การพัฒนากรอบการจัดการช่องโหว่ระบบสารสนเทศเพื่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์ กรณีศึกษา กองบัญชาการกองทัพภาคที่ 2

พันตรี ทัญญะ สิทธิมณีวรรณ

การศึกษาค้นคว้าอิสระนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิทยาศาสตรมหาบัณฑิต
แขนงวิชาเทคโนโลยีสารสนเทศและการสื่อสาร สาขาวิชาวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยสุโขทัยธรรมาธิราช
พ.ศ. 2564

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

Maj. Tunya Sittimaneewan

An Independent Study Submitted in Partial Fulfillment of the Requirements for the Degree of Master of Science in Information and Communication Technology

School of Science and Technology
Sukhothai Thammathirat Open University

2021

หัวข้อการศึกษาค้นคว้าอิสระ การพัฒนากรอบการจัดการช่องโหว่ระบบสารสนเทศ
เพื่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์
กรณีศึกษา กองบัญชาการกองทัพภาคที่ 2

ชื่อและนามสกุล พันตรี ทัญญะ สิทธิมณีวรรณ

แขนงวิชา เทคโนโลยีสารสนเทศและการสื่อสาร

สาขาวิชา วิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยสุโขทัยธรรมาธิราช

อาจารย์ที่ปรึกษา ผู้ช่วยศาสตราจารย์ ดร.ขจิตพรรณ กฤตพลวิมาน

การศึกษาค้นคว้าอิสระนี้ ได้รับความเห็นชอบให้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรระดับปริญญาโท เมื่อวันที่ 20 กันยายน 2565

คณะกรรมการสอบการศึกษาค้นคว้าอิสระ

..... ประธานกรรมการ
(ผู้ช่วยศาสตราจารย์ ดร.ขจิตพรรณ กฤตพลวิมาน)

..... กรรมการ
(รองศาสตราจารย์ ดร.วิภา เจริญภัณฑารักษ์)

.....
(อาจารย์ ดร.สิทธิชัย รัชยศโยธิน)
ประธานกรรมการประจำสาขาวิชาวิทยาศาสตร์และเทคโนโลยี

ชื่อการศึกษาค้นคว้าอิสระ การพัฒนากรอบการจัดการช่องโหว่ระบบสารสนเทศเพื่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์ กรณีศึกษา กองบัญชาการกองทัพภาคที่ 2

ผู้ศึกษา พันตรี ทัญญะ สิทธิมณีวรรณ **รหัสนักศึกษา** 2639600317

ปริญญา วิทยาศาสตร์มหาบัณฑิต (เทคโนโลยีสารสนเทศและการสื่อสาร)

อาจารย์ที่ปรึกษา ผู้ช่วยศาสตราจารย์ ดร.ขจิตพรรณ กฤตพลวิมาน **ปีการศึกษา** 2564

บทคัดย่อ

การวิจัยนี้มีวัตถุประสงค์เพื่อ (1) พัฒนากรอบการจัดการช่องโหว่ (2) วิเคราะห์และประเมินช่องโหว่ และ (3) กำหนดวิธีแก้ไขช่องโหว่ระบบสารสนเทศขององค์กร 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 หลังจากดำเนินการทดลองตามกรอบการจัดการช่องโหว่ที่พัฒนาขึ้น พบว่าเหลือเพียง 3 ช่องโหว่ คิดเป็นร้อยละ 9 จากจำนวนช่องโหว่ที่ประเมินพบ และผลการประเมินประสิทธิภาพกรอบการจัดการช่องโหว่ระบบสารสนเทศ อยู่ในระดับมาก โดยมีค่าเฉลี่ย ($\bar{X}$) เท่ากับ 4.48 และส่วนเบี่ยงเบนมาตรฐาน (**S.D.**) เท่ากับ 0.64

คำสำคัญ: กรอบการจัดการช่องโหว่, การรักษาความมั่นคงปลอดภัยทางไซเบอร์, การวิเคราะห์ช่องโหว่

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

Author: Major Tunya Sittimaneewan **ID:** 2639600317

Degree: Master of Science (Information and Communication Technology)

Independent Study advisor: Dr. Khajitpan Kritpolviman**,** Assistant Professor;

Academic year: 2021

Abstract

This research aimed (1) to develop the vulnerability management framework, (2) to analyze and assess vulnerabilities, and (3) to determine vulnerability-remediating solutions for the organization's information systems. The NIST cybersecurity framework and vulnerability management life cycle by CDC were used as the framework prototypes for developing the vulnerability management framework of this organization.

The research methodologies consisted of 1) studying the environment and characteristics of the organization's information systems, 2) developing the information system vulnerability management framework, and 3) implementing the developed framework in the criteria of asset management, assessment, remediation, re-assessment, and verification. By using vulnerability analyzing tools of Nessus Essentials edition and Nexpose Community edition software, 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 determine vulnerability-remediating solutions. The 34 vulnerabilities that affected and took the risk to the organization were reduced to 3 vulnerabilities as a consequence of the implementation of this developed vulnerability management framework in practice. The percentage of vulnerability was reduced from 100 to 9. Additionally, the performance evaluation of this developed framework was at a high level with the average value ($\bar{X}$) was 4.48 and the standard deviation value ($S.D.$) was 0.64.

Keywords: Vulnerability Management Framework, Cybersecurity, Vulnerability Analysis

กิตติกรรมประกาศ

การศึกษาค้นคว้าอิสระเล่มนี้ ผู้วิจัยได้รับความอนุเคราะห์และความกรุณาอย่างดียิ่งจาก อาจารย์ ผศ.ดร.ขจิตพรรณ กฤตพลวิมาน อาจารย์ที่ปรึกษาการศึกษาค้นคว้าอิสระ ที่ได้ให้คำปรึกษา ให้คำแนะนำ และตรวจสอบการทำการศึกษาค้นคว้าอิสระครั้งนี้ ด้วยความเอาใจใส่เป็นอย่างยิ่ง ผู้วิจัยขอกราบขอบพระคุณเป็นอย่างสูง ในความทุ่มเทของอาจารย์ที่ปรึกษา จนนำไปสู่ความสำเร็จของงานวิจัยในครั้งนี้

ขอขอบคุณผู้บังคับบัญชา เพื่อนร่วมงาน ซึ่งเป็นผู้ที่เกี่ยวข้องกับระบบสารสนเทศขององค์กร ที่ให้ความช่วยเหลือ สนับสนุน ที่สละเวลาอันมีค่าในการตอบแบบสอบถามงานวิจัยที่เกี่ยวข้องกับองค์กรเป็นอย่างดี ประโยชน์ของการศึกษาค้นคว้าอิสระเล่มนี้ ผู้วิจัยขอมอบไว้เพื่อประโยชน์ขององค์กร และหน่วยงานอื่นๆ ที่จะนำไปใช้เพื่อประโยชน์ต่อองค์กร

ขอขอบคุณเพื่อนๆ นักศึกษาร่วมรุ่น ที่ให้กำลังใจและให้คำปรึกษาที่ดีเสมอมา

ขอขอบคุณ อาจารย์ นันท์ณรัตน์ สิทธิมณีวรรณ และลูกๆ ผู้อยู่เบื้องหลัง คอยให้กำลังใจให้คำปรึกษา ช่วยเหลือ และเป็นแรงผลักดันให้ผู้วิจัยสามารถทำงานวิจัยนี้ด้วยความ มานะ อดทน

สุดท้ายนี้ผู้วิจัยขอกราบขอบพระคุณ บิดา มารดา ที่ได้อบรมสั่งสอน และเลี้ยงดูตลอดจนเป็นผู้ที่คอยให้โอกาสทางด้านการศึกษาแก่ผู้วิจัยมาตลอดชีวิต ขอขอบพระคุณคณาจารย์ทุกท่านที่ได้ประสิทธิ์ประสาทวิชาความรู้ จนทำให้ผู้วิจัยได้มีประสบการณ์ ความรู้ คิด วิเคราะห์ นำมาใช้ในการวิจัย จนทำการศึกษาค้นคว้าอิสระนี้ได้ประสบความสำเร็จลุล่วงไปได้ด้วยดี

พันตรี ทัญญะ สิทธิมณีวรรณ

กันยายน 2565

สารบัญ

สารบัญ (ต่อ)

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญตาราง

หน้า

สารบัญตาราง (ต่อ)

หน้า

สารบัญตาราง (ต่อ)

หน้า

สารบัญภาพ

หน้า

สารบัญภาพ (ต่อ)

หน้า

สารบัญภาพ (ต่อ)

หน้า

บทที่ 1
บทนำ

1. ความเป็นมาและความสำคัญของปัญหา

ระบบสารสนเทศของกองบัญชาการกองทัพภาคที่ 2 มีที่ตั้งอยู่ที่ ค่ายสุรนารี อ.เมือง จ.นครราชสีมา ในปัจจุบันมีการใช้งานกันอย่างแพร่หลาย อีกทั้งยังครอบคลุมการทำงานของหน่วยงานทหารทุกหน่วยในภาคตะวันออกเฉียงเหนือ ภารกิจงานที่เกี่ยวกับระบบสารสนเทศขององค์กรนั้นมีภารกิจหลายประการ ไม่ว่าจะเป็นการส่งข่าวสารผ่านทางระบบออนไลน์ การประชุมทางไกลผ่านจอภาพ เว็บไซต์ขององค์กร ระบบจำลองยุทธ์ที่ใช้การฝึกผ่านระบบออนไลน์ ระบบประมูลการจัดซื้อจัดจ้าง และระบบอื่นๆ อีกหลายระบบ จากอดีตที่ผ่านมาระบบสารสนเทศขององค์กรนั้นเคยถูกโจมตีจากผู้ไม่หวังดีในหลากหลายรูปแบบเช่น DDOS การเปลี่ยนหน้า Home Page การนำข้อมูลไปเผยแพร่ในสังคมออนไลน์ เป็นต้น กองบัญชาการกองทัพภาคที่ 2 จึงได้จัดหาระบบมาป้องกันการเจาะระบบในรูปแบบฮาร์ดแวร์ ซึ่งก็สามารถใช้งานได้ระดับที่น่าพอใจ แต่อย่างไรก็ดีระบบสารสนเทศขององค์กรนั้นยังไม่เคยผ่านการตรวจสอบ หรือการประเมินความเสี่ยงในด้านต่างๆ อย่างเป็นรูปธรรม นั่นหมายถึงระบบอาจจะยังไม่ปลอดภัยสูงสุด ดังนั้นจึงเป็นที่มาในการทำงานการศึกษาค้นคว้าอิสระในเรื่อง การพัฒนากรอบการจัดการช่องโหว่ระบบสารสนเทศเพื่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์ กองบัญชาการกองทัพภาคที่ 2 ขึ้นมา เพื่อที่ผู้วิจัยซึ่งเป็นกำลังพลของกองทัพภาคที่ 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 มาสังเคราะห์ขั้นตอนในการประเสี่ยงในงานวิจัย พบว่าสามารถดำเนินการประเมินความเสี่ยงช่องโหว่ขององค์กรได้อย่างมีประสิทธิภาพ ผู้วิจัยจึงได้นำกรอบแนวคิดของ NIST มาปรับปรุงขั้นตอนและร่วมกับกรอบวงจรชีวิตในการจัดการช่องโหว่ ของศูนย์ควบคุมโรค สหรัฐอเมริกา (Vulnerability Management Life Cycle By CDC, 2021) ข้อดีของการนำกรอบแนวคิดของ CDC องค์กรสามารถนำมาปฏิบัติใช้ได้เป็นวงรอบซึ่งจะส่งผลดีต่อมาตราการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างมีประสิทธิภาพ ดังนั้นผู้วิจัยจึงนำข้อดีของกรอบแนวคิดทั้งสองมาพัฒนากรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กรเพื่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของกองบัญชาการกองทัพภาคที่ 2 ต่อไป

2. วัตถุประสงค์การศึกษา

1) เพื่อพัฒนากรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กร

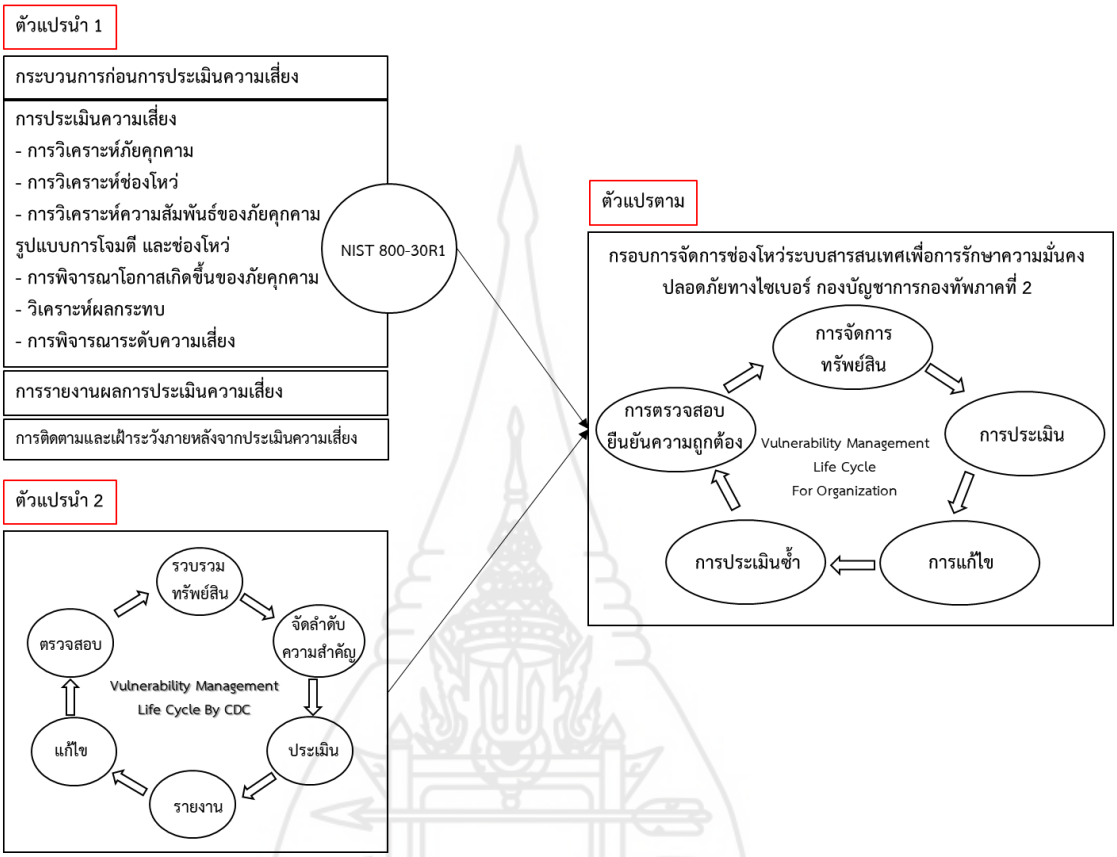
2) เพื่อวิเคราะห์และประเมินช่องโหว่หรือจุดอ่อนของทรัพยากรระบบสารสนเทศขององค์กร

3) เพื่อกำหนดวิธีแก้ไขและหาแนวทางป้องกันการเข้าถึงช่องโหว่หรือจุดอ่อนของระบบสารสนเทศขององค์กร

3. กรอบแนวคิดการวิจัย

กรอบแนวคิดการวิจัยเรื่องการพัฒนากรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กร ได้นำขั้นตอนจากกรอบความมั่นคงปลอดภัยไซเบอร์ 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 จึงทำให้เกิดกรอบการจัดการช่องโหว่

ระบบสารสนเทศเพื่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์ กรณีศึกษา กองบัญชาการกองทัพภาคที่ 2 ตามภาพที่ 1.1



ภาพที่ 1.1 กรอบแนวคิดการวิจัย

4. สมมติฐานในการศึกษา

กรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กรที่พัฒนาขึ้นมา โดยใช้การผสมผสานจากกรอบแนวคิด NIST Cybersecurity Framework และ Vulnerability Management Life Cycle By CDC สามารถแก้ไขปัญหาช่องโหว่หรือจุดอ่อนของระบบสารสนเทศขององค์กรได้ โดยไม่มีความเสี่ยงช่องโหว่ในระดับสูง (ระดับความเสี่ยงจะสามารถคำนวณได้จากการนำค่าของโอกาสเกิดคูณกับผลกระทบ [Likelihood] x [Impact] = [Risk] ที่ให้เห็นว่ามีค่าของโอกาสเกิดและผลกระทบแบ่งเป็น สูง กลาง ต่ำ หากมี (ผลกระทบมาก x โอกาสเกิดบ่อย) จะทำให้ความเสี่ยงอยู่ในระดับสูง รายละเอียดอธิบายไว้ในหัวข้อที่ 2.1.11

5. ขอบเขตของการวิจัย

5.1 ด้านเนื้อหาการวิจัย

เนื้อหาของการวิจัยจะเป็นพัฒนากรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กร โดยใช้หลักการกรอบแนวคิดของ NIST Cybersecurity Framework และ Vulnerability Management Life Cycle By CDC มาเป็นต้นแบบในการพัฒนาโดยเน้นการทดลองในการประเมินช่องโหว่ระบบสารสนเทศ (Vulnerability Assessment)

5.2 ด้านทรัพยากร

ดำเนินการจัดการช่องโหว่ระบบสารสนเทศ โดยมีอุปกรณ์เครื่องแม่ข่ายในภารกิจงานของระบบสารสนเทศเป็นหลักในการประเมินความเสี่ยงช่องโหว่ และอุปกรณ์อื่นๆ โดยดำเนินการจากการจัดลำดับความสำคัญของทรัพยากร โดยวิเคราะห์จากผลกระทบที่มีผลต่อองค์กร รายละเอียดอุปกรณ์ที่เข้ารับการประเมินมีดังนี้

1) เครื่องแม่ข่ายระบบศูนย์ข่าวอัตโนมัติ (AMC SERVER)
2) เครื่องมีข่ายเว็บไซต์องค์กร (WEB SERVER)
3) เครื่องแม่ข่ายประชุมทางไกลผ่านจอภาพ เครื่องหลัก (OpenMCU 1)
4) เครื่องแม่ข่ายประชุมทางไกลผ่านจอภาพ เครื่องสำรอง (OpenMCU 2)
5) เครื่องแม่ข่ายระบบจำลองยุทธ (ARM2WAS)
6) เครื่องแม่ข่ายเครือข่ายเสมือนส่วนตัว (VPN PPTP)
7) อุปกรณ์ไฟร์วอลล์ (FIREWALL FORTIGATE 1000D)
8) อุปกรณ์สวิตช์ (ARUBA 293 0F JL259A L2 SWITCH)

5.3 ด้านเวลา

ระยะเวลาในการทำการวิจัยเริ่มตั้งแต่เดือน มีนาคม 2565 ถึง เดือน กันยายน 2565 ดังแสดงในหัวข้อระยะเวลาและขั้นตอนในการดำเนินงาน

6. ข้อจำกัดในการวิจัย

การแสดงสถานะในรายการทรัพย์สินหรืออุปกรณ์ระบบสารสนเทศขององค์กรเป็นรายการที่อ้างอิงไม่ใช่สถานะรายการจริงเนื่องจากต้องการรักษาชั้นความลับ และความปลอดภัยข้อมูลขององค์กร เช่น หมายเลข IP Address อุปกรณ์สารสนเทศ ชื่อ DNS Server เป็นต้น

7. นิยามศัพท์เฉพาะ

7.1 ความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) “การรักษาความมั่นคงปลอดภัยไซเบอร์” หมายความว่า มาตรการหรือการดำเนินการที่กำหนดขึ้น เพื่อป้องกัน รับมือและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกประเทศ อันกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ (พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พุทธศักราช 2562, 2562)

7.2 การจัดการช่องโหว่ (Vulnerability Management) คือ แนวทางปฏิบัติที่เป็นวัฏจักรในการระบุ จำแนก จัดลำดับความสำคัญ แก้ไข และบรรเทา ช่องโหว่ของซอฟต์แวร์ การจัดการช่องโหว่เป็นส่วนสำคัญในการรักษาความปลอดภัยคอมพิวเตอร์และความปลอดภัยของเครือข่าย

7.3 การประเมินช่องโหว่ (Vulnerability Assessment) หรือเรียกว่า **การค้นหาช่องโหว่ (Vulnerability Scan)** หรือเรียกสั้นๆว่า **(VA)** เป็นการใช้เครื่องมือในการทดสอบหาช่องโหว่ของระบบปฏิบัติการ (OS) ซอฟต์แวร์ หรืออุปกรณ์ Network/Security ว่ามีช่องโหว่ใดบ้าง และมีระดับความรุนแรงเท่าใด เพื่อให้ผู้ดูแลระบบทราบและทำการแก้ไขเพื่อปิดช่องโหว่นั้นโดยอ้างอิงจาก database ของเครื่องมือที่มี โดยเครื่องมือทำ VA สำหรับหาช่องโหว่ของ Server ยกตัวอย่างเช่น Nexpose, Nessus, OpenVAS เป็นต้น

7.4 การประเมินความเสี่ยง (Risk Assessment) เป็นการวัดระดับความรุนแรงของความเสี่ยงเพื่อพิจารณาจัดลำดับความสำคัญของความเสี่ยงที่มีอยู่โดยการประเมินจากโอกาสที่จะเกิด (Likelihood) และผลกระทบ (Impact) เพื่อให้ทราบระดับความเสี่ยงช่องโหว่ที่มีผลต่อระบบสารสนเทศขององค์กร

8. ประโยชน์ที่คาดว่าจะได้รับ

1) ได้กรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กรเพื่อใช้เป็นกรอบหลักการในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร

2) ได้ทราบวิธีแก้ไขและแนวทางป้องกันการเข้าถึงช่องโหว่หรือจุดอ่อนของระบบสารสนเทศ พร้อมทั้งวิเคราะห์ช่องโหว่หรือจุดอ่อนของทรัพยากรระบบสารสนเทศขององค์กรได้

บทที่ 2
วรรณกรรมที่เกี่ยวข้อง

การศึกษาค้นคว้าอิสระฉบับนี้ได้ทบทวนทฤษฎี แนวคิด และงานวิจัยที่เกี่ยวข้องกับการจัดการช่องโหว่ระบบสารสนเทศ รวมถึงวิเคราะห์และการประเมินความเสี่ยงช่องโหว่ระบบสารสนเทศ เพื่อรวบรวมข้อมูลที่เป็นประโยชน์ต่อการกำหนดแนวทางและวิธีการศึกษา เพื่อนำมาดำเนินการพัฒนากรอบการจัดการช่องโหว่ระบบสารสนเทศเพื่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์กองบัญชาการกองทัพภาคที่ 2 โดยได้แบ่งออกเป็นหัวข้อดังนี้

1. แนวคิด/ทฤษฎี ที่เกี่ยวข้อง

1) กรอบงานความปลอดภัยทางไซเบอร์ของ NIST (NIST Cybersecurity Framework)

2) การระบุเพื่อการบริหารจัดการความเสี่ยง Identify.Risk Assessment (ID.RA)

3) การควบคุมความปลอดภัย NIST Special Publication 800-53 Rev.4

4) กระบวนการประเมินความเสี่ยงตามกรอบแนวคิด NIST 800-30R1 Guide for Conducting Risk Assessment

5) วงจรชีวิตการจัดการช่องโหว่โดย CDC (Vulnerability Management Life Cycle by CDC)

6) ปัจจัยผลกระทบทางเทคนิค (Technical Impact Factors)

7) ปัจจัยผลกระทบทางธุรกิจ (Business Impact Factor)

8) การประเมินช่องโหว่ (Vulnerability Assessment) หรือ การค้นหาช่องโหว่ (Vulnerability Scan)

9) การประเมินค่าระดับความเสี่ยง Risk Assessment

10) การประเมินค่าโอกาสที่จะเกิด (Likelihood) และ ผลกระทบ (Impact)

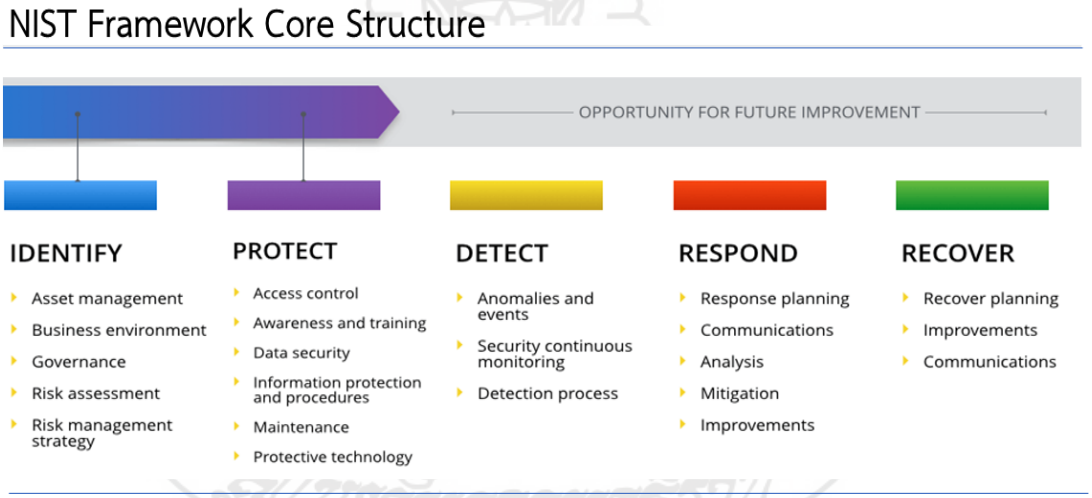
11) การประเมินระดับความสำคัญของความเสี่ยง (Risk Determination)

2. งานวิจัยที่เกี่ยวข้อง

1. แนวคิด/ทฤษฎี ที่เกี่ยวข้อง

1.1 กรอบงานความปลอดภัยทางไซเบอร์ของ NIST (NIST Cybersecurity Framework)

มาตรฐาน NIST Cybersecurity Framework หรือเรียก NIST CSF Version 1.1 ซึ่งเผยแพร่โดยสถาบันมาตรฐานและเทคโนโลยีแห่งชาติ (National Institute of Standards and Technology: NIST) ของสหรัฐอเมริกา Framework อีกทั้งยังแพร่หลายไปยังทุกภูมิภาคทั่วโลก รวมถึงประเทศไทย ในหลายๆ องค์กรได้นำ Framework นี้ไปประยุกต์ใช้รับมือกับภัยคุกคามไซเบอร์ Framework นี้ได้นำเสนอหลักการและแนวทางในการปฏิบัติที่ดีที่สุดในการบริหารจัดการความเสี่ยง เพื่อยกระดับความมั่นคงปลอดภัยขององค์กร รวมไปถึงช่วยให้องค์กรสามารถวางแผนป้องกัน ตรวจจับ และตอบสนองต่อภัยคุกคามได้อย่างรวดเร็วอย่างเป็นระบบ โดยหัวใจสำคัญของ Framework คือ การทำงานฟังก์ชันหลักของโครงสร้างพื้นฐานสารสนเทศที่สำคัญ 5 กระบวนการหลัก ดังภาพที่ 2.1



ภาพที่ 2.1 ภาพรวมกรอบงานความปลอดภัยทางไซเบอร์ของ (NIST Cybersecurity Framework)
ที่มา : https://www.praetorian.com/blog/nist-cybersecurity-framework-vs-nist-special-publication-800-53/

Identify : การระบุและเข้าใจถึงบริบทต่างๆ เพื่อการบริหารจัดการความเสี่ยง

Protect : การวางมาตรฐานควบคุมเพื่อปกป้องระบบขององค์กร

Detect : การกำหนดขั้นตอนและกระบวนการต่างๆ เพื่อตรวจจับสถานการณ์ที่ผิดปกติ

Respond : การกำหนดขั้นตอนและกระบวนการ เพื่อรับมือกับสถานการณ์ผิดปกติที่เกิดขึ้น

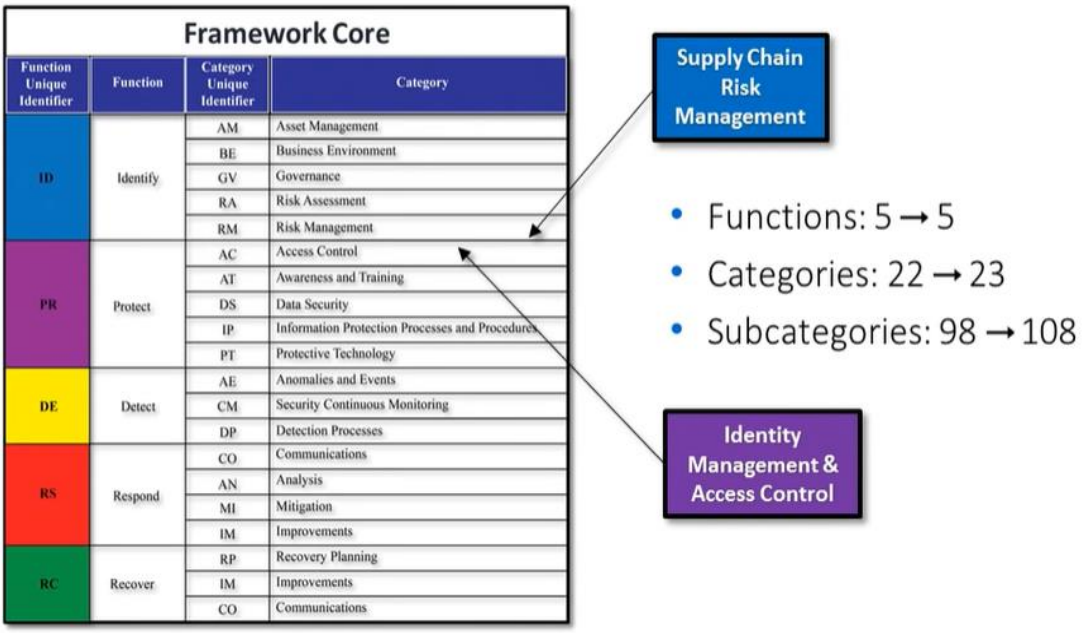
Recovery : การกำหนดขั้นตอนและกระบวนการต่างๆ เพื่อให้ธุรกิจสามารถดำเนินการได้อย่างต่อเนื่อง และฟื้นฟูระบบให้กลับมาเป็นเหมือนเดิม

ซึ่งแต่ละฟังก์ชัน ก็จะแบ่งออกเป็นฟังก์ชันย่อยๆ พร้อมระบุเอกสารอ้างอิงต่างๆ เช่น ISO/IEC 27001:2013, COBIT 5, NIST SP800-53 เพื่อให้นำกระบวนหรือแนวทางปฏิบัติจากเอกสารเหล่านั้นมาใช้เพื่อดำเนินการตามฟังก์ชันย่อยๆ เหล่านี้ได้ทันที โดยที่ผ่านมานั้นได้มีการจัดทำไว้ทั้งหมด 2 เวอร์ชัน คือเวอร์ชัน 1.0 และ เวอร์ชัน 1.1 ซึ่งแตกต่างกันที่ เวอร์ชัน 1.1 มีการเพิ่ม Categories จาก 22 เป็น 23 ข้อและ Subcategories จาก 98 ข้อ เป็น 108 ข้อ นอกเหนือจากนั้นยังมีการทบทวนสาระสำคัญจากปัจจัยการผลิต มีการระบุและพิจารณาประเด็นสำคัญหลายประการในระหว่างการอัปเดตคือ

1) เสริมสร้างการตรวจสอบและการจัดการข้อมูลใน Core Framework

2) เพิ่มคำแนะนำสำหรับความเสี่ยงในการซื้อและห่วงโซ่อุปทานการจัดการ (Supply Chain Risk Management)

3) วิธีการวัดและสร้างตัวชี้วัดเพื่อความชัดเจนในระดับการดำเนินงานและความสัมพันธ์กิจกรรม โดยสามารถแสดง NIST Cybersecurity Framework V1.1 ดังภาพที่ 2.2



ภาพที่ 2.2 การปรับปรุงหมวดหมู่ของ NIST Cybersecurity Framework V1.1

ที่มา : https://nvlpubs.nist.gov/cswp/nist.cswp.04162018.pdf

1.2 การระบุเพื่อการบริหารจัดการความเสี่ยง Identify.Risk Assessment (ID.RA)

งานวิจัยครั้งนี้จะเน้นเฉพาะประเด็นที่เป็นกระบวนการ Identify หรือกระบวนการเตรียมการบริหารความมั่นคงปลอดภัยไซเบอร์เป็นหลัก กระบวนการดังกล่าวจะเป็นการวิเคราะห์ ทำความเข้าใจบริบททรัพยากรขององค์กรที่มีอยู่ เพื่อบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์อย่างเป็นระบบจากกระบวนการหลัก Identify มีกระบวนการย่อยที่ใช้ประเมินความเสี่ยงนั้น คือ Risk Assessment (ID.RA) ซึ่งจะกล่าวถึงการจัดการช่องโหว่ขององค์กรดังภาพที่ 2.3

Function	Category	Subcategory	Informative References
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**ID.RA-1:** Asset vulnerabilities are identified and documented	**CIS CSC** 4 **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04, DSS05.01, DSS05.02 **ISA 62443-2-1:2009** 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 **ISO/IEC 27001:2013** A.12.6.1, A.18.2.3 **NIST SP 800-53 Rev. 4** CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5
		ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources	**CIS CSC** 4 **COBIT 5** BAI08.01 **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 **ISO/IEC 27001:2013** A.6.1.4 **NIST SP 800-53 Rev. 4** SI-5, PM-15, PM-16
		ID.RA-3: Threats, both internal and external, are identified and documented	**CIS CSC** 4 **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04 **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 **ISO/IEC 27001:2013** Clause 6.1.2 **NIST SP 800-53 Rev. 4** RA-3, SI-5, PM-12, PM-16
		ID.RA-4: Potential business impacts and likelihoods are identified	**CIS CSC** 4 **COBIT 5** DSS04.02 **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 **ISO/IEC 27001:2013** A.16.1.6, Clause 6.1.2 **NIST SP 800-53 Rev. 4** RA-2, RA-3, SA-14, PM-9, PM-11
		ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	**CIS CSC** 4 **COBIT 5** APO12.02 **ISO/IEC 27001:2013** A.12.6.1 **NIST SP 800-53 Rev. 4** RA-2, RA-3, PM-16

ภาพที่ 2.3 รายการระบุเพื่อการบริหารจัดการความเสี่ยง Risk Assessment (ID.RA)
ที่มา : https://nvlpubs.nist.gov/cswp/nist.cswp.04162018.pdf

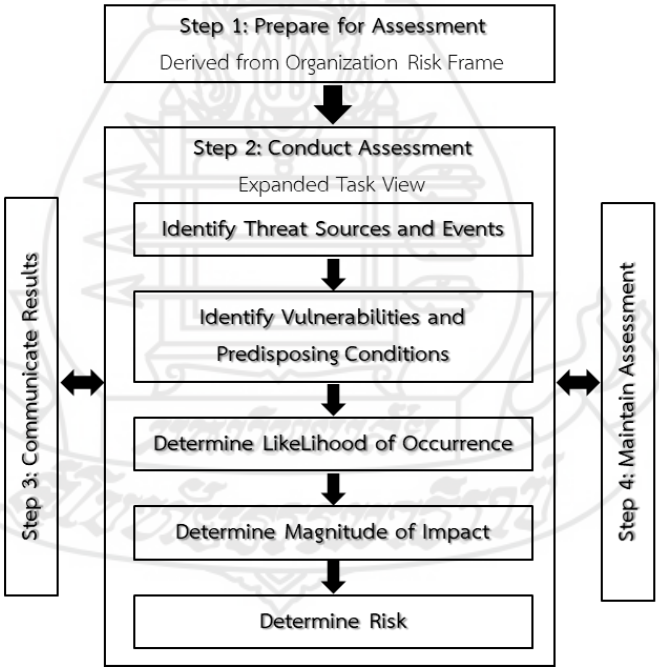
1.3 การควบคุมความปลอดภัย (NIST Special Publication 800-53 Rev.4)

NIST Special Publication 800-53 เป็นส่วนหนึ่งของ Special Publication 800-series โดยอ้างอิงจาก NIST Cybersecurity Framework V1.1 เป็นเอกสารที่รายงานเกี่ยวกับการวิจัยของห้องปฏิบัติการเทคโนโลยีสารสนเทศ (ITL) แนวทางปฏิบัติและความพยายามในการขยายงานด้านความปลอดภัยของระบบข้อมูลและกิจกรรมของ ITL กับภาคอุตสาหกรรมรัฐบาลและนักวิชาการองค์กร ครอบคลุมขั้นตอนใน Risk Management Framework ที่ระบุถึงการเลือกการควบคุมความปลอดภัยสำหรับระบบข้อมูล ตามข้อกำหนดด้านความปลอดภัยใน Federal Information Processing Standard (FIPS) 200 ซึ่งรวมถึงการเลือกชุดเริ่มต้นของการรักษาความปลอดภัยพื้นฐาน การควบคุมโดยอาศัยการวิเคราะห์ผลกระทบ กรณีที่เลวร้ายที่สุดของ FIPS 199

การปรับแต่งการควบคุมความปลอดภัยพื้นฐานและการเสริมการควบคุมความปลอดภัยตามการประเมินความเสี่ยงขององค์กร ความปลอดภัยของข้อมูล และระบบสารสนเทศของรัฐบาลกลาง การจัดประเภทความปลอดภัยของระบบข้อมูล (ต่ำ ปานกลาง หรือสูง) จะกำหนดการรวบรวมพื้นฐานของการควบคุมที่ต้องนำไปใช้และตรวจสอบ หน่วยงานมีความสามารถในการปรับการควบคุมเหล่านี้และปรับแต่งให้เหมาะสมกับเป้าหมายหรือสภาพแวดล้อมขององค์กรมากขึ้น

1.4 กระบวนการประเมินความเสี่ยงตามกรอบแนวคิด NIST 800-30R1 Guide for Conducting Risk Assessment

หลักการสำคัญที่นำมาใช้ในการประเมินความเสี่ยงด้านไซเบอร์ เป็นการนำมาตรฐาน NIST มาประยุกต์ใช้เนื่องจากเป็นมาตรฐานที่ได้รับการยอมรับในระดับสากล ประกอบกับการมีขั้นตอนในการประเมินความเสี่ยงที่ชัดเจนและไม่ซับซ้อน อีกทั้งมีความสอดคล้องกับมาตรฐานสากลด้านการรักษาความมั่นคงปลอดภัยสารสนเทศอื่น ๆ ยกตัวอย่างเช่น ISO 27001:2013 Information Security Management System COBIT5 COSO เป็นต้น (Moeller, 2010) โดยการประเมินความเสี่ยงมีด้วยกันทั้งหมด 4 ขั้นตอน ดังภาพที่ 2.4 ดังนี้



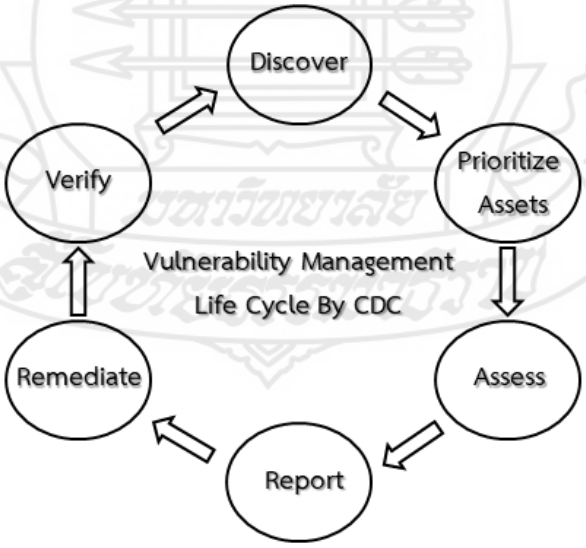
ภาพที่ 2.4 กระบวนการประเมินความเสี่ยงตามกรอบแนวคิด NIST 800-30R1 Guide for Conducting Risk Assessment

ที่มา : Gallagher, P.D. (2012). Guide for Conducting Risk Assessments. NIST Special Publication 800-30 R1. September.

จากภาพ 2.4 เป็นการอธิบายถึงภาพรวมขั้นตอนการประเมินความเสี่ยงตาม NIST 800-30R1 Guide for Conducting Risk Assessment (Gallagher, 2012) ซึ่งเป็นการปรับปรุง จาก NIST 800-30 (Stoneburner, Goguen and Feringa, 2002) โดยอ้างอิงมาจาก NIST Special Publication 800-53 Rev.4 ประกอบไปด้วยขั้นตอนหลัก 4 ขั้นตอน ได้แก่ กระบวนการก่อนการประเมินความเสี่ยง การประเมินความเสี่ยง การรายงานผลการประเมินความเสี่ยง และการติดตามผลการประเมินความเสี่ยงตามวงรอบ (อนาวิล แก้วสอาด และ ณัฐวี อุตกฤษฎ์, 2564) ซึ่งในบทความวิชาการนี้ ผู้เขียนบทความจะอธิบายขั้นตอนแต่ละขั้นตอนจากการศึกษาค้นคว้าวิจัยกรอบแนวคิดนี้เพื่อให้ผู้ที่ศึกษาสามารถนำไปเป็นแนวทางในการประยุกต์ใช้ร่วมกับบริบทขององค์กรตนเองได้

1.5 วงจรชีวิตการจัดการช่องโหว่โดย CDC (Vulnerability Management Life Cycle by CDC)

กรอบแนวคิด Vulnerability Management Life Cycle by CDC (Centers for Disease Control and Prevention) ซึ่งเป็นศูนย์ควบคุมโรคของสหรัฐอเมริกา หน่วยงานทางด้าน IT ของศูนย์นี้ได้แนะนำให้องค์กรงานเครือข่ายของศูนย์ควบคุมโรคนั้นได้ใช้เป็นกรอบรักษาความมั่นคงปลอดภัยทางไซเบอร์ โดยการจัดการช่องโหว่ระบบสารสนเทศขององค์กรในรูปแบบของวัฏจักรการจัดการช่องโหว่ มีจุดมุ่งหมายเพื่อให้องค์กรสามารถระบุจุดอ่อนด้านความปลอดภัยของระบบคอมพิวเตอร์ จัดลำดับความสำคัญของสินทรัพย์ ประเมิน รายงาน และแก้ไขจุดอ่อน และตรวจสอบว่าได้กำจัดไปแล้ว โดยมีฟังก์ชันการทำงานหลักของโครงสร้างพื้นฐานสารสนเทศที่สำคัญ 6 กระบวนการหลัก ดังภาพที่ 2.5



ภาพที่ 2.5 วงจรชีวิตการจัดการช่องโหว่ (Vulnerability Management Life Cycle By CDC)
ที่มา: https://www.cdc.gov/cancer/npcr/tools/security/vmlc.htm

รวบรวมทรัพย์สิน (Discover) : รวบรวมทรัพย์สินทั้งหมดทั่วทั้งเครือข่ายและระบุรายละเอียดของโฮสต์รวมถึงระบบปฏิบัติการและบริการแบบเปิดเพื่อระบุช่องโหว่ พัฒนาพื้นฐานเครือข่าย ระบุช่องโหว่ด้านความปลอดภัยตามกำหนดการอัตโนมัติปกติ

จัดลำดับความสำคัญของสินทรัพย์ (Prioritize Assets) : จัดหมวดหมู่สินทรัพย์ออกเป็นกลุ่มหรือหน่วยธุรกิจ และกำหนดมูลค่าธุรกิจให้กับกลุ่มสินทรัพย์ตามความสำคัญต่อการดำเนินธุรกิจ

ประเมิน (Assess) : กำหนดโปรไฟล์ความเสี่ยงพื้นฐาน เพื่อให้คุณสามารถขจัดความเสี่ยงโดยพิจารณาจากความสำคัญของสินทรัพย์ ภัยคุกคามจากช่องโหว่ และการจัดประเภทสินทรัพย์

รายงาน (Report) :วัดระดับความเสี่ยงทางธุรกิจที่เกี่ยวข้องกับทรัพย์สินตามนโยบายความปลอดภัย จัดทำเอกสารแผนการรักษาความปลอดภัย ตรวจสอบกิจกรรมที่น่าสงสัยและอธิบายช่องโหว่ที่ทราบ

แก้ไข (Remediate) : จัดลำดับความสำคัญและแก้ไขช่องโหว่ตามลำดับตามความเสี่ยงทางธุรกิจ สร้างการควบคุมและแสดงความคืบหน้า

ตรวจสอบ (Verify) : ตรวจสอบว่าช่องโหว่ซึ่งอาจก่อให้ภัยคุกคามถูกกำจัดผ่านการตรวจสอบติดตามผล

1.6 ปัจจัยผลกระทบทางเทคนิค (Technical Impact Factors)

ปัจจัยผลกระทบทางเทคนิค (OWASP Testing Guide, The Open Web Application Security Project (OWASP), 2008) เป็นปัจจัยที่สอดคล้องกับประเด็นด้านความปลอดภัย ได้แก่ การรักษาความลับ ความสมบูรณ์ ความพร้อมใช้งาน และความรับผิดชอบ เป้าหมายคือการประเมินขนาดของผลกระทบต่อระบบหากมีการบุกรุกโดยใช้ประโยชน์จากช่องโหว่ ซึ่งส่งผลกระทบด้านเทคนิคต่อระบบสารสนเทศขององค์กรได้ โดยมีค่าคะแนนของแต่ละหัวข้อปัจจัยที่ส่งผลกระทบ โดยให้ค่าคะแนนจากค่าปัจจัยผลกระทบทางเทคนิคน้อยไปจนถึงมากตั้งแต่ 0 ถึง 9 นำมาหาค่าเฉลี่ยเพื่อให้ได้ค่าผลกระทบทางเทคนิคของระบบสารสนเทศที่มีต่อองค์กร ดังนี้

การสูญเสียความลับ (Loss of Confidentiality) ข้อมูลสามารถเปิดเผยได้มากน้อยเพียงใดและมีความละเอียดอ่อนเพียงใด

เปิดเผยข้อมูลที่ไม่สำคัญน้อยที่สุด (Minimal non-sensitive data disclosed) มีค่าคะแนนเท่ากับ 2

เปิดเผยข้อมูลสำคัญน้อยที่สุด (Minimal critical data disclosed) มีค่าคะแนนเท่ากับ 6

เปิดเผยข้อมูลที่ไม่สำคัญอย่างกว้างขวาง (Extensive non-sensitive data disclosed) มีค่าคะแนนเท่ากับ 6

เปิดเผยข้อมูลสำคัญอย่างยิ่ง (Extensive critical data disclosed) มีค่าคะแนนเท่ากับ 7

ข้อมูลทั้งหมดถูกเปิดเผย (All data disclosed) มีค่าคะแนนเท่ากับ 9

การสูญเสียความสมบูรณ์ (Loss of Integrity) ข้อมูลเสียหายได้มากน้อยเพียงใดและเสียหายเพียงใด

ข้อมูลที่เสียหายเล็กน้อยน้อยที่สุด (Minimal slightly corrupt data) มีค่าคะแนนเท่ากับ 1

ข้อมูลที่เสียหายร้ายแรงน้อยที่สุด (Minimal seriously corrupt data) มีค่าคะแนนเท่ากับ 3

ข้อมูลที่เสียหายเล็กน้อยอย่างกว้างขวาง (Extensive slightly corrupt data) มีค่าคะแนนเท่ากับ 5

ข้อมูลที่เสียหายอย่างร้ายแรงอย่างกว้างขวาง (Extensive seriously corrupt data) มีค่าคะแนนเท่ากับ 7

ข้อมูลทั้งหมดเสียหายทั้งหมด (All data totally corrupt) มีค่าคะแนนเท่ากับ 9

การสูญเสียความพร้อมในการให้บริการ (Loss of Availability) บริการที่สูญเสียไป มีความสำคัญเพียงใด

บริการรองขั้นต่ำถูกขัดจังหวะ (Minimal secondary services interrupted) มีค่าคะแนนเท่ากับ 1

บริการหลักหยุดชะงักน้อยที่สุด (Minimal primary services interrupted) มีค่าคะแนนเท่ากับ 5

บริการรองจำนวนมากถูกขัดจังหวะ (Extensive secondary services interrupted) มีค่าคะแนนเท่ากับ 5

บริการหลักที่กว้างขวางถูกขัดจังหวะ (Extensive primary services interrupted) มีค่าคะแนนเท่ากับ 7

บริการทั้งหมดหายไปอย่างสมบูรณ์ (All services completely lost) มีค่าคะแนนเท่ากับ 9

การสูญเสียความรับผิดชอบ (Loss of Accountability) การกระทำของตัวแทนภัยคุกคามสามารถตรวจสอบย้อนกลับไปยังบุคคลได้หรือไม่

ติดตามได้อย่างสมบูรณ์ (Fully traceable) มีค่าคะแนนเท่ากับ 1

ติดตามได้ (Possibly traceable) มีค่าคะแนนเท่ากับ 7

ติดตามไม่ได้ (Completely anonymous) มีค่าคะแนนเท่ากับ 9

1.7 ปัจจัยผลกระทบทางธุรกิจ (Business Impact Factor)

ผลกระทบทางธุรกิจเกิดจากผลกระทบทางเทคนิค (OWASP Testing Guide, The Open Web Application Security Project (OWASP), 2008) เป็นการนำเอาระบบสารสนเทศ / อุปกรณ์สารสนเทศมาประเมินผลกระทบทางธุรกิจขององค์กรโดยใช้สมมุติฐานกรณีสินทรัพย์ / ระบบสารสนเทศ ล้มเหลว / ไม่สามารถใช้งานได้ ก่อให้เกิดความเสี่ยงที่จะส่งผลกระทบเสียหายต่อธุรกิจขององค์กรได้ โดยมีค่าคะแนนของแต่ละหัวข้อปัจจัยผลกระทบทางธุรกิจ โดยให้ค่าคะแนนจากค่าปัจจัยผลกระทบทางธุรกิจน้อยไปจนถึงมากตั้งแต่ (0 ถึง 9) นำมาหาค่าเฉลี่ยเพื่อให้ได้ค่าผลกระทบเสียหายต่อธุรกิจขององค์กร ดังนี้

ความเสียหายทางการเงิน (Financial damage) ความเสียหายทางการเงินจะเป็นผลมาจากการหาประโยชน์อย่างไร

น้อยกว่าค่าใช้จ่ายในการแก้ไขจุดอ่อน (Less than the cost to fix the vulnerability) มีค่าคะแนนเท่ากับ 1

ผลกระทบเล็กน้อยต่อกำไรประจำปี (Minor effect on annual profit) มีค่าคะแนนเท่ากับ 3

ผลกระทบอย่างมีนัยสำคัญต่อกำไรประจำปี (Significant effect on annual profit) มีค่าคะแนนเท่ากับ (7)

การล้มละลาย (bankruptcy) มีค่าคะแนนเท่ากับ 9

ความเสียหายต่อชื่อเสียง (Reputation damage) การแสวงประโยชน์จะส่งผลให้เกิดความเสียหายต่อชื่อเสียงที่จะเป็นอันตรายต่อธุรกิจหรือไม่

ความเสียหายน้อยที่สุด (Minimal damage) มีค่าคะแนนเท่ากับ 1

การสูญเสียบัญชีหลัก (Loss of major accounts) มีค่าคะแนนเท่ากับ 4

การสูญเสียค่าความนิยม (Loss of goodwill) มีค่าคะแนนเท่ากับ 5

ความเสียหายต่อแบรนด์ (Brand damage) มีค่าคะแนนเท่ากับ 9

การไม่ปฏิบัติตาม (Non-compliance) การไม่ปฏิบัติตามทำให้เกิดการเปิดเผยมากน้อยเพียงใด

การละเมิดเล็กน้อย (Minor violation) มีค่าคะแนนเท่ากับ 2

การละเมิดที่ชัดเจน (Clear violation) มีค่าคะแนนเท่ากับ 5

การละเมิดรายละเอียดสูง (High profile violation) มีค่าคะแนนเท่ากับ 7

การละเมิดความเป็นส่วนตัว (Privacy violation) สามารถเปิดเผยข้อมูลส่วนบุคคลที่สามารถระบุตัวตนได้มากน้อยเพียงใด

หนึ่งคน (One individual) มีค่าคะแนนเท่ากับ 3

หลายร้อยคน (Hundreds of people) มีค่าคะแนนเท่ากับ 5
หลายพันคน (Thousands of people) มีค่าคะแนนเท่ากับ 7
ผู้คนนับล้าน (millions of people) มีค่าคะแนนเท่ากับ 9

1.8 การประเมินช่องโหว่ (Vulnerability Assessment)

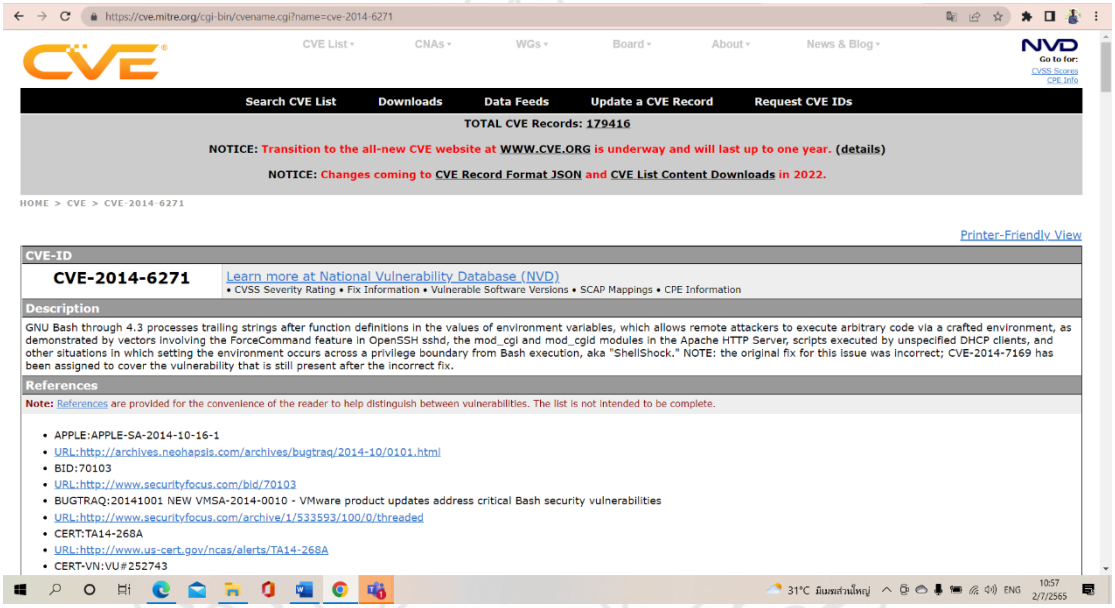
เป็นการตรวจสอบค้นหาช่องโหว่ของระบบ ตั้งแต่ช่องโหว่ในกระบวนการทำงานของระบบ เซิร์ฟเวอร์ และเครือข่าย ไปจนถึงอุปกรณ์รักษาความปลอดภัย ทำให้ทราบถึงช่องโหว่ภายในองค์กร และนำไปสู่การแก้ไขปรับปรุงได้อย่างถูกจุด อันเป็นการลดความเสี่ยงจากภัยคุกคามที่อาจเกิดขึ้น

ช่องโหว่ (Vulnerability) ในบริบทของความมั่นคงของระบบคอมพิวเตอร์ หมายถึงจุดอ่อน หรือความล่อแหลม ความอ่อนแอของระบบคอมพิวเตอร์หรือระบบเครือข่ายที่เปิดโอกาสให้สิ่งที่เป็นภัยคุกคามสามารถเข้าถึงระบบสารสนเทศขององค์กรได้

การค้นหาช่องโหว่ (Vulnerability Scan) หรือเรียกสั้นๆว่า VA นั้น เป็นการใช้เครื่องมือในการค้นหาช่องโหว่ของ Service หรือ Application โดยอ้างอิงจาก database ของเครื่องมือที่มี โดยเครื่องมือทำ VA สำหรับค้นหาช่องโหว่ของ Service ของ Server ยกตัวอย่างเช่น Nexpose, Nessus, OpenVAS เป็นต้น และหากต้องการค้นหาช่องโหว่ของ Web Application จะยกตัวอย่างเช่น Acunetix, Net Sparker, OWASP ZAP เป็นต้น โดยหากเป็นเครื่องมือ VA ที่ค้นหาช่องโหว่ของ Service จะทำการประเมินความเสี่ยงที่ตรวจพบ ตามความเสี่ยงที่ปรากฏต่อสาธารณะแล้ว CVE (Common Vulnerabilities and Exposures) และหากเป็นเครื่องมือ VA สำหรับ Web Application มักจะประเมินความเสี่ยงที่ตรวจพบตามลักษณะของช่องโหว่ เช่น SQL Injection, Cross Site Scripting, XML eXternal Entity เป็นต้น หรือบางเครื่องมือก็จะยึดหลักตาม CWE(Common Weakness Enumeration) ซึ่งอย่างที่กล่าวไป จะเห็นว่า VA นั้นเป็นการใช้เครื่องมือค้นหาช่องโหว่ที่เคยประกาศมาแล้วทั้งสิ้น

ข้อมูลช่องโหว่ (Vulnerability Database) เป็นรายละเอียดช่องโหว่ในรูปแบบต่างๆ ที่ได้รวบรวมไว้โดยองค์กรต่างๆ ที่เกี่ยวข้องกับการดูแลรักษาความปลอดภัย แจ้งเตือน และแก้ไขช่องโหว่ โดยส่วนมากก็จะมีการแบ่งปันข้อมูลร่วมกันเพื่อให้ได้มาถึงข้อมูลที่หลากหลายที่ถูกต้องและรวดเร็ว มีรายละเอียดดังนี้

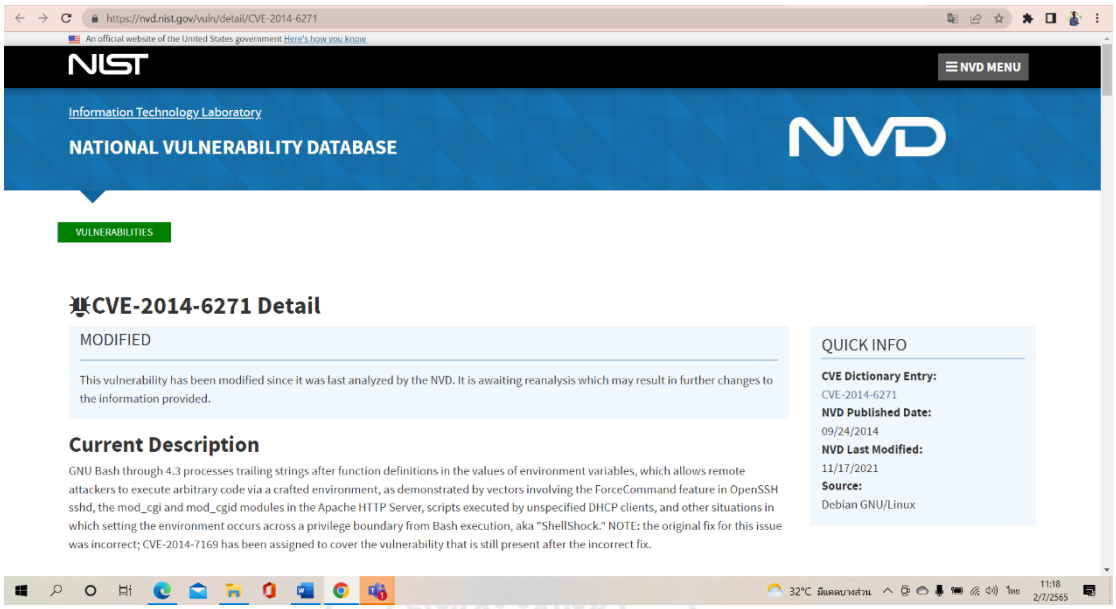
1) Common Vulnerabilities and Exposures (CVE) เป็นโครงการรักษาความปลอดภัย ที่มีเป้าหมายสำคัญในการดูแลซอฟต์แวร์ที่เผยแพร่แบบสาธารณะ โดยโครงการนี้ได้รับเงินทุนสนับสนุนจากกระทรวงความมั่นคงแห่งมาตุภูมิของรัฐบาลกลางแห่งประเทศสหรัฐอเมริกา และกำกับดูแลโดยองค์กรไม่แสวงหาผลกำไร MITRE Corporation CVE เป็นเสมือนอภิธานศัพท์ของช่องโหว่ต่าง ๆ ใช้ระบบ Security Content Automation Protocol (SCAP) ในการรวบรวมข้อมูลช่องโหว่ความปลอดภัย เพื่อเปิดเผยสู่สาธารณะ โดยจะทำเป็นรายการโดยอ้างอิงจากตัวระบุข้อมูลต่าง ๆ แล้วจัดตั้งชื่อไอดีเฉพาะตัวให้แต่ละรายการที่ถูกค้นพบ ทั้งนี้ในข้อมูล CVE จะไม่มีการเผยแพร่ข้อมูลทางเทคนิค หรือวิธีแก้ปัญหาแต่อย่างใด ตัวอย่างเช่น CVE-2014-6271 (CVE-คริสต์ศักราชที่ตรวจพบ-หมายเลขช่องโหว่) ดังภาพที่ 2.6



ภาพที่ 2.6 รายละเอียดหมายเลขช่องโหว่ของ CVE

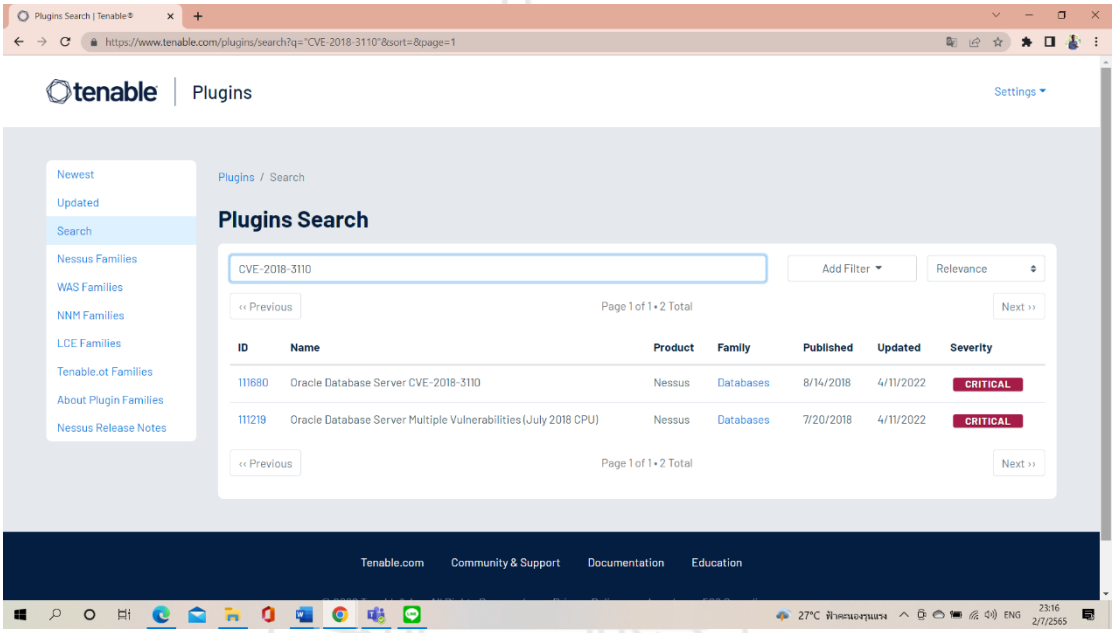
ที่มา: https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2014-6271

2) National Vulnerability Database (NVD) เป็นฐานข้อมูลช่องโหว่แห่งชาติอีกตัวหนึ่งของรัฐบาลกลางแห่งประเทศสหรัฐอเมริกา ที่รวบรวมข้อมูลจากฐานข้อมูลหลายแห่งเอาไว้ด้วยกัน โดยมีฐานข้อมูลจาก Common Vulnerabilities and Exposures (CVE) เป็นองค์ประกอบหลัก และจะเพิ่มในส่วนการนำเสนอข้อมูลการวิเคราะห์ช่องโหว่เพิ่มเข้ามาด้วย ตามภาพที่ 2.7



ภาพที่ 2.7 รายละเอียดข้อมูลการวิเคราะห์ช่องโหว่ NVD
ที่มา: https://nvd.nist.gov/vuln/detail/CVE-2014-6271

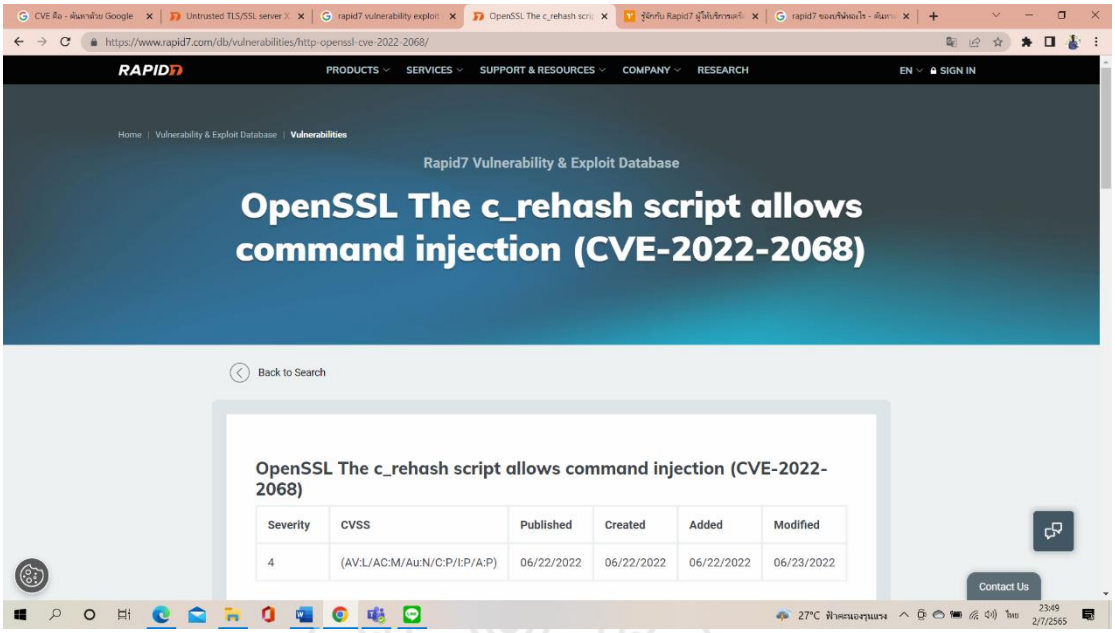
3) Tenable Plugins เป็นฐานข้อมูลช่องโหว่ของบริษัท Tenable ที่สร้างขึ้นมาใช้กับโปรแกรมสแกนช่องโหว่ที่ชื่อ Nessus เป็นข้อมูลเกี่ยวกับช่องโหว่ใหม่ๆ ที่ถูกค้นพบและเผยแพร่สู่สาธารณะ เป็น Plugins เพื่อหาข้อมูลจากช่องโหว่ที่ประเมินพบ เขียนด้วยภาษาสคริปต์ Nessus Attack (NASL) ประกอบด้วยข้อมูลช่องโหว่ ชุดการดำเนินการแก้ไขที่ง่ายขึ้น และอัลกอริทึมเพื่อทดสอบการมีอยู่ของปัญหาด้านความปลอดภัย Tenable Research ได้เผยแพร่ Plugins จำนวน 172,904 ID ครอบคลุม 70,027 CVE ID และ 30,940 Bugtraq ID ตามภาพที่ 2.8



ภาพที่ 2.8 รายละเอียดข้อมูลช่องโหว่ Tenable Plugins

ที่มา: https://www.tenable.com/plugins

4) Vulnerability & Exploit Database Rapid7 รายละเอียดทางเทคนิคสำหรับช่องโหว่มากกว่า 180,000 รายการและการเจาะช่องโหว่ 4,000 รายการมีให้สำหรับผู้เชี่ยวชาญด้านความปลอดภัยและนักวิจัยเพื่อตรวจสอบค้นหาช่องโหว่ ใช้รวมกับเครื่องมือสแกนช่องโหว่ที่ชื่อ Nexpose ของ Rapid7 เอง ดังภาพที่ 2.9



ภาพที่ 2.9 รายละเอียดข้อมูลช่องโหว่ Vulnerability & Exploit Database Rapid7
ที่มา: https:// www.rapid7.com/db/

1.9 การประเมินค่าระดับความเสี่ยง (Risk Assessment)

เป็นการวิเคราะห์และจัดลำดับความเสี่ยง โดยพิจารณาจากการประเมินจากโอกาสที่จะเกิดความเสี่ยง (Likelihood) และความรุนแรงของผลกระทบจากเหตุการณ์ความเสี่ยง (Impact) ต่อการบรรลุวัตถุประสงค์ของกระบวนการทำงานขององค์กร โดยค่าโอกาสที่จะเกิด และความรุนแรงของผลกระทบจากเหตุการณ์ความเสี่ยง สามารถหาจากการคำนวณจาก Common Vulnerability Scoring System (CVSS)

Common Vulnerability Scoring System (CVSS) เป็นการประเมินความรุนแรงของช่องโหว่ โดยจะมีคะแนนแสดงถึงความรุนแรง ในแต่ละระดับที่แตกต่างกันไปตามชนิดของช่องโหว่นั้นๆ ระดับคะแนนนี้จะช่วยให้บุคลากรที่เกี่ยวข้องกับระบบสารสนเทศขององค์กร ตัดสินใจได้ง่ายขึ้นว่า จะรับมือกับช่องโหว่นี้อย่างไร และตอนไหน เช่น ถ้าเป็นช่องโหว่ที่มีความรุนแรงมาก ก็จะพิจารณายกเลิกงานทั้งหมดที่ปฏิบัติอยู่ เพื่อแก้ไขปัญหาอย่างเร่งด่วนที่สุดก่อน หลักเกณฑ์การให้

คะแนน Common Vulnerability Scoring System (CVSS) จะพิจารณาจากตัวชี้วัดหลายอย่าง ประกอบไปด้วย ความยากง่ายในการโจมตี ความซับซ้อน ระดับความลับของช่องโหว่ เงื่อนไขในการโจมตี ฯลฯระบบคะแนน CVSS จะมีอยู่ 2 รูปแบบ คือ CVSS v2.0 สำหรับความรุนแรงระดับ "ต่ำ" และ CVSS v3.0 สำหรับความรุนแรงระดับ "สูง" ดังตารางที่ 2.1

ตารางที่ 2.1 ค่าคะแนนระดับความรุนแรง CVSS

CVSS v2.0 Ratings		**CVSS v3.0 Ratings**	
ความรุนแรง	**ช่วงคะแนนฐาน**	**ความรุนแรง**	**ช่วงคะแนนฐาน**
		ไม่มี (None)	0.0
ต่ำ (Low)	0.0-3.9	ต่ำ (Low)	0.1-3.9
กลาง (Medium)	4.0-6.9	กลาง (Medium)	4.0-6.9
สูง (High)	7.0-10.0	สูง (High)	7.0-8.9
		รุนแรง (Critical)	9.0-10.0

ที่มา : https://nvd.nist.gov/vuln-metrics/cvss

1.10 การประเมินค่าโอกาสที่จะเกิด (Likelihood) และ ผลกระทบ (Impact)

ความเสี่ยงประกอบไปด้วยปัจจัยหลัก คือ โอกาสที่จะเกิดความเสี่ยง (Likelihood) กับผลกระทบของความเสี่ยง (Impact) (OWASP Testing Guide, The Open Web Application Security Project (OWASP), 2008) ซึ่งโอกาสที่จะเกิดความเสี่ยงหมายถึงความเป็นไปได้ที่จะเกิดเหตุการณ์หรือความเสี่ยง ส่วนผลกระทบของความเสี่ยง หมายถึง ผลลัพธ์ของเหตุการณ์หรือความเสี่ยงนั้น โดยงานวิจัยนี้ได้แบ่งระดับความเสี่ยงตามตารางที่ 2.2 ดังนี้

ตารางที่ 2.2 ช่วงคะแนนโอกาส และผลกระทบ

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

- ระดับต่ำ (LOW) รายละเอียดทั่วไปของระบบสารสนเทศ เป็นจุดอ่อนหรือช่องโหว่ที่มีความเสี่ยงต่อการถูกบุกรุกระดับต่ำซึ่งไม่มีผลกระทบต่อความเสียหายของระบบสารสนเทศ

- ระดับกลาง (MEDIUM) หมายถึงจุดอ่อนหรือช่องโหว่ที่มีความเสี่ยงต่อการถูกบุกรุกระดับกลางและผลกระทบของการบุกรุกจะทำให้ระบบสารสนเทศมีความเสียหายในระดับกลาง

- ระดับสูง (HIGH) หมายถึงจุดอ่อนหรือช่องโหว่ที่มีความเสี่ยงต่อการถูกบุกรุกระดับสูงผู้บุกรุกสามารถใช้ช่องโหว่ที่ประเมินพบนี้โจมตีระบบได้ทันทีและสร้างความเสียหายต่อระบบสารสนเทศในระดับสูง

1.11 การประเมินระดับความสำคัญของความเสี่ยง (Risk Determination)

ระดับความเสี่ยงจะสามารถคำนวณได้จากการนำค่าของโอกาสเกิดคูณกับผลกระทบ [Likelihood] x [Impact] = [Risk] ที่ให้เห็นว่ามีค่าของโอกาสเกิดและผลกระทบแบ่งเป็น สูง กลาง ต่ำ หากมีผลกระทบมาก โอกาสเกิดบ่อย จะทำให้ความเสี่ยงนั้นสูงตาม (OWASP Testing Guide, The Open Web Application Security Project (OWASP), 2008) สามารถอธิบายออกมาตามตารางที่ 2.3 ดังนี้

ตารางที่ 2.3 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)	ระดับความเสี่ยงต่ำมากแต่ให้บันทึกไว้ (Note)	ระดับความเสี่ยงต่ำ (Low)	ระดับความเสี่ยงปานกลาง (Medium)
		ระดับต่ำ (Low) (1)	ระดับกลาง (Medium) (2)	ระดับสูง (High) (3)
		โอกาสเกิด (Likelihood)		

- ระดับความเสี่ยงต่ำมากแต่ให้บันทึกไว้ (Note) หมายถึง Note หมายความว่าไม่มีความเสี่ยง หรือ เว็บไซต์/เว็บแอปพลิเคชัน/เครื่องคอมพิวเตอร์แม่ข่ายมีการควบคุมที่เพียงพอ/สถานะยังมีความปลอดภัย แต่ยังคงต้องบันทึกรายละเอียดข้อมูลต่างๆ ของช่องโหว่ที่ได้รับการ (Note) มีผลมาจากเมตริกความเสี่ยง (1 x 1 = Note)

- ระดับความเสี่ยงต่ำ (Low) หมายถึง มีความเสี่ยงต่อการถูกบุกรุกระดับต่ำซึ่งไม่มีผลกระทบต่อความเสียหายของระบบสารสนเทศ (Low) มีผลมาจากเมตริกความเสี่ยง (2 x 1 = Low) หรือ (1 x 2 = Low)

- ระดับความเสี่ยงปานกลาง (Medium) หมายถึง มีความเสี่ยงต่อการถูกบุกรุกระดับกลางและผลกระทบของการบุกรุกจะทำให้ระบบสารสนเทศมีความเสียหายในระดับกลาง

(Medium) มีผลมาจากเมตริกความเสี่ยง (3 x 1 = Medium) , (2 x 2 = Medium) หรือ (1 x 3 = Medium)

- ระดับความเสี่ยงสูง (High) หมายถึงมีความเสี่ยงต่อการถูกบุกรุกระดับสูง ผู้บุกรุกสามารถใช้ช่องโหว่ที่ประเมินพบนี้โจมตีระบบได้ทันทีและสร้างความเสียหายต่อระบบสารสนเทศในระดับสูง (High) มีผลมาจากเมตริกความเสี่ยง (3 x 2 = High) หรือ (3 x 2 = High)

- ระดับความเสี่ยงวิกฤต (Critical) หมายถึง มีความเสี่ยงต่อการถูกบุกรุกระดับสูงมาก ผู้บุกรุกสามารถใช้ช่องโหว่ที่ประเมินพบนี้โจมตีระบบได้ทันทีและสร้างความเสียหายต่อระบบสารสนเทศในระดับวิกฤต มีผลกระทบต่อองค์อย่างกว้างขวางและร้ายแรงสูงสุด (Critical) มีผลมาจากเมตริกความเสี่ยง (3 x 3 = Critical)

2. งานวิจัยที่เกี่ยวข้อง

จากการค้นหางานวิจัย บทความวิชาการ วารสารวิชาการ ที่เกี่ยวข้องส่วนใหญ่แล้วพบว่าเป็นการประเมินช่องโหว่ระบบสารสนเทศ (Vulnerability Assessment) กล่าวถึงเรื่อง การประเมินช่องโหว่ การใช้เครื่องมือในการค้นหาช่องโหว่ที่แตกต่างกันไปในแต่ละงานวิจัย อีกทั้งได้อ้างอิงกรอบต่างๆ ในเรื่องการรักษาความปลอดภัยระบบสารสนเทศ เช่น มาตรฐาน ISO/IEC 27001_หลักการ CIA, NIST Cybersecurity Framework และมาตรฐานอื่นๆ อย่างไรก็ดียังไม่พบว่าได้มีการนำกรอบที่กล่าวมา นำมาเพื่อใช้เป็นการพัฒนาเป็นกรอบสำหรับการจัดการช่องโหว่สารสนเทศขององค์กร ให้เกิดความต่อเนื่องและเป็นหลักการให้กับองค์กรแต่อย่างใด เป็นเพียงการใช้เครื่องมือในการค้นหาช่องโหว่ การแก้ไขช่องโหว่ การประเมินความเสี่ยงช่องโหว่ที่ส่งผลกระทบต่อองค์กร ไม่ได้ทำเป็นโมเดลหรือกรอบการจัดการช่องโหว่อย่างเป็นระบบที่ถาวร กล่าวคือเป็นการประเมินช่องโหว่ (Vulnerability Assessment) ไม่ใช่การจัดการช่องโหว่ (Vulnerability Management) นั่นเอง ตัวอย่างงานวิจัยเช่น

1) ธเนศ อมรทัศนสุข (2557) ได้นำเสนอการประเมินช่องโหว่ระบบเทคโนโลยีสารสนเทศ กรณีศึกษา ธนาคารพาณิชย์แห่งหนึ่งในประเทศไทย พบว่า การประเมินช่องโหว่ระบบเทคโนโลยีสารสนเทศ เป็นการวิเคราะห์การทำงานของเครื่องมือตรวจสอบหรือค้นหาช่องโหว่ (Vulnerability Scan Tools) ในเชิงประสิทธิภาพ โดยมุ่งเน้นไปที่การเปรียบเทียบช่องโหว่ และจุดอ่อนระบบสารสนเทศโดยใช้เทคนิคการประเมินช่องโหว่ (Vulnerability Assessment) โดยศึกษากรณีตัวอย่างระบบงานหลักของธนาคารพาณิชย์แห่งหนึ่ง เปรียบเทียบข้อดี-ข้อเสียของเครื่องมือที่มีวางจำหน่ายในท้องตลาด และนำช่องโหว่ที่ตรวจพบจากเครื่องมือไปดำเนินการแก้ไข เพื่อลดความเสี่ยงของระบบสารสนเทศขององค์กร

2) สุรทศ ไตรติลานันท์ และ สุรพล รวยสูงเนิน (2559) ได้นำเสนอ กรณีศึกษา: โมเดลทางด้านเทคนิคสำหรับวิธีการประเมินความเสี่ยง ความมั่นคงปลอดภัยในระบบสารสนเทศสำหรับโรงพยาบาล พบว่า การประเมินและจัดลำดับระดับความเสี่ยงความมั่นคงปลอดภัยสารสนเทศสำหรับโรงพยาบาลในประเทศไทยยังไม่มีขั้นตอนหรือเทคนิคที่เป็นมาตรฐาน ผู้วิจัยทำการศึกษาและประยุกต์แนวปฏิบัติรวมถึงมาตรฐานสากลที่เกี่ยวข้องกับการประเมินความเสี่ยงสารสนเทศ และการทดสอบประเมินความมั่นคงปลอดภัยสารสนเทศโดยการประเมินช่องโหว่ (Vulnerability Assessment) ด้วยวิธีการใช้เครื่องมือทางเทคนิคเพื่อช่วยในการตรวจสอบค้นหาช่องโหว่ และนำไปสู่ขั้นตอนการกำหนดโมเดลการประเมินระดับความมั่นคงปลอดภัยสารสนเทศที่สอดคล้องต่อบริบทสารสนเทศสำหรับโรงพยาบาล โดยจากการทดสอบประเมินด้วยโมเดลและวิธีการทางเทคนิคที่ถูกพัฒนาขึ้นพบว่าผลการประเมินมีระดับความเสี่ยงความมั่นคงปลอดภัยสารสนเทศแปรผันตรงตามปัจจัยผลกระทบธุรกิจที่หน่วยงานกำหนดเพื่อให้สอดคล้องและสะท้อนต่อสภาพแวดล้อมจริงของสารสนเทศสำหรับโรงพยาบาล

3) เรืออากาศตรีหญิง ณัชณภัทร ใจอดทน (2560) ได้นำเสนอการประเมินค่าช่องโหว่ของเว็บไซต์และการป้องกัน กรณีศึกษา: เว็บไซต์กรมควบคุมการปฏิบัติทางอากาศ พบว่า งานวิจัยได้ทำการศึกษาค้นคว้าเพื่อค้นหาช่องโหว่หรือจุดอ่อนของเว็บไซต์ กรมควบคุมการปฏิบัติทางอากาศ (www.daoc.rtaf.mi.th) ว่าเว็บไซต์ดังกล่าวมีช่องโหว่หรือจุดอ่อนหรือไม่ ช่องโหว่หรือจุดอ่อนนั้นมีระดับความรุนแรงและมีผลกระทบต่อเว็บไซต์อย่างไร โดยใช้โปรแกรม Acunetix Web Vulnerability Scanner เป็นเครื่องมือในการค้นหาช่องโหว่ของเว็บไซต์และการค้นหาช่องโหว่โดยใช้วิธีการทดสอบเจาะระบบโดยใช้เทคนิค Local File Disclosure ในการค้นหาช่องโหว่ซึ่งผู้วิจัยได้แบ่งขั้นตอนในการค้นหาช่องโหว่ของเว็บไซต์เป็น 3 ขั้นตอน ประกอบด้วย (1) การวางแผนและเตรียมการ (Planning and Preparation) (2) การประเมินค่าของช่องโหว (Vulnerability Assessment) (3) การทำรายงานวิธีการแก้ไขและการป้องกันช่องโหว่

4) จิราพัชร์ พันธุ์ถาวรชัย (2561) ได้นำเสนอแนวทางการสร้างกรอบการพัฒนาการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์ พบว่า การออกแบบกรอบการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์ โดยอ้างอิง NIST Cybersecurity Framework เพื่อให้เห็นถึงวิธีการที่จะยืนยันว่าผลการประเมินตนเอง ที่ได้จากกรอบการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์ ความสอดคล้องกับการรับรู้ของผู้ให้บริการคลาวด์ งานวิจัยนี้จึงออกแบบให้มีวัตถุประสงค์หลัก 3 ข้อ 1) การดำเนินการศึกษาเพื่อพัฒนากรอบที่ใช้การประเมินความเสี่ยงและภัยคุกคามด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์ 2) ทำการพัฒนากรอบการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์ 3) การดำเนินการพัฒนาแอปพลิเคชันประเมินตนเองสำหรับประเมินผลการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์

5) พัชรวัฒน์ โกสิตงามดีวงศ์ (2563) ได้นำเสนอการประเมินช่องโหว่ระบบบริหารจัดการทางการแพทย์ กรณีศึกษา: โรงพยาบาลภูมิพลอดุลยเดช กรมแพทย์ทหารอากาศ พบว่า งานวิจัยนี้ได้ทำการศึกษาค้นคว้าเพื่อค้นหาช่องโหว่ของระบบ Bhumibol Health information system (BHIS) ว่าระบบดังกล่าวมีช่องโหว่หรือไม่ มีระดับความรุนแรงและมีผลกระทบต่อระบบอย่างไร โดยใช้โปรแกรมประยุกต์เป็นเครื่องมือในการค้นหาช่องโหว่ และใช้วิธีการทดสอบเจาะระบบโดยใช้เทคนิค Information Disclosure ซึ่งได้แบ่งขั้นตอนในการค้นหาช่องโหว่ของระบบเป็น 4 ขั้นตอน ประกอบด้วย (1) Planning คือ การวางแผนก่อนการดำเนินงาน (2) Discovery คือ กระบวนการค้นหาช่องโหว่ระบบ (3) Attack คือ กระบวนการโจมตีเป้าหมายเมื่อมีการค้นพบช่องโหว่ (4) Report คือ ขั้นตอนการรายงานการประเมินผล

6) อนาวิล แก้วสะอาด และ ณัฐวี อุตกฤษฎ์ (2564) ได้นำเสนอแนวทางการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ระดับองค์กร พบว่า เป็นการอธิบายถึงภาพรวมขั้นตอนการประเมินความเสี่ยงตาม NIST 800-30R1 Guide โดยประกอบไปด้วยขั้นตอนหลัก 4 ขั้นตอน ได้แก่กระบวนการก่อนการประเมินความเสี่ยง การประเมินความเสี่ยง การรายงานผลการประเมินความเสี่ยง และการติดตามผลการประเมินความเสี่ยงตามวงรอบ ซึ่งในบทความวิชาการนี้ผู้เขียนบทความจะอธิบายขั้นตอนแต่ละขั้นตอนจากการศึกษาค้นคว้าวิจัยกรอบแนวคิดนี้ เพื่อให้ผู้ที่ศึกษาสามารถนำไปเป็นแนวทางในการประยุกต์ใช้ร่วมกับบริบทขององค์กรตนเองได้

7) ขนิษฐา สิทธิเทียมจันทร์ สุภาพร นพเวช และสาธิต สุวรรณเวช (2564) ได้นำเสนอการประเมินช่องโหว่ระบบสารสนเทศ กรณีศึกษามหาวิทยาลัยราชภัฏรำไพพรรณี พบว่า การประเมินช่องโหว่ระบบสารสนเทศภายในมหาวิทยาลัย โดยมีขั้นตอนการตรวจสอบระบบด้วยการป้อนระบบเป้าหมายทีละระบบ จากนั้นค้นหาพอร์ตที่เสี่ยงต่อการถูกโจมตีเมื่อพบทำการตรวจสอบความปลอดภัย ทั้งนี้ระบบการพิสูจน์ทราบตัวตนเป็นระบบแรกที่บุคลากรจะต้องยืนยันตัวตนก่อนใช้บริการอินเทอร์เน็ตซึ่งพบว่ายังไม่มีความปลอดภัยเพียงพอ การใช้รหัสผ่านที่ไม่ได้มีการเข้ารหัสความลับที่ใช้จำนวนบิตที่มาก หากผู้ประสงค์ร้ายเข้ามาใช้งานภายในมหาวิทยาลัยและใช้เครื่องมือในการตรวจจับค้นหารหัสผ่านจะสามารถตรวจจับและเข้าสู่ระบบได้อย่างง่ายดาย จากนั้นตรวจสอบระบบสารสนเทศอื่น ๆ ภายในมหาวิทยาลัยพบว่าซอฟต์แวร์ที่ใช้ของระบบสารสนเทศมีช่องโหว่เป็นส่วนใหญ่ขาดการอัปเดตเวอร์ชันให้ทันสมัย

จากการทบทวนวรรณกรรมทั้ง 7 งานวิจัยนั้นผู้วิจัยได้นำมาสรุปเปรียบเทียบในรูปแบบตารางทบทวนวรรณกรรมตามตารางที่ 2.4 ดังนี้

ตารางที่ 2.4 ตารางทบทวนวรรณกรรม

ชื่อผู้วิจัย	เรื่องงานวิจัย	ปี	แนวคิด/ทฤษฎี/วิธีการ				เครื่องมือการวิจัย										
							ตรวจสอบช่องโหว่				ประเมินความเสี่ยง				ประเมินประสิทธิภาพ		
			NIST	ISO:27001	OWAPS	อื่นๆ	NESSUS	NEXPOSE	NMAP	อื่นๆ	CVSS SCORE	Impact+Likelihood	Owaps Risk	อื่นๆ	แบบสอบถาม	สัมภาษณ์	อื่นๆ
ธเนศ อมรทัศนสุข	การตรวจประเมินช่องโหว่ระบบเทคโนโลยีสารสนเทศ กรณีศึกษาธนาคารพาณิชย์แห่งหนึ่งในประเทศไทย	2557	✓				✓	✓		✓	✓	✓					
สุรทศ ไตรติลานันท์ และ สุรพล รวยสูงเนิน	กรณีศึกษา: โมเดลทางด้านเทคนิคสำหรับวิธีการประเมินความเสี่ยงความมั่นคงปลอดภัยในระบบสารสนเทศสำหรับโรงพยาบาล.	2559	✓		✓	✓					✓	✓	✓				

ตารางที่ 2.4 (ต่อ)

ชื่อผู้วิจัย	เรื่องงานวิจัย	ปี	แนวคิด/ทฤษฎี/วิธีการ				เครื่องมือการวิจัย										
							ตรวจสอบช่องโหว่				ประเมินความเสี่ยง				ประเมินประสิทธิภาพ		
			NIST	ISO:27001	OWAPS	อื่นๆ	NESSUS	NEXPOSE	NMAP	อื่นๆ	CVSS SCORE	Impact+Likelihood	Owaps Risk	อื่นๆ	แบบสอบถาม	สัมภาษณ์	อื่นๆ
เรืออากาศตรีหญิง ณัชณภัทร ใจอดทน	การประเมินค่าช่องโหว่ของเว็บไซต์และการป้องกัน กรณีศึกษาเว็บไซต์กรมควบคุม การปฏิบัติทางอากาศ	2560			✓					✓		✓					
จิราพัชร์ พันธุ์ถาวรชัย	แนวทางการสร้างกรอบการพัฒนาการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์	2561	✓	✓											✓	✓	

ตารางที่ 2.4 (ต่อ)

ชื่อผู้วิจัย	เรื่องงานวิจัย	ปี	แนวคิด/ทฤษฎี/วิธีการ				เครื่องมือการวิจัย										
							ตรวจสอบช่องโหว่				ประเมินความเสี่ยง				ประเมินประสิทธิภาพ		
			NIST	ISO:27001	OWAPS	อื่นๆ	NESSUS	NEXPOSE	NMAP	อื่นๆ	CVSS SCORE	Impact+Likelihood	Owaps Risk	อื่นๆ	แบบสอบถาม	ผู้เชี่ยวชาญ	อื่นๆ
พัชรวัฒน์ โกสิตงามดีวงศ์	การประเมินช่องโหว่ระบบบริหารจัดการทางการแพทย์ กรณีศึกษาโรงพยาบาลภูมิพลอดุลยเดช กรมแพทย์ทหารอากาศ	2563	✓				✓		✓			✓					
อนาวิล แก้วสอาด และ ณัฐวี อุตกฤษฎ์	แนวทาง การบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ระดับองค์กร	2564	✓				✓					✓					
ขนิษฐา สิทธิเทียม จันทร์ สุภาพร นพเวช และสาธิต สุวรรณเวช	การตรวจประเมินช่องโหว่ระบบสารสนเทศ กรณีศึกษามหาวิทยาลัยราชภัฏรำไพพรรณี	2564		✓						✓		✓					

ซึ่งจากการศึกษางานวิจัย บทความทางวิชาการเหล่านี้พบว่ามี มีแนวคิด ทฤษฎี วิธีการและเครื่องมือการวิจัย ที่สามารถนำมาประยุกต์ใช้ในงานวิจัยได้ สำหรับงานวิจัยในครั้งนี้ผู้วิจัยได้ใช้แนวทางจาก อนาวิล แก้วสะอาด และ ณัฐวี อุตกฤษฎ์ (2564) บทความวิชาการ เรื่อง แนวทางการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ระดับองค์กร มาเป็นต้นแบบงานวิจัย ซึ่งใช้กรอบแนวความคิดของ NIST โดยอิงกระบวนการประเมินความเสี่ยงตามกรอบแนวคิด NIST 800-30R1 Guide for Conducting Risk Assessment ซึ่งเป็นเอกสารแนะนำในการปฏิบัติด้านประเมินความเสี่ยงขององค์กรของ NIST นอกจากนั้นผู้วิจัยยังได้ศึกษาแนวความคิดจาก CDC ในเรื่องของ วงจรชีวิตการจัดการช่องโหว่โดย CDC (Vulnerability Management Life Cycle by CDC) ข้อดีของ วงจรชีวิตของการจัดการช่องโหว่นี้ คือช่วยทำให้สามารถกำหนดกรอบการพัฒนากรอบการจัดการช่องโหว่ได้อย่างเป็นรูปธรรมมากยิ่งขึ้น โดยการพัฒนากรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กรในครั้งนี้ ได้ผสมผสานแนวคิดของ CDC และ NIST 800-30R1 Guide เพื่อให้ได้กรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กร และสามารถนำไปปฏิบัติได้จริงในรูปแบบที่เป็นระบบและหลักการที่ถูกต้อง และในเนื้อหางานวิจัยนี้ก็ได้นำขั้นตอนการประเมินช่องโหว่ ที่มีการใช้เครื่องมือ Nessus และ Nexpose ในการสแกนช่องโหว่ และการคำนวณ CVSS Score ในการหาโอกาสที่จะเกิด และผลกระทบ ซึ่งนำไปสู่ผลระดับความเสี่ยงของอุปกรณ์ระบบสารสนเทศ ที่มีผลกระทบขององค์กร ซึ่งได้แนวทางมาจาก สุรทศ ไตรติลานันท์ และ สุรพล รวยสูงเนิน (2559) งานวิจัยเรื่อง กรณีศึกษา: โมเดลทางด้านเทคนิคสำหรับวิธีการประเมินความเสี่ยง ความมั่นคงปลอดภัยในระบบสารสนเทศสำหรับโรงพยาบาล นอกจากนั้นงานวิจัยนี้ยังได้ทำการประเมินประสิทธิภาพของกรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กร โดยใช้แนวทางของ จิราพัชร์ พันธุ์ถาวรชัย (2561) งานวิจัยเรื่อง การสร้างกรอบการพัฒนาการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์ ซึ่งมีลักษณะการพัฒนาโมเดลคล้ายๆ งานของผู้วิจัย โดยจะมีการประเมินประสิทธิภาพกรอบงานที่พัฒนาขึ้นมาเพื่อให้ได้ความถูกต้อง และความน่าเชื่อถือของกรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กร ส่วนงานวิจัยอื่นๆ จากงานวิจัยที่เกี่ยวข้อง ผู้วิจัยนำมาประกอบการค้นคว้าเพิ่มเติม เช่น รายละเอียดช่องโหว่ การแก้ไขช่องโหว่ ผลการทดลองการประเมินช่องโหว่ เพื่อให้งานวิจัยนี้สมบูรณ์มากยิ่งขึ้น

จากการทบทวนวรรณกรรม งานวิจัยที่เกี่ยวข้อง และแนวคิดของ CDC ที่ค้นคว้าเพิ่มเติม ผู้วิจัยจึงรวบรวมและวิเคราะห์นำข้อดีต่างๆ ของงานวิจัยทั้ง 3 งาน ที่เป็นต้นแบบ รวมทั้งงานวิจัยที่เกี่ยวข้องอื่นๆ มาเป็นแนวทางของงานวิจัย การพัฒนากรอบการจัดการช่องโหว่ระบบสารสนเทศเพื่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์ กองบัญชาการกองทัพภาคที่ 2 โดยหวังเป็นอย่างยิ่งว่าจะนำงานวิจัยนี้ใช้เป็นกรอบในการจัดการช่องโหว่ระบบสารสนเทศขององค์กรต่อไป

บทที่ 3
วิธีดำเนินการศึกษา

งานการศึกษาค้นคว้าอิสระฉบับนี้เป็นการศึกษาแนวความคิด ทฤษฎี ที่เกี่ยวกับการจัดการช่องโหว่ระบบสารสนเทศ เพื่อนำมาพัฒนากรอบการจัดการช่องโหว่ระบบสารสนเทศกองบัญชาการกองทัพภาคที่ 2 โดยศึกษาทฤษฎีที่เกี่ยวข้องในการจัดการช่องโหว่ การใช้เครื่องมือในการประเมินช่องโหว่ วิเคราะห์และประเมินความเสี่ยงของช่องโหว่ที่พบบนอุปกรณ์ระบบสารสนเทศขององค์กร ซึ่งอาจจะเป็นจุดอ่อนที่จะถูกโจมตีจากผู้ไม่หวังดีต่อระบบสารสนเทศขององค์กรได้ และประเด็นสำคัญของงานวิจัยนี้ คือ การนำกรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กรที่ได้พัฒนาขึ้นมานี้ ใช้เป็นส่วนหนึ่งของมาตรการ การรักษาความมั่นคงปลอดภัยทางไซเบอร์ขององค์กรต่อไป โดยวิธีดำเนินการวิจัย ของงานวิจัยนี้มุ่งเน้นไปที่ขั้นตอนการทดลองการปฏิบัติตามกรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กรมีวิธีดำเนินการดังนี้

1) ศึกษาข้อมูล ทฤษฎี และงานวิจัยที่เกี่ยวข้องกับการพัฒนากรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กร

2) ศึกษาสภาพแวดล้อมและลักษณะของระบบสารสนเทศขององค์กร

3) เครื่องมือและอุปกรณ์ที่ใช้ในการวิจัย

4) การพัฒนากรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กร

5) ดำเนินการทดลองตามกรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กร

5.1) การจัดการทรัพย์สิน (Assets Management)

5.1.1) การรวบรวมอุปกรณ์สารสนเทศ (Discovering)

5.1.2) การประเมินระดับผลกระทบต่อองค์กรของอุปกรณ์สารสนเทศ (Assets Assessment)

5.1.3) การจัดลำดับความสำคัญอุปกรณ์สารสนเทศตามผลกระทบต่อองค์กร (Assets Prioritization)

5.2) การประเมิน (Assessment)

5.2.1) การประเมินช่องโหว่ (Vulnerability Assessment) ใช้เครื่องมือประเมินช่องโหว่ Nessus และ Nexpose ซึ่งรองรับ CVSS SCORE

5.2.2) การประเมินค่าระดับความเสี่ยง (Risk Assessment) การประเมินค่าโอกาสและผลกระทบใช้วิธี การคำนวณตาม CVSS Base Vector

5.2.3) แสดงความสำคัญระดับความเสี่ยง (Risk Rating)

5.2.4) จัดทำรายงานในด้านต่างๆ (Report)

5.3) การแก้ไข (Remediation)

5.4) การประเมินซ้ำ (Re-Assessment)

5.5) การตรวจสอบยืนยันความถูกต้อง (Verification)

6) การประเมินประสิทธิภาพกรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กร

7) ระยะเวลาและขั้นตอนในการดำเนินงาน

8) ผลลัพธ์จากการดำเนินงาน

9) การสรุปผลการวิจัย

1. ศึกษาข้อมูล ทฤษฎี และงานวิจัยที่เกี่ยวข้องกับการพัฒนากรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กร

ผู้วิจัยได้ทำการศึกษาสำรวจแนวคิดและงานวิจัยที่เกี่ยวข้อง ซึ่งอ้างอิงตามกรอบความมั่นคงปลอดภัยไซเบอร์ของ NIST โดยอิงกระบวนการประเมินความเสี่ยงตามกรอบแนวคิดของ NIST 800-30R1 Guide for Conducting Risk Assessment และวงจรชีวิตการจัดการช่องโหว่โดย CDC (Vulnerability Management Life Cycle by CDC) เพื่อให้ได้กรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กรที่มีความสอดคล้องกับเป้าหมายของการวิจัย

2. ศึกษาสภาพแวดล้อมและลักษณะของระบบสารสนเทศขององค์กร

ระบบสารสนเทศกองบัญชาการกองทัพภาคที่ 2 ประกอบไปด้วยระบบเครือข่าย และอุปกรณ์ระบบสารสนเทศในด้านต่างๆ ผู้วิจัยได้รวบรวมจากสภาพและลักษณะในปัจจุบันตามความเป็นจริงดังนี้

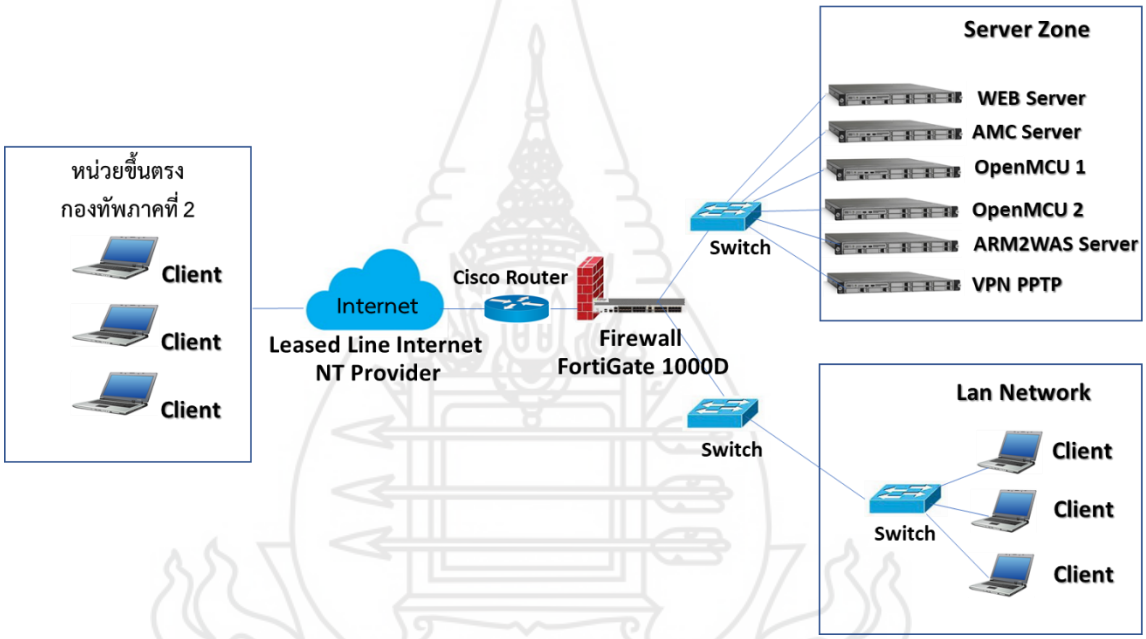
1) ระบบเครือข่ายภายใน (Intranet) ใช้ในการติดต่อสื่อสารภายในกองบัญชาการกองทัพภาคที่ 2

2) ระบบเครือข่ายภายนอก (Internet) ใช้ในการติดต่อสื่อสารกันระหว่างกองบัญชาการกองทัพภาคที่ 2 และหน่วยขึ้นตรงกับกองทัพภาคที่ 2 ที่ไม่มีโครงข่ายเฉพาะกองทัพบก

3) ระบบโครงข่ายกองทัพบก (E-Army) เป็นเครือข่ายเฉพาะของกองทัพบกที่สร้างขึ้นมาเพื่อใช้ในการติดต่อสื่อสารระหว่าง กองทัพบก กับหน่วยขึ้นตรงของกองทัพบกในส่วนภูมิภาค

ระบบสารสนเทศกองบัญชาการกองทัพภาคที่ 2 เป็นระบบที่พัฒนาขึ้นมาเพื่อช่วยปฏิบัติงานในภารกิจต่างๆ เพื่อตอบสนองนโยบายของผู้บังคับบัญชา โดยใช้เทคโนโลยีและอุปกรณ์ที่มีอยู่ในปัจจุบัน เข้ามาช่วยในการพัฒนางานระบบสารสนเทศ ตามภารกิจขององค์กรที่มีอยู่ อาทิเช่น ระบบศูนย์ข่าวอัตโนมัติ (AMC) ใช้ในการรับ-ส่งข่าวออนไลน์ ระบบประชุมทางไกลผ่านจอภาพ (Open MCU Conference) เว็บไซต์ขององค์กร (Web Sever) เครื่องแม่ข่ายระบบจำลองยุทธ (M2Was Server) ใช้ในการฝึกจำลองยุทธบนแผนที่ดิจิทัลผ่านระบบออนไลน์ เป็นต้น โดยมีผังระบบเครือข่ายตามภาพที่ 3.1

ผังระบบเครือข่ายระบบสารสนเทศ กองบัญชาการกองทัพภาคที่ 2



ภาพที่ 3.1 ผังระบบเครือข่ายระบบสารสนเทศ กองบัญชาการกองทัพภาคที่ 2

จากการศึกษาสภาพแวดล้อมขององค์กร พบได้ว่ามีโอกาสเกิดปัญหาที่อาจจะถูกโจมตีทางด้านไซเบอร์จากผู้ไม่หวังดีได้ โดยเฉพาะอย่างยิ่งกับอุปกรณ์ระบบสารสนเทศที่มีการใช้งานผ่านเครือข่ายภายนอก (Internet) ซึ่งล่อแหลมต่อการถูกโจมตีได้ง่ายกว่าเครือข่ายภายใน และโครงข่ายกองทัพบกเป็นอย่างมาก อีกทั้งยังไม่ได้มีการประเมินความเสี่ยงช่องโหว่ของอุปกรณ์ระบบสารสนเทศขององค์กร จึงทำให้มีความเสี่ยงสูงที่จะถูกโจมตีทางไซเบอร์มากขึ้นไปอีก จึงเป็นที่มาของการทำงานวิจัยของผู้วิจัยในครั้งนี้

3. เครื่องมือที่ใช้ในการศึกษา

ในการวิจัยครั้งนี้ผู้วิจัยได้กำหนดให้มีเครื่องมือและอุปกรณ์ที่ใช้ในการศึกษา ดังนี้

3.1 เครื่องมือในการศึกษา

1) แบบประเมินประสิทธิภาพกรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กรที่พัฒนาขึ้นมา

3.2 ฮาร์ดแวร์ที่ใช้ในการวิจัยประกอบด้วย

1) คอมพิวเตอร์แบบพกพาที่มีซีพียูไม่ต่ำกว่า Intel Core 2 Duo

2) ฮาร์ดดิสก์ที่มีความจุไม่ต่ำกว่า 120 GB

3) หน่วยความจำไม่ต่ำกว่า 2 GB

3.3 ซอฟต์แวร์ที่ใช้ในการวิจัยประกอบด้วย

1) ระบบปฏิบัติ การ Microsoft Windows (Notebook) สำหรับการติดตั้งโปรแกรมตรวจสอบช่องโหว่

2) โปรแกรมตรวจสอบช่องโหว่ Nessus เวอร์ชัน Essentials

3) โปรแกรมตรวจสอบช่องโหว่ Nexpose เวอร์ชัน Community Edition

4) โปรแกรมคำนวณ ค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐาน Microsoft Excel

3.4 เครื่องบริการ (Server) ที่ใช้ในการรับการประเมินช่องโหว่

1) รองรับระบบปฏิบัติการ Windows หรือ Linux

2) รองรับการใช้งาน ภาษา ASP ASP.NET PHP หรือ JSP

3) รองรับการใช้งานฐานข้อมูล MySQL หรือ MS Access

4) มีพื้นที่ใช้งานไม่น้อยกฎ 100 GB

4. การพัฒนากรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กร

4.1 แนวคิดการพัฒนากรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กร

การพัฒนากรอบการจัดการช่องโหว่ระบบสารสนเทศของ กองบัญชาการกองทัพภาคที่ 2 ที่ผู้วิจัยได้ทำการศึกษาค้นคว้าในครั้งเพื่อจะใช้เป็นต้นแบบในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร ผู้วิจัยมีความสนใจ การประเมินความเสี่ยงด้านไซเบอร์เป็นการนำมาตรฐาน NIST มาประยุกต์ใช้ (อนาวิล แก้วสอาด และ ณัฐวี อุตกฤษฎ์, 2564) สำหรับมาตรฐาน NIST

Cybersecurity Framework หรือเรียก NIST CSF Version 1.1 ซึ่งเผยแพร่โดยสถาบันมาตรฐานและเทคโนโลยีแห่งชาติ (National Institute of Standards and Technology: NIST) ของสหรัฐอเมริกา มีการทำงานฟังก์ชันหลักของโครงสร้างพื้นฐานสารสนเทศที่สำคัญ 5 กระบวนการหลักในการปรับปรุงความปลอดภัยความเสี่ยงพื้นฐานสำหรับองค์กร โดยในงานวิจัยครั้งนี้จะเอาเฉพาะประเด็นที่เป็นกระบวนการ Identify หรือกระบวนการเตรียมการบริหารความมั่นคงปลอดภัยไซเบอร์เป็นหลัก กระบวนการดังกล่าวจะเป็นการวิเคราะห์ ทำความเข้าใจบริบททรัพยากรขององค์กรที่มีอยู่เพื่อบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์อย่างเป็นระบบจากกระบวนการหลัก Identify มีกระบวนการย่อยที่ใช้ประเมินความเสี่ยงนั้นคือ Risk Assessment ที่จะใช้ในงานวิจัยครั้งนี้โดยจะมีกระบวนการประเมินความเสี่ยงตามกรอบแนวคิดของ NIST 800-30R1 Guide for Conducting Risk Assessment เป็นกระบวนการที่นำมาใช้พัฒนากรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กร

นอกจากกรอบแนวคิดของ NIST แล้วในงานวิจัยในครั้งนี้ยังได้ศึกษาและวิเคราะห์กรอบแนวคิดอีกรูปแบบหนึ่งนั่นคือ Vulnerability Management Life Cycle โดย CDC (Centers for Disease Control and Prevention) ซึ่งเป็นศูนย์ควบคุมโรคของสหรัฐอเมริกา โดยองค์กรงานทางด้าน IT ของศูนย์นี้ได้แนะนำให้องค์กรงานเครือข่ายของศูนย์ควบคุมโรคนั้นได้ใช้เป็นกรอบรักษาความมั่นคงปลอดภัยทางไซเบอร์ โดยการจัดการช่องโหว่ระบบสารสนเทศขององค์กรในรูปแบบของวงจรชีวิตการจัดการช่องโหว่ สามารถกำหนดการปฏิบัติเป็นวงรอบของการจัดการได้

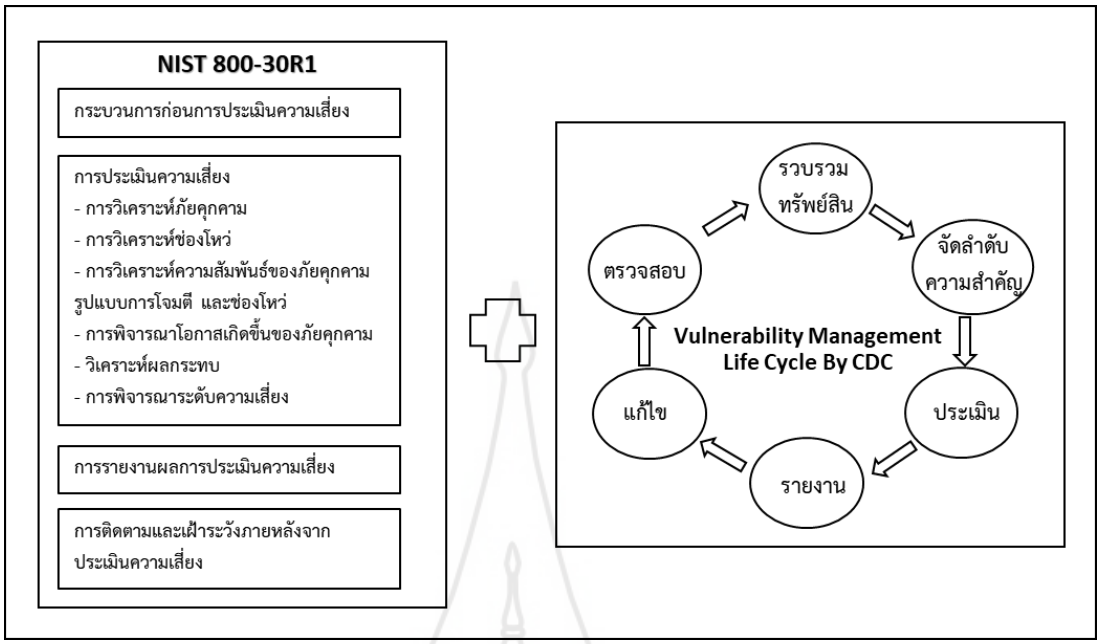
4.2 โมเดลกรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กร

จากกระบวนการประเมินความเสี่ยงตามกรอบแนวคิดของ NIST 800-30R1 Guide และวงจรชีวิตการจัดการช่องโหว่โดย CDC จากการตรวจสอบพบว่ากรอบแนวคิดของทั้งสองนั้น มีความคล้ายคลึงกันและมีภาพรวมไปในแนวทางเดียวกัน โดยเฉพาะเรื่องการประเมินช่องโหว (Vulnerability Assessment) ต่างกันเฉพาะรายละเอียดในแต่ขั้นตอนย่อย ผู้วิจัยจึงได้นำรายละเอียดมาเสนอ เพื่อให้เห็นความสอดคล้องของกรอบแนวคิดของทั้งสองระบบ เพื่อที่จะนำไปวิเคราะห์ และประยุกต์ใช้ในงานวิจัยของผู้วิจัยต่อไป ดังมีรายละเอียดตามตารางที่ 3.1

ตารางที่ 3.1 ความสอดคล้องของแนวคิดการจัดการช่องโหว่ NIST 800-30R1 Guide กับ CDC

NIST 800-30R1 Guide for Conducting Risk Assessment	**Steps in the Vulnerability Management Life Cycle by CDC**
1. กระบวนการก่อนการประเมินความเสี่ยง (Prepare for Assessment)	1. สำรวจทรัพย์สินหรืออุปกรณ์ที่จะทำการประเมิน (Discover)
	2. Prioritize Assets: จัดลำดับความสำคัญ
2. การประเมินความเสี่ยง (Conduct Risk Assessment) 2.1 การวิเคราะห์ภัยคุกคาม 2.2 การวิเคราะห์ช่องโหว่ 2.3 การวิเคราะห์ความสัมพันธ์ของภัยคุกคาม รูปแบบการโจมตี และช่องโหว่ 2.4 การพิจารณาโอกาสเกิดขึ้นของภัยคุกคาม (Likelihood Determination) 2.5 วิเคราะห์ผลกระทบ (Impact Analysis) 2.6 การพิจารณาระดับความเสี่ยง (Risk Determination)	3. Assess: การประเมินช่องโหว่
3. การรายงานผลการประเมินความเสี่ยง (Communicating and Sharing Risk Assessment Information)	4. รายงานเพื่อวิเคราะห์ และแจ้งหน่วยงานที่เกี่ยวข้อง (Report)
4. การติดตามและเฝ้าระวังภายหลังจากการประเมินความเสี่ยง (Maintain Risk Assessment)	5. แก้ไขช่องโหว่ที่พบ (Remediate)
	6. ตรวจสอบว่าช่องโหว่ถูกปิด (Verify)

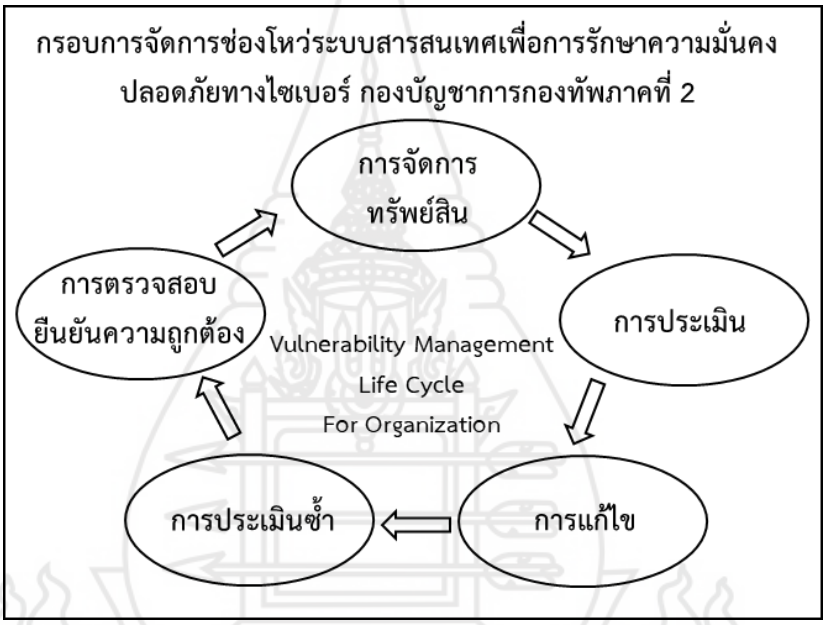
โดย Risk Assessment Process ของ NIST นั้นมีข้อมูลค่อนข้างละเอียด ได้อธิบายถึงการประเมินความเสี่ยง (Conduct Risk Assessment) เช่น การวิเคราะห์ภัยคุกคามในหลายๆ รูปแบบเช่น ภัยคุกคามจากธรรมชาติ, สภาพแวดล้อม, ภัยคุกคามจากมนุษย์ทั้งตั้งใจและไม่ตั้งใจ และมีลำดับของการประเมินเป็นขั้นตอน แต่ในงานวิจัยในครั้งนี้จะวิเคราะห์และตรวจสอบเฉพาะการประเมินในส่วนของทรัพยากรของระบบสารสนเทศขององค์กรเพียงเท่านั้น ส่วนลำดับขั้นตอน Vulnerability Management Life Cycle by CDC จะมีเฉพาะหัวข้อหลักของการจัดการช่องโหว่ แต่อย่างไรก็ดีผู้วิจัยนั้นสนใจและเชื่อมั่นในรูปแบบของวงจรชีวิตในการทำงานของ VMLC ของ CDC ที่สามารถนำมาใช้พัฒนาเป็นกรอบการจัดการช่องโหว่ขององค์กรของผู้วิจัยได้ อีกทั้งยังผสมผสานเข้ากับขั้นตอนของ NIST 800-30R1 Guide ทำให้มีองค์ประกอบการทำงานของการพัฒนากรอบการจัดการช่องโหว่มีความสมบูรณ์มากยิ่งขึ้น ดังภาพที่ 3.2



ภาพที่ 3.2 กรอบแนวความคิดต้นแบบการพัฒนากรอบการจัดการช่องโหว่ระบบสารสนเทศ

กรอบการจัดการช่องโหว่ระบบสารสนเทศเพื่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์ กองบัญชาการกองทัพภาคที่ 2 ที่พัฒนาขึ้นมานั้น ได้นำข้อดีจากการเปรียบเทียบข้อดีและข้อจำกัด ตารางที่ 2.3 จากการทบทวนกรรมของ 1) อนาวิล แก้วสะอาด และ ณัฐวี อุตกฤษฎ์ (2564) แนวทางการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ระดับองค์กร 2) สุรทศ ไตรติลานันท์ และ สุรพล รวยสูงเนิน (2559) กรณีศึกษา: โมเดลทางด้านเทคนิคสำหรับวิธีการประเมินความเสี่ยง ความมั่นคงปลอดภัยในระบบสารสนเทศสำหรับโรงพยาบาล ข้อดีในงานวิจัยแรกนั้นคืออธิบายกรอบอ้างอิงได้อย่างชัดเจน และยังมีกรอบขั้นตอนการปฏิบัติที่เป็นกรอบสำคัญที่สามารถนำมาเป็นต้นแบบได้ กล่าวคือนำแนวคิดของ NIST Cybersecurity Framework ในขั้นตอน Risk Assessment โดยมี NIST 800-30R1 Guide เป็นต้นแบบในการพัฒนา จากนั้นได้นำข้อดีของงานวิจัยที่สองนั่นคือ มีตัวอย่างในการประเมินความเสี่ยงช่องโหว่ระบบสารสนเทศที่ตรวจพบค่อนข้างละเอียด มีที่มาที่ไปของการคำนวณหาระดับความเสี่ยงช่องโหว่ ซึ่งเป็นประโยชน์ต่อผู้วิจัย กล่าวคือนำข้อดีในงานวิจัยที่สองนั้นไปเสริมงานวิจัยแรก ในขั้นตอนย่อยโดยใช้แนวคิดการทดสอบการประเมินความมั่นคงปลอดภัยสารสนเทศโดยการประเมินช่องโหว่ (Vulnerability Assessment) ของงานวิจัยที่สองนั่นเอง เช่น การประเมินค่าระดับความเสี่ยงคือขั้นตอนการกำหนดค่าของโอกาส และผลกระทบโดยคำนวณจากเกณฑ์ที่เป็นมาตรฐาน คือ CVSS Base Score, การประเมินระดับความสำคัญของความเสี่ยงโดยประยุกต์ใช้วิธีการประเมินความเสี่ยงตามมาตรฐานขององค์กร OWASP RISK RATING

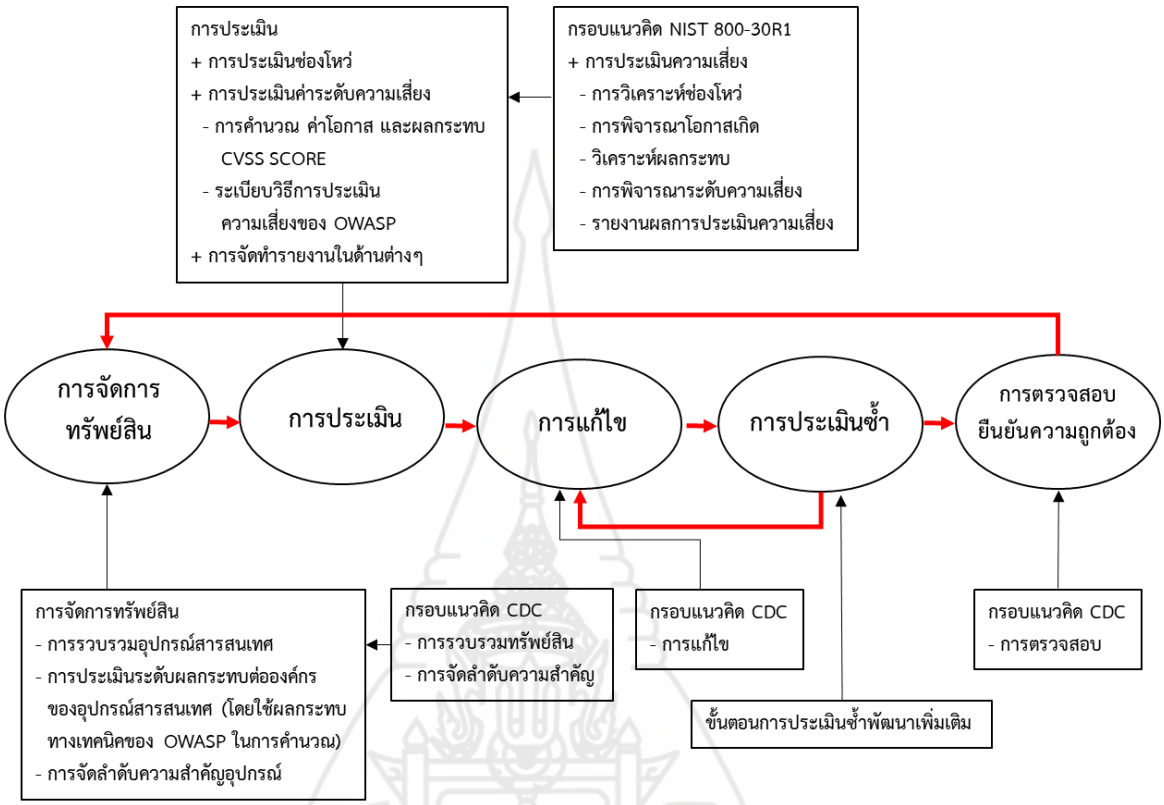
ผู้วิจัยได้นำความสอดคล้องจากกรอบแนวคิดของการจัดการช่องโหว่ระหว่าง NIST กับ CDC ในตารางที่ 3.1 กล่าวคือ ได้ใช้แนวคิด NIST 800-30R1 Guide (Risk Assessment Process) จากงานวิจัยของ อนาวิล แก้วสะอาด และ ณัฐวี อุตกฤษฎ์ (2564) แนวทางการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ระดับองค์กร และกรอบแนวคิด VMLC CDC โดยการสืบค้นกรอบการรักษาความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร CDC ซึ่งได้กล่าวในรายละเอียดมาแล้วในเบื้องต้น นำมาพัฒนากรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กร จึงทำให้เกิดกรอบการจัดการช่องโหว่ระบบสารสนเทศเพื่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์ กรณีศึกษากองบัญชาการกองทัพภาคที่ 2 ดังภาพที่ 3.3



ภาพที่ 3.3 โมเดลกรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กร

จากภาพที่ 3.3 จากกรอบแนวคิดกรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กร ที่ได้พัฒนาขึ้นมานั้น ผู้วิจัยได้นำข้อดีของทั้งสองกรอบแนวคิด และได้ลดขั้นตอนหมายถึงรวมขั้นตอนที่สามารถปฏิบัติได้ในเรื่องเดียวกันเช่นในกรอบ CDC ได้ปรับขั้นตอน รวบรวมทรัพย์สิน กับจัดลำดับความสำคัญ รวมเป็นขั้นตอนเดียวของกรอบที่พัฒนาขึ้นมาคือ การจัดการทรัพย์สิน และได้นำขั้นตอน การรายงาน เข้าไปอยู่ในขั้นตอน การประเมิน เพื่อง่ายต่อการปฏิบัติ ส่วนหัวใจหลักสำคัญคือขั้นตอนการประเมินความเสี่ยงช่องโหว่ยังคงดำเนินตามกรอบของ NIST 800-30R1 ซึ่งจะอยู่ในขั้นตอน การประเมิน ของกรอบที่พัฒนาขึ้นมา นอกจากนั้นยังได้นำการคำนวณหาค่าโอกาสที่จะเกิดและค่าผลกระทบ โดยคำนวณจากเกณฑ์ที่เป็นมาตรฐาน คือ CVSS และ การประเมินระดับความสำคัญของความเสี่ยงโดยประยุกต์ใช้วิธีการประเมินความเสี่ยงตามมาตรฐานขององค์กร

OWASP RISK RATING มาอยู่ในขั้นตอนการประเมินของกรอบที่พัฒนาขึ้นมาด้วย ทั้งนี้เพื่อปรับให้เหมาะสมกับองค์กรในการนำกรอบแนวคิดดังกล่าวมาใช้สามารถแสดงได้ตามภาพที่ 3.4



ภาพที่ 3.4 องค์ประกอบการพัฒนากรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กร

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

การประเมินความเสี่ยงระบบสารสนเทศขององค์กรเป็นขั้นตอนหรือกระบวนการในการจัดระดับความสำคัญของความเสี่ยงหรือช่องโหว่ที่ประเมินพบ โดยมีกรอบแนวทางมาตรฐานที่กำหนดไว้ โดยที่แต่ละองค์กรนำมาปฏิบัติ หรือประยุกต์ใช้ให้สอดคล้องกับความเหมาะสมขององค์กร มาตรฐานหรือแนวทางการประเมินความเสี่ยงระบบสารสนเทศขององค์กรที่ผู้วิจัยได้นำมาเป็นแนวทางในการทำงานวิจัยที่ได้อธิบายไปแล้วนั้นคือ NIST 800-30R1 และวงจรชีวิตของ CDC แต่จากการที่ผู้วิจัยได้ศึกษาจากทฤษฎีที่เกี่ยวข้อง และจากการตารางทบทวนวรรณกรรม พบเพิ่มเติมว่า

มาตรฐานหรือแนวทางการประเมินความเสี่ยงระบบสารสนเทศขององค์กรที่นิยมใช้ในระดับสากลมีดังนี้

1) COBIT 5 (Control Objectives for Information and Related Technology) เป็นมาตรฐาน ที่มีจุดประสงค์ในการสร้างความมั่นใจว่าการใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศนั้นสอดคล้องกับวัตุประสงค์เชิงธุรกิจขององค์กร เพื่อให้เกิดการใช้ทรัพยากรอย่างมีประสิทธิผลอันจะส่งประโยชน์สูงสุดแก่องค์กร ช่วยให้เกิดความสมดุลระหว่างความเสี่ยงด้านเทคโนโลยีสารสนเทศ และผลตอบแทนของการลงทุนในระบบสารสนเทศซึ่งจะทำให้การควบคุมการใช้งานเทคโนโลยีสารสนเทศในองค์กรเป็นไปอย่างถูกต้อง และมีประสิทธิผล ส่งผลให้ตรงกับความต้องการทางธุรกิจ และบรรลุเป้าหมายทางธุรกิจที่ตั้งเป้าไว้ (ที่มา: https://www.isaca.org/resources/news-and-trends/industry-news/2017/cobit-5-for-riska-powerful-tool-for-risk-management)

2) ISO/IEC 27001 หรือระบบการบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศ Information Security Management System (ISMS) (สุรทศ ไตรติลานันท์ และ สุรพล รวยสูงเนิน,2559) เป็นแนวทางในการบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศได้กำหนดกระบวนการในการประเมินความเสี่ยงประกอบด้วยขั้นตอนดังนี้

2.1) การระบุทรัพย์สินด้านระบบสารสนเทศ (Identify major assets)

2.2) การอธิบายเกี่ยวกับความสำคัญต่อธุรกิจ หรือมูลค่าของทรัพย์สิน (Assess asset value in terms)

2.3) การระบุภัยคุกคามที่อาจเกิดขึ้น กับทรัพย์สิน หรือระบบสารสนเทศ (Identify threats)

2.4) การระบุจุดอ่อน หรือช่องโหว่ของทรัพย์สิน หรือระบบสารสนเทศ (Identify vulnerabilities)

2.5) การประเมินระดับความเสี่ยง (Identify measures of risk)

2.6) การกำหนดหรืออธิบายเกี่ยวกับความเสี่ยง (Security Requirements)

2.7) การกำหนดวิธีการควบคุมความเสี่ยง (Security Controls)

2.8) การประเมินระดับความเสี่ยงที่ลดลงหลังจากระบุจุดควบคุม (Reduce Risk)

2.9) การพิจารณาว่าอยู่ในเกณฑ์ความเสี่ยงที่ยอมรับได้หรือไม่ (Risk Acceptance)

3) OWASP (Open Web Application Security Project) แนวทางการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ระดับองค์กร โดยเป็นกระบวนการทดสอบความมั่นคงปลอดภัยของเว็บแอปพลิเคชัน (OWASP Testing Guide, The Open Web Application Security Project (OWASP), 2008) มีรูปแบบในการประเมินความเสี่ยงประกอบไปด้วยขั้นตอนที่สำคัญดังนี้

3.1) การระบุความเสี่ยงด้านสารสนเทศ (Identify Risk)

3.2) การประมาณระดับโอกาสที่ความเสี่ยงอาจเกิดขึ้น (Estimating Likelihood)

3.3) การประมาณระดับผลกระทบที่มีผลต่อระบบสารสนเทศ (Estimating Impact)

3.4) การกำหนดระดับความเสี่ยงของระบบสารสนเทศ (Determining Severity of the Risk)

3.5) การปรับปรุงให้มีกระบวนการจัดลำดับความเสี่ยงให้มีความเหมาะสม (Deciding What to Fix)

3.6) การเลือกรูปแบบเพื่อใช้ในการประเมินและจัดลำดับความเสี่ยง (Customizing Your Risk Rating Model)

จากกรอบแนวคิดมาตรฐานดังกล่าว ผู้วิจัยได้นำมาเปรียบเทียบเพื่อให้เห็นภาพรวมความสอดคล้องที่คล้ายคลึงกัน และขั้นตอนที่นำมาประยุกต์เป็นกรอบการจัดการช่องโหว่ของผู้วิจัย โดยจะมีกรอบแนวคิดที่ได้เปรียบเทียบดังนี้ 1) ISO/IEC 27001:2013 (ISMS) 2) NIST 800-R1 3) OWASP ส่วน COBIT 5 นั้นผู้วิจัยจะไม่นำมาเปรียบเทียบเพราะขั้นตอนการประเมินความเสี่ยงของ COBIT 5 นั้นก็จะอ้างอิงมาตรฐานอื่นเช่น ISO/IEC 27001 , ISO/IEC 27005, COSO นำมาเป็นกระบวนการในการประเมินความเสี่ยง รายละเอียดตามตารางที่ 3.2 ดังนี้

ตารางที่ 3.2 การวิเคราะห์กรอบแนวคิดมาตราฐานการประเมินความเสี่ยง

	กรอบแนวคิดมาตราฐานการประเมินความเสี่ยง			
ลำดับ	**ISMS (ISO/IEC 27001)**	**NIST 800-R1(NIST)**	**OWASP**	**CDC**
1.	Identify major assets	Prepare for Assessment	NA	Discover
2.	Assess asset value in terms		NA	Prioritize Assets
3.	Identify threats	Identify Threat Sources and Events	Identify Risk	Assess
4.	Identify vulnerabilities	Identify vulnerabilities		
5.	NA	Determine Likelihood	Estimating Likelihood	
6.	NA	Determine Impact	Estimating Impact	
7.	Identify measures of risk	Determine Risk	Determining Severity of the Risk	
8.	Security Requirements	Define Security Controls with Effectiveness	Deciding What to Fix	NA
9.	Security Controls			NA
10.	Reduce Risk	NA	NA	NA
11.	Risk Acceptance	NA	NA	NA
12.	NA	Communicate Results	NA	Report
13.	NA	NA	Customizing Your Risk Rating Model	NA
14.	NA	Maintain Risk Assessment	NA	Remediate Verify

จากตารางที่ 3.2 จะเห็นได้ว่ากรอบแนวคิดของ ISMS และ NIST 800-R1 จะคล้ายคลึงและสอดคล้องกันโดยจะมีกระบวนการ การรวบรวมข้อมูลหรือทรัพย์สิน การประเมินความเสี่ยง และคำแนะนำเอกสารการรายงานความเสี่ยงที่เกิดขึ้น ทางด้านกรอบแนวคิดของ OWASP ก็จะเน้นเรื่องขั้นตอนการประเมินความเสี่ยงเป็นหลัก ส่วนวงจรชีวิตของ CDC นั้นจะเป็นกรอบแนวคิดหัวข้อหลักๆ ในการปฏิบัติที่เป็นวงรอบ ดังนั้นในการที่ผู้วิจัยเลือกใช้กรอบแนวคิดของ NIST 800-R1 ก็จะมีผลไม่แตกต่างกันจากกรอบแนวคิดของ ISMS และเมื่อนำประยุกต์เข้ากับวงจรชีวิตของ CDC โดยมีขั้นตอนการคำนวณหาค่าความเสี่ยง จากระเบียบวิธีการประเมินความเสี่ยงของ OWASP ก็จะ

ส่งผลให้กรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กรที่พัฒนาขึ้นมานั้น มีมาตรฐานการประเมินความเสี่ยงช่องโหว่ที่น่าเชื่อถือ สามารถนำไปใช้กับองค์กรของผู้วิจัยได้อย่างเหมาะสม สำหรับกรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กรที่พัฒนาขึ้นมาจากกรอบแนวคิดของ NIST 800-R1 และ วงจรชีวิตของ CDC ผู้วิจัยได้นำมาเปรียบเทียบกับกรอบแนวคิดมาตรฐานการประเมินความเสี่ยงที่นิยมใช้กันในระดับสากลโดยมีรายละเอียดตามตารางที่ 3.3 ดังนี้

ตารางที่ 3.3 เปรียบเทียบกรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กรและกรอบแนวคิดมาตรฐานการประเมินความเสี่ยง

กรอบการจัดการช่องโหว่ระบบสานสนเทศขององค์กร (NIST 800-R1 + CDC)			กรอบแนวคิดมาตรฐานการประเมินความเสี่ยง		
ลำดับ	กระบวนการ	ขั้นตอนในกระบวนการ	ISMS	NIST	OWASP
1.	การจัดการทรัพย์สิน (Assets Management)	1.1 การรวบรวมอุปกรณ์สารสนเทศ (Discovering)	✓	✓	X
		1.2 การประเมินระดับผลกระทบต่อองค์กรของอุปกรณ์สารสนเทศ (Assets Assessment)	✓	✓	X
		1.3 การจัดลำดับความสำคัญอุปกรณ์สารสนเทศตามผลกระทบต่อองค์กร (Assets Prioritization)	X	X	✓
2.	การประเมิน (Assessment)	2.1 การประเมินช่องโหว่ (Vulnerability Assessment)	✓	✓	X
		2.2 การประเมินค่าระดับความเสี่ยง (Risk Assessment)			
		- CVSS SCORE	X	X	X
		- Determine Likelihood	X	✓	✓
		- Determine Impact	X	✓	✓
		2.3 แสดงความสำคัญระดับความเสี่ยง (Risk Rating)	✓	✓	✓
		2.4 จัดทำรายงานในด้านต่างๆ (Report)	✓	✓	X
3.	การแก้ไข (Remediation)		✓	✓	X
4.	การประเมินซ้ำ (Re-Assessment)		X	X	X
5.	การตรวจสอบยืนยันความถูกต้อง (Verification)		X	X	X

จากตารางที่ 3.3 จะเห็นได้ว่ากรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กรที่พัฒนาขึ้นมานั้น เป็นกระบวนการที่เน้นการพัฒนาให้เป็นกระบวนการที่สมบูรณ์กล่าวคือ ได้นำข้อดีในแต่ละขั้นตอนของกรอบแนวคิดที่นำมาเป็นต้นแบบในการพัฒนาคือกรอบแนวคิดการประเมินความเสี่ยงระบบสารสนเทศของ NIST 800-R1 และ CDC นอกจากนั้นยังนำระเบียบวิธีการประเมินความเสี่ยงระบบสารสนเทศของ OWASP นำมาเป็นขั้นตอนสำคัญของกรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กร นอกจากนั้นแล้ว กรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กรที่พัฒนาขึ้น ยังได้เพิ่มเติมการแก้ไข การประเมินซ้ำ และตรวจสอบความถูกต้อง สามารถนำไปปฏิบัติได้ในรูปแบบวงจรชีวิตที่เป็นการปฏิบัติตามวงรอบ สามารถกำหนดตามความเหมาะสมขององค์กรผู้วิจัย

สาเหตุที่ผู้วิจัยเลือกกรอบแนวคิดการรักษาความมั่นคงปลอดภัยไซเบอร์ ของ NIST Cybersecurity Framework (NIST CSF 1.1) เป็นต้นแบบในการพัฒนากรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กรของผู้วิจัยนั้น เนื่องจาก NIST CSF 1.1 กรอบการทำงานด้านความมั่นคงปลอดภัยไซเบอร์ที่ใช้งานอย่างแพร่หลายมาก คือ NIST Cybersecurity Framework หรือเรียก NIST CSF Version 1.1 ซึ่งเผยแพร่โดยสถาบันมาตรฐานและเทคโนโลยีแห่งชาติ (National Institute of Standards and Technology: NIST) ของสหรัฐอเมริกา ซึ่งประเทศไทยเองได้นำ NIST CSF มาเป็นต้นแบบส่วนหนึ่งในการจัดทำ พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 โดยมาตรา 13 วรรคสอง ได้กำหนดกรอบมาตรฐานตามแบบ NIST Cybersecurity Framework โดยให้คำนึงถึงหลักการบริหารความเสี่ยง โดยอย่างน้อยต้องประกอบด้วยวิธีการและมาตรการ ดังต่อไปนี้ 1) การระบุความเสี่ยงที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล (Identify) 2) มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect) 3) มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect) 4) มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond) 5) มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover) ที่มา: http://web.krisdika.go.th/lawHeadPDF.jsp?formatFile=pdf&hID=0 และเพื่อให้สอดคล้องกับนโยบายของกองทัพบก ซึ่งเป็นหน่วยเหนือของหน่วยงานผู้วิจัย ได้ใช้กรอบการรักษาความมั่นคงปลอดภัยไซเบอร์ NIST Cybersecurity Framework โดยนำกรอบแนวทางการปฏิบัติงานของศูนย์ความปลอดภัยกองทัพบก ได้ยึดถือการดำเนินการตามหลักหน้าที่พื้นฐานของสถาบันมาตรฐานและเทคโนโลยีแห่งสหรัฐอเมริกา (National Institute of Standards and Technology : NIST) ทั้ง 5 ประการ (IPDRR : Identify, Protect, Detect, Respond, Recover) (พลตรี วาสิฏฐ์ มณีโชต, 2560, น. 64) สำหรับวงจรชีวิตการจัดการช่องโหว่โดย CDC (Vulnerability Management Life Cycle by CDC (VMLC)) ที่ผู้วิจัยนำมาเป็นต้นแบบในการพัฒนากรอบการจัดการช่องโหว่ระบบสารสนเทศของ

องค์กรของผู้วิจัยนั้น มีวัตถุประสงค์เพื่อให้องค์กรสามารถระบุจุดอ่อนด้านความปลอดภัยของระบบคอมพิวเตอร์ จัดลำดับความสำคัญของสินทรัพย์ ประเมิน รายงาน และแก้ไขจุดอ่อน และตรวจสอบว่าได้กำจัดไปแล้ว โดยจุดเด่นก็คือการที่สามารถนำมากำหนดเป็นวงรอบหรือวงจรชีวิต ในการจัดการช่องโหว่ระบบสารสนเทศขององค์กรได้ตามวัตถุประสงค์ของงานวิจัยนี้ เมื่อนำกรอบแนวคิดของทั้งสองมาประยุกต์ขั้นตอนและวิธีการ ทำให้ได้เป็นขั้นตอนของกรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กรที่พัฒนาขึ้นมาทั้ง 5 ขั้นตอนตามภาพที่ 3.4 นั้นสามารถสรุปได้เป็นข้อดี ซึ่งอธิบายถึงการนำกรอบแนวคิดทั้งสองมาเป็นต้นแบบในงานวิจัยได้ดังนี้

1) เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์มีประสิทธิภาพ และเพื่อให้มีมาตรการป้องกัน รับมือและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์อันกระทบต่อความมั่นคงของรัฐและความสงบเรียบร้อยภายในประเทศ ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2565 ที่ได้บัญญัติไว้

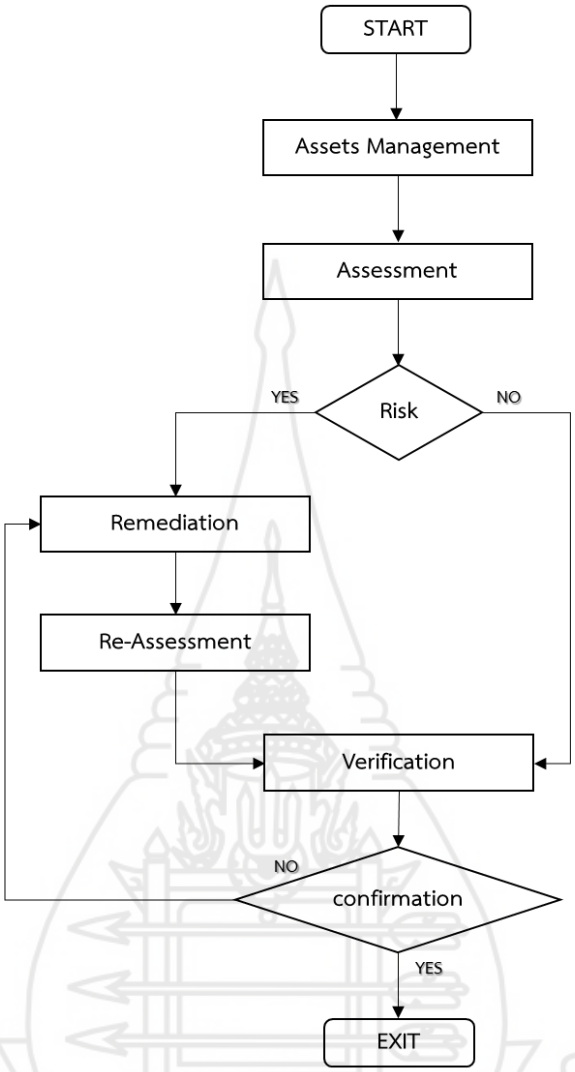
2) เพื่อให้สอดคล้องกับกองทัพบกซึ่งเป็นหน่วยบังคับบัญชากองทัพภาคที่ 2 ซึ่งได้ดำเนินการนำกรอบแนวคิดของ NIST Cybersecurity Framework มาใช้งาน

3) เพื่อให้ได้ขั้นตอนที่เหมาะสมสำหรับองค์กรของผู้วิจัยโดยนำขั้นตอนการประเมินความเสี่ยงของ NIST 800-R1 ซึ่งมีขั้นตอนในการลดความเสี่ยงที่ชัดเจน และเมื่อนำมาประยุกต์ร่วมกับวงจรชีวิตของ CDC ซึ่งเป็นวงรอบในการจัดการช่องโหว่ ทำให้กรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กร มีการดำเนินการที่มีกรอบการปฏิบัติและวงรอบในการดำเนินการสำหรับการจัดการช่องโหว่ หรือจุดอ่อน ได้อย่างมีประสิทธิภาพ และเหมาะสมกับองค์กรของผู้วิจัย

5. ดำเนินการทดลองตามกรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กร

การดำเนินการทดลองของงานวิจัยในครั้งนี้ ได้ดำเนินการทดลองที่แผนกกรรมวิธีข้อมูลกองทัพภาคที่ 2 ซึ่งเป็นหน่วยงานที่รับผิดชอบระบบสารสนเทศขององค์กร โดยจะทำการทดลองกับอุปกรณ์แม่ข่ายที่ใช้ในภารกิจต่างๆ ของกองทัพภาคที่ 2 รายละเอียดจะอยู่ในหัวข้อต่อไป

กรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กร แสดงเป็นแผนผังหรืออัลกอลิทึมในแต่ขั้นตอนแสดงให้เห็นภาพรวมการทำงานตามวงจรชีวิต (Vulnerability Management Life Cycle For Organization) การดำเนินการทดลองตามกรอบการจัดการช่องโหว่สารสรเทศขององค์กรจะดำเนินการตามขั้นตอนของอัลกอลิทึม ตามกรอบที่พัฒนาขึ้นมาดังภาพที่ 3.5



ภาพที่ 3.5 ผังวงจรการทำงานกรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กร

5.1 การจัดการทรัพย์สิน (Assets Management)

5.1.1 การรวบรวมอุปกรณ์สารสนเทศ (Discovering)

งานวิจัยนี้ ได้รวบรวมและเตรียมอุปกรณ์ที่เป็นเครื่องแม่ข่ายซึ่งให้บริการในงานภารกิจต่างๆ ขององค์กร เพื่อทำการประเมินช่องโหว่ อาทิเช่น เครื่องแม่ข่ายระบบศูนย์อัตโนมัติ (Automatic Message Center : AMC) ใช้ในการรับ-ส่งข่าวออนไลน์ เครื่องแม่ข่ายระบบประชุมทางไกลผ่านจอภาพ (Open MCU Conference) เครื่องแม่ข่ายเว็บไซต์ขององค์กร (Web Sever) เครื่องแม่ข่ายระบบจำลองยุทธ (ARMY2 WARSIM : ARM2Was) ใช้ในการฝึกจำลองยุทธบนแผนที่ดิจิทัลผ่านระบบออนไลน์ เป็นต้น ดังมีรายละเอียดอุปกรณ์ตามตารางที่ 3.4 รายการอุปกรณ์ระบบสารสนเทศ

ตารางที่ 3.4 รายการอุปกรณ์ระบบสารสนเทศ

ลำดับ	ชื่อเครื่อง	หมายเลขไอพี
1.	AMC SERVER	203.xxx.xxx.xxx
2.	SERVER (ARMY2.MI.TH)	203.xxx.xxx.xxx
3.	OpenMCU 1	10.105.xxx.xxx
4.	OpenMCU 2	10.105.xxx.xxx
5.	ARM2WAS	10.105.xxx.xxx
6.	VPN PPTP	203.xxx.xxx.xxx
7.	Firewall FortiGate 1000D	10.105.xxx.xxx
8.	Aruba 293 0F JL259A (L2 Switch)	10.105.xxx.xxx

5.1.2 การประเมินระดับผลกระทบต่อองค์กรของอุปกรณ์สารสนเทศ (Assets Assessment)

เป็นการจัดกลุ่มอุปกรณ์ระบบสารสนเทศเพื่อจัดลำดับเข้าประเมินช่องโหว่ โดยมีแนวคิดในการจัดคือ จัดกลุ่มที่มีผลกระทบต่อองค์กรมากที่สุด กล่าวคือถ้าอุปกรณ์ เกิดความเสียหายไม่สามารถดำเนินงานได้จะส่งผลต่อภารกิจเสียหายร้ายแรงต่อองค์กรมากที่สุด จนไปถึงกลุ่มที่มีผลกระทบต่อองค์กรน้อยที่สุด เพื่อจัดลำดับในการประเมินช่องโหว่ระบบสารสนเทศขององค์กรต่อไป การประเมินผลกระทบต่อภารกิจขององค์กรนั้น ได้แนวความคิดจากปัจจัยผลกระทบทางธุรกิจและปัจจัยผลกระทบทางเทคนิคของ OWASP (OWASP Testing Guide, 2008) มาประยุกต์ใช้กับองค์กร ในขั้นตอนนี้จะใช้ค่าเวกเตอร์ของปัจจัยผลกระทบทางธุรกิจและปัจจัยผลกระทบทางเทคนิคของ OWASP จากงานวิจัยของ สุรทศ ไตรติลานันท์ และ สุรพล รวยสูงเนิน (2559) กรณีศึกษา: โมเดลทางด้านเทคนิคสำหรับวิธีการประเมินความเสี่ยง ความมั่นคงปลอดภัยในระบบสารสนเทศสำหรับโรงพยาบาล มาปรับใช้ให้เข้ากับบริบทขององค์กรของผู้วิจัย

โดยมีวิธีการคำนวณตามสมการ (1) ดังนี้

BI = AVERAGE(Fd[x], Rd[x], Nc[x], Pv[x]) (1)

BI คือ Business Impact Value

Fd[x], Rd[x], Nc[x], Pv[x] ใช้ค่าเวกเตอร์ปัจจัยผลกระทบทางธุรกิจ ตามตารางที่ 3.5

ตารางที่ 3.5 ปัจจัยผลกระทบทางธุรกิจ (Business Impact Factor)

Business Impact Factor	Case of Metric	Rating
ความเสียหายทางการเงิน Financial Damage (Fd)	น้อยกว่าค่าใช้จ่ายในการแก้ไขจุดอ่อน (Less than the cost to fix vulnerability)	1
	ผลกระทบเล็กน้อยต่อกำไรประจำปี (Minor effect on annual profit)	3
	ผลกระทบอย่างมีนัยสำคัญต่อกำไรประจำปี (Significant effect on annual profit)	7
	การล้มละลาย (Bankruptcy)	9
ความเสียหายต่อชื่อเสียง Reputation damage (Rd)	ความเสียหายน้อยที่สุด (Minimal damage)	1
	การสูญเสียบัญชีหลัก (Loss of major accounts)	4
	การสูญเสียค่าความนิยม (Loss of goodwill)	5
	ความเสียหายต่อแบรนด์ (Brand damage)	9
การไม่ปฏิบัติตาม Non-compliance (Nc)	การละเมิดเล็กน้อย (Minor violation)	2
	การละเมิดที่ชัดเจน (Clear violation)	5
	การละเมิดรายละเอียดสูง (High profile violation)	7
การละเมิดความเป็นส่วนตัว Privacy violation (Pv)	หนึ่งคน (One individual)	3
	หลายร้อยคน (Hundreds of people)	5
	หลายพันคน (Thousands of people)	7
	ผู้คนนับล้าน (Millions of people)	9

แต่จากการศึกษาเพิ่มจากเอกสารอ้างอิงของ OWASP Testing Guide, The Open Web Application Security Project (OWASP), 2008. พบว่านอกจากปัจจัยผลกระทบทางธุรกิจ ยังมีปัจจัยสำคัญอีกหนึ่งปัจจัยคือ ปัจจัยผลกระทบทางเทคนิค ซึ่งผู้วิจัยเห็นว่าเหมาะสมกับบริบทขององค์กรของผู้วิจัย ซึ่งเป็นแนวทางในการประเมินทางด้านเทคนิค มากกว่าเชิงธุรกิจ โดยมีค่าเวกเตอร์ ของปัจจัยผลกระทบทางเทคนิค ที่ส่งผลกระทบต่อองค์กร ดังตารางที่ 3.6

ตารางที่ 3.6 ปัจจัยผลกระทบทางเทคนิค (Technical Impact Factors)

Technical Impact Factors	Case of Metric	Rating
การสูญเสียความลับ Loss of Confidentiality (Lc)	เปิดเผยข้อมูลที่ไม่สำคัญน้อยที่สุด (Minimal non-sensitive data disclosed)	2
	เปิดเผยข้อมูลสำคัญน้อยที่สุด (Minimal critical data disclosed)	6
	เปิดเผยข้อมูลที่ไม่สำคัญอย่างกว้างขวาง (Extensive non-sensitive data disclosed)	6
	เปิดเผยข้อมูลสำคัญอย่างยิ่ง (Extensive critical data disclosed)	7
	ข้อมูลทั้งหมดถูกเปิดเผย (All data disclosed)	9

ตารางที่ 3.6 (ต่อ)

Technical Impact Factors	Case of Metric	Rating
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
การสูญเสียความรับผิดชอบ Loss of Accountability (LAc)	ติดตามได้อย่างสมบูรณ์ (Fully traceable)	1
	ติดตามได้ (Possibly traceable)	7
	ไม่ทราบบุคคลโดยสมบูรณ์ (completely anonymous)	9

จากตารางที่ 3.5 และ 3.6 ผู้วิจัยได้วิเคราะห์ในแต่ละเวกเตอร์ของปัจจัยผลกระทบทั้งสองปัจจัย จะให้ความสำคัญปัจจัยผลกระทบทางเทคนิค มากกว่าปัจจัยผลกระทบทางธุรกิจ สืบเนื่องจากองค์กรของผู้วิจัยมิได้เป็นองค์กรเชิงธุรกิจแต่อย่างใด ในด้านปัจจัยผลกระทบทางเทคนิคนั้นผู้วิจัยได้เลือกเวกเตอร์ในหัวข้อ CIA ซึ่งเป็นหลักพื้นฐานด้านความปลอดภัยสารสนเทศ การบริหารจัดการระบบความมั่นคงปลอดภัยข้อมูล (Information Security) CIA ประกอบไปด้วย การรักษาความลับของข้อมูล (Confidentiality) , การรักษาความถูกต้องของข้อมูล (Integrity) และ การทำให้ระบบมีความมั่นคงและมีเสถียรภาพในการให้บริการอย่างต่อเนื่อง (Availability) ซึ่งก็ตรงกับเวกเตอร์ของปัจจัยผลกระทบทางเทคนิคที่ผู้วิจัยได้เลือกใช้คือ การรักษาความลับ (Lc), ความสมบูรณ์ (Li), ความพร้อมใช้งาน (La) ส่วนปัจจัยผลกระทบทางธุรกิจผู้วิจัยได้เลือกเวกเตอร์ในหัวข้อ ความเสียหายต่อชื่อเสียง (Rd) ซึ่งเป็นหัวข้อที่เหมาะสมในการไปคำนวณค่าระดับผลกระทบต่อองค์กรจากที่ได้กล่าวมาแล้วนั้นองค์กรของผู้วิจัยไม่ได้เป็นองค์กรเชิงธุรกิจแต่อย่างใดจึงไม่ได้นำเวกเตอร์ของปัจจัยผลกระทบทางธุรกิจในหัวข้ออื่นมาใช้แต่อย่างใด จากเหตุผลดังกล่าวผู้วิจัยจึงได้วิเคราะห์นำค่า

เวกเตอร์ของทั้งสองปัจจัยผลกระทบนำมาปรับใช้ให้สอดคล้องกับบริบทขององค์กรผู้วิจัยให้เหมาะสมมากที่สุด โดยนำมาปรับเป็นปัจจัยผลกระทบต่อองค์กร และดำเนินการประเมินเพื่อจัดลำดับของอุปกรณ์ระบบสารสนเทศเพื่อเข้าทำการประเมินความเสี่ยงช่องโหว่ต่อไป ตามตารางที่ 3.7 ดังนี้

ตารางที่ 3.7 ปัจจัยผลกระทบต่อองค์กร (Organization Impact)

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

เมื่อได้ปัจจัยผลกระทบต่อองค์กรแล้ว ผู้วิจัยได้ทำการปรับปรุงเปลี่ยนแปลงสมการในการคำนวณหาค่าผลกระทบต่อองค์กร โดยรูปแบบสมการนั้นยังคงเดิมตามแบบของ (OWASP) ปรับเปลี่ยนเฉพาะเวกเตอร์และชื่อของผลกระทบเปลี่ยนจาก BI เป็น OI ได้สมการดังนี้

วิธีการคำนวณตามสมการ (2) ซึ่งได้ปรับปรุงมาจากสมการ (1) ดังนี้

OI = AVERAGE(Lc[x], Li[x], La[x], Rd[x]) (2)

OI คือ Organization Impact Value

Lc[x], Li[x], La[x], Pd[x] ใช้ค่าเวกเตอร์ปัจจัยผลกระทบต่อองค์กร ตามตารางที่ 3.7

จากการคำนวณตามสมการ (2) จะได้ค่าระดับผลกระทบต่อองค์กรของอุปกรณ์ระบบสารสนเทศตามตารางที่ 3.8 ดังนี้

ตารางที่ 3.8 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
OpenMCU 2	6	5	5	4	5.00
ARM2WAS	6	3	5	4	4.5
Firewall FortiGate 1000D	2	3	5	1	2.75
Aruba 293 0F JL259A (L2 Switch)	2	1	5	1	2.25

จากตารางที่ 3.8 จะเห็นได้ว่าค่าเวกเตอร์ที่ให้ค่าคะแนนในแต่ละหัวข้อนั้นแตกต่างกันไปตามค่าผลกระทบของอุปกรณ์ที่มีผลต่อองค์กรที่มีค่าคะแนนน้อยถึงค่าคะแนนมาก (0-9) อย่างมีนัยสำคัญ ทั้งนี้ค่าดังกล่าวจะคิดเกณฑ์การให้คะแนนตามสมมติฐานการเกิดเหตุการณ์รุนแรงมากที่สุดต่ออุปกรณ์ให้บริการของเครื่องแม่ข่าย กล่าวคือเครื่องแม่ข่ายถูกโจมตีหรือโจรกรรมข้อมูลจนไม่สามารถให้บริการงานตามภารกิจต่างๆ ได้ จะส่งผลกระทบต่อองค์กรมากน้อยเพียงใด จะเห็นได้จากตารางที่ 3.6 ว่าเครื่องแม่ข่าย 2 เครื่องคือ AMC Server และ WEB Server จะมีค่าคะแนนของหัวข้อเวกเตอร์ต่างๆ ค่อนข้างสูง ส่งผลให้ระดับผลกระทบต่อองค์กรมีค่าสูงตามการคำนวณจากสมการที่ (2) ทั้งนี้ นัยสำคัญคือเครื่องแม่ข่ายทั้ง 2 เครื่องนั้น ทำงานอยู่บนเครือข่ายภายนอกให้บริการตลอด 24 ชม. และยังมีข้อมูล (Data) ที่สำคัญอยู่ในระบบถ้าถูกโจรกรรมไปจะส่งผลเสียหาย

ต่อองค์กรอย่างร้ายแรง จึงเป็นที่มาของค่าคะแนนผลกระทบที่สูงในหัวข้อเวกเตอร์ต่างๆ ส่วนเครื่องแม่ข่ายอื่นก็จะไล่เรียงตามลำดับลงมาตามความรุนแรงที่จะส่งผลกระทบต่อองค์กร ในกรณีเกิดเหตุการณ์รุนแรงต่อเครื่องแม่ข่ายนั้นๆ เช่น เครื่องแม่ข่าย OpenMCU 1 เป็นเครื่องแม่ข่ายที่ใช้ในภารกิจการประชุมทางไกล เป็นการใช้ในภารกิจเป็นครั้งๆ ไปไม่ได้ใช้ตลอด 24 ชม. อีกทั้งยังมีเครื่องแม่ข่ายสำรองคือ OpenMCU 2 ดังนั้นเครื่องแม่ข่าย OpenMCU 1 จึงมีค่าคะแนนตามหัวข้อเวกเตอร์ต่ำกว่าเครื่องแม่ข่าย AMC Server และ WEB Server

5.1.3 การจัดลำดับความสำคัญอุปกรณ์สารสนเทศตามผลกระทบต่อองค์กร (Assets Prioritization)

หลังจากการคำนวณค่าผลกระทบของอุปกรณ์ระบบสารสนเทศที่มีต่อองค์กรแล้วขั้นตอนต่อไปคือการจัดกลุ่มและจัดทำแผนการดำเนินการประเมินช่องโหว่ โดยให้ความสำคัญกับอุปกรณ์ที่มีค่าผลกระทบต่อองค์กรในระดับสูงก่อนเป็นอันดับแรก แล้วดำเนินการต่อไประดับที่ต่ำกว่าในลำดับถัดไป ในการศึกษาในครั้งนี้กำหนดวันเวลาในการประเมินช่องโหว่ โดยคำนึงถึงการปฏิบัติงานจริงของอุปกรณ์ระบบสารสนเทศขององค์กร เพื่อไม่ให้ส่งผลกระทบต่อภารกิจขององค์กร โดยใช้เวลาในช่วงที่ไม่มีการปฏิบัติงานตามภารกิจต่างๆ หลังเวลาราชการไปแล้วตามตารางที่ 3.9

ตารางที่ 3.9 แผนการดำเนินการประเมินช่องโหว่

ลำดับ	Assets/System	IP Number	Date	Time
1.	AMC Server	203.xxx.xxx.xxx	03/06/22	10:00 PM
2.	WEB Server	203.xxx.xxx.xxx	06/06/22	8:00 PM
3.	OpenMCU 1	10.0.xxx.xxx	09/06/22	5:00 PM
4.	VPN PPTP	203.xxx.xxx.xxx	12/06/22	8:00 PM
5.	OpenMCU 2	10.0.xxx.xxx	03/09/22	5:00 PM
6.	ARM2WAS	10.0.xxx.xxx	06/09/22	1:00 PM
7.	Firewall FortiGate 1000D	10.0.xxx.xxx	09/09/22	8:00 PM
8.	Aruba 293 0F JL259A (L2 Switch)	10.0.xxx.xxx	12/09/22	8:00 PM

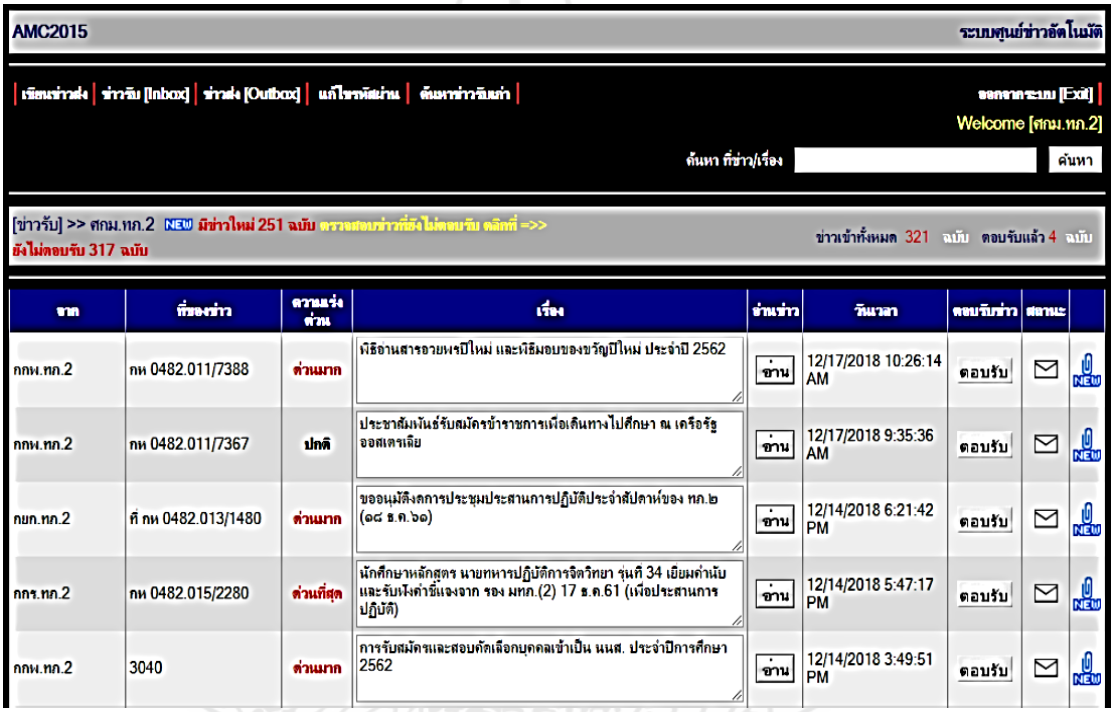
งานวิจัยครั้งนี้ผู้วิจัยได้ร่วมกับผู้ดูแลระบบสารสนเทศขององค์กร (Admin) โดยผู้วิจัยให้ข้อเสนอแนะจากการประเมินผลกระทบต่อระบบสารสนเทศของอุปกรณ์เครื่องแม่ข่ายตามผลการประเมิน เป็นการตัดสินใจร่วมกันเลือกอุปกรณ์ในการทดลองตามขั้นตอนงานวิจัยโดยเลือกอุปกรณ์สารสนเทศที่มีลำดับผลกระทบต่อองค์กรมากที่สุด 4 ลำดับ และให้ผู้ดูแลระบบได้เลือกห้วงเวลาเพื่อให้เหมาะสมและสอดคล้องกับห้วงเวลาในการดำเนินการทดลองของผู้วิจัยและไม่ส่งผลกระทบต่อภารกิจของทางราชการ ดังตารางที่ 3.10

ตารางที่ 3.10 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

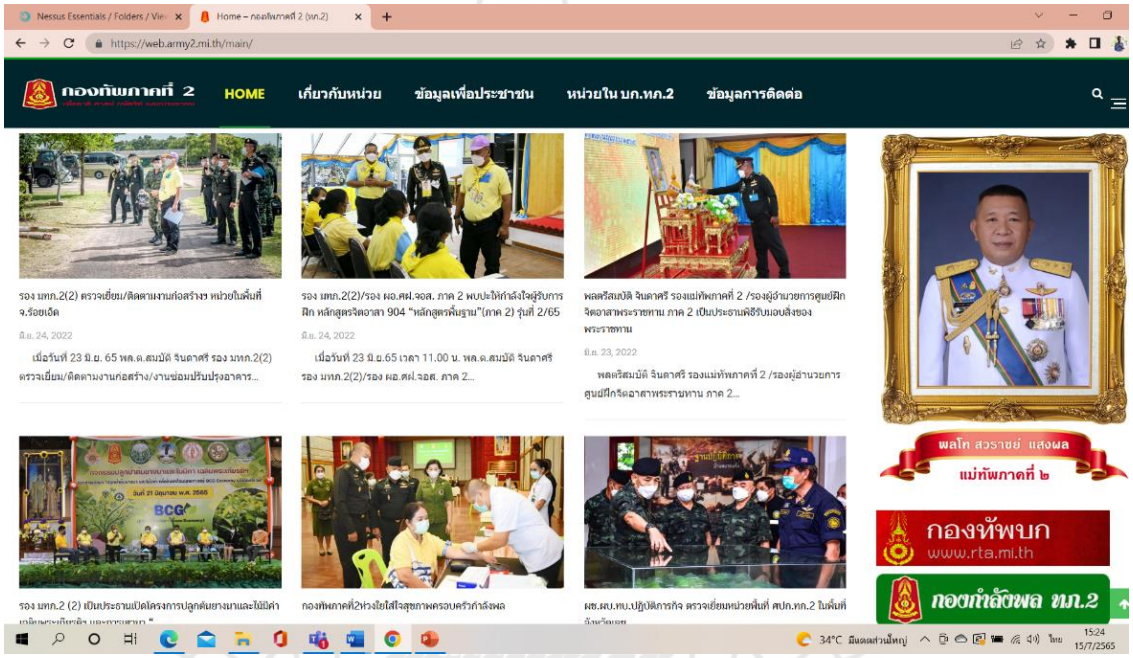
สำหรับอุปกรณ์สารสนเทศที่เข้ารับการประเมินช่องโหว่มีลำดับความสำคัญและรายละเอียดคุณลักษณะทางเทคนิค และภารกิจงานที่ให้บริการดังนี้

1) AMC Server ระบบศูนย์ข่าวอัตโนมัติ กองทัพภาคที่ 2 (Automatic Message Center : AMC) มีลำดับความสำคัญในการเข้ารับการประเมินช่องโหว่เป็นลำดับที่ 1 โดยมีค่าลำดับผลกระทบต่อองค์กรอยู่ในระดับที่สูงมีค่าคะแนนอยู่ที่ 8.00 เครื่องแม่ข่ายเครื่องนี้มีข้อมูลที่สำคัญเพราะเป็นการส่งข่าวสารทางราชการมีหน่วยใช้งานอยู่ประมาณ 200 กว่าหน่วยงาน หากมีเหตุการณ์รุนแรงต่อเครื่องแม่ข่าย AMC นี้จะส่งผลกระทบเสียหายอย่างร้ายแรง ส่งผลถึงภาพลักษณ์ขององค์กรทำให้เกิดความเสียหาย คุณลักษณะทางเทคนิค OS: Windows Server / IIS เป็นระบบที่ให้บริการ ในรูปแบบ Web Sever ใช้ในภารกิจการรับส่งข่าวผ่านทางเครือข่ายภายใน และเครือข่าย Internet เป็นการพัฒนาซอฟต์แวร์ขึ้นมาใช้เองลักษณะคล้ายการรับส่ง E-Mail โดยทั่วไป แต่จะใช้ได้เฉพาะหน่วยงานภายในองค์กรเท่านั้น เวลาใช้งานตลอด 24 ชม. รูปแบบการให้บริการตามภาพที่ 3.6



ภาพที่ 3.6 ระบบศูนย์ข่าวอัตโนมัติ กองทัพภาคที่ 2 (Automatic Message Center : AMC)

2) WEB Server คุณลักษณะทางเทคนิค OS: Linux Kernel 2.6 / Apache เป็นระบบที่ให้บริการเว็บไซต์ของกองทัพภาคที่ 2 เป็นแหล่งนำเสนอข้อมูลในด้านต่างๆ ของกองทัพภาคที่ 2 รวมทั้งข้อมูลเว็บไซต์ของหน่วยงานภายใต้การบังคับบัญชาของกองทัพภาคที่ 2 ที่ฝากไว้กับเครื่องแม่ข่ายเครื่องนี้ นอกจากนั้นยังมีข้อมูล back-end ที่ใช้ภายในรวมอยู่ด้วย ซึ่งจะส่งผลเสียหายหากถูกโจรกรรมข้อมูลไปได้ และมีผลเสียต่อภาพลักษณ์ด้วยเช่นกัน แต่อย่างไรก็ดีข้อมูลดังกล่าวนี้ยังมีความสำคัญน้อยกว่าข้อมูลที่อยู่ในเครื่องแม่ข่าย AMC โดยค่าคะแนนของเครื่องแม่ข่ายเว็บไซต์ (WEB Server) มีค่า 7.25 อยู่ในระดับที่สูงแต่ก็ยังน้อยกว่า AMC Server โดยจะอยู่ในลำดับที่ 2 ในการเข้ารับการประเมินช่องโหว่ รายละเอียดตามภาพที่ 3.7



ภาพที่ 3.7 เว็บไซต์กองทัพภาคที่ 2

ที่มา : https://web.army2.mi.th/

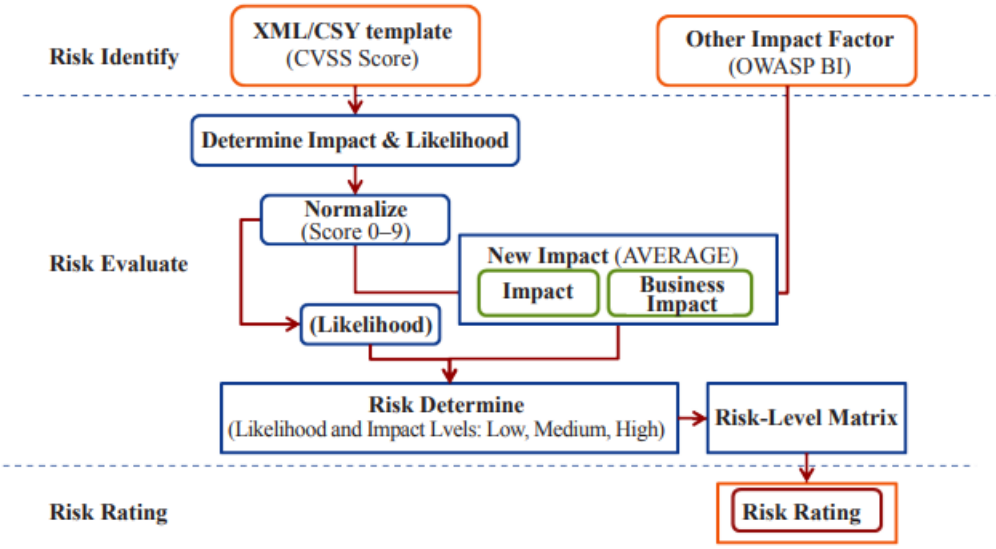
3) OpenMCU 1 (Open Multipoint Control Unit) เป็นเครื่องแม่ข่ายที่ใช้ในภารกิจประชุมทางไกลผ่านจอภาพ มีลำดับในการเข้ารับการประเมินช่องโหว่อยู่ในลำดับที่ 3 ด้วยข้อมูลที่มีทั้งภาพและเสียง ถือว่าเป็นข้อมูลที่สำคัญ แต่อย่างไรก็ดีระดับผลกระทบต่อองค์กรก็จะต่ำกว่าเครื่องแม่ข่ายในลำดับ 1 และ 2 เนื่องจากระบบจะใช้เครือข่ายภายใน โดยเป็นโครงข่ายกองทัพบกเป็นส่วนใหญ่ ยกเว้นหน่วยที่โครงข่ายกองทัพบกยังไม่สามารถใช้ได้ก็จะเข้าระบบด้วยเครือข่ายภายนอกเข้ามา จึงยังถือว่ามีระดับผลกระทบต่อองค์กรในระดับที่สูง โดยมีค่าคะแนนระดับผลกระทบอยู่ที่ 7.00 โดยหัวข้อเวกเตอร์ที่ค่าคะแนนสูงก็คือเรื่องภาพลักษณ์ขององค์กร คุณลักษณะทางเทคนิค OS: Linux Kernel 3.0 on Ubuntu 12.04 (precise) เป็นระบบที่ให้บริการเว็บไซต์ประชุมทางไกลผ่านจอภาพผ่านโครงข่ายภายในของกองทัพบก E-Army รองรับการเชื่อมเครือข่ายอินเทอร์เน็ต โดยผ่าน VPN เป็นแอปพลิเคชัน Open source ที่กองทัพภาคที่ 2 พัฒนาขึ้นมาเอง รายละเอียดตามภาพที่ 3.8

ภาพที่ 3.8 ระบบการประชุมทางไกลผ่านจอภาพ กองทัพภาคที่ 2

4) VPN PPTP (VPN Point-to-Point Tunneling Protocol) คุณลักษณะทางเทคนิค OS: Linux_kernel:2.6.32 เป็นระบบที่ให้บริการเชื่อมต่อระยะไกลจากหน่วยงานที่ระบบโครงข่ายภายในกองทัพบกไปไม่ถึง ให้ผ่านเครือข่าย Internet เข้ามาเพื่อใช้งานเว็บไซต์ประชุมทางไกลผ่านจอภาพ เป็นเครื่องแม่ข่ายที่ต่อเชื่อมกับเครือข่ายภายนอกจึงเป็นเครื่องแม่ข่ายที่มีค่าผลกระทบต่อองค์กรที่มีโอกาสที่จะถูกโจรกรรมอยู่พอสมควรแต่ไม่มีค่าคะแนนสูงเท่าเครื่องแม่ข่ายที่ผ่านมาเนื่องจากเครื่องแม่ข่าย VPN PPTP เปิดพอร์ตใช้งานไม่มากนัก จึงมีค่าคะแนนอยู่ในลำดับที่ 4 ของการเข้ารับการประเมินช่องโหว่ โดยมีค่าคะแนนผลกระทบต่อองค์กรอยู่ที่ 6.25

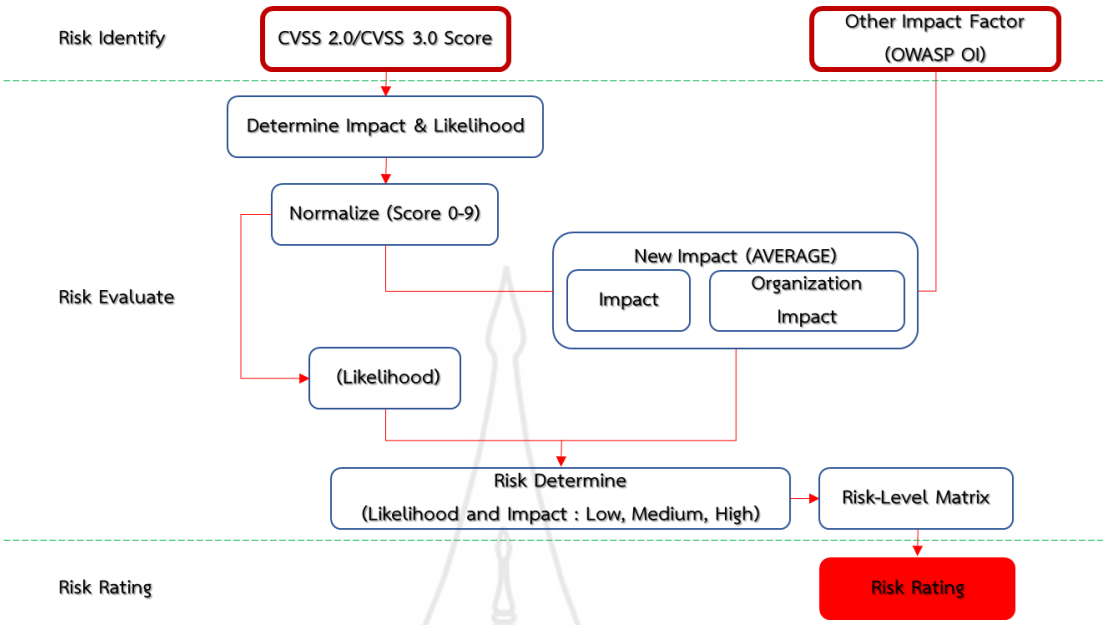
5.2 การประเมิน (Assessment)

ขั้นตอนการประเมินความเสี่ยงการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของกองบัญชาการกองทัพภาคที่ 2 แบ่งเป็น 3 ขั้นตอนคือ 1) การระบุความเสี่ยง 2) การประเมินค่าระดับความเสี่ยง 3) การให้คะแนนระดับความสำคัญของความเสี่ยง แสดงในภาพที่ 3.9



ภาพที่ 3.9 ระเบียบวิธีการประเมินความเสี่ยงช่องโหว่ที่ประเมินพบ (Risk Assess Method)
ที่มา : สุรทศ ไตรติลานันท์ และ สุรพล รวยสูงเนิน (2559) The Journal of KMUTNB., Vol. 26, No. 1, Jan.–Apr. 2016

จากระเบียบวิธีการประเมินความเสี่ยงช่องโหว่ที่ประเมินพบ (Risk Assess Method) ตามภาพที่ 3.9 นั้นผู้วิจัยได้ปรับเปลี่ยนบางขั้นตอนเพื่อให้เหมาะสมกับงานวิจัยของผู้วิจัย กล่าวคือ ได้เพิ่ม CVSS 3.0 ค่าคะแนนความรุนแรงระดับ "สูง" ซึ่งผู้วิจัยได้ใช้ในการหาค่าระดับโอกาสที่จะเกิดและผลกระทบของช่องโหว่ที่ประเมินพบ เนื่องจากในงานวิจัยของ สุรทศ ไตรติลานันท์ และ สุรพล รวยสูงเนิน (2559) กรณีศึกษา: โมเดลทางด้านเทคนิคสำหรับวิธีการประเมินความเสี่ยง ความมั่นคงปลอดภัยในระบบสารสนเทศสำหรับโรงพยาบาล นั้นมีเฉพาะ CVSS 2.0 เท่านั้น นอกจากนั้นผู้วิจัยยังได้ปรับค่า Business Impact มาเป็นค่า Organization Impact โดย ได้ใช้ค่าจาก ปัจจัยผลกระทบทางเทคนิค (Technical Impact Factors) OWASP Testing Guide,(2008) เป็นค่าหลักในการประเมิน ร่วมกับ ปัจจัยกระทบต่อธุรกิจ (Business Impact Factors) OWASP Testing Guide,(2008) บางส่วน เพื่อให้สอดคล้องกับองค์กรของผู้วิจัย ซึ่งไม่ได้เป็นองค์กรเกี่ยวกับด้านธุรกิจ จึงได้เป็นขั้นตอนที่สอดคล้องกับบริบทขององค์กรของผู้วิจัยดังภาพที่ 3.10

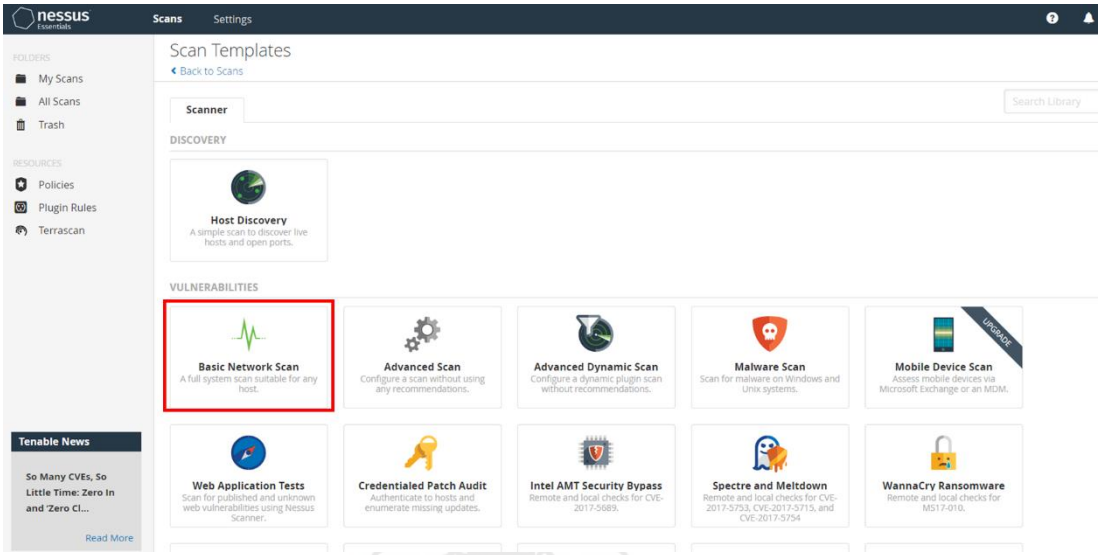


ภาพที่ 3.10 ระเบียบวิธีการประเมินความเสี่ยงช่องโหว่ที่ประเมินพบ การปรับแก้ไขระเบียบวิธีการประเมินความเสี่ยง (Risk Assess Method Edit)

5.2.1 การประเมินช่องโหว่ (Vulnerability Assessment) คือขั้นตอนการระบุ (Risk Identify) ตามภาพที่ 3.10 เป็นการค้นหาช่องโหว่ระบบสารสนเทศ หรือการทำ **Vulnerability Scan** นั่นเอง โดยงานวิจัยนี้ใช้เครื่องมือช่วยตรวจสอบประเมินช่องโหว่อัตโนมัติ งานวิจัยนี้เลือกใช้เครื่องมือตรวจสอบประเมินช่องโหว่ที่อัตโนมัติคือ Nessus ซึ่งรองรับ CVSS SCORE และใช้การแสดงผลลัพธ์ในรูปแบบ XML Format ทำการสำเนาหรือนำเข้า Excel Data Sheet หรือ Access Data Table หรือฐานข้อมูลอื่นๆ ที่สามารถคำนวณหรือประมวลผลได้และเพื่อให้เกิดความเชื่อถือได้ในการดำเนินการประเมินช่องโหว่ จึงได้เพิ่มเครื่องมือในการประเมินช่องโหว่เพื่อเป็นการเปรียบเทียบเครื่องมือดังกล่าวคือ Nexpose

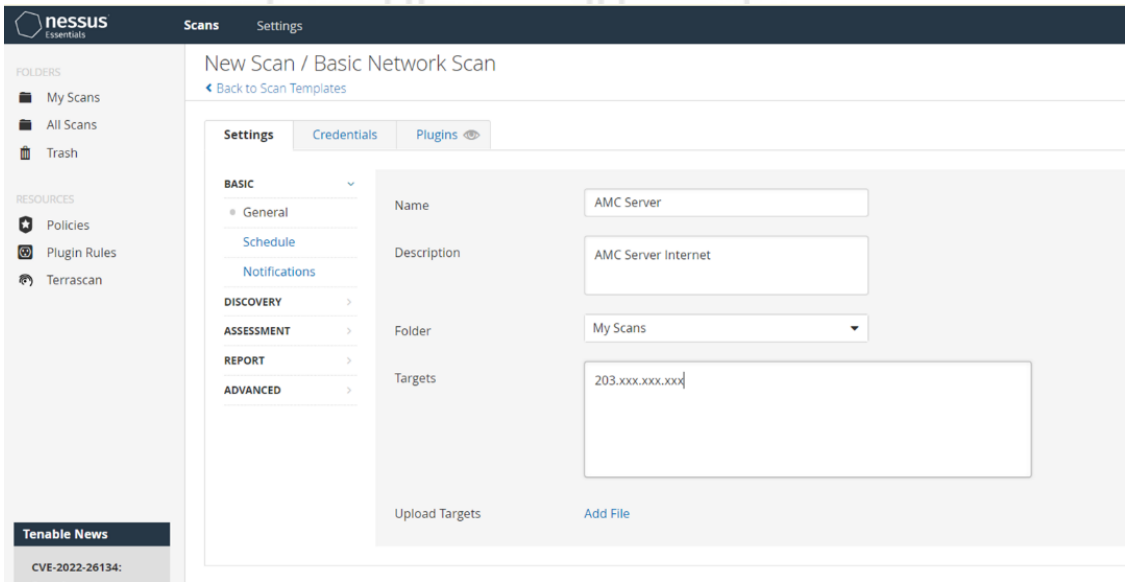
1) Nessus เป็นเครื่องมือใช้ในการประเมินช่องโหว่ของบริษัท Tenable Network Security ซึ่งงานวิจัยนี้ใช้ Nessus เวอร์ชัน essentials เป็นรุ่นที่ให้ผู้ที่สนใจหรือนักศึกษาได้นำมาใช้โดยไม่เสียค่าใช้จ่าย แต่มีข้อจำกัดในการใช้งานเช่น Scan สูงสุด 16 หมายเลขไอพี ซึ่งสามารถศึกษาเพิ่มเติมได้ที่ https://www.tenable.com/products/nessus/nessus-essentials มีขั้นตอนในการประเมินช่องโหว่ดังนี้

1.1) สร้างการประเมินช่องโหว่ โดยการเลือกรูปแบบการประเมินช่องโหว่เป็น Basic Network Scan เพื่อประเมินช่องโหว่ตามรูปที่ 3.11 หน้าจอการเลือกรูปแบบการประเมินช่องโหว่



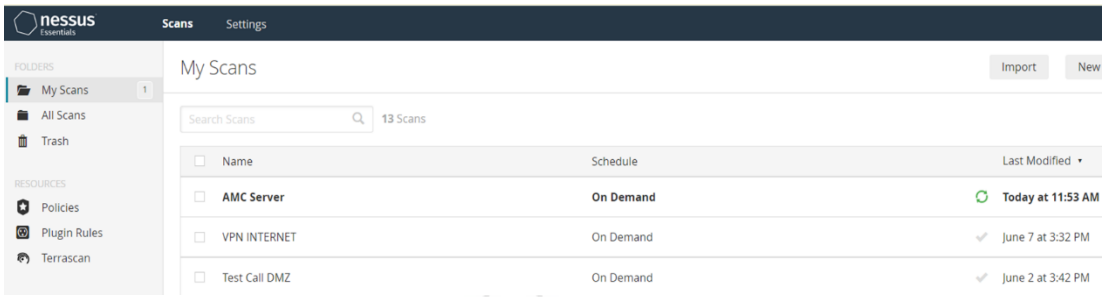
ภาพที่ 3.11 หน้าจอการเลือกรูปแบบการประเมินช่องโหว่ของ Nessus

1.2) กำหนดอุปกรณ์ปลายทาง ตั้งชื่อระบบงานในช่อง Name และกำหนดอุปกรณ์ที่ใช้ในการดำเนินการลงในช่อง Target ตามรูปที่ 3.12 หน้าจอการตั้งค่าการประเมินช่องโหว่



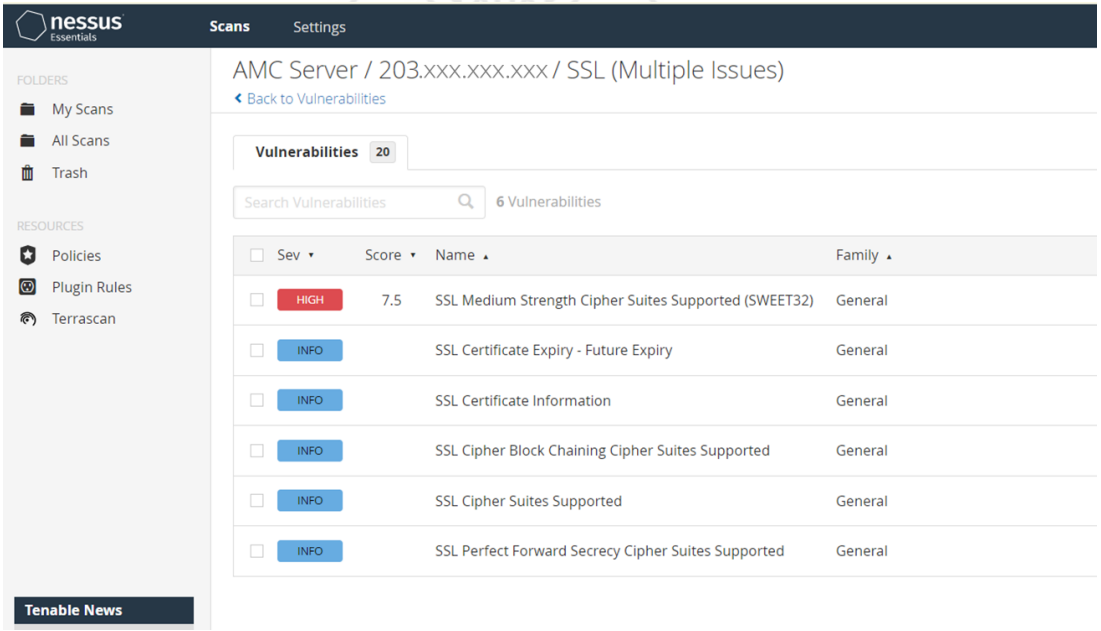
ภาพที่ 3.12 หน้าจอการตั้งค่าการประเมินช่องโหว่ของ Nessus

1.3) ดำเนินการประเมินช่องโหว่ ภาพที่ 3.13 การทำงานของเครื่องมือประเมินช่องโหว่ ซึ่งในขั้นตอนนี้ระบบจะทำการสแกนช่องโหว่ระบบสารสนเทศที่เราได้กำหนดอุปกรณ์ปลายทางเอาไว้



ภาพที่ 3.13 การทำงานของเครื่องมือประเมินช่องโหว่ของ Nessus

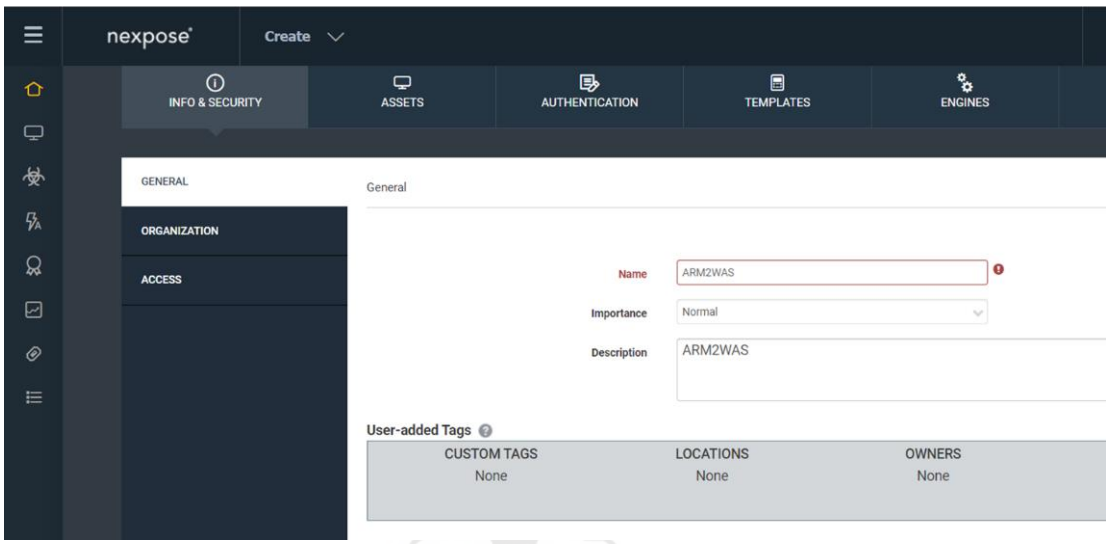
1.4) ผลที่แสดงจากการสแกนช่องโหว่ที่ประเมินพบ ดังภาพที่ 3.14 การทำงานของเครื่องมือประเมินช่องโหว่ ซึ่งในขั้นตอนนี้ระบบจะแสดงผลการสแกนช่องโหว่ระบบสารสนเทศที่พบของอุปกรณ์ปลายทางที่ทำการสแกน



ภาพที่ 3.14 การแสดงของการสแกนช่องโหว่ที่ประเมินพบของ Nessus

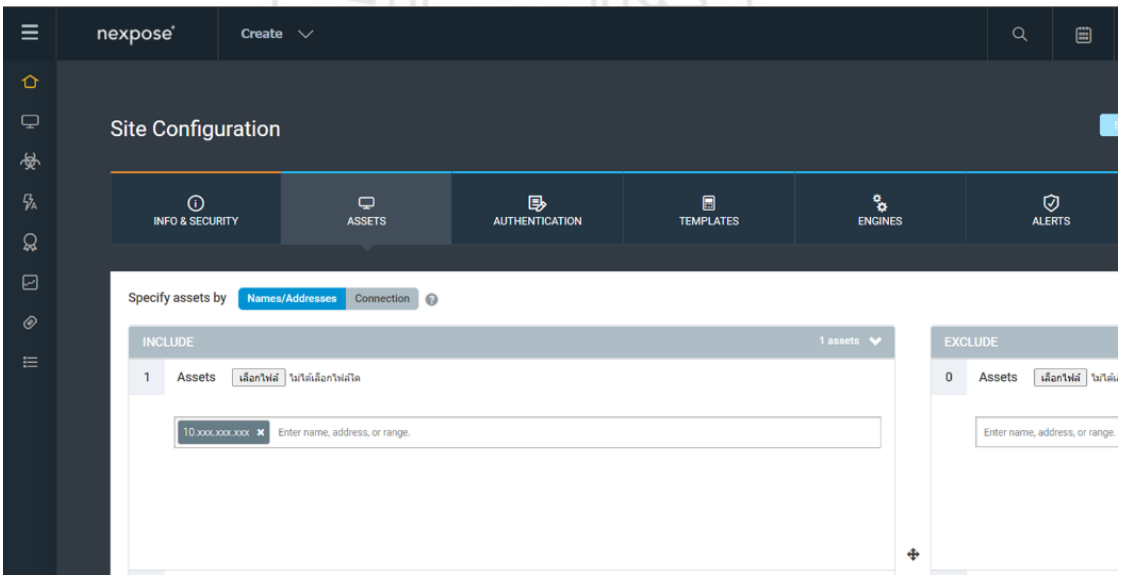
2) Nexpose เป็นเครื่องมือใช้ในการเมินช่องโหว่ของบริษัท Rapid7 ซึ่งสามารถศึกษาเพิ่มเติมได้ที่ที่ https://docs.rapid7.com/nexpose/ เวอร์ชันที่ใช้งาน Nexpose Community Edition มีขั้นตอนในการประเมินช่องโหว่เทคโนโลยีสารสนเทศ ดังนี้

2.1) สร้างการประเมินช่องโหว่ กำหนดชื่อของระบบงานที่ต้องการประเมินช่องโหว่ดังภาพที่ 3.15 หน้าจอการตั้งชื่อระบบงานของ Nexpose



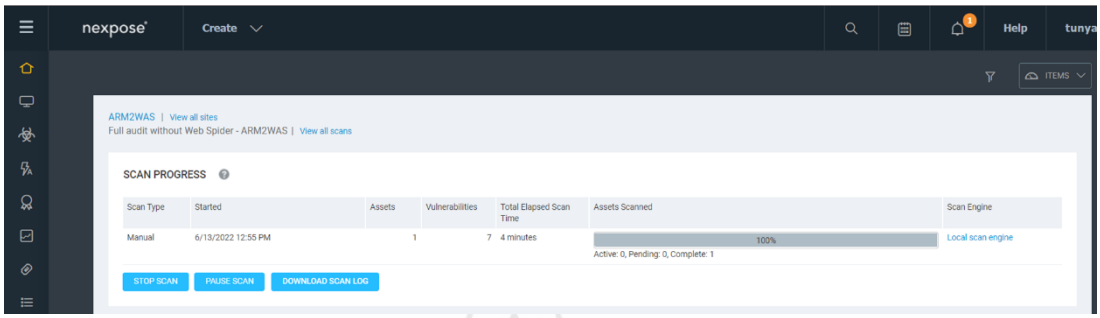
ภาพที่ 3.15 หน้าจอการตั้งชื่อระบบงานของ Nexpose

2.2) กำหนดอุปกรณ์เพื่อประเมินช่องโหว่ตามรูปที่ 3.16 หน้าจอการเลือกรูปแบบการประเมินช่องโหว่ของ Nexpose จากนั้นกด Save and Scan ที่ชื่อระบบงานที่ตั้งไว้



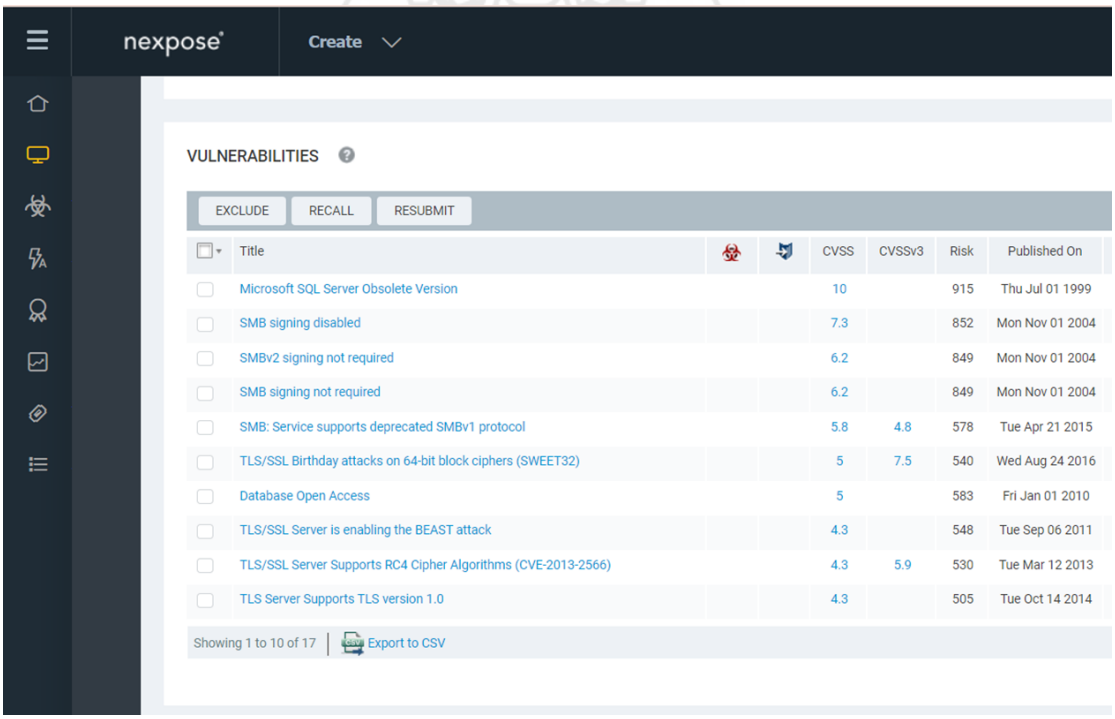
ภาพที่ 3.16 หน้าจอการเลือกรูปแบบการประเมินช่องโหว่ของ Nexpose

2.3) ดำเนินการประเมินช่องโหว่ ภาพที่ 3.17 การทำงานของเครื่องมือประเมินช่องโหว่ ซึ่งในขั้นตอนนี้ระบบจะทำการสแกนช่องโหว่ระบบสารสนเทศที่เราได้กำหนดอุปกรณ์ปลายทางเอาไว้



ภาพที่ 3.17 การทำงานของเครื่องมือประเมินช่องโหว่ของ Nexpose

2.4) ผลที่แสดงจากการสแกนช่องโหว่ที่ประเมินพบ ดังภาพที่ 3.18 การทำงานของเครื่องมือประเมินช่องโหว่ ซึ่งในขั้นตอนนี้ระบบจะแสดงผลการสแกนช่องโหว่ระบบสารสนเทศที่พบของอุปกรณ์ปลายทางที่ทำการสแกน



ภาพที่ 3.18 การแสดงผลการสแกนช่องโหว่ที่ประเมินพบของ Nexpose

2.5) เหตุผลที่ผู้วิจัยเลือกเครื่องมือประเมินช่องโหว่ หรือเครื่องมือสแกนช่องโหว่ (Vulnerability Assessment Tool) Nessus และ Nexpose ซึ่งเป็นเครื่องมือที่ใช้ซอฟต์แวร์ในรุ่นที่แจกจ่ายให้ใช้งานโดยไม่มีค่าลิขสิทธิ์ (Freeware) มีคุณลักษณะที่สามารถนำมาดำเนินการวิจัยในขั้นตอนการทดลองได้อย่างมีประสิทธิภาพ กล่าวคือ มีชุดข้อมูลที่ใช้ในการประเมินความเสี่ยงช่องโหว่ของอุปกรณ์สารสนเทศ หรือเครื่องแม่ข่ายที่ส่งผลกระทบต่อภารกิจขององค์กร เช่น ค่า Common Vulnerability Scoring System : CVSS ซึ่งใช้ในการคำนวณหาระดับความรุนแรงของช่องโหว่ ข้อมูล Common Vulnerability Exposure : CVE เป็นข้อมูลของช่องโหว่ซึ่งอธิบายรายละเอียดของช่องโหว่ มีการจัดเก็บเป็นฐานข้อมูลช่องโหว่ที่ยอมรับ เก็บเป็นชุดหมายเลขและมีการใช้เป็นดัชนีอ้างอิงในการนำไปใช้แก้ไขช่องโหว่ที่ค้นพบ และเครื่องมือประเมินช่องโหว่ทั้งสองเครื่องมือยังมีฐานข้อมูลรายละเอียดช่องโหว่ของตัวเครื่องมือเองด้วยจึงสะดวกในการค้นหาข้อมูลช่องโหว่ ซึ่งมีประสิทธิภาพเพียงพอสำหรับงานวิจัยนี้ เนื่องจากงานวิจัยนี้มุ่งเน้นในการพัฒนากรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กรเป็นหลัก

จากงานวิจัยของ สุรทศ ไตรติลานันท์ และ สุรพล รวยสูงเนิน (2559) กรณีศึกษา: โมเดลทางด้านเทคนิคสำหรับวิธีการประเมินความเสี่ยง ความมั่นคงปลอดภัยในระบบสารสนเทศสำหรับโรงพยาบาล ได้นำเสนอข้อมูลจาก ศูนย์วิเคราะห์เทคโนโลยีการรับประกันข้อมูล (The Information Assurance Technology Analysis Center : IATAC) เป็นข้อมูลรายงานรับรองเครื่องมือสนับสนุนการตรวจสอบหาช่องโหว่ ซึ่งแต่ละเครื่องมือมีคุณสมบัติแตกต่างกันขึ้นอยู่กับขอบเขตของการทดสอบความรู้ความเชี่ยวชาญของผู้ทำการทดสอบ โดยแบ่งเป็น 7 ประเภทสรุปคุณลักษณะได้ตามตารางที่ 3.11

ตารางที่ 3.11 รายละเอียดเปรียบเทียบคุณลักษณะข้อมูลของเครื่องมือประเมินช่องโหว่

ลักษณะ	เครื่องมือ	เป้าหมาย	ลิขสิทธิ์	มาตรฐาน
Network Scanner	eEye Retina	Network, OS, Web App/Services, DB	Commercial	SCAP, OVAL, CVE, CVSS
	GFI LANguard	UNIX, Windows	Commercial/Freeware	OVAL, CVE
Host Scanner	Assuria Auditor/ Auditor RA	Windows, UNIX, Linux	Shareware	CVE, CVSS
	NileSOFT Secuguard SSE		Commercial	CVE

ตารางที่ 3.11 (ต่อ)

ลักษณะ	เครื่องมือ	เป้าหมาย	ลิขสิทธิ์	มาตรฐาน
DB Scanner	Imperva Scuba	Oracle, DB2, SQL Server, Sybase	Freeware	NA
	Safety-Lab Shadow	Oracle, DB2, SQL Server, Sybase, MySQL, SAP DB	Commercial	
Web Application Scanner	Acunetix	NA	Commercial	NA
	Burp Suite	HTTP/HTTPS, Web Server	Open Source	
	Nikto			
Multi Scanner	Open VAS	Network, Web App	Open Source	NA
	Symantec Risk Automation suite	Network Devices, Host Oss, DB, Network App	Commercial	SCAP, OVAL, CVE, CVSS
	Nessus	Network, Windows, Unix, Linux, SQL DB, Web server	Commercial/Freeware	CVE,CVSS
	Nexpose	Networks, operating systems, databases, Web applications	Commercial/Freeware	CVE,CVSS
Automated Penetration Test Tools	CANVAS	All Common Platform and App	Commercial	NA
	Metasploit	Web App, Network, DB Server		CVE
Vulnerability Scan Consolidators	Prolific Solutions pro VM Auditor	NA	Commercial	NA
	ASG			SCAP, OVAL, CVE, CVSS
	Skybox Risk Control	Systems, Devices		CVE

ที่มา : Information Assurance Tools Report–Vulnerability Assessment, Information Assurance Technology Analysis Center (IATAC), 6th ed., May 2, 2011.

จากตารางที่ 3.11 จะเห็นได้ว่าเครื่องมือประเมินช่องโหว่ Nessus และ Nexpose นอกจากจะมีข้อดีของ CVE / CVSS / ฐานข้อมูลช่องโหว่ของเครื่องเองแล้ว ข้อดีอีกประการคือ เป็น

เครื่องมือที่มีลักษณะทำงานเป็นการประเมินช่องโหว่ที่หลากหลายเป้าหมาย (Multi Scanner) คือทำการประเมินได้ทั้ง ระบบเครือข่าย, ระบบปฏิบัติการ, ฐานข้อมูล และ เว็บเซิร์ฟเวอร์ จึงเป็นเครื่องมือที่เหมาะสมที่นำมาใช้ในงานวิจัยนี้ โดยเฉพาะกับองค์กรที่มีเครื่องแม่ข่ายที่ให้บริการในหลายรูปแบบ

3) ผลการดำเนินการประเมินช่องโหว่ ของเครื่องมือ Nessus และ Nexpose หลังจากดำเนินการประเมินช่องโหว่แล้วพบช่องโหว่ดังนี้

3.1) ผลการดำเนินการประเมินช่องโหว่ของเครื่องมือ Nessus ตามตารางที่ 3.12

ตารางที่ 3.12 ผลการดำเนินการประเมินช่องโหว่ Nessus

ลำดับ	ชื่อเครื่อง	หมายเลขไอพี	High	Medium	Low
1.	AMC Server	203.xxx.xxx.xxx	1	2	0
2.	Web Server	203.xxx.xxx.xxx	0	3	0
3.	OpenMCU 1	10.0.xxx.xxx	1	2	3
4.	VPN PPTP	10.0.xxx.xxx	0	3	0

3.2) ผลการดำเนินการประเมินช่องโหว่ของเครื่องมือ Nexpose ตามตารางที่ 3.13

ตารางที่ 3.13 ผลการดำเนินการประเมินช่องโหว่ Nexpose

ลำดับ	ชื่อเครื่อง	หมายเลขไอพี	High	Medium	Low
1.	AMC Server	203.xxx.xxx.xxx	1	4	3
2.	Web Server	203.xxx.xxx.xxx	2	3	2
3.	OpenMCU 1	10.0.xxx.xxx	1	4	1
4.	VPN PPTP	10.0.xxx.xxx	1	2	3

3.3) ผลการดำเนินงานประเมินช่องโหว่ระบบเทคโนโลยีสารสนเทศที่ได้จากเครื่องมือทั้ง 2 เครื่องมือสามารถสรุปรวมช่องโหว่อุปกรณ์ตามขอบเขตระบบงานหลักที่มีผลกระทบกับองค์กร ตามตารางที่ 3.14 สรุปผลการประเมินช่องโหว่

ตารางที่ 3.14 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	10.0.xxx.xxx	1	4	3

จากตารางที่ 3.14 ผลการดำเนินงานประเมินช่องโหว่ระบบเทคโนโลยีสารสนเทศที่ได้จากเครื่องมือทั้ง 2 เครื่องมือ ในการรวมช่องโหว่อุปกรณ์หมายถึงตัดช่องโหว่ที่ซ้ำกันโดยนับรวมเป็นช่องโหว่เดียว เช่น การประเมินช่องโหว่ของเครื่องแม่ข่าย AMC จะมีผลการประเมินช่องโหว่ของแต่ละเครื่องมือดังนี้

1) ผลการประเมินช่องโหว่ของอุปกรณ์ AMC Server โดยเครื่องมือ Nessus พบช่องโหว่ จำนวน 3 ช่องโหว่ ดังนี้

1.1) ช่องโหว่ SSL Medium Strength Cipher Suites Supported (SWEET32) Base score (ระดับสูง)

1.2) ช่องโหว่ TLS Version 1.0 Protocol Detection Base score (ระดับกลาง)

1.3) ช่องโหว่ TLS Version 1.1 Protocol Deprecated Base score (ระดับกลาง)

2) ผลการประเมินช่องโหว่ของอุปกรณ์ AMC Server โดยเครื่องมือ Nexpose พบช่องโหว่ จำนวน 8 ช่องโหว่ดังนี้

2.1) ช่องโหว่ TLS/SSL Birthday attacks on 640- bit block ciphers (SWEET32) : Base score (ระดับสูง)

2.2) ช่องโหว่ DNS server allows cache snooping : Base score (ระดับกลาง)

2.3) ช่องโหว่ Nameserver Processes Recursive Queries : Base score (ระดับกลาง)

2.4) ช่องโหว่ TLS/SSL Server is enabling the BEAST attack : Base score (ระดับกลาง)

2.5) ช่องโหว่ TLS Server Supports TLS version 1.0 : Base score (ระดับกลาง)

2.6) ช่องโหว่ HTTP OPTIONS Method Enabled : Base score (ระดับต่ำ)

2.7) ช่องโหว่ TLS Server Supports TLS version 1.1 : Base score (ระดับต่ำ)

2.8) ช่องโหว่ TLS/SSL Server Supports The Use of Static Key Ciphers : Base score (ระดับต่ำ)

3) ผลการประเมินช่องโหว่ของอุปกรณ์ AMC Server โดยเครื่องมือทั้ง 2 เครื่องมือในข้อ *1)* และ *2)* พบช่องโหว่รวมทั้งหมด จำนวน 11 ช่องโหว่ แต่จากตารางที่ 3.12 พบว่าจำนวนช่องโหว่ของอุปกรณ์เครื่องแม่ข่าย AMC นั้น มีจำนวนช่องโหว่ 8 ช่องโหว่ สามารถอธิบายได้ดังนี้

3.1) นับจำนวนช่องโหว่ที่เหมือนกันหรือซ้ำกันให้เป็นช่องโหว่เพียงช่องโหว่เดียว จากหัวข้อที่ *1)* และ *2)* จะมีช่องโหว่ที่เหมือนกันดังนี้

3.1.1) ช่องโหว่หัวข้อ *1.1)* และ *2.1)* เป็นช่องโหว่ SWEET32 และ มีระดับความรุนแรง สูง เช่นเดียวกัน โดยได้เลือกช่องโหว่หัวข้อ *1.1)* ในการนับจำนวนช่องโหว่เพียงช่องโหว่เดียว

3.1.2) ช่องโหว่หัวข้อ *1.2)* และ *2.5)* เป็นช่องโหว่ TLS version 1.0 และมีระดับความรุนแรง ปานกลาง เช่นเดียวกัน โดยได้เลือกช่องโหว่หัวข้อ *1.2)* ในการนับจำนวนช่องโหว่เพียงช่องโหว่เดียว

3.1.3) ช่องโหว่หัวข้อ *1.3)* และ *2.7)* เป็นช่องโหว่ TLS version 1.1 เช่นเดียวกัน แต่มีระดับความรุนแรงที่แตกต่างกัน ช่องโหว่หัวข้อ *1.3)* จะมีระดับความรุนแรง ปาน-กลาง ส่วนช่องโหว่หัวข้อ *2.7)* จะมีความรุนแรงระดับ ต่ำ โดยได้เลือกช่องโหว่หัวข้อ *1.3)* ในการนับจำนวนช่องโหว่เพียงช่องโหว่เดียว

3.2) จากเหตุผลในข้อที่ *3.1)* นั้นจะได้ผลรวมโดยการคัดช่องโหว่ที่เหมือนหรือซ้ำกันออก จากผลรวมของช่องโหว่ที่ใช้เครื่องมือทั้ง 2 เครื่องมือในการประเมินช่องโหว่ของอุปกรณ์เครื่องแม่ข่าย AMC ที่มีผลรวมเท่ากับ 11 ช่องโหว่ และจากการนับจำนวนช่องโหว่ที่เหมือนกันหรือซ้ำกันให้เป็นช่องโหว่เพียงช่องโหว่เดียวจึงได้ผลดังตารางที่ 3.12 โดยผลรวมช่องโหว่ของอุปกรณ์เครื่องแม่ข่าย AMC จะมีจำนวนช่องโหว่ 8 ช่องโหว่ โดยมี ระดับความรุนแรงสูง 1 ช่องโหว่ ระดับความรุนแรงปานกลาง 5 ช่องโหว่ และระดับความรุนแรงต่ำ 2 ช่องโหว่

3.3) ตัวอย่างรูปแบบรายละเอียดช่องโหว่จากการประเมินช่องโหว่ระบบสารสนเทศขององค์กรมีรายละเอียดตามตารางที่ 3.15 ดังนี้

ตารางที่ 3.15 ตัวอย่างรูปแบบรายละเอียดช่องโหว่จากการประเมินช่องโหว่ระบบสารสนเทศขององค์กร

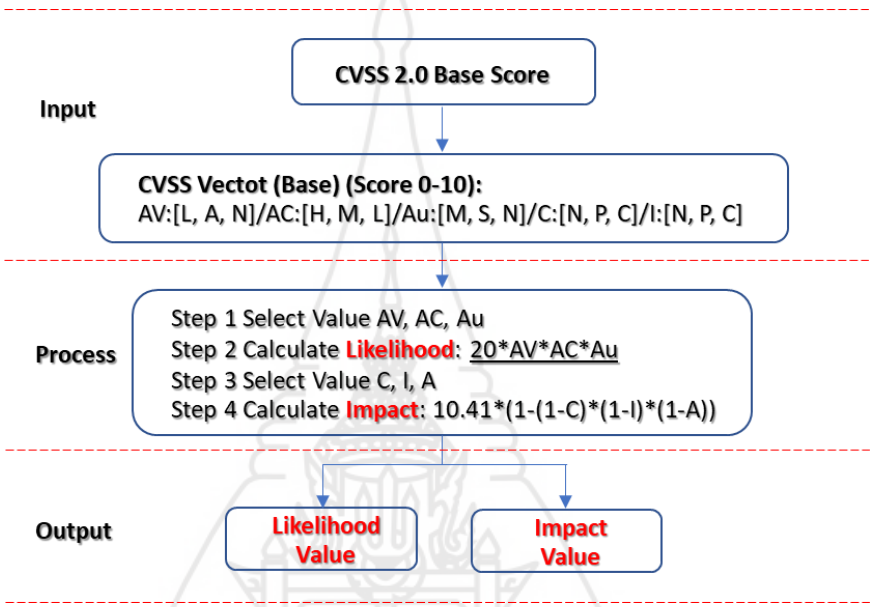
ลำดับ	ชื่อช่องโหว่	รายละเอียด	ข้อมูลอ้างอิง	อุปกรณ์สารสนเทศ	ข้อมูลความเสี่ยง CVSS	Base Score
1.	SSL Medium Strength Cipher Suites Supported (SWEET32)	โฮสต์ระยะไกลสนับสนุนการใช้การเข้ารหัส SSL ที่มีการเข้ารหัสระดับกลาง ถือว่ามีความรุนแรงปานกลางเป็นการเข้ารหัสที่ใช้ความยาวของกุญแจ (มากกว่า 64 บิต และน้อยกว่า 112 บิต key, or 3DES)	1. tenable plugins #42873 2. CVE: CVE-2016-2183	AMC Server Por :443 / tcp / www	CVSS v3.0 Base Score 7.5 CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N CVSS v2.0 Base Score: 5.0 CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N	High
2.	Nameserver Processes Recursive Queries	การอนุญาตให้ Nameserver ประมวลผลการสืบค้นแบบเรียกซ้ำที่มาจากระบบอื่นๆ ในบางสถานการณ์ อาจถูกผู้โจมตีดำเนินการโจมตีแคชซึ่งทำให้เกิดการหยุดให้บริการของเครื่องแม่ข่ายได้	1. dns-processes-recursive-queries	AMC Server Port: 53 / UDP	CVSS v2.0 Base Score 5 CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P	Medium

ตารางที่ 3.15 (ต่อ)

ลำดับ	ชื่อช่องโหว่	รายละเอียด	ข้อมูลอ้างอิง	อุปกรณ์สารสนเทศ	ข้อมูลความเสี่ยง CVSS	Base Score
3.	HTTP OPTIONS Method Enabled	เว็บเซิร์ฟเวอร์ที่ตอบสนองต่อเมธอด OPTIONS HTTP จะเปิดเผยวิธีการอื่นๆ ที่เว็บเซิร์ฟเวอร์สนับสนุน วิธีนี้สามารถช่วยให้ผู้โจมตีค้นหาข้อมูลเกี่ยวกับการกำหนดค่าเซิร์ฟเวอร์และเป็นช่องโหว่ในการโจมตีได้	1. http-options-method-enabled	AMC Server Port: 443 / tcp / www	CVSS v2.0 Base Score 2.6 CVSS v2.0 Vector: CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N	Low
4.	TLS/SSL Server Supports The Use of Static Key Ciphers	เซิร์ฟเวอร์ได้รับการกำหนดค่าให้รองรับการเข้ารหัสที่เรียกว่ารหัสลับแบบคงที่ รหัสเหล่านี้ไม่รองรับ "Forward Secrecy" ในข้อกำหนดใหม่สำหรับ HTTP/2 การเข้ารหัสนี้ถูกขึ้นบัญชีดำ	1. ssl-static-key-ciphers	AMC Server Port: 443 / tcp / www	CVSS v2.0 Base Score 2.6 CVSS v2.0 Vector: CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N	Low

5.2.2 การประเมินค่าระดับความเสี่ยง (Risk Assessment) คือขั้นตอนการประเมินค่าระดับความเสี่ยง (Risk Evaluate) ตามภาพที่ 3.10 เป็นขั้นตอนการคำนวณหรือประเมินค่าระดับความสำคัญของความเสี่ยงแบ่งเป็น 7 ขั้นตอนดังนี้

1) การประเมินค่าโอกาสและผลกระทบใช้วิธี การคำนวณตาม CVSS 2.0 Base Vector ตามภาพที่ 3.19



ภาพที่ 3.19 CVSS 2.0 Base Score Method

ที่มา : สุรทศ ไตรติลานันท์ และ สุรพล รวยสูงเนิน (2559) The Journal of KMUTNB., Vol. 26, No. 1, Jan.–Apr. 2016

การประเมินค่าโอกาสและผลกระทบ มีวิธีการคำนวณตามสมการ (3) และ (4) ดังนี้

$$Lik = 20* AV*AC*Au \quad (3)$$

$$Imp = 10.41*(1-(1-C)*(1-I)*(1-A)) \quad (4)$$

เมื่อ Imp คือ Impact Value

Lik คือ Likelihood หรือ Exploitability Value

C, I, A, AV, AC, Au มีค่าตามตารางที่ 3.16

ตารางที่ 3.16 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
	มีผลกระทบอย่างครบถ้วน C: complete	0.66
ผลกระทบความครบถ้วนสมบูรณ์ Integrity Impact (I)	ไม่มีผลกระทบ N: none	0
	มีผลกระทบบางส่วน P: partial	0.275
	มีผลกระทบอย่างครบถ้วน C: complete	0.66
ผลกระทบความพร้อมใช้งาน Availability Impact (A)	ไม่มีผลกระทบ N: none	0
	มีผลกระทบบางส่วน P: partial	0.275
	มีผลกระทบอย่างครบถ้วน C: complete	0.66

ที่มา: CVSS: A complete Guide to the Common Vulnerability Scoring System Version 2.0

2) การปรับค่าคะแนนให้อยู่ในช่วงระดับคะแนนให้สอดคล้อง OWASP RISK RATING ให้มีช่วงคะแนนอยู่ระหว่าง 1–9 มีวิธีการคำนวณตามสมการ (5), (6) และ (7)

$$NLik = Norm(Likelihood\ Value) \quad (5)$$

$$NImp = Norm(Impact\ Value) \quad (6)$$

$$Norm(X_i) = 9*(X_i)/X_n \quad (7)$$

เมื่อ NLik คือ Normalize Likelihood Value (เป็นการปรับระดับค่าโอกาสจากช่วงค่าคะแนน 0 – 10 มาเป็นช่วงค่าคะแนน 0 – 9 ตามช่วงคะแนนตามตารางที่ 2.2

NImp คือ Normalize Impact Value (เป็นการปรับระดับค่าผลกระทบจาก

ช่วงค่าคะแนน 0 – 10 มาเป็นช่วงค่าคะแนน 0 – 9 ตามช่วงคะแนนตามตารางที่ 2.2

X_i คือ Likelihood or Impact Value (ค่าคะแนนของค่าโอกาสและผลกระทบที่หาได้จากสมการ (3) และ (4)

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

3) การเพิ่มปัจจัยด้านผลกระทบ Organization Impact = Factor [X] โดยทำการประเมินผลกระทบต่อองค์กรของแต่ละสารสนเทศโดยใช้สมมติฐานกรณีสินทรัพย์/ระบบสารสนเทศ ล้มเหลว/ไม่สามารถใช้งานได้มีวิธีการคำนวณตามสมการ (2)

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

OI คือ Organization Impact Value

Lc[x], Li[x], La[x], Pd[x] ใช้ค่า Vector ตามตารางที่ 3.7

4) การประเมินค่าปัจจัยผลกระทบรวมโดยมีวิธีการคำนวณตามสมการ (8)

New Impact(NI) = Average(I, OI) (8)

I คือ Impact Value

OI คือ Organization Impact

5) การประเมินระดับโอกาสและระดับผลกระทบ

โดยใช้ค่า NLik จากขั้นตอนที่ 2) เป็นค่า LikelihoodValue

และค่า New Impact จากขั้นตอนที่ 4) เป็นค่า Impact Value ประเมินตามตารางที่ 2.2

6) การประเมินระดับความสำคัญของความเสี่ยงของแต่ละความเสี่ยงโดยนำค่า Likelihood Level และ Impact Level ประเมินตามตารางที่ 2.3

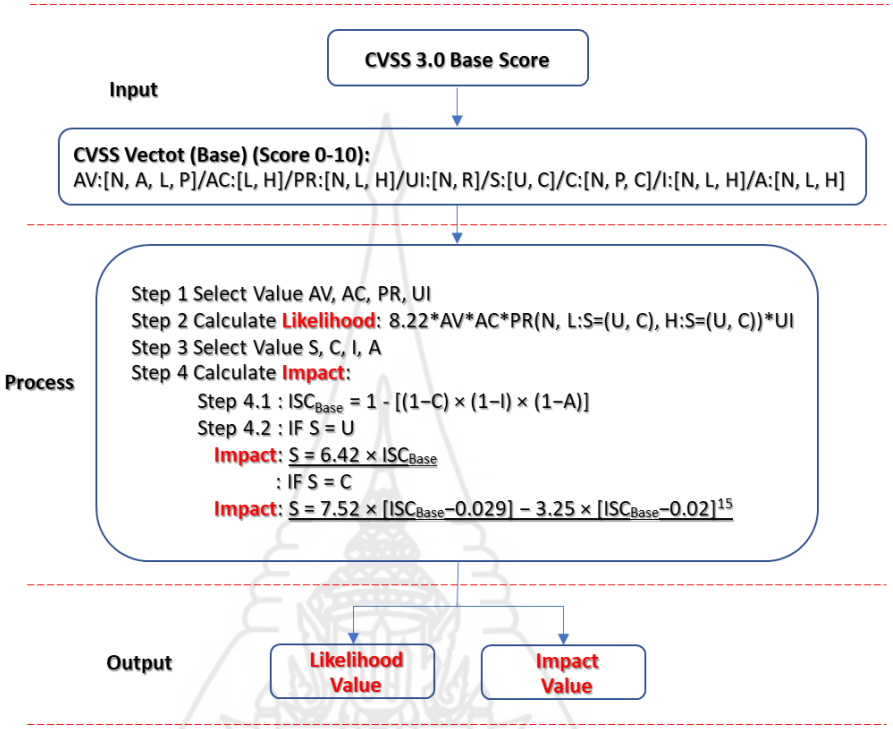
7) จากการศึกษาเพิ่มเติมพบว่าจากงานวิจัย สุรทศ ไตรติลานันท์ และ สุรพล รวยสูงเนิน (2559) The Journal of KMUTNB., Vol. 26, No. 1, Jan.–Apr. 2016 ที่ผู้วิจัยได้นำขั้นตอนในการคำนวณการประเมินค่าโอกาสและผลกระทบ มาเป็นต้นแบบของงานวิจัยของผู้วิจัยนั้นจะเป็นค่า CVSS 2.0 แต่งานการวิจัยของผู้วิจัยมีการใช้ค่าของ การประเมินค่าโอกาสและผลกระทบหรือ CVSS 3.0 สำหรับความรุนแรงระดับ "สูง" ผู้วิจัยได้ศึกษาค้นคว้าเพิ่มเติมจาก https://www.first.org/cvss/v3.0/specification-document พบว่าค่า Vector ใน Base Metrics ของ CVSS 3.0 ได้มีค่าที่เปลี่ยนแปลงจาก CVSS 2.0 ดังตารางที่ 3.17

ตารางที่ 3.17 ความหมายและค่า Base Metric CVSS 3.0

Base Metric	Case of Metric	Value
เวกเตอร์การโจมตี Attack Vector (AV)	ทุกเครือข่ายที่เกี่ยวข้อง N: Network	0.85
	เครือข่ายใกล้เคียง A: Adjacent Network	0.62
	เครือข่ายภายใน L: Local	0.55
	ทางกายภาพ P: Physical	0.2
ความซับซ้อนของการโจมตี Attack Complexity (AC)	ต่ำ L: Low	0.77
	สูง H: High	0.44
สิทธิ์ที่จำเป็น Privilege Required (PR)	ไม่มี N: None	0.85
	ต่ำ L: Low	0.62 (0.68 if Scope (S) is Changed)
	สูง H: High	0.27 (0.50 if Scope (S) is Changed)
การโต้ตอบกับผู้ใช้ User Interaction (UI)	ไม่จำเป็น N: None	0.85
	ต้องการ R: Required	0.62
ขอบเขต Scope (S)	ไม่เปลี่ยนแปลง U: Unchanged	$6.42 \times ISC_{Base}$
	เปลี่ยนแปลง C: Changed	$7.52 \times [ISC_{Base} - 0.029] - 3.25 \times [ISC_{Base} - 0.02]^{15}$
ผลกระทบต่อการรักษาความลับ Confidentiality Impact (C)	ไม่มี N: none	0
	ต่ำ L: Low	0.22
	สูง H: High	0.56
ผลกระทบต่อความครบถ้วนสมบูรณ์ Integrity Impact (I)	ไม่มี N: none	0
	ต่ำ L: Low	0.22
	สูง H: High	0.56
ผลกระทบต่อความพร้อมใช้งาน Availability Impact (A)	ไม่มี N: none	0
	ต่ำ L: Low	0.22
	สูง H: High	0.56

ที่มา : https://www.first.org/cvss/v3.0/specification-document

สำหรับการประเมินค่าโอกาสและผลกระทบใช้วิธี การคำนวณตาม CVSS 3.0 Base Vector สามารถแสดงเป็นขั้นตอนและวิธีการ ตามภาพที่ 3.20



ภาพที่ 3.20 CVSS 3.0 Base Score Method

จากภาพที่ 3.20 สามารถเขียนสมการของการประเมินค่าโอกาสและผลกระทบในส่วนของ CVSS 3.0 และมีวิธีการคำนวณตามสมการ (9) และ (10) ดังนี้

$$Lik = 8.22*AV*AC*\ PR(N, L:S=(U, C), H:S=(U, C))*UI \quad (9)$$

$$Imp = [\ ISC_{Base} = 1 - ((1-C) \times (1-I) \times (1-A))\ ]$$

IF S = U

$$S = 6.42 \times ISC_{Base}$$

IF S = C

$$S = 7.52 \times [ISC_{Base}-0.029] - 3.25 \times [ISC_{Base}-0.02]^{15} \quad (10)$$

เมื่อ Imp คือ Impact Value / ISC_{Base} คือ คะแนนย่อยผลกระทบ

Lik คือ Likelihood หรือ Exploitability Value

S, C, I, A, AV, AC, PR, UI มีค่าตามตารางที่ 3.17

สำหรับเครื่องมือการประเมินความเสี่ยงของงานวิจัยนี้ผู้วิจัยได้นำแนวทางมาจากงานวิจัยของ สุรทศ ไตรติลานันท์ และ สุรพล รวยสูงเนิน กรณีศึกษา: โมเดลทางด้านเทคนิคสำหรับวิธีการประเมินความเสี่ยงความมั่นคงปลอดภัยในระบบสารสนเทศสำหรับโรงพยาบาล ซึ่งจากตารางทบทวนวรรณกรรม ตารางที่ 2.4 เครื่องมือที่ใช้ในการประเมินความเสี่ยงที่ผู้วิจัยได้นำมาเป็นต้นแบบประกอบไปด้วย 1) CVSS SCORE 2) ค่าโอกาสที่จะเกิด และค่าผลกระทบ 3) ระเบียบวิธีการประเมินความเสี่ยงของ OWASP ซึ่งจุดเด่นของเครื่องมือการประเมินความเสี่ยงระบบสารสนเทศทั้ง 3 เครื่องนี้ จะมีกระบวนการดำเนินการปฏิบัติที่สัมพันธ์กัน กล่าวคือมีการหาค่าความรุนแรงของช่องโหว่เพื่อได้ค่าโอกาสที่จะเกิดและค่าผลกระทบ นำไปสู่ผลของความเสี่ยงระบบสารสนเทศขององค์กรอย่างชัดเจน ซึ่งอธิบายได้ตามตัวอย่างที่การประเมินค่าระดับความเสี่ยงที่ผ่านมาข้างต้นนั้น จึงเป็นสาเหตุให้ผู้วิจัยนำเครื่องมือการประเมินความเสี่ยงทั้ง 3 เครื่องมือมาใช้ในงานวิจัยนี้

5.2.3 แสดงระดับความสำคัญของความเสี่ยง (Risk Rating) คือขั้นตอนการให้คะแนนระดับความสำคัญของความเสี่ยง ตามภาพที่ 3.10 เป็นขั้นตอนแสดงระดับความสำคัญของความเสี่ยงสารสนเทศ ภาพรวม หรือแสดงแยกตามระบบสารสนเทศเป้าหมายดังหัวข้อต่อไปนี้

1) ผลการประเมินผลกระทบที่มีต่อองค์กรของระบบสารสนเทศเป้าหมายซึ่งมีผลการประเมินตามตารางที่ 3.18

ตารางที่ 3.18 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 3.18

Organization Impact Factor

Loss of Confidentiality (Lc) = A| All data disclosed |9

Loss of Integrity (Li) = E2| Extensive seriously corrupt data |7

Loss of Availability (La) = E2| Extensive primary services interrupted |7

Reputation damage (Rd) = B| Brand damage |9

B) คำนวณผลกระทบต่อองค์กรของอุปกรณ์เครื่องแม่ข่ายตามสมการที่ (2)

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) ผลการประเมินค่าความเสี่ยงของระบบสารสนเทศขององค์กรซึ่งมีผลการประเมินตามตารางที่ 3.19 และ 3.20

ตารางที่ 3.19 ตัวอย่างผลการประเมินผลกระทบและโอกาสที่จะเกิดจาก CVSS VECTOR

Assets/System	Vulnerability	CVSS	L	I	OI	NI
AMC SERVER	TLS/SSL Server is enabling the BEAST attack	CVSS2#AV:N /AC:M/Au:N/ C:P/I:N/A:N	7.74	2.61	8.00	5.31
WEB Server	X.509 Certificate Subject CN Does Not Match the Entity Name	CVSS2#AV:N /AC:H/Au:N/ C:C/I:C/A:N	4.41	8.28	7.25	7.77
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
OpenMCU 1	Unix Operating System Unsupported Version Detection	CVSS:3.0/AV: N/AC:L/PR:N /UI:N/S:C/C: H/I:H/A:H	3.51	5.40	7.00	6.20

ตัวอย่างที่ 2 OpenMCU 1 (กรณี CVSS 2.0)

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 (3)

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

Lik = 20*1*0.61*0.704 = 8.6

B) คำนวณค่าผลกระทบ (Imp) ตามสมการ (4)

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 (5)

NLik = Norm(Lik) = $9*(X_i)/X_n$ ตามสมการ (7)

NLik = 9*8.6/10 = 7.74 ตามสมการ

ดังนั้นค่าคะแนนผลกระทบ (Likelihood) L คือ 7.74

D) ปรับค่าผลกระทบใหม่ (NImp) ตามสมการ (6)

NImp = Norm(Imp) = $9*(X_i)/X_n$ ตามสมการ (7)

NImp = 9*2.86/10 = 2.61

ดังนั้นค่าคะแนนผลกระทบ (Impact) I คือ 2.61

E) นำค่าผลกระทบต่อองค์กร (OI) จากตารางที่ 3.18

OI = 7.00

F) คำนวณค่าผลกระทบใหม่ (NI) ตามสมการที่ (8)

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 2.3

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) ประเมิน
ระดับความสำคัญความเสี่ยงก่อนเพิ่มผลกระทบต่อองค์กร
(RISK) และหลังเพิ่มผลกระทบต่อองค์กร (RISK+) ตามตารางที่ 3.18

RISK = L × I = 3 × 1 = Medium

RISK+ = L × NI = 3 × 2 = High

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

ตัวอย่างที่ 3 OpenMCU 1 (กรณี CVSS 3.0)

ชื่อช่องโหว่ : Unix Operating System Unsupported Version Detection

มีค่า Vector : CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

A) คำนวณค่าโอกาส (Lik) จากสมการ (9)

Lik = 8.22*AV[N]*AC[L]*PR[N]*UI[N]

Lik = 8.22*0.85*0.77*0.85*0.85 = 3.9

B) คำนวณค่าผลกระทบ (Imp) ตามสมการ (10)

Imp = [ISC_{Base} = 1 − ((1−C) × (1−I) × (1−A))]

IF S = U

S = 6.42 × ISC_{Base}

IF S = C

S = S7.52 × [ISC_{Base}−0.029] − 3.25 × [ISC_{Base}−0.02]^{15}

Imp = [ISC_{Base} = 1 − ((1−C[H]) × (1−I[H]) × (1−A[H]))]

$ISC_{Base} = 1 - ((1-0.56) \times (1-0.56) \times (1-0.56))$

$ISC_{Base} = 0.90$

IF S = C

$S = 7.52 \times [0.9-0.029] - 3.25 \times [0.9-0.02]^{15}$

S = 6.00

Imp = 6.00

C) ปรับค่าโอกาสใหม่ (NLik) ตามสมการ (5)

NLik = Norm(Lik) = $9*(X_i)/X_n$ ตามสมการ (7)

NLik = 9*3.9/10 = 3.51

ดังนั้นค่าคะแนนผลกระทบ (Likelihood) L คือ 3.51

D) ปรับค่าผลกระทบใหม่ (NImp) ตามสมการ (6)

NImp = Norm(Imp) = $9*(X_i)/X_n$ ตามสมการ (7)

NImp = 9*6.0/10 = 5.40

ดังนั้นค่าคะแนนผลกระทบ (Impact) I คือ 5.40

E) นำค่าผลกระทบต่อองค์กร (OI) จากตารางที่ 3.18

OI = 7.00

F) คำนวณค่าผลกระทบใหม่ (NI) ตามสมการที่ (8)

NI = Average (I, OI)

NI = Average (5.40, 7.00) = 6.20

ดังนั้นค่าคะแนนผลกระทบใหม่ NI คือ 6.20

G) นำค่า L, I, และ NI จากขั้นตอน C), D), F) ประเมินระดับโอกาส/ผลกระทบตามตารางที่ 2.3

L × I = MEDIUM (2) × MEDIUM (2) = 2 × 2

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

H) นำค่า L × I และ L × NI จากขั้นตอน G) ประเมินระดับความสำคัญความเสี่ยงก่อนเพิ่มผลกระทบต่อองค์กร (RISK) และหลังเพิ่มผลกระทบต่อองค์กร (RISK+) ตามตารางที่ 3.20

RISK = L × I = 2 × 2 = Medium

RISK+ = L × NI = 2 × 3 = High

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

ตารางที่ 3.20 ตัวอย่างรูปแบบผลการประเมินความเสี่ยงช่องโหว่ระบบสารสนเทศขององค์กร

Assets/System	Vulnerability	L x I	Risk	L x NI	Risk+
AMC SERVER	TLS/SSL Server is enabling the BEAST attack	3 x 1	Med	3 x 2	High
WEB Server	X.509 Certificate Subject CN Does Not Match the Entity Name	2 x 1	Low	2 x 2	Med
OpenMCU Server 1	SSH Server Supports RC4 Cipher Algorithms	3 x 1	Med	3 x 2	High
OpenMCU Server 1	Unix Operating System Unsupported Version Detection	2 x 2	Med	2 x 3	High

จากตารางที่ 3.20 เป็นผลของการคำนวณค่าความเสี่ยง ของขั้นตอนการประเมินความเสี่ยงช่องโหว่ที่ประเมินพบ ที่ส่งผลกระทบต่อองค์กร จากตัวอย่างในตารางพบว่าในการคำนวณรูปแบบความเสี่ยงตามปกติจะได้ระดับความเสี่ยงตรงกับค่า Base Score มาตรฐาน เช่น ในเครื่องแม่ข่าย AMC มีช่องโหว่ที่ชื่อ TLS/SSL Server is enabling the BEAST attack คำนวณค่าระดับความเสี่ยงได้ค่าระดับปานกลาง แต่เมื่อเพิ่มค่าผลกระทบขององค์กร (NI) เข้าไปในการคำนวณด้วยแล้วจะทำให้ค่าระดับความเสี่ยงเพิ่มขึ้นเป็นค่าระดับสูง

5.2.4 การจัดทำรายงานในด้านต่างๆ (Report)

สำหรับขั้นตอนการรายงานผลของการประเมินความเสี่ยงช่องโหว่ที่มีผลกระทบต่อระบบสารสนเทศขององค์กรนั้นเป็นขั้นตอนที่จัดทำขึ้นเพื่อรายงานให้ผู้ที่มีส่วนเกี่ยวข้องต่อระบบสารสนเทศขององค์กรเช่น ในส่วนของผู้บังคับบัญชา และ CIO ขององค์กร จะได้รับทราบและให้การสนับสนุนในการแก้ปัญหาที่ตรวจพบ เพื่อที่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับการดูแลรักษาความมั่นคงปลอดภัยต่อระบบสารสนเทศขององค์กร จะได้นำรายงานที่จัดทำขึ้นมานี้ไปแก้ไขจุดบกพร่องหรือจุดอ่อนของระบบสารสนเทศ ตามกรอบการจัดการช่องโหว่ฯ ที่พัฒนาขึ้นมานี้ได้อย่างสมบูรณ์ โดยมีรูปแบบดังนี้

1) รายงานการประเมินความเสี่ยง (Risk Assessment Report) เป็นรูปแบบการรายงานสรุปการประเมินความเสี่ยงช่องโหว่ที่ประเมินพบ และจะส่งผลกระทบต่อองค์กร เป็นรายงานเพื่อแจ้งให้ผู้บังคับบัญชา หรือ CIO ระบบสารสนเทศขององค์กร และผู้ที่เกี่ยวข้องกับระบบสารสนเทศขององค์กรที่ควรทราบ ตามตารางที่ 3.21

ตารางที่ 3.21 ตัวอย่างรายงานผลการประเมินความเสี่ยงช่องโหว่ระบบสารสนเทศขององค์กร

อุปกรณ์/ระบบสารสนเทศ	**ช่องโหว่ที่ประเมินพบ**	**ผลการประเมินความเสี่ยง RISK**	**ผลการประเมินความเสี่ยง+ผลกระทบต่อองค์กร RSIK+**	**หมายเหตุ**
ระบบศูนย์ข่าวอัตโนมัติ (AMC Server)	TLS/SSL Server is enabling the BEAST attack	ระดับกลาง	ระดับสูง	กำลังดำเนินการแก้ไข
เว็บไซต์กองทัพภาคที่ 2 (WEB Server)	X.509 Certificate Subject CN Does Not Match the Entity Name	ระดับต่ำ	ระดับกลาง	กำลังดำเนินการแก้ไข
ระบบประชุมทางไกล OpenMCU 1	SSH Server Supports RC4 Cipher Algorithms	ระดับกลาง	ระดับสูง	กำลังดำเนินการแก้ไข
เครือข่ายส่วนตัวเสมือน VPN PPTP	TLS Server Supports TLS version 1.1	ระดับต่ำ	ระดับกลาง	กำลังดำเนินการแก้ไข

2) รายงานการประเมินช่องโหว่ที่ประเมินพบ (Vulnerability Assessment Report) เป็นรูปแบบการรายงานที่แจ้งให้ผู้ที่เกี่ยวข้องกับระบบสารสนเทศขององค์กรที่มีหน้าที่ในการแก้ไขปัญหาที่เกิดขึ้นกับระบบสารสนเทศขององค์กร ตามตารางที่ 3.22

ตารางที่ 3.22 ตัวอย่างรูปแบบรายงานผลการประเมินความเสี่ยงช่องโหว่ระบบสารสนเทศขององค์กรพร้อมรายละเอียดช่องโหว่และข้อเสนอแนะในการแก้ไข

ลำดับ	ชื่อช่องโหว่	ข้อมูลอ้างอิง	อุปกรณ์สารสนเทศ	รายละเอียด	ข้อเสนอแนะในการแก้ไข	RISK+
1.	SSL Medium Strength Cipher Suites Supported (SWEET32)	1. tenable plugins #42873 2. CVE: CVE-2016-2183	AMC Server Port :443 / tcp / www	โฮสต์ระยะไกลสนับสนุนการใช้การเข้ารหัส SSL ที่มีการเข้ารหัสระดับกลาง ถือว่ามีความรุนแรงปานกลางเป็นการเข้ารหัสที่ใช้ความยาวของกุญแจ (มากกว่า 64 บิต และน้อยกว่า 112 บิต key, or 3DES)	ดำเนินการปรับตั้งค่าให้รับการเข้ารหัส SSL Cipher มีความปลอดภัยมากกว่า 112 บิต (3DES) กำหนดค่าเว็บเซิร์ฟเวอร์ให้เข้ารหัสแบบ 128 บิต และแก้ไข SWEET32 โดยการปิดใช้งาน (3DES) Value=0	Medium
2.	TLS Version 1.0 Protocol Detection	1. tenable plugins #104743	AMC Server Port: 443 / tcp / www	บริการระยะไกลยอมรับการเชื่อมต่อที่เข้ารหัสโดยใช้ TLS 1.0 TLS 1.0 มีข้อบกพร่องในการออกแบบการเข้ารหัสจำนวนมาก	เปิดใช้งานการสนับสนุนสำหรับ TLS 1.2 และ 1.3 และปิดใช้งานการสนับสนุนสำหรับ TLS 1.0	Medium

ตารางที่ 3.22 (ต่อ)

ลำดับ	ชื่อช่องโหว่	ข้อมูลอ้างอิง	อุปกรณ์สารสนเทศ	รายละเอียด	ข้อเสนอแนะในการแก้ไข	RISK+
3.	TLS Version 1.1 Protocol Deprecated	1. tenable plugins #157288	AMC Server Port: 443 / tcp / www	การเชื่อมต่อที่เข้ารหัสโดยใช้ TLS 1.1 มีข้อบกพร่องในการออกแบบการเข้ารหัสจำนวนมาก	เปิดใช้งานการสนับสนุนสำหรับ TLS 1.2 และ/หรือ 1.3 และปิดใช้งานการสนับสนุนสำหรับ TLS 1.1	Medium
4.	Nameserver Processes Recursive Queries	1. dns-processes-recursive-queries 2.http://technet.microsoft.com/en-us/library/cc787724(v=ws.10).aspx	AMC Server Port: 53 / UDP	การอนุญาตให้ Nameserver ประมวลผลการสืบค้นแบบเรียกซ้ำที่มาจากระบบอื่นๆ ในบางสถานการณ์ อาจถูกผู้โจมตีดำเนินการโจมตีแคชซึ่งทำให้เกิดการหยุดให้บริการของเครื่องแม่ข่ายได้	ปิดการใช้งานการเรียกซ้ำบนเซิร์ฟเวอร์ DNS	Medium

5.3 การแก้ไขช่องโหว่ (Remediation)

จุดอ่อนหรือช่องโหว่ที่ได้จากการตรวจพบนั้น จะรายงานมาให้ผู้ที่ดูแลระบบสารสนเทศขององค์กรเพื่อจัดบุคลากรที่ปฏิบัติหน้าที่ทำการแก้ไขปัญหาช่องโหว่ที่ประเมินพบ โดยที่บุคลากรดังกล่าวสามารถศึกษาได้จากรายละเอียดการแก้ไขหรือข้อเสนอแนะที่แนบมาพร้อมกับรายงานการตรวจพบช่องโหว่ โดยอาจศึกษาเพิ่มจากข้อมูลอ้างอิงจากรายงานการตรวจพบช่องโหว่ในอินเทอร์เน็ตเช่น tenable plugins #428732 , CVE: CVE-2016-2183 เป็นต้น

5.3.1 ศึกษารายละเอียดจากรายงานการประเมินช่องโหว่

จากรายงานที่ได้รับมาจากการประเมินช่องโหว่ บุคลากรผู้ปฏิบัติหน้าที่ในการแก้ไขช่องโหว่ควรศึกษาจากรายละเอียดข้อเสนอแนะเพื่อหาวิธีแก้ไข ตัวอย่างเช่นศึกษารายละเอียดจากตารางที่ 3.23 ดังนี้

ตารางที่ 3.23 ตัวอย่างรายงานการประเมินช่องโหว่ที่ประเมินพบและส่งไปดำเนินการแก้ไข

ลำดับ	ชื่อช่องโหว่	ข้อมูลอ้างอิง	อุปกรณ์สารสนเทศ	รายละเอียด	ข้อเสนอแนะในการแก้ไข	RISK+
1.	SSL Medium Strength Cipher Suites Supported (SWEET32)	1. tenable plugins #42873 2. CVE: CVE-2016-2183	AMC Server Port :443 / tcp / www	โฮสต์ระยะไกลสนับสนุนการใช้การเข้ารหัส SSL ที่มีการเข้ารหัสระดับกลาง ถือว่ามีความรุนแรงปานกลางเป็นการเข้ารหัสที่ใช้ความยาวของกุญแจ (มากกว่า 64 บิต และน้อยกว่า 112 บิต key,or 3DES)	ดำเนินการปรับตั้งค่าให้รับการเข้ารหัส SSL Cipher มีความปลอดภัยมากกว่า 112 บิต (3DES) กำหนดค่าเว็บเซิร์ฟเวอร์ให้เข้ารหัสแบบ 128 บิต และแก้ไข SWEET32 โดยการปิดใช้งาน (3DES) Value=0	Medium

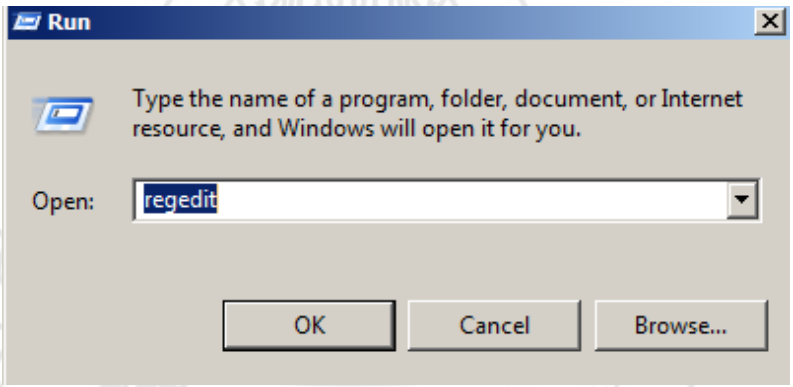
จากตัวอย่างรายละเอียดในตารางพบช่องโหว่ที่ชื่อว่า SSL Medium Strength Cipher Suites Supported (SWEET32) ผู้วิจัยได้ศึกษาเพิ่มโดยมีรายละเอียดดังนี้ ช่องโหว่ที่ชื่อว่า SWEET32 คือ อัลกอริทึมเข้ารหัส Triple Data Encryption Standard (3DES) ซึ่งถูกพัฒนาตั้งแต่ปี 1998 กำลังจะถูกประกาศให้ยกเลิกการใช้งานโดย NIST หลังจากที่มีการค้นพบข้อบกพร่องรวมไปถึงงานวิจัยหลายงานที่ออกมาเปิดเผยปัญหาซึ่งอาจส่งผลต่อคุณลักษณะด้านความปลอดภัยในการใช้งาน

อัลกอริทึมโดยตรงหนึ่งในการโจมตีที่ส่งผลกระทบต่อ 3DES คือ Sweet32 ซึ่งแสดงให้ถึงความเป็นไปได้ในทางปฏิบัติที่ทำให้ผู้โจมตีสามารถสกัดข้อมูลที่ใช้งานได้ออกจากข้อมูลที่ถูกเข้ารหัสภายใต้เงื่อนไขการโจมตี เช่น ผู้โจมตีจะต้องทำการดักจับข้อมูลที่ถูกเข้ารหัสให้ถึงจุดหนึ่ง (ตามงานวิจัยคือ 785 GB) เพื่อให้สามารถหาการชนกัน (collision) ที่เป็นผลมาจากขนาดของบล็อคที่น้อยของอัลกอริทึมได้ NIST มีการวางแผนที่จะลดขนาดของบล็อคจาก 2^32 เป็น 2^20 โดยการเปลี่ยนแปลงนี้จะถูกประกาศในการแก้ไข Special Pulibcation 800-67 ซึ่งจะมีการเปิดให้ลงความเห็นในการแปลี่ยนแปลงเร็วๆ นี้ โดยในระยะยาว NIST ก็จะมีการประกาศไทม์ไลน์เพื่อที่จะยกเลิกการใช้งาน 3DES เช่นเดียวกัน ในขณะเดียวกัน NIST วางแผนที่จะไม่อนุญาตให้มีการใช้ 3DES ในโพรโทคอลอย่าง TLS หรือ IPSEC โดยแนะนำให้มีการเปลี่ยนไปใช้อัลกอริทึมที่มีความแข็งแกร่งกว่าอย่าง AES แทน

5.3.2 ดำเนินการแก้ไขช่องโหว่

จากการศึกษารายละเอียดจากรายงานการประเมินช่องโหว่ตามข้อ 5.3.1 นั้นสามารถนำมาหาข้อมูลในการแก้ไขเพิ่มจากข้อมูลอ้างอิง และข้อเสนอแนะในการแก้ไข และข้อมูลจากอินเทอร์เน็ตเพิ่มได้และนำมาแก้ไขช่องโหว่ตามตัวอย่างการแก้ไขช่องโหว่ที่ชื่อ SWEET32 ดังนี้

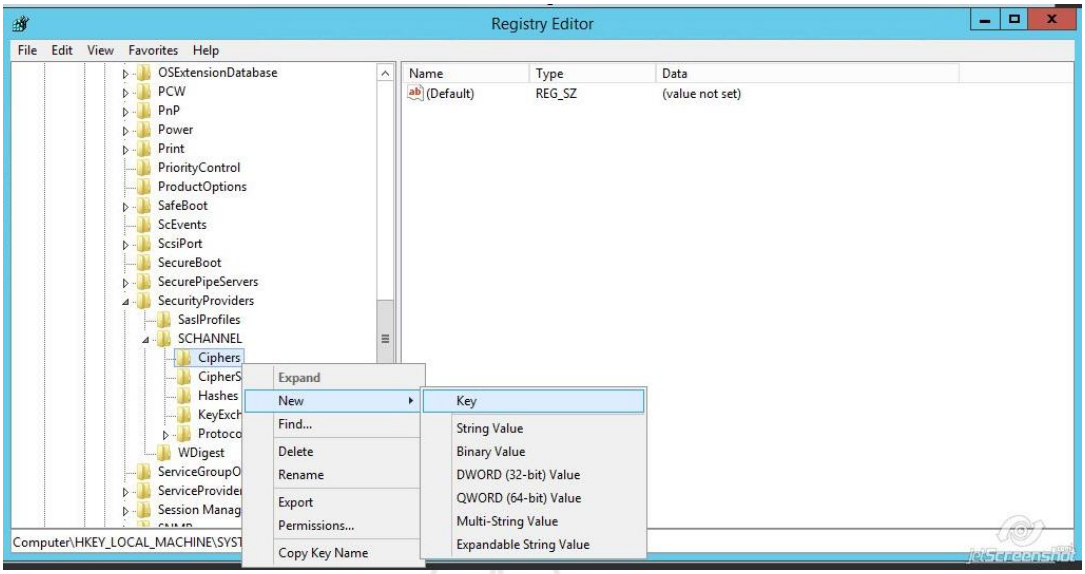
1) คลิก Start, Run, พิมพ์ regedit, และคลิก OK ตามภาพที่ 3.21



ภาพที่ 3.21 การเปิดตัวแก้ไขรีจิสทรี

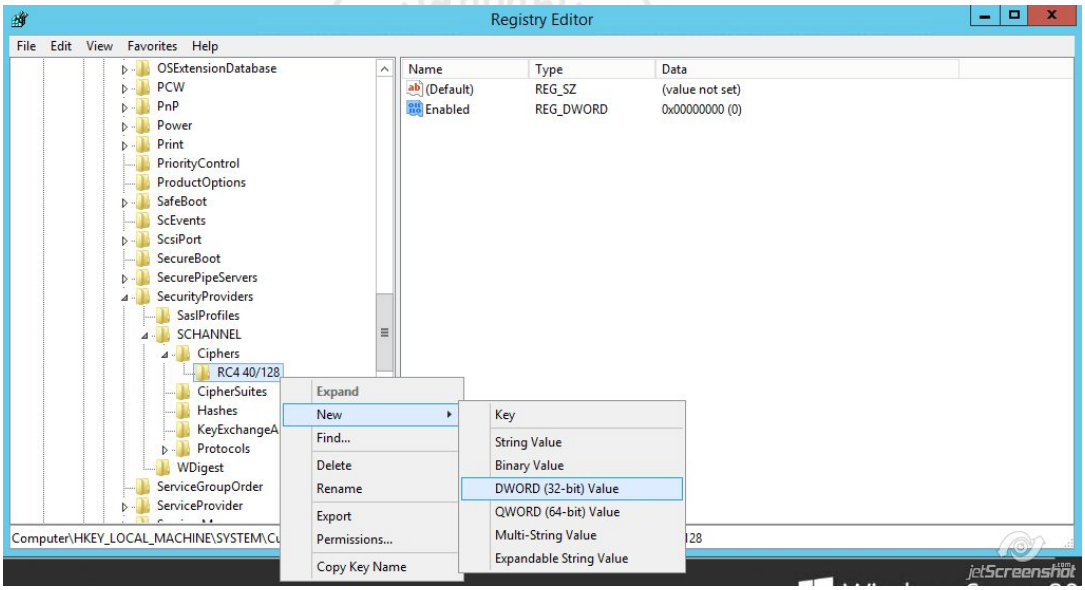
2) ไปที่HKey_Local_Machine\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\Ciphers

3) คลิกขวาแล้วไปที่ Ciphers >> New >> Key แล้วให้สร้างคีย์ขึ้นมาใหม่ โดยกำหนดชื่อ Name the key = 'RC4 40/128' ตามภาพที่ 3.22



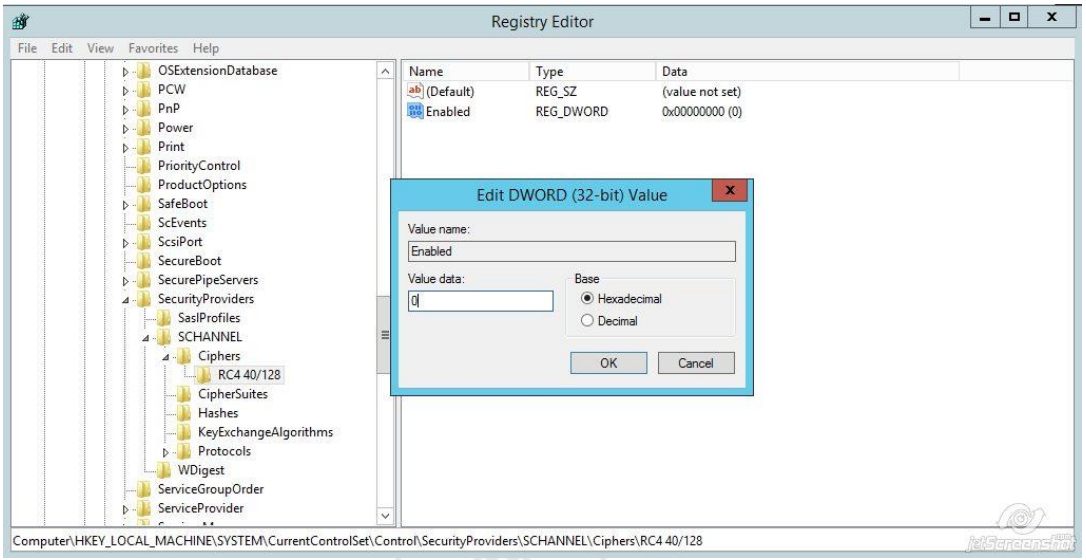
ภาพที่ 3.22 การกำหนดชื่อ Name the key = 'RC4 40/128'

4) คลิกขวาที่ RC4 40/128 >> New >> DWORD (32-bit) Value ตั้งชื่อค่าเป็น ' Enabled ' ตามภาพที่ 3.23



ภาพที่ 3.23 การเข้าไปตั้งค่า Enabled ที่ DWORD (32-bit) Value

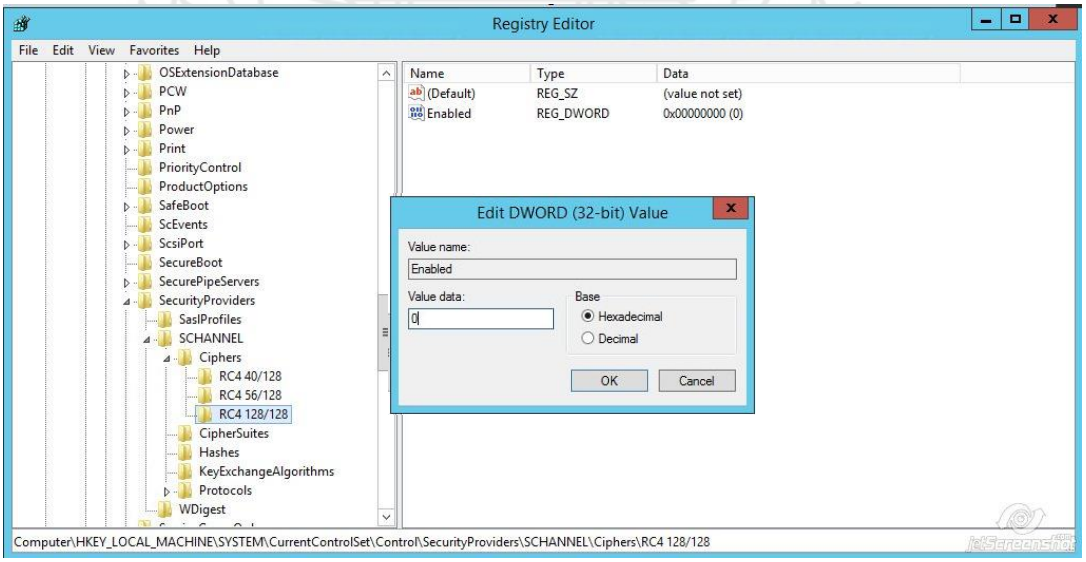
5) ดับเบิลคลิกที่ค่า Enabled ที่สร้างขึ้นและตรวจสอบให้แน่ใจว่ามีศูนย์ (0) ใน Value Data: field >> คลิก OK ตามภาพที่ 3.24



ภาพที่ 3.24 การตั้งค่า Enabled Value Data : 0

6) สร้างคีย์อีกสองคีย์ในชื่อ 'RC4 56/128' และ 'RC4 128/128' ในไดเร็กทอรี Ciphers ทำซ้ำขั้นตอนที่ 4 และ 5 สำหรับแต่ละข้อ

7) หลังจากขั้นตอนที่ 6 เสร็จสิ้น จะมีคีย์ทั้งหมด 3 คีย์สำหรับ RC4 ใน Ciphers ค่า DWORD ชื่อ ' Enabled ' โดยมีข้อมูลค่าเป็นศูนย์ (0) ทุกคีย์ ตามภาพที่ 3.25



ภาพที่ 3.25 การตั้งค่า Enabled Value Data : 0 คีย์ที่เพิ่มเติม

8) รีสตาร์ท Windows Server เพื่อเริ่มต้นค่าการเปลี่ยนแปลง

5.3.3 รายงานแก้ไขช่องโหว่

เมื่อดำเนินการในขั้นตอนการแก้ไขช่องโหว่ที่ประเมินพบเป็นที่เรียบร้อยแล้ว ควรดำเนินการทำรายงานการแก้ไขช่องโหว่ส่งกลับไปยังหน่วยงานหรือบุคลากรที่ดำเนินการประเมินความเสี่ยงช่องโหว่ระบบสารสนเทศขององค์กร เพื่อนำข้อมูลไปดำเนินการประเมินซ้ำ (Re-Assessment) ลักษณะรายงานตามตารางที่ 3.24

ตารางที่ 3.24 ตัวอย่างรายงานการดำเนินการแก้ไขช่องโหว่ที่ประเมินพบ

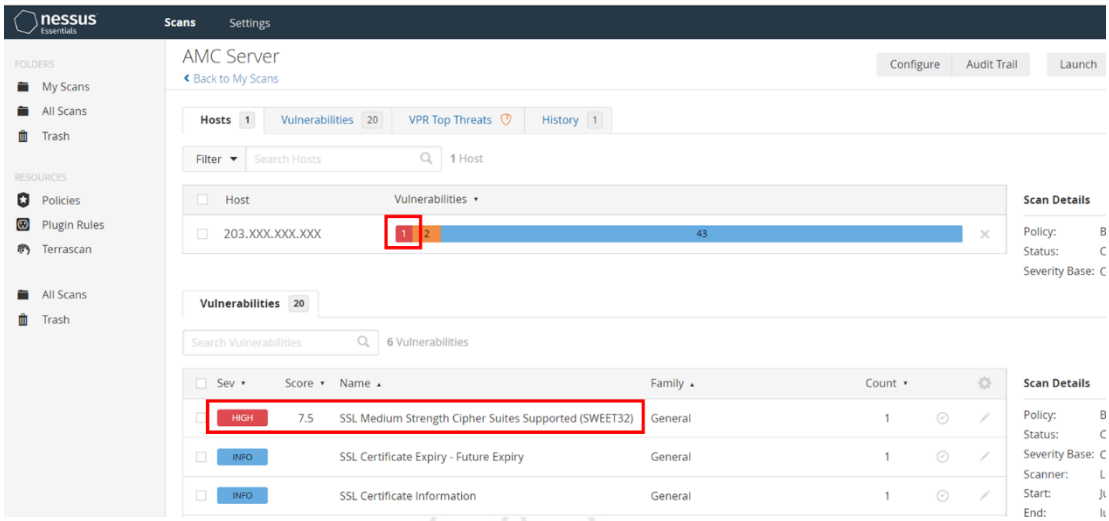
ลำดับ	ชื่อช่องโหว่	อุปกรณ์สารสนเทศ	การดำเนินการแก้ไขช่องโหว่	หมายเหตุ
1.	SSL Medium Strength Cipher Suites Supported (SWEET32)	AMC Server Port :443 / tcp / www	การปิด Weak cipher (3DES) ที่ถูกใช้โดย Web Server IIS ดำเนินการปรับตั้งค่าให้รับการเข้ารหัส SSL Cipher มีความปลอดภัยมากกว่า 112 บิต (3DES) กำหนดค่าเว็บเซิร์ฟเวอร์ให้เข้ารหัสแบบ 128 บิต และแก้ไข SWEET32 โดยการปิดใช้งาน (3DES) Value=0	แก้ไขเรียบร้อย
2.	TLS Version 1.0 Protocol Detection	1.tenable plugins #104743	เปิดใช้งานการสนับสนุนสำหรับ TLS 1.2 และ 1.3 และปิดใช้งานการสนับสนุนสำหรับ TLS 1.0	แก้ไขเรียบร้อย

5.4 การประเมินซ้ำ (Re-Assessment)

การดำเนินการสำหรับการประเมินซ้ำหลังจากช่องโหว่ที่ตรวจสอบพบได้รับการแก้ไขแล้วเป็นขั้นตอนในการตรวจสอบการแก้ไขช่องโหว่หรือจุดอ่อนที่มีความเสี่ยงต่อระบบสารสนเทศขององค์กรนั้นได้ปิดช่องโหว่ที่มีความเสี่ยงแล้ว โดยมีการดำเนินการดังนี้

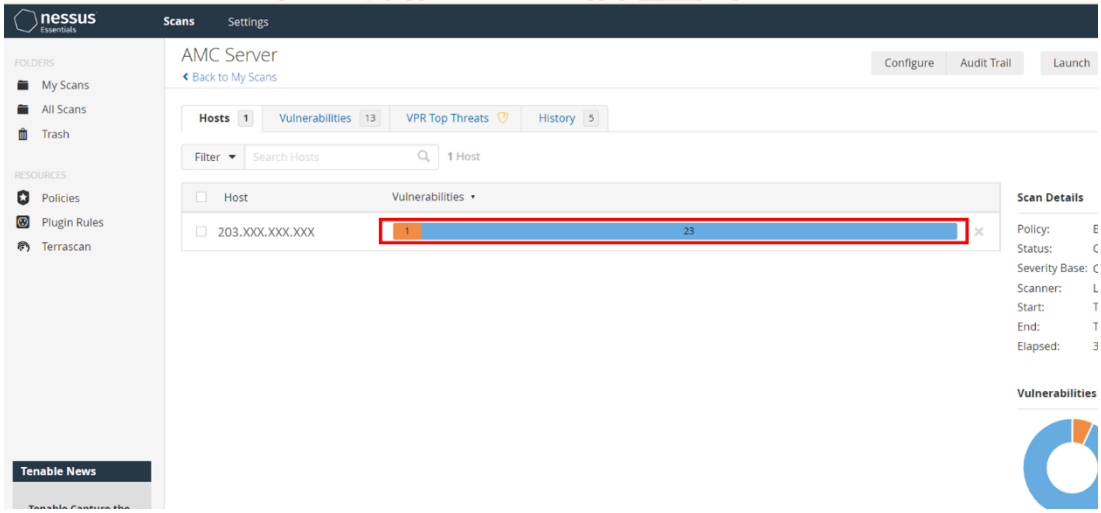
5.4.1 การประเมินช่องโหว่ซ้ำ (Re-Vulnerability Assessment) ในการดำเนินการขั้นตอนนี้จะเป็นการเริ่มกระบวนการใหม่ทั้งหมดในหัวข้อที่ 5.2.1 การประเมินช่องโหว่ (Vulnerability Assessment) โดยใช้เครื่องมือที่ระบุในหัวข้อดังกล่าวนั่นคือเครื่องมือประเมินช่องโหว่อัตโนมัติ Nessus และ Nexpose ทำการสแกนช่องโหว่ของอุปกรณ์ระบบสารสนเทศที่ได้รับการแก้ไขช่องโหว่มาแล้ว ตามตัวอย่างการสแกนซ้ำช่องโหว่ที่ตรวจสอบและได้รับการแก้ไขแล้ว กรณีของช่องโหว่ที่ชื่อว่า SSL Medium Strength Cipher Suites Supported (SWEET32) ดังนี้

1) ตัวอย่างการสแกนช่องโหว่ที่ตรวจสอบพบครั้งแรกตรวจพบช่องโหว่ที่มีชื่อว่า SSL Medium Strength Cipher Suites Supported (SWEET32) ตามภาพที่ 3.26



ภาพที่ 3.26 ผลการสแกนช่องโหว่ครั้งแรก

2) ตัวอย่างการสแกนซ้ำช่องโหว่ที่ได้รับการแก้ไขแล้ว จะเห็นว่าไม่มีช่องโหว่ที่มีชื่อว่า SSL Medium Strength Cipher Suites Supported (SWEET32) ที่ค่า Base Score ระดับสูงแล้ว ตามภาพที่ 3.27



ภาพที่ 3.27 ผลการสแกนซ้ำช่องโหว่ที่ประเมินพบ

5.4.2 กรณีพบช่องโหว่หลังการแก้ไขแล้ว ให้ดำเนินการแก้ไขช่องโหว่ (Remediation) ซ้ำอีกครั้งจนกว่าช่องโหว่นั้นจะปิดลงอย่างสมบูรณ์

5.4.3 กรณีไม่พบช่องโหว่หลังการแก้ไขแล้ว ให้ดำเนินการรวบรวมจัดทำรายงานการดำเนินการประเมินช่องโหว่ระบบสารสนเทศขององค์กร ตลอดจนไปถึงการแก้ไขช่องโหว่ที่ประเมินพบ และผลการตรวจสอบซ้ำหลังจากการแก้ไขช่องโหว่ เพื่อดำเนินการส่งรายงานดังกล่าวไปดำเนินการในขั้นตอนการตรวจสอบยืนยันความถูกต้อง (Verification) ต่อไป

5.5 การตรวจสอบยืนยันความถูกต้อง (Verification)

รวบรวมข้อมูลทำเป็นรูปแบบรายงานตั้งแต่ขั้นตอนเริ่มต้นตามกรอบการจัดการช่องโหว่ระบบสารสนเทศเพื่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์ กรณีศึกษา กองบัญชาการกองทัพภาคที่ 2 เพื่อนำเสนอคณะกรรมการตรวจสอบช่องโหว่ระบบสารสนเทศ เพื่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ทภ.2 เพื่อให้ช่วยตรวจสอบความถูกต้องในการจัดการช่องโหว่ (Vulnerability Management) และให้ข้อเสนอแนะ ในการแก้ไขปรับปรุงในการแก้ไขช่องโหว่สารสนเทศขององค์กรที่เกิดขึ้น เพื่อความถูกต้องและเพิ่มประสิทธิภาพในการป้องกันความเสี่ยงที่เกิดขึ้นจากช่องโหว่ระบบสารสนเทศที่จะส่งผลกระทบต่อภารกิจขององค์กรต่อไป โดยรายงานข้อมูลต่างๆ ที่ส่งให้ศูนย์ไซเบอร์กองทัพบกให้ตรวจสอบความถูกต้องดังนี้

1) รายงานการประเมินช่องโหว่ที่ประเมินพบ
2) รายงานการแก้ไขช่องโหว่ที่ประเมินพบ
3) รายงานการประเมินช่องโหว่ซ้ำ

6. การประเมินประสิทธิภาพกรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กร

งานวิจัยในเรื่อง การพัฒนากรอบการจัดการช่องโหว่ระบบสารสนเทศเพื่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์ กรณีศึกษา กองบัญชาการกองทัพภาคที่ 2 ในครั้งนี้ ได้จัดทำขั้นตอนการประเมินประสิทธิภาพกรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กรขึ้นมาเพื่อเสริมความน่าเชื่อถือ ของกรอบการจัดการช่องโหว่ดังกล่าว เพื่อที่จะได้นำกรอบนี้ไปเป็นหลักการในการปฏิบัติดำเนินงานได้จริง และเป็นจุดเริ่มต้นในก้าวแรกในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ที่เป็นหลักการโดยมีระเบียบและทฤษฎีในการปฏิบัติรองรับ โดยขั้นตอนการประเมินประสิทธิภาพกรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กร มีรายละเอียดดังนี้

6.1 การกำหนดเกณฑ์พิจารณาระดับค่าคะแนน

6.1.1 การกำหนดระดับค่าคะแนนของแบบประเมินประสิทธิภาพระดับคะแนนของมาตรวัดตามมาตราส่วนประมาณค่ากำหนดระดับค่าคะแนนในการตอบแบบประเมินประสิทธิภาพเกี่ยวกับกรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กร 5 ระดับดังนี้

ระดับมากที่สุด ให้น้ำหนักคะแนนเป็น 5 คะแนน

ระดับมาก ให้น้ำหนักคะแนนเป็น 4 คะแนน

ระดับปานกลาง ให้น้ำหนักคะแนนเป็น 3 คะแนน

ระดับน้อย ให้น้ำหนักคะแนนเป็น 2 คะแนน

ระดับน้อยที่สุด ให้น้ำหนักคะแนนเป็น 1 คะแนน

6.1.2 การแปลความหมายระดับค่าคะแนนเฉลี่ยของแบบประเมินประสิทธิภาพ การแปลความหมายระดับค่าคะแนนเฉลี่ยของข้อมูลที่เก็บได้จากแบบประเมินประสิทธิภาพข้อมูลวัดมาตราส่วนประมาณค่าพิจารณาตามช่วงคะแนนสำหรับการแปลผลดังนี้

ระดับคะแนนเฉลี่ย 4.50 - 5.00 หมายถึง มีระดับมากที่สุด

ระดับคะแนนเฉลี่ย 3.50 - 4.49 หมายถึง มีระดับมาก

ระดับคะแนนเฉลี่ย 2.50 - 3.49 หมายถึง มีระดับปานกลาง

ระดับคะแนนเฉลี่ย 1.50 - 2.49 หมายถึง มีระดับน้อย

ระดับคะแนนเฉลี่ย 1.00 - 1.49 หมายถึง มีระดับน้อยที่สุด

6.1.3 การแปลความหมายระดับค่าคะแนนเฉลี่ยของดัชนีความสอดคล้องของข้อคำถามระดับค่าคะแนนดัชนีความสอดคล้องของข้อคำถามที่ใช้ในการสอบถามความคิดเห็นจากผู้ที่เกี่ยวข้องกับระบบสารสนเทศ กองบัญชาการกองทัพภาคที่ 2 โดยใช้การแปลความหมายระดับค่าคะแนนเฉลี่ยเป็น 2 ระดับ ดังนี้

ระดับคะแนนเฉลี่ย -1.00 - 0.49 หมายถึง มีระดับความสอดคล้องไม่เหมาะสม

ระดับคะแนนเฉลี่ย 0.50 - 1.00 หมายถึง มีระดับความสอดคล้องเหมาะสม

6.2 สถิติในการวิเคราะห์ข้อมูล

การวิเคราะห์ข้อมูลการวิจัย ดำเนินการโดยนำข้อมูลจากการตอบแบบสอบถามการประเมินประสิทธิภาพ กรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กร มาวิเคราะห์แล้วประเมินผลข้อมูลโดยใช้โปรแกรมสำเร็จรูป Microsoft Excel เพื่อใช้ในการวิเคราะห์และรายงานผลค่าทางสถิติและประมวลผลหาความสัมพันธ์ทางสถิติด้วยระดับความเชื่อมั่น 95 เปอร์เซ็นต์ และมีความคลาดเคลื่อนที่ยอมรับได้ 0.05 เปอร์เซ็นต์เป็นเกณฑ์ในการยอมรับหรือปฏิเสธสมมติฐานในการศึกษาสถิติที่ใช้ในการวิเคราะห์

1) ค่าเฉลี่ย หาค่าเฉลี่ยของคะแนนการประเมินโดยคำนวณจากสูตร ดังนี้

$$\bar{x} = \frac{\sum x}{n}$$

เมื่อ $\bar{x}$ แทน ค่าเฉลี่ย

$\sum x$ แทน ผลรวมของคะแนนทั้งหมด

n แทน จำนวนข้อมูลทั้งหมด

2) ส่วนเบี่ยงเบนมาตรฐาน (Standard Deviation) คำนวณจากสูตรดังนี้

$$S.D. = \sqrt{\frac{\sum(x - \bar{x})^2}{n - 1}}$$

เมื่อ $S.D.$ แทน ส่วนเบี่ยงเบนมาตรฐาน

x แทน ค่าของข้อมูลแต่ละตัว

$\bar{x}$ แทน ค่าเฉลี่ยของกลุ่มตัวอย่าง

n แทน จำนวนตัวอย่าง

7. ระยะเวลาและขั้นตอนในการดำเนินงาน

รายการ	เวลา (เดือน) มี.ค. 65	เม.ย. 65	พ.ค. 65	มิ.ย. 65	ก.ค. 65	ส.ค. 65	ก.ย. 65
1. ศึกษาข้อมูล ทฤษฎี และงานวิจัยที่เกี่ยวข้องกับการประเมินความเสี่ยงช่องโหว่ระบบสารสนเทศ	→	→					
2. การรวบรวมข้อมูลเกี่ยวกับคุณลักษณะของระบบที่จะทำการประเมินความเสี่ยง		→	→				
3. การพัฒนากรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กร			→	→			
4. ดำเนินการทดลองตามกรอบการจัดการช่องโหว่สารสนเทศขององค์กรที่พัฒนาขึ้นมา				→	→		
5. ผลลัพธ์จากการดำเนินงาน					→	→	
6. การสรุปผลการวิจัย						→	→

บทที่ 4
ผลการวิเคราะห์ข้อมูล

ผลการดำเนินงานจากการทดลองตามวิธีการดำเนินการวิจัย การพัฒนากรอบการจัดการช่องโหว่ระบบสารสนเทศเพื่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์ กรณีศึกษา กองบัญชาการกองทัพภาคที่ 2 พบว่าอุปกรณ์ระบบสารสนเทศเป้าหมายที่ทำงานวิจัยในครั้งนี้มีช่องโหว่ที่ประเมินพบอยู่จำนวนหลายช่องโหว่ด้วยกัน โดยมีความเสี่ยงจากการประเมินความเสี่ยงช่องโหว่ที่ส่งผลกระทบต่อองค์กรแตกต่างกันไปตามคุณลักษณะของช่องโหว่นั้นๆ รวมถึงวิธีแก้ไขช่องโหว่ที่เกิดจะต้องแก้ไขรูปแบบใด ซึ่งผู้วิจัยได้สรุปผลการดำเนินการจากวิธีการดำเนินการวิจัยรายละเอียดดังนี้

1. การจัดการทรัพย์สิน (Assets Management)

จากการรวบรวมอุปกรณ์สารสนเทศ (Discovering) และการประเมินระดับผลกระทบต่อองค์กรของอุปกรณ์สารสนเทศ (Assets Assessment) นำมาซึ่งผล การจัดลำดับความสำคัญอุปกรณ์สารสนเทศตามผลกระทบต่อองค์กร (Assets Prioritization) เพื่อกำหนดอุปกรณ์สารสนเทศขององค์กร เข้ารับการประเมินช่องโหว่ มีอุปกรณ์สารสนเทศเข้ารับการประเมินช่องโหว่ตามตารงที่ 4.1 ดังนี้

ตารางที่ 4.1 อุปกรณ์สารสนเทศที่เข้ารับการประเมินช่องโหว่

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

2. การประเมิน (Assessment)

2.1 การประเมินช่องโหว่ (Vulnerability Assessment)

สรุปผลการดำเนินการประเมินช่องโหว่ ระบบเทคโนโลยีสารสนเทศขององค์กร ที่ได้จากเครื่องมือทั้ง 2 พบว่าเครื่องสแกนช่องโหว่ Nexpose ตรวจพบช่องโหว่ได้มากกว่า Nessus ผู้วิจัยจึงได้สรุปรวมช่องโหว่ของทั้งสองเครื่องมือตรวจสอบช่องโหว่ดังกล่าว โดยนำช่องโหว่ที่ประเมินพบว่าเป็นช่องโหว่ที่ซ้ำกันบนอุปกรณ์เครื่องแม่ข่ายเดียวกันออก จะนับเป็นแค่ช่องโหว่ผลการประเมินช่องโหว่ที่รวบรวมจากการสแกนช่องโหว่ของทั้งสองเครื่องมือดังที่ได้อธิบายไว้ในหัวข้อที่ 3. จากบทที่ 3 มีรายละเอียดตามตารางที่ 4.2

ตารางที่ 4.2 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

2.1.1 รายละเอียดช่องโหว่จากการประเมินช่องโหว่ระบบสารสนเทศขององค์กรมีรายละเอียดตามตารางที่ 4.3 ดังนี้

ตารางที่ 4.3 รายละเอียดช่องโหว่จากการประเมินช่องโหว่ระบบสารสนเทศขององค์กร

ลำดับ	ชื่อช่องโหว่	รายละเอียด	ข้อมูลอ้างอิง	อุปกรณ์สารสนเทศ	ข้อมูลความเสี่ยง CVSS	Base Score
1.	SSL Medium Strength Cipher Suites Supported (SWEET32)	โฮสต์ระยะไกลสนับสนุนการใช้การเข้ารหัส SSL ที่มีการเข้ารหัสระดับกลาง ถือว่ามีความรุนแรงปานกลาง เป็นการเข้ารหัสที่ใช้ความยาวของกุญแจ (มากกว่า 64 บิต และน้อยกว่า 112 บิต key, or 3DES)	1. tenable plugins #42873 2. CVE: CVE-2016-2183	AMC Server Por :443 / tcp / www	CVSS v3.0 Base Score 7.5 CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N	High
2.	TLS Version 1.0 Protocol Detection	การเชื่อมต่อที่เข้ารหัสโดยใช้ TLS 1.0 มีข้อบกพร่องในการออกแบบการเข้ารหัสจำนวนมาก	1. tenable plugins #104743	AMC Server Port: 443 / tcp / www	CVSS v3.0 Base Score 6.5 CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N	Medium
3.	TLS Version 1.1 Protocol Deprecated	การเชื่อมต่อที่เข้ารหัสโดยใช้ TLS 1.1 มีข้อบกพร่องในการออกแบบการเข้ารหัสจำนวนมาก	1. tenable plugins #157288	AMC Server Port: 443 / tcp / www	CVSS v3.0 Base Score 6.5 CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N	Medium

ตารางที่ 4.3 (ต่อ)

ลำดับ	ชื่อช่องโหว่	รายละเอียด	ข้อมูลอ้างอิง	อุปกรณ์สารสนเทศ	ข้อมูลความเสี่ยง CVSS	Base Score
4.	Nameserver Processes Recursive Queries	การอนุญาตให้ Nameserver ประมวลผลการสืบค้นแบบเรียกซ้ำที่มาจากระบบอื่นๆ ในบางสถานการณ์ อาจถูกผู้โจมตีดำเนินการโจมตีแคชซึ่งทำให้เกิดการหยุดให้บริการของเครื่องแม่ข่ายได้	1. dns-processes-recursive-queries	AMC Server Port: 53 / UDP	CVSS v2.0 Base Score 5 CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P	Medium
5.	DNS server allows cache snooping	เซิร์ฟเวอร์ DNS นี้อ่อนไหวต่อการสอดแนมแคช DNS โดยที่ผู้โจมตีสามารถสืบค้นข้อมูลแบบไม่เรียกซ้ำไปยังเซิร์ฟเวอร์ DNS โดยมองหาบันทึกที่อาจได้รับการแก้ไขแล้วโดยเซิร์ฟเวอร์ DNS นี้ สำหรับไคลเอ็นต์อื่นๆ ผู้โจมตีสามารถใช้ข้อมูลนี้เพื่อเริ่มการโจมตีอื่นๆ ทั้งนี้ขึ้นอยู่กับการตอบสนอง	1. dns-allows-cache-snooping	AMC Server Port: 53 / UDP / TCP	CVSS v2.0 Base Score 5 CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N	Medium

ตารางที่ 4.3 (ต่อ)

ลำดับ	ชื่อช่องโหว่	รายละเอียด	ข้อมูลอ้างอิง	อุปกรณ์สารสนเทศ	ข้อมูลความเสี่ยง CVSS	Base Score
6.	TLS/SSL Server is enabling the BEAST attack	ผู้โจมตีอาจเข้าถึงการสนทนาระหว่างเว็บเซิร์ฟเวอร์และเว็บเบราว์เซอร์ได้ โดยใช้เทคนิคการโจมตีแบบคนกลาง หากไม่มีการเข้ารหัส จะสามารถเข้าถึงข้อมูลทั้งหมดที่แลกเปลี่ยนระหว่างเว็บเซิร์ฟเวอร์และเว็บเบราว์เซอร์ การเข้ารหัส TLS 1.0 หรือเก่ากว่า สามารถถูกทำลายได้อย่างรวดเร็ว ทำให้ผู้โจมตีมีโอกาสรับฟังการสนทนาหากเซิร์ฟเวอร์รองรับ TLS 1.0 ผู้โจมตีสามารถทำให้เชื่อว่านี่เป็นโพรโทคอลเดียวที่ไคลเอ็นต์สามารถใช้ได้ สิ่งนี้เรียกว่าการโจมตีดาวน์เกรดโพรโทคอล จากนั้นผู้โจมตีสามารถใช้การโจมตีของ BEAST เพื่อดักฟังได้	1. CVE-2011-3389	AMC Server Port: 53 / UDP / TCP	CVSS v2.0 Base Score 4.3 CVSS v2.0 Vector: CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N	Medium

ตารางที่ 4.3 (ต่อ)

ลำดับ	ชื่อช่องโหว่	รายละเอียด	ข้อมูลอ้างอิง	อุปกรณ์สารสนเทศ	ข้อมูลความเสี่ยง CVSS	Base Score
7.	HTTP OPTIONS Method Enabled	เว็บเซิร์ฟเวอร์ที่ตอบสนองต่อเมธอด OPTIONS HTTP จะเปิด เผยวิธีการอื่นๆ ที่เว็บเซิร์ฟเวอร์สนับสนุน วิธีนี้สามารถช่วยให้ผู้โจมตีค้นหาข้อมูลเกี่ยวกับการกำหนดค่าเซิร์ฟเวอร์และเป็นช่องโหวในการโจมตีได้	1. http-options-method-enabled	AMC Server Port: 443 / tcp / www	CVSS v2.0 Base Score 2.6 CVSS v2.0 Vector: CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N	Low
8.	TLS/SSL Server Supports The Use of Static Key Ciphers	เซิร์ฟเวอร์ได้รับการกำหนดค่าให้รองรับการเข้ารหัสที่เรียกว่ารหัสลับแบบคงที่ รหัสเหล่านี้ไม่รองรับ "Forward Secrecy" ในข้อ กำหนดใหม่สำหรับ HTTP/2 การเข้ารหัสเหล่านี้ถูกขึ้นบัญชีดำ	1. ssl-static-key-ciphers	AMC Server Port: 443 / tcp / www	CVSS v2.0 Base Score 2.6 CVSS v2.0 Vector: CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N	Low
9.	FTP credentials transmitted unencrypted	เซิร์ฟเวอร์สนับสนุนวิธีการรับรองความถูกต้องโดยข้อมูลประจำตัวจะถูกส่งเป็นข้อความธรรมดาผ่านช่องทางที่ไม่ได้เข้ารหัส หากผู้โจมตีสกัดกั้นการรับส่งข้อมูลระหว่างไคลเอนต์และเซิร์ฟเวอร์นี้ ข้อมูลประจำตัวจะถูกเปิดเผย	1. ftp-plaintext-auth	WEB Server Port: 21 / TCP	CVSS v2.0 Base Score 7.3 CVSS v2.0 Vector: CVSS2#AV:A/AC:M/Au:N/C:C/I:C/A:N	High

ตารางที่ 4.3 (ต่อ)

ลำดับ	ชื่อช่องโหว่	รายละเอียด	ข้อมูลอ้างอิง	อุปกรณ์สารสนเทศ	ข้อมูลความเสี่ยง CVSS	Base Score
10.	X.509 Certificate Subject CN Does Not Match the Entity Name	ในการตรวจจับและป้องกันการโจมตีแบบแอบฟัง จะต้องตรวจสอบความถูกต้องของใบรับรอง ไม่เช่นนั้นผู้โจมตีอาจเปิดการโจมตีแบบคนกลางและเข้าควบคุมสตรีมข้อมูลได้อย่างเต็มที่ สิ่งที่สำคัญเป็นพิเศษคือความถูกต้องของ CN ของหัวเรื่อง ซึ่งควรตรงกับชื่อของเอนทิตี (ชื่อโฮสต์)	1. certificate-common-name-mismatch	WEB Server Port: 21 / TCP	CVSS v2.0 Base Score 7.1 CVSS v2.0 Vector: CVSS2#AV:N/AC:H/Au:N/C:C/I:C/A:N	High
11.	SSL Certificate Cannot Be Trusted	SSL Certificate มีลายมือชื่อดิจิทัลที่ไม่เป็นที่ยอมรับหรือมีการจัดทำ Certificate โดยหน่วยงานที่ไม่เป็นที่ยอมรับในระดับสากล	1. tenable plugins #51192	WEB Server Port: 21 / tcp / ftp	CVSS v3.0 Base Score 6.5 CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N	Medium
12.	SSL Self-Signed Certificate	SSL Certificate มีลายมือชื่อดิจิทัลที่ไม่เป็นที่ยอมรับหรือมีการจัดทำ Certificate โดยหน่วยงานที่ไม่เป็นที่ยอมรับในระดับสากล	1. tenable plugins #57582	WEB Server Port: 21 / tcp / ftp	CVSS v3.0 Base Score 6.5 CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N	Medium

ตารางที่ 4.3 (ต่อ)

ลำดับ	ชื่อช่องโหว่	รายละเอียด	ข้อมูลอ้างอิง	อุปกรณ์สารสนเทศ	ข้อมูลความเสี่ยง CVSS	Base Score
13.	Untrusted TLS/SSL server X.509 certificate	SSL Certificate มีลายมือชื่อดิจิทัลที่ไม่เป็นที่ยอมรับหรือมีการจัดทำ Certificate โดยหน่วยงานที่ไม่เป็นที่ยอมรับในระดับสากล	1. tls-untrusted-ca	WEB Server Port: 21 / 443 / TCP	CVSS v2.0 Base Score 5.8 CVSS v2.0 Vector: CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:N	Medium
14.	Test-cgi Script Information Disclosure Vulnerability	เว็บเซิร์ฟเวอร์สร้างสคริปต์ทดสอบที่เปิดเผยรายละเอียดการกำหนดค่าของเว็บเซิร์ฟเวอร์แก่ใครก็ตามที่สามารถเชื่อมต่อกับเครื่องได้	1. CVE-1999-0070 2. http-apache-0010	WEB Server Port: 888 / 80 / 443 / TCP	CVSS v2.0 Base Score 5 CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N	Medium
15.	Self-signed TLS/SSL certificate on 203.xxx.xxx.xxx	ใบรับรอง TLS/SSL ของเซิร์ฟเวอร์มีการลงชื่อด้วยตนเอง ใบรับรองที่ลงนามเองไม่สามารถเชื่อถือได้ตามค่าเริ่มต้น โดยเฉพาะอย่างยิ่งเนื่องจากการโจมตีโดยคนกลาง TLS/SSL มักใช้ใบรับรองที่ลงนามเองเพื่อดักฟังการเชื่อมต่อ TLS/SSL	1. ssl-self-signed-certificate	WEB Server Port: 21 / TCP	CVSS v2.0 Base Score 4.3 CVSS v2.0 Vector: CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N	Medium
16.	HTTP OPTIONS Method Enabled	เว็บเซิร์ฟเวอร์ที่ตอบสนองต่อเมธอด OPTIONS HTTP จะเปิดเผยวิธีการอื่นๆ ที่เว็บเซิร์ฟเวอร์สนับสนุน วิธีนี้สามารถช่วยให้ผู้โจมตีค้นหาข้อมูลเกี่ยวกับการกำหนดค่าเซิร์ฟเวอร์และเป็นช่องโหว่ในการโจมตีได้	1. http-options-method-enabled	WEB Server Port: 888 / TCP	CVSS v2.0 Base Score 2.6 CVSS v2.0 Vector: CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N	Low

ตารางที่ 4.3 (ต่อ)

ลำดับ	ชื่อช่องโหว่	รายละเอียด	ข้อมูลอ้างอิง	อุปกรณ์สารสนเทศ	ข้อมูลความเสี่ยง CVSS	Base Score
17.	TLS/SSL Server Supports The Use of Static Key Ciphers	เซิร์ฟเวอร์ได้รับการกำหนดค่าให้รองรับการเข้ารหัสที่เรียกว่ารหัสลับแบบคงที่ รหัสเหล่านี้ไม่รองรับ "Forward Secrecy" ในข้อกำหนดใหม่สำหรับ HTTP/2 การเข้ารหัสเหล่านี้ถูกขึ้นบัญชีดำ	1. ssl-static-key-ciphers	WEB Server Port: 443 / TCP CATEGORIES: Network	CVSS v2.0 Base Score 2.6 CVSS v2.0 Vector: CVSS2# AV:N/AC:H/Au:N/C:P/I:N/A:N	Low
18.	Unix Operating System Unsupported Version Detection	การขาดการสนับสนุนหมายความว่าผู้ผลิตจะไม่ออกแพตช์ความปลอดภัยใหม่สำหรับผลิตภัณฑ์ ดังนั้นจึงมีแนวโน้มที่จะมีช่องโหว่ด้านความปลอดภัย	1. tenable plugins #33850 2. IAVA: 0001-A-0502, 0001-A-0648	OpenMCU 1	CVSS v3.0 Base Score 10.0 CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/ C:H/I:H/A:H	High
19.	SSH Birthday attacks on 64-bit block ciphers (SWEET32)	รหัสบล็อกดั้งเดิมที่มีขนาดบล็อก 64 บิตมีความเสี่ยงที่จะเกิดการชนกันในทางปฏิบัติเมื่อใช้ในโหมด Cipher Block Chaining (CBC) ความปลอดภัยของรหัสบล็อกมักจะลดลงเหลือขนาดกุญแจ เข้ารหัส เป็นไปได้ที่จะใช้การชนกันเพื่อดึงข้อมูลข้อความธรรมดา	1. CVE: CVE-2016-2183	OpenMCU 1 Port: 22 / tcp	CVSS v3.0 Base Score 7.5 CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/ C:H/I:N/A:N	High
20.	Unencrypted Telnet Server	โฮสต์ระยะไกลกำลังเรียกใช้เซิร์ฟเวอร์ Telnet ผ่านช่องทางที่ไม่ได้เข้ารหัส	1. tenable plugins #42263	OpenMCU 1 Port: 1423 / tcp / telnet	CVSS v3.0 Base Score 6.5 CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C :L/I:L/A:N	Medium

ตารางที่ 4.3 (ต่อ)

ลำดับ	ชื่อช่องโหว่	รายละเอียด	ข้อมูลอ้างอิง	อุปกรณ์สารสนเทศ	ข้อมูลความเสี่ยง CVSS	Base Score
21.	SSH Weak Algorithms Supported	Nessus ตรวจพบว่าเซิร์ฟเวอร์ ที่ให้บริการ SSH ระยะไกลได้กำหนดค่าการใช้รหัส Arcfour หรือไม่มีรหัสเลย ซึ่งการเข้า Arcfour เป็นการเข้ารหัสที่อ่อนแอ	1. tenable plugins #90317	OpenMCU 1 Port: 22 / tcp / ssh	CVSS v2.0 Base Score: 4.3 CVSS v2.0 Vector: CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N	Medium
22.	SSH Server Supports RC4 Cipher Algorithms	เซิร์ฟเวอร์ที่ให้บริการ SSH ระยะไกลได้กำหนดค่าการเข้ารหัส Arcfour หรือ RC4 เป็นการเข้ารหัสที่อ่อนแอ ถูกถอดรหัสได้ง่าย	1. ssh-rc4-ciphers	OpenMCU 1 Port: 22 / tcp	CVSS v2.0 Base Score: 4.3 CVSS v2.0 Vector: CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N	Medium
23.	SSH Server Supports diffie-hellman-group1-sha1	โมดูลัสเฉพาะที่เสนอเมื่อใช้ diffie-hellman-group1-sha1 มีขนาด 1024 บิตเท่านั้น ขนาดนี้ถือว่าอ่อนแอและอยู่ในขอบเขตทางทฤษฎีของการโจมตีที่เรียกว่า Logjam	1. CVE: CVE-2015-4000	OpenMCU 1 Port: 22 / tcp	CVSS v3.0 Base Score 3.7 CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N	Medium
24.	SSH Weak Key Exchange Algorithms Enabled	เซิร์ฟเวอร์ SSH ระยะไกลได้รับการกำหนดค่าให้อนุญาตอัลกอริทึมการแลกเปลี่ยนกุญแจซึ่งถือว่าอ่อนแอ	1. tenable plugins #1539537	OpenMCU 1 Port: 22 / tcp / ssh	CVSS v3.0 Base Score 3.7 CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N	Low

ตารางที่ 4.3 (ต่อ)

ลำดับ	ชื่อช่องโหว่	รายละเอียด	ข้อมูลอ้างอิง	อุปกรณ์สารสนเทศ	ข้อมูลความเสี่ยง CVSS	Base Score
25.	SSH Server CBC Mode Ciphers Enabled	เซิร์ฟเวอร์ SSH รับการกำหนดค่าให้รองรับการเข้ารหัส Cipher Block Chaining (CBC) อาจทำให้ผู้โจมตีสามารถกู้คืนข้อความธรรมดาจากข้อความไซเฟอร์เท็กซ์ได้	1. tenable plugins #70658	OpenMCU 1 Port: 22 / tcp / ssh	CVSS v2.0 Base Score: 2.6 CVSS v2.0 Vector: CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N	Low
26.	SSH Weak MAC Algorithms Enabled	เซิร์ฟเวอร์ SSH ระยะไกลได้รับการกำหนดค่าให้อนุญาตอัลกอริทึม MD5 และ MAC 96 บิต ซึ่งทั้งสองอย่างนี้ถือว่าอ่อนแอ	1. tenable plugins #71049	OpenMCU 1 Port: 22 / tcp / ssh	CVSS v2.0 Base Score: 2.6 CVSS v2.0 Vector: CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N	Low
27.	X.509 Certificate Subject CN Does Not Match the Entity Name	การป้องกันการโจมตีแบบแอบฟังจะ ต้องตรวจสอบความถูกต้องของใบรับรอง เพราะผู้โจมตีอาจเปิดการโจมตีแบบคนกลางและเข้าควบคุมข้อมูลได้ สิ่งที่สำคัญคือความถูกต้องของ CN ของหัวเรื่อง ซึ่งควรตรงกับชื่อของเอนทิตี (ชื่อโฮสต์)	1. certificate-common-name-mismatch	VPN PPTP Port: 4444 / TCP	CVSS v2.0 Base Score 7.1 CVSS v2.0 Vector: CVSS2#AV:N/AC:H/Au:N/C:C/I:C/A:N	High
28.	SSL Certificate Cannot Be Trusted	SSL Certificate มีลายมือชื่อดิจิทัลที่ไม่เป็นที่ยอมรับหรือมีการจัดทำ Certificate โดยหน่วยงานที่ไม่เป็นที่ยอมรับในระดับสากล	1. tenable plugins #51192	VPN PPTP Port: 4444 / tcp / www	CVSS v3.0 Base Score 6.5 CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N	Medium

ตารางที่ 4.3 (ต่อ)

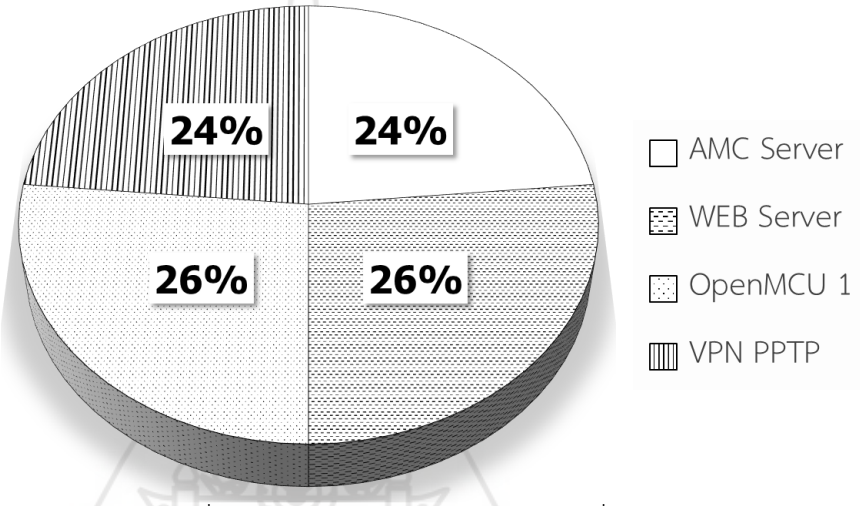
ลำดับ	ชื่อช่องโหว่	รายละเอียด	ข้อมูลอ้างอิง	อุปกรณ์สารสนเทศ	ข้อมูลความเสี่ยง CVSS	Base Score
29.	SSL Self-Signed Certificate	SSL Certificate มีลายมือชื่อดิจิทัลที่ไม่เป็นที่ยอมรับหรือมีการจัดทำ Certificate โดยหน่วยงานที่ไม่เป็นที่ยอมรับในระดับสากล	1. tenable plugins #57582	VPN PPTP Port: 4444 / tcp / www	CVSS v3.0 Base Score 6.5 CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N	Medium
30.	TLS Version 1.1 Protocol Deprecated	การเชื่อมต่อที่เข้ารหัสโดยใช้ TLS 1.1 มีข้อบกพร่องในการออกแบบการเข้ารหัสจำนวนมาก	1. tenable plugins #157288	VPN PPTP Port: 4444 / tcp / www	CVSS v3.0 Base Score 6.5 CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N	Medium
31.	Untrusted TLS/SSL server X.509 certificate	ใบรับรอง TLS/SSL ของเซิร์ฟเวอร์ได้รับการลงนามโดยผู้ออกใบรับรอง (CA) ที่ไม่เป็นที่รู้จักหรือไม่น่าเชื่อถือ กรณีนี้อาจเกิดขึ้นได้จากใบรับรองหมดอายุหรือถูกเพิกถอน ชื่อโฮสต์ของเซิร์ฟเวอร์ไม่ตรงกับที่กำหนดค่าไว้ในใบรับรอง เวลา/วันที่ไม่ถูกต้อง หรือใช้ใบรับรองที่ลงนามเอง	1.tls-untrusted-ca	VPN PPTP Port: 4444 / tcp	CVSS v2.0 Base Score 5.8 CVSS v2.0 Vector: CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:N	Medium
32.	TLS Server Supports TLS version 1.1	การเชื่อมต่อที่การเข้ารหัสที่รุ่นต่ำกว่า TLS 1.1 มีข้อบกพร่องในการออกแบบการเข้ารหัสจำนวนมาก	1. tlsv1_1-enabled	VPN PPTP Port: 4444 / tcp	CVSS v2.0 Base Score 2.6 CVSS v2.0 Vector: CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N	Low

ตารางที่ 4.3 (ต่อ)

ลำดับ	ชื่อช่องโหว่	รายละเอียด	ข้อมูลอ้างอิง	อุปกรณ์สารสนเทศ	ข้อมูลความเสี่ยง CVSS	Base Score
33.	TLS/SSL Server Supports The Use of Static Key Ciphers	เซิร์ฟเวอร์ได้รับการกำหนดค่าให้รองรับการเข้ารหัสที่เรียกว่ารหัสลับแบบคงที่ รหัสเหล่านี้ไม่รองรับ "Forward Secrecy" ในข้อกำหนดใหม่สำหรับ HTTP/2 การเข้ารหัสเหล่านี้ถูกขึ้นบัญชีดำ	1. ssl-static-key-ciphers	VPN PPTP Port: 4444 / tcp	CVSS v2.0 Base Score 2.6 CVSS v2.0 Vector: CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N	Low
34.	TLS/SSL Server Is Using Commonly Used Prime Numbers	เซิร์ฟเวอร์ใช้หมายเลขเฉพาะทั่วไปหรือค่าเริ่มต้นเป็นพารามิเตอร์ระหว่างการแลกเปลี่ยนกุญแจ Diffie-Hellman สิ่งนี้ทำให้เซสชั่นที่ปลอดภัยเสี่ยงต่อการโจมตีด้วยการคำนวณล่วงหน้า ผู้โจมตีสามารถใช้เวลาจำนวนมากเพื่อสร้างการค้นหา	1. tls-dh-primes	VPN PPTP Port: 4444 / tcp	CVSS v2.0 Base Score 2.6 CVSS v2.0 Vector: CVSS2#AV:N/AC:H/Au:N/C:N/I:P/A:N	Low

จากตารางที่ 4.3 จำนวนช่องโหว่ที่ประเมินพบของแต่ละอุปกรณ์ระบบสารสนเทศขององค์กร มีจำนวนช่องโหว่ตามอุปกรณ์เครื่องแม่ข่ายที่เข้ารับการประเมินดังนี้

- เครื่องแม่ข่าย AMC Server พบช่องโหว่จำนวน 8 ช่องโหว่
- เครื่องแม่ข่าย WEB Server พบช่องโหว่จำนวน 9 ช่องโหว่
- เครื่องแม่ข่าย OpenMCU 1 พบช่องโหว่จำนวน 9 ช่องโหว่
- เครื่องแม่ข่าย VPN PPTP พบช่องโหว่จำนวน 8 ช่องโหว่



ภาพที่ 4.1 อัตราส่วนร้อยละของช่องโหว่ที่ประเมินพบ

จากภาพที่ 4.1 จะเห็นได้ว่าจำนวนช่องโหว่ของอุปกรณ์สารสนเทศทั้ง 4 อุปกรณ์มีจำนวนช่องโหว่ที่ใกล้เคียงกัน ซึ่งแสดงให้เห็นว่าการประเมินช่องโหว่ในงานวิจัยในครั้งนี้มีรูปแบบของช่องโหว่คล้ายๆ กัน เครื่องแม่ข่ายที่ให้บริการในด้านระบบเว็บเซิร์ฟเวอร์ เช่น เครื่องแม่ข่าย AMC Server และ เครื่องแม่ข่าย WEB Server จากการประเมินช่องโหว่พบช่องโหว่ชนิด TSL/SSL/X.509 ทั้ง 2 เครื่อง และช่องโหว่ชนิด TSL/SSL/X.509 ยังพบได้ในเครื่องแม่ข่าย VPN PPTP ซึ่งความเป็นจริงแล้ว เครื่องแม่ข่าย VPN PPTP เป็นเครื่องแม่ข่ายที่ไม่ได้ให้บริการเกี่ยวกับเว็บเซิร์ฟเวอร์แต่อย่างใด เป็นเครื่องแม่ข่ายที่ให้บริการในการจัดสรรเข้าใช้งานในระบบสารสนเทศในด้านต่างๆ ขององค์กร จากการประเมินช่องโหว่ของเครื่องแม่ข่าย VPN PPTP พบช่องโหว่ชนิด TSL/SSL/X.509 ผ่านทางพอร์ตหมายเลข 4444 ซึ่งเป็นพอร์ตที่โพรโทคอล TCP ใช้งานในการโอนถ่ายข้อมูล ซึ่งโพรโทคอล TCP จะทำงานในกรณีของการบริการในด้านระบบเว็บเซิร์ฟเวอร์ด้วย จึงเป็นสาเหตุที่ประเมินพบช่องโหว่ชนิด TSL/SSL/X.509 ส่วนช่องโหว่ที่แตกต่างออกไปจากการประเมินช่องโหว่นั้นจะพบอยู่ในเครื่องแม่

ข่าย OpenMCU 1 ที่ให้บริการในการประชุมทางไกลผ่านจอภาพ พบว่าเป็นช่องโหว่ชนิด SSH/Telnet/FTP ซึ่งเป็นโพรโทคอลสำหรับการเข้าใช้งานและโอนถ่ายข้อมูลจากระยะไกล สรุปได้ว่าเครื่องแม่ข่ายที่มีช่องโหว่คล้ายๆ กัน เป็นเครื่องแม่ข่ายที่ให้บริการในด้านระบบเว็บเซิร์ฟเวอร์ ดังนี้ AMC Server WEB Server ส่วน VPN PPTP มีช่องโหว่ที่คล้ายกันก็จริง แต่ไม่ได้ให้บริการเว็บเซิร์ฟเวอร์แต่อย่างใด สำหรับเครื่องแม่ข่ายที่มีช่องโหว่ที่แตกต่างไปจากเครื่องแม่ข่ายอื่นๆ คือเครื่องแม่ข่าย OpenMCU 1 ทั้งนี้ช่องโหว่ต่างๆ ที่ประเมินพบก็ขึ้นอยู่กับลักษณะการให้บริการของเครื่องแม่ข่ายนั้นๆ ด้วย

2.1.2 จากการประเมินช่องโหว่ของเครื่องแม่ข่ายระบบสารสนเทศขององค์กร ตามตารางที่ 4.3 พบเพิ่มเติมว่ามีช่องโหว่รูปแบบและลักษณะเดียวกัน จะมีชื่อช่องโหว่ซ้ำกันแต่จะเป็นช่องโหว่ที่อยู่บนเครื่องแม่ข่ายที่ต่างกันดังตารางที่ 4.4

ตารางที่ 4.4 ช่องโหว่ที่ซ้ำกันในการประเมินช่องโหว่อุปกรณ์เครื่องแม่ข่าย

ชื่อช่องโหว่	**รายละเอียดช่องโหว่**	**อุปกรณ์เครื่องแม่ข่ายที่ช่องโหว่ซ้ำ**	**ข้อมูลความเสี่ยง CVSS**	**ระดับความรุนแรง (Base Score)**
1. TLS Version 1.1 Protocol Deprecated	การเชื่อมต่อที่เข้ารหัสโดยใช้ TLS 1.1 มีข้อบกพร่องในการออกแบบการเข้ารหัสจำนวนมาก	1. AMC Server Port: 443 / tcp / www 2. VPN PPTP Port: 4444 / tcp / www	CVSS v3.0 Base Score 6.5 CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N	Medium
2. HTTP OPTIONS Method Enabled	เว็บเซิร์ฟเวอร์ที่ตอบสนองต่อเมธอด OPTIONS HTTP จะเปิดเผยวิธีการอื่นๆ ที่เว็บเซิร์ฟเวอร์สนับสนุน วิธีนี้สามารถช่วยให้ผู้โจมตีค้นหาข้อมูลเกี่ยวกับการกำหนดค่าเซิร์ฟเวอร์และเป็นช่องโหว่ในการโจมตีได้	1. AMC Server Port: 443 / tcp / www 2. WEB Server Port: 888 / tcp	CVSS v2.0 Base Score 2.6 CVSS v2.0 Vector: CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N	Low
3. TLS/SSL Server Supports The Use of Static Key Ciphers	เซิร์ฟเวอร์ได้รับการกำหนดค่าให้รองรับการเข้ารหัสที่เรียกว่ารหัสลับแบบคงที่ รหัสเหล่านี้ไม่รองรับ "Forward Secrecy" ในข้อกำหนดใหม่สำหรับHTTP/2 การเข้ารหัสเหล่านี้ถูกขึ้นบัญชีดำ	1. AMC Server Port: 443 / tcp / www 2. WEB Server Port: 443 / tcp 3. VPN PPTP Port: 4444 / tcp	CVSS v2.0 Base Score 2.6 CVSS v2.0 Vector: CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N	Low

ตารางที่ 4.4 (ต่อ)

ชื่อช่องโหว่	รายละเอียดช่องโหว่	อุปกรณ์เครื่องแม่ข่ายที่ช่องโหว่ซ้ำ	ข้อมูลความเสี่ยง CVSS	ระดับความรุนแรง (Base Score)
4. X.509 Certificate Subject CN Does Not Match the Entity Name	การป้องกันการโจมตีแบบแอบฟังจะ ต้องตรวจสอบความถูกต้องของใบรับรอง เพราะผู้โจมตีอาจเปิดการโจมตีแบบคนกลางและเข้าควบคุมข้อมูลได้ สิ่งที่สำคัญคือความถูกต้องของ CN ของหัวเรื่อง ซึ่งควรตรงกับชื่อของเอนทิตี (ชื่อโฮสต์))	1. WEB Server Port: 21 / tcp 2. VPN PPTP Port: 4444 / tcp	CVSS v2.0 Base Score 7.1 CVSS v2.0 Vector: CVSS2#AV:N/AC:H/Au:N/C:C/I:C/A:N	High
5. SSL Certificate Cannot Be Trusted	SSL Certificate มีลายมือชื่อดิจิทัลที่ไม่เป็นที่ยอมรับหรือมีการจัดทำ Certificate โดยหน่วยงานที่ไม่เป็นที่ยอมรับในระดับสากล	1. WEB Server Port: 21 / TCP / FTP 2. VPN PPTP Port: 4444 / TCP / www	CVSS v3.0 Base Score 6.5 CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N	Medium
6. SSL Self-Signed Certificate	SSL Certificate มีลายมือชื่อดิจิทัลที่ไม่เป็นที่ยอมรับหรือมีการจัดทำ Certificate โดยหน่วยงานที่ไม่เป็นที่ยอมรับในระดับสากล	1. WEB Server Port: 21 / TCP / FTP 2. VPN PPTP Port: 4444 / TCP / www	CVSS v3.0 Base Score 6.5 CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N	Medium

ตารางที่ 4.4 (ต่อ)

ชื่อช่องโหว่	รายละเอียดช่องโหว่	อุปกรณ์เครื่องแม่ข่ายที่ช่องโหว่ซ้ำ	ข้อมูลความเสี่ยง CVSS	ระดับความรุนแรง (Base Score)
7. Untrusted TLS/SSL server X.509 certificate	ใบรับรอง TLS/SSL ของเซิร์ฟเวอร์ได้รับการลงนามโดยผู้ออกใบรับรอง (CA) ที่ไม่เป็นที่รู้จักหรือไม่น่าเชื่อถือ กรณีนี้อาจเกิดขึ้นได้จาก ใบรับรองหมดอายุหรือถูกเพิกถอน ชื่อโฮสต์ของเซิร์ฟเวอร์ไม่ตรงกับที่กำหนดค่าไว้ในใบรับรอง เวลา/วันที่ไม่ถูกต้อง หรือใช้ใบรับรองที่ลงนามเอง	1. WEB Server Port: 21 / 443 / TCP 2. VPN PPTP Port: 4444 / TCP	CVSS v2.0 Base Score 5.8 CVSS v2.0 Vector: CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:N	Medium

จากตารางที่ 4.4 พบว่ามีช่องโหว่ที่ประเมินซ้ำกันจำนวน 7 ช่องโหว่ ช่องโหว่ที่ซ้ำกันนั้นเป็นช่องโหว่ชนิดหรือรูปแบบเดียวกัน ส่วนมากจะเป็นช่องโหว่ที่ประเมินได้จากเครื่องแม่ข่ายที่ให้บริการเว็บไซต์ หรือเว็บเซิร์ฟเวอร์ จากการตรวจสอบพบว่าช่องโหว่ที่ซ้ำกันนั้นมีค่าระดับความรุนแรง (BASE SCORE) ที่เท่ากัน และค่าคำนวณความเสี่ยง (CVSS VECTOR) ที่เท่ากัน โดยแตกต่างเฉพาะพอร์ตหมายเลข ขึ้นอยู่กับเครื่องแม่ข่ายนั้นๆ จะใช้พอร์ตใดในการให้บริการ

2.1.3 การวิเคราะห์ช่องโหว่จากการประเมินช่องโหว่ระบบสารสนเทศขององค์กร

จากผลการประเมินช่องโหว่ในตารางที่ 4.3 สามารถนำเอาข้อมูลมาวิเคราะห์เพื่อให้ทราบถึงรายละเอียดในด้านต่างๆ ของช่องโหว่ที่ประเมินพบ สามารถอธิบายได้ดังนี้

1) รูปแบบชนิดช่องโหว่ รายละเอียดช่องโหว่ที่ประเมินทั้ง 4 อุปกรณ์พบว่ามีช่องโหว่ที่แตกต่างกันไปตามลักษณะรูปแบบของโพรโทคอลที่เกี่ยวข้องกับช่องโหว่ที่ประเมินพบ โดยช่องโหว่ที่พบแบ่งได้ตามประเภทของช่องโหว่ตามตารางที่ 4.5 ดังนี้

ตารางที่ 4.5 รูปแบบและลักษณะโพรโทคอลที่เกี่ยวข้องกับช่องโหว่ที่ประเมินพบ

ชื่อช่องโหว่	ชนิดรูปแบบช่องโหว่					
	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				
X.509 Certificate Subject CN Does Not Match the Entity Name	1					
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				
SSH Weak MAC Algorithms Enabled		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					
ผลการประเมินช่องโหว่จำนวนทั้งสิ้น 34 ช่องโหว่	**18**	**10**	**2**	**1**	**1**	**2**

1.1) TLS/SSL/X.509 เป็นโพรโทคอลที่เกี่ยวข้องกับการสร้างการเชื่อมโยงที่พิสูจน์ตัวตนและเข้ารหัสระหว่างคอมพิวเตอร์เครือข่าย โพรโทคอล TLS/SSL จะเข้ารหัสการรับส่งข้อมูลทางอินเทอร์เน็ตทุกประเภท จึงทำให้การส่งข้อมูลบนอินเทอร์เน็ตปลอดภัย และยังเกี่ยวข้องกับใบรับรองดิจิทัล (certificate) ใบรับรอง TLS/SSL (หรือเรียกอีกอย่างว่า TLS หรือ SSL /TLS certificate) เป็นเอกสารดิจิทัลที่ผูกข้อมูลประจำตัวของเว็บไซต์กับคู่กุญแจการเข้ารหัสซึ่งประกอบด้วยกุญแจสาธารณะและกุญแจส่วนตัว กุญแจสาธารณะที่รวมอยู่ในใบรับรองช่วยให้เว็บเบราว์เซอร์สามารถ เริ่มต้น เซสชั่นการสื่อสารที่เข้ารหัสกับเว็บเซิร์ฟเวอร์ผ่านไฟล์ TLS และ HTTPS โพรโทคอล กุญแจส่วนตัวจะถูกเก็บไว้อย่างปลอดภัยบนเซิร์ฟเวอร์และใช้เพื่อเซ็นชื่อแบบดิจิทัลหน้าเว็บและเอกสารอื่น ๆ ใบรับรอง TLS/SSL ยังรวมถึงการระบุข้อมูลเกี่ยวกับเว็บไซต์รวมถึงชื่อโดเมนและระบุข้อมูลเกี่ยวกับเจ้าของเว็บไซต์อีกทางเลือกหนึ่ง หากใบรับรอง TLS/SSL ของเว็บเซิร์ฟเวอร์ลงนามโดยผู้ออกใบรับรอง (Certificate Authority : CA) ที่เชื่อถือได้แบบสาธารณะ เนื้อหาที่เซ็นชื่อแบบดิจิทัลจากเซิร์ฟเวอร์จะได้รับความไว้วางใจจากเว็บเบราว์เซอร์และระบบปฏิบัติการของผู้ใช้ปลายทางว่าเป็นเซิร์ฟเวอร์ ใบรับรอง TLS/SSL คือประเภทของ ใบรับรอง X.509 ตัวอย่างช่องโหว่ที่เกิดกับโพรโทคอล เช่น โพรโทคอล TLS 1.2 มีความเสี่ยงเป็นพิเศษต่อการโจมตีผู้ไม่หวังดี หรือแฮกเกอร์จะดักจับแพ็กเก็ตข้อมูลในช่วงกลางของเซสชั่น และส่งแพ็กเก็ตเหล่านั้นหลังจากอ่านหรือแก้ไขแพ็กเก็ตก่อให้เกิดความเสียหายต่อข้อมูลได้ ซึ่งต้องแก้ไขด้วยการเปิดใช้ โพรโทคอล TLS 1.3 แทนโพรโทคอล TLS 1.2 เป็นต้น

1.2) SSH/FTP/TELNET เป็นโพรโทคอล หรือแอปพลิเคชัน โพรโทคอลเกี่ยวข้องกับการติดต่อระยะไกล (Remote) การส่งข้อมูลหรือโอนถ่ายข้อมูลจากระยะไกล การขอเข้าใช้งานจากระยะไกล ระบบการรักษาความปลอดภัยก็แตกต่างกันตามโพรโทคอล การโจมตีช่องโหว่ที่เกิดขึ้นเช่น ผู้โจมตีใช้การดักขโมยข้อมูลระหว่างไคลเอ็นต์และเซิร์ฟเวอร์ผ่านทางโพรโทคอล telnet ซึ่งข้อมูลที่ดักได้อาจจะเป็นชื่อที่ใช้ Login และรหัสผ่าน ที่ไม่ได้ถูกเข้ารหัสไว้ โดยใช้โปรแกรมประเภท Sniffer ทั่วๆ ไป ดักขโมยชื่อผู้ใช้คือ root และรหัสผ่าน ความเสียหายต่อข้อมูลอย่างมาก วิธีแก้ไขคือยกเลิกการใช้โพรโทคอล telnet โดยใช้โพรโทคอล SSH แทน และใช้ SFTP แทนโพรโทคอลของ FTP

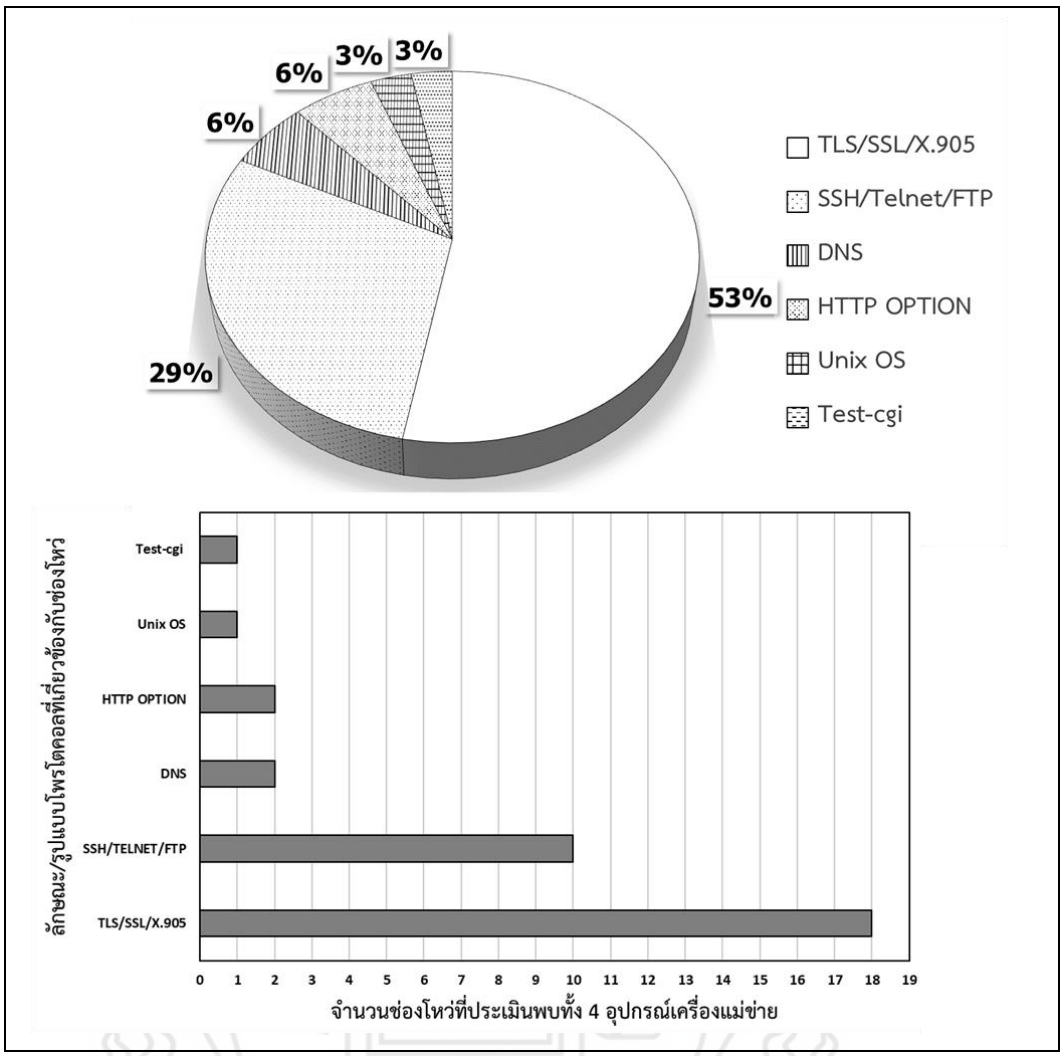
1.3) DNS (Domain Name System หรือ Domain Name Server) คือระบบที่มีไว้สำหรับบริหารจัดการข้อมูลของชื่อโดเมนเนม (Domain Name) และ ทำหน้าที่ในการแปลงชื่อโดเมนเนมดังกล่าวเป็นหมายเลขไอพีแอดเดรส (IP Address) เพื่อนำหมายเลขไอพีดังกล่าวไปติดต่อยัง Sever อื่น ๆ ที่ต้องการต่างๆ เช่น Sever Email Hosting , Server Web Hosting การโจมตีช่องโหว่ที่เกิดขึ้นเช่น การอนุญาตให้ Nameserver ประมวลผลการสืบค้นแบบเรียกซ้ำที่มาจากระบบใดๆ ในบางสถานการณ์ อาจช่วยผู้โจมตีดำเนินการปฏิเสธบริการทำให้เซิร์ฟเวอร์ให้บริการไม่ได้ หรือโจมตีแคชได้จะส่งผลทำให้เซิร์ฟเวอร์ให้บริการไม่ได้

1.4) test-cgi เป็นส่วนหนึ่งของการติดตั้ง Apache เริ่มต้น มีการติดตั้งสคริปต์ cgi-bin เริ่มต้นสองตัวคือ printenv และ test-cgi ได้รวมสคริปต์เหล่านี้ไว้ในการติดตั้งสคริปต์นี้ให้ข้อมูลเกี่ยวกับการติดตั้ง เช่น http://<host name>:<port number>/cgi-bin/test-cgi ซึ่งผู้ไม่หวังดีสามารถนำไปใช้ประโยชน์ในการโจมตีได้

1.5) Unix OS เป็นระบบปฏิบัติการประเภทหนึ่ง ที่เป็นเทคโนโลยีแบบเปิด (Open System) ซึ่งเป็นแนวคิดที่ผู้ใช้ไม่ต้องผูกติดกับระบบใดระบบหนึ่ง หรืออุปกรณ์ยี่ห้อเดียวกัน นอกจากนี้ Unix ยังถูกออกแบบมาเพื่อตอบสนองการใช้งานในลักษณะให้มีผู้ใช้หลายคน ในเวลาเดียวกัน เรียกว่า มัลติยูสเซอร์ (Multiusers) และสามารถทำงานได้หลายๆ งานในเวลาเดียวกัน ลักษณะนี้เรียกว่า มัลติทาสกิ้ง (Multitasking) งานวิจัยนี้เครื่องที่เข้ารับการประเมินช่องโหว่เป็นระบบปฏิบัติการ ลีนุกซ์ (Linux OS) ซึ่งก็มีรากฐานมาจาก Unix OS นั้นเอง จากการประเมินช่องโหว่พบว่าเป็น เวอร์ชัน Linux Kernel 3.0 on Ubuntu 12.04 ที่ไม่มีการอัปเดตแพตช์ฟอร์มความปลอดภัยแล้วจึงทำให้เสี่ยงต่อการถูกโจมตีจากผู้ไม่หวังดีได้

1.6) HTTP OPTION เมธอด OPTIONS บนโพรโทคอล HTTP เป็นเมธอดที่ทำให้ผู้ร้องขอข้อมูลโดยใช้เมธอดดังกล่าวสามารถเห็นได้ว่าเว็บเซิร์ฟเวอร์ให้บริการเข้าถึงข้อมูลด้วยเมธอดใดบ้าง เมื่อเว็บเซิร์ฟเวอร์ได้รับการร้องขอข้อมูลด้วยเมธอด OPTIONS เว็บเซิร์ฟเวอร์จะทำการตอบกลับด้วยข้อความ Allow ด้วยชื่อเมธอดที่สามารถใช้งานได้ เช่น Allow: GET, POST, OPTIONS ซึ่งเป็นข้อมูลที่ผู้ไม่หวังดีสามารถนำไปใช้เป็นข้อมูลในการเข้าโจมตีหรือเจาะระบบของอุปกรณ์สารสนเทศได้

จากช่องโหว่ที่ประเมินพบ จะเห็นได้ว่าจำนวนช่องโหว่ที่เกี่ยวข้องกับโพรโทคอล TTS/SSL ที่ใช้สำหรับเข้ารหัสและป้องกันข้อมูลในขณะที่มีการส่งข้อมูลกันข้าม Internet มีจำนวนช่องโหว่มากที่สุดคิดเป็นร้อยละ 53 ลำดับรองลงมาคือ ช่องโหว่ที่เกี่ยวข้องกับโพรโทคอล SSH/Telnet/FTP ใช้ในการเข้าถึงระบบสารสนเทศจากระยะไกล คิดเป็นร้อยละ 29 ส่วนลำดับอื่นๆ จะมีช่องโหว่ที่ใกล้เคียงเป็นจำนวนน้อยไม่ถึงร้อยละ 10 ตามภาพที่ 4.2



ภาพที่ 4.2 จำนวนและอัตราร้อยละของช่องโหว่ตามกลุ่มโพรโทคอล

จากจำนวนและอัตราร้อยละของกลุ่มช่องโหว่จากกลุ่มช่องโหว่ที่มากที่สุดคือกลุ่มช่องโหว่โพรโทคอล TLS/SSL และรองลงมาคือกลุ่มช่องโหว่โพรโทคอล SSL/Telnet/FTP สามารถวิเคราะห์ได้ว่ากลุ่มช่องโหว่ทั้ง 2 กลุ่มนี้มีโอกาสมากที่สุดที่จะถูกโจมตีจากผู้ไม่หวังดี และจะส่งผลกระทบและมีความเสี่ยงมากที่สุดต่อระบบสารสนเทศขององค์กร จึงควรพิจารณาและหาวิธีแก้ไขให้ได้มากที่สุด

2) รายละเอียดช่องโหว่ที่ประเมินแยกตามอุปกรณ์เครื่องแม่ข่าย พบว่ามีช่องโหว่ที่เกี่ยวข้องกับ พอร์ต (Port) ที่เปิดให้บริการ และระดับความรุนแรงของช่องโหว่ ที่แตกต่างกันไปตามรูปแบบของอุปกรณ์เครื่องแม่ข่ายที่นำมารับการประเมินช่องโหว่ ตามตารางที่ 4.6 ถึง 4.9 ดังนี้

ตารางที่ 4.6 รายละเอียดการประเมินช่องโหว่ที่พบเครื่องแม่ข่าย AMC Server

ลำดับ	ชื่อช่องโหว่	AMC Server อุปกรณ์สารสนเทศ	ระดับความรุนแรง (Base Score)
1.	SSL Medium Strength Cipher Suites Supported (SWEET32)	AMC Server Port :443 / tcp / www	High
2.	TLS Version 1.0 Protocol Detection	AMC Server Port: 443 / tcp / www	Medium
3.	TLS Version 1.1 Protocol Deprecated	AMC Server Port: 443 / tcp / www	Medium
4.	Nameserver Processes Recursive Queries	AMC Server Port: 53 / UDP	Medium
5.	DNS server allows cache snooping	AMC Server Port: 53 / UDP / TCP	Medium
6.	TLS/SSL Server is enabling the BEAST attack	AMC Server Port: 53 / UDP / TCP	Medium
7.	HTTP OPTIONS Method Enabled	AMC Server Port: 443 / tcp / www	Low
8.	TLS/SSL Server Supports The Use of Static Key Ciphers	AMC Server Port: 443 / tcp / www	Low

จากตารางที่ 4.6 พบว่าการประเมินช่องโหว่ของเครื่องแม่ข่าย AMC Server มีจำนวนช่องโหว่ที่ประเมินพบทั้งสิ้นจำนวน 8 ช่องโหว่ มี พอร์ต (Port) ที่เกี่ยวข้องกับช่องโหว่ทั้งสิ้น 2 พอร์ต คือ Port : 443 และ Port : 53 โดย Port : 443 มีช่องโหว่ที่เกี่ยวข้องจำนวน 5 ช่องโหว่ และ Port : 53 มีช่องโหว่ที่เกี่ยวข้องจำนวน 3 ช่องโหว่ ในส่วนระดับความรุนแรงมีระดับความรุนแรงระดับสูง 1 ช่องโหว่ ระดับกลาง 5 ช่องโหว่ ระดับต่ำ 2 ช่องโหว่

ตารางที่ 4.7 รายละเอียดการประเมินช่องโหว่ที่พบเครื่องแม่ข่าย WEB Server

WEB Server			
ลำดับ	**ชื่อช่องโหว่**	**อุปกรณ์สารสนเทศ**	**ระดับความรุนแรง (Base Score)**
1.	FTP credentials transmitted unencrypted	WEB Server Port: 21 / TCP	High
2.	X.509 Certificate Subject CN Does Not Match the Entity Name	WEB Server Port: 21 / TCP	High
3.	SSL Certificate Cannot Be Trusted	WEB Server Port: 21 / tcp / ftp	Medium
4	SSL Self-Signed Certificate	WEB Server Port: 21 / tcp / ftp	Medium
5.	Untrusted TLS/SSL server X.509 certificate	WEB Server Port: 21 / 443 / TCP	Medium
6.	Test-cgi Script Information Disclosure Vulnerability	WEB Server Port: 888 / 80 / 443 / TCP	Medium
7.	Self-signed TLS/SSL certificate on 203.xxx.xxx.xxx	WEB Server Port: 21 / TCP	Medium
8.	HTTP OPTIONS Method Enabled	WEB Server Port: 888 / TCP	Low
9.	TLS/SSL Server Supports The Use of Static Key Ciphers	WEB Server Port: 443 / TCP	Low

จากตารางที่ 4.7 พบว่าการประเมินช่องโหว่ของเครื่องแม่ข่าย WEB Server มีจำนวนช่องโหว่ที่ประเมินพบทั้งสิ้นจำนวน 9 ช่องโหว่ มี พอร์ต (Port) ที่เกี่ยวข้องกับช่องโหว่ทั้งสิ้น 4 พอร์ต คือ Port : 21 / Port : 443 / Port : 888 และ Port : 80 โดย Port : 21 มีช่องโหว่ที่เกี่ยวข้องจำนวน 6 ช่องโหว่ Port : 443 มีช่องโหว่ที่เกี่ยวข้องจำนวน 3 ช่องโหว่ Port : 888 มีช่องโหว่ที่เกี่ยวข้องจำนวน 2 ช่องโหว่ และ Port : 80 มีช่องโหว่ที่เกี่ยวข้องจำนวน 1 ช่องโหว่ และยังพบว่าบางช่องโหว่มีความเกี่ยวข้องกับพอร์ตมากกว่า 1 พอร์ต์ คือ ช่องโหว่ Test-cgi Script Information Disclosure Vulnerability มีความเกี่ยวข้องกับพอร์ต 888 / 80 และ 443 และช่องโหว่ Untrusted TLS/SSL server X.509 certificate มีความเกี่ยวข้องกับพอร์ต 24 และ 443 ในส่วนของระดับความรุนแรงมีระดับความรุนแรง ระดับสูง 2 ช่องโหว่ ระดับกลาง 5 ช่องโหว่ ระดับต่ำ 2 ช่องโหว่

ตารางที่ 4.8 รายละเอียดการประเมินช่องโหว่ที่พบเครื่องแม่ข่าย OpenMCU 1

OpenMCU 1			
ลำดับ	**ชื่อช่องโหว่**	**อุปกรณ์สารสนเทศ**	**ระดับความรุนแรง (Base Score)**
1.	Unix Operating System Unsupported Version Detection	OpenMCU 1	High
2.	SSH Birthday attacks on 64-bit block ciphers (SWEET32)	OpenMCU 1 Port: 22 / tcp	High
3.	Unencrypted Telnet Server	OpenMCU 1 Port: 1423 / tcp / telnet	Medium
4.	SSH Weak Algorithms Supported	OpenMCU 1 Port: 22 / tcp / ssh	Medium
5.	SSH Server Supports RC4 Cipher Algorithms	OpenMCU 1 Port: 22 / tcp	Medium
6.	SSH Server Supports diffie-hellman-group1-sha1	OpenMCU 1 Port: 22 / tcp	Medium
7.	SSH Weak Key Exchange Algorithms Enabled	OpenMCU 1 Port: 22 / tcp / ssh	Low
8.	SSH Server CBC Mode Ciphers Enabled	OpenMCU 1 Port: 22 / tcp / ssh	Low
9.	SSH Weak MAC Algorithms Enabled	OpenMCU 1 Port: 22 / tcp / ssh	Low

จากตารางที่ 4.8 พบว่าการประเมินช่องโหว่ของเครื่องแม่ข่าย OpenMCU 1 มีจำนวนช่องโหว่ที่ประเมินพบทั้งสิ้นจำนวน 9 ช่องโหว่ มี พอร์ต (Port) ที่เกี่ยวข้องกับช่องโหว่ทั้งสิ้น 2 พอร์ต คือ Port : 22 และ Port : 1423 โดย Port : 22 มีช่องโหว่ที่เกี่ยวข้องจำนวน 7 ช่องโหว่ Port : 1423 มีช่องโหว่ที่เกี่ยวข้องจำนวน 1 ช่องโหว่ และยังพบว่าบางช่องโหว่ไม่มีความเกี่ยวข้องกับพอร์ตใดๆอย่างชัดเจน คือ ช่องโหว่ Unix Operating System Unsupported Version Detection ซึ่งจากการศึกษาของผู้วิจัยพบว่าเป็นช่องโหว่ที่เกี่ยวกับ ซอฟต์แวร์ระบบปฏิบัติการคอมพิวเตอร์ (Operating System : OS) ที่ล้าสมัย ไม่อัปเดตแพทช์ด้านการรักษาความปลอดภัย ซึ่งผู้วิจัยอนุมานได้ว่ามีในการโจมตีของผู้ไม่หวังดี สามารถทำได้ผ่านทาง พอร์ตของเครื่องแม่ข่าย OpenMCU 1 ได้หลายพอร์ต เนื่องจากซอฟต์แวร์ระบบปฏิบัติการคอมพิวเตอร์นั้นล้าสมัย ไม่อัปเดตแพทช์ด้านการ

รักษาความปลอดภัยแล้ว ในส่วนของระดับความรุนแรงมีระดับความรุนแรง ระดับสูง 2 ช่องโหว่ ระดับกลาง 4 ช่องโหว่ ระดับต่ำ 3 ช่องโหว่

ตารางที่ 4.9 รายละเอียดการประเมินช่องโหว่ที่พบเครื่องแม่ข่าย VPN PPTP

VPN PPTP			
ลำดับ	**ชื่อช่องโหว่**	**อุปกรณ์สารสนเทศ**	**ระดับความรุนแรง (Base Score)**
1.	X.509 Certificate Subject CN Does Not Match the Entity Name	VPN PPTP Port: 4444 / TCP	High
2.	SSL Certificate Cannot Be Trusted	VPN PPTP Port: 4444 / tcp / www	Medium
3.	SSL Self-Signed Certificate	VPN PPTP Port: 4444 / tcp / www	Medium
4.	TLS Version 1.1 Protocol Deprecated	VPN PPTP Port: 4444 / tcp / www	Medium
5.	Untrusted TLS/SSL server X.509 certificate	VPN PPTP Port: 4444 / tcp	Medium
6.	TLS Server Supports TLS version 1.1	VPN PPTP Port: 4444 / tcp	Low
7.	TLS/SSL Server Supports The Use of Static Key Ciphers	VPN PPTP Port: 4444 / tcp	Low
8.	TLS/SSL Server Is Using Commonly Used Prime Numbers	VPN PPTP Port: 4444 / tcp	Low

จากตารางที่ 4.9 พบว่าการประเมินช่องโหว่ของเครื่องแม่ข่าย VPN PPTP มีจำนวนช่องโหว่ที่ประเมินพบทั้งสิ้นจำนวน 8 ช่องโหว่ มี พอร์ต (Port) ที่เกี่ยวข้องกับช่องโหว่ทั้งสิ้น 1 พอร์ต คือ Port : 4444 โดย Port : 4444 มีช่องโหว่ที่เกี่ยวข้องจำนวน 8 ช่องโหว่ ในส่วนของระดับความรุนแรงมีระดับความรุนแรง ระดับสูง 1 ช่องโหว่ ระดับกลาง 4 ช่องโหว่ ระดับต่ำ 3 ช่องโหว่

จากตารางที่ 4.6 ถึง 4.9 เป็นการแสดงผลของการประเมินช่องโหว่ที่พบแบบแยกอุปกรณ์เครือข่ายที่เข้ารับการประเมินช่องโหว่ นำมาวิเคราะห์และอธิบายได้ดังนี้

พอร์ต (Port) ในงานวิจัยนี้หมายถึง พอร์ตเสมือน (virtual port) ซึ่งไม่ใช่พอร์ตกายภาพ (Port serial) หรือ พอร์ตอื่นๆ ที่เรามองเห็น แต่พอร์ตเสมือนนี้ หมายถึง พื้นที่เล็กๆ ในหน่วยความจำของเครื่อง ที่กันเอาไว้เพื่อการสื่อสารระหว่างโปรแกรมต่างๆ ในระบบจากเครื่องอื่นที่อยู่ในหรือนอกเครือข่าย โดยทั่วไปมีพอร์ตเสมือนสองประเภทคือ TCP และ UDP TCP ย่อมาจาก Transmission Control Protocol ส่วน UDP ย่อมาจาก User Datagram Protocol โดยจะมีการ

กำหนดเป็นหมายเลขเอาไว้เช่นที่เกี่ยวข้องกับช่องโหว่ที่ประเมินพบเช่น Port : 443 เป็นต้น และจากการประเมินช่องโหว่พบว่า พอร์ตที่เกี่ยวข้องกับช่องโหว่ที่ประเมินพบนั้นมีดังนี้

Port : 80 เป็นพอร์ต TCP ใช้สำหรับการรับส่งข้อมูล หรือที่เรียกว่า Hypertext Transfer Protocol หรือ HTTP หรือการใช้งานเว็บเซิร์ฟเวอร์ URL ที่ขึ้นต้นด้วย "http://" การใช้โพรโทคอลนี้เพื่อรับ-ส่งข้อมูลโดยใช้พอร์ต 80 การทำงานของ HTTP อยู่ในระดับ Application Layer บนโพรโทคอล TCP/IP ส่งข้อมูลเป็นแบบ Clear text คือ ไม่มีการเข้ารหัสข้อมูลในระหว่างการส่ง (None-Encryption) จึงสามารถถูกดักจับได้ และอ่านข้อมูลนั้นรู้เรื่อง จากการประเมินช่องโหว่ของอุปกรณ์เครื่องแม่ข่ายทั้ง 4 เครื่อง พบพอร์ต 80 ที่เกี่ยวข้องกับช่องโหว่ที่ประเมินมีจำนวน 1 ช่องโหว่

Port : 443 เป็นพอร์ต TCP ใช้สำหรับการรับส่งข้อมูลที่ปลอดภัย หรือที่เรียกว่า Hypertext Transfer Protocol Secure หรือ HTTPS หรือการใช้งานเว็บเซิร์ฟเวอร์ URL ที่ขึ้นต้นด้วย "https://" การใช้โพรโทคอลนี้เพื่อรับ-ส่งข้อมูลถึงโดยใช้พอร์ต 443 การทำงานของ HTTPS เป็นการทำงานเหมือนกับ HTTP ธรรมดาแต่ทำอยู่บน SSL/TSL เพื่อให้เกิดความปลอดภัยในการส่งข้อมูลมากยิ่งขึ้น จากการประเมินช่องโหว่ของอุปกรณ์เครื่องแม่ข่ายทั้ง 4 เครื่อง พบพอร์ต 443 ที่เกี่ยวข้องกับช่องโหว่ที่ประเมิน มีจำนวน 8 ช่องโหว่

Port : 53 เป็นพอร์ต TCP/UDP มีโพรโทคอลที่สำคัญมากที่ใช้พอร์ต UDP ในการรับส่งข้อมูล เช่น DNS (Domain Name System) โพรโทคอลและ SNMP (Simple Mail Transfer Protocol) โพรโทคอล โพรโทคอลทั้งสองใช้พอร์ต UDP จากการประเมินช่องโหว่ของอุปกรณ์เครื่องแม่ข่ายทั้ง 4 เครื่อง พบพอร์ต 53 ที่เกี่ยวข้องกับช่องโหว่ที่ประเมิน มีจำนวน 3 ช่องโหว่

Port : 21 เป็นพอร์ต TCP/FTP ที่ใช้งานโดย FTP (File Transfer Protocol) เป็นระบบโอนย้ายไฟล์ข้ามระบบเครื่องคอมพิวเตอร์ที่มีความปลอดภัย โดยใช้โพรโทคอล TCP เป็นกลไกขนส่งข้อมูล การเข้าใช้งานชื่อข้อมูลผู้ใช้ (User) รหัสผ่าน (Password) จากนั้นจะแสดงชื่อโฟลเดอร์ และชื่อไฟล์ ทำให้โอนย้ายไฟล์ ระหว่างไคลเอนต์ และ FTP Server หรือระหว่างเครื่องสองเครื่องที่อยู่ห่างไกลกันได้ จากการประเมินช่องโหว่ของอุปกรณ์เครื่องแม่ข่ายทั้ง 4 เครื่อง พบพอร์ต 21 ที่เกี่ยวข้องกับช่องโหว่ที่ประเมิน มีจำนวน 6 ช่องโหว่

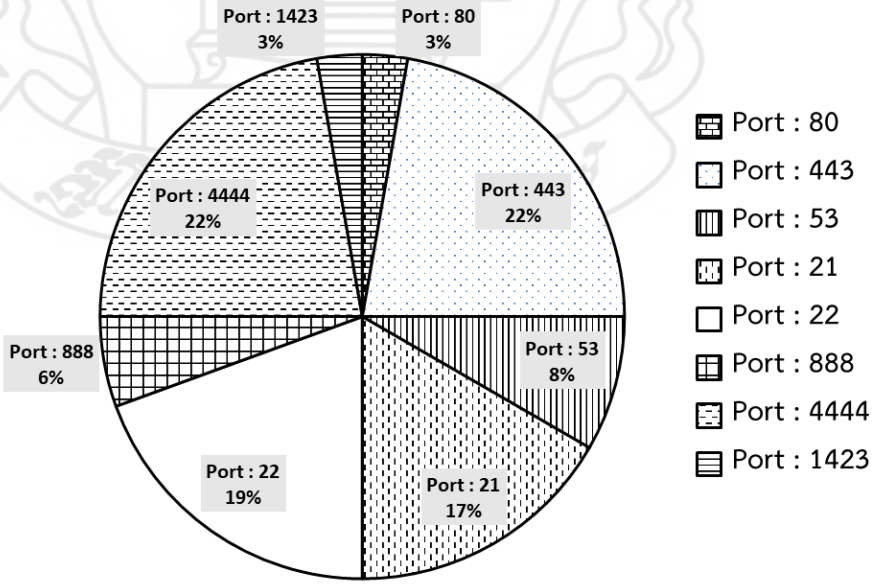
Port : 22 เป็นพอร์ต TCP/SSH ที่ใช้งานโดย Secure Shell หรือ SSH คือโพรโทคอลสำหรับเครือข่ายคอมพิวเตอร์ ที่ออกแบบมาเพื่อให้เข้าถึงคอมพิวเตอร์เครื่องอื่น ๆ จากระยะไกล และทำงานต่าง ๆ บนเครื่องนั้น SSH ออกแบบมาใช้ทดแทน TELNET เนื่องด้วยเหตุผลด้านความปลอดภัย เพราะ SSH ใช้วิธีเข้ารหัสข้อมูลที่ส่งผ่านระหว่างเครื่องพอร์ตมาตรฐานของ SSH คือ พอร์ต 22 จากการประเมินช่องโหว่ของอุปกรณ์เครื่องแม่ข่ายทั้ง 4 เครื่อง พบพอร์ต 22 ที่เกี่ยวข้องกับช่องโหว่ที่ประเมิน มีจำนวน 7 ช่องโหว่

Port : 888 เป็นพอร์ต TCP ใช้สำหรับการรับส่งข้อมูล หรือที่เรียกว่า Hypertext Transfer Protocol หรือ HTTP เหมือนกับ Port : 80 แต่โดยส่วนมาก Port : 888 จะถูกใช้งานจาก เว็บเซิร์ฟเวอร์ Apache จากการประเมินช่องโหว่ของอุปกรณ์เครื่องแม่ข่ายทั้ง 4 เครื่อง พบพอร์ต 888 ที่เกี่ยวข้องกับช่องโหว่ที่ประเมิน มีจำนวน 2 ช่องโหว่

Port : 4444 เป็นพอร์ต TCP/UDP โพรโทคอล HTTP และ TSL/SSL ใช้พอร์ตนี้เพื่อสื่อสารข้อมูลผ่านเครือข่าย โพรโทคอล HTTP กำหนดรูปแบบสำหรับการสื่อสารระหว่างอินเทอร์เน็ตเบราว์เซอร์และเว็บไซต์ โพรโทคอลควบคุมการถ่ายโอน โดยมีโพรโทคอล TSL/SSL ใช้สำหรับการสื่อสารที่เข้ารหัส จากการประเมินช่องโหว่ของอุปกรณ์เครื่องแม่ข่ายทั้ง 4 เครื่อง พบพอร์ต 4444 ที่เกี่ยวข้องกับช่องโหว่ที่ประเมิน มีจำนวน 8 ช่องโหว่

Port : 1423 เป็นพอร์ต TCP/Telnet โพรโทคอล Telnet เป็นบริการเข้าใช้เครื่องคอมพิวเตอร์จากระยะไกล ผู้ใช้นั้นสามารถขอเข้าใช้ได้ โดยติดต่อเครือข่ายที่ได้รับอนุญาต การขอใช้นั้น ผู้ใช้จะป้อนคำสั่งที่เครื่องของตัวเองไปยังเครื่องที่ขอเข้าใช้ แล้วผลก็จะกลับมาแสดงที่หน้าจอเรา เทลเน็ตเป็นชื่อของโพรโทคอลที่ใช้ในการจำลองเทอร์มินัลผ่านระบบเครือข่ายอินเทอร์เน็ต เป็นโพรโทคอลในชุด TCP/IP เป็นที่นิยมใช้งานกันอย่างแพร่หลายในกลุ่มของผู้ดูแลระบบเครือข่ายในองค์กร เพราะสามารถควบคุมเครื่องเซิร์ฟเวอร์ได้จากระยะไกล จากการประเมินช่องโหว่ของอุปกรณ์เครื่องแม่ข่ายทั้ง 4 เครื่อง พบพอร์ต 1423 ที่เกี่ยวข้องกับช่องโหว่ที่ประเมิน มีจำนวน 1 ช่องโหว่

ภาพรวม พอร์ต หมายเลขต่างๆ ที่พบจากการประเมินช่องโหว่ระบบสารสนเทศขององค์กร แสดงในรูปแผนภูมิในรายละเอียดที่เกี่ยวข้องได้ดังนี้



ภาพที่ 4.3 อัตราส่วนร้อยละของพอร์ตที่เกี่ยวข้องกับช่องโหว่ที่ประเมินพบ

จากภาพที่ 4.3 จำนวน พอร์ตที่พบเป็นจำนวนมาก คือ Port : 4444 อัตราส่วนร้อยละ 22 Port : 443 อัตราส่วนร้อยละ 22 Port : 22 อัตราส่วนร้อยละ 19 และ Port : 21 อัตราส่วนร้อยละ 17 ตามลำดับ พบว่า Port : 4444 Port : 443 และ Port : 21 นั้นจะเป็นพอร์ตที่เกี่ยวข้องกับช่องโหว่ชนิด TSL/SSL/X.509 ซึ่งลักษณะช่องโหว่ประเภทนี้จะเกี่ยวข้องกับระบบเว็บเซิร์ฟเวอร์ ซึ่งจะพบพอร์ตที่เป็นปัญหาเกี่ยวกับช่องโหว่ TSL/SSL/X.509 จะพบได้บนอุปกรณ์เครือข่ายที่เข้ารับการประเมินช่องโหว่ เช่น AMC Sever / WEB Server / VPN PPTP ซึ่งเป็นเครื่องแม่ข่ายที่ให้บริการในด้านระบบเว็บเซิร์ฟเวอร์ จึงวิเคราะห์ได้ว่า พอร์ตและช่องโหว่ที่เกี่ยวข้องกับช่องโหว่ชนิด TSL/SSL/X.509 มีจำนวนมากกว่าช่องโหว่ชนิดอื่น ดังนั้นจึงจำเป็นต้องให้ความสำคัญอย่างเร่งด่วนในการแก้ปัญหาที่จะเกิดขึ้น เพราะอาจจะเป็นช่องทางในการถูกโจมตีจากผู้ไม่หวังดีผ่านทางพอร์ต 4444/443/21 มากที่สุด เช่นเดียวกับ Port : 22 ซึ่งมีจำนวนช่องโหว่ที่เกี่ยวข้องกับพอร์ตหมายเลข 22 เป็นจำนวนมากเช่นเดียวกัน เป็นพอร์ตที่เกี่ยวข้องกับช่องโหว่ชนิด SSH/Telnet/FTP ซึ่งเป็นการเข้าใช้งาน หรือควบคุมเครื่องอื่นๆ จากระยะไกล (Remote) จากอุปกรณ์ที่เข้ารับการประเมินช่องโหว่พบว่า พอร์ตหมายเลข 22 ที่เกี่ยวข้องกับช่องโหว่ชนิด SSH/Telnet/FTP จะพบบนเครื่องแม่ข่าย OpenMCU 1 ซึ่งเป็นแม่ข่ายให้บริการประชุมทางไกลผ่านจอภาพ จากการสอบถามผู้จัดการระบบสารสนเทศขององค์กร (Admin) พบว่าเครื่องแม่ข่ายดังกล่าวนั้นใช้ระบบปฏิบัติการ Linux Kernel 3.0 on Ubuntu 12.04 ซึ่งไม่มีการอัปเดตแพทช์ด้านการรักษาความปลอดภัย จึงอาจเป็นสาเหตุให้เกิดปัญหาช่องโหว่ที่เกิดขึ้นซึ่งอาจทำให้เกิดความเสียหายต่อระบบสารสนเทศได้ จึงควรเร่งดำเนินการแก้ไข เช่น อัปเดตระบบปฏิบัติการใหม่เป็นต้น ส่วนพอร์ตที่พบจำนวนเล็กน้อยคือ Port : 53 / Port : 80 / Port : 888 / Port : 1423 ถือว่าเกี่ยวข้องกับช่องโหว่ที่สำคัญเช่นเดียวกัน ควรดำเนินการในการแก้ไขช่องโหว่ที่ใช้พอร์ตหมายเลขดังกล่าวให้หมดไปเพื่อป้องกันรักษาความปลอดภัยระบบสารสนเทศขององค์กร

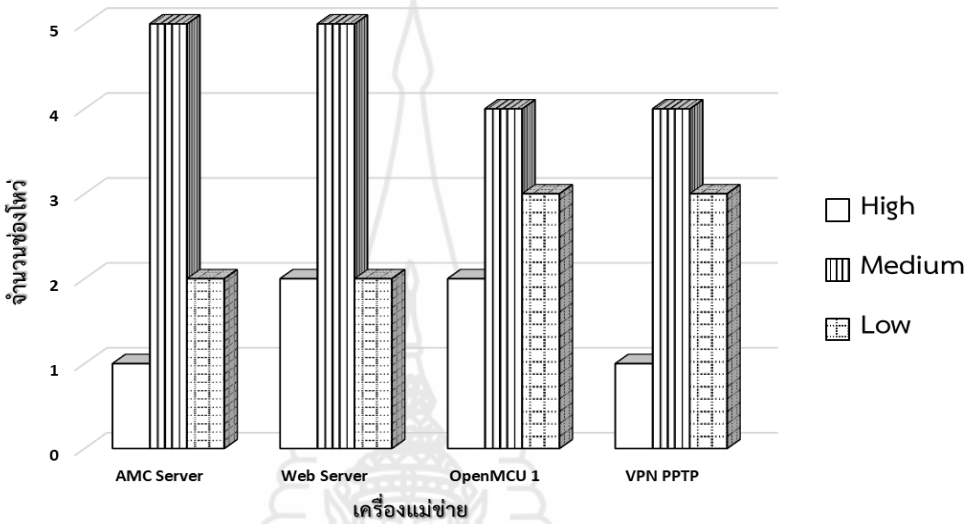
3) ระดับความรุนแรงของช่องโหว่ จากตารางที่ 4.6 ถึง 4.9 พบว่าจากการประเมินช่องโหว่ ตรวจพบระดับความรุนแรงช่องโหว่ตามอุปกรณ์เครื่องแม่ข่ายที่เข้ารับการประเมินดังนี้

3.1) ระดับความรุนแรงของช่องโหว่ที่ประเมินพบแยกตามอุปกรณ์เครื่องแม่ข่าย

- เครื่องแม่ข่าย AMC Server พบระดับความรุนแรงสูง 1 ช่องโหว่ ระดับความรุนแรงปานกลาง 5 ช่องโหว่ ระดับความรุนแรงต่ำ 2 ช่องโหว่
- เครื่องแม่ข่าย WEB Server พบระดับความรุนแรงสูง 2 ช่องโหว่ ระดับความรุนแรงปานกลาง 5 ช่องโหว่ ระดับความรุนแรงต่ำ 2 ช่องโหว่

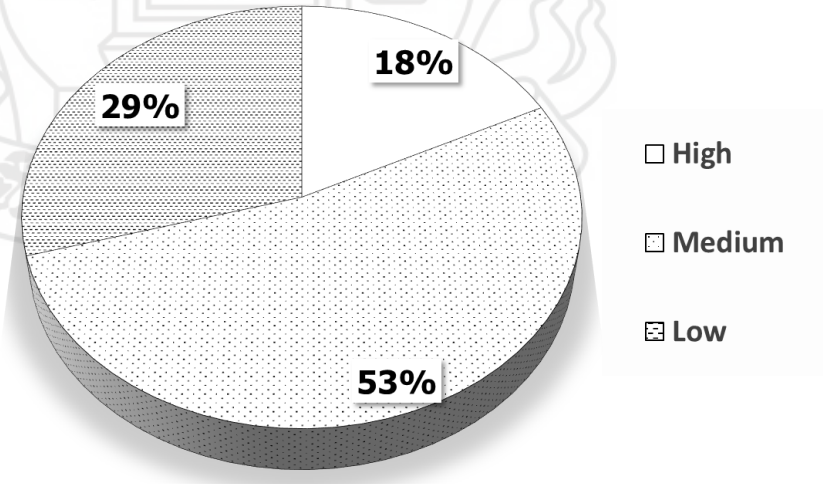
- เครื่องแม่ข่าย OpenMCU 1 พบระดับความรุนแรงสูง 2 ช่องโหว่ ระดับความรุนแรงปานกลาง 4 ช่องโหว่ ระดับความรุนแรงต่ำ 3 ช่องโหว่

- เครื่องแม่ข่าย VPN PPTP พบระดับความรุนแรงสูง 1 ช่องโหว่ ระดับความรุนแรงปานกลาง 5 ช่องโหว่ ระดับความรุนแรงต่ำ 2 ช่องโหว่



ภาพที่ 4.4 ระดับความรุนแรงของช่องโหว่ที่ประเมินพบแยกตามอุปกรณ์เครื่องแม่ข่าย

3.2) ระดับความรุนแรงของช่องโหว่ที่ประเมินพบของอุปกรณ์เครื่องแม่ข่ายทั้งหมดที่เข้ารับการประเมินช่องโหว่ คิดเป็นอัตราส่วนร้อยละได้ดังนี้



ภาพที่ 4.5 อัตราส่วนร้อยละระดับความรุนแรงของช่องโหว่ที่ประเมินพบ

ระดับความรุนแรงสูง (High) มีจำนวน 6 ช่องโหว่ คิดเป็น 18 %
ระดับความรุนแรงปานกลาง (Medium) มีจำนวน 18 ช่องโหว่ คิดเป็น 53 %
ระดับความรุนแรงต่ำ (Low) มีจำนวน 10 ช่องโหว่ คิดเป็น 29 %

จากภาพที่ 4.4 และ 4.5 อธิบายได้ว่าในการประเมินช่องโหว่ของอุปกรณ์เครื่องแม่ข่ายที่เข้ารับการประเมินช่องโหว่ มีระดับความรุนแรงที่ใกล้เคียงกัน กล่าวคือมีระดับความรุนแรงสูงอยู่ในจำนวนน้อย ระดับความรุนแรงปานกลางอยู่ในจำนวนมาก และระดับความรุนแรงต่ำอยู่ในจำนวนน้อย ทุกอุปกรณ์เครื่องแม่ข่าย และคิดเป็นอัตราส่วนร้อยละของระดับความรุนแรงทั้งหมดรวมทุกอุปกรณ์จะเห็นว่าช่องโหว่ที่มีระดับความรุนแรงปานกลางจะมีจำนวนมากที่สุด คิดเป็นร้อยละ 53 ตามภาพที่ 4.5 ดังนั้นระดับความรุนแรงของช่องโหว่ระบบสารสนเทศขององค์กร ภาพรวมจะอยู่ในระดับความรุนแรงปานกลาง อย่างไรก็ดีก็ต้องให้ความสำคัญทุกระดับความรุนแรงที่เกิดขึ้นเพื่อลดปัญหาที่อาจเกิดขึ้นจากการโจมตีของผู้ไม่หวังดี

นอกจากนี้ผู้วิจัยยังได้ใช้มาตรฐานความมั่นคงปลอดภัยของเว็บแอปพลิเคชัน (OWASP 10) นำมาประเมินกับช่องโหว่ที่ประเมินพบ พบว่ามีช่องโหว่ตามมาตรฐาน OWASP 10 ในระดับ A02 (Cryptographic Failures) 19 ช่องโหว่ ซึ่งเป็นช่องโหว่ที่เกี่ยวข้องกับโพรโทคอล TTS/SSL เกี่ยวกับการเข้ารหัสที่อ่อนแอ และมีระดับความรุนแรงสูงสุดของงานวิจัยนี้ 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

2.2 การประเมินค่าระดับความเสี่ยง (Risk Assessment)

ผลการประเมินความเสี่ยงช่องโหว่ของอุปกรณ์ระบบสารสนเทศที่ส่งผลกระทบต่อองค์กร แสดงโดยการจัดเรียงตามลำดับความเสี่ยงตามคอลัมน์ Risk+ ซึ่งเป็นผลลัพธ์ที่มาจาก L x NI ที่ได้อธิบายไว้ในบทที่ 3 ตามตารางที่ 4.10 ดังนี้

ตารางที่ 4.10 รายละเอียดการประเมินค่าระดับความเสี่ยงช่องโหว่ของอุปกรณ์ระบบสารสนเทศที่ส่งผลกระทบต่อองค์กร

ลำดับ	ชื่อช่องโหว่	อุปกรณ์สารสนเทศ	ข้อมูลความเสี่ยง CVSS	L	I	OI	NI	L x I	Risk	L x NI	Risk+
1.	DNS server allows cache snooping	AMC Server Port: 53 / UDP / TCP	CVSS v2.0 Base Score 5 CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N	9.00	2.61	8.00	5.31	3 X 1	Med	3 X 2	High
2.	Nameserver Processes Recursive Queries	AMC Server Port: 53 / UDP	CVSS v2.0 Base Score 5 CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P	9.00	2.61	8.00	5.31	3 X 1	Med	3 X 2	High
3.	TLS/SSL Server is enabling the BEAST attack	AMC Server Port: 53 / UDP / TCP	CVSS v2.0 Base Score 4.3 CVSS v2.0 Vector: CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N	7.74	2.61	8.00	5.31	3 X 1	Med	3 X 2	High
4.	FTP credentials transmitted unencrypted	WEB Server Port: 21 / TCP	CVSS v2.0 Base Score 7.3 CVSS v2.0 Vector: CVSS2#AV:A/AC:M/Au:N/C:C/I:C/A:N	4.95	8.28	7.25	7.77	2 X 3	High	2 X 3	High

ตารางที่ 4.10 (ต่อ)

ลำดับ	ชื่อช่องโหว่	อุปกรณ์สารสนเทศ	ข้อมูลความเสี่ยง CVSS	L	I	OI	NI	L x I	Risk	L x NI	Risk+
5.	X.509 Certificate Subject CN Does Not Match the Entity Name	WEB Server Port: 21 / TCP	CVSS v2.0 Base Score 7.1 CVSS v2.0 Vector: CVSS2#AV:N/AC:H/Au:N/C:C/I:C/A:N	4.41	8.28	7.25	7.77	2 X 3	High	2 X 3	High
6.	Self-signed TLS/SSL certificate on 203.xxx.xxx.xxx	WEB Server Port: 21 / TCP	CVSS v2.0 Base Score 4.3 CVSS v2.0 Vector: CVSS2#AV:N/AC:M/Au:N/C:N/I:P/A:N	7.74	2.61	7.25	4.93	3 X 1	High	3 X 2	High
7.	Test-cgi Script Information Disclosure Vulnerability	WEB Server Port: 888 / 80 / 443 / TCP	CVSS v2.0 Base Score 5 CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:N/I:P/A:N	9.00	2.61	7.25	4.93	3 X 1	High	3 X 2	High
8.	Unix Operating System Unsupported Version Detection	OpenMCU 1	CVSS v3.0 Base Score 10.0 CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H	3.51	5.40	7.00	6.20	2 X 2	Med	2 X 3	High
9.	SSH Weak Algorithms Supported	OpenMCU 1 Port: 22 / tcp / ssh	CVSS v2.0 Base Score: 4.3 CVSS v2.0 Vector: CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N	7.74	2.61	7.00	4.81	3 X 1	Med	3 X 2	High

ตารางที่ 4.10 (ต่อ)

ลำดับ	ชื่อช่องโหว่	อุปกรณ์สารสนเทศ	ข้อมูลความเสี่ยง CVSS	L	I	OI	NI	L x I	Risk	L x NI	Risk+
10.	SSH Server Supports RC4 Cipher Algorithms	OpenMCU 1 Port: 22 / tcp	CVSS v2.0 Base Score: 4.3 CVSS v2.0 Vector: CVSS2#AV:N/AC:M/Au:N/C:P/I:N/A:N	7.74	2.61	7.00	4.81	3 X 1	Med	3 X 2	High
11.	X.509 Certificate Subject CN Does Not Match the Entity Name	VPN PPTP Port: 4444 / TCP	CVSS v2.0 Base Score 7.1 CVSS v2.0 Vector: CVSS2#AV:N/AC:H/Au:N/C:C/I:C/A:N	4.41	8.28	6.25	7.27	2 X 3	High	2 X 3	High
12.	Untrusted TLS/SSL server X.509 certificate	VPN PPTP Port: 4444 / tcp	CVSS v2.0 Base Score 5.8 CVSS v2.0 Vector: CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:N	7.74	4.41	6.25	5.33	3 X 2	High	3 X 2	High
13.	SSL Medium Strength Cipher Suites Supported (SWEET32)	AMC Server Port :443 / tcp / www	CVSS v3.0 Base Score 7.5 CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N	3.51	3.24	8.00	5.62	2 X 2	Med	2 x 2	Med
14.	TLS Version 1.0 Protocol Detection	AMC Server Port: 443 / tcp / www	CVSS v3.0 Base Score 6.5 CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N	1.98	3.78	8.00	5.89	1 X 2	Low	1 X 3	Med

ตารางที่ 4.10 (ต่อ)

ลำดับ	ชื่อช่องโหว่	อุปกรณ์สารสนเทศ	ข้อมูลความเสี่ยง CVSS	L	I	OI	NI	L x I	Risk	L x NI	Risk+
15.	TLS Version 1.1 Protocol Deprecated	AMC Server Port: 443 / tcp / www	CVSS v3.0 Base Score 6.5 CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N	1.98	3.78	8.00	5.89	1 X 2	Low	1 X 3	Med
16.	HTTP OPTIONS Method Enabled	AMC Server Port: 443 / tcp / www	CVSS v2.0 Base Score 2.6 CVSS v2.0 Vector: CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N	4.41	2.61	8.00	5.30	2 X 1	Low	2 X 2	Med
17.	TLS/SSL Server Supports The Use of Static Key Ciphers	AMC Server Port: 443 / tcp / www	CVSS v2.0 Base Score 2.6 CVSS v2.0 Vector: CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N	4.41	2.61	8.00	5.30	2 X 1	Low	2 X 2	Med
18.	SSL Certificate Cannot Be Trusted	WEB Server Port: 21 / tcp / ftp	CVSS v3.0 Base Score 6.5 CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N	3.51	2.25	7.25	4.75	2 X 1	Low	2 X 2	Med
19.	SSL Self-Signed Certificate	WEB Server Port: 21 / tcp / ftp	CVSS v3.0 Base Score 6.5 CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N	3.51	2.25	7.25	4.75	2 X 1	Low	2 X 2	Med
20.	Untrusted TLS/SSL server X.509 certificate	WEB Server Port: 21 / 443 / TCP	CVSS v2.0 Base Score 5.8 CVSS v2.0 Vector: CVSS2#AV:N/AC:M/Au:N/C:P/I:P/A:N	4.43	0.88	7.25	4.06	2 X 1	Low	2 X 2	Med

ตารางที่ 4.10 (ต่อ)

ลำดับ	ชื่อช่องโหว่	อุปกรณ์สารสนเทศ	ข้อมูลความเสี่ยง CVSS	L	I	OI	NI	L x I	Risk	L x NI	Risk+
21.	HTTP OPTIONS Method Enabled	WEB Server Port: 888 / TCP	CVSS v2.0 Base Score 2.6 CVSS v2.0 Vector: CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N	4.41	2.61	7.25	4.93	2 X 1	Low	2 X 2	Med
22.	TLS/SSL Server Supports The Use of Static Key Ciphers	WEB Server Port: 443 / TCP CATEGORIES: Network	CVSS v2.0 Base Score 2.6 CVSS v2.0 Vector: CVSS2# AV:N/AC:H/Au:N/C:P/I:N/A:N	4.41	2.61	7.25	4.93	2 X 1	Low	2 X 2	Med
23.	SSH Birthday attacks on 64-bit block ciphers (SWEET32)	OpenMCU 1 Port: 22 / tcp	CVSS v3.0 Base Score 7.5 CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N	3.51	3.24	7.00	5.12	2 X 2	Med	2 X 2	Med
24.	Unencrypted Telnet Server	OpenMCU 1 Port: 1423 / tcp / telnet	CVSS v3.0 Base Score 6.5 CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N	3.51	2.25	7.00	4.62	2 X 1	Low	2 X 2	Med
25.	SSH Server CBC Mode Ciphers Enabled	OpenMCU 1 Port: 22 / tcp / ssh	CVSS v2.0 Base Score: 2.6 CVSS v2.0 Vector: CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N	4.41	2.61	7.00	4.80	2 X 1	Low	2 X 2	Med

ตารางที่ 4.10 (ต่อ)

ลำดับ	ชื่อช่องโหว่	อุปกรณ์สารสนเทศ	ข้อมูลความเสี่ยง CVSS	L	I	OI	NI	L x I	Risk	L x NI	Risk+
26.	SSH Weak MAC Algorithms Enabled	OpenMCU 1 Port: 22 / tcp / ssh	CVSS v2.0 Base Score: 2.6 CVSS v2.0 Vector: CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N	4.41	2.61	7.00	4.80	2 X 1	Low	2 X 2	Med
27.	SSL Certificate Cannot Be Trusted	VPN PPTP Port: 4444 / tcp / www	CVSS v3.0 Base Score 6.5 CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N	3.51	2.25	6.25	4.25	2 X 1	Low	2 X 2	Med
28.	SSL Self-Signed Certificate	VPN PPTP Port: 4444 / tcp / www	CVSS v3.0 Base Score 6.5 CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N	3.51	2.50	6.25	4.25	2 X 1	Low	2 X 2	Medium
29.	TLS Server Supports TLS version 1.1	VPN PPTP Port: 4444 / tcp	CVSS v2.0 Base Score 2.6 CVSS v2.0 Vector: CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N	4.41	2.61	6.25	4.43	2 X 1	Low	2 X 2	Med
30.	TLS/SSL Server Supports The Use of Static Key Ciphers	VPN PPTP Port: 4444 / tcp	CVSS v2.0 Base Score 2.6 CVSS v2.0 Vector: CVSS2#AV:N/AC:H/Au:N/C:P/I:N/A:N	4.41	2.61	6.25	4.43	2 X 1	Low	2 X 2	Med

ตารางที่ 4.10 (ต่อ)

ลำดับ	ชื่อช่องโหว่	อุปกรณ์สารสนเทศ	ข้อมูลความเสี่ยง CVSS	L	I	OI	NI	L x I	Risk	L x NI	Risk+
31.	TLS/SSL Server Is Using Commonly Used Prime Numbers	VPN PPTP Port: 4444 / tcp	CVSS v2.0 Base Score 2.6 CVSS v2.0 Vector: CVSS2#AV:N/AC:H/Au:N/C:N/I:P/A:N	4.41	2.61	6.25	4.43	2 X 1	Low	2 X 2	Med
32.	SSH Server Supports diffie-hellman-group1-sha1	OpenMCU 1 Port: 22 / tcp	CVSS v3.0 Base Score 3.7 CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N	1.98	1.26	7.00	4.13	1 X 1	Low	1 X 2	Low
33.	SSH Weak Key Exchange Algorithms Enabled	OpenMCU 1 Port: 22 / tcp / ssh	CVSS v3.0 Base Score 3.7 CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N	1.98	1.26	7.00	4.13	1 X 1	Low	1 X 2	Low
34.	TLS Version 1.1 Protocol Deprecated	VPN PPTP Port: 4444 / tcp / www	CVSS v3.0 Base Score 6.5 CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N	1.98	3.78	6.25	5.01	1 X 2	Low	1 X 2	Low

2.3 แสดงความสำคัญระดับความเสี่ยง (Risk Rating)

ตารางที่ 4.11 แสดงความสำคัญระดับความเสี่ยงเรียงลำดับตามผลการประเมินระดับความเสี่ยง แสดงโดยการจัดเรียงตามลำดับความเสี่ยงตามคอลัมน์ Risk+

ลำดับ	ชื่อช่องโหว่	ข้อมูลอ้างอิง	อุปกรณ์สารสนเทศ	RISK+
1.	Nameserver Processes Recursive Queries	1. dns-processes-recursive-queries	AMC Server Port: 53 / UDP	High
2.	DNS server allows cache snooping	1. dns-allows-cache-snooping	AMC Server Port: 53 / UDP / TCP	High
3.	TLS/SSL Server is enabling the BEAST attack	1. CVE-2011-3389	AMC Server Port: 53 / UDP / TCP	High
4.	FTP credentials transmitted unencrypted	1. ftp-plaintext-auth	WEB Server Port: 21 / TCP	High
5.	X.509 Certificate Subject CN Does Not Match the Entity Name	1. certificate-common-name-mismatch	WEB Server Port: 21 / TCP	High
6.	Self-signed TLS/SSL certificate on 203.xxx.xxx.xxx	1. ssl-self-signed-certificate	WEB Server Port: 21 / TCP	High
7.	Test-cgi Script Information Disclosure Vulnerability	1. CVE-1999-0070 2. http-apache-0010	WEB Server Port: 888 / 80 / 443 / TCP	High
8.	Unix Operating System Unsupported Version Detection	1. tenable plugins #33850	OpenMCU 1	High
9.	SSH Weak Algorithms Supported	1. tenable plugins #90317	OpenMCU 1 Port: 22 / tcp / ssh	High
10.	SSH Server Supports RC4 Cipher Algorithms	1. ssh-rc4-ciphers	OpenMCU 1 Port: 22 / tcp	High
11.	X.509 Certificate Subject CN Does Not Match the Entity Name	1. certificate-common-name-mismatch	VPN PPTP Port: 4444 / TCP	High
12.	Untrusted TLS/SSL server X.509 certificate	1. tls-untrusted-ca	VPN PPTP Port: 4444 / tcp	High

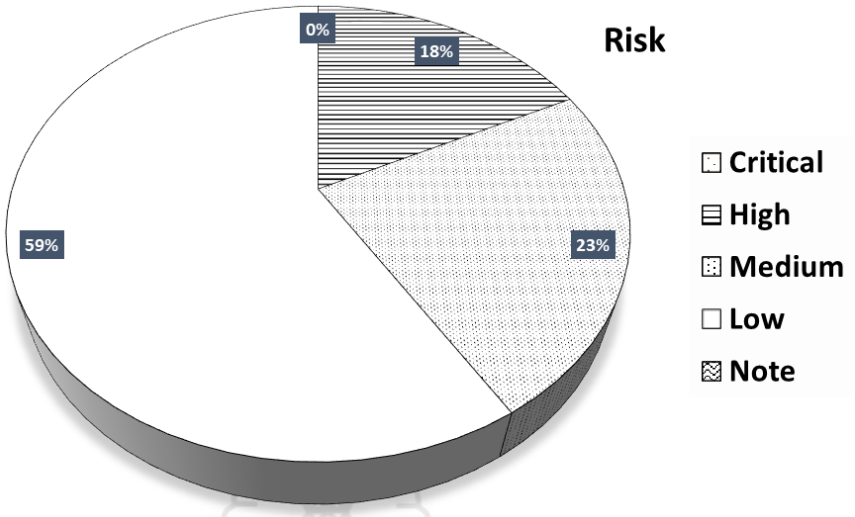
ตารางที่ 4.11 (ต่อ)

ลำดับ	ชื่อช่องโหว่	ข้อมูลอ้างอิง	อุปกรณ์สารสนเทศ	RISK+
13.	SSL Medium Strength Cipher Suites Supported (SWEET32)	1. tenable plugins #42873 2. CVE: CVE-2016-2183	AMC Server Port :443 / tcp / www	Med
14.	TLS Version 1.0 Protocol Detection	1. tenable plugins #104743	AMC Server Port: 443 / tcp / www	Med
15.	TLS Version 1.1 Protocol Deprecated	1. tenable plugins #157288	AMC Server Port: 443 / tcp / www	Med
16.	HTTP OPTIONS Method Enabled	1. http-options-method-enabled	AMC Server Port: 443 / tcp / www	Med
17.	TLS/SSL Server Supports The Use of Static Key Ciphers	1. ssl-static-key-ciphers	AMC Server Port: 443 / tcp / www	Med
18.	SSL Certificate Cannot Be Trusted	1. tenable plugins #51192	WEB Server Port: 21 / tcp / ftp	Med
19.	SSL Self-Signed Certificate	1. tenable plugins #57582	WEB Server Port: 21 / tcp / ftp	Med
20.	Untrusted TLS/SSL server X.509 certificate	1. tls-untrusted-ca	WEB Server Port: 21 / 443 / TCP	Med
21.	HTTP OPTIONS Method Enabled	1. http-options-method-enabled	WEB Server Port: 888 / TCP	Med
22.	TLS/SSL Server Supports The Use of Static Key Ciphers	1. ssl-static-key-ciphers	WEB Server Port: 443 / TCP CATEGORIES: Network	Med
23.	SSH Birthday attacks on 64-bit block ciphers (SWEET32)	1. CVE: CVE-2016-2183	OpenMCU 1 Port: 22 / tcp	Med
24.	Unencrypted Telnet Server	1. tenable plugins #42263	OpenMCU 1 Port: 1423 / tcp / telnet	Med
25.	SSH Server CBC Mode Ciphers Enabled	1. tenable plugins #70658	OpenMCU 1 Port: 22 / tcp / ssh	Med

ตารางที่ 4.11 (ต่อ)

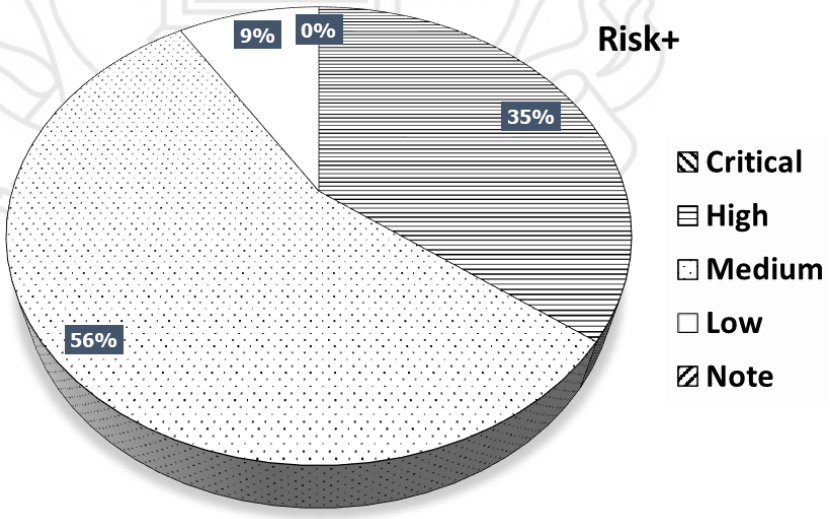
ลำดับ	ชื่อช่องโหว่	ข้อมูลอ้างอิง	อุปกรณ์สารสนเทศ	RISK+
26.	SSH Weak MAC Algorithms Enabled	1. tenable plugins #71049	OpenMCU 1 Port: 22 / tcp / ssh	Med
27..	SSL Certificate Cannot Be Trusted	1. tenable plugins #51192	VPN PPTP Port: 4444 / tcp / www	Med
28.	SSL Self-Signed Certificate	1. tenable plugins #57582	VPN PPTP Port: 4444 / tcp / www	Medium
29.	TLS Server Supports TLS version 1.1	1. tlsv1_1-enabled	VPN PPTP Port: 4444 / tcp	Med
30.	TLS/SSL Server Supports The Use of Static Key Ciphers	1. ssl-static-key-ciphers	VPN PPTP Port: 4444 / tcp	Med
31.	TLS/SSL Server Is Using Commonly Used Prime Numbers	1. tls-dh-primes	VPN PPTP Port: 4444 / tcp	Med
32.	SSH Server Supports diffie-hellman-group1-sha1	1. CVE: CVE-2015-4000	OpenMCU 1 Port: 22 / tcp	Low
33.	SSH Weak Key Exchange Algorithms Enabled	1. tenable plugins #1539537	OpenMCU 1 Port: 22 / tcp / ssh	Low
34.	TLS Version 1.1 Protocol Deprecated	1. tenable plugins #157288	VPN PPTP Port: 4444 / tcp / www	Low

จากการประเมินความเสี่ยงของระบบสารสนเทศขององค์กรที่ได้จากการคำนวณหาความเสี่ยงของการประเมินช่องโหว่ที่ประเมินพบตามสมการ โอกาสที่จะเกิด x ผลกระทบ (L x I) คิดเป็นอัตราส่วนร้อยละ ตามภาพที่ 4.6



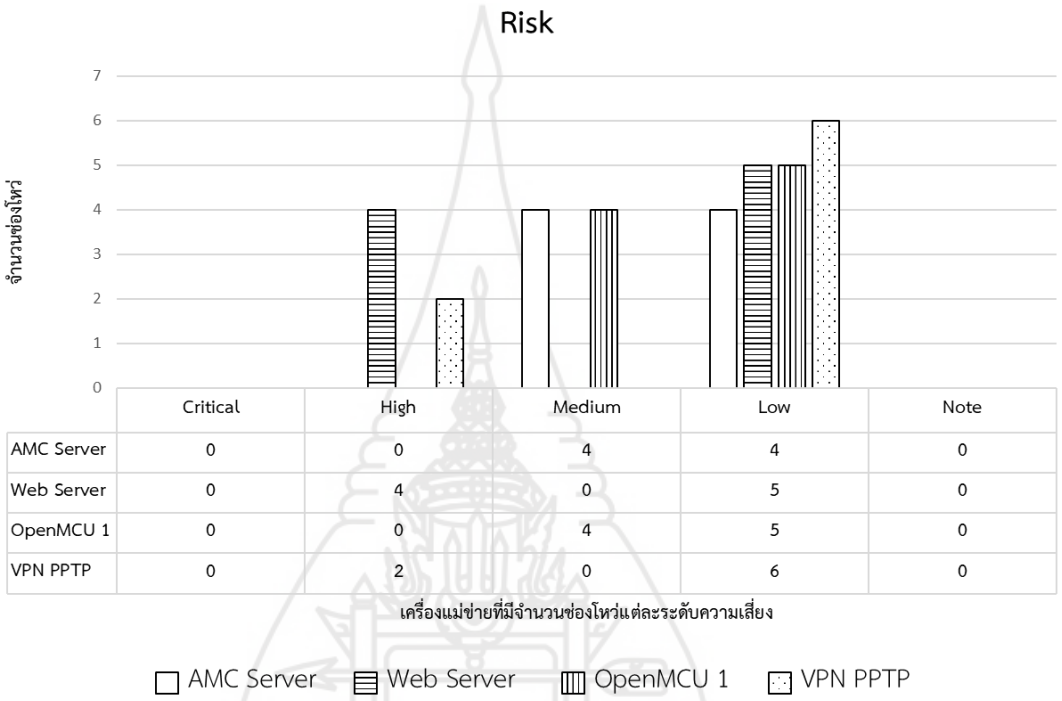
ภาพที่ 4.6 อัตราส่วนร้อยละการประเมินความเสี่ยงช่องโหว่ระบบสารสนเทศขององค์กร (Risk)

จากการประเมินความเสี่ยงของระบบสารสนเทศขององค์กรที่ได้จากการคำนวณหาความเสี่ยงของการประเมินช่องโหว่ที่ประเมินพบโดยใช้ค่าผลกระทบที่ได้มาจากการหาค่าเฉลี่ยของผลกระทบ กับ ผลกระทบต่อองค์กร (ที่คำนวณมาจากปัจจัยผลกระทบ) คือ NI = Average(I, OI) ตามสมการ โอกาสที่จะเกิด x ผลกระทบใหม่ (L x NI) คิดเป็นอัตราส่วนร้อยละ ตามภาพที่ 4.7



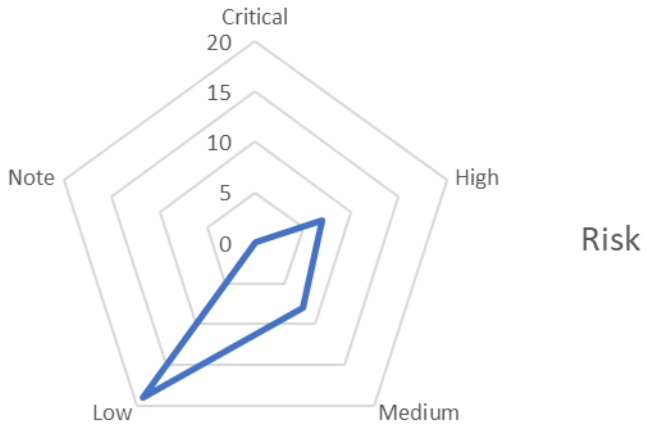
ภาพที่ 4.7 อัตราส่วนร้อยละการประเมินความเสี่ยงช่องโหว่ระบบสารสนเทศขององค์กร (Risk+)

การประเมินความเสี่ยงช่องโหว่ระบบสารสนเทศขององค์กรจากภาพที่ 4.6 พบว่าเมื่อผู้วิจัยได้เพิ่มปัจจัยผลกระทบต่อองค์กรในกรณีที่เกิดความเสียหายไม่สามารถดำเนินงานได้ จะส่งผลต่อภารกิจเสียหายร้ายแรงต่อองค์กรมากที่สุด มารวมคำนวณในการหาค่าความเสี่ยงตามภาพที่ 4.7 นั้น สามารถวิเคราะห์ภาพรวมของผลการประเมินความเสี่ยงช่องโหว่ระบบสารสนเทศขององค์กรอธิบายตามภาพที่ 4.8 ถึง 4.11 ได้ดังนี้

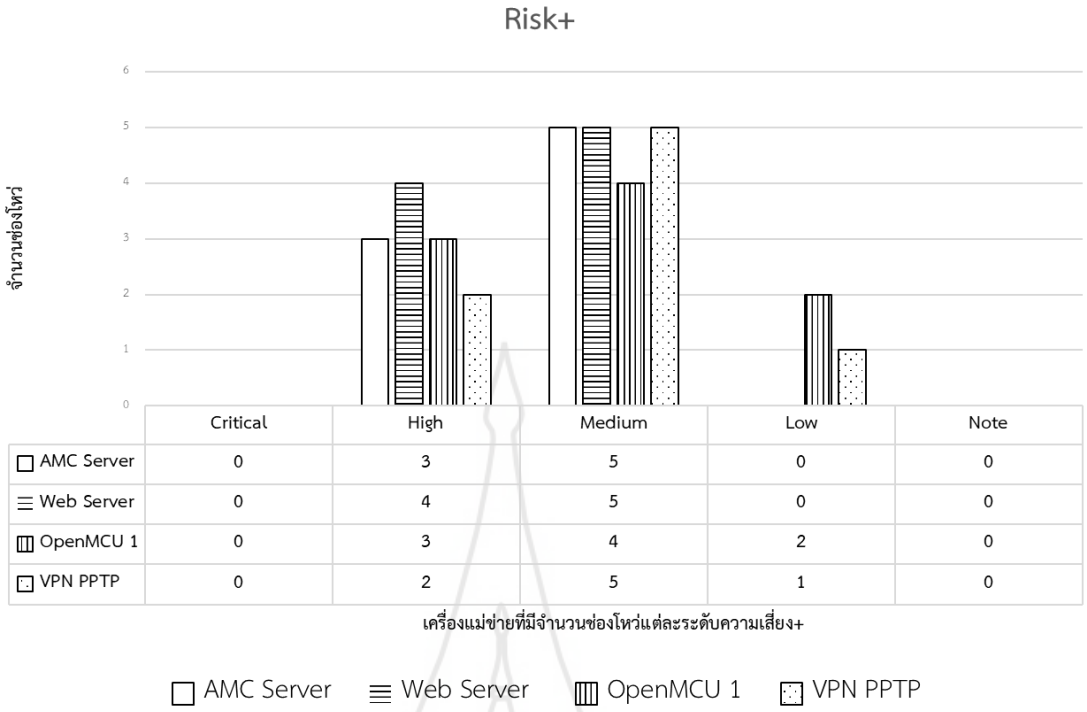


	Critical	High	Medium	Low	Note
AMC Server	0	0	4	4	0
Web Server	0	4	0	5	0
OpenMCU 1	0	0	4	5	0
VPN PPTP	0	2	0	6	0

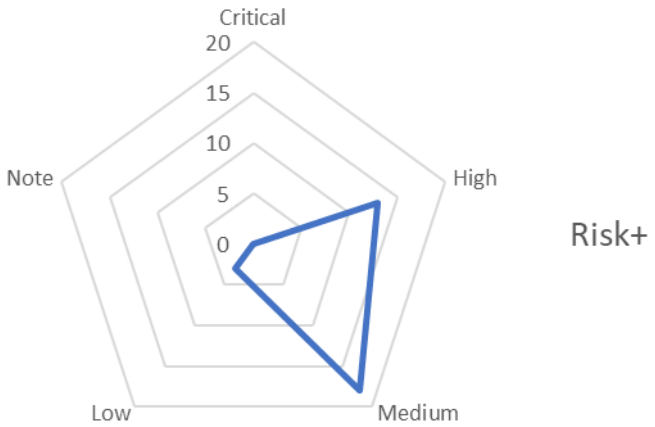
ภาพที่ 4.8 ผลการประเมินความเสี่ยงช่องโหว่ระบบสารสนเทศขององค์กร (Risk)



ภาพที่ 4.9 ภาพรวมผลการประเมินความเสี่ยงช่องโหว่ระบบสารสนเทศขององค์กร (Risk)



ภาพที่ 4.10 ผลการประเมินความเสี่ยงช่องโหว่ระบบสารสนเทศขององค์กร (Risk+)



ภาพที่ 4.11 ภาพรวมผลการประเมินความเสี่ยงช่องโหว่ระบบสารสนเทศขององค์กร (Risk+)

พบว่าก่อนเพิ่มปัจจัยผลกระทบขององค์กร ภาพรวมระบบสารสนเทศขององค์กรมีแนวโน้มระดับความเสี่ยงอยู่ในระดับต่ำถึงระดับกลางเล็กน้อย และหลังเพิ่มปัจจัยผลกระทบขององค์กร มีแนวโน้มความเสี่ยงอยู่ในระดับกลางถึงระดับสูง แสดงดังภาพที่ 4.6 ถึง 4.11 ซึ่งสามารถวิเคราะห์ได้ว่าอุปกรณ์ระบบสารสนเทศที่มีความสำคัญต่อองค์กร เป็นอีกปัจจัยความเสี่ยงและเมื่อนำเป็นปัจจัยผลกระทบต่อองค์กรมาร่วมในการประเมินความเสี่ยงช่องโหว่ระบบสารสนเทศขององค์กรจะส่งผลให้เกิดความเสี่ยงสูงขึ้น ดังนั้นนอกจากจะแก้ไขในเรื่องของช่องโหว่ระบบสารสนเทศแล้ว สำหรับอุปกรณ์เองก็ต้องมีแผนงานรองรับ เพื่อสนับสนุนและป้องกันการเกิดภารกิจที่อาจเกิดความเสียหายด้วย

2.4 รายงานผลการประเมินความเสี่ยงช่องโหว่ระบบสารสนเทศขององค์กรพร้อมรายละเอียดช่องโหว่และข้อเสนอแนะในการแก้ไข (Report)

ตารางที่ 4.12 รูปแบบรายงานผลการประเมินความเสี่ยงช่องโหว่ระบบสารสนเทศขององค์กรพร้อมรายละเอียดช่องโหว่และข้อเสนอแนะในการแก้ไข

ลำดับ	ชื่อช่องโหว่	ข้อมูลอ้างอิง	อุปกรณ์สารสนเทศ	รายละเอียด	ข้อเสนอแนะในการแก้ไข	RISK+
1.	Nameserver Processes Recursive Queries	1. dns-processes-recursive-queries	AMC Server Port: 53 / UDP	การอนุญาตให้ Nameserver ประมวลผลการสืบค้นแบบเรียกซ้ำที่มาจากระบบอื่นๆ ในบางสถานการณ์ อาจถูกผู้โจมตีดำเนินการโจมตีแคชซึ่งทำให้เกิดการหยุดให้บริการของเครื่องแม่ข่ายได้	ปิดการใช้งานการเรียกซ้ำบนเซิร์ฟเวอร์ DNS	High
2.	DNS server allows cache snooping	1. dns-allows-cache-snooping	AMC Server Port: 53 / UDP / TCP	เครื่องแม่ข่าย DNS สามารถสืบค้นข้อมูลแบบไม่เรียกซ้ำได้ โดยมองหาบันทึกที่อาจได้รับการแก้ไขแล้วโดยเครื่องแม่ข่าย DNS ผู้โจมตีสามารถใช้ข้อมูลนี้เพื่อเริ่มการโจมตีได้	จำกัดการประมวลผลการสืบค้น DNS เฉพาะระบบที่ควรได้รับอนุญาตให้ใช้เนมเซิร์ฟเวอร์นี้	High

ตารางที่ 4.12 (ต่อ)

ลำดับ	ชื่อช่องโหว่	ข้อมูลอ้างอิง	อุปกรณ์สารสนเทศ	รายละเอียด	ข้อเสนอแนะในการแก้ไข	RISK+
3.	TLS/SSL Server is enabling the BEAST attack	1. CVE-2011-3389	AMC Server Port: 53 / UDP / TCP	ผู้โจมตีอาจเข้าถึงการสนทนาระหว่างเว็บเซิร์ฟเวอร์และเว็บเบราว์เซอร์ได้โดยใช้เทคนิคการโจมตีแบบคนกลาง หากไม่มีการเข้ารหัส จะสามารถเข้าถึงข้อมูลทั้งหมดที่แลกเปลี่ยนระหว่างเว็บเซิร์ฟเวอร์และเว็บเบราว์เซอร์ การเข้ารหัส TLS 1.0 หรือเก่ากว่า สามารถถูกทำลายได้อย่างรวดเร็ว ทำให้ผู้โจมตีมีโอกาสรับฟังการสนทนา หากเซิร์ฟเวอร์รองรับ TLS 1.0 ผู้โจมตีสามารถทำให้เชื่อว่านี่เป็นโพรโทคอลเดียวที่ไคลเอ็นต์สามารถใช้ได้ สิ่งนี้เรียกว่าการโจมตีดาวน์เกรดโพรโทคอล จากนั้นผู้โจมตีสามารถใช้การโจมตีของ BEAST เพื่อดักฟังได้	ปิดใช้งานโพรโทคอล SSLv3 และ TLS 1.0 เปิดใช้งาน โพรโทคอล TLS 1.2	High
4.	FTP credentials transmitted unencrypted	1. ftp-plaintext-auth	WEB Server Port: 21 / TCP	เซิร์ฟเวอร์สนับสนุนวิธีการรับรองความถูกต้องโดยข้อมูลประจำตัวจะถูกส่งเป็นข้อความธรรมดาผ่านช่องทางที่ไม่ได้เข้ารหัส ผู้โจมตีสามารถดักการรับส่งข้อมูลระหว่างไคลเอนต์และเซิร์ฟเวอร์นี้ ข้อมูลประจำตัวจะถูกเปิดเผย	ปิดใช้งานวิธีการตรวจสอบข้อความธรรมดาหรือเปิดใช้งานการเข้ารหัสสำหรับบริการ FTP	High

ตารางที่ 4.12 (ต่อ)

ลำดับ	ชื่อช่องโหว่	ข้อมูลอ้างอิง	อุปกรณ์สารสนเทศ	รายละเอียด	ข้อเสนอแนะในการแก้ไข	RISK+
5.	X.509 Certificate Subject CN Does Not Match the Entity Name	1. certificate-common-name-mismatch	WEB Server Port: 21 / TCP	ในการตรวจจับและป้องกันการโจมตีแบบแอบฟังจะต้องตรวจสอบความถูกต้องของใบรับรอง ไม่เช่นนั้นผู้โจมตีอาจเปิดการโจมตีแบบคนกลางและเข้าควบคุมสตรีมข้อมูลได้อย่างเต็มที่ สิ่งที่สำคัญเป็นพิเศษคือความถูกต้องของ CN ของหัวเรื่อง ซึ่งควรตรงกับชื่อของเอนทิตี (ชื่อโฮสต์)	ฟิลด์ชื่อสามัญของหัวเรื่อง (CN) ในใบรับรอง X.509 ควรได้รับการแก้ไขเพื่อให้สอดคล้องกับชื่อของเอนทิตีที่แสดงใบรับรอง (เช่น ชื่อโฮสต์) ซึ่งทำได้โดยการตรวจสอบความถูกต้องของ Certificate หรือ เปลี่ยนไปใช้ Certificate ที่ออกโดยหน่วยงานหรือองค์กรที่เป็นที่ยอมรับในระดับสากล	High
6.	Self-signed TLS/SSL certificate on 203.xxx.xxx.xxx	1. ssl-self-signed-certificate	WEB Server Port: 21 / TCP	ใบรับรอง TLS/SSL ของเซิร์ฟเวอร์มีการลงชื่อด้วยตนเอง ใบรับรองที่ลงนามเองไม่สามารถเชื่อถือได้ตามค่าเริ่มต้น โดยเฉพาะอย่างยิ่งเนื่องจากการโจมตีโดยคนกลาง TLS/SSL มักใช้ใบรับรองที่ลงนามเองเพื่อดักฟังการเชื่อมต่อ TLS/SSL	ตรวจสอบความถูกต้องของ Certificate หรือ เปลี่ยนไปใช้ Certificate ที่ออกโดยหน่วยงานหรือองค์กรที่เป็นที่ยอมรับในระดับสากล	High
7.	Test-cgi Script Information Disclosure Vulnerability	1. CVE-1999-0070 2. http-apache-0010	WEB Server Port: 888 / 80 / 443 / TCP	เว็บเซิร์ฟเวอร์สร้างสคริปต์ทดสอบที่เปิดเผยรายละเอียดการกำหนดค่าของเว็บเซิร์ฟเวอร์แก่ใครก็ตามที่สามารถเชื่อมต่อกับเครื่องได้	ค้นหาไฟล์ "test-cgi" ในโครงสร้างการติดตั้ง Apache โดยปกติในไดเร็กทอรีชื่อ "cgi-bin" ให้ย้ายไฟล์นี้หรือลบทิ้ง	High

ตารางที่ 4.12 (ต่อ)

ลำดับ	ชื่อช่องโหว่	ข้อมูลอ้างอิง	อุปกรณ์สารสนเทศ	รายละเอียด	ข้อเสนอแนะในการแก้ไข	RISK+
8.	Unix Operating System Unsupported Version Detection	1. tenable plugins #33850 2. IAVA: 0001-A-0502, 0001-A-0648	OpenMCU 1	การขาดการสนับสนุนหมายความว่าผู้ผลิตจะไม่ออกแพตช์ความปลอดภัยใหม่สำหรับผลิตภัณฑ์ ดังนั้นจึงมีแนวโน้มที่จะมีช่องโหว่ด้านความปลอดภัย	อัปเกรดเป็นเวอร์ชันของระบบปฏิบัติการ Unix ที่ได้รับการสนับสนุนในปัจจุบัน	High
9.	SSH Weak Algorithms Supported	1. tenable plugins #90317	OpenMCU 1 Port: 22 / tcp / ssh	Nessus ตรวจพบว่าเซิร์ฟเวอร์ ที่ให้บริการ SSH ระยะไกลได้กำหนดค่าการใช้รหัส Arcfour หรือไม่มีรหัสเลย ซึ่งการเข้า Arcfour เป็นการเข้ารหัสที่อ่อนแอ	ปิดใช้งานอัลกอริทึม HMAC MD5 ที่ใช้ 96 บิต หรือน้อยกว่า 128 บิต โดยกำหนดค่าที่ภายในการกำหนดค่า sshd_config	High
10.	SSH Server Supports RC4 Cipher Algorithms	1. ssh-rc4-ciphers	OpenMCU 1 Port: 22 / tcp	เซิร์ฟเวอร์ที่ให้บริการ SSH ระยะไกลได้กำหนดค่าการเข้ารหัส Arcfour หรือ RC4 เป็นการเข้ารหัสที่อ่อนแอ ถูกถอดรหัสได้ง่าย	ปิดใช้งานการสนับสนุน SSH สำหรับการเข้ารหัส RC4 โดยลบ arcfour, arcfour128 และ arcfour256 ออกจากรายการ Ciphers ที่ระบุใน sshd_config	High

ตารางที่ 4.12 (ต่อ)

ลำดับ	ชื่อช่องโหว่	ข้อมูลอ้างอิง	อุปกรณ์สารสนเทศ	รายละเอียด	ข้อเสนอแนะในการแก้ไข	RISK+
11.	X.509 Certificate Subject CN Does Not Match the Entity Name	1. certificate-common-name-mismatch	VPN PPTP Port: 4444 / TCP	ในการตรวจจับและป้องกันการโจมตีแบบแอบฟัง จะต้องตรวจสอบความถูกต้องของใบรับรอง ไม่เช่นนั้นผู้โจมตีอาจเปิดการโจมตีแบบคนกลางและเข้าควบคุมสตรีมข้อมูลได้อย่างเต็มที่ สิ่งที่สำคัญเป็นพิเศษคือความถูกต้องของ CN ของหัวเรื่อง ซึ่งควรตรงกับชื่อของเอนทิตี (ชื่อโฮสต์)	ฟิลด์ชื่อสามัญของหัวเรื่อง (CN) ในใบรับรอง X.509 ควรได้รับการแก้ไขเพื่อให้สอดคล้องกับชื่อของเอนทิตีที่แสดงใบรับรอง (เช่น ชื่อโฮสต์) ซึ่งทำได้โดยการสร้างใบรับรองใหม่ซึ่งมักจะลงนามโดยผู้ออกใบรับรอง (CA) ที่ได้รับความไว้วางใจจากทั้งไคลเอนต์และเซิร์ฟเวอร์	High
12.	Untrusted TLS/SSL server X.509 certificate	1. tls-untrusted-ca	VPN PPTP Port: 4444 / tcp	ใบรับรอง TLS/SSL ของเซิร์ฟเวอร์ได้รับการลงนามโดยผู้ออกใบรับรอง (CA) ที่ไม่เป็นที่รู้จักหรือไม่น่าเชื่อถือ กรณีนี้อาจเกิดขึ้นได้จากใบรับรองหมดอายุหรือถูกเพิกถอน ชื่อโฮสต์ของเซิร์ฟเวอร์ไม่ตรงกับที่กำหนดค่าไว้ในใบรับรอง เวลา/วันที่ไม่ถูกต้อง หรือใช้ใบรับรองที่ลงนามเอง	จัดหาใบรับรองใหม่จาก CA ที่มีมาตรฐานระดับสากล และตรวจสอบให้แน่ใจว่าการกำหนดค่าเซิร์ฟเวอร์ถูกต้อง	High

ตารางที่ 4.12 (ต่อ)

ลำดับ	ชื่อช่องโหว่	ข้อมูลอ้างอิง	อุปกรณ์สารสนเทศ	รายละเอียด	ข้อเสนอแนะในการแก้ไข	RISK+
13.	SSL Medium Strength Cipher Suites Supported (SWEET32)	1. tenable plugins #42873 2. CVE: CVE-2016-2183	AMC Server Port :443 / tcp / www	โฮสต์ระยะไกลสนับสนุนการใช้การเข้ารหัส SSL ที่มีการเข้ารหัสระดับกลาง ถือว่ามีความรุนแรงปานกลางเป็นการเข้ารหัสที่ใช้ความยาวของกุญแจ (มากกว่า 64 บิต และน้อยกว่า 112 บิต key, or 3DES)	ปรับตั้งค่าให้รับการเข้ารหัส SSL Cipher มีความปลอดภัยมากกว่า 112 bit (3DES) กำหนดค่าเว็บเซิร์ฟเวอร์ให้เข้ารหัสแบบ 128 บิต และแก้ไข SWEET32 โดยการปิดใช้งาน 3DES Value=0	Med
14.	TLS Version 1.0 Protocol Detection	1. tenable plugins #104743	AMC Server Port: 443 / tcp / www	การเชื่อมต่อที่เข้ารหัสโดยใช้ TLS 1.0 มีข้อบกพร่องในการออกแบบการเข้ารหัสจำนวนมาก	ปิดใช้งาน TLS 1.0 ให้เปิดใช้งาน TLS 1.2 และ 1.3	Med
15.	TLS Version 1.1 Protocol Deprecated	1. tenable plugins #157288	AMC Server Port: 443 / tcp / www	การเชื่อมต่อที่เข้ารหัสโดยใช้ TLS 1.1 มีข้อบกพร่องในการออกแบบการเข้ารหัสจำนวนมาก	ปิดใช้งาน TLS 1.1 ให้เปิดใช้งาน TLS 1.2 และ 1.3	Med
16.	HTTP OPTIONS Method Enabled	1. http-options-method-enabled	AMC Server Port: 443 / tcp / www	เว็บเซิร์ฟเวอร์ที่ตอบสนองต่อเมธอด OPTIONS HTTP จะเปิดเผยวิธีอื่นๆ ที่เว็บเซิร์ฟเวอร์สนับสนุน ซึ่งช่วยให้ผู้โจมตีจำกัดขอบเขตและเพิ่มความพยายาม	ปิดใช้งานวิธี HTTP OPTIONS บนเว็บเซิร์ฟเวอร์	Med

ตารางที่ 4.12 (ต่อ)

ลำดับ	ชื่อช่องโหว่	ข้อมูลอ้างอิง	อุปกรณ์สารสนเทศ	รายละเอียด	ข้อเสนอแนะในการแก้ไข	RISK+
17.	TLS/SSL Server Supports The Use of Static Key Ciphers	1. ssl-static-key-ciphers	AMC Server Port: 443 / tcp / www	เซิร์ฟเวอร์ได้รับการกำหนดค่าให้รองรับการเข้ารหัสที่เรียกว่ารหัสลับแบบคงที่ รหัสเหล่านี้ไม่รองรับ "Forward Secrecy" ในข้อกำหนดใหม่สำหรับ HTTP/2 การเข้ารหัสเหล่านี้ถูกขึ้นบัญชีดำ	Microsoft IIS ปิดใช้งานชุดการเข้ารหัสกุญแจคงที่ ปิดการใช้งาน โพรโทคอล SSLv2, SSLv3 และ TLSv1 ของ Firefox 27, Chrome 22, IE 11, Opera 14 และ Safari 7 ให้ใช้โพรโทคอล TLSv1.1 และ TLSv1.2 แทน	Med
18.	SSL Certificate Cannot Be Trusted	1. tenable plugins #51192	WEB Server Port: 21 / tcp / ftp	SSL Certificate มีลายมือชื่อดิจิทัลที่ไม่เป็นที่ยอมรับหรือมีการจัดทำ Certificate โดยหน่วยงานที่ไม่เป็นที่ยอมรับในระดับสากล	ซื้อหรือสร้างใบรับรอง SSL Certificate ที่ออกโดยหน่วยงานหรือองค์กรที่เป็นที่ยอมรับในระดับสากล	Med
19.	SSL Self-Signed Certificate	1. tenable plugins #57582	WEB Server Port: 21 / tcp / ftp	SSL Certificate มีลายมือชื่อดิจิทัลที่ไม่เป็นที่ยอมรับหรือมีการจัดทำ Certificate โดยหน่วยงานที่ไม่เป็นที่ยอมรับในระดับสากล	ซื้อหรือสร้างใบรับรอง SSL Certificate ที่ออกโดยหน่วยงานหรือองค์กรที่เป็นที่ยอมรับในระดับสากล	Med
20.	Untrusted TLS/SSL server X.509 certificate	1. tls-untrusted-ca	WEB Server Port: 21 / 443 / TCP	SSL Certificate มีลายมือชื่อดิจิทัลที่ไม่เป็นที่ยอมรับหรือมีการจัดทำ Certificate โดยหน่วยงานที่ไม่เป็นที่ยอมรับในระดับสากล	ซื้อหรือสร้างใบรับรอง SSL Certificate ที่ออกโดยหน่วยงานหรือองค์กรที่เป็นที่ยอมรับในระดับสากล	Med

ตารางที่ 4.12 (ต่อ)

ลำดับ	ชื่อช่องโหว่	ข้อมูลอ้างอิง	อุปกรณ์สารสนเทศ	รายละเอียด	ข้อเสนอแนะในการแก้ไข	RISK+
21.	HTTP OPTIONS Method Enabled	1. http-options-method-enabled	WEB Server Port: 888 / TCP	เว็บเซิร์ฟเวอร์ที่ตอบสนองต่อเมธอด OPTIONS HTTP จะเปิดเผยวิธีอื่นๆ ที่เว็บเซิร์ฟเวอร์สนับสนุน ซึ่งช่วยให้ผู้โจมตีจำกัดขอบเขตและเพิ่มความพยายาม	ปิดใช้งานเมธอด OPTIONS โดยรวมสิ่งต่อไปนี้ในการกำหนดค่า Apache: <Limit OPTIONS> Order deny,allow Deny from all </Limit>	Med
22.	TLS/SSL Server Supports The Use of Static Key Ciphers	1. ssl-static-key-ciphers	WEB Server Port: 443 / TCP CATEGORIES: Network	เซิร์ฟเวอร์ได้รับการกำหนดค่าให้รองรับการเข้ารหัสที่เรียกว่ารหัสลับแบบคงที่ รหัสเหล่านี้ไม่รองรับ "Forward Secrecy" ในข้อกำหนดใหม่สำหรับ HTTP/2 การเข้ารหัสเหล่านี้ถูกขึ้นบัญชีดำ	ปิดใช้งานการสนับสนุน TLS/SSL สำหรับชุดการเข้ารหัสกุญแจแบบคงที่โพรโทคอล SSLv2, SSLv3 และ TLSv1 และการกำหนดค่าสำหรับ Firefox 27, Chrome 22, IE 11, Opera 14 และ Safari 7 ให้ใช้โพรโทคอล TLSv1.1 และ TLSv1.2 แทน	Med

ตารางที่ 4.12 (ต่อ)

ลำดับ	ชื่อช่องโหว่	ข้อมูลอ้างอิง	อุปกรณ์สารสนเทศ	รายละเอียด	ข้อเสนอแนะในการแก้ไข	RISK+
23.	SSH Birthday attacks on 64-bit block ciphers (SWEET32)	1. CVE: CVE-2016-2183	OpenMCU 1 Port: 22 / tcp	รหัสบล็อกดั้งเดิมที่มีขนาดบล็อก 64 บิตมีความเสี่ยงที่จะเกิดการชนกันในทางปฏิบัติเมื่อใช้ในโหมด Cipher Block Chaining (CBC) ความปลอดภัยของรหัสบล็อกมักจะลดลงเหลือขนาดกุญแจ เข้ารหัส เป็นไปได้ที่จะใช้การชนกันเพื่อดึงข้อมูลข้อความธรรมดา	ปิดใช้งานการสนับสนุน SSH สำหรับชุดการเข้ารหัส 3DES ลบการเข้ารหัส 3DES ทั้งหมดออกจากรายการรหัสที่ระบุในsshd_config	Med
24.	Unencrypted Telnet Server	1. tenable plugins #42263	OpenMCU 1 Port: 1423 / tcp / telnet	โฮสต์ระยะไกลกำลังเรียกใช้เซิร์ฟเวอร์ Telnet ผ่านช่องทางที่ไม่ได้เข้ารหัส	ปิดใช้งานบริการ Telnet และใช้ SSH แทน	Med
25..	SSH Server CBC Mode Ciphers Enabled	1. tenable plugins #70658	OpenMCU 1 Port: 22 / tcp / ssh	เซิร์ฟเวอร์ SSH ได้รับการกำหนดค่าให้รองรับการเข้ารหัส Cipher Block Chaining (CBC) วิธีนี้อาจทำให้ผู้โจมตีสามารถกู้คืนข้อความธรรมดาจากข้อความไซเฟอร์เท็กซ์ได้	ติดต่อผู้จำหน่ายหรือศึกษาเอกสารประกอบของผลิตภัณฑ์เพื่อปิดใช้งานการเข้ารหัสลับโหมด CBC และเปิดใช้งานการเข้ารหัสโหมดการเข้ารหัส CTR หรือ GCM	Med
26.	SSH Weak MAC Algorithms Enabled	1. tenable plugins #71049	OpenMCU 1 Port: 22 / tcp / ssh	เซิร์ฟเวอร์ SSH ระยะไกลได้รับการกำหนดค่าให้อนุญาตอัลกอริทึม MD5 และ MAC 96 บิต ซึ่งทั้งสองอย่างนี้ถือว่าอ่อนแอ	ติดต่อผู้จำหน่ายหรือศึกษาเอกสารประกอบผลิตภัณฑ์เพื่อปิดใช้งานอัลกอริทึม MD5 และ MAC 96 บิต	Med

ตารางที่ 4.12 (ต่อ)

ลำดับ	ชื่อช่องโหว่	ข้อมูลอ้างอิง	อุปกรณ์สารสนเทศ	รายละเอียด	ข้อเสนอแนะในการแก้ไข	RISK+
27..	SSL Certificate Cannot Be Trusted	1. tenable plugins #51192	VPN PPTP Port: 4444 / tcp / www	SSL Certificate มีลายมือชื่อดิจิทัลที่ไม่เป็นที่ยอมรับหรือมีการจัดทำ Certificate โดยหน่วยงานที่ไม่เป็นที่ยอมรับในระดับสากล	ซื้อหรือสร้างใบรับรอง SSL ที่เหมาะสมสำหรับบริการนี้	Med
28.	SSL Self-Signed Certificate	1. tenable plugins #57582	VPN PPTP Port: 4444 / tcp / www	SSL Certificate มีลายมือชื่อดิจิทัลที่ไม่เป็นที่ยอมรับหรือมีการจัดทำ Certificate โดยหน่วยงานที่ไม่เป็นที่ยอมรับในระดับสากล	ซื้อหรือสร้างใบรับรอง SSL ที่เหมาะสมสำหรับบริการนี้	Medium
29.	TLS Server Supports TLS version 1.1	1. tlsv1_1-enabled	VPN PPTP Port: 4444 / tcp	การเชื่อมต่อที่การเข้ารหัสที่รุ่นต่ำกว่า TLS 1.1 มีข้อบกพร่องในการออกแบบการเข้ารหัสจำนวนมาก	ปิดใช้งานการสนับสนุนโพรโทคอล TLS/SSL ที่ไม่ปลอดภัยกำหนดค่าเซิร์ฟเวอร์เพื่อให้ไคลเอนต์ใช้ TLS เวอร์ชัน 1.2 โดยใช้การเข้ารหัสที่พิสูจน์ตัวตนด้วยรหัสลับ	Med
30.	TLS/SSL Server Supports The Use of Static Key Ciphers	1. ssl-static-key-ciphers	VPN PPTP Port: 4444 / tcp	เซิร์ฟเวอร์ได้รับการกำหนดค่าให้รองรับการเข้ารหัสที่เรียกว่ารหัสลับแบบคงที่ รหัสเหล่านี้ไม่รองรับ "Forward Secrecy" ในข้อกำหนดใหม่สำหรับ HTTP/2 การเข้ารหัสเหล่านี้ถูกขึ้นบัญชีดำ	ปิดใช้งานการสนับสนุน TLS/SSL สำหรับชุดการเข้ารหัสกุญแจแบบคงที่โพรโทคอล SSLv2, SSLv3 และ TLSv1 และการกำหนดค่าสำหรับ Firefox 27, Chrome 22, IE 11, Opera 14 และ Safari 7 ให้ใช้โพรโทคอล TLSv1.1 และ TLSv1.2 แทน	Med

ตารางที่ 4.12 (ต่อ)

ลำดับ	ชื่อช่องโหว่	ข้อมูลอ้างอิง	อุปกรณ์สารสนเทศ	รายละเอียด	ข้อเสนอแนะในการแก้ไข	RISK+
31.	TLS/SSL Server Is Using Commonly Used Prime Numbers	1. tls-dh-primes	VPN PPTP Port: 4444 / tcp	เซิร์ฟเวอร์ใช้หมายเลขเฉพาะทั่วไปหรือค่าเริ่มต้นเป็นพารามิเตอร์ระหว่างการแลกเปลี่ยนกุญแจ Diffie-Hellman สิ่งนี้ทำให้เซสชั่นที่ปลอดภัยเสี่ยงต่อการโจมตีด้วยการคำนวณล่วงหน้า ผู้โจมตีสามารถใช้เวลาจำนวนมากเพื่อสร้างการค้นหา	แนะนำให้ใช้กลุ่ม DH 2048 บิตหรือสูงกว่า โดยใช้คำสั่ง CLI ต่อไปนี้ใน FortiOS: # conf ระบบ global # set dh-params 2048 # end	Med
32.	SSH Server Supports diffie-hellman-group1-sha1	1. CVE: CVE-2015-4000	OpenMCU 1 Port: 22 / tcp	โมดูลัสเฉพาะที่เสนอเมื่อใช้ diffie-hellman-group1-sha1 มีขนาด 1024 บิตเท่านั้น ขนาดนี้ถือว่าอ่อนแอและอยู่ในขอบเขตทางทฤษฎีของการโจมตีที่เรียกว่า Logjam	ปิดใช้งานการสนับสนุน SSH สำหรับ ssh-diffie-hellman-group1-sha1 ขั้นตอนการแก้ไขการกำหนดค่า ลบ ssh-diffie-hellman-group1-sha1 ออกจากรายการ KexAlgorithms ที่ระบุใน sshd_config	Low

ตารางที่ 4.12 (ต่อ)

ลำดับ	ชื่อช่องโหว่	ข้อมูลอ้างอิง	อุปกรณ์สารสนเทศ	รายละเอียด	ข้อเสนอแนะในการแก้ไข	RISK+
33.	SSH Weak Key Exchange Algorithms Enabled	1. tenable plugins #1539537	OpenMCU 1 Port: 22 / tcp / ssh	เซิร์ฟเวอร์ SSH ระยะไกลได้รับการกำหนดค่าให้อนุญาตอัลกอริทึมการแลกเปลี่ยนกุญแจซึ่งถือว่าอ่อนแอ	การแก้ไขการเปิดใช้งานอัลกอริทึมการแลกเปลี่ยนคีย์ SSH ที่อ่อนแอ แก้ไข/etc/ssh/sshd_config ให้ใช้ค่า KexAlgorithms curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256	Low
34.	TLS Version 1.1 Protocol Deprecated	1. tenable plugins #157288	VPN PPTP Port: 4444 / tcp / www	การเชื่อมต่อที่เข้ารหัสโดยใช้ TLS 1.1 มีข้อบกพร่องในการออกแบบการเข้ารหัสจำนวนมาก	เปิดใช้งานการสนับสนุนสำหรับ TLS 1.2 และ/หรือ 1.3 และปิดใช้งานการสนับสนุนสำหรับ TLS 1.1	Low

3. การแก้ไข (Remediation)

ผู้วิจัยได้นำเสนอรายงานผลการประเมินความเสี่ยงช่องโหว่ระบบสารสนเทศขององค์กร พร้อมรายละเอียดช่องโหว่และข้อเสนอแนะในการแก้ไข ต่อบุคลากรที่มีส่วนเกี่ยวข้องกับระบบสารสนเทศขององค์กร เพื่อดำเนินการแก้ไขช่องโหว่ที่ประเมินพบตามรายการในตารางที่ 4.12 พร้อมกับรายงานการดำเนินการแก้ไขช่องโหว่ที่ประเมินพบโดยมีรายละเอียดการแก้ไขตามตารางที่ 4.13 ดังนี้

ตารางที่ 4.13 รายงานการแก้ไขช่องโหว่ระบบสารสนเทศขององค์กรที่ประเมินพบ

ลำดับ	ชื่อช่องโหว่	อุปกรณ์สารสนเทศ	การดำเนินการแก้ไขช่องโหว่	ผลการแก้ไข
1.	Nameserver Processes Recursive Queries	AMC Server Port: 53 / UDP	ปิดการใช้งานการเรียกซ้ำบนเซิร์ฟเวอร์ DNS	แก้ไขเรียบร้อย
2.	DNS server allows cache snooping	AMC Server Port: 53 / UDP / TCP	จำกัดการประมวลผลการสืบค้น DNS เฉพาะระบบที่ควรได้รับอนุญาตให้ใช้ Name Server	แก้ไขเรียบร้อย
3.	TLS/SSL Server is enabling the BEAST attack	AMC Server Port: 53 / UDP / TCP	ปิดใช้งาน SSLv3 และ TLS 1.0 เปิดการใช้งาน TLS 1.2	แก้ไขเรียบร้อย
4.	FTP credentials transmitted unencrypted	WEB Server Port: 21 / TCP	เปิดใช้งานการเข้ารหัสสำหรับบริการ FTP	แก้ไขเรียบร้อย
5.	X.509 Certificate Subject CN Does Not Match the Entity Name	WEB Server Port: 21 / TCP	เปลี่ยนไปใช้ Certificate ที่ออกโดยหน่วยงานหรือองค์กรที่เป็นที่ยอมรับในระดับสากล	แก้ไขเรียบร้อย
6.	Self-signed TLS/SSL certificate on 203.xxx.xxx.xxx	WEB Server Port: 21 / TCP	เปลี่ยนไปใช้ Certificate ที่ออกโดยหน่วยงานหรือองค์กรที่เป็นที่ยอมรับในระดับสากล	แก้ไขเรียบร้อย

ตารางที่ 4.13 (ต่อ)

ลำดับ	ชื่อช่องโหว่	อุปกรณ์สารสนเทศ	การดำเนินการแก้ไขช่องโหว่	ผลการแก้ไข
7.	Test-cgi Script Information Disclosure Vulnerability	WEB Server Port: 888 / 80 / 443 / TCP	ย้าย "test-cgi" ออกจากโฟล์เดอร์ใน "cgi-bin"	แก้ไขเรียบร้อย
8.	Unix Operating System Unsupported Version Detection	OpenMCU 1	อัปเกรดเวอร์ชันของระบบปฏิบัติการ Linux Ubantu	แก้ไขเรียบร้อย
9.	SSH Weak Algorithms Supported	OpenMCU 1 Port: 22 / tcp / ssh	กำหนดค่า SSH โดยปิดใช้งาน HMAC MD5 หรือ 96 บิต	แก้ไขเรียบร้อย
10.	SSH Server Supports RC4 Cipher Algorithms	OpenMCU 1 Port: 22 / tcp	ปิดใช้งานการเข้ารหัส RC4 ลบ arcfour, arcfour128 และ arcfour256 ออกจากรายการ Ciphers ที่ระบุใน sshd_config	แก้ไขเรียบร้อย
11.	X.509 Certificate Subject CN Does Not Match the Entity Name	VPN PPTP Port: 4444 / TCP	ปิด Port: 4444 tcp / www เนื่องจากไม่ได้ใช้งาน	แก้ไขเรียบร้อย
12.	Untrusted TLS/SSL server X.509 certificate	VPN PPTP Port: 4444 / tcp	ปิด Port: 4444 tcp / www เนื่องจากไม่ได้ใช้งาน	แก้ไขเรียบร้อย
13.	SSL Medium Strength Cipher Suites Supported (SWEET32)	AMC Server Port :443 / tcp / www	กำหนดค่าเว็บเซิร์ฟเวอร์ให้เข้ารหัสแบบ 128 บิต และแก้ไข SWEET32 โดยการปิดใช้งาน (3DES) Value=0	แก้ไขเรียบร้อย
14.	TLS Version 1.0 Protocol Detection	AMC Server Port: 443 / tcp / www	เปิดใช้งานการสนับสนุนสำหรับ TLS 1.2 และ 1.3 และปิดใช้งานการสนับสนุนสำหรับ TLS 1.0	แก้ไขเรียบร้อย

ตารางที่ 4.13 (ต่อ)

ลำดับ	ชื่อช่องโหว่	อุปกรณ์สารสนเทศ	การดำเนินการแก้ไขช่องโหว่	ผลการแก้ไข
15.	TLS Version 1.1 Protocol Deprecated	AMC Server Port: 443 / tcp / www	เปิดใช้งาน TLS 1.2 และ 1.3 และปิดใช้งาน TLS 1.1	แก้ไขเรียบร้อย
16.	HTTP OPTIONS Method Enabled	AMC Server Port: 443	ปิดใช้งานวิธี HTTP OPTIONS บนเว็บเซิร์ฟเวอร์	แก้ไขเรียบร้อย
17.	TLS/SSL Server Supports The Use of Static Key Ciphers	AMC Server Port: 443 / tcp / www	ปิดการใช้งาน SSLv2, SSLv3 และ TLSv1 บนเบราว์เซอร์ ให้ใช้โพรโทคอล TLSv1.1 และ TLSv1.2 แทน	แก้ไขเรียบร้อย
18.	SSL Certificate Cannot Be Trusted	WEB Server Port: 21 / tcp / ftp	ซื้อหรือสร้างใบรับรอง SSL Certificate ที่ออกโดยหน่วยงานหรือองค์กรที่เป็นที่ยอมรับในระดับสากล	รอการแก้ไข
19.	SSL Self-Signed Certificate	WEB Server Port: 21 / tcp / ftp	ซื้อหรือสร้างใบรับรอง SSL Certificate ที่ออกโดยหน่วยงานหรือองค์กรที่เป็นที่ยอมรับในระดับสากล	รอการแก้ไข
20.	Untrusted TLS/SSL server X.509 certificate	WEB Server Port: 21 / 443 / TCP	ซื้อหรือสร้างใบรับรอง SSL Certificate ที่ออกโดยหน่วยงานหรือองค์กรที่เป็นที่ยอมรับในระดับสากล	รอการแก้ไข
21.	HTTP OPTIONS Method Enabled	WEB Server Port: 888 / TCP	ปิดใช้งานเมธอด OPTIONS โดยแก้ไขที่ Apache: ดังนี้ <Limit OPTIONS> Order deny,allow Deny from all </Limit>	แก้ไขเรียบร้อย
22.	TLS/SSL Server Supports The Use of Static Key Ciphers	WEB Server Port: 443 / TCP	ปิดการใช้งาน SSLv2, SSLv3 และ TLSv1 บนเบราว์เซอร์ ให้ใช้โพรโทคอล TLSv1.1 และ TLSv1.2 แทน	แก้ไขเรียบร้อย

ตารางที่ 4.13 (ต่อ)

ลำดับ	ชื่อช่องโหว่	อุปกรณ์สารสนเทศ	การดำเนินการแก้ไขช่องโหว่	ผลการแก้ไข
23.	SSH Birthday attacks on 64-bit block ciphers (SWEET32)	OpenMCU 1 Port: 22 / tcp	ปิดใช้งานการสนับสนุน SSH สำหรับชุดการเข้ารหัส 3DES	แก้ไขเรียบร้อย
24.	Unencrypted Telnet Server	OpenMCU 1 Port: 1423 / tcp / telnet	ปิดใช้งานบริการ Telnet และใช้ SSH แทน	แก้ไขเรียบร้อย
25.	SSH Server CBC Mode Ciphers Enabled	OpenMCU 1 Port: 22 / tcp / ssh	ปิดใช้งานการเข้ารหัสลับโหมด CBC และเปิดใช้งานการเข้ารหัสโหมดการเข้ารหัส CTR หรือ GCM	แก้ไขเรียบร้อย
26.	SSH Weak MAC Algorithms Enabled	OpenMCU 1 Port: 22 / tcp / ssh	ปิดใช้งานอัลกอริทึม MD5 และ MAC 96 บิต	แก้ไขเรียบร้อย
27.	SSL Certificate Cannot Be Trusted	VPN PPTP Port: 4444 / tcp / www	ปิด Port: 4444 tcp / www เนื่องจากไม่ได้ใช้งาน	แก้ไขเรียบร้อย
28.	SSL Self-Signed Certificate	VPN PPTP Port: 4444 / tcp / www	ปิด Port: 4444 tcp / www เนื่องจากไม่ได้ใช้งาน	แก้ไขเรียบร้อย
29.	TLS Server Supports TLS version 1.1	VPN PPTP Port: 4444 / tcp	ปิดใช้งานการสนับสนุนโพรโทคอล TLS/SSL ที่ไม่ปลอดภัยเปิดใช้ TLS เวอร์ชัน 1.2	แก้ไขเรียบร้อย
30.	TLS/SSL Server Supports The Use of Static Key Ciphers	VPN PPTP Port: 4444 / tcp	ปิดการใช้งาน SSLv2, SSLv3 และ TLSv1 บนเบราว์เซอร์ ให้ใช้โพรโทคอล TLSv1.1 และ TLSv1.2 แทน	แก้ไขเรียบร้อย
31.	TLS/SSL Server Is Using Commonly Used Prime Numbers	VPN PPTP Port: 4444 / tcp	ปิด Port: 4444 tcp / www เนื่องจากไม่ได้ใช้งาน	แก้ไขเรียบร้อย

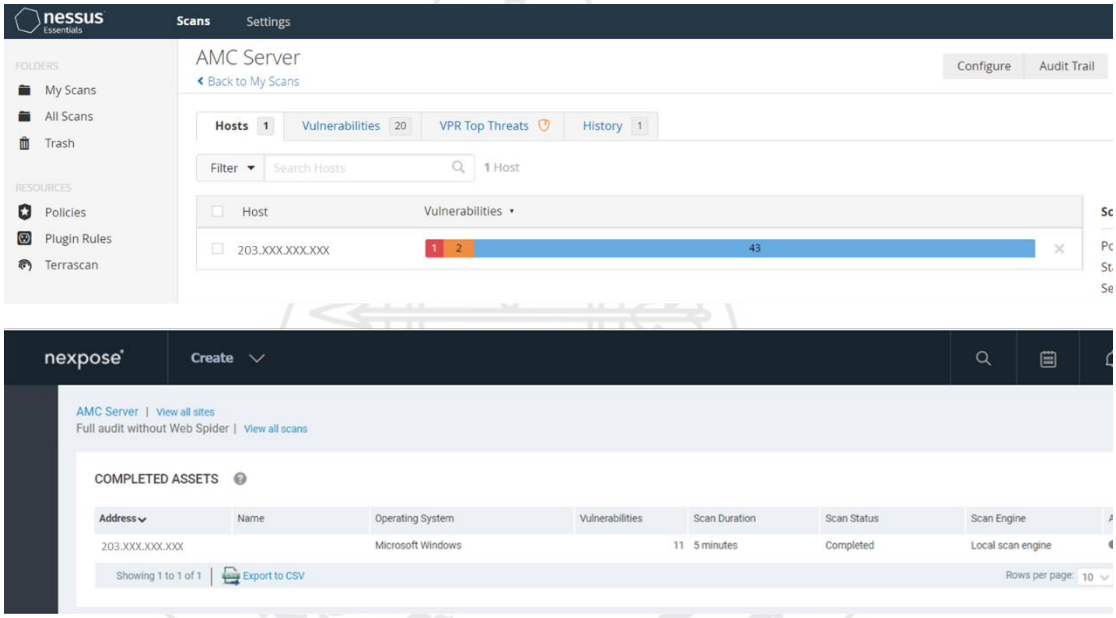
ตารางที่ 4.13 (ต่อ)

ลำดับ	ชื่อช่องโหว่	อุปกรณ์สารสนเทศ	การดำเนินการแก้ไขช่องโหว่	ผลการแก้ไข
32.	SSH Server Supports diffie-hellman-group1-sha1	OpenMCU 1 Port: 22 / tcp	ปิดใช้งานการสนับสนุน SSH สำหรับ ssh-diffie-hellman-group1-sha1	แก้ไขเรียบร้อย
33.	SSH Weak Key Exchange Algorithms Enabled	OpenMCU 1 Port: 22 / tcp / ssh	ดำเนินการแก้ไข Hashing Algorithm Certificate	แก้ไขเรียบร้อย
34.	TLS Version 1.1 Protocol Deprecated	VPN PPTP Port: 4444 / tcp / www	เปิดใช้งาน TLS 1.2 และ 1.3 และปิดใช้งาน TLS 1.1	แก้ไขเรียบร้อย

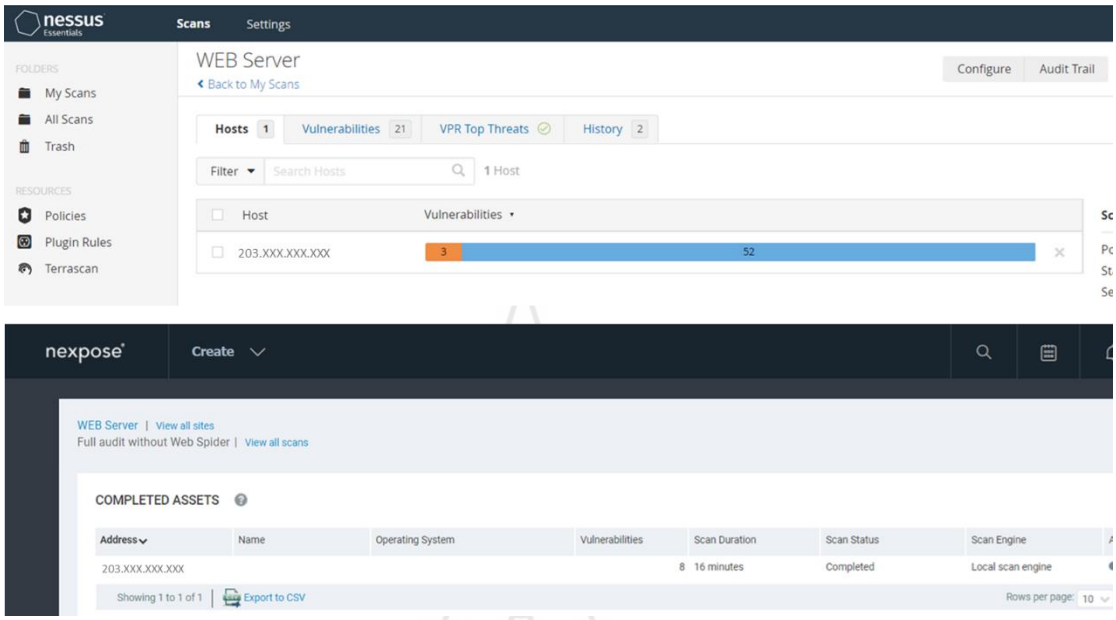
4. การประเมินซ้ำ (Re-Assessment)

หลังจากที่ได้ดำเนินการแก้ไขช่องโหว่เสร็จเรียบร้อยแล้ว นำผลจากรายงานการดำเนินการแก้ไขช่องโหว่มาดำเนินการประเมินช่องโหว่ระบบสารสนเทศขององค์กรซ้ำอีกครั้ง เพื่อให้มั่นใจได้ว่าช่องโหว่ได้ถูกแก้ไขแล้วจริง หรือถ้าแก้ไขไม่ได้จะต้องดำเนินการอย่างไร เพื่อลดความเสี่ยงช่องโหว่ที่จะมีผลกระทบต่อองค์กร ขั้นตอนการประเมินช่องโหว่ซ้ำจะดำเนินการเหมือนขั้นตอนในการประเมินช่องโหว่ระบบสารสนเทศขององค์กรทุกประการ รายละเอียดในการประเมินช่องโหว่ในการทดลองงานวิจัยมีดังนี้

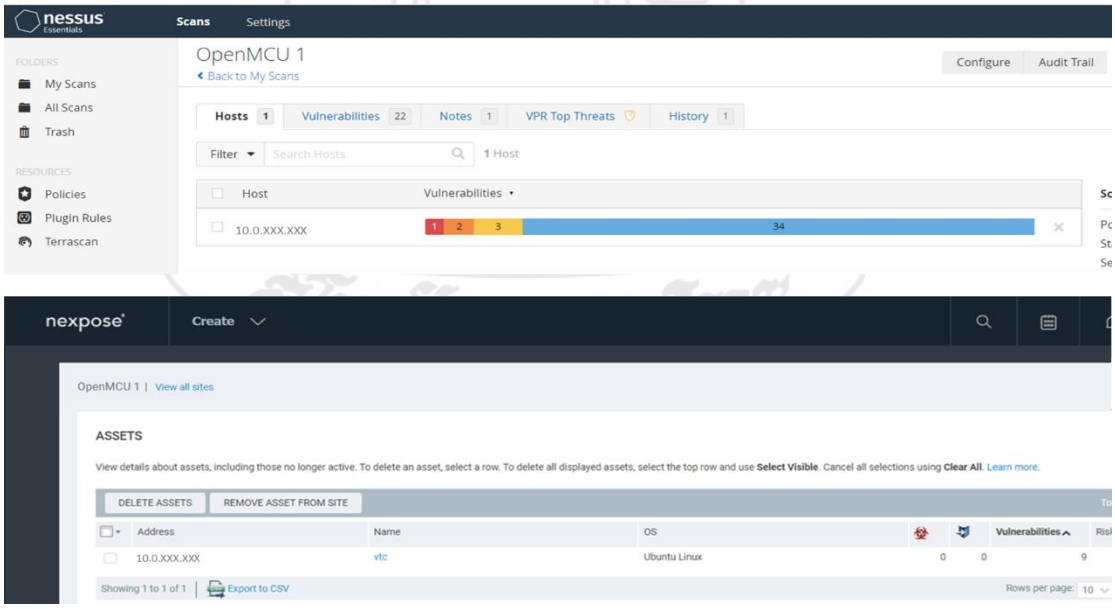
4.1 ผลการดำเนินการประเมินช่องโหว่ระบบสารสนเทศขององค์กรก่อนการแก้ไขช่องโหว่ตามภาพที่ 4.12 ถึง 4.15



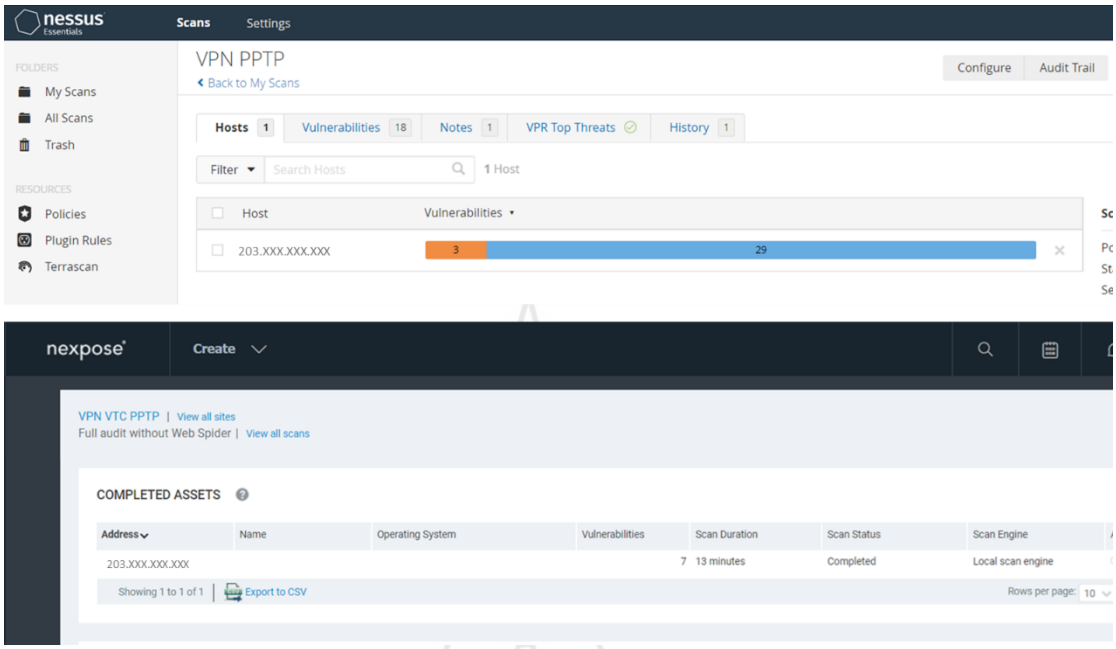
ภาพที่ 4.12 ผลการสแกนอุปกรณ์สารสนเทศ AMC Server ก่อนการแก้ไขช่องโหว่ของเครื่องมือ Nessus และ Nexpose



ภาพที่ 4.13 ผลการสแกนอุปกรณ์สารสนเทศ WEB Server ก่อนการแก้ไขช่องโหว่ของเครื่องมือ Nessus และ Nexpose



ภาพที่ 4.14 ผลการสแกนอุปกรณ์สารสนเทศ Open MCU 1 ก่อนการแก้ไขช่องโหว่ของเครื่องมือ Nessus และ Nexpose

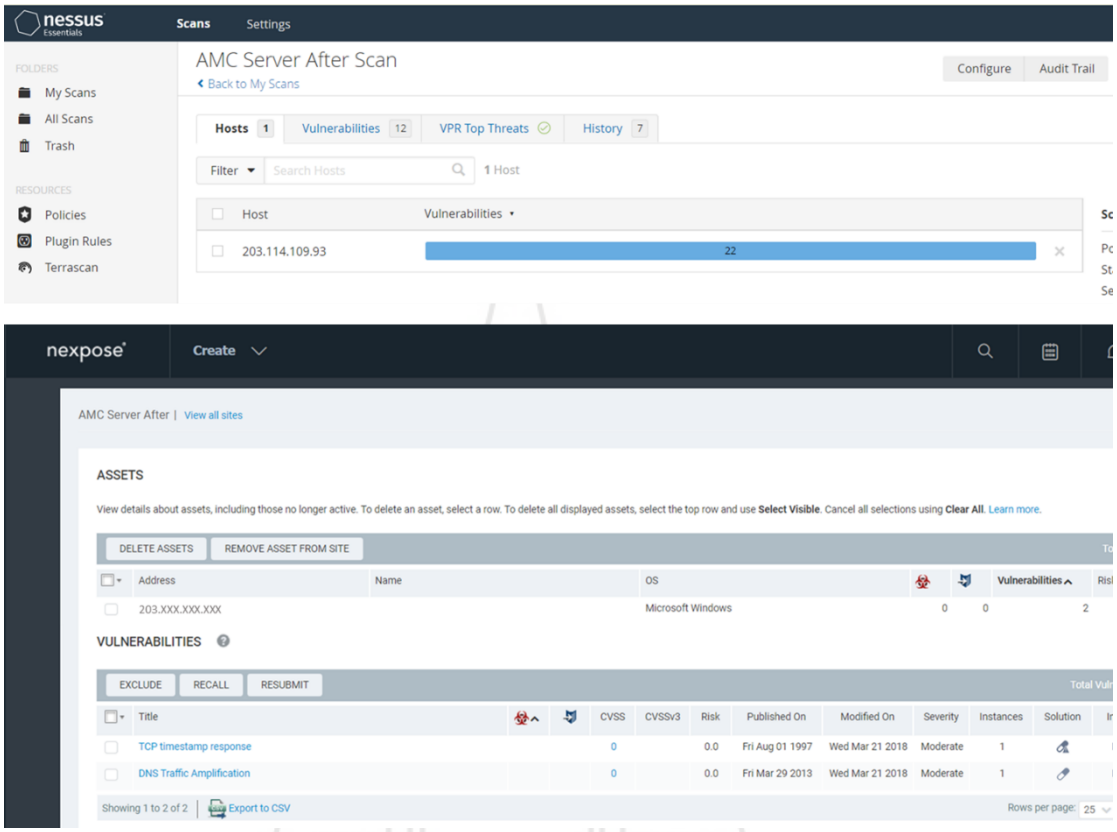


ภาพที่ 4.15 ผลการสแกนอุปกรณ์สารสนเทศ VPN PPTP ก่อนการแก้ไขช่องโหว่ของเครื่องมือ Nessus และ Nexpose

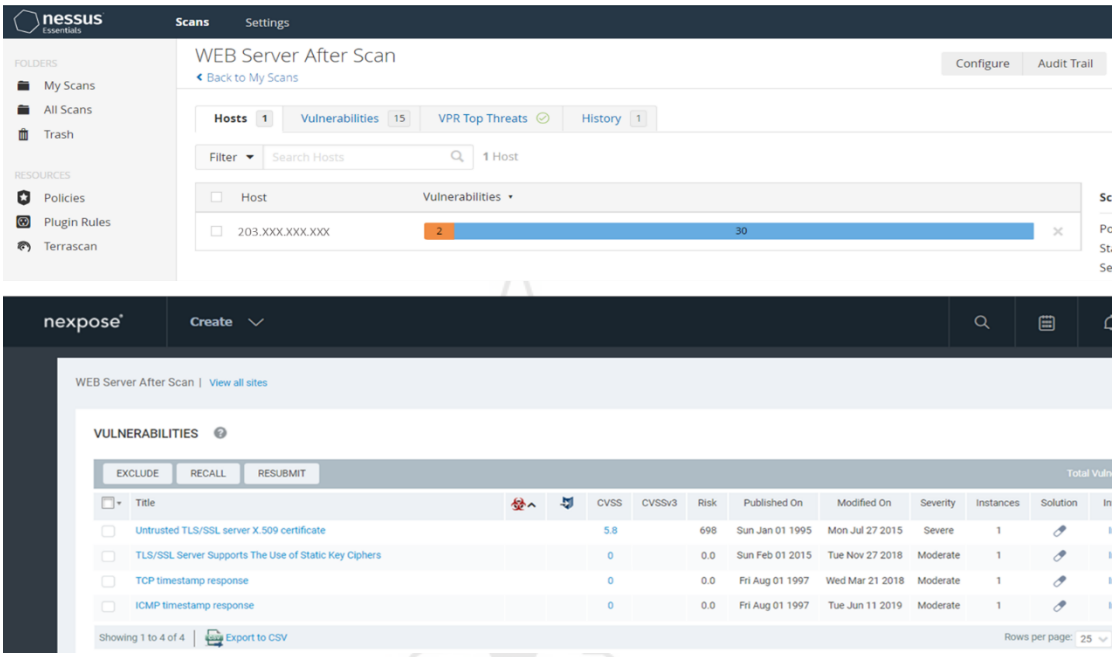
ตารางที่ 4.14 สรุปผลการประเมินช่องโหว่ก่อนการแก้ไขช่องโหว่

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

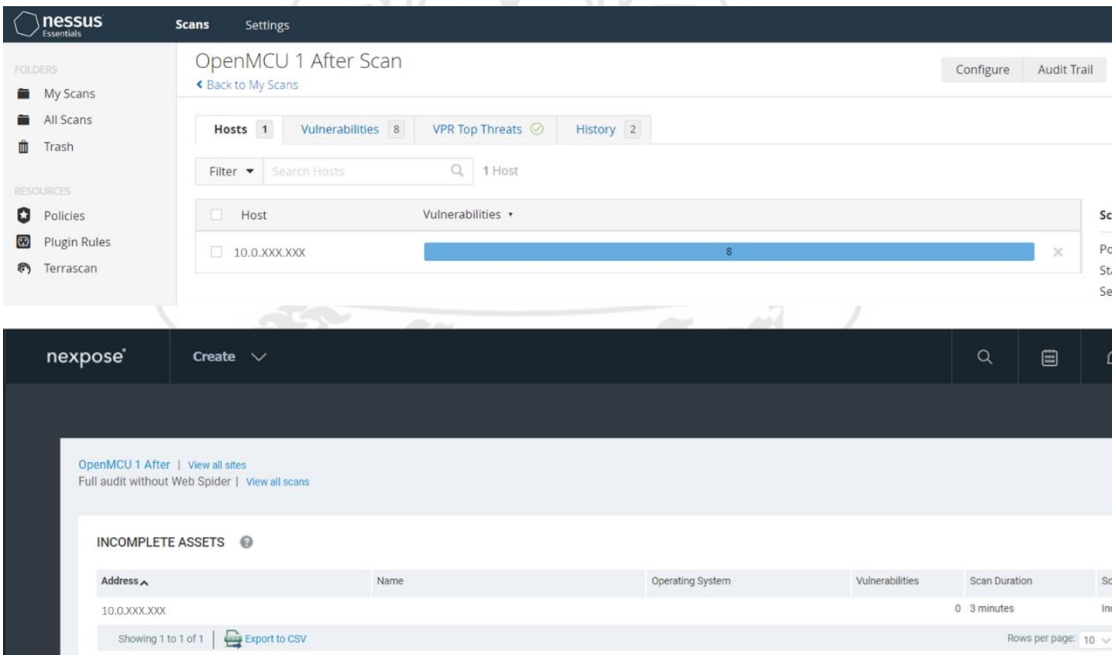
4.2 ผลการดำเนินการประเมินช่องโหว่ระบบสารสนเทศขององค์กรหลังการแก้ไขช่องโหว่ตามภาพที่ 4.16 ถึง 4.19



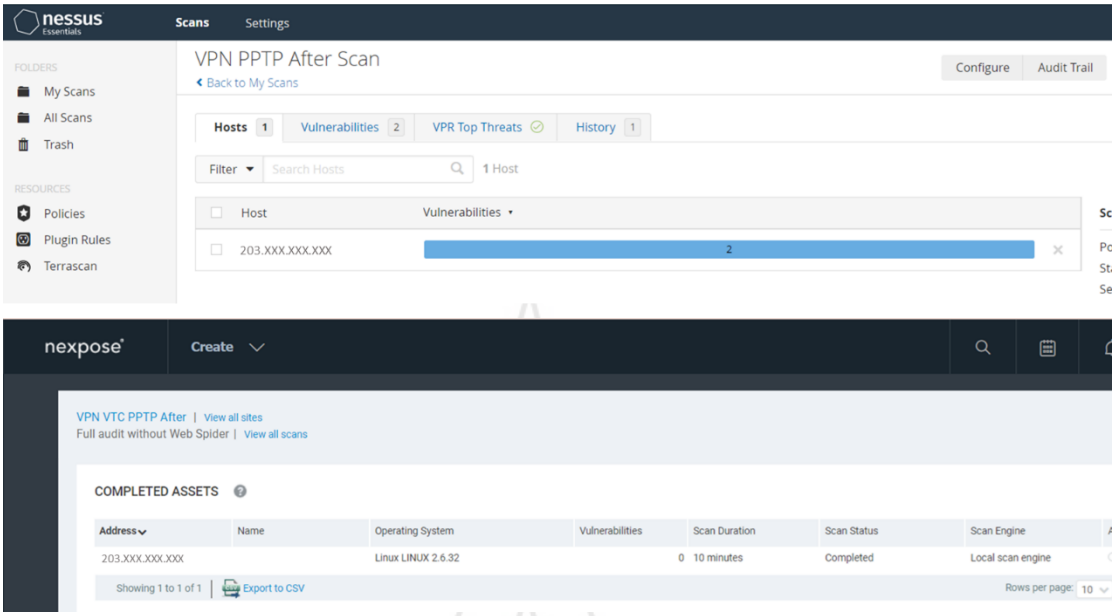
ภาพที่ 4.16 ผลการสแกนอุปกรณ์สารสนเทศ AMC Server หลังการแก้ไขช่องโหว่ของเครื่องมือ Nessus และ Nexpose



ภาพที่ 4.17 ผลการสแกนอุปกรณ์สารสนเทศ WEB Server หลังการแก้ไขช่องโหว่ของเครื่องมือ Nessus และ Nexpose



ภาพที่ 4.18 ผลการสแกนอุปกรณ์สารสนเทศ Open MCU 1 หลังการแก้ไขช่องโหว่ของเครื่องมือ Nessus และ Nexpose



ภาพที่ 4.19 ผลการสแกนอุปกรณ์สารสนเทศ VPN PPTP หลังการแก้ไขช่องโหว่ของเครื่องมือ Nessus และ Nexpose

ตารางที่ 4.15 ผลการประเมินช่องโหว่ซ้ำหลังการแก้ไขช่องโหว่

ลำดับ	ชื่อเครื่อง	หมายเลขไอพี	High	Medium	Low
1.	AMC Server	203.xxx.xxx.xxx	0	0	0
2.	Web Server	203.xxx.xxx.xxx	0	3	0
3.	OpenMCU 1	10.0.xxx.xxx	0	0	0
4.	VPN PPTP	203.xxx.xxx.xxx	0	0	0
ผลการประเมินช่องโหว่จำนวนทั้งสิ้น 3 ช่องโหว่			**0**	**3**	**0**

จากการประเมินช่องโหว่หลังการแก้ไขช่องโหว่ที่ประเมินพบ พบว่าช่องโหว่ที่ประเมินพบลดลงอย่างมาก แสดงให้เห็นว่าการแก้ไขช่องโหว่ของแผนกหรือบุคลากรที่เกี่ยวข้องกับระบบสารสนเทศขององค์กร ตามคำแนะนำการแก้ไขช่องโหว่ที่แนบไปกับรายงานการประเมินช่องโหว่ นั้นสามารถนำไปปฏิบัติได้อย่างมีประสิทธิภาพ อย่างไรก็ดีก็ยังเหลือช่องโหว่เพียงเล็กน้อยซึ่งระดับความรุนแรงอยู่ที่ระดับกลางตามตารางที่ 4.15

4.3 สรุปผลการดำเนินการประเมินช่องโหว่ระบบสารสนเทศขององค์กรซ้ำหลังจากการแก้ไขช่องโหว่ที่ประเมินพบ

หลังจากการดำเนินการประเมินช่องโหว่ระบบสารสนเทศขององค์กรซ้ำแล้ว พบว่ายังมีช่องโหว่ที่ยังไม่สามารถกำจัดได้ รายละเอียดตามรายงานจากบุคลากรที่ทำการแก้ไข ช่องโหว่ดังกล่าวแสดงตามตารางที่ 4.16 ดังนี้

ตารางที่ 4.16 รายงานช่องโหว่ที่ประเมินพบหลังจากการประเมินซ้ำ

ลำดับ	ชื่อช่องโหว่	อุปกรณ์สารสนเทศ	การดำเนินการแก้ไขช่องโหว่	ระดับความเสี่ยง (Risk+)	ผลการแก้ไข
1.	SSL Certificate Cannot Be Trusted	WEB Server Port: 21 / tcp / ftp	ซื้อหรือสร้างใบรับรอง SSL Certificate ที่ออกโดยหน่วยงานหรือองค์กรที่เป็นที่ยอมรับในระดับสากล	ปานกลาง (Med)	รอการแก้ไข
2.	SSL Self-Signed Certificate	WEB Server Port: 21 / tcp / ftp	ซื้อหรือสร้างใบรับรอง SSL Certificate ที่ออกโดยหน่วยงานหรือองค์กรที่เป็นที่ยอมรับในระดับสากล	ปานกลาง (Med)	รอการแก้ไข
3.	Untrusted TLS/SSL server X.509 certificate	WEB Server Port: 21 / 443 / TCP	ซื้อหรือสร้างใบรับรอง SSL Certificate ที่ออกโดยหน่วยงานหรือองค์กรที่เป็นที่ยอมรับในระดับสากล	ปานกลาง (Med)	รอการแก้ไข

ช่องโหว่ที่ประเมินพบจากการตรวจสอบซ้ำตามตารางที่ 4.16 พบว่าจะเป็นช่องโหว่ที่เกี่ยวข้องกับโพรโทคอล TLS/SSL ทั้งหมด และเกี่ยวข้องกับ Certificate หรือใบรับรองอิเล็กทรอนิกส์ เป็นไฟล์ข้อมูลขนาดเล็ก ที่ได้มีการผูกไว้กับ Private Key ของเครื่องเซิร์ฟเวอร์ เพื่อยืนยันตัวตนและความถูกต้องในการส่งข้อมูลระหว่างเครื่องเซิร์ฟเวอร์ กับเว็บเบราว์เซอร์หรือ Application ที่ใช้งาน มีการเข้ารหัสและถอดรหัสผ่านเทคโนโลยี SSL/TLS หากข้อมูลถูกดักจับไปได้ ข้อมูลก็ยังมีความปลอดภัย เพราะแฮกเกอร์จะไม่สามารถถอดรหัสข้อมูลได้ เนื่องจากข้อมูลที่ได้ไป จะอยู่ในรูปแบบที่อ่านไม่ออก จะต้องมีกุญแจถอดรหัสที่เหมาะสมและตรงกันเท่านั้น จึงจะสามารถถอดรหัสได้ SSL ย่อมาจาก Secure Socket Layer ซึ่งปัจจุบันได้พัฒนาขึ้นมาเป็น TLS (Transport Layer Security) คือ เทคโนโลยีการเข้ารหัสข้อมูล เพื่อเพิ่มความปลอดภัยในการสื่อสารหรือส่งข้อมูลบนเครือข่ายอินเทอร์เน็ต ระหว่างเครื่องเซิร์ฟเวอร์กับเว็บเบราว์เซอร์หรือ Application ที่ใช้งาน เพื่อให้ข้อมูล

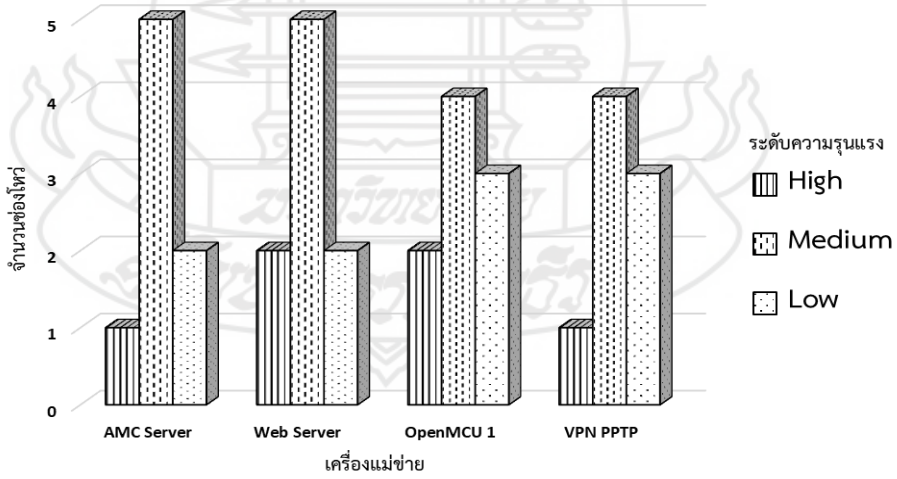
ปลอดภัยจากการเข้าถึงข้อมูลจากแฮกเกอร์ โดยวิธีการเรียกใช้งาน จะเรียกผ่านโพรโทคอล HTTPS หรือโพรโทคอลความปลอดภัยอื่นๆ ตามแต่วิธีการใช้งาน

จากการสอบถามไปยังผู้ควบคุมระบบสารสนเทศ (Admin) อุปกรณ์ที่เข้ารับการประเมินช่องโหว่ ทราบว่าเป็นการใช้ใบรับรองอิเล็กทรอนิกส์ ในรูปแบบที่ไม่เสียค่าใช้จ่าย สมัครใช้บริการจากผู้ให้บริการบนอินเทอร์เน็ต โดยไม่ได้ออกโดยหน่วยงานหรือองค์กรที่เป็นที่ยอมรับในระดับสากล ซึ่งอาจจะเกิดความเสี่ยงที่มาจากการถูกโจมตีระบบสารสนเทศขององค์กรจากผู้ไม่หวังดี

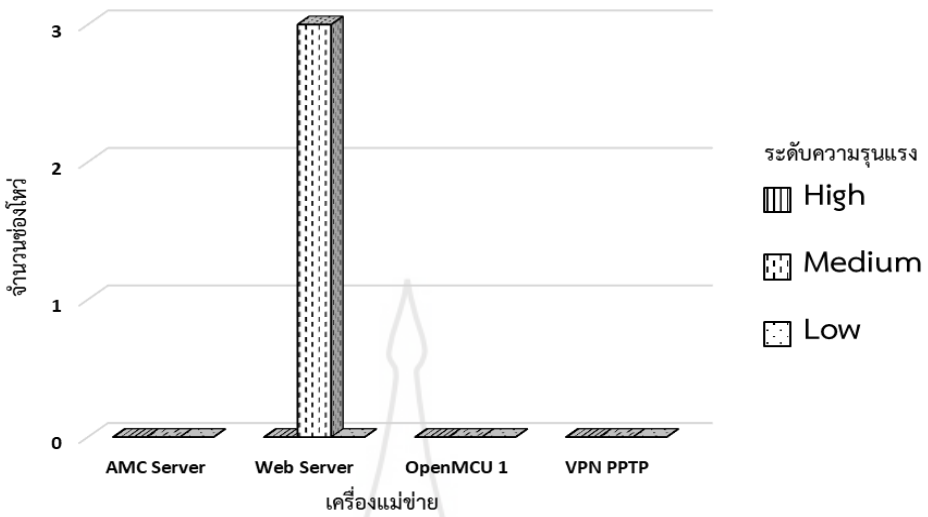
การแก้ไขต่อช่องโหว่ดังกล่าวนี้ จะต้องทำรายงานถึงหัวหน้าผู้ดูแลระบบสารสนเทศขององค์กร (CIO) จนถึงผู้บังคับบัญชาชั้นสูงในการของบประมาณเพื่อนำมาจัดหาใบรับรองอิเล็กทรอนิกส์ที่ถูกต้องและออกโดยหน่วยงานหรือองค์กรที่เป็นที่ยอมรับในระดับสากล ซึ่งสามารถหาข้อมูลได้จาก https://ssl.in.th/ ซึ่งจะเป็นรายละเอียดทางด้านงานธุรการต่อไป

4.4 ภาพรวมของการดำเนินการประเมินช่องโหว่ระบบสารสนเทศขององค์กรซ้ำหลังจากการแก้ไขช่องโหว่ที่ประเมินพบ และภาพรวมการประเมินความเสี่ยงช่องโหว่ระบบสารสนเทศขององค์กร

1) จำนวนช่องโหว่ก่อนและหลังการแก้ไขช่องโหว่ และการประเมินช่องโหว่ซ้ำ

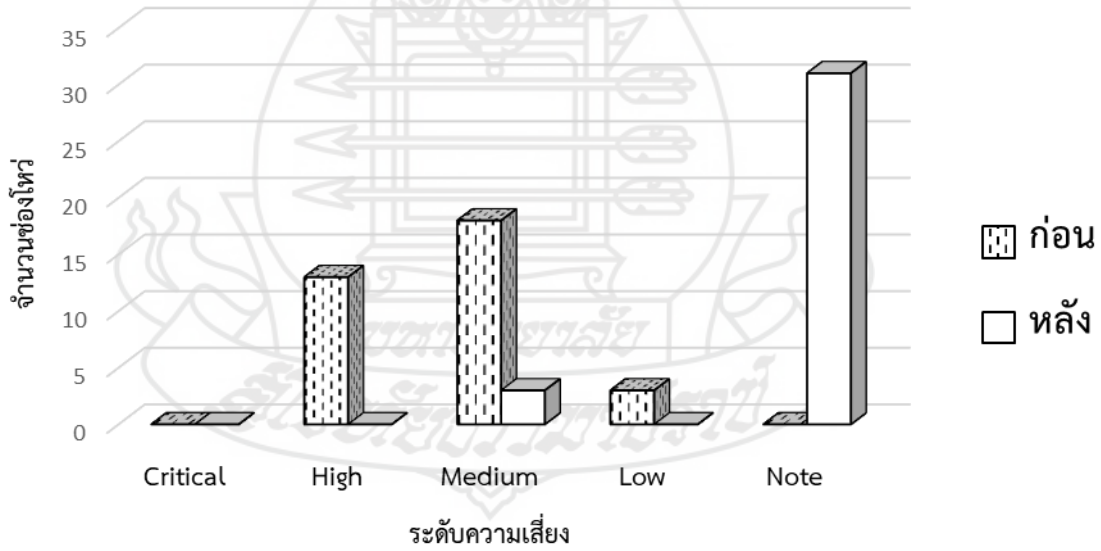


ภาพที่ 4.20 จำนวนช่องโหว่ก่อนการแก้ไข และก่อนการประเมินช่องโหว่ซ้ำ

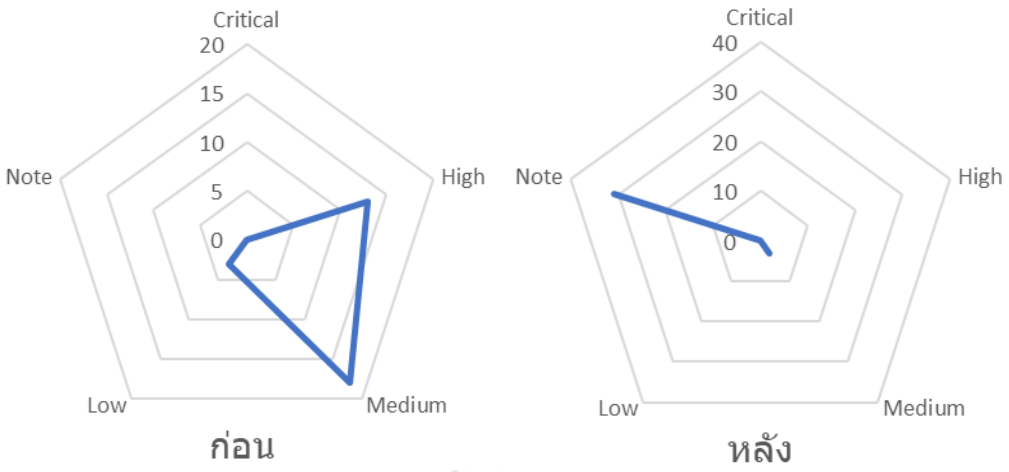


ภาพที่ 4.21 จำนวนช่องโหว่หลังการแก้ไข และหลังการประเมินช่องโหว่ซ้ำ

2) ผลการประเมินความเสี่ยงช่องโหว่ที่มีผลต่อองค์กรก่อนและหลังการแก้ไขช่องโหว่และการประเมินช่องโหว่ซ้ำ



ภาพที่ 4.22 ผลการประเมินความเสี่ยงช่องโหว่ที่มีผลต่อองค์กรก่อนและหลังการแก้ไขช่องโหว่ และการประเมินช่องโหว่ซ้ำ



ภาพที่ 4.23 แนวโน้มทิศทางความเสี่ยงช่องโหว่ที่มีผลต่อองค์กรก่อนและหลังการแก้ไขช่องโหว่ และการประเมินช่องโหว่ซ้ำ

สรุปผลการประเมินความเสี่ยงช่องโหว่ที่ส่งผลต่ออุปกรณ์สารสนเทศขององค์กร ในการปฏิบัติงานในภารกิจต่าง หลังจากที่ได้ทำตามขั้นตอนของการทดลองตามกรอบในงานวิจัยในครั้งนี้ จะเห็นได้ว่าจำนวนช่องโหว่ได้ลดน้อยลงหลังจากการแก้ไข ส่งผลถึงการประเมินความเสี่ยงช่องโหว่ที่ส่งผลต่ออุปกรณ์สารสนเทศขององค์กร จากเดิมก่อนการแก้ไขช่องโหว่นั้นมีความเสี่ยงอยู่ระดับกลางถึงระดับสูง หลังจากทำการแก้ไขช่องโหว่และทำการประเมินช่องโหว่ซ้ำ จะสังเกตุได้จากภาพแผนภูมิหลังการประเมินช่องโหว่เส้นกราฟจะชี้ไปที่ระดับ Note หมายความว่าไม่มีความเสี่ยง หรือ เว็บไซต์/เว็บแอพพลิเคชั่น/เครื่องคอมพิวเตอร์แม่ข่ายมีการควบคุมที่เพียงพอ/สถานะยังมีความปลอดภัย แต่ยังคงต้องบันทึกรายละเอียดข้อมูลต่างๆ ของช่องโหว่ที่ได้รับการแก้ไข และยังมีส่วนปลายเล็กน้อยชี้ไปยังความเสี่ยง ระดับปานกลาง (Medium) นั่นคือจำนวนช่องโหว่ที่ยังคงอยู่ สาเหตุที่ยังคงมีช่องโหว่คือเป็นช่องโหว่ที่เกี่ยวกับใบรับรองดิจิทัลที่ไม่เป็นที่ยอมรับในระดับสากล (SSL Certificate) ต้องใช้งบประมาณในการจัดซื้อ ซึ่งจะต้องแก้ไขทางธุรการต่อไป จากผลการประเมินความเสี่ยงช่องจำนวน 34 ช่องโหว่ ช่องโหว่ที่ได้รับแก้ไขเรียบร้อยและไม่มีความเสี่ยงจำนวน 31 ช่องโหว่ และยังเหลือช่องโหว่ระดับปานกลาง 3 ช่องโหว่ จึงมีค่าเฉลี่ยรวมความเสี่ยงของช่องโหว่ที่ส่งผลกระทบต่อองค์กรอยู่ในระดับ ต่ำ ดังนั้นจึงสรุปได้ว่าการดำเนินการตามกระบวนการ กรอบการจัดการช่องโหว่สารสนเทศขององค์กร ของวิจัยนี้สามารถกำจัดช่องโหว่หรือจุดอ่อนของระบบสารสนเทศขององค์กรได้อย่างมีประสิทธิภาพ

5 . การตรวจสอบยืนยันความถูกต้อง (Verification)

การตรวจสอบยืนยันความถูกต้อง เป็นการดำเนินการในขั้นสุดท้ายในการดำเนินงานตามกรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กรก่อนที่จะสรุปผลการดำเนินการภายใต้กรอบดังกล่าวให้ผู้บังคับบัญชา และผู้ที่มีส่วนเกี่ยวข้องในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ต่อระบบสารสนเทศขององค์กรได้รับทราบ และแนวทางการดำเนินการตามกรอบการจัดการช่องโหว่ฯ การตรวจสอบยืนยันความถูกต้อง ต้องอาศัยองค์กรและบุคคลที่มีความเข้าใจในบริบทของการรักษาความมั่นคงปลอดภัยทางไซเบอร์ฯ โดยเฉพาะมาช่วยดำเนินการตรวจสอบยืนยันความถูกต้อง พร้อมกับให้คำแนะนำเพิ่มเติมในการดำเนินการตามกรอบการจัดการช่องโหว่ฯ องค์กรของผู้วิจัยเป็นองค์กรของภาครัฐในส่วนของการป้องกันประเทศเป็นหลัก ดังนั้นข้อมูลหรือข่าวสารต่างๆ จะมีชั้นความลับในการดำเนินการ และการตรวจสอบยืนยันความถูกต้องนั้นจึงไม่ควรให้องค์กรภายนอก หรือเอกชนมาดำเนินการ จากเหตุผลดังกล่าวผู้วิจัยจึงเสนอแนวทางให้การตรวจสอบยืนยันความถูกต้อง โดยใช้บุคลากรในองค์กรของระบบสารสนเทศกองบัญชาการกองทัพภาคที่ 2 เพราะจะสามารถทราบถึงภาพรวมขององค์กรได้อย่างสมบูรณ์ ทั้งนี้จะเป็นรูปแบบของคณะกรรมการในการสอบตรวจสอบความถูกต้อง กรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กร คณะกรรมการดังกล่าวประกอบไปด้วย 1) ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer : CIO) 2) ผู้จัดการผู้บริหารระบบสารสนเทศ (Administrator : Admin) 3) เจ้าหน้าที่ปฏิบัติการสารสนเทศ (information technology operator)

คณะกรรมการที่จัดตั้งขึ้นมามีหน้าที่ในการตรวจสอบ และสอบทวน การปฏิบัติตามกรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กร ตามรายละเอียดของรายงานในด้านต่างๆ จากเจ้าหน้าที่ปฏิบัติการสารสนเทศ หรือ ผู้จัดการ ผู้บริหารระบบสารสนเทศ สอบทวนขั้นปฏิบัติตามกรอบดังกล่าวว่าสามารถกำจัดช่องโหว่ระบบสารสนเทศ และลดความเสี่ยงที่จะเกิดผลกระทบต่อองค์กร ตามวัตถุประสงค์ของกรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กรได้ถูกต้องหรือไม่ พร้อมกับให้คำแนะนำ และข้อเสนอแนะเมื่อเกิดประเด็นหรือปัญหาข้อขัดข้องต่างๆ ที่เกิดขึ้นเพื่อปรับปรุงกรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กร ให้มีประสิทธิภาพมากยิ่งขึ้น ทั้งในด้านความน่าเชื่อถือ ความครบถ้วนสมบูรณ์ และความพร้อมใช้งาน

6. ผลการประเมินประสิทธิภาพ กรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กร

การประเมินประสิทธิภาพของกรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กร ตามสมมติฐานการวิจัยคือ กรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กรที่พัฒนาขึ้นมา โดยใช้การผสมผสานจากกรอบแนวคิด NIST Cybersecurity Framework และ Vulnerability Management Life Cycle By CDC สามารถแก้ไขปัญหาช่องโหว่หรือจุดอ่อนของระบบสารสนเทศขององค์กรได้ โดยไม่มีความเสี่ยงช่องโหว่ในระดับสูง

ผู้วิจัยได้จัดทำแบบสอบถาม สำหรับสอบถามกลุ่มผู้ที่มีส่วนเกี่ยวข้องกับระบบสารสนเทศกองบัญชาการกองทัพภาคที่ 2 ถึงเรื่องที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ โดยตอบแบบสอบถามกรอบการจัดการช่องโหว่ขององค์กรในงานวิจัย การพัฒนากรอบการจัดการช่องโหว่ระบบสารสนเทศเพื่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์ กรณีศึกษา กองบัญชาการกองทัพภาคที่ 2 คำถามในแบบสอบจะใช้ขั้นตอนของกรอบการจัดการช่องโหว่ขององค์กรที่ผู้วิจัยได้พัฒนาขึ้นมา 6 ขั้นตอนดังนี้ 1) การจัดการทรัพย์สิน 2) การประเมิน 3) การแก้ไข 4) การประเมินซ้ำ 5) การตรวจสอบยืนยันความถูกต้อง และ 1 หัวข้อสำหรับคำคิดเห็นต่อการนำไปใช้งาน เป็นขั้นตอนที่ 6 โดยมีผู้ตอบแบบสอบถามแบ่งออกเป็น 3 กลุ่มดังนี้

1) กลุ่มผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer : CIO จำนวน 4 คน ได้แก่

กลุ่มผู้บริหารระบบสารสนเทศขององค์กร ท่านที่ 1
ตำแหน่ง หัวหน้าแผนกเทคโนโลยีสารสนเทศและการสื่อสาร

กลุ่มผู้บริหารระบบสารสนเทศขององค์กร ท่านที่ 2
ตำแหน่ง ผู้ช่วยนายทหารเทคโนโลยีสารสนเทศ

กลุ่มผู้บริหารระบบสารสนเทศขององค์กร ท่านที่ 3
ตำแหน่ง ผู้ช่วยนายทหารการสื่อสาร

กลุ่มผู้บริหารระบบสารสนเทศขององค์กร ท่านที่ 4
ตำแหน่ง นายทหารปฏิบัติการสารสนเทศ

2) กลุ่มผู้จัดการระบบสารสนเทศ (Administrator : Admin) จำนวน 4 คน ได้แก่

ผู้จัดการระบบสารสนเทศขององค์กร ท่านที่ 1
ตำแหน่ง หัวหน้าแผนกกรรมวิธีข้อมูล

ผู้จัดการระบบสารสนเทศขององค์กร ท่านที่ 2
ตำแหน่ง รองหัวหน้าแผนกกรรมวิธีข้อมูล

ผู้จัดการระบบสารสนเทศขององค์กร ท่านที่ 3
ตำแหน่ง เจ้าหน้าที่กรรมวิธีข้อมูล

ผู้จัดการระบบสารสนเทศขององค์กร ท่านที่ 4
ตำแหน่ง เจ้าหน้าที่กรรมวิธีข้อมูล

3) กลุ่มเจ้าหน้าที่ปฏิบัติการสารสนเทศ (information technology operator) จำนวน 11 คน ได้แก่

เจ้าหน้าที่ปฏิบัติการระบบสารสนเทศขององค์กร ท่านที่ 1
ตำแหน่ง เจ้าหน้าที่ควบคุมเครื่องจักรคำนวณอาวุโส

เจ้าหน้าที่ปฏิบัติการระบบสารสนเทศขององค์กร ท่านที่ 2
ตำแหน่ง เจ้าหน้าที่ควบคุมเครื่องจักรคำนวณ

เจ้าหน้าที่ปฏิบัติการระบบสารสนเทศขององค์กร ท่านที่ 3
ตำแหน่ง เจ้าหน้าที่ควบคุมเครื่องจักรคำนวณ

เจ้าหน้าที่ปฏิบัติการระบบสารสนเทศขององค์กร ท่านที่ 4
ตำแหน่ง เจ้าหน้าที่ควบคุมเครื่องจักรคำนวณ

เจ้าหน้าที่ปฏิบัติการระบบสารสนเทศขององค์กร ท่านที่ 5
ตำแหน่ง เจ้าหน้าที่ควบคุมเครื่องจักรคำนวณ

เจ้าหน้าที่ปฏิบัติการระบบสารสนเทศขององค์กร ท่านที่ 6
ตำแหน่ง เจ้าหน้าที่ควบคุมเครื่องจักรคำนวณ

เจ้าหน้าที่ปฏิบัติการระบบสารสนเทศขององค์กร ท่านที่ 7
ตำแหน่ง เจ้าหน้าที่กรรมวิธีข้อมูล

เจ้าหน้าที่ปฏิบัติการระบบสารสนเทศขององค์กร ท่านที่ 8
ตำแหน่ง เจ้าหน้าที่กรรมวิธีข้อมูล

เจ้าหน้าที่ปฏิบัติการระบบสารสนเทศขององค์กร ท่านที่ 9
ตำแหน่ง เจ้าหน้าที่กรรมวิธีข้อมูล

เจ้าหน้าที่ปฏิบัติการระบบสารสนเทศขององค์กร ท่านที่ 10
ตำแหน่ง เจ้าหน้าที่กรรมวิธีข้อมูล

เจ้าหน้าที่ปฏิบัติการระบบสารสนเทศขององค์กร ท่านที่ 11
ตำแหน่ง เจ้าหน้าที่กรรมวิธีข้อมูล

รวมทั้งสิ้น 19 คน

จากการตอบแบบสอบถามผู้มีส่วนเกี่ยวข้องกับระบบสารสนเทศขององค์กรทางด้านความมั่นคงปลอดภัยทางไซเบอร์และแนวคิดทฤษฎีที่เกี่ยวข้อง ผู้วิจัยได้นำมาจัดทำแบบประเมินประสิทธิภาพสำหรับประเมินประสิทธิภาพ กรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กร โดยสอบถามจากผู้มีส่วนเกี่ยวข้องกับระบบสารสนเทศขององค์กรจำนวนทั้งหมด 19 คน โดยแยกหัวข้อการประเมินเป็น 6 หัวข้อ คือ 1) การจัดการทรัพย์สิน (Assets Management) 2) การประเมิน (Assessment) 3) การแก้ไขช่องโหว่ (Remediation) 4) การประเมินซ้ำ (Re-Assessment) 5) การตรวจสอบยืนยันความถูกต้อง (Verification) และ 6. ความคิดเห็นต่อกรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กร ผลการประเมินจากการตอบแบบสอบถามของผู้มีส่วนเกี่ยวข้องกับระบบสารสนเทศขององค์กรมีดังนี้

ผู้วิจัยนำมาคำนวณหาค่าเฉลี่ย และส่วนเบี่ยงเบนมาตรฐาน ของแต่ละหัวข้อแบบสอบถามมีผลดังนี้

1) การจัดการทรัพย์สิน มีค่าเฉลี่ยเท่ากับ 4.53 และส่วนเบี่ยงเบนมาตรฐานเท่ากับ 0.63 การแปลผลเท่ากับ มากที่สุด แสดงให้เห็นว่ามีการจัดการทรัพย์สินในการเข้าประเมินช่องโหว่อย่างเหมาะสม

2) การประเมิน มีค่าเฉลี่ยเท่ากับ 4.52 และส่วนเบี่ยงเบนมาตรฐานเท่ากับ 0.61 การแปลผลเท่ากับ มากที่สุด แสดงให้เห็นว่ามีการประเมินช่องโหว่ โดยใช้เครื่องมือประเมินช่องโหว่ที่มีมาตรฐานและการประเมินความเสี่ยงช่องโหว่ เป็นไปตามหลักการและทฤษฎีที่ถูกต้องเหมาะสม

3) การแก้ไขช่องโหว่ มีค่าเฉลี่ยเท่ากับ 4.41 และส่วนเบี่ยงเบนมาตรฐานเท่ากับ 0.59 การแปลผลเท่ากับ มาก แสดงให้เห็นว่าการแก้ไขช่องโหว่ที่มีความเสี่ยง สามารถปฏิบัติได้ถูกต้องตามรายละเอียดคำแนะนำการแก้ไขช่องโหว่จากรายงาน นำมาซึ่งการปิดช่องโหว่ที่เป็นจุดอ่อนได้อย่างสมบูรณ์ ถึงแม้จะเหลือช่องโหว่ที่ไม่สามารถปิดได้ แต่ก็ทราบสาเหตุ มีรายงานให้ทราบ และบอกถึงวิธีแก้ไขพร้อมขอรับการสนับสนุนงบประมาณในการจัดหาใบรับรองดิจิทัลที่เป็นที่ยอมรับในระดับสากล

4) การประเมินซ้ำ มีค่าเฉลี่ยเท่ากับ 4.55 และส่วนเบี่ยงเบนมาตรฐานเท่ากับ 0.65 การแปลผลเท่ากับ มากที่สุด แสดงให้เห็นว่าการปฏิบัติตามขั้นตอนการประเมินซ้ำนั้นเป็นเรื่องที่สำคัญ ในการตรวจสอบการแก้ไขช่องโหว่ทำให้การจัดการช่องโหว่นั้นมีความสมบูรณ์มากยิ่งขึ้น

5) การตรวจสอบยืนยันความถูกต้อง มีค่าเฉลี่ยเท่ากับ 4.25 และส่วนเบี่ยงเบนมาตรฐานเท่ากับ 0.71 การแปลผลเท่ากับ มาก แสดงให้เห็นว่าคณะกรรมการที่จัดตั้งขึ้นมาตามข้อ 4.5 นั้นสามารถช่วยตรวจสอบ อีกทั้งสามารถให้คำแนะนำในการปฏิบัติในการจัดการช่องโหว่ได้อย่างเหมาะสม

6) ความคิดเห็นต่อกรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กร มีค่าเฉลี่ยเท่ากับ 4.53 และส่วนเบี่ยงเบนมาตรฐานเท่ากับ 0.69 การแปลผลเท่ากับ มากที่สุด แสดงให้เห็นว่าความคิดเห็นของผู้มีส่วนเกี่ยวข้องกับระบบสารสนเทศขององค์กร ที่ได้ตอบแบบสอบถามนั้นมีความคิดเห็นในเชิงบวกต่อกรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กร ที่จะนำกรอบดังกล่าวไปใช้เพื่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร

จากข้อมูลค่าเฉลี่ยและส่วนเบี่ยงเบนมาตรฐานทั้ง 6 หัวข้อข้างต้นนั้น สามารถหาค่าเฉลี่ยรวมเท่ากับ 4.48 และส่วนเบี่ยงเบนมาตรฐานรวมเท่ากับ 0.64 ระดับการจัดการช่องโหว่ระบบสารสนเทศขององค์กรอยู่ในระดับ มาก แสดงให้เห็นกรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กร เป็นกระบวนการที่สำคัญต่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร และเหมาะสมอย่างยิ่งในการนำไปใช้เป็นเครื่องมือหรือวิธีการในการป้องกันระบบสารสนเทศขององค์กรต่อไป และจากผลรวมของค่าเฉลี่ย และส่วนเบี่ยงเบนมาตรฐานนั้นสามารถแสดงผลของการประเมินประสิทธิภาพของกรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กร ดังตารางที่ 4.17

ตารางที่ 4.17 ค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐานของผลการประเมินประสิทธิภาพ กรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กร

ลำดับ	ผู้มีส่วนเกี่ยวข้องกับระบบสารสนเทศขององค์กร รายการประเมิน	$\bar{x}$	S.D.	การแปลผล
1.	การจัดการทรัพย์สิน (Assets Management)			
	1.1 การระบุอุปกรณ์เครื่องแม่ข่ายสอดคล้องกับประเด็นการรักษาความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร	4.63	0.68	มากที่สุด
	1.2 การประเมินอุปกรณ์เครื่องแม่ข่ายที่ส่งผลกระทบต่อองค์กรโดยใช้ค่าคะแนนปัจจัยผลกระทบทางเทคนิคเป็นการประเมินผลกระทบที่เหมาะสมกับองค์กร	4.47	0.53	มาก
	1.3 การจัดลำดับความสำคัญของอุปกรณ์เครื่องแม่ข่ายในการเข้ารับการประเมินช่องโหว่ ซึ่งเป็นผลจากการประเมินอุปกรณ์เครื่องแม่ข่ายที่ส่งผลกระทบต่อองค์กรมีลำดับที่สอดคล้องกับภารกิจขององค์กร	4.56	0.67	มากที่สุด
	1.4 ห้วงเวลาที่เข้ารับการประเมินช่องโหว่ของอุปกรณ์เครื่องแม่ข่ายไม่กระทบต่อภารกิจขององค์กร	4.43	0.61	มาก
	1.5 มีระบบสำรองที่สามารถทำงานคู่ขนานหรือทดแทนระบบเดิมได้	4.58	0.68	มากที่สุด
	รวม	**4.53**	**0.63**	**มากที่สุด**
2.	การประเมิน (Assessment)			
	2.1 เครื่องมือที่ใช้ในการประเมินช่องโหว่มีความง่ายในการจัดการหรือการใช้งาน	4.37	0.60	มาก
	2.2 เครื่องมือที่ใช้ในการประเมินช่องโหว่สามารถตรวจพบช่องโหว่ได้สมบูรณ์	4.63	0.58	มากที่สุด
	2.3 เครื่องมือที่ใช้ในการประเมินช่องโหว่มีรายละเอียดช่องโหว่และรายละเอียดการแก้ไขอย่างชัดเจน	4.63	0.61	มากที่สุด
	2.4 เครื่องมือที่ใช้ในการประเมินช่องโหว่สามารถระบุระดับความรุนแรงของช่องโหว่ที่ประเมินได้	4.26	0.65	มาก
	2.5 หลักการและทฤษฎีในการประเมินค่าระดับความเสี่ยงช่องโหว่ที่ส่งผลกระทบอุปกรณ์เครื่องแม่ข่ายในการปฏิบัติภารกิจขององค์กรนั้นมีความน่าเชื่อถือสามารถนำมาประเมินความเสี่ยงช่องโหว่ได้	4.29	0.56	มาก
	2.6 การนำปัจจัยผลกระทบทางด้านเทคนิคมาใช้ในการประเมินความเสี่ยงอุปกรณ์เครื่องแม่ข่ายสามารถช่วยวิเคราะห์ความเสี่ยงต่ออุปกรณ์เครื่องแม่ข่ายได้ดียิ่งขึ้น	4.59	0.62	มากที่สุด

ตารางที่ 4.17 (ต่อ)

ลำดับ	ผู้มีส่วนเกี่ยวข้องกับระบบสารสนเทศขององค์กร รายการประเมิน	$\bar{x}$	S.D.	การแปลผล
	2.7 การแสดงความสำคัญของระดับความเสี่ยงช่องโหว่ช่วยให้สามารถจัดการช่องโหว่ที่ประเมินพบได้อย่างถูกต้องและรวดเร็วมากยิ่งขึ้น	4.47	0.56	มาก
	2.8 รายงานผลการประเมินความเสี่ยงมีรายละเอียดที่ใช้ในการแก้ไขช่องโหว่ได้สมบูรณ์	4.68	0.67	มากที่สุด
	รวม	**4.52**	**0.61**	**มากที่สุด**
3.	การแก้ไขช่องโหว่ (Remediation)			
	3.1 การแก้ไขช่องโหว่ที่ประเมินพบสามารถปฏิบัติได้อย่างถูกต้องตามรายละเอียดการแก้ไขช่องโหว่จากรายงานการประเมินความเสี่ยงช่องโหว่ที่ได้รับมา	4.53	0.61	มากที่สุด
	3.2 ข้อมูลช่องโหว่ที่ทำการแก้ไขนอกจากรายละเอียดจากรายงานการประเมินความเสี่ยงช่องโหว่แล้ว ยังสามารถหารายละเอียดจากแหล่งอื่นๆ ได้สะดวก เช่น อินเทอร์เน็ต	4.21	0.59	มาก
	3.3 การแก้ไขช่องโหว่สามารถปิดช่องโหว่ที่มีความเสี่ยงอย่างสมบูรณ์	4.47	0.57	มาก
	3.4 การรายงานแก้ไขช่องโหว่ที่ถูกต้องและรวดเร็ว	4.42	0.55	มาก
	3.5 การประสานงานเพื่อความสอดคล้องในการแก้ไขช่องโหว่ระหว่างผู้ปฏิบัติในขั้นตอนการแก้ไขกับผู้ปฏิบัติในขั้นตอนการประเมินซ้ำ	4.44	0.63	มาก
	รวม	**4.41**	**0.59**	**มาก**
4.	การประเมินซ้ำ (Re-Assessment)			
	4.1 ขั้นตอนการประเมินซ้ำหลังจากการแก้ไขช่องโหว่มีกระบวนการสำคัญและมีความเหมาะสมเพื่อให้ทราบผลของการแก้ไขช่องโหว่	4.58	0.76	มากที่สุด
	4.2 กระบวนการประเมินซ้ำเป็นการปฏิบัติที่ไม่ซับซ้อนเพราะใช้รูปแบบขั้นตอนการประเมินแบบเดิม	4.53	0.62	มากที่สุด
	4.3 มีรายงานการประเมินซ้ำที่สมบูรณ์	4.68	0.59	มากที่สุด
	4.4 ทราบสาเหตุกรณีพบช่องโหว่จากการประเมินซ้ำ สามารถให้รายละเอียดในการแก้ไขเพิ่มเติมได้	4.34	0.64	มาก
	4.5 การรายงานผลการประเมินซ้ำมีรายละเอียดอย่างชัดเจน	4.65	0.63	มากที่สุด
	รวม	**4.55**	**0.65**	**มากที่สุด**

ตารางที่ 4.17 (ต่อ)

ลำดับ	ผู้มีส่วนเกี่ยวข้องกับระบบสารสนเทศขององค์กร รายการประเมิน	$\bar{x}$	S.D.	การแปลผล
5.	การตรวจสอบยืนยันความถูกต้อง (Verification)			
	5.1 มีการตรวจสอบความถูกต้องในการประเมินช่องโหว่ การประเมินความเสี่ยงช่องโหว่ที่ส่งผลกระทบกับอุปกรณ์เครื่องแม่ข่ายสารสนเทศขององค์กร การแก้ไขช่องโหว่ ในรูปแบบของ คณะกรรมการ จากคำสั่งแต่งตั้งคณะกรรมการตรวจสอบความถูกต้องการจัดการช่องโหว่ระบบสารสนเทศขององค์กร	4.32	0.75	มาก
	5.2 คณะกรรมการประกอบไปด้วยบุคลากรที่มีความรู้ความสามารถ ในการตรวจสอบความถูกต้องในการประเมินช่องโหว่	4.26	0.83	มาก
	5.3 คณะกรรมการให้คำแนะนำและวิธีการแก้ปัญหากรณีตรวจสอบพบข้อบกพร่องในการประเมินช่องโหว่	4.18	0.54	มาก
	รวม	**4.25**	**0.71**	**มาก**
6.	ความคิดเห็นต่อกรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กร			
	6.1 ท่านคิดว่ากรอบการจัดการช่องโหว่นี้สามารถใช้เป็นกรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กรได้	4.38	0.74	มาก
	6.2 กรอบการจัดการช่องโหว่นี้ ควรกำหนดเป็นหลักการนำเสนอผู้บังคับบัญชาอนุมัติใช้เป็นกรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กร เพื่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์ กองทัพภาคที่ 2	4.68	0.64	มากที่สุด
	รวม	**4.53**	**0.69**	**มากที่สุด**
	ผลรวม	**4.48**	**0.64**	**มาก**

บทที่ 5
สรุปการศึกษา อภิปรายผล และข้อเสนอแนะ

งานวิจัยนี้เป็นการค้นคว้าหาวิธีการและศึกษาองค์ความรู้ต่างๆ เพื่อการจัดการช่องโหว่หรือจุดอ่อนของระบบสารสนเทศขององค์กร ในรูปแบบของกรอบการจัดการช่องโหว่ เพื่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์อย่างยั่งยืน ไม่เฉพาะแค่การประเมินช่องโหว่เพียงประเด็นเดียว งานวิจัยนี้ได้ดำเนินการเป็นระบบและขั้นตอนในภาพรวมครอบคลุมการจัดการช่องโหว่อย่างสมบูรณ์ โดยมีกระบวนการดำเนินการภายใต้กรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กร

1. สรุปการศึกษา

1.1 การพัฒนากรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กร เพื่อให้ได้กรอบการจัดการช่องโหว่ระบบสารสนเทศเพื่อการรักษาความมั่นคงปลอดภัยด้านไซเบอร์กองบัญชาการกองทัพภาคที่ 2 ได้ใช้หลักการจากกรอบความมั่นคงปลอดภัยทางไซเบอร์ของ NIST (NIST Cybersecurity Framework) โดยนำกระบวนการดำเนินการจากเอกสารแนะนำแนวทางการปฏิบัติกระบวนการประเมินความเสี่ยงตามกรอบแนวคิด NIST 800-30R1 Guide for Conducting Risk Assessment และ ได้ใช้แนวคิด วงจรชีวิตการจัดการช่องโหว่โดย CDC (Vulnerability Management Life Cycle By CDC) จากหลักการทั้ง 2 กรอบแนวคิดต้นแบบ ได้นำมาวิเคราะห์ผสมผสาน จนได้กรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กร โดยมีกระบวนการหลัก 5 กระบวนการด้วยกันคือ 1) การจัดการทรัพย์สิน (Assets Management) 2) การประเมิน (Assessment) 3) การแก้ไขช่องโหว่ (Remediation) 4) การประเมินซ้ำ (Re-Assessment) 5) การตรวจสอบยืนยันความถูกต้อง (Verification)

1.2 จากการดำเนินตามกระบวนการกรอบการจัดการช่องโหว่สารสนเทศขององค์กร สามารถสรุปผลตามหัวข้อได้ดังนี้

1) กำหนดอุปกรณ์เครื่องแม่ข่ายในการเข้ารับการประเมินช่องโหว่ โดยคัดเลือกด้วยวิธีการนำปัจจัยผลกระทบต่อองค์กร นำมาประเมินอุปกรณ์เครื่องแม่ข่ายในการเข้ารับการประเมินช่องโหว่ได้อย่างเหมาะสม

2) จากการทดลองการประเมินช่องโหว่โดยใช้เครื่องมือในการประเมินช่องโหว่ 2 เครื่องมือ คือ Nessus เวอร์ชัน Essentials และ Nexpose เวอร์ชัน Community ทำให้การประเมินช่องโหว่มีความละเอียดมากยิ่งขึ้นโดยพบช่องโหว่ทั้งสิ้นจำนวน 34 ช่องโหว่ จากการวิเคราะห์ช่องโหว่ที่ตรวจพบสรุปได้ดังนี้

2.1) รูปแบบชนิดช่องโหว่ จากการประเมินช่องโหว่ทั้ง 4 อุปกรณ์เครื่องแม่ข่าย พบว่ามีช่องโหว่ที่แตกต่างกันไปตามลักษณะโพรโทคอลที่ให้บริการตามตารางที่ 5.1 ดังนี้

ตารางที่ 5.1 ลักษณะของชนิดรูปแบบของช่องโหว่ตามลักษณะโพรโทคอล

รูปแบบ/ชนิด	**TLS/SSL/ X.509**	**SSH/FTP/ TELNET**	**DNS**	**Test-cgi**	**Unix Os**	**HTTP OPTION**
จำนวนช่องโหว่	18	10	2	1	1	2

กลุ่มช่องโหว่ที่มีจำนวนมาก คือ กลุ่มช่องโหว่โพรโทคอล TLS/SSL/X.509 ซึ่งเป็นโพรโทคอลที่ให้บริการเกี่ยวกับเว็บไซต์หรือเว็บเซิร์ฟเวอร์ และ กลุ่มช่องโหว่ SSH/FTP/TELNET เป็นโพรโทคอลที่เกี่ยวข้องกับการติดต่อระยะไกล ซึ่งทั้ง 2 โพรโทคอล เป็นการให้บริการจากเครือข่ายภายนอก (Internet) ดังนั้นโอกาสที่จะถูกโจมตีจากผู้ไม่หวังดี ซึ่งอาจส่งผลกระทบต่อระบบสารสนเทศขององค์กรเป็นไปได้มากที่สุด จึงควรพิจารณา ให้ความสำคัญ ทำการแก้ไข หรือกำจัด ช่องโหว่ของกลุ่มโพรโทคอลทั้ง 2 กลุ่ม เป็นลำดับแรก

2.2) ลักษณะ พอร์ต (Port) ที่ตรวจพบในการประเมินช่องโหว่ จากการประเมินช่องโหว่ทั้ง 4 อุปกรณ์เครื่องแม่ข่าย พบว่ามีพอร์ตหมายเลขต่างๆ ที่เปิดใช้งานหรือให้บริการที่เกี่ยวข้องกับช่องโหว่ที่ประเมินพบตามตารางที่ 5.2 ดังนี้

ตารางที่ 5.2 จำนวนพอร์ตที่เกี่ยวข้องกับช่องโหว่ที่ประเมินพบ

เครื่องแม่ข่าย	**Port: 80**	**Port: 443**	**Port: 53**	**Port: 21**	**Port: 22**	**Port: 888**	**Port: 4444**	**Port: 1423**
AMC Server		5	3					
WEB Server	1	3		6		2		
OpenMCU 1					7			1
VPN PPTP							8	
รวมพอร์ตที่ประเมินพบ	**1**	**8**	**3**	**6**	**7**	**2**	**8**	**1**

พอร์ตที่พบเป็นจำนวนมาก คือ Port : 4444 Port : 443 Port : 22 และ Port : 21 ตามลำดับ Port : 4444 Port : 443 และ Port : 21 นั้นจะเป็นพอร์ตที่เกี่ยวข้องกับช่องโหว่ชนิด TSL/SSL/X.509 ซึ่งลักษณะช่องโหว่ประเภทนี้จะเกี่ยวข้องกับระบบเว็บเซิร์ฟเวอร์ ซึ่งจะพบพอร์ตที่เป็นปัญหาเกี่ยวกับช่องโหว่ TSL/SSL/X.509 จะพบได้บนอุปกรณ์เครือข่ายที่เข้ารับการประเมินช่องโหว่ เช่น AMC Sever / WEB Server / VPN PPTP ซึ่งเป็นเครื่องแม่ข่ายที่ให้บริการในด้านระบบเว็บเซิร์ฟเวอร์ จึงวิเคราะห์ได้ว่า พอร์ตและช่องโหว่ที่เกี่ยวข้องกับช่องโหว่ชนิด TSL/SSL/X.509 มีจำนวนมากกว่าช่องโหว่ชนิดอื่น ดังนั้นจึงจำเป็นต้องให้ความสำคัญอย่างเร่งด่วนในการแก้ปัญหาที่จะเกิดขึ้น เพราะอาจจะเป็นช่องทางในการถูกโจมตีจากผู้ไม่หวังดีผ่านทางพอร์ต 4444/443/21 มากที่สุด เช่นเดียวกับ Port : 22 ซึ่งมีจำนวนช่องโหว่ที่เกี่ยวข้องกับพอร์ตหมายเลข 22 เป็นจำนวนมากเช่นเดียวกัน เป็นพอร์ตที่เกี่ยวข้องกับช่องโหว่ชนิด SSH/Telnet/FTP ซึ่งเป็นการเข้าใช้งาน หรือควบคุมเครื่องอื่นๆ จากระยะไกล (Remote) จากอุปกรณ์ที่เข้ารับการประเมินช่องโหว่ พบว่า พอร์ตหมายเลข 22 ที่เกี่ยวข้องกับช่องโหว่ชนิด SSH/Telnet/FTP จะพบบนเครื่องแม่ข่าย OpenMCU 1 ซึ่งเป็นแม่ข่ายให้บริการประชุมทางไกลผ่านจอภาพ จึงควรเร่งดำเนินการแก้ไข และควรปิดพอร์ตที่ไม่มีความจำเป็นต้องใช้ หรือไม่ได้ให้บริการ เช่นกัน

2.3) ระดับความรุนแรงที่ตรวจพบในการประเมินช่องโหว่ จากการประเมินช่องโหว่ทั้ง 4 อุปกรณ์เครื่องแม่ข่าย พบว่ามีระดับความรุนแรง ที่เกี่ยวข้องกับช่องโหว่ที่ประเมินพบดังนี้

ตารางที่ 5.3 ระดับความรุนแรงที่ตรวจพบจากการประเมินช่องโหว่

เครื่องแม่ข่าย	ระดับความรุนแรง		
	สูง (High)	กลาง (Medium)	ต่ำ (Low)
AMC Server	1	5	2
WEB Server	2	5	2
OpenMCU 1	2	4	3
VPN PPTP	1	5	2
รวมระดับความรุนแรง	**6**	**19**	**9**

ระดับความรุนแรงที่ตรวจพบจากการประเมินช่องโหว่ พบว่าระดับความรุนแรงของช่องโหว่ระบบสารสนเทศขององค์กร ภาพรวมอยู่ในระดับกลาง ซึ่งถือว่าเป็นระดับที่จะต้องแก้ไขให้เป็นไปตามวัตถุประสงค์ของกรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กร กล่าวคือ ทำการแก้ไขโดยวิธีที่สามารถกำจัดช่องโหว่ เพื่อให้ระดับความรุนแรงอยู่ในระดับต่ำ หรือไม่มีระดับความรุนแรง

2.4) การประเมินค่าระดับความเสี่ยงช่องโหว่ระบบสารสนเทศขององค์กร พบระดับความเสี่ยงของช่องโหว่ จากการประเมินค่าระดับความเสี่ยง ตามตารางที่ 5.4 และ 5.5 ดังนี้

ตารางที่ 5.4 ระดับความเสี่ยงที่ประเมินพบจากการประเมินค่าระดับความเสี่ยงช่องโหว่ (Risk)

	ระดับความรุนแรงกรณียังไม่เพิ่มปัจจัยผลกระทบต่อองค์กร (Risk)				
เครื่องแม่ข่าย	**ระดับวิกฤต (Critical)**	**ระดับสูง (High)**	**ระดับกลาง (Medium)**	**ระดับต่ำ (Low)**	**ระดับบันทึก (Note)**
AMC Server	0	0	4	4	0
WEB Server	0	4	0	5	0
OpenMCU 1	0	0	4	5	0
VPN PPTP	0	2	0	6	0
รวมระดับความเสี่ยง	**0**	**6**	**8**	**20**	**0**

ตารางที่ 5.5 ระดับความเสี่ยงที่ประเมินพบจากการประเมินค่าระดับความเสี่ยงช่องโหว่ (Risk+)

	ระดับความรุนแรงกรณีเพิ่มปัจจัยผลกระทบต่อองค์กร (Risk+)				
เครื่องแม่ข่าย	**ระดับวิกฤต (Critical)**	**ระดับสูง (High)**	**ระดับกลาง (Medium)**	**ระดับต่ำ (Low)**	**ระดับบันทึก (Note)**
AMC Server	0	3	5	0	0
WEB Server	0	4	5	0	0
OpenMCU 1	0	3	4	2	0
VPN PPTP	0	2	5	1	0
รวมระดับความเสี่ยง	0	12	19	3	0

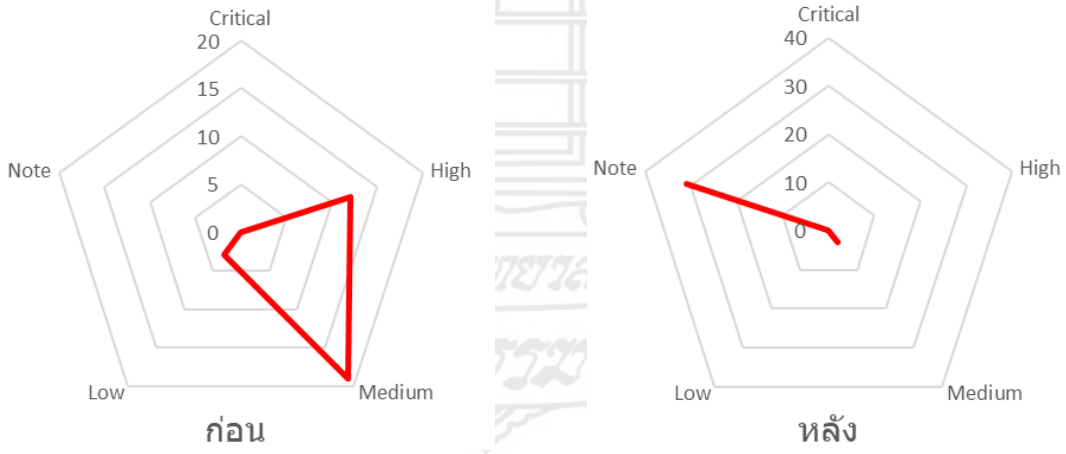
ด้านการประเมินค่าระดับความเสี่ยง ได้ใช้การประเมินค่าโอกาสและผลกระทบ จากการคำนวณตาม CVSS ร่วมกับระเบียบวิธีการประเมินความเสี่ยงของ OWASP จึงทำให้การประเมินค่าระดับความเสี่ยงงานวิจัยนี้มีความน่าเชื่อถือ พบว่าก่อนเพิ่มปัจจัยผลกระทบขององค์กร ภาพรวมระบบสารสนเทศขององค์กร มีแนวโน้มระดับความเสี่ยงอยู่ในระดับต่ำถึงระดับกลางเล็กน้อย และหลังเพิ่มปัจจัยผลกระทบขององค์กร มีแนวโน้มความเสี่ยงอยู่ในระดับกลางถึงระดับสูง แสดงให้เห็นว่าการนำค่าปัจจัยผลกระทบขององค์กร เข้ามาร่วมในการคำนวณหาค่าความเสี่ยงของ

ช่องโหว่จะทำให้ค่าความเสี่ยงช่องโหว่ที่ส่งผลกระทบต่อองค์กรมีค่าความเสี่ยงสูงขึ้น ซึ่งจะส่งผลดีในการตระหนักถึงการรักษาความมั่นคงปลอดภัยทางไซเบอร์ โดยเฉพาะเครื่องแม่ข่ายที่มีความเสี่ยง

3) สรุปการประเมินช่องโหว่ และระดับความเสี่ยงช่องโหว่ หลังจากการแก้ไขช่องโหว่ และการประเมินซ้ำ

ตารางที่ 5.6 ระดับความเสี่ยงช่องโหว่ ที่ประเมินพบจากการประเมินค่าระดับความเสี่ยงช่องโหว่หลังจากการแก้ไขช่องโหว่ และหลังจากการประเมินซ้ำ

เครื่องแม่ข่าย	ระดับความรุนแรงกรณีเพิ่มปัจจัยผลกระทบต่อองค์กร (Risk+)				
	ระดับวิกฤต (Critical)	ระดับสูง (High)	ระดับกลาง (Medium)	ระดับต่ำ (Low)	ระดับบันทึก (Note)
AMC Server	0	0	0	0	8
WEB Server	0	0	3	0	6
OpenMCU 1	0	0	0	0	9
VPN PPTP	0	0	0	0	8
รวมระดับความเสี่ยง	**0**	**0**	**3**	**0**	**31**



ภาพที่ 5.1 แนวโน้มทิศทางความเสี่ยงช่องโหว่ที่มีผลต่อองค์กร ก่อนและหลังการประเมินช่องโหว่ซ้ำ

จากผลการวิจัยการประเมินช่องโหว่ที่พบและมีความเสี่ยงทั้งหมดจำนวน 34 ช่องโหว่ หลังจากการแก้ไขช่องโหว่ที่ประเมินพบ และการประเมินซ้ำแล้วนั้น พบแค่เพียงช่องโหว่ที่มีผลการประเมินค่าระดับความเสี่ยงปานกลาง จำนวน 3 ช่องโหว่ สรุปได้ว่าการดำเนินการตามกระบวนการ กรอบการจัดการช่องโหว่สารสนเทศขององค์กร จากงานวิจัยนี้สามารถกำจัดช่องโหว่

หรือจุดอ่อน และสามารถลดระดับความเสี่ยงช่องโหว่ที่ส่งผลกระทบต่อระบบสารสนเทศขององค์กรได้อย่างมีประสิทธิภาพ โดยมีผลตามตารางที่ 5.6 และแนวโน้มทิศทางความเสี่ยงตามภาพที่ 5.1

1.3 ผู้วิจัยได้ดำเนินการประเมินประสิทธิภาพ กรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กร โดยจัดทำแบบสอบถามในการประเมินประสิทธิภาพโดยมีกลุ่มตัวอย่างจำนวน 19 คน โดยทั้งหมดเป็นบุคลากรที่เกี่ยวข้องกับระบบสารสนเทศขององค์กร ผลการประเมินจากการตอบแบบสอบถามของผู้มีส่วนเกี่ยวข้องกับระบบสารสนเทศขององค์กร มีค่าเฉลี่ยรวมเท่ากับ 4.48 และส่วนเบี่ยงเบนมาตรฐานเท่ากับ 0.64 ระดับการประเมินประสิทธิภาพ กรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กรอยู่ในระดับ มาก โดยสามารถแสดงผลของการประเมิน ดังตารางที่ 5.7

ตารางที่ 5.7 แสดงผลค่าเฉลี่ย ส่วนเบี่ยงเบนมาตรฐานของผลการประเมินประสิทธิภาพ กรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กร

ลำดับ	รายการประเมิน (ผู้มีส่วนเกี่ยวข้องกับระบบสารสนเทศขององค์กร)	$\bar{x}$	S.D.	การแปลผล
1.	การจัดการทรัพย์สิน (Assets Management)	4.53	0.63	มากที่สุด
2.	การประเมิน (Assessment)	4.52	0.61	มากที่สุด
3.	การแก้ไขช่องโหว่ (Remediation)	4.41	0.59	มาก
4.	การประเมินซ้ำ (Re-Assessment)	4.55	0.65	มากที่สุด
5.	การตรวจสอบยืนยันความถูกต้อง (Verification)	4.25	0.71	มาก
6.	ความคิดเห็นต่อกรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กร	4.53	0.69	มากที่สุด
	ผลรวม	**4.48**	**0.64**	**มาก**

สรุปผลการประเมินประสิทธิภาพกรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กรอยู่ในระดับ มาก แสดงให้เห็นว่ากรอบการจัดการช่องโหว่นี้สามารถนำไปใช้เป็นกรอบการจัดการช่องโหว่ระบบสารสนเทศเพื่อการรักษาความมั่นคงปลอดภัย กองบัญชาการกองทัพภาคที่ 2 และควรนำเสนอผู้บังคับบัญชาชั้นสูงของกองทัพภาคที่ 2 เพื่ออนุมัติเป็นหลักการในการใช้กรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กรต่อไป

2. อภิปรายผล

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 สามารถพัฒนาขึ้นมาเป็นกรอบการจัดการช่อง

โหว่ระบบสารสนเทศขององค์กร และสามารถประเมินช่องโหว่ ประเมินความเสี่ยงช่องโหว่ ตลอดจนการกำจัดช่องโหว่ ซึ่งส่งผลกระทบต่อองค์ได้ ซึ่งแสดงให้เห็นในงานวิจัยนี้

ผลการประเมินประสิทธิภาพกรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กรอยู่ในระดับ มาก แสดงให้เห็นว่ากรอบการจัดการช่องโหว่นี้สามารถนำไปใช้เป็นกรอบการจัดการช่องโหว่ระบบสารสนเทศเพื่อการรักษาความมั่นคงปลอดภัย กองบัญชาการกองทัพภาคที่ 2 และควรนำเสนอผู้บังคับบัญชาชั้นสูงของกองทัพภาคที่ 2 เพื่ออนุมัติเป็นหลักการในการใช้กรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กรต่อไป

3. ปัญหาและอุปสรรค

3.1 องค์กรของผู้วิจัยเป็นองค์กรที่มีภารกิจด้านป้องกันประเทศ รายละเอียดบางรายการเป็นชั้นความลับจึงไม่สามารถเปิดเผยได้อย่างสมบูรณ์จึงอาจทำให้รายละเอียดบางรายการขาดความสมบูรณ์

3.2 ผลการทดลองบางรายการอาจต้องใช้งบประมาณในการแก้ไขที่สูง เช่น ช่องโหว่บางรายการต้องใช้งบประมาณในการแก้ไข เช่น ช่องโหว่ที่เกี่ยวข้องกับใบรับรองดิจิทัล จะต้องจัดหาจากผู้ให้บริการที่ได้รับการยอมรับในระดับสากล จึงอาจจะทำให้ผลการทดลองยังไม่ได้รับการแก้ไขเนื่องจากต้องรองบประมาณในการแก้ไข

3.3 งานวิจัยมีระยะเวลาการดำเนินการค่อนข้างจำกัดเนื่องจาก ภารกิจ งานในหน้าที่ทั้งของผู้วิจัยเอง และบุคลากรผู้เกี่ยวข้องกับระบบสารสนเทศ ที่ช่วยเหลือสนับสนุนผู้วิจัย จึงส่งผลทำให้งานวิจัยมีขีดจำกัดพอสมควร

4. ข้อเสนอแนะ

4.1 งานวิจัยนี้ดำเนินการตามปัจจัยสภาพแวดล้อมระบบสารสนเทศขององค์กรผู้วิจัย มีการดำเนินการทดลองใช้กรอบที่พัฒนาขึ้นมา ตามระยะเวลาที่กำหนดและสอดคล้องตามวัตถุประสงค์ของคณะกรรมการตรวจสอบการปฏิบัติตามกรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กร สำหรับแนวทางการประยุกต์ใช้ในองค์กรอื่นๆ หรือหน่วยงานใกล้เคียงที่มีองค์ประกอบคล้ายกัน ก็ควรจะศึกษาสภาพแวดล้อม องค์ประกอบของระบบสารสนเทศขององค์กร เพื่อนำไปปรับปรุงให้สอดคล้องกับสภาพแวดล้อมขององค์กรนั้นๆ เพราะอาจจะมีข้อจำกัดเรื่องเครื่องมือที่ใช้ในการประเมินช่องโหว่ที่มีประสิทธิภาพทางด้านเทคนิคที่เหมาะสมกับการประเมินช่องโหว่อุปกรณ์สารสนเทศของแต่ละองค์กรซึ่งจะไม่เหมือนกัน

4.2 งานวิจัยนี้ผู้วิจัยไม่ได้เปรียบเทียบผลการประเมินความเสี่ยงช่องโหว่ตามกรอบ NIST 800-30R1 และกรอบ CDC เนื่องจากงานวิจัยนี้มุ่งเน้นในการพัฒนากรอบการจัดการช่องโหว่ซึ่งนำกรอบแนวคิดของ NIST 800-30R1 และการดำเนินงานที่เป็นวงรอบลักษณะวงจรชีวิตของ CDC มาใช้เป็นกรอบแนวคิดหลักและปรับใช้กับองค์กรของผู้วิจัยอย่างเหมาะสม ดังนั้นหากผู้วิจัยใช้กรอบแนวคิดของ NIST 800-30R1 เป็นกรอบแนวคิดเดียวในการประเมินความเสี่ยงช่องโหว่ หรือใช้กรอบแนวคิดวงจรชีวิตของ CDC เป็นกรอบแนวคิดเดียวในการประเมินความเสี่ยงช่องโหว่ ผลการวิจัยจะไม่แตกต่างกัน เนื่องจากงานวิจัยนี้ ได้ใช้การประเมินค่าโอกาสและผลกระทบ จากการคำนวณตาม CVSS ร่วมกับระเบียบวิธีการประเมินความเสี่ยงของ OWASP ในการประเมินความเสี่ยงของช่องโหว่ซึ่งเป็นหัวใจหลักของกรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กร เพียงระเบียบวิธีการประเมินความเสี่ยงของช่องโหว่เพียงระเบียบวิธีการเดียวเท่านั้น

4.3 แนวทางพัฒนางานวิจัยในอนาคต

4.3.1 ควรวิจัยเพิ่มเติมเกี่ยวกับการค้นหาจุดอ่อนของระบบสารสนเทศโดยประยุกต์แนวทาง Penetration Test และเพิ่มจำนวนเครื่องมือที่ใช้ในการประเมินช่องโหว่ เพื่อเปรียบเทียบความถูกต้องให้มากยิ่งขึ้น

4.3.2 การประเมินช่องโหว่ควรดำเนินการต่ออุปกรณ์ระบบสารสนเทศอื่นๆ ที่ยังไม่ได้ทำการประเมินช่องโหว่ในงานวิจัยนี้ เช่น อุปกรณ์ ไฟร์วอลล์(Firewall) สวิตซ์ฮับ (Switch hub) เพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์ที่สมบูรณ์ตามกรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กร

4.3.3 ประเด็นความเสี่ยง นอกจากการประเมินความเสี่ยงอุปกรณ์เครื่องแม่ข่ายระบบสารสนเทศแล้ว ควรนำเรื่องความเสี่ยงในด้านอื่นๆ เช่นปัจจัยความเสี่ยงที่เกิดจากมนุษย์ สภาพแวดล้อม นำมาดำเนินการประเมินความเสี่ยง และควรมีการประเมินประสิทธิภาพทางด้านเทคนิคเพิ่มเติม นอกจากใช้แบบสอบถามในการประเมินประสิทธิภาพของกรอบที่พัฒนาขึ้นมา เพื่อประโยชน์สูงสุดต่อองค์กร

4.4 แนวทางการนำไปใช้งานจริงทั้งภายในองค์กร และภายนอกองค์กรเพื่อให้ง่ายต่อการปฏิบัติของบุคลากรผู้เกี่ยวข้องกับระบบสารสนเทศขององค์กร ที่อาจจะขาดความเข้าใจระเบียบวิธีการประเมินความเสี่ยงระบบสารสนเทศขององค์ที่เพียงพอ ควรดำเนินการให้เป็นระบบอัตโนมัติมากขึ้นเช่นขั้นตอนในการคำนวณหาค่าความเสี่ยงของช่องโหว่ที่มีผลกระทบต่อระบบสารสนเทศขององค์กร โดยพัฒนาเป็นโปรแกรมประเมินความเสี่ยงเพื่อความสะดวกและรวดเร็วในการปฏิบัติตามกรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กรมากยิ่งขึ้น

บรรณานุกรม

บรรณานุกรม

ขนิษฐา สิทธิเทียมจันทร์ และคณะ. (2564). การประเมินช่องโหว่ระบบสารสนเทศ กรณีศึกษา มหาวิทยาลัยราชภัฏรำไพพรรณี. *รายงานสืบเนื่องมหาวิทยาลัยเทคโนโลยีราชมงคลรัตนโกสินทร์*, 5(1), 56-62.

จิราพัชร์ พันธุ์ถาวรชัย. (2561). *แนวทางการสร้างกรอบพัฒนาการคืนสภาพได้ด้านไซเบอร์สำหรับการประมวลผลแบบคลาวด์.* (รายงานการศึกษาค้นคว้าอิสระ ปริญญามหาบัณฑิต ไม่ได้ตีพิมพ์). มหาวิทยาลัยศรีปทุม, กรุงเทพฯ.

ธเนศ อมรทัศนสุข. (2557). *การประเมินช่องโหว่ระบบเทคโนโลยีสารสนเทศ กรณีศึกษา ธนาคารพาณิชย์แห่งหนึ่งในประเทศไทย.* (รายงานการศึกษาค้นคว้าอิสระ ปริญญามหาบัณฑิต ไม่ได้ตีพิมพ์). มหาวิทยาลัยเทคโนโลยีมหานคร, กรุงเทพฯ.

พลตรี วาสิฏฐ์ มณีโชต. (2560). *แนวทางการพัฒนามาตรฐานการรักษาความปลอดภัย ของกองทัพบกในอนาคต.* สืบค้นจาก http://www.dsdw2016.dsdw.go.th/doc_pr/ndc_2559-2560/PDF/wpa_8223/ALL.pdf.

พัชรวัฒน์ โกสิตงามดีวงศ์. (2563). การประเมินช่องโหว่ระบบบริหารจัดการทางการแพทย์ กรณีศึกษา โรงพยาบาลภูมิพลอดุลยเดช กรมแพทย์ทหารอากาศ. *วารสารบัณฑิตวิทยาลัยมหาวิทยาลัยธุรกิจบัณฑิตย์*, 9(1), 1-17.

เรืออากาศตรีหญิง ณัชณภัทร ใจอดทน. (2560). *การประเมินค่าช่องโหว่ของเว็บไซต์และการป้องกัน กรณีศึกษา เว็บไซต์กรมควบคุมการปฏิบัติทางอากาศ.* (รายงานการศึกษาค้นคว้าอิสระ ปริญญามหาบัณฑิต ไม่ได้ตีพิมพ์). มหาวิทยาลัยธุรกิจบัณฑิตย์, กรุงเทพฯ.

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

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พุทธศักราช 2562. (2562, 27 พฤษภาคม) *ราชกิจจานุเบกษา.* เล่ม 136 ตอนที่ 69 ก. หน้า 20-51.

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

Andrew Van Der Stock, Brian Glas, Neil Smithline and Torsten Gigler. (2021). *OWASP Top 10-2021.* Retrieved from https://muras.eu/assets/img/OWASP_top_10_2021.pdf

CDC. (2021). *Vulnerability Management Life Cycle*. Retrieved from https://www.cdc.gov/cancer/npcr/tools/security/vmlc.htm

FIRST.Org, Inc. (2019). *Common Vulnerability Scoring System v3 . 0 : Specification Document.* Retrieved from https://www.first.org/cvss/v3.0/specification-document

Gallagher, P.D. (2012). *Guide for Conducting Risk Assessments. NIST Special Publication 800-30 R1*. Retrieved from https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf

Karen Mercedes Goertzel. (2011). *Information Assurance Tools Report–Vulnerability Assessment (IATAC).* Retrieved from https://csiac.org/wp-content/uploads/2021/07/vulnerability_assessment.pdf

NIST. (2018). *Framework for Improving Critical Infrastructure Cybersecurity.* Retrieved from https://nvlpubs.nist.gov/cswp/nist.cswp.04162018.pdf

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

Peter Mell, Karen Scarfone and Sasha Romanosky. (2007). *A Complete Guide to the Common Vulnerability Scoring System Version 2.0.* Retrieved from https://www.first.org/cvss/v2/guide

Stoneburner G., Goguen A. and Feringa A. (2002). *Guide for Information Technology Systems. NIST Special Publication 800-30 Risk Management.* Retrieved From https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30.pdf

ภาคผนวก ก

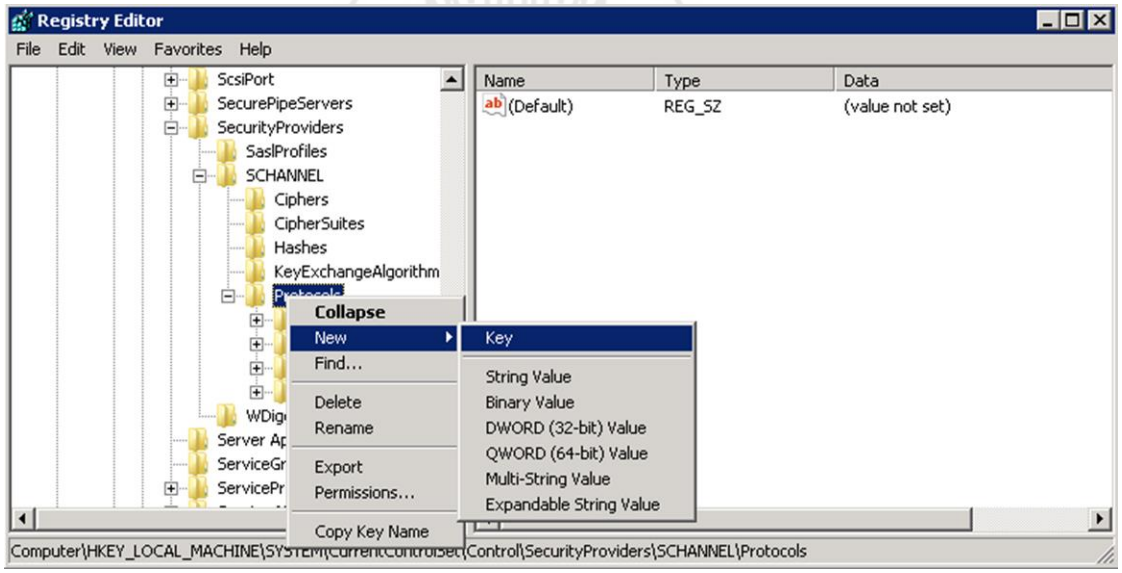
การแก้ไขช่องโหว่ตามรูปแบบและชนิดช่องโหว่

1) การแก้ไขช่องโหว่รูปแบบหรือชนิด TLS/SSL/X.509

ตัวอย่างการแก้ไขช่องโหว่ TLS Version 1.0 Protocol Detection ของอุปกรณ์เครื่องแม่ข่าย AMC Server มีรายละเอียดช่องโหว่คือ การเชื่อมต่อที่เข้ารหัสโดยใช้ TLS 1.0 มีข้อบกพร่องในการออกแบบการเข้ารหัสจำนวนมาก วิธีแก้ไขให้ดำเนินการปิดใช้งาน TLS 1.1 ให้เปิดใช้งาน TLS 1.2 และ TLS 1.3

ขั้นตอนการปิดใช้งาน TLS 1.1

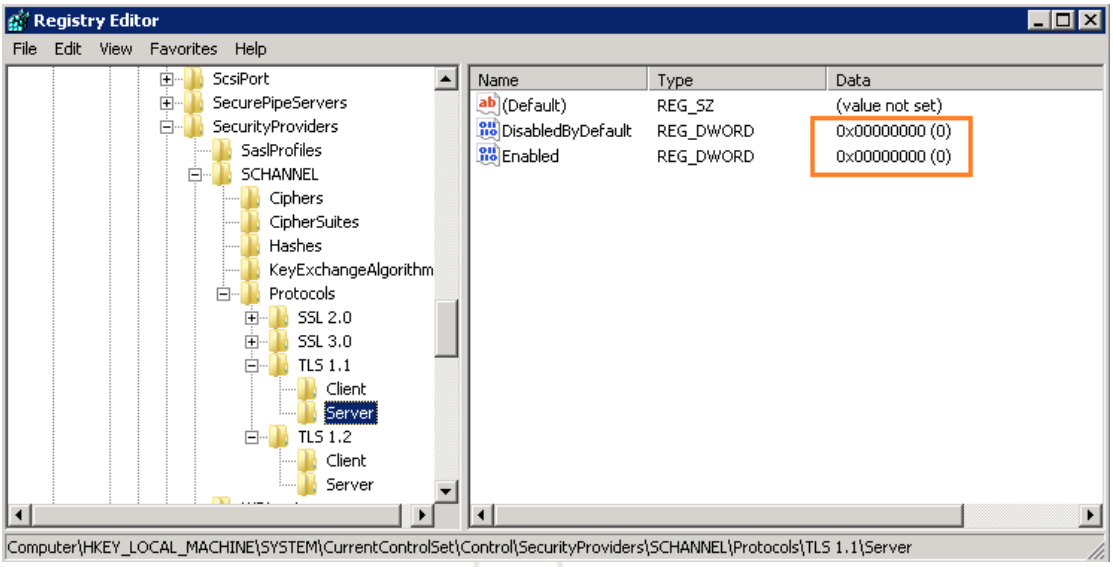
1. ทำการเปิด Command Prompt หรือ Run
2. สั่งเปิดหรือพิมพ์ regedit
3. เปิดค่า HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Control/SecurityProviders/SCHANNEL/Protocols
4. คลิกขวา ที่โฟลเดอร์ Protocals เลือก New > Key
5. เพิ่มโฟลเดอร์ TLS 1.1



6. สร้างโฟลเดอร์ Client และ Server
7. คลิกขวา สร้าง DWORD และระบุค่าดังตัวอย่าง

DisabledByDefault [Value = 0]

Enabled [Value = 0]



ขั้นตอนการเปิดใช้งาน TLS 1.2 และ TLS 1.3

1. ทำตามขั้นตอนการปิดการใช้งาน TLS 1.1 ทุกประการ
2. คลิกขวา สร้าง DWORD และระบุค่าดังนี้

DisabledByDefault [Value = 0]

Enabled [Value = 1]

2) การแก้ไขช่องโหว่รูปแบบหรือชนิด SSH/FTP/TELNET

ตัวอย่างการแก้ไขช่องโหว่ SSH Server Supports RC4 Cipher Algorithms ของอุปกรณ์เครื่องแม่ข่าย OpenMCU 1 มีรายละเอียดช่องโหว่คือ เซิร์ฟเวอร์ที่ให้บริการ SSH ระยะไกลได้กำหนดค่าการเข้ารหัส Arcfour หรือ RC4 เป็นการเข้ารหัสที่อ่อนแอ ถูกถอดรหัสได้ง่าย วิธีแก้ไขให้ดำเนินการปิดใช้งานการสนับสนุน SSH สำหรับการเข้ารหัส RC4 โดยลบ arcfour, arcfour128 และ arcfour256 ออกจากรายการ Ciphers ที่ระบุไว้ใน sshd_config

ขั้นตอนการปิดใช้การเข้ารหัส SSH ที่อ่อนแอบนระบบปฏิบัติการ Linux

1. ล็อกอินเข้าสู่เซิร์ฟเวอร์ในฐานะ root
2. เปิดไฟล์ sshd_config ที่ อยู่ใน/etc/ssh เพิ่มคำสั่งต่อไปนี้

Ciphers aes256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes128-ctr
MACs hmac-sha2-512-etm@openssh.com,hmac-sha2-256-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-512,hmac-sha2-256,hmac-ripemd160,hmac-sha1
KexAlgorithms diffie-hellman-group-exchange-sha256,diffie-hellman-group14-sha1,diffie-hellman-group-exchange-sha1

3. ตรวจสอบให้มั่นใจว่าไม่มีชุดคำสั่ง arcfour, arcfour128 และ arcfour256 อยู่ในไฟล์ sshd_config

4. ใช้คำสั่งรีสตาร์ท service sshd restart เพื่อให้การเปลี่ยนแปลงมีผลใน SSH และเริ่มบริการ sshd ใหม่

3) การแก้ไขช่องโหว่รูปแบบหรือชนิด DNS

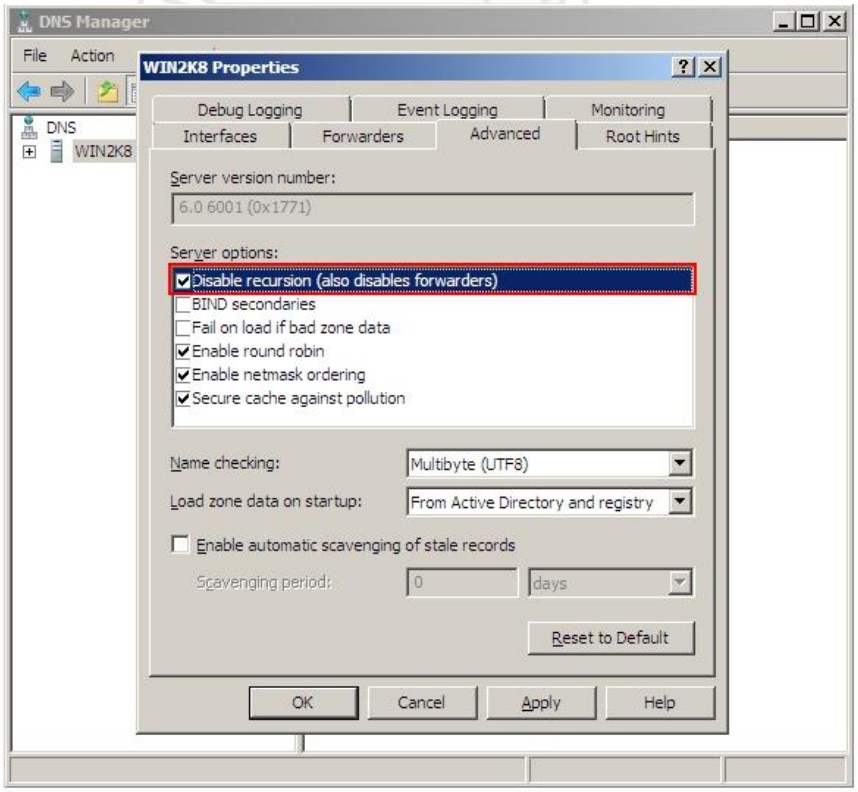
ตัวอย่างการแก้ไขช่องโหว่ Nameserver Processes Recursive Queries ของอุปกรณ์เครื่องแม่ข่าย AMC Server มีรายละเอียดช่องโหว่คือ การอนุญาตให้ Nameserver ประมวลผลการสืบค้นแบบเรียกซ้ำที่มาจากระบบอื่นๆ ในบางสถานการณ์ อาจถูกผู้โจมตีดำเนินการโจมตีแคชซึ่งทำให้เกิดการหยุดให้บริการของเครื่องแม่ข่ายได้ วิธีแก้ไขให้ดำเนินการปิดการใช้งานการเรียกซ้ำบนเซิร์ฟเวอร์ DNS

ขั้นตอนการปิดการใช้งานการเรียกซ้ำบนเซิร์ฟเวอร์ DNS

1. เปิด DNS Manager ไปที่ Start > All Programs > Administrative Tools > DNS

2. คลิกขวาบนเครื่องแม่ข่ายที่ต้องการแล้วเลือก Properties

3. เลือกแท็บ Advanced แล้วทำเครื่องหมายถูกที่รายการ Disable recursion (also disables forwarders) แล้วคลิก Apply

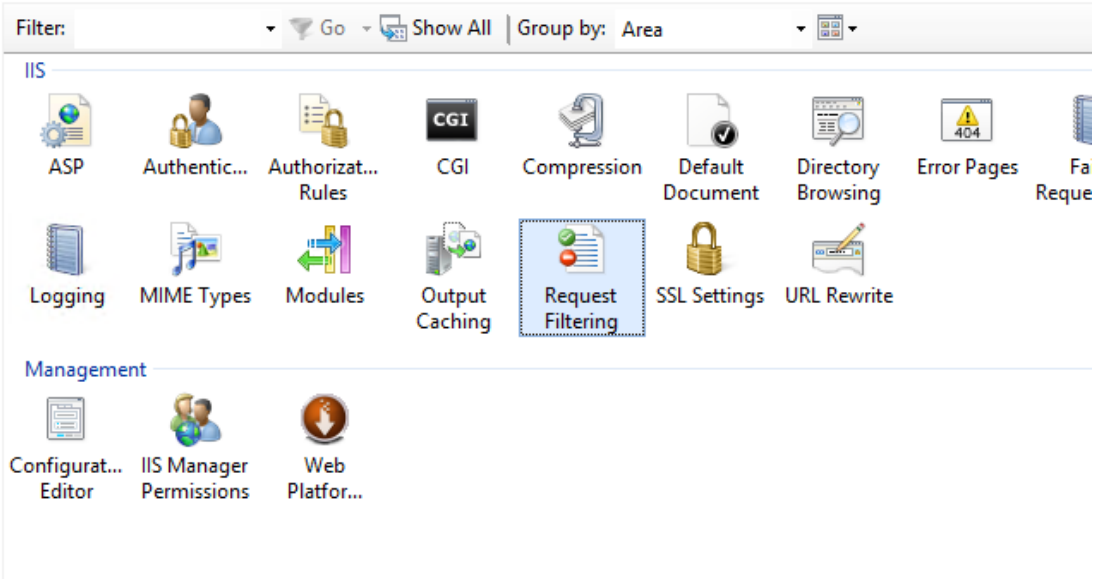


4) การแก้ไขช่องโหว่รูปแบบหรือชนิด HTTP OPTION

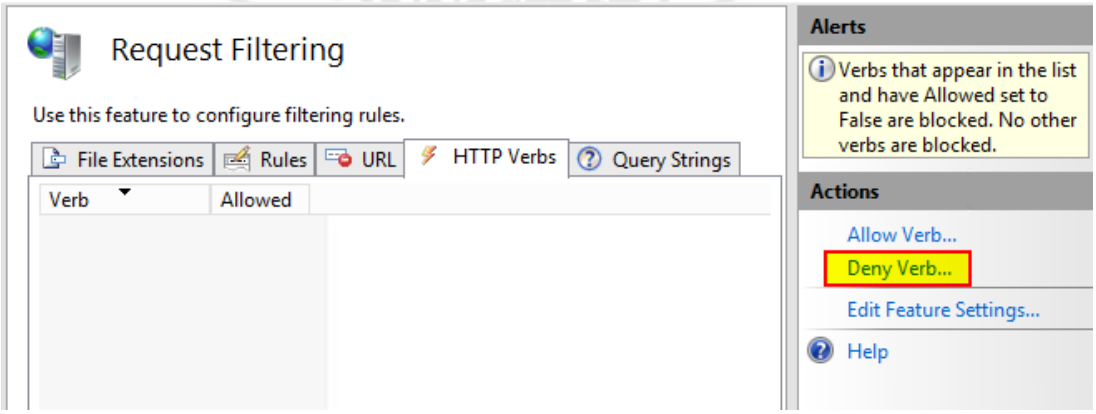
4.1) ตัวอย่างการแก้ไขช่องโหว่ HTTP OPTIONS Method Enabled ของอุปกรณ์เครื่องแม่ข่าย AMC Server มีรายละเอียดช่องโหว่คือ เว็บเซิร์ฟเวอร์ที่ตอบสนองต่อเมธอด OPTIONS HTTP จะเปิดเผยวิธีการอื่นๆ ที่เว็บเซิร์ฟเวอร์สนับสนุน วิธีนี้สามารถช่วยให้ผู้โจมตีค้นหาข้อมูลเกี่ยวกับการกำหนดค่าเซิร์ฟเวอร์และเป็นช่องโหว่ในการโจมตีได้ วิธีแก้ไขให้ดำเนินการปิดใช้งาน HTTP OPTIONS บนเว็บเซิร์ฟเวอร์

ขั้นตอนการปิดใช้งาน HTTP OPTIONS บน IIS

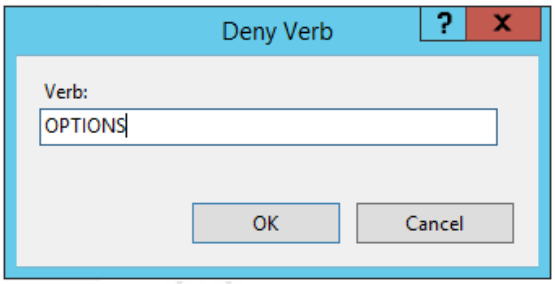
1. เปิด IIS Manager
2. ไปที่ Request Filtering แล้วเลือกเปิดหน้าต่าง Request Filtering



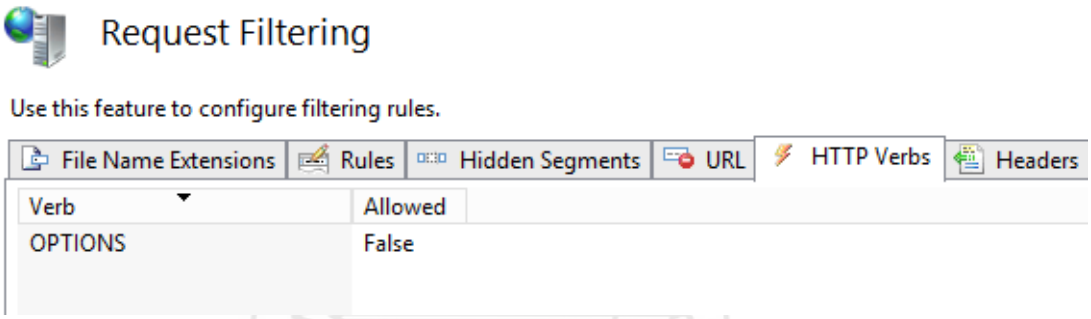
3. เลือกหัวข้อ HTTP Verbs แล้วคลิกให้เลือก Deny Verb ที่รายการ Actions ทางด้านขวา



4. จะปรากฏหน้าต่างตอบโต้ขึ้นมาให้ใส่ข้อความ “OPTIONS” ลงไปที่ช่องตอบโต้ แล้วคลิกตกลง



5. จะปรากฏหน้าแจ้งให้ทราบว่าได้ทำการปิดใช้งาน HTTP OPTIONS แล้วสังเกตจากข้อความ False ในคอลัมพ์ Allowed



4.2) ตัวอย่างการแก้ไขช่องโหว่ HTTP OPTIONS Method Enabled ของอุปกรณ์เครื่องแม่ข่าย WEB Server มีรายละเอียดช่องโหว่คือ เว็บเซิร์ฟเวอร์ที่ตอบสนองต่อเมธอด OPTIONS HTTP จะเปิดเผยวิธีการอื่นๆ ที่เว็บเซิร์ฟเวอร์สนับสนุน วิธีนี้สามารถช่วยให้ผู้โจมตีค้นหาข้อมูลเกี่ยวกับการกำหนดค่าเซิร์ฟเวอร์และเป็นช่องโหว่ในการโจมตีได้ วิธีแก้ไขให้ดำเนินการปิดใช้งาน HTTP OPTIONS บนเว็บเซิร์ฟเวอร์

ขั้นตอนการปิดใช้งาน HTTP OPTIONS บน Apache

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
```

ภาคผนวก ข

แบบสอบถามการประเมินประสิทธิภาพ กรอบการจัดการช่องโหว่ระบบสารสนเทศ
เพื่อการรักษามั่นคงปลอดภัย กองบัญชาการกองทัพภาคที่ 2

แบบประเมินประสิทธิภาพเรื่อง “การพัฒนากรอบการจัดการช่องโหว่ระบบสารสนเทศเพื่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์ กรณีศึกษา กองบัญชาการกองทัพภาคที่ 2”

<u>คำชี้แจง</u>

แบบประเมินประสิทธิภาพนี้ได้จัดทำขึ้นเพื่อสอบถามความคิดเห็นของท่านเกี่ยวกับความสามารถในการจัดการช่องโหว่ระบบสารสนเทศขององค์กร และใช้ในการประเมินประสิทธิภาพกรอบการจัดการช่องโหว่ระบบสารสนเทศที่ผู้วิจัยได้พัฒนาขึ้นมา ผู้วิจัยใคร่ขอความร่วมมือในการตอบแบบสอบถาม โดยขอความกรุณาท่านให้ข้อมูลหรือแสดงความคิดเห็นที่ตรงกับความเป็นจริงมากที่สุด ข้อมูลที่ได้จะนำไปใช้ประกอบการศึกษาวิจัยทางวิชาการเท่านั้น ขอรับรองว่าข้อมูลที่ได้จากแบบสอบถามจะไม่มีผลกระทบหรือก่อให้เกิดความเสียหายกับท่านหรือผู้ที่เกี่ยวข้องแต่ประการใด ข้อคำถามในแบบสอบถาม แบ่งออกเป็น 3 ส่วน คือ

ส่วนที่ 1 ข้อมูลทั่วไปเกี่ยวกับผู้ตอบแบบสอบถาม

ส่วนที่ 2 ความคิดเห็นเกี่ยวกับกรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กร

ส่วนที่ 3 ความคิดเห็นและข้อเสนอแนะอื่น ๆ

การแปลผลระดับความคิดเห็น แบ่งเป็น 5 ระดับดังต่อไปนี้

5 หมายถึง ระดับมากที่สุด

4 หมายถึง ระดับมาก

3 หมายถึง ระดับปานกลาง

2 หมายถึง ระดับน้อย

1 หมายถึง ระดับน้อยที่สุด

นิยามคำศัพท์ที่เกี่ยวข้อง

1. กรอบการจัดการช่องโหว่ (Vulnerability Management Framework) หมายถึง "กรอบการปฏิบัติที่เป็นวัฏจักรในการระบุ จำแนก จัดลำดับความสำคัญ แก้ไข และบรรเทา" ช่องโหว่ของซอฟต์แวร์ การจัดการช่องโหว่เป็นส่วนสำคัญในการรักษาความปลอดภัยคอมพิวเตอร์และความปลอดภัยของเครือข่าย และต้องไม่สับสนกับการประเมินช่องโหว่

2. ความมั่นคงปลอดภัยทางไซเบอร์ (CYBER SECURITY) หมายถึง “การรักษาความมั่นคงปลอดภัยไซเบอร์” หมายความว่า มาตรการหรือการดำเนินการที่กำหนดขึ้น เพื่อป้องกัน รับมือและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกประเทศ อันกระทบต่อความมั่นคงของรัฐความมั่นคงทางเศรษฐกิจความมั่นคงทางทหาร และความสงบ เรียบร้อยภายในประเทศ

3. การวิเคราะห์ช่องโหว่ (Vulnerability Analysis) เป็นการประเมินช่องโหว่ที่ค้นพบในระบบปฏิบัติการ (OS) ซอฟต์แวร์ หรืออุปกรณ์ Network/Security ว่ามีช่องโหวใดบ้าง และมีระดับความรุนแรงเท่าใด มีความเสี่ยงที่ส่งผลกระทบต่อองค์กรมากน้อยเพียงใด เพื่อให้ผู้ดูแลระบบทราบและทำการแก้ไขเพื่อปิดช่องโหว่นั้น

ผู้วิจัย

พ.ต.ทัญญะ สิทธิมณีวรรณ E-mail : tunya.rabbit@gmail.com โทรศัพท์ 09-9462-9519

นักศึกษา หลักสูตรปริญญาวิทยาศาสตรมหาบัณฑิต แขนงวิชาเทคโนโลยีสารสนเทศและการสื่อสาร

สาขาวิชาวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยสุโขทัยธรรมาธิราช

ส่วนที่ 1 สถานภาพทั่วไปของผู้ตอบแบบประเมินตนเอง

โปรดทำเครื่องหมาย ✓ ในช่อง ☐ ที่ตรงกับข้อมูลของท่าน เพียงช่องเดียว

1. เพศ ☐ 1) ชาย ☐ 2) หญิง

2. อายุ ☐ 1) 20-30 ปี ☐ 2) 31-40 ปี

☐ 3) 41-50 ปี ☐ 4) 51-60 ปี

3. ตำแหน่ง ☐ 1) เจ้าหน้าที่ระดับปฏิบัติการสารสนเทศ ☐ 2) ผู้ดูแลระบบสารสนเทศ

☐ 3) ผู้บริหารระบบสารสนเทศ ☐ 4) ผู้บริหารองค์กร

4. ระยะเวลาที่ปฏิบัติงาน ☐ 1) น้อยกว่า 1 ปี ☐ 2) 1-5 ปี

☐ 3) 5-10 ปี ☐ 4) มากกว่า 10 ปี

5. ท่านทราบถึงช่องโหว่ระบบสารสนเทศหรือไม่ ☐ 1) ทราบ ☐ 2) ไม่ทราบ

ส่วนที่ 2 ระดับความคิดเห็นของผู้มีส่วนเกี่ยวข้องกับระบบสารสนเทศขององค์กรต่อกรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กร

โปรดทำเครื่องหมาย ✓ ในช่อง ที่ตรงกับระดับความคิดเห็นของท่านมากที่สุด

หัวข้อวิเคราะห์กรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กร	ระดับความเห็น				
	5	4	3	2	1
1. การจัดการทรัพย์สิน (Assets Management)					
1.1 การระบุอุปกรณ์เครื่องแม่ข่ายสอดคล้องกับประเด็นการรักษาความมั่นคงปลอดภัยทางไซเบอร์ขององค์กร					
1.2 การประเมินอุปกรณ์เครื่องแม่ข่ายที่ส่งผลกระทบต่อองค์กรโดยใช้ค่าคะแนนปัจจัยผลกระทบทางเทคนิคเป็นการประเมินผลกระทบที่เหมาะสมกับองค์กร					
1.3 การจัดลำดับความสำคัญของอุปกรณ์เครื่องแม่ข่ายในการเข้ารับการประเมินช่องโหว่ ซึ่งเป็นผลจากการประเมินอุปกรณ์เครื่องแม่ข่ายที่ส่งผลกระทบต่อองค์กรมีลำดับที่สอดคล้องกับภารกิจขององค์กร					
1.4 ห้วงเวลาที่เข้ารับการประเมินช่องโหว่ของอุปกรณ์เครื่องแม่ข่ายไม่กระทบต่อภารกิจขององค์กร					
1.5 มีระบบสำรองที่สามารถทำงานคู่ขนานหรือทดแทนระบบเดิมได้					
2. การประเมิน (Assessment)					
2.1 เครื่องมือที่ใช้ในการประเมินช่องโหว่มีความง่ายในการจัดการหรือการใช้งาน					
2.2 เครื่องมือที่ใช้ในการประเมินช่องโหว่สามารถตรวจพบช่องโหว่ได้สมบูรณ์					
2.3 เครื่องมือที่ใช้ในการประเมินช่องโหว่มีรายละเอียดช่องโหว่และรายละเอียดการแก้ไขอย่างชัดเจน					
2.4 เครื่องมือที่ใช้ในการประเมินช่องโหว่สามารถระบุระดับความรุนแรงของช่องโหว่ที่ประเมินได้					

หัวข้อวิเคราะห์กรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กร	ระดับความเห็น				
	5	4	3	2	1
2.5 หลักการและทฤษฎีในการประเมินค่าระดับความเสี่ยงช่องโหว่ที่ส่งผลกระทบอุปกรณ์เครื่องแม่ข่ายในการปฏิบัติภารกิจขององค์กรนั้นมีความน่าเชื่อถือสามารถนำมาประเมินความเสี่ยงช่องโหว่ได้					
2.6 การนำปัจจัยผลกระทบทางด้านเทคนิคมาใช้ในการประเมินความเสี่ยงอุปกรณ์เครื่องแม่ข่ายสามารถช่วยวิเคราะห์ความเสี่ยงต่ออุปกรณ์เครื่องแม่ข่ายได้ดียิ่งขึ้น					
2.7 การแสดงความสำคัญของระดับความเสี่ยงช่องโหว่ช่วยให้สามารถจัดการช่องโหว่ที่ประเมินพบได้อย่างถูกต้องและรวดเร็วมากยิ่งขึ้น					
2.8 รายงานผลการประเมินความเสี่ยงมีรายละเอียดที่ใช้ในการแก้ไขช่องโหว่ได้สมบูรณ์					
3. การแก้ไข (Remediation)					
3.1 การแก้ไขช่องโหว่ที่ประเมินพบสามารถปฏิบัติได้อย่างถูกต้องตามรายละเอียดการแก้ไขช่องโหว่จากรายงานการประเมินความเสี่ยงช่องโหว่ที่ได้รับมา					
3.2 ข้อมูลช่องโหว่ที่ทำการแก้ไขนอกจากรายละเอียดจากรายงานการประเมินความเสี่ยงช่องโหว่แล้ว ยังสามารถหารายละเอียดจากแหล่งอื่นๆ ได้สะดวก เช่น อินเทอร์เน็ต					
3.3 การแก้ไขช่องโหว่สามารถปิดช่องโหว่ที่มีความเสี่ยงอย่างสมบูรณ์					
3.4 การรายงานแก้ไขช่องโหว่ที่ถูกต้องและรวดเร็ว					
3.5 การประสานงานเพื่อความสอดคล้องในการแก้ไขช่องโหว่ระหว่างผู้ปฏิบัติในขั้นตอนการแก้ไขกับผู้ปฏิบัติในขั้นตอนการประเมินซ้ำ					
4. การประเมินซ้ำ (Re-Assessment)					
4.1 ขั้นตอนการประเมินซ้ำหลังจากการแก้ไขช่องโหว่ มีกระบวนการสำคัญและมีความเหมาะสมเพื่อให้ทราบผลของการแก้ไขช่องโหว่					
4.2 กระบวนการประเมินซ้ำเป็นการปฏิบัติที่ไม่ซับซ้อนเพราะใช้รูปแบบขั้นตอนการประเมินแบบเดิม					

หัวข้อวิเคราะห์กรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กร	ระดับความเห็น				
	5	4	3	2	1
4.3 มีรายงานการประเมินซ้ำที่สมบูรณ์					
4.4 ทราบสาเหตุกรณีพบช่องโหว่จากการประเมินซ้ำ สามารถให้รายละเอียดในการแก้ไขเพิ่มเติมได้					
4.5 การรายงานผลการประเมินซ้ำมีรายละเอียดอย่างชัดเจน					
5. การตรวจสอบยืนยันความถูกต้อง (Verification)					
5.1 มีการตรวจสอบความถูกต้องในการประเมินช่องโหว่ การประเมินความเสี่ยงช่องโหว่ที่ส่งผลกระทบกับอุปกรณ์เครื่องแม่ข่ายสารสนเทศขององค์กร การแก้ไขช่องโหว่ ในรูปแบบของ คณะกรรมการ จากคำสั่งแต่งตั้งคณะกรรมการตรวจสอบความถูกต้องการจัดการช่องโหว่ระบบสารสนเทศขององค์กร					
5.2 คณะกรรมการประกอบไปด้วยบุคลากรที่มีความรู้ความสามารถ ในการตรวจสอบความถูกต้องในการประเมินช่องโหว่					
5.3 คณะกรรมการให้คำแนะนำและวิธีการแก้ปัญหากรณีตรวจสอบพบข้อบกพร่องในการประเมินช่องโหว่					
6. ความคิดเห็นต่อกรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กร					
6.1 ท่านคิดว่ากรอบการจัดการช่องโหว่นี้สามารถใช้เป็นกรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กรได้					
6.2 กรอบการจัดการช่องโหว่นี้ ควรกำหนดเป็นหลักการนำเสนอผู้บังคับบัญชาอนุมัติใช้เป็นกรอบการจัดการช่องโหว่ระบบสารสนเทศขององค์กร เพื่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์ กองทัพภาคที่ 2					

ส่วนที่ 3 ความคิดเห็นและข้อเสนอแนะอื่น ๆ

.....

.....

.....

.....

ผู้วิจัย ขอกราบขอบพระคุณที่ท่านได้กรุณาเสียสละเวลาในการตอบแบบสอบถาม

ภาคผนวก ค

หนังสือขอความอนุเคราะห์กรุณาอนุมัติให้นักศึกษาทำการศึกษาค้นคว้าอิสระ

ที่ อว ๐๖๐๒.๒๕/๗๐๖

สาขาวิทยาศาสตร์และเทคโนโลยี
มหาวิทยาลัยสุโขทัยธรรมาธิราช
ตำบลบางพูด อำเภอปากเกร็ด
จังหวัดนนทบุรี ๑๑๑๒๐

๘ มิถุนายน ๒๕๖๕

เรื่อง ขอความอนุเคราะห์กรุณาอนุมัติให้นักศึกษาทำการศึกษาค้นคว้าอิสระ

เรียน แม่ทัพภาคที่ ๒

ด้วย พันตรี ทัญญะ สิทธิมณีวรรณ รหัสประจำตัวนักศึกษา ๒๖๓๙๖๐๐๓๑๗ นักศึกษาปริญญาโท หลักสูตรวิทยาศาสตร์มหาบัณฑิต แขนงวิชาเทคโนโลยีสารสนเทศและการสื่อสาร สาขาวิชาวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยสุโขทัยธรรมาธิราช ปัจจุบันอยู่ระหว่างการทำการศึกษาค้นคว้าอิสระ "การพัฒนากรอบการจัดการช่องโหว่ระบบสารสนเทศเพื่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์ กรณีศึกษา กองบัญชาการกองทัพภาคที่ ๒" โดยมี ผู้ช่วยศาสตราจารย์ ดร.ชจิตพรรณ กฤตพลวิมาน เป็นอาจารย์ที่ปรึกษา

ในการนี้ สาขาวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยสุโขทัยธรรมาธิราช พิจารณาแล้วเห็นว่า พันตรี ทัญญะ สิทธิมณีวรรณ เป็นบุคลากรของกองบัญชาการกองทัพภาคที่ ๒ และงานวิจัยดังกล่าวนี้จะเป็นประโยชน์ต่อองค์กรของท่าน จึงใคร่ขอความอนุเคราะห์จากท่าน ได้กรุณาอนุมัติการทำการศึกษาค้นคว้าอิสระในครั้งนี้ เพื่อที่นักศึกษาจะได้ดำเนินการตามขั้นตอนของการวิจัยต่อไป

จึงเรียนมาเพื่อโปรดให้ความอนุเคราะห์ และขอขอบคุณมา ณ โอกาสนี้ สำหรับการดำเนินการ นักศึกษาจะได้ประสานในรายละเอียดกับส่วนราชการที่เกี่ยวข้องเพิ่มเติมโดยตรงต่อไป

ขอแสดงความนับถือ

(อาจารย์ ดร.สิทธิชัย รัชยศโยธิน)
ประธานกรรมการประจำสาขาวิชาวิทยาศาสตร์และเทคโนโลยี

สาขาวิชาวิทยาศาสตร์และเทคโนโลยี
โทรศัพท์ ๐ ๒๕๐๔ ๘๒๘๑
โทรสาร ๐ ๒๕๐๓ ๔๙๓๒

ประวัติผู้ศึกษา

ชื่อ	พันตรี ทัญญะ สิทธิมณีวรรณ
วัน เดือน ปีเกิด	6 มิถุนายน 2513
สถานที่เกิด	อำเภอสีคิ้ว จังหวัดนครราชสีมา
ประวัติการศึกษา	วิทยาศาสตรบัณฑิต สาขาวิทยาการคอมพิวเตอร์
	สถาบันราชภัฏนครราชสีมา 2543
สถานที่ทำงาน	แผนกเทคโนโลยีสารสนเทศและการสื่อสาร กองทัพภาคที่ 2
ตำแหน่งปัจจุบัน	นายทหารดำเนินกรรมวิธีข้อมูล
	แผนกเทคโนโลยีสารสนเทศและการสื่อสาร กองทัพภาคที่ 2