูลที่สำคัญไว้และควรจัดหาอุปกรณ์เกี่ยวกับความมั่นคงปลอดภัยเครือข่ายมาใช้งาน

การสัมภาษณ์แนวนโยบายจากผู้บริหารไอซีทีของมหาวิทยาลัยราชภัฏสวนดุสิตโดยใช้แบบสัมภาษณ์เชิงลึก วิเคราะห์ข้อมูลเชิงคุณภาพ ในประเด็นต่างๆ ดังต่อไปนี้

1) สรุปผลสัมภาษณ์อธิการบดี ผู้ช่วยอธิการบดีฝ่ายเทคโนโลยีสารสนเทศและซีไอโอของมหาวิทยาลัยราชภัฏสวนดุสิต มีความเห็นว่าจำเป็นอย่างยิ่งในการกำหนดนโยบายการใช้ระบบเครือข่ายของมหาวิทยาลัย เพราะมีผู้ใช้ระบบเครือข่ายมากขึ้นความต้องการในการใช้งานก็มีหลากหลายและมีพฤติกรรมแตกต่างกันจึงควรมีการกำหนดนโยบายให้ชัดเจน เพื่อจะได้เป็นแนวปฏิบัติเดียวกันและจะต้องทำอย่างจริงจัง ควรมีการเผยแพร่นโยบายและสร้างความตระหนักให้เกิดกับบุคลากรของมหาวิทยาลัย

2) สรุปผลสัมภาษณ์ผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ รองผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ ผู้ช่วยผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ มีความเห็นว่าในการใช้งานระบบสารสนเทศของมหาวิทยาลัย ควรมีการกำหนดสิทธิ์ของผู้ใช้โดยแบ่งเป็น 4 ระดับคือ ผู้บริหาร อาจารย์ เจ้าหน้าที่และนักศึกษา ควรต้องมีผู้บริหารด้านความมั่นคงปลอดภัยระบบเครือข่าย (Security Manager) อย่างน้อย 1 คน ที่มีหน้าที่รับผิดชอบโดยตรงและมีเจ้าหน้าที่ดูแลรักษาความมั่นคงปลอดภัยของระบบเครือข่ายหลักและควรกำหนดหน้าที่ความรับผิดชอบของเจ้าหน้าที่ไว้อย่างชัดเจน ควรมีการจัดทำนโยบายความมั่นคงปลอดภัยและจัดอบรมให้ความรู้แก่บุคลากร เกี่ยวกับการสร้างความมั่นคงปลอดภัยให้กับระบบและควรมีการกำหนดระเบียบปฏิบัติและควรจัดทำคู่มือและขั้นตอนการปฏิบัติงานอย่างชัดเจน

3) สรุปการสัมภาษณ์หัวหน้ากลุ่มงานเทคนิคและเครือข่าย ผู้ดูแลระบบเครือข่ายของมหาวิทยาลัยราชภัฏสวนดุสิต มีความเห็นว่าควรสร้างความตระหนักให้กับผู้ใช้และกำหนดระเบียบปฏิบัติในการใช้งาน ควรมีการกำหนดสิทธิ์ในการเข้าใช้ข้อมูลโดยผู้ใช้ต้องผ่านการพิสูจน์ตัวตน ควรมีการสำรองข้อมูลถ้าระบบเกิดมีปัญหาก็สามารถนำข้อมูลมาใช้ได้ ควรมีการจำกัดระยะเวลาการใช้งานสำหรับระบบสารสนเทศที่มีความสำคัญสูงหรือมีความเสี่ยงสูง เช่น การใช้ระบบบริหารการศึกษาในการลงทะเบียน การเพิ่มถอนรายวิชา การส่งเกรด ระบบการเงิน เป็นต้น และควรมีการบันทึกเข้าใช้งานระบบสารสนเทศ

3. ระบบการจัดการความมั่นคงปลอดภัยบนระบบเครือข่ายคอมพิวเตอร์ที่เหมาะสมกับมหาวิทยาลัยราชภัฏสวนดุสิตควรเป็นอย่างไร

ผู้วิจัยได้นำข้อมูลจากการมาตรฐานความมั่นคงปลอดภัยของระบบเครือข่าย วิเคราะห์ผลที่ได้จากการตรวจจับการบุกรุกและการประเมินความเสี่ยงของการตรวจสอบสภาพปัจจุบันของระบบเครือข่ายและผลสรุปความแตกต่างของระบบเครือข่ายก่อนและหลังจากการแก้ปัญหาโดยการปิดช่องโหว่ของเซิร์ฟเวอร์ ผลการศึกษาพฤติกรรมการใช้งานระบบเครือข่ายอินเทอร์เน็ตและผลการสัมภาษณ์ผู้บริหารทางด้านไอซีทีแล้ว ผู้วิจัยได้สร้างรูปแบบระบบการจัดการความมั่นคงปลอดภัยบนระบบเครือข่ายคอมพิวเตอร์สำหรับมหาวิทยาลัยราชภัฏสวนดุสิตและได้จัดการสนทนากลุ่มโดยเชิญผู้เชี่ยวชาญทางด้านไอซีทีเพื่อร่วมแสดงความคิดเห็นพิจารณารูปแบบระบบการจัดการ ความมั่นคงปลอดภัยบนระบบเครือข่ายคอมพิวเตอร์ที่เหมาะสมสำหรับมหาวิทยาลัยราชภัฏสวนดุสิต

สรุปผลการศึกษาและข้อเสนอแนะ

1. สรุปผลการศึกษาและอภิปราย

ในการพัฒนาระบบการจัดการความมั่นคงปลอดภัยบนระบบเครือข่ายคอมพิวเตอร์สำหรับมหาวิทยาลัยราชภัฏสวนดุสิต มหาวิทยาลัยควรดำเนินการดังนี้

1.1 จัดเตรียมอุปกรณ์ที่จำเป็นต่อการ ใช้งานเพื่อสร้างความมั่นคงปลอดภัยของระบบเครือข่าย เช่น ไฟร์วอลล์ ระบบตรวจจับและป้องกันการบุกรุกเครือข่าย (IDS/ IPS) เซิร์ฟเวอร์ที่ใช้ในการอัพเดทแพทช์ (Update Patch) ของระบบปฏิบัติการ (Operating System Update Server) และโปรแกรมประยุกต์ (Application Software) เป็นต้น

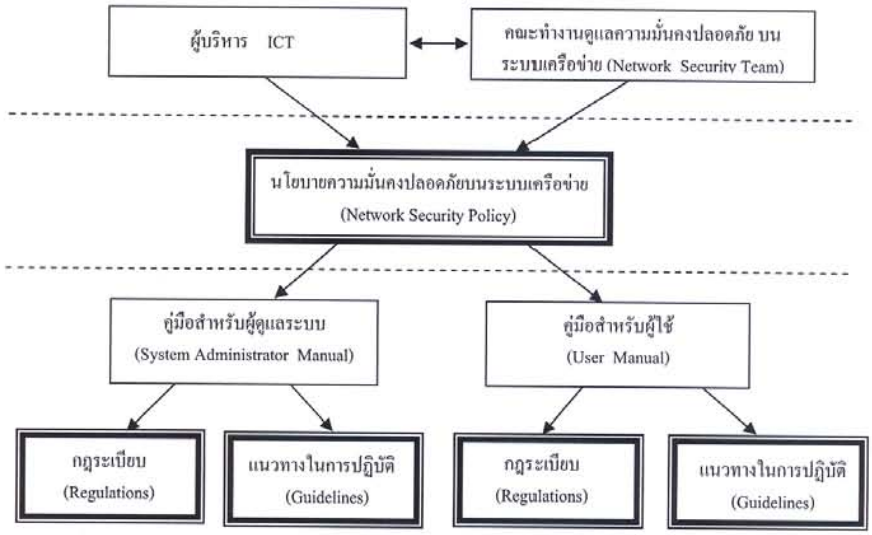
1.2 จัดตั้งคณะทำงานที่ทำหน้าที่ดูแลความมั่นคงปลอดภัยบนระบบเครือข่ายคอมพิวเตอร์ กำหนดหน้าที่ความรับผิดชอบและสนับสนุนการใช้นโยบายและการปฏิบัติงาน

1.3 สร้างความเข้าใจและความตระหนักต่อผู้ใช้ให้ปฏิบัติตามนโยบาย มีคุณธรรมจริยธรรมในการใช้งานโดยจัดโครงการฝึกอบรมให้กับผู้ใช้งานในแต่ละระดับ

1.4 กำหนดกฎระเบียบและแนวทางการปฏิบัติในการใช้ระบบเครือข่ายและบทลงโทษที่ชัดเจน

รูปแบบระบบการจัดการความมั่นคงปลอดภัยบนระบบเครือข่ายคอมพิวเตอร์สำหรับมหาวิทยาลัยราชภัฏสวนดุสิต มีดังนี้

รูปแบบระบบการจัดการความมั่นคงปลอดภัยบนระบบเครือข่ายคอมพิวเตอร์สำหรับมหาวิทยาลัยราชภัฏสวนดุสิต ควรเริ่มจากคณะทำงานดูแลความมั่นคงปลอดภัยบนระบบเครือข่ายที่มีหน้าที่รับผิดชอบในการกำหนดนโยบายความมั่นคงปลอดภัยบนระบบเครือข่ายโดยกระบวนการกำหนดนโยบายประกอบด้วย การกำหนดนโยบายและการนำนโยบายไปสู่การปฏิบัติ นโยบายนี้ใช้เป็นกรอบในการปฏิบัติงานโดยกำหนดแนวนโยบายเพื่อเป็นกรอบกว้างๆ ที่จะนำไปสู่ภาคปฏิบัติที่ชัดเจนขึ้น เมื่อกำหนดนโยบายความมั่นคงปลอดภัยบนระบบเครือข่ายแล้วนำเสนอผู้บริหารเพื่อพิจารณาและประกาศใช้เป็นนโยบายของมหาวิทยาลัย จากนโยบายที่กำหนดนำมาสู่ภาคปฏิบัติที่ชัดเจนขึ้นโดยจัดทำคู่มือสำหรับการปฏิบัติงาน คู่มือแบ่งออกเป็น 2 ประเภท คือ คู่มือสำหรับผู้ดูแลระบบ (System Administrator Manual) และคู่มือสำหรับผู้ใช้ (User Manual) ส่วนประกอบของคู่มือจะประกอบด้วยกฎระเบียบ (Regulations) ที่ต้องปฏิบัติตามและแนวทางในการปฏิบัติงาน (Guidelines) ซึ่งเป็นรายละเอียดในการดำเนินงาน (ดังภาพ)



2. ข้อเสนอแนะ

2.1 ข้อเสนอแนะสำหรับการนำผลการวิจัยไปประยุกต์ใช้

2.1.1 ระบบการจัดการ ความมั่นคงปลอดภัยบนระบบเครือข่ายคอมพิวเตอร์ จะไม่มีลักษณะคงที่แน่นอนตายตัว จะปรับเปลี่ยนไปตามยุคตามสมัยตามวิวัฒนาการของเทคโนโลยีที่เปลี่ยนไป ดังนั้น การพัฒนาระบบการจัดการ ความมั่นคงปลอดภัยบนระบบเครือข่ายคอมพิวเตอร์ควรจะมีลักษณะที่สามารถยืดหยุ่นปรับเปลี่ยนแก้ไขได้

2.1.2 การสร้างความมั่นคงปลอดภัยบนระบบเครือข่ายคอมพิวเตอร์ จะต้องทำเป็นระบบและทำอย่างต่อเนื่องไม่มีวันจบ ถึงแม้ระบบจะมีความมั่นคงปลอดภัยในวันนี้ วันข้างหน้าระบบอาจถูกบุกรุกเพราะมีช่องโหว่ใหม่ๆ เกิดขึ้นอยู่เรื่อยๆ ดังนั้นการสร้างความมั่นคงปลอดภัยบนระบบเครือข่ายจะต้องเตรียมทั้งอุปกรณ์ทางด้าน ฮาร์ดแวร์ ซอฟต์แวร์และพีเพิลแวร์ ซึ่งอุปกรณ์เกี่ยวกับความมั่นคงปลอดภัยเป็นอุปกรณ์ที่มีราคาแพงและเทคโนโลยีจะมีการเปลี่ยนแปลงอย่างรวดเร็ว การรักษาความมั่นคงปลอดภัยเครือข่ายก็จะต้องลงทุนไปเรื่อยๆ อย่างไม่มีที่สิ้นสุด ดังนั้นเพื่อเป็นการประหยัดค่าใช้จ่าย มหาวิทยาลัยควรจะลงทุนกับอุปกรณ์พื้นฐานเกี่ยวกับความมั่นคงปลอดภัยเครือข่ายเท่าที่จำเป็นและควรมีการกำหนดนโยบาย กฎระเบียบและแนวทางในการปฏิบัติเกี่ยวกับการใช้ระบบเพื่อเป็นมาตรการให้บุคลากรปฏิบัติตามซึ่งจะช่วยรักษาระบบให้เกิดความความมั่นคงปลอดภัยได้อีกทางหนึ่ง

2.1.3 ข้อมูลที่ได้จากการสำรวจพฤติกรรมการใช้ระบบเครือข่ายอินเทอร์เน็ตสะท้อนให้เห็นว่าผู้ใช้ยังขาดความเข้าใจและความตระหนักในการรักษาความมั่นคงปลอดภัยบนระบบเครือข่ายคอมพิวเตอร์ของมหาวิทยาลัย มหาวิทยาลัยจะต้องสร้างความเข้าใจและสร้างความตระหนัก

ให้เกิดกับบุคลากรโดยการให้ความร่วมมือในการรักษาความมั่นคงปลอดภัยบนระบบเครือข่ายและมหาวิทยาลัยจะต้องชี้แจงให้บุคลากรได้ทราบถึงผลเสียหายที่อาจเกิดขึ้นถ้าทุกคนไม่ระมัดระวังอาจเป็นเหตุให้เกิดความเสี่ยงต่อภัยคุกคามที่อาจเกิดขึ้น จากการที่ผู้ใช้ไม่ปฏิบัติตามนโยบายทั้งโดยเจตนาและไม่เจตนา และมหาวิทยาลัยควรมีการกระตุ้นให้บุคลากรให้ความร่วมมือในการปฏิบัติตามกฎระเบียบว่าด้วยการใช้ระบบเครือข่ายอินเทอร์เน็ตโดยเคร่งครัด ซึ่งถ้าฝ่าฝืนจะต้องได้รับโทษตามเกณฑ์ที่มหาวิทยาลัยกำหนด

2.1.4 มหาวิทยาลัยต่างๆ ควรมีความร่วมมือกันในการวิจัยและพัฒนาระบบการจัดการ ความมั่นคงปลอดภัยบนระบบเครือข่ายคอมพิวเตอร์และใช้ทรัพยากรต่างๆ ร่วมกันทั้งบุคลากรและซอฟต์แวร์เพื่อเป็นการประหยัดค่าใช้จ่ายและแก้ปัญหาการขาดแคลนบุคลากร

2.2 ข้อเสนอแนะสำหรับการวิจัยในอนาคต

2.2.1 การวิจัยนี้เป็นการพัฒนาระบบการจัดการ ความมั่นคงปลอดภัยบนระบบเครือข่ายคอมพิวเตอร์ในระดับเบื้องต้นและเมื่อมหาวิทยาลัยมีความพร้อมในระดับเบื้องต้นแล้วควรพัฒนาอย่างต่อเนื่องในระดับกลางและระดับสูงต่อไป

2.2.2 เนื่องจากปัจจุบันมหาวิทยาลัยราชภัฏสวนดุสิตก็มีบริการระบบเครือข่ายไร้สายทั้งภายในมหาวิทยาลัยและที่ศูนย์การศึกษาทุกศูนย์ สำหรับงานวิจัยต่อไปจึงควรพัฒนาระบบการจัดการความมั่นคงปลอดภัยบนระบบเครือข่ายคอมพิวเตอร์ให้ครอบคลุมถึงระบบเครือข่ายไร้สายด้วย

2.2.3 ควรทำการศึกษาวิจัยเพิ่มเติมเพื่อหาจุดคุ้มทุนในการลงทุนกับอุปกรณ์ขั้นพื้นฐานเกี่ยวกับความมั่นคงปลอดภัยบนระบบเครือข่ายคอมพิวเตอร์

เอกสารอ้างอิง

ศิริวรรณ อภิสิริเดช. (2547). **มาตรฐานสากลสำหรับการสร้างความมั่นคงปลอดภัย(ISO/ IEC 17799:2000) และกรณีศึกษา**. โครงการอบรมการป้องกันความปลอดภัยข้อมูลคอมพิวเตอร์ ครั้งที่ 4. พฤศจิกายน 2547 (หน้า 24-25). กรุงเทพฯ : ศูนย์ประสานงานการรักษาความปลอดภัยคอมพิวเตอร์ประเทศไทย.

ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ. (2547). **มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชั่น 1) ประจำปี 2547**. กรุงเทพฯ : ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ, กระทรวงวิทยาศาสตร์และเทคโนโลยี.

_____. (2547). **รายงานผลการศึกษานโยบายความปลอดภัยของเครือข่ายสำหรับประเทศไทย**. กรุงเทพ ฯ : ฝ่ายพัฒนานโยบายและกฎหมาย, กระทรวงวิทยาศาสตร์และเทคโนโลยี.

Yamane,T. (1970). **Statistics an Introductory Analysis.** (2nd ed.). Tokyo : John Weatherhill.