การประชุมเสนอผลงานวิจัยระดับชาติ มหาวิทยาลัยสุโขทัยธรรมาธิราช ครั้งที่ 12
The 12th STOU National Research Conference

การพัฒนากรอบการจัดการช่องโหว่ระบบสารสนเทศเพื่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์ กรณีศึกษา กองบัญชาการกองทัพภาคที่ 2

Framework Development of Information System Vulnerability Management for Cyber Security: Case Study of the Second Army Area Headquarter

ทัญญะ สิทธิมณีวรรณ (Tunya Sittimaneewan) [1] ขจิตพรรณ กฤตพลวิมาน (Khajitpan Kritpolviman) [2] *

บทคัดย่อ

การวิจัยนี้มีวัตถุประสงค์เพื่อพัฒนากรอบการจัดการช่องโหว่ วิเคราะห์และประเมินช่องโหว่ และกำหนดวิธีแก้ไขช่องโหว่ระบบสารสนเทศขององค์กร โดยใช้กรอบการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของ NIST และ วงจรชีวิตการจัดการช่องโหว่ของ CDC นำมาเป็นต้นแบบในการพัฒนากรอบการจัดการช่องโหว่ขององค์กร ระเบียบวิธีวิจัยประกอบด้วย 1) ศึกษาสภาพแวดล้อมและลักษณะของระบบสารสนเทศขององค์กร 2) พัฒนากรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กร และ 3) ดำเนินการทดลองตามกรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กร ได้แก่ การจัดการทรัพย์สินอุปกรณ์ระบบสารสนเทศ การประเมิน การแก้ไขช่องโหว่ การประเมินซ้ำ และการตรวจสอบยืนยันความถูกต้อง โดยใช้ซอฟต์แวร์วิเคราะห์ช่องโหว่ Nessus เวอร์ชัน Essentials และ Nexpose เวอร์ชัน Community สำหรับประเมินช่องโหว่ของเครื่องแม่ข่ายให้บริการงานภารกิจต่างๆ ขององค์กร ได้แก่ เครื่องแม่ข่ายระบบศูนย์อัตโนมัติ เครื่องแม่ข่ายระบบประชุมทางไกลผ่านจอภาพ เครื่องแม่ข่ายเว็บไซต์ขององค์กร และเครื่องแม่ข่ายเครือข่ายส่วนตัวเสมือน (VPN) ผลการวิจัยพบว่ากรอบการจัดการช่องโหว่ระบบสารสนเทศที่พัฒนานี้สามารถนำมาวิเคราะห์ช่องโหว่ และหาวิธีการแก้ไขช่องโหว่ได้ จากการสำรวจช่องโหว่ที่ส่งผลกระทบและมีความเสี่ยงต่อองค์กรมี 34 ช่องโหว่ หลังจากดำเนินการทดลองตามกรอบการจัดการช่องโหว่ที่พัฒนาขึ้นพบว่าเหลือเพียง 3 ช่องโหว่ คิดเป็นร้อยละ 9 จากจำนวนช่องโหว่ที่ประเมินพบ และผลการประเมินประสิทธิภาพกรอบการจัดการช่องโหว่ระบบสารสนเทศ อยู่ในระดับมาก ($\bar{X}$=4.48, S.D.=0.64)

คำสำคัญ กรอบการจัดการช่องโหว่ การรักษาความมั่นคงปลอดภัยทางไซเบอร์ การวิเคราะห์ช่องโหว่

[1] นักศึกษาหลักสูตรวิทยาศาสตร์มหาบัณฑิต แขนงวิชาเทคโนโลยีสารสนเทศและการสื่อสาร มหาวิทยาลัยสุโขทัยธรรมาธิราช 2639600317@stou.ac.th

[2] ผู้ช่วยศาสตราจารย์ สาขาวิชาวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยสุโขทัยธรรมาธิราช Khajitpan.Mak@stou.ac.th, * Corresponding Author

Abstract

This research aimed to develop the vulnerability management framework, analyze and assess vulnerabilities, and determine vulnerability remediating solution for the organization's information systems. NIST cybersecurity framework and vulnerability management life cycle by CDC were used as the framework prototypes for developing vulnerability management framework of this organization. The research methodologies consisted of 1) study the environment and characteristics of the organization's information systems, 2) develop the information system vulnerability management framework, and 3) implement the developed framework in the criteria of assets management, assessment, remediation, re-assessment, and verification. By using vulnerability analyzing tools of Nessus Essentials edition and Nexpose Community edition softwares, vulnerabilities of organization service mission servers such as Automatic Message Center server, Open MCU Conference server, web server, and VPN server were assessed. The research results showed that the developed framework was able to analyze vulnerabilities and to determine the vulnerability remediating solutions. The 34 vulnerabilities that affected and took risk to the organization were reduced to 3 vulnerabilities, approximately 9 percentage decrease, as a consequence of the implementation of this developed vulnerability management framework in practice. Additionally the performance evaluation of this developed framework was in the high level ($\bar{X}$=4.48, S.D.=0.64).

Keywords: Vulnerability management framework, Cybersecurity, Vulnerability analysis

บทนำ

ระบบสารสนเทศของกองบัญชาการกองทัพภาคที่ 2 ปัจจุบันมีภารกิจงานที่เกี่ยวกับระบบสารสนเทศขององค์กรอยู่หลายประการ ไม่ว่าจะเป็นการส่งข่าวสารผ่านทางระบบออนไลน์ การประชุมทางไกลผ่านจอภาพ เว็บไซต์ขององค์กร และระบบอื่นๆ จากอดีตที่ผ่านมาระบบสารสนเทศขององค์กรนั้นเคยถูกโจมตีจากผู้ไม่หวังดีในหลากหลายรูปแบบเช่น DDOS การเปลี่ยนหน้า Home Page การนำข้อมูลไปเผยแพร่ในสังคมออนไลน์ เป็นต้น กองบัญชาการกองทัพภาคที่ 2 จึงได้จัดหาระบบมาป้องกันการเจาะระบบในรูปแบบฮาร์ดแวร์ ซึ่งก็สามารถใช้งานได้ระดับที่น่าพอใจ แต่อย่างไรก็ดีระบบสารสนเทศขององค์กรนั้นยังไม่เคยผ่านการตรวจสอบ หรือการประเมินความเสี่ยงในด้านต่างๆ อย่างเป็นรูปธรรม ทำให้ระบบอาจจะยังไม่ปลอดภัยสูงสุด จึงเป็นที่มาในการทำงานวิจัย และเพื่อที่ผู้วิจัยซึ่งเป็นกำลังพลของกองทัพภาคที่ 2 และปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศขององค์กรอยู่แล้ว จะได้ทราบถึงช่องโหว่หรือจุดอ่อนต่างๆ ของระบบเพื่อทำการแก้ไขและนำเสนอผลงานวิจัยนี้ต่อผู้บังคับบัญชาเพื่อทำเป็นหลักการในการป้องกันระบบสารสนเทศขององค์กรต่อไป

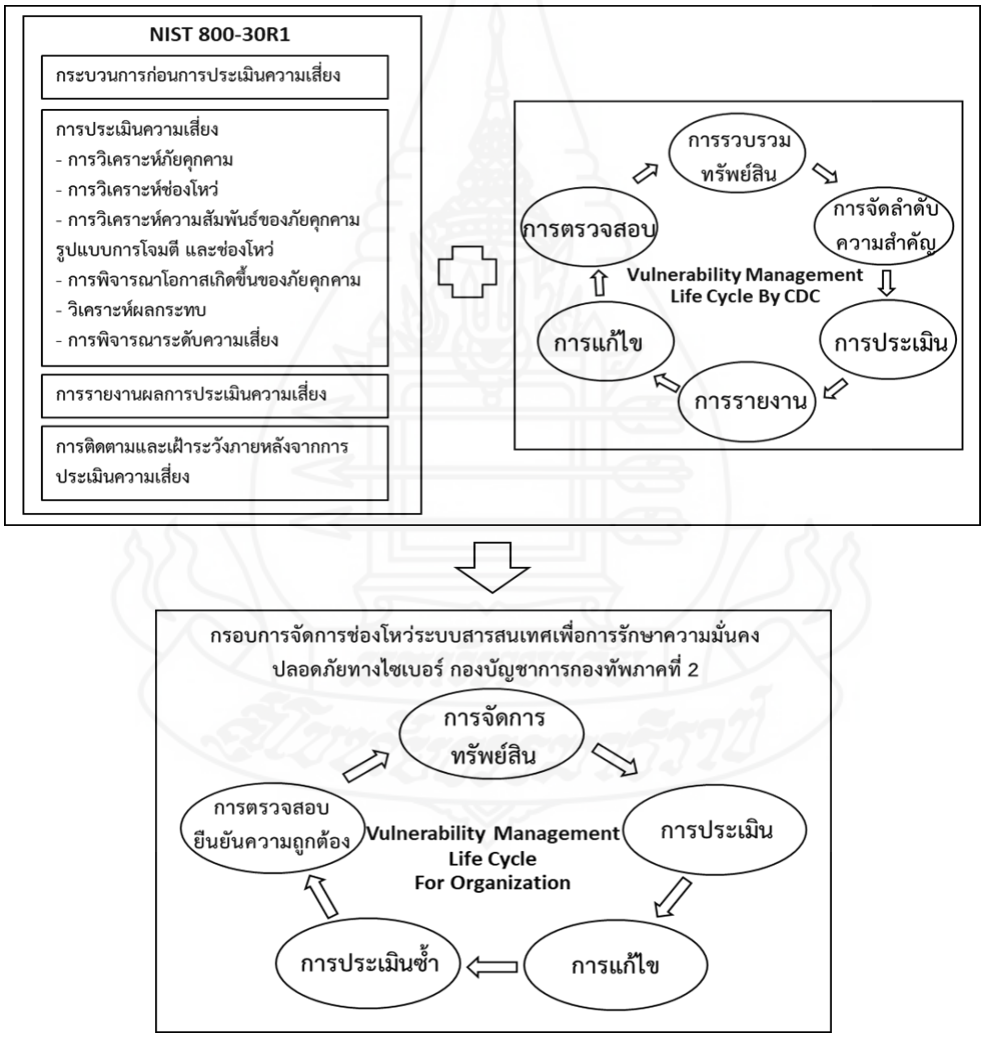
จากเหตุผลดังกล่าวผู้วิจัยจึงได้ทำรายงานการศึกษาค้นคว้าอิสระฉบับนี้ขึ้นมาเพื่อเป็นการนำเสนอแนวทางในการพัฒนากรอบการจัดการช่องโหว่ (Vulnerability Management) โดยการวิเคราะห์ เพื่อค้นหาช่องโหว่ของระบบสารสนเทศขององค์กร โดยอ้างอิงกรอบการรักษาความมั่นคงปลอดภัยทางไซเบอร์ (NIST Cybersecurity Framework) ซึ่งเป็นหนึ่งในกรอบทำงานด้านความมั่นคงปลอดภัยไซเบอร์ซึ่งเป็นที่นิยมใช้อย่างมากในปัจจุบัน (NIST, 2018) โดยดำเนินการตามกระบวนการประเมินความเสี่ยงตามกรอบแนวคิด NIST 800-30R1 Guide for Conducting Risk Assessment (Gallagher, P.D., 2012) จากการศึกษางานวิจัยที่ใช้กรอบแนวคิดของ NIST งานวิจัยเรื่อง การประเมินช่องโหว่ระบบบริหารจัดการทางการแพทย์ กรณีศึกษา โรงพยาบาลภูมิพลอดุลยเดช กรมแพทย์ทหารอากาศ (พัชรวัฒน์ โกสิตงามดีวงศ์, 2563) พบว่าผู้วิจัยได้นำกรอบแนวคิด NIST ในการดำเนินกระบวนการทำ Security Testing (Technical Guide to Information Security Testing and Assessment of Nation Institute of Standard and Technology U.S.Department Commerce, 2008) มาปรับใช้ในงานวิจัยพบว่าสามารถใช้กำจัดช่องโหว่ขององค์กรอย่างมีประเสิทธิภาพ และงานวิจัยเรื่อง โมเดลทางด้านเทคนิคสำหรับวิธีการประเมินความเสี่ยงความมั่นคงปลอดภัยในระบบสารสนเทศสำหรับโรงพยาบาล (สุรทศ ไตรติลานันท์ และ สุรพล รวยสูงเนิน, 2559) ได้นำกรอบแนวคิดของ NIST 800-30 และกรอบแนวคิดอื่นๆ มาสังเคราะห์ขั้นตอนในการประเมินความเสี่ยงในงานวิจัย พบว่าสามารถประเมินความเสี่ยงช่องโหว่ขององค์กรได้อย่างมีประสิทธิภาพ ผู้วิจัยจึงได้นำกรอบแนวคิดของ NIST มาปรับปรุงขั้นตอนและร่วมกับกรอบวงจรชีวิตในการจัดการช่องโหว่ ของศูนย์ควบคุมโรค สหรัฐอเมริกา (Vulnerability Management Life Cycle By CDC, 2021) ข้อดีของการนำกรอบแนวคิดของ CDC องค์กรสามารถนำมาปฏิบัติใช้ได้เป็นวงรอบซึ่งจะส่งผลดีต่อมาตราการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างมีประสิทธิภาพ ดังนั้นผู้วิจัยจึงนำข้อดีของกรอบแนวคิดทั้งสองมาพัฒนากรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กร เพื่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของกองบัญชาการกองทัพภาคที่ 2 ต่อไป

วัตถุประสงค์

1. เพื่อพัฒนากรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กร
2. เพื่อวิเคราะห์และประเมินช่องโหว่หรือจุดอ่อนของทรัพยากรระบบสารสนเทศขององค์กร
3. เพื่อกำหนดวิธีแก้ไขและหาแนวทางป้องกันการเข้าถึงช่องโหว่หรือจุดอ่อนของระบบสารสนเทศขององค์กร

กรอบแนวคิด

กรอบแนวคิดการวิจัยเรื่องการพัฒนากรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กร ได้นำขั้นตอนจากกรอบกรอบความมั่นคงปลอดภัยไซเบอร์ NIST กับ วงจรชีวิตการจัดการช่องโหว่โดย CDC กล่าวคือ ได้ใช้แนวคิด NIST 800-30R1 Guide (Risk Assessment Process) แนวทางการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ระดับองค์กร (อนาวิล แก้วสะอาด และ ณัฐวี อุตกฤษฎ์ ,2564) และกรอบแนวคิด VMLC CDC โดยการนำขั้นตอนจากกรอบแนวคิดทั้งสอง นำมาพัฒนากรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กร จึงทำให้เกิดกรอบการจัดการช่องโหว่ระบบสารสนเทศเพื่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์ กรณีศึกษา กองบัญชาการกองทัพภาคที่ 2 ตามภาพที่ 1



ภาพที่ 1 กรอบแนวคิดการพัฒนากรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กร

วิธีดำเนินการวิจัย

1. ศึกษาข้อมูล ทฤษฎี และงานวิจัยที่เกี่ยวข้องกับการพัฒนากรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กร

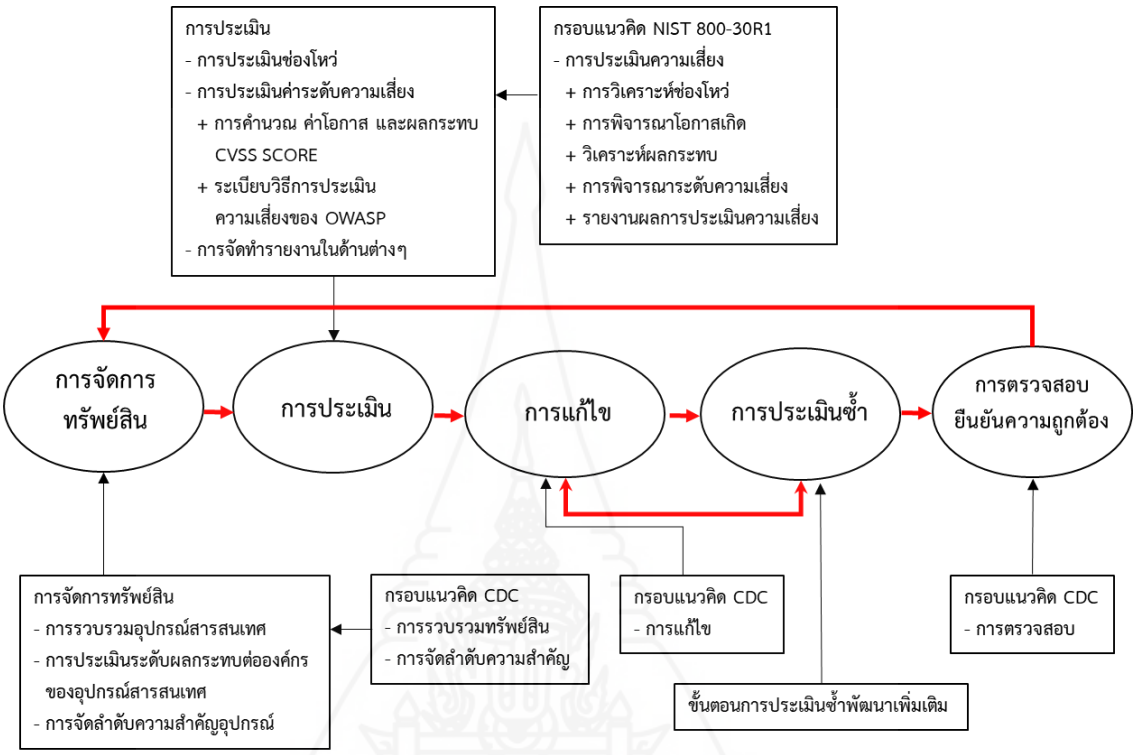
ผู้วิจัยได้ทำการศึกษาสำรวจแนวคิดและงานวิจัยที่เกี่ยวข้องซึ่งอ้างอิงตามกรอบความมั่นคงปลอดภัยไซเบอร์ของ NIST โดยอิงกระบวนการประเมินความเสี่ยงตามกรอบแนวคิดของ NIST 800-30R1 Guide for Conducting Risk Assessment (National Institute of Standards and Technology Special Publication 800-30, 2021) และวงจรชีวิตการจัดการช่องโหว่โดย CDC (Vulnerability Management Life Cycle By CDC) เพื่อให้ได้กรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กรที่มีความสอดคล้องกับเป้าหมายของการวิจัย

2. ศึกษาสภาพแวดล้อมและลักษณะของระบบสารสนเทศขององค์กร

ระบบสารสนเทศกองบัญชาการกองทัพภาคที่ 2 เป็นระบบที่พัฒนาขึ้นมาเพื่อช่วยปฏิบัติงานในภารกิจต่างๆ โดยใช้เทคโนโลยีที่มีอยู่ในปัจจุบันเข้ามาช่วยในการพัฒนางานตามภารกิจที่มีอยู่ เช่น ระบบศูนย์ข่าวอัตโนมัติ ระบบประชุมทางไกลผ่านจอภาพ เว็บไซต์ขององค์กร ระบบจำลองยุทธ จากการศึกษาพบว่ามีโอกาสเกิดปัญหาที่อาจจะถูกโจมตีทางด้านไซเบอร์จากผู้ไม่หวังดีได้ โดยเฉพาะอย่างยิ่งกับอุปกรณ์ที่มีการใช้งานผ่านเครือข่ายภายนอก

3. การพัฒนากรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กร

จากกรอบแนวคิดการวิจัย ผู้วิจัยได้นำข้อดีของทั้งสองกรอบแนวคิด และได้ลดขั้นตอนการดำเนินงาน โดยรวมขั้นตอนที่สามารถปฏิบัติได้ในเรื่องเดียวกันเช่นในกรอบ CDC ได้ปรับขั้นตอน การรวบรวมทรัพย์สิน กับ การจัดลำดับความสำคัญ รวมเป็นขั้นตอน การจัดการทรัพย์สิน ของกรอบที่พัฒนาขึ้นมา และได้นำขั้นตอน การรายงาน เข้าไปอยู่ในขั้นตอน การประเมิน เพื่อง่ายต่อการปฏิบัติ ส่วนหัวใจหลักสำคัญคือขั้นตอนการประเมินความเสี่ยงช่องโหว่ยังคงดำเนินตามกรอบของ NIST 800-30R1 ซึ่งจะอยู่ในขั้นตอน ประเมิน ของกรอบที่พัฒนาขึ้นมา ทั้งนี้เพื่อปรับให้เหมาะสมกับองค์กร ในการนำกรอบแนวคิดดังกล่าวมาใช้สามารถแสดงได้ตามภาพที่ 2

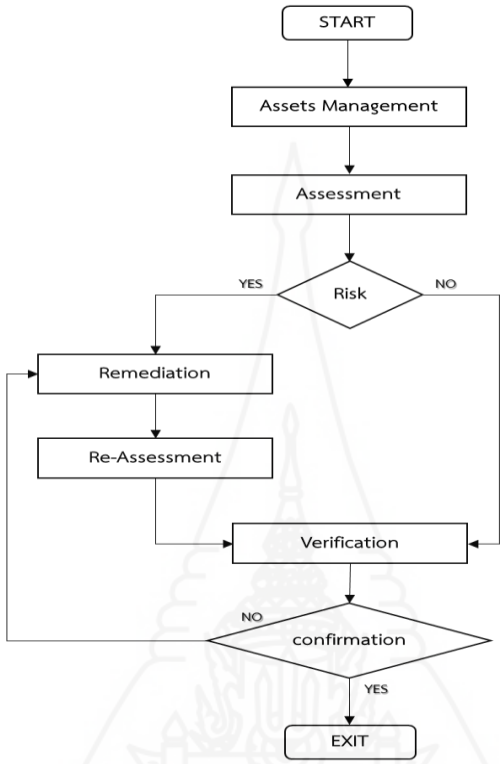


ภาพที่ 2 องค์ประกอบการพัฒนากรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กร

จากการวิเคราะห์ตามกรอบแนวคิดการพัฒนากรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กร จึงทำให้ได้กระบวนการในการดำเนินงานตามกรอบนี้ 5 ขั้นตอนด้วยกันคือ (1) การจัดการทรัพย์สินอุปกรณ์ระบบสารสนเทศ (Assets Management) (2) การประเมิน (Assessment) (3) การแก้ไขช่องโหว่ (Remediation) (4) การประเมินซ้ำ (Re-Assessment) (5) การตรวจสอบยืนยันความถูกต้อง (Verification)

4. ดำเนินการทดลองตามกรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กร

การดำเนินการทดลองตามกรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กร สามารถแสดงออกมาเป็นแผนผังหรืออัลกอลิทึม ตามกรอบที่พัฒนาขึ้นมาดังภาพที่ 3



ภาพที่ 3 ผังวงจรการทำงานกรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กร

4.1 การจัดการทรัพย์สินอุปกรณ์ระบบสารสนเทศ (Assets Management)

สำหรับการจัดการทรัพย์สินอุปกรณ์ระบบสารสนเทศ จะเป็นการรวบรวมอุปกรณ์สารสนเทศ ในที่นี้คือเครื่องแม่ข่ายที่ให้บริการงานในภารกิจต่างๆ เพื่อนำมาเข้ารับการประเมินช่องโหว่ โดยมีขั้นตอนการปฏิบัติดังนี้ (1) การรวบรวมอุปกรณ์สารสนเทศ (Discovering) (2) การประเมินระดับผลกระทบต่อองค์กรของอุปกรณ์สารสนเทศ (Assets Assessment) (3) การจัดลำดับความสำคัญอุปกรณ์สารสนเทศตามผลกระทบต่อองค์กร (Assets Prioritizetion) จากขั้นตอนทั้ง 3 ขั้นตอน ทำให้ได้อุปกรณ์เครื่องแม่ข่ายเข้ารับการประเมินช่องโหว่ตามตารางที่ 1 ดังนี้

ตารางที่ 1 การจัดอุปกรณ์สารสนเทศเข้ารับการประเมินช่องโหว่ในงานวิจัย

Assets/System	Lc	Li	La	Rd	OI Rating	วันเวลาเข้าตรวจประเมิน	
AMC Server	9	7	7	9	8.00	03/06/22	10:00 PM
WEB Server	6	5	9	9	7.25	06/06/22	8:00 PM
OpenMCU 1	7	7	5	9	7.00	09/06/22	5:00 PM
VPN PPTP	6	7	7	5	6.25	12/06/22	8:00 PM

จากตารางที่ 1 อุปกรณ์เครื่องแม่ข่ายที่เข้ารับการประเมินช่องโหว่จะพบค่า Lc, Li, La, Rd ซึ่งเป็นค่าปัจจัยผลกระทบต่อองค์กร (Organization Impact Factor) มีค่าคะแนน 0 – 9 โดยมีค่าเวกเตอร์ตามตารางที่ 2 ดังนี้

ตารางที่ 2 ปัจจัยผลกระทบต่อองค์กร (สุรทศ ไตรติลานันท์ และ สุรพล รวยสูงเนิน, 2559) (OWASP, 2008)

Organization Impact Factor	Case of Metric	Rating
การสูญเสียความลับ Loss of Confidentiality (Lc)	เปิดเผยข้อมูลที่ไม่ละเอียดอ่อนน้อยที่สุด (Minimal non-sensitive data disclosed)	2
	เปิดเผยข้อมูลสำคัญน้อยที่สุด (Minimal critical data disclosed)	6
	เปิดเผยข้อมูลที่ไม่ละเอียดอ่อนอย่างกว้างขวาง (Extensive non-sensitive data disclosed)	6
	เปิดเผยข้อมูลสำคัญอย่างยิ่ง (Extensive critical data disclosed)	7
	ข้อมูลทั้งหมดถูกเปิดเผย (All data disclosed)	9
การสูญเสียความสมบูรณ์ Loss of Integrity (Li)	ข้อมูลที่เสียหายเล็กน้อยน้อยที่สุด (Minimal slightly corrupt data)	1
	ข้อมูลที่เสียหายร้ายแรงน้อยที่สุด (Minimal seriously corrupt data)	3
	ข้อมูลที่เสียหายเล็กน้อยอย่างกว้างขวาง (Extensive slightly corrupt data)	5
	ข้อมูลที่เสียหายอย่างร้ายแรงอย่างกว้างขวาง (Extensive seriously corrupt data)	7
	ข้อมูลทั้งหมดเสียหายทั้งหมด (All data totally corrupt)	9
การสูญเสียความพร้อมในการให้บริการ Loss of Availability (La)	บริการรองน้อยที่สุดถูกขัดจังหวะ (Minimal secondary services interrupted)	1
	บริการหลักหยุดชะงักน้อยที่สุด (Minimal primary services interrupted)	5
	บริการรองจำนวนมากถูกขัดจังหวะ (Extensive secondary services interrupted)	5
	บริการหลักที่กว้างขวางหยุดชะงัก (Extensive primary services interrupted)	7
	บริการทั้งหมดหายไปอย่างสมบูรณ์ (All services completely lost)	9
ความเสียหายต่อชื่อเสียง Reputation damage (Rd)	ความเสียหายน้อยที่สุด (Minimal damage)	1
	การสูญเสียบัญชีหลัก (Loss of major accounts)	4
	การสูญเสียค่าความนิยม (Loss of goodwill)	5
	ความเสียหายต่อแบรนด์ (Brand damage)	9

ปัจจัยผลกระทบต่อองค์กร ตามตารางที่ 2 นำมาคำนวณหาค่าผลกระทบต่อองค์กร ของอุปกรณ์เครื่องแม่ข่ายในกรณีที่ไม่สามารถให้บริการได้เพื่อจะจัดลำดับความสำคัญในการเข้าประเมินช่องโหว่ โดยใช้สมการที่ (1) ดังนี้

OI = AVERAGE(Lc[x], Li[x], La[x], Rd[x]) (1)

OI คือ Organization Impact Value และ Lc[x], Li[x], La[x], Pd[x] ใช้ค่าตามตารางที่ 2

จากคำนวณตามสมการ (1) จะได้ค่าระดับผลกระทบต่อองค์กรของอุปกรณ์ระบบสารสนเทศตามตารางที่ 1

4.2 การประเมิน (Assessment)

ขั้นตอนการประเมินความเสี่ยงความมั่นคงปลอดภัยสารสนเทศของกองบัญชาการกองทัพภาคที่ 2 โดยแบ่งเป็น 3 ขั้นตอนคือ 1) การประเมินช่องโหว่ 2) การประเมินค่าระดับความเสี่ยง 3) การจัดทำรายงานในด้านต่างๆ

4.2.1 การประเมินช่องโหว่ (Vulnerability Assessment) คือขั้นตอนการระบุ (Risk Identify) เป็นการค้นหาช่องโหว่ของระบบสารสนเทศ หรือการทำ Vulnerability Scan โดยงานวิจัยนี้ใช้เครื่องมือช่วยตรวจสอบประเมินช่องโหว่อัตโนมัติ งานวิจัยนี้เลือกใช้เครื่องมือตรวจสอบประเมินช่องโหว่ที่อัตโนมัติคือ Nessus และ Nexpose ซึ่งรองรับ CVSS SCORE ผลการประเมินช่องโหว่พบจำนวนช่องโหว่ตามตารางที่ 3 ดังนี้

ตารางที่ 3 สรุปผลการประเมินช่องโหว่

ลำดับ	ชื่อเครื่อง	หมายเลขไอพี	High	Medium	Low
1.	AMC Server	203.xxx.xxx.xxx	1	5	2
2.	Web Server	203.xxx.xxx.xxx	2	5	2
3.	OpenMCU 1	10.0.xxx.xxx	2	4	3
4.	VPN PPTP	203.xxx.xxx.xxx	1	4	3
ผลการประเมินช่องโหว่จำนวนทั้งสิ้น 34 ช่องโหว่			6	18	10

ตารางที่ 4 รายละเอียดช่องโหว่ที่ประเมินพบ

ชื่อช่องโหว่	ชนิดรูปแบบช่องโหว่						รวม
	TLS/SSL/ X.509	SSH/FTP/ TELNET	DNS	Test-cgi	Unix OS	HTTP OPTION	
Nameserver Processes Recursive Queries			1				
DNS server allows cache snooping			1				
TLS/SSL Server is enabling the BEAST attack	1						
FTP credentials transmitted unencrypted	1	1					
X.509 Certificate Subject CN Does Not Match the Entity Name							
Self-signed TLS/SSL certificate on 203.xxx.xxx.xxx	1						
Test-cgi Script Information Disclosure Vulnerability				1			
Unix Operating System Unsupported Version Detection					1		
SSH Weak Algorithms Supported		1					
SSH Server Supports RC4 Cipher Algorithms		1					
X.509 Certificate Subject CN Does Not Match the Entity Name		1					
SSL Self-Signed Certificate	1						
Untrusted TLS/SSL server X.509 certificate	1						
SSL Medium Strength Cipher Suites Supported (SWEET32)	1						
TLS Version 1.0 Protocol Detection	1						
TLS Version 1.1 Protocol Deprecated	1						
HTTP OPTIONS Method Enabled						1	
TLS/SSL Server Supports The Use of Static Key Ciphers	1						
SSL Certificate Cannot Be Trusted	1						
SSL Self-Signed Certificate	1						
Untrusted TLS/SSL server X.509 certificate	1						
HTTP OPTIONS Method Enabled						1	
TLS/SSL Server Supports The Use of Static Key Ciphers	1						
SSH Birthday attacks on 64-bit block ciphers (SWEET32)		1					
Unencrypted Telnet Server		1					
SSH Server CBC Mode Ciphers Enabled		1					
SSH Weak MAC Algorithms Enabled		1					
SSL Certificate Cannot Be Trusted	1						
TLS Server Supports TLS version 1.1	1						
TLS/SSL Server Supports The Use of Static Key Ciphers	1						
TLS/SSL Server Is Using Commonly Used Prime Numbers	1						
SSH Server Supports diffie-hellman-group1-sha1		1					
SSH Weak Key Exchange Algorithms Enabled		1					
TLS Version 1.1 Protocol Deprecated	1						
	18	10	2	1	1	2	34

จากข้อมูลในตารางพบว่าชนิดของช่องโหว่ที่พบจำนวนมากที่สุดคือช่องโหว่ชนิด TLS/SSL/X.509 รองลงมาเป็นช่องโหว่ชนิด SSH/FTP/Telnet ซึ่งเป็นโพรโทคอลที่ให้บริการอยู่บนเครื่องแม่ข่ายเว็บเซิร์ฟเวอร์ และช่องโหว่ที่ประเมินพบนั้นเกี่ยวข้องกับพอร์ตที่เปิดให้บริการพบมากที่สุกคือพอร์ต 443 พอร์ต 21 และ 22 ซึ่งเป็นพอร์ต TCP/FTP ซึ่งใช้ในการรับส่งข้อมูลที่เรียกว่า HTTP หรือการใช้งานเว็บเวิร์ฟเวอร์นั่นเอง รวมถึงการให้บริการรับส่งข้อมูลแบบเข้ารหัสด้วย จากผลการวิเคราะห์และประเมินช่องโหว่ดังกล่าว ช่องโหว่ที่ประเมินพบส่วนมากเป็นช่องโหว่ที่เกิดจากเครื่องแม่ข่ายที่ให้บริการในลักษณะของเว็บเซิร์ฟเวอร์ ซึ่งใช้งานจากเครื่อข่ายภายนอก นอกจากนี้ผู้วิจัยยังได้ใช้มาตรฐานความมั่นคงปลอดภัยของเว็บแอปพลิเคชัน (OWASP 10) นำมาประเมินกับช่องโหว่ที่ประเมินพบ พบว่ามีช่องโหว่ตามมาตรฐาน OWASP 10 ในระดับ A02 (Cryptographic Failures) 19 ช่องโหว่ ซึ่งเกี่ยวกับการเข้ารหัสที่อ่อนแอ ซึ่งก็ตรงกับการวิเคราะห์ช่องโหว่ที่กล่าวมาแล้ว โดยพบจากเครื่องมือ Nessus จำนวน 9 ช่องโหว่ และเครื่องมือ Nexpose จำนวน 10 ช่องโหว่ ซึ่งแสดงให้ว่าเครื่องมือทั้งสองมีประสิทธิภาพทางด้านเทคนิคในการประเมินช่องโหว่ที่เกี่ยวกับเว็บแอปพลิเคชันในระดับที่เท่ากัน สำหรับเครื่องมือประเมินช่องโหว่ Nessus และ Nexpose นอกจากจะมีข้อดีของ CVE / CVSS / ฐานข้อมูลช่องโหว่ของเครื่องเองแล้ว ข้อดีอีกประการคือ เป็นเครื่องมือที่มีลักษณะทำงานเป็นการประเมินช่องโหว่ที่หลากหลายเป้าหมาย (Multi Scanner) คือทำการประเมินได้ทั้ง ระบบเครือข่าย, ระบบปฏิบัติการ, ฐานข้อมูล และ เว็บเซิร์ฟเวอร์ จึงเป็นเครื่องมือที่เหมาะสมที่นำมาใช้ในงานวิจัยนี้ โดยเฉพาะกับองค์กรที่มีเครื่องแม่ข่ายที่ให้บริการในหลายรูปแบบ

4.2.2 การประเมินค่าระดับความเสี่ยง (Risk Assessment) คือขั้นตอนการประเมินค่าระดับความเสี่ยง (Risk Evaluate) เป็นขั้นตอนการคำนวณหรือประเมินค่าระดับความสำคัญของความเสี่ยงแบ่งเป็น 6 ขั้นตอนดังนี้

1) การประเมินค่าโอกาสและผลกระทบใช้วิธี การคำนวณตาม CVSS 2.0 Base Vector

การประเมินค่าโอกาสและผลกระทบและมีวิธีการคำนวณตามสมการ (2) และ (3) ดังนี้

Lik = 20* AV*AC*Au (2)

Imp = 10.41*(1-(1-C)*(1-I)*(1-A)) (3)

เมื่อ Imp คือ Impact Value และ Lik คือ Likelihood หรือ Exploitability ValueC, I, A, AV, AC, Au มีค่าตามตารางที่ 5

ตารางที่ 5 ความหมายและค่า Base Metric CVSS 2.0

Base Metric	Case of Metric	Value
เวกเตอร์การเข้าถึง Access Vector (AV)	กำหนดเฉพาะเครือข่ายภายใน L: requires local access	0.395
	เครือข่ายใกล้เคียงเข้าถึงได้ A: adjacent network accessible	0.646
	เข้าถึงได้จากทุกเครือข่าย N: network accessible	1
ความซับซ้อนการเข้าถึง Access Complexity (AC)	มีความซับซ้อนสูง H: high	0.35
	มีความซับซ้อนปานกลาง M: medium	0.61
	มีความซับซ้อนต่ำ L: low	0.71
การพิสูจน์ตัวจริง Authentication (Au)	ตรวจสอบสิทธิ์หลายครั้ง M: requires multiple instances of authentication	0.45
	ตรวจสอบสิทธิ์รายการเดียว S: requires single instances of authentication	0.56
	ไม่มีการตรวจสอบสิทธิ์ N: requires no authentication	0.704
ผลกระทบต่อการรักษาความลับ Confidentiality Impact (C)	ไม่มีผลกระทบ N: none	0
	มีผลกระทบบางส่วน P: partial	0.275
	มีผลกระทบอย่างครับถ้วน C: complete	0.66
ผลกระทบความครบถ้วนสมบูรณ์ Integrity Impact (I)	ไม่มีผลกระทบ N: none	0
	มีผลกระทบบางส่วน P: partial	0.275
	มีผลกระทบอย่างครับถ้วน C: complete	0.66
ผลกระทบความพร้อมใช้งาน Availability Impact (A)	ไม่มีผลกระทบ N: none	0
	มีผลกระทบบางส่วน P: partial	0.275
	มีผลกระทบอย่างครบถ้วน C: complete	0.66

ที่มา: (A Complete Guide to the Common Vulnerability Scoring System Version 2.0 Retrieved November 6, 2021)

2) การปรับค่าคะแนนให้อยู่ในช่วงระดับคะแนนให้สอดคล้อง OWASP RISK RATING ให้มีช่วงคะแนนอยู่ระหว่าง 1–9 มีวิธีการคำนวณตามสมการ (4), (5) และ (6)

NLik = Norm(Likelihood Value) (4)

NImp = Norm(Impact Value) (5)

Norm(Xi) = 9*(Xi)/Xn (6)

เมื่อ NLik คือ Normalize Likelihood Value (เป็นการปรับระดับค่าโอกาสจากช่วงค่าคะแนน 0 – 10 มาเป็นช่วงค่าคะแนน 0 – 9 ตามช่วงคะแนนตามตารางที่ 6)

NImp คือ Normalize Impact Value (เป็นการปรับระดับค่าผลกระทบจากช่วงค่าคะแนน 0 – 10 มาเป็นช่วงค่าคะแนน 0 – 9 ตามช่วงคะแนนตามตารางที่ 6)

Xi คือ Likelihood or Impact Value (ค่าคะแนนของค่าโอกาสและผลกระทบที่หาได้จากสมการ (2) และ (3)

Xn คือ Rate Number of Old Value (ค่าช่วงคะแนนเดิมก่อนจะปรับเป็นช่วงคะแนนใหม่ ในที่นี้ Xn มีค่าเท่ากับ 10)

ตารางที่ 6 ช่วงคะแนนโอกาส และผลกระทบ (OWASP Testing Guide, 2008)

Likelihood and Impact Levels	
0 to < 3	ระดับต่ำ LOW (1)
3 to < 6	ระดับกลาง MEDIUM (2)
6 to < 9	ระดับสูง HIGH (3)

3) การเพิ่มปัจจัยด้านผลกระทบ (สุรทศ ไตรติลานันท์ และ สุรพล รวยสูงเนิน, 2559) Organization Impact = Factor [X] โดยทำการประเมินผลกระทบต่อองค์กรโดยใช้สมมติฐานกรณี ระบบสารสนเทศล้มเหลว/ไม่สามารถใช้งานได้มีวิธีการคำนวณตามสมการ (1)

4) การประเมินค่าปัจจัยผลกระทบรวมโดยมีวิธีการคำนวณตามสมการ (7)

New Impact(NI) = Average(I, OI) .....(7)

I คือ Impact Value และ OI คือ Organization Impact

5) การประเมินระดับโอกาสและระดับผลกระทบ

โดยใช้ค่า NLik จากขั้นตอนที่ 2) เป็นค่า LikelihoodValue

และค่า New Impact จากขั้นตอนที่ 4) เป็นค่า Impact Value ประเมินตามตารางที่ 7

6) การประเมินระดับความสำคัญของความเสี่ยงของแต่ละความเสี่ยงโดยนำค่า Likelihood Level และ Impact Level มาประเมินตามตารางที่ 7

ตารางที่ 7 เมตริกความเสี่ยง (OWASP Testing Guide, 2008)

ความรุนแรงของความเสี่ยงโดยรวม (Overall Risk Severity)				
ผลกระทบ (Impact)	ระดับสูง (High) (3)	ระดับความเสี่ยงปานกลาง (Medium)	ระดับความเสี่ยงสูง (High)	ระดับความเสี่ยงวิกฤต (Critical)
	ระดับกลาง (Medium) (2)	ระดับความเสี่ยงต่ำ (Low)	ระดับความเสี่ยงปานกลาง (Medium)	ระดับความเสี่ยงสูง (High)
	ระดับต่ำ (Low) (1)	ระดับความเสี่ยงต่ำมาก แต่ให้บันทึกไว้ (Note)	ระดับความเสี่ยงต่ำ (Low)	ระดับความเสี่ยงปานกลาง (Medium)
		ระดับต่ำ (Low) (1)	ระดับกลาง (Medium) (2)	ระดับสูง (High) (3)
	โอกาสเกิด (Likelihood)			

ตัวอย่างการประเมินความเสี่ยงช่องโหว่ที่ส่งลกระทบต่อองค์กร

1) ผลการประเมินผลกระทบองค์กรของระบบสารสนเทศเป้าหมายซึ่งมีผลการประเมินตามตารางที่ 8

ตารางที่ 8 ระดับผลกระทบของอุปกรณ์ระบบสารสนเทศที่มีต่อองค์กร

Assets/System	Lc	Li	La	Rd	OI Rating
AMC Server	9	7	7	9	8.00
WEB Server	6	5	9	9	7.25
OpenMCU 1	7	7	5	9	7.00
VPN PPTP	6	7	7	5	6.25

ตัวอย่างที่ 1 AMC Server หาค่าผลกระทบของอุปกรณ์ระบบสารสนเทศที่มีต่อองค์กร

A) ระบุระดับผลกระทบตามตารางที่ 8

Organization Impact Factor โดยมีค่า Lc = 9 , Li = 7 , La = 7 , Rd = 9

B) คำนวณผลกระทบต่อองค์กร ของอุปกรณ์เครื่องแม่ข่ายตามสมการที่ (1)

OI = AVERAGE (Lc[A], Li[E2], La[E2], Rd[B])

OI = AVERAGE (9, 7, 7, 9) = 8.00

ดังนั้นระดับผลกระทบ (OI Rating) คือ 8.00

2) ผลการการประเมินค่าความเสี่ยงของระบบสารสนเทศขององค์กร มีผลการประเมินตามตารางที่ 9 และ 10

ตัวอย่างที่ 2 OpenMCU Server 1 ชื่อช่องโหว่ : SSH Server Supports RC4 Cipher Algorithms

มีค่า Vector : CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N

A) คำนวณค่าโอกาส (Lik) จากสมการ .....(2)

Lik = 20*AV[N]*AC[M]*Au[N]

Lik = 20*1*0.61*0.704 = 8.6

B) คำนวณค่าผลกระทบ (Imp) ตามสมการ .....(3)

Imp = 10.41*(1-(1-C[P])*(1-I[N])*(1-A[N]))

Imp = 10.41*(1-(1-0.275)*(1-0)*(1-0)) = 2.9

C) ปรับค่าโอกาสใหม่ (NLik) ตามสมการ .....(4)

NLik = Norm(Lik) = $9*(X_i)/X_n$ .....(6)

NLik = 9*8.6/10 = 7.74 ตามสมการ

ดังนั้นค่าคะแนนผลกระทบ (Likelihood) L คือ 7.74

D) ปรับค่าผลกระทบใหม่ (NImp) ตามสมการ .....(5)

NImp = Norm(Imp) = $9*(X_i)/X_n$ .....(6)

NImp = 9*2.86/10 = 2.61

ดังนั้นค่าคะแนนผลกระทบ (Impact) I คือ 2.61

E) นำค่าผลกระทบต่อองค์กร (OI) จากตารางที่ 7

OI = 7.00

F) คำนวณค่าผลกระทบใหม่ (NI) ตามสมการที่ .....(7)

NI = Average (I, OI)

NI = Average (2.61, 7.00) = 4.80

ดังนั้นค่าคะแนนผลกระทบใหม่ NI คือ 4.80

G) นำค่า L, I, และ NI จากขั้นตอน C), D), F) ประเมินระดับโอกาส/ผลกระทบตามตารางที่ 6

L × I = HIGH (3) × LOW (1) = 3 × 1

L × NI = HIGH (3) × MEDIUM (2) = 3 × 2

H) นำค่า L × I และ L × NI จากขั้นตอน G) มาประเมินระดับความสำคัญความเสี่ยงก่อนเพิ่มผลกระทบต่อองค์กร (RISK) และหลังเพิ่มผลกระทบต่อองค์กร (RISK+) ตามตารางที่ 9

RISK = L × I = 3 × 1 = Medium

RISK+ = L × NI = 3 × 2 = High

ดังนั้นระดับความเสี่ยงก่อนเพิ่มผลกระทบต่อองค์กร (RISK) คือ MEDIUM และหลังเพิ่มผลกระทบต่อองค์กร (RISK+) คือ HIGH

ตารางที่ 9 ตัวอย่างผลการประเมินผลกระทบและโอกาสที่จะเกิด

Assets/System	Vulnerability	CVSS	L	I	OI	NI
OpenMCU 1	SSH Server Supports RC4 Cipher Algorithms	CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N	7.74	2.61	7.00	4.80

ตารางที่ 10 ตัวอย่างรูปแบบผลการประเมินความเสี่ยงช่องโหว่ระบบสารสนเทศขององค์กร

Assets/System	Vulnerability	L x I	Risk	L x NI	Risk+
OpenMCU 1	SSH Server Supports RC4 Cipher Algorithms	3 x 1	Med	3 x 2	High

จากตารางที่ 10 เป็นผลของการคำนวณค่าความเสี่ยง ของขั้นตอนการประเมินความเสี่ยงช่องโหว่ที่ประเมินพบที่ส่งผลกระทบต่อองค์กร จากตัวอย่างในตารางพบว่าในการคำนวณรูปแบบความเสี่ยงตามปกติจะได้ระดับความเสี่ยงตรงกับค่า Base Score มาตรฐาน เช่น ในเครื่องแม่ข่าย OpenMCU 1 มีช่องโหว่ที่ชื่อ SSH Server Supports RC4 Cipher Algorithms คำนวณค่าระดับความเสี่ยงได้ค่าระดับ (ปานกลาง) แต่เมื่อเพิ่มค่าผลกระทบขององค์กร (NI) เข้าไปในการคำนวณด้วยแล้วจะทำให้ค่าระดับความเสี่ยงเพิ่มขึ้นเป็นค่าระดับ (สูง)

4.2.3 การจัดทำรายงานในด้านต่างๆ (Report) การรายงานผลของการประเมินความเสี่ยงช่องโหว่ที่มีผลกระทบต่อระบบสารสนเทศขององค์กร เป็นขั้นตอนที่จัดทำขึ้นเพื่อรายงานให้ผู้ที่มีสวนเกี่ยวข้องต่อระบบสารสนเทศขององค์กรเช่น ในส่วนของผู้บังคับบัญชา และ CIO ขององค์กร จะได้รับทราบและให้การสนับสนุนในการแก้ปัญหาที่ตรวจพบเพื่อที่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับการดูแลรักษาความมั่นคงปลอดภัยต่อระบบสารสนเทศขององค์กร จะได้นำรายงานที่จัดทำขึ้นมานี้ไปแก้ไขจุดบกพร่องหรือจุดอ่อนของระบบสารสนเทศ ตามกรอบการจัดการช่องโหว่ฯ ที่พัฒนาขึ้นมานี้ได้อย่างสมบูรณ์

ตารางที่ 10 ตัวอย่างรายงานผลการประเมินค่าความเสี่ยงช่องโหว่ระบบสารสนเทศขององค์กร

อุปกรณ์/ระบบสารสนเทศ	ช่องโหว่ที่ประเมินพบ	ผลการประเมินความเสี่ยง RISK	ผลการประเมินความเสี่ยง+ผลกระทบต่อองค์กร RSIK+	หมายเหตุ
ระบบศูนย์ข่าวอัตโนมัติ (AMC Server)	TLS/SSL Server is enabling the BEAST attack	ระดับกลาง	ระดับสูง	กำลังดำเนินการแก้ไข
ระบบประชุมทางไกล OpenMCU 1	SSH Server Supports RC4 Cipher Algorithms	ระดับกลาง	ระดับสูง	กำลังดำเนินการแก้ไข

4.3 การแก้ไขช่องโหว่ (Remediation)

รายละเอียดช่องโหว่ที่พบนั้น เครื่องมือ Nessus และ Nexpose มีข้อมูลของช่องโหว่ที่พบและวิธีการแก้ไขอย่างละเอียด ซึ่งสอดคล้องการงานวิจัย การประเมินช่องโหว่ระบบเทคโนโลยีสารสนเทศ กรณีศึกษา ธนาคารพาณิชย์แห่งหนึ่งในประเทศไทย (ธเนศ อมรทัศนสุข, 2557) และงานวิจัย การประเมินช่องโหว่ระบบบริหารจัดการทางการแพทย์ กรณีศึกษาโรงพยาบาลภูมิพลอดุลยเดช กรมแพทย์ทหารอากาศ (พัชรวัฒน์ โกสิตงามดีวงศ์, 2563) ซึ่งต่างออกไปจากงานวิจัย การประเมินช่องโหว่ระบบสารสนเทศ กรณีศึกษา มหาวิทยาลัยราชภัฏรำไพพรรณี (ขนิษฐา สิทธิเทียมจันทร์ สุภาพร นพเวช และสาธิต สุวรรณเวช, 2564) ที่ใช้โอเพนซอร์สในการประเมินพบว่ารายละเอียดที่ที่ใช้ในการแก้ไขช่องโหว่ไม่ละเอียดเท่าที่ควร ดังนั้นในการแก้ไขช่องโหว่ในงานวิจัยนี้ส่วนใหญ่จะรายละเอียดการแก้ไขมาจาก เครื่องมือ Nessus และ Nexpose ที่ใช้ในงานวิจัยนี้

ตัวอย่างการแก้ไขช่องโหว่ที่ชื่อ HTTP OPTIONS Method Enabled ของอุปกรณ์เครื่องแม่ข่าย WEB Server มีรายละเอียดช่องโหว่คือ เว็บเซิร์ฟเวอร์ที่ตอบสนองต่อเมธอด OPTIONS HTTP จะเปิดเผยวิธีการอื่นๆ ที่เว็บเซิร์ฟเวอร์สนับสนุน วิธีนี้สามารถช่วยให้ผู้โจมตีค้นหาข้อมูลเกี่ยวกับการกำหนดค่าเซิร์ฟเวอร์และเป็นช่องโหว่ในการโจมตีได้ วิธีแก้ไขให้ดำเนินการปิดใช้งาน HTTP OPTIONS บนเว็บเซิร์ฟเวอร์ ขั้นตอนการปิดใช้งาน HTTP OPTIONS บน Apache มีดังนี้

1) ก่อนดำเนินการปิดใช้งาน HTTP ต้องเปิด mod_rewrite (.htaccess) ในเว็บเซิร์ฟเวอร์ Apache เปิดไฟล์ .htaccess โดยทั่วไปจะอยู่ที่ /var/www/html/.htaccess โดยใช้คำสั่ง

$ sudo vi /var/www/html/.htaccess

2) ปิดการใช้งาน HTTP OPTIONS วิธีเพิ่มบรรทัดต่อไปนี้ใน ไฟล์. htaccess เพื่อปิดใช้งานเมธอด OPTIONS, TRACE และ TRACK โดยใช้คำสั่ง

```
RewriteEngine On
RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK|OPTIONS)
RewriteRule .* - [F]
```

3) รีสตาร์ท Apache Web Server เพื่อใช้การเปลี่ยนแปลงโดยใช้คำสั่ง

$ sudo service apache2 restart

สำหรับแนวทางป้องกันการเข้าถึงช่องโหว่หรือจุดอ่อนของระบบสารสนเทศขององค์กร ควรนำผลจากการวิเคราะห์ช่องโหว่ที่ประเมินพบ นำมาศึกษารายละเอียดทางด้านเทคนิค เช่น พอร์ตที่เปิดใช้งาน โพรโทคอลต่างๆ ที่เกี่ยวข้องกับช่องโหว่ เพื่อทำการแก้ไขช่องโหว่ และกำหนดแนวทางป้องกัน โดยให้ความสำคัญจากผลวิเคราะห์ ถึงรูปแบบและแนวทางที่จะก่อให้เกิดปัญหาจากช่องโหว่นั้นๆ ได้ และควรกำหนดใช้กรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กรที่พัฒนาขึ้นมา ดำเนินการขั้นตอนตามกรอบให้สมบูรณ์และกำหนดวงรอบในการปฏิบัติให้เหมาะสม ทำให้สามารถป้องกันการถูกโจมตีหรือการเข้าถึงช่องโหว่จากผู้ไม่หวังดีได้

4.4 การประเมินซ้ำ (Re-Assessment)

การประเมินซ้ำ คือขั้นการประเมินช่องโหว่ซ้ำ เป็นการเริ่มกระบวนการใหม่ทั้งหมดในการทำการสแกนช่องโหว่ของอุปกรณ์ระบบสารสนเทศที่ได้รับการแก้ไขช่องโหว่มาแล้ว กรณีพบช่องโหว่หลังจากการแก้ไขแล้ว ให้ดำเนินการการแก้ไขช่องโหว่จนกว่าช่องโหว่นั้นจะปิดลงอย่างสมบูรณ์ กรณีไม่พบช่องโหว่หลังการแก้ไข ให้ดำเนินการรวบรวมจัดทำรายงานการดำเนินการประเมินช่องโหว่ของระบบสารสนเทศของ เพื่อดำเนินการส่งรายงานดังกล่าวไปดำเนินการในขั้นตอนการตรวจสอบยืนยันความถูกต้อง (Verification) ต่อไป

4.5 การตรวจสอบยืนยันความถูกต้อง (Verification)

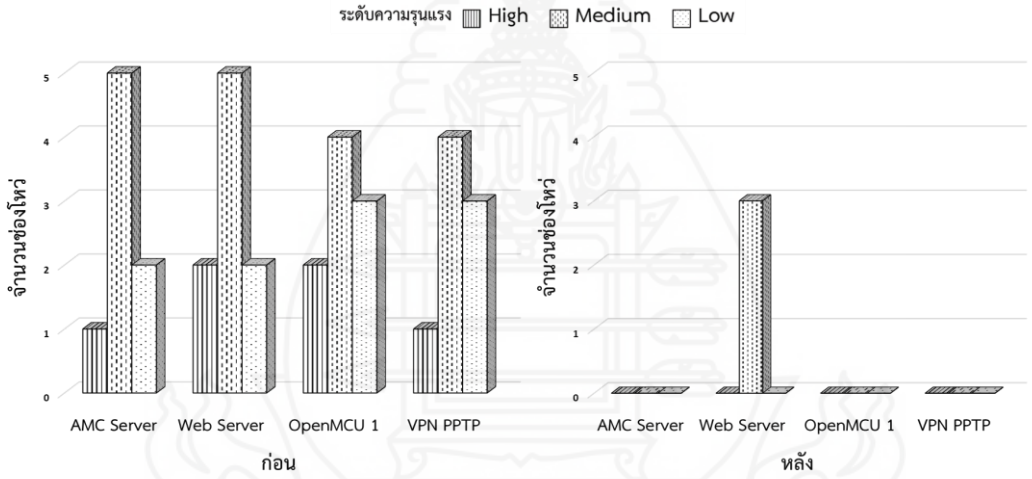
รวบรวมข้อมูลทำเป็นรูปแบบรายงานตั้งแต่ขั้นตอนเริ่มต้นตามกรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กร นำเสนอคณะกรรมการ การรักษาความมั่นคงปลอดภัยไซเบอร์ ทภ.2 เพื่อให้ช่วยตรวจสอบความถูกต้องในการจัดการช่องโหว่ และให้ข้อเสนอแนะในการแก้ไขปรับปรุงในการแก้ไขช่องโหว่สารสนเทศขององค์กรที่เกิดขึ้น เพื่อความถูกต้องและเพิ่มประสิทธิภาพในการป้องกันความเสี่ยงที่เกิดขึ้นจากช่องโหว่ของระบบสารสนเทศที่จะส่งผลกระทบต่อองค์กร

ผลการวิจัย

1. จากการดำเนินตามกระบวนการกรอบการจัดการช่องโหว่สารสนเทศขององค์กร สามารถกำหนดอุปกรณ์เครื่องแม่ข่ายในการเข้ารับการประเมินช่องโหว่ โดยคัดเลือกด้วยวิธีการนำปัจจัยผลกระทบทางด้านเทคนิคมาประเมินอุปกรณ์เครื่องแม่ข่ายได้อย่างเหมาะสม โดยใช้เครื่องมือในการประเมิน 2 เครื่องมือ คือ Nessus เวอร์ชัน Essentials และ Nexpose

เวอร์ชัน Community ทำให้การประเมินช่องโหว่มีความละเอียดมากยิ่งขึ้น ด้านการประเมินค่าระดับความเสี่ยง ได้ใช้การประเมินค่าโอกาสและผลกระทบ จากการคำนวณตาม CVSS รวมกับ ระเบียบวิธีการประเมินความเสี่ยงของ OWASP เพื่อให้การประเมินค่าระดับความเสี่ยงงานวิจัยนี้มีความน่าเชื่อถือ

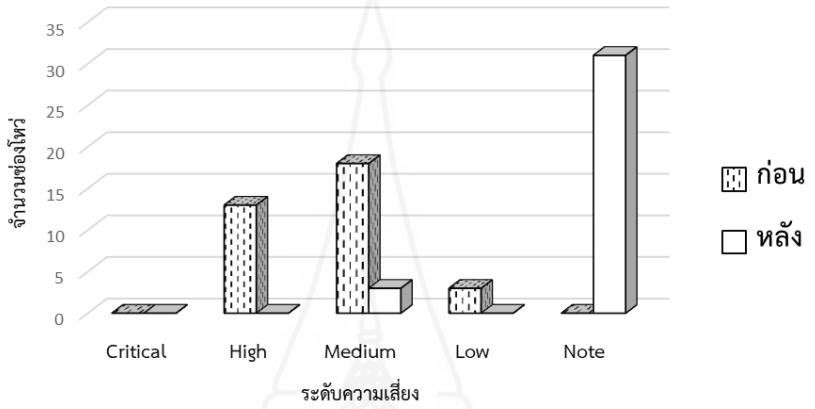
2. จากผลการทดลองการประเมินช่องโหว่ที่พบและมีความเสี่ยงทั้งหมดจำนวน 34 ช่องโหว่ ช่องโหว่ที่ประเมินพบจำนวนมากที่สุดคือช่องโหว่ชนิด TLS/SSL/X.509 รองลงมาเป็นช่องโหว่ชนิด SSH/FTP/Telnet ซึ่งเป็นโพรโทคอลที่ให้บริการอยู่เครื่องแม่ข่ายเว็บเซิร์ฟเวอร์ สามารถวิเคราะห์ได้ว่าช่องโหว่ที่ประเมินพบส่วนมากเป็นช่องโหว่ที่เกิดจากเครื่องแม่ข่ายที่ให้บริการในลักษณะของเว็บเซิร์ฟเวอร์ ซึ่งใช้งานจากเครื่อข่ายภายนอก จึงควรให้ความสำคัญในการป้องกันการเข้าถึงของผู้ไม่หวังดีอย่างเข้มงวด หลังจากการแก้ไขช่องโหว่และการประเมินซ้ำ พบช่องโหว่ความรุนแรงระดับ กลาง จำนวน 3 ช่องโหว่ ตามภาพที่ 4 ซึ่งแสดงว่าจากการทดลองการแก้ไขช่องโหว่ และการใช้แนวทางการป้องกันการเข้าถึงช่องโหว่ โดยปฏิบัติตามกรอบที่พัฒนาขึ้นมานั้นสามารถปัญหาที่เกิดจากช่องโหว่ได้



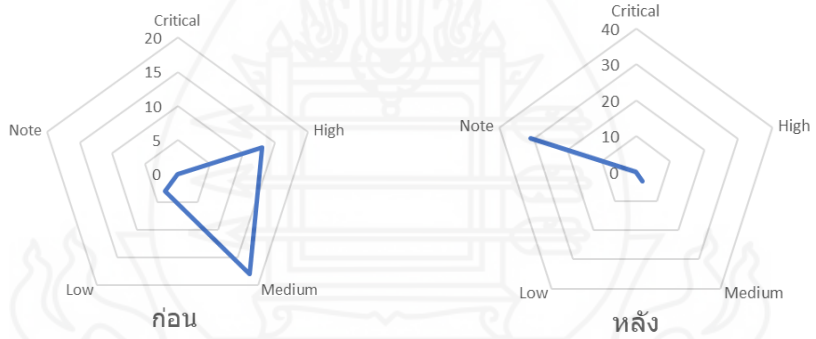
ภาพที่ 4 เปรียบเทียบจำนวนช่องโหว่ก่อนและหลังการประเมินช่องโหว่ซ้ำ

3. การประเมินความเสี่ยงช่องโหว่ที่มีผลต่อองค์กร พบว่าหลังการประเมินช่องโหว่ซ้ำ ความเสี่ยงของช่องโหว่ลดลงอย่างชัดเจนจะเหลือความเสี่ยงของช่องโหว่ระดับปานกลาง 3 ช่องโหว่ ตามภาพที่ 5 แนวโน้มทิศทางความเสี่ยงช่องโหว่มีทิศทางที่น่าพอใจ โดยความเสี่ยงของช่องโหว่อยู่ระดับ ต่ำ ดังแสดงตามภาพที่ 6 สังเกตุจากภาพแผนภูมิหลังการประเมินช่องโหว่เส้นกราฟจะชี้ไปที่ระดับ Note หมายความว่าไม่มีความเสี่ยง หรือ เว็บไซต์/เว็บแอพพลิเคชั่น/เครื่องคอมพิวเตอร์แม่ข่ายมีการควบคุมที่เพียงพอ/สถานะยังมีความปลอดภัย แต่ยังคงต้องบันทึกรายละเอียดข้อมูลต่างๆ ของช่องโหว่ที่ได้รับการแก้ไขและยังมีส่วนปลายเล็กน้อยชี้ไปยังความเสี่ยง ระดับปานกลาง (Medium) นั่นคือจำนวนช่องโหว่ที่ยังคงอยู่ สาเหตุที่ยังคงมีช่องโหว่คือ เป็นช่องโหว่ที่เกี่ยวกับใบรับรองดิจิทัลที่ไม่เป็นที่ยอมรับในระดับสากล (SSL Certificate) ต้องใช้งบประมาณในการจัดซื้อ ซึ่งจะต้องแก้ไขทางธุรการต่อไป จากผลการประเมินความเสี่ยงช่องจำนวน 34 ช่องโหว่ ช่องโหว่ที่ได้รับแก้ไขเรียบร้อยและไม่มีความเสี่ยงจำนวน 31 ช่องโหว่ และยังเหลือช่องโหว่ระดับปานกลาง 3 ช่องโหว่ จึงมีค่าเฉลี่ยรวมความเสี่ยงของช่อง

โหว่ที่ส่งผลกระทบต่อองค์กรอยู่ในระดับ ต่ำ ดังนั้นจึงสรุปได้ว่าการดำเนินการตามกระบวนการ กรอบการจัดการช่องโหว่สารสนเทศขององค์กร ของวิจัยนี้สามารถกำจัดช่องโหว่หรือจุดอ่อนของระบบสารสนเทศขององค์กรได้อย่างมีประสิทธิภาพ



ภาพที่ 5 ผลการประเมินความเสี่ยงช่องโหว่ที่มีผลต่อองค์กร ก่อนและหลังการประเมินช่องโหว่ซ้ำ



ภาพที่ 6 แนวโน้มทิศทางความเสี่ยงช่องโหว่ที่มีผลต่อองค์กร ก่อนและหลังการประเมินช่องโหว่ซ้ำ

4. การประเมินประสิทธิภาพ กรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กร โดยจัดทำแบบสอบถามในการประเมินประสิทธิภาพโดยมีกลุ่มตัวอย่างจำนวน 19 คน โดยทั้งหมดเป็นบุคลากรที่เกี่ยวข้องกับระบบสารสนเทศขององค์กร ทำการประเมินประสิทธิภาพด้านการจัดการทรัพย์สินอุปกรณ์สารสนเทศ การประเมิน การแก้ไขช่องโหว่ การประเมินซ้ำ การตรวจสอบยืนยันความถูกต้อง และความคิดเห็นต่อกรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กร ผลการประเมินมีค่าเฉลี่ยโดยรวมเท่ากับ 4.48 และค่าเบี่ยงเบนมาตรฐานเท่ากับ 0.64 ระดับการประเมินประสิทธิภาพกรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กรอยู่ในระดับ มาก

อภิปรายผลการวิจัย

กรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กร เป็นงานวิจัยที่ดำเนินการขึ้นมาเพื่อพัฒนาการรักษาความมั่นคงปลอดภัยทางด้านไซเบอร์ของกองบัญชาการกองทัพภาคที่ 2 โดยเฉพาะ ซึ่งสอดคล้องกับความต้องการของผู้ที่เกี่ยวข้องกับระบบสารสนเทศขององค์กร ซึ่งผู้ที่เกี่ยวข้องกับระบบสารสนเทศขององค์กรเห็นด้วยกับกรอบการจัดการช่องโหว่ในงานวิจัยนี้ ทั้งนี้ก็ควรจะดำเนินการตรวจสอบกระบวนการตามกรอบการจัดการช่องโหว่ดังกล่าวให้ครบถ้วน และควรใช้เวลาในการทดสอบหรือทดลองใช้จนเกิดความมั่นใจต่อกรอบการจัดการช่องโหว่ ก่อนที่จะนำไปเป็นกรอบหลักในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ต่อไป

จากการประเมินช่องโหว่ที่ประเมินพบทั้ง 34 ช่องโหว่นั้น เมื่อนำมาประเมินตามมาตราฐานความมั่นคงปลอดภัยของเว็บแอปพลิเคชัน (OWASP 10) พบว่ามีช่องโหว่ตามมาตรฐาน OWASP 10 ในระดับ A02 (Cryptographic Failures) ซึ่งเกี่ยวกับการเข้ารหัสที่อ่อนแอโดยพบจากเครื่องมือ Nessus จำนวน 9 ช่องโหว่ และเครื่องมือ Nexpose จำนวน 10 ช่องโหว่ ซึ่งแสดงให้ว่าเครื่องมือทั้งสองมีประสิทธิภาพทางด้านเทคนิคในการประเมินช่องโหว่ที่เกี่ยวกับเว็บแอปพลิเคชันในระดับที่เท่ากัน

ในการประเมินความเสี่ยงช่องโหว่ที่ส่งผลต่ออุปกรณ์สารสนเทศขององค์กร จากการทดลองตามกรอบในงานวิจัยจะเห็นได้ว่าจำนวนช่องโหว่ได้ลดน้อยลงหลังจากการแก้ไข ส่งผลถึงการประเมินความเสี่ยงช่องโหว่ที่ส่งผลต่ออุปกรณ์สารสนเทศขององค์กร จากเดิมก่อนการแก้ไขช่องโหว่นั้นมีความเสี่ยงอยู่ระดับปานกลางถึงระดับสูง หลังจากทำการแก้ไขช่องโหว่และทำการประเมินช่องโหว่ซ้ำ พบว่าผลการประเมินความเสี่ยงลดลง โดยภาพรวมการประเมินความเสี่ยงช่องโหว่ที่ส่งผลต่ออุปกรณ์สารสนเทศขององค์กรอยู่ในเกณฑ์ระดับต่ำ ซึ่งผลการประเมินความเสี่ยงสอดคล้องกับงานวิจัย กรณีศึกษา: โมเดลทางด้านเทคนิคสำหรับวิธีการประเมินความเสี่ยงความมั่นคงปลอดภัยในระบบสารสนเทศสำหรับโรงพยาบาล (สุรทศ ไตรติลานันท์ และ สุรพล รวยสูงเนิน, 2559) ในเรื่องการใช้ปัจจัยผลกระทบมารวมในการประเมินความเสี่ยงเพื่อให้ได้กระประเมินความเสี่ยงช่องโหว่ที่มีประสิทธิภาพมากยิ่งขึ้น โดยวิเคราะห์จากสภาพแวดล้อมอุปกรณ์ระบบสารสนเทศขององค์กร จนทำให้สามารถทราบและกำจัดช่องโหว่ที่ประเมินได้อย่างถูกต้องและสมบูรณ์ และยังสอดคล้องกับงานวิจัย แนวทางการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ระดับองค์กร (อนาวิล แก้วสอาด และ ณัฐวี อุตกฤษฎ์, 2564) ซึ่งได้อธิบายกรอบแนวคิด NIST 800-30R1 Guide (Risk Assessment Process) ซึ่งเป็นการจัดการความเสี่ยงต่อระบบสารสนเทศขององค์กรโดยมีแนวทางการปฏิบัติที่สามารถนำมาจัดการความเสี่ยงของช่องโหว่ได้อย่างสมบูรณ์ และเมื่อผู้วิจัยนำปรับปรุงร่วมกับวงจรชีวิตการจัดการช่องโหว่โดย CDC สามารถพัฒนาขึ้นมาเป็นกรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กร และสามารถประเมินช่องโหว่ ประเมินความเสี่ยงช่องโหว่ ตลอดจนการกำจัดช่องโหว่ ซึ่งส่งผลกระทบต่อองค์ได้ ซึ่งแสดงให้เห็นในงานวิจัยนี้

ผลการประเมินประสิทธิภาพกรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กรอยู่ในระดับ มาก แสดงให้เห็นว่ากรอบการจัดการช่องโหว่นี้สามารถนำไปใช้เป็นกรอบการจัดการช่องโหว่ระบบสารสนเทศเพื่อการรักษาความมั่นคงปลอดภัยกองบัญชาการกองทัพภาคที่ 2 และควรนำเสนอผู้บังคับบัญชาชั้นสูงของกองทัพภาคที่ 2 เพื่ออนุมัติเป็นหลักการในการใช้กรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กรต่อไป

ข้อเสนอแนะ

งานวิจัยนี้ดำเนินการตามปัจจัยสภาพแวดล้อมระบบสารสนเทศขององค์กรผู้วิจัย มีการดำเนินการทดลองใช้กรอบที่พัฒนาขึ้นมา ตามระยะเวลาที่กำหนดและสอดคล้องตามวัตถุประสงค์ของคณะกรรมการตรวจสอบการปฏิบัติตามกรอบการ

จัดการช่องโหว่ระบบสารสนเทศขององค์กร สำหรับแนวทางการประยุกต์ใช้ในองค์กรอื่นๆ หรือหน่วยงานใกล้เคียงที่มีองค์ประกอบคล้ายกัน ก็ควรจะศึกษาสภาพแวดล้อม องค์ประกอบของระบบสารสนเทศขององค์กร เพื่อนำไปปรับปรุงให้สอดคล้องกับสภาพแวดล้อมขององค์กรนั้นๆ เพราะอาจจะมีข้อจำกัดเรื่องเครื่องมือที่ใช้ในการประเมินช่องโหว่ที่มีประสิทธิภาพทางด้านเทคนิคที่เหมาะสมกับการประเมินช่องโหว่อุปกรณ์สารสนเทศของแต่ละองค์กรซึ่งจะไม่เหมือนกัน

ในงานวิจัยนี้ผู้วิจัยไม่ได้เปรียบเทียบผลการประเมินช่องโหว่ตามกรอบ NIST 800-30R1 และกรอบ CDC เนื่องจากงานวิจัยนี้มุ่งเน้นในการพัฒนากรอบการจัดการช่องโหว่ซึ่งนำกรอบแนวคิดของ NIST 800-30R1 และการดำเนินงานที่เป็นวงรอบลักษณะวงจรชีวิตของ CDC มาใช้เป็นกรอบแนวคิดหลักและปรับใช้กับองค์กรของผู้วิจัยอย่างเหมาะสม ดังนั้นหากผู้วิจัยใช้กรอบแนวคิดของ NIST 800-30R1 เป็นกรอบแนวคิดเดียวสำหรับวิเคราะห์และประเมินความเสี่ยง ผลการวิจัยจะไม่แตกต่างจากเดิม เนื่องจากงานวิจัยนี้เน้นที่การประเมินช่องโหว่ และประเมินความเสี่ยงของช่องโหว่

สำหรับแนวทางพัฒนางานวิจัยในอนาคต ควรวิจัยเพิ่มเติมเกี่ยวกับการค้นหาจุดอ่อนของระบบสารสนเทศโดยประยุกต์แนวทาง Penetration Test และเพิ่มจำนวนเครื่องมือที่ใช้ในการประเมินช่องโหว่ เพื่อเปรียบเทียบความถูกต้องให้มากยิ่งขึ้น ประเด็นความเสี่ยง นอกจากการประเมินความเสี่ยงอุปกรณ์เครื่องแม่ข่ายระบบสารสนเทศแล้ว ควรนำเรื่องความเสี่ยงในด้านอื่นๆ เช่นปัจจัยความเสี่ยงที่เกิดจากมนุษย์ สภาพแวดล้อม นำมาดำเนินการประเมินความเสี่ยง และควรมีการประเมินประสิทธิภาพทางด้านเทคนิคเพิ่มเติม นอกจากใช้แบบสอบถามในการประเมินประสิทธิภาพของกรอบที่พัฒนาขึ้นมาเพื่อประโยชน์สูงสุดต่อองค์กร

เอกสารอ้างอิง

ขนิษฐา สิทธิเทียมจันทร์ สุภาพร นพเวช และสาธิต สุวรรณเวช. (2564). การประเมินช่องโหว่ระบบสารสนเทศ กรณีศึกษามหาวิทยาลัยราชภัฏรำไพพรรณี. รายงานสืบเนื่อง การประประชุมระดับชาติ มหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์, 2564(5), 56-62.

ธเนศ อมรทัศนสุข. (2557). การประเมินช่องโหว่ระบบเทคโนโลยีสารสนเทศ กรณีศึกษา ธนาคารพาณิชย์แห่งหนึ่งในประเทศไทย. [สารนิพนธ์]. มหาวิทยาลัยเทคโนโลยีมหานคร.

พัชรวัฒน์ โกสิตงามดีวงศ์. (2563). การประเมินช่องโหว่ระบบบริหารจัดการทางการแพทย์ กรณีศึกษา โรงพยาบาลภูมิพลอดุลยเดช กรมแพทย์ทหารอากาศ

สุรทศ ไตรติลานันท์ และ สุรพล รวยสูงเนิน. (2559). กรณีศึกษา: โมเดลทางด้านเทคนิคสำหรับวิธีการประเมินความเสี่ยงความมั่นคงปลอดภัยในระบบสารสนเทศสำหรับโรงพยาบาล. วารสารวิชาการพระจอมเกล้าพระนครเหนือ, 26(1), 29-40.

อนาวิล แก้วสอาด และ ณัฐวี อุตกฤษฎ์ (2564). แนวทางการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ระดับองค์กร. วารสารสถาบันวิชาการป้องกันประเทศ, 12(1), 6-20.

NIST. Framework for Improving Critical Infrastructure Cybersecurity. Retrieved September 5, 2021 from https://nvlpubs.nist.gov/cswp/ nist.cswp. 04162018.pdf

National Institute of Standards and Technology Special Publication 8 0 0 -3 0 , Revision 1 , Guide for Conducting Risk Assessments, Retrieved September 5, 2021 from https://nvlpubs.nist.gov/ nistpubs/ legacy/ sp/ nistspecialpublication800-30r1.pdf

OWASP Testing Guide, The Open Web Application Security Project (OWASP), 2008. Retrieved January 9, 2022 from https://owasp.org/www-project-web-security-testing-guide/assets/archive/ OWASP_ Testing_Guide_v3.pdf

Vulnerability Management Life Cycle By CDC. Retrieved September 5, 2021 from https://www.cdc.gov/ cancer/npcr/tools/security/vmlc.htm

A Complete Guide to the Common Vulnerability Scoring System Version 2.0 Retrieved November 6, 2021 from https://www.first.org/ cvss/v2/guide