แนวทางการป้องกันภัยจากมัลแวร์เรียกค่าไถ่ในระบบควบคุมอุตสาหกรรม ในโรงงานเขตพื้นที่พระนครศรีอยุธยา: กรณีศึกษาคริปโทล็อกเกอร์

Guidelines for Ransomware Protections on Industrial Control Systems in Phra Nakhon Si Ayutthaya-based Factories: A Case Study of CryptoLocker

พิทยา นครไทย[1] , ณัทกฤช พรหมจันทร์[2] และ คริชณะ ฉิมมณี[1,*]

[1] วิทยาลัยนวัตกรรมดิจิทัลเทคโนโลยี มหาวิทยาลัยรังสิต

[2] สำนักปฏิบัติการ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

Phitaya Nakhonthai[1], Naughtakid Phromchan[2], and Krishna Chimmanee[1]

[1] College of Digital Innovation Technology, Rangsit University

[2] Office of Operations, National Cyber Security Agency

Received: February 17, 2024 | Revised: May 31, 2024 | Accepted: July 25, 2024

บทความวิจัย (Research Article)

บทคัดย่อ

ในยุคของอุตสาหกรรม 5.0 ระบบควบคุมในโรงงานอุตสาหกรรมมีการเชื่อมต่อผ่านเครือข่ายคอมพิวเตอร์ ด้วยเหตุนี้จึงกลายเป็นหนึ่งในเป้าหมายหลักที่ถูกโจมตีโดยมัลแวร์เรียกค่าไถ่ ดังนั้น งานวิจัยฉบับนี้จึงมีวัตถุประสงค์เพื่อหาแนวทางการป้องกันภัยคุกคามจากมัลแวร์เรียกค่าไถ่ที่เหมาะสม สำหรับระบบควบคุมในโรงงานอุตสาหกรรม ซึ่งเป็นงานวิจัยเชิงคุณภาพ โดยใช้การประชุมทางวิชาการกลุ่มเป้าหมายที่กำหนดหรือการสนทนากลุ่มเพื่อหาแนวทางป้องกันมัลแวร์เรียกค่าไถ่ตลอดจนข้อปฏิบัติในการรับมือการโจมตีจากมัลแวร์เรียกค่าไถ่ภายในระบบควบคุมในโรงงานอุตสาหกรรม ผลจากการวิจัย คือ 1) ได้แผนภาพแนวทางป้องกันมัลแวร์เรียกค่าไถ่แสดงถึงความสัมพันธ์ระหว่างเทคโนโลยีสารสนเทศ (IT), เทคโนโลยีเชิงปฏิบัติการ (OT) และระบบควบคุมอุตสาหกรรม (ICS) บนพื้นฐาน 5 ขั้นตอนของแนวทางของสถาบันมาตรฐานและเทคโนโลยีแห่งชาติ กระทรวงพาณิชย์ของสหรัฐอเมริกา และ 2) ได้โมเดล (Model) ในการใช้งานจริงระหว่างไอทีโซน (IT Zone) และโอทีโซน (OT Zone) โดยให้ความสำคัญกับฐานข้อมูล และการพิสูจน์ตัวตน ซึ่งเป็นจุดอ่อนในปัจจุบัน และได้นำไปใช้จริงในโรงงานอุตสาหกรรมขนาดใหญ่เป็นกรณีศึกษา

คำสำคัญ: ระบบควบคุมอุตสาหกรรม, มัลแวร์เรียกค่าไถ่, เอ็นไอเอสที

* Corresponding Author, Email: sanon.s@rsu.ac.th

Abstract

In the era of Industry 5.0, control systems in industrial plants are connected through computer networks. Consequently, these systems have become primary targets for ransomware attacks. Therefore, this research aimed to identify appropriate measures to protect against ransomware threats for industrial control systems. It was a qualitative study utilizing focus group discussions or targeted academic conferences to find ransomware prevention measures and response practices for ransomware attacks within industrial control systems. The results of the research were: 1) A technological diagram that illustrates the relationship among Information Technology (IT), Operational Technology (OT), and Industrial Control Systems (ICS) convergence based on the five-step framework of the National Institute of Standards and Technology (NIST), under the U.S. Department of Commerce, and 2) A practical model for implementation between IT Zone and OT Zone, with a particular emphasis on databases and authentication, which are current vulnerabilities. This model was applied in large industrial plants as a case study.

Keywords: Industrial Control Systems, Ransomware, NIST

บทนำ

ในยุคของอุตสาหกรรม 5.0 ระบบควบคุมในโรงงานอุตสาหกรรม เชื่อมต่อผ่านอินเตอร์เฟสเครือข่ายที่หลากหลายในการเชื่อมต่อระหว่างคอมพิวเตอร์ควบคุมเครื่องจักรเพื่อสื่อสารข้อมูลการผลิต ปัจจุบันการปฏิวัติอุตสาหกรรมครั้งที่ 5 ได้นำระบบอัจฉริยะ และหุ่นยนต์ร่วมปฏิบัติช่วยพัฒนากระบวนการผลิตให้มีประสิทธิภาพ รวดเร็ว และมีความแม่นยำสูงมากขึ้น นอกจากนี้ความต้องการในการส่งข้อมูลมายังเครื่องแม่ข่าย เพื่อบันทึกข้อมูลสำหรับตรวจสอบแบบเรียลไทม์ ซึ่งเป็นข้อมูลสำคัญ ถือเป็นปัจจัยสำคัญในการขับเคลื่อนให้เกิดประสิทธิภาพ และส่งผลให้การผลิตมีข้อผิดพลาดที่ลดลง ด้วยเหตุนี้ระบบควบคุมในโรงงานอุตสาหกรรมจึงกลายเป็นหนึ่งในเป้าหมายหลักที่ถูกโจมตีโดยผู้คุกคามหลายราย ล่าสุดรายงานโดย Alamri (2023) จากเว็บไซต์ดารกอส (Dragos) พบว่าสถิติร้อยละ 70 ในไตรมาสที่ 2 ปี 2566 การโจมตีจากมัลแวร์เรียกค่าไถ่ ได้มุ่งเป้าโจมตีไปที่ภาคการผลิต ซึ่งเพิ่มขึ้นเป็นจำนวนมากเมื่อเทียบที่ผ่านมา ทำให้การดำเนินงานหลายองค์กรในส่วนสายการผลิตในระบบควบคุมในโรงงานอุตสาหกรรมได้รับผลกระทบต้องหยุดชะงักลง

บทความวิจัยฉบับนี้เป็นงานวิจัยเชิงคุณภาพ โดยใช้การประชุมทางวิชาการกลุ่มเป้าหมายที่กำหนดหรือสนทนากลุ่ม (Focus Group) เป็นเครื่องมือการวิจัยเพื่อหาแนวทางการป้องกันภัยจากมัลแวร์เรียกค่าไถ่ตลอดจนข้อปฏิบัติในการรับมือในกรณีที่ถูกโจมตีจากมัลแวร์เรียกค่าไถ่ภายในระบบควบคุมในโรงงานอุตสาหกรรมโดยใช้กรณีศึกษาภัยคุกคามที่เกิดขึ้นจริง มาหาแนวทางป้องกันบนพื้นฐานของเอ็นไอเอสที (NIST) จากนั้นได้นำแนวทางที่นำเสนอมาใช้เป็นกรณีศึกษากับโรงงานอุตสาหกรรมขนาดใหญ่แห่งหนึ่ง เพื่อเป็นการ

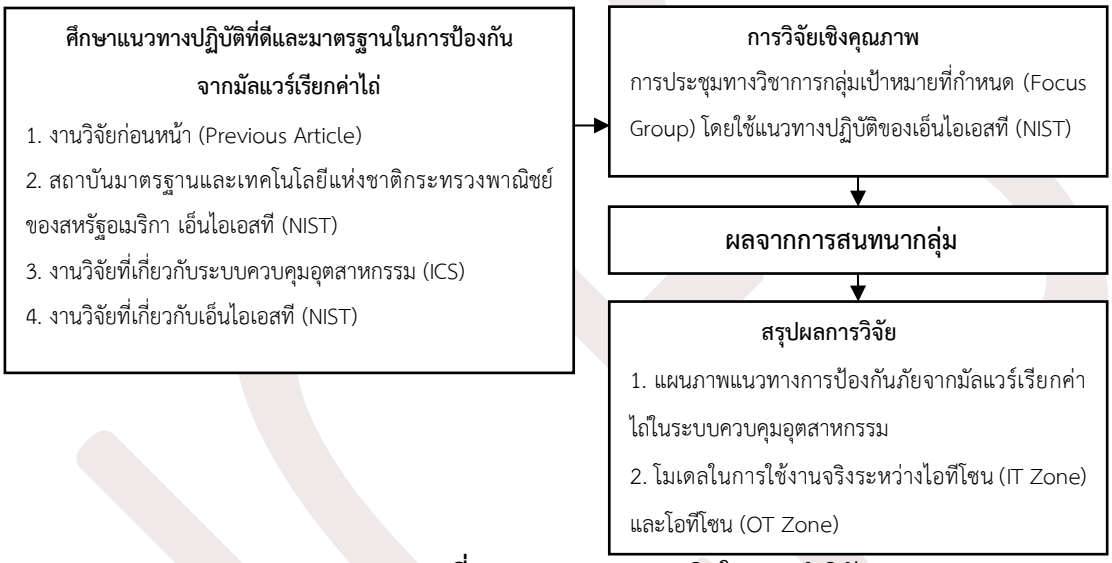
พิสูจน์ว่าแนวทางที่นำเสนอสามารถใช้งานได้จริงและเป็นประโยชน์ช่วยเติมเต็มแนวทางการป้องกันภัยจากมัลแวร์เรียกค่าไถ่ให้กับเจ้าหน้าที่ทางสารสนเทศป้องกันภัยจากมัลแวร์เรียกค่าไถ่

วัตถุประสงค์

1) แผนภาพแนวทางการป้องกันภัยจากมัลแวร์เรียกค่าไถ่ในระบบควบคุมอุตสาหกรรมในโรงงาน

2) โมเดลในการใช้งานจริงระหว่างไอทีโซน (IT Zone) และโอทีโซน (OT Zone) ในระบบควบคุมอุตสาหกรรมในโรงงานเขตพื้นที่พระนครศรีอยุธยา เพื่อป้องกันภัยจากมัลแวร์เรียกค่าไถ่คริปโทล็อกเกอร์

กรอบแนวคิดการวิจัย



ภาพที่ 1 กรอบแนวความคิดในการทำวิจัย

งานวิจัยฉบับนี้เป็นงานวิจัยเชิงคุณภาพโดยใช้การประชุมกลุ่มเป้าหมายที่กำหนด (Focus Group) เพื่อให้ได้แนวทางป้องกันภัยจากมัลแวร์เรียกค่าไถ่ที่เหมาะสมของระบบควบคุมในโรงงานอุตสาหกรรม (ICS) โดยศึกษาแนวทางปฏิบัติจากแหล่งข้อมูลงานวิจัยที่เกี่ยวข้อง โดยในงานวิจัยก่อนหน้านี้ได้นำเสนอกรณีศึกษาจากเหตุการณ์ที่เกิดขึ้นจริง ซึ่งได้ทำการวิเคราะห์ทางนิติวิทยาดิจิทัลจากการโจมตีของมัลแวร์เรียกค่าไถ่คริปโทล็อกเกอร์ เพื่อใช้เป็นข้อมูลสำหรับหาแนวทางการป้องกันภัยจากมัลแวร์ ดังนั้น ในงานวิจัยฉบับนี้จึงได้นำเสนอแนวทางปฏิบัติกรอบการทำงานด้านความมั่นคงปลอดภัยไซเบอร์บนมาตรฐานเอ็นไอเอสที (NIST) ซึ่งเป็นกรอบการทำงานที่ได้รับการยอมรับอย่างแพร่หลายในปัจจุบัน สำหรับการบริหารจัดการและลดความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ กระบวนการวิธีครอบคลุมดังนี้

1) ศึกษาแนวทางปฏิบัติที่ดีและมาตรฐานในการป้องกันจากมัลแวร์เรียกค่าไถ่

(1) งานวิจัยก่อนหน้า “กรณีศึกษาจากเหตุการณ์ที่เกิดขึ้นจริง”

(2) สถาบันมาตรฐานและเทคโนโลยีแห่งชาติ กระทรวงพาณิชย์ของสหรัฐอเมริกาเอ็นไอเอสที

(3) งานวิจัยที่เกี่ยวกับระบบควบคุมอุตสาหกรรม และเอ็นไอเอสที

2) การประชุมกลุ่มเป้าหมายที่กำหนด (Focus Group) โดยใช้แนวทางปฏิบัติของเอ็นไอเอสที

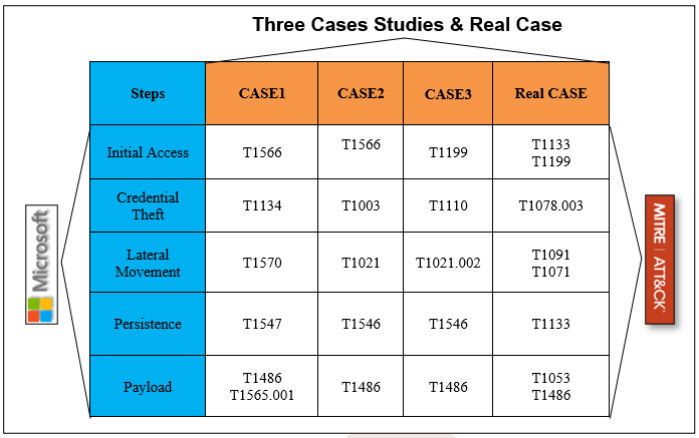
3) ผลจากการสนทนากลุ่ม

4) สรุปผลการวิจัย

ทบทวนวรรณกรรมที่เกี่ยวข้อง

1) งานวิจัยก่อนหน้า (Previous Article) “กรณีศึกษาจากเหตุการณ์ที่เกิดขึ้นจริง”

Nakhonthai & Chimmanee (2022, pp. 416-421) ได้นำเสนอบทความการวิเคราะห์ทางนิติวิทยาศาสตร์ดิจิทัลจากกรณีศึกษาการโจมตีที่เกิดขึ้นจริงจากมัลแวร์เรียกค่าไถ่คริปโทล็อกเกอร์ (CryptoLocker) ซึ่งประกอบด้วย 3 กรณีศึกษา โดยเป็นการวิจัยเชิงเอกสาร (Research Document) และ 1 กรณีศึกษาที่เกิดขึ้นจากเหตุการณ์จริง ซึ่งในทุกกรณีได้ใช้การวิเคราะห์ และเปรียบเทียบด้วยกรอบการโจมตีด้วยกรอบแนวคิดของไมโครซอฟต์ (Microsoft Framework) (Microsoft Threat Intelligence, 2020) เนื่องจากในโรงงานร้อยละ 95 ใช้ระบบปฏิบัติการเป็นไมโครซอฟต์ วินโดว์ (Microsoft Windows) และกรอบแนวคิดของไมเตอร์แอทแทค (MITER ATT&CK Framework) เพื่อระบุและติดตามภัยคุกคามทางไซเบอร์ (Rajesh et al., 2022, pp. 4-12) บทความยังให้รายละเอียดของกรณีจริง และไทม์ไลน์ทางนิติวิทยาศาสตร์ดิจิทัลแก่เจ้าหน้าที่ดูแลระบบเครือข่าย และสถาปนิกด้านความมั่นคงปลอดภัยทางไซเบอร์เพื่อเพิ่มประสบการณ์ โดยสรุปผลการวิเคราะห์ขั้นตอนการโจมตีจากกรณีศึกษาทั้งหมดในภาพที่ 2 โดยในตารางคอลัมน์ที่ 1 คือ เทคนิคการโจมตี 5 ขั้นตอนของกรอบแนวคิดของไมโครซอฟต์ คอลัมน์ที่ 2-4 เป็นกรณีศึกษาที่เกิดขึ้นจริง และคอลัมน์ที่ 5 เป็นการโจมตีที่เกิดขึ้นจริง เช่นการเข้าถึงครั้งแรก (Initial Access) ด้วยเทคนิค (Techniques) T1133 ซึ่งคือ การเข้าถึงและควบคุมคอมพิวเตอร์ภายในระบบควบคุมอุตสาหกรรมจากระยะไกลผ่านบริการที่เปิดให้เข้าถึงจากภายนอก และเทคนิค T1199 ซึ่งหมายถึง บุคคลที่สามที่เชื่อถือได้ ซึ่งอาจเป็นคู่ค้า หรือผู้ให้บริการ ขั้นตอนในลำดับถัดมาการเคลื่อนที่ภายในเครือข่าย (Lateral movement) ได้ใช้เทคนิค T1091 ซึ่งคือ การแพร่กระจายมัลแวร์ผ่านยูเอสบีแฟลชไดรฟ์ (USB Flash Drive) และได้ใช้เทคนิค T1071 ซึ่งคือ การใช้โพรโทคอลชั้นแอปพลิเคชัน (Application) การถ่ายโอนไฟล์ด้วยโพรโทคอล (Protocol) เอสเอ็มบี (SMB) เป็นต้น ประโยชน์ของงานวิจัยก่อนหน้านี้ คือ ได้รวบรวมข้อมูลขั้นตอนการโจมตีและวิเคราะห์ด้วยกรอบแนวคิดของไมโครซอฟต์ และใช้หมายเลขเทคนิคของไมเตอร์แอทแทคเพื่อเป็นกรณีศึกษาให้เจ้าหน้าที่ดูแลระบบเครือข่าย (Network Administrator) และสถาปนิกด้านความมั่นคงปลอดภัยทางไซเบอร์ (Security Architect) สำหรับใช้เพื่อเข้าใจขั้นตอนการโจมตี



Steps	CASE1	CASE2	CASE3	Real CASE
Initial Access	T1566	T1566	T1199	T1133 T1199
Credential Theft	T1134	T1003	T1110	T1078.003
Lateral Movement	T1570	T1021	T1021.002	T1091 T1071
Persistence	T1547	T1546	T1546	T1133
Payload	T1486 T1565.001	T1486	T1486	T1053 T1486

ภาพที่ 2 ขั้นตอนเจาะระบบของคริปโทล็อกเกอร์ จากกรอบแนวคิดของไมโครซอฟต์และไมเตอร์แอทแทค

จากภาพที่ 2 การโจมตีที่เกิดขึ้นจริงจากมัลแวร์เรียกค่าไถ่คริปโทล็อกเกอร์ (CryptoLocker) (Real Case) ดังนั้นแผนเผชิญเหตุ และการป้องกันจึงอยู่ในขั้นตอนต่อไป ซึ่งนำเสนอแนวทางการป้องกันภัยจากมัลแวร์เรียกค่าไถ่ที่เหมาะสมของระบบควบคุมในโรงงานอุตสาหกรรม จากแนวทางของเอ็นไอเอสที

2) สถาบันมาตรฐานและเทคโนโลยีแห่งชาติ กระทรวงพาณิชย์ของสหรัฐอเมริกา (NIST)

เอ็นไอเอสที (NIST) ในปี ค.ศ 2018 ได้นำเสนอเฟรมเวิร์ก กรอบการพัฒนาระบบความมั่นคงปลอดภัยโครงสร้างพื้นฐานสำคัญ (Framework for Improving Critical Infrastructure Cybersecurity) หรือซีเอฟเอส (CSF) ซึ่งเป็นการกำหนดแนวทางการจัดการความเสี่ยงด้านความปลอดภัยไซเบอร์ เพื่อยกระดับความมั่นคงปลอดภัยขององค์กรทั่วไป รวมไปถึงช่วยให้องค์กรสามารถวางแผน ป้องกัน ตรวจจับและตอบสนองต่อภัยคุกคามได้อย่างรวดเร็วและเป็นระบบ ถัดมาในปี ค.ศ. 2021 เอ็นไอเอสที ได้นำเสนอเวอร์ชัน (Version) ของเอ็นไอเอสทีไออาร์ แปดสามเจ็ดสี่ฉบับร่าง (Draft NISTIR 8374: Cybersecurity Framework Profile for Ransomware Risk Management) ซึ่งเป็นเฟรมเวิร์กที่มุ่งเน้นไปสำหรับมัลแวร์เรียกค่าไถ่โดยเฉพาะและได้ให้คำแนะนำในเบื้องต้นสำหรับสนับสนุนการป้องกัน ตอบสนอง และกู้คืน จากเหตุการณ์มัลแวร์เรียกค่าไถ่ (Chimmanee & Chotrungrat, 2021, pp. 104-118) ล่าสุดเพื่อรับมือต่อสถานการณ์ปัจจุบันเอ็นไอเอสทีได้นำเสนอเฟรมเวิร์กแนวทางปฏิบัติ (Guideline) ฉบับล่าสุดเอ็นไอเอสที เวอร์ชัน SP 800-82 Rev.3 การรักษาความปลอดภัยของระบบเทคโนโลยีการดำเนินงาน (OT) ให้ครอบคลุมการรักษาความปลอดภัยในภาคอุตสาหกรรม ได้ออกคู่มือการรักษาความปลอดภัยเทคโนโลยีการปฏิบัติงานนำเสนอล่าสุดในเดือนกันยายน ปี ค.ศ. 2023 สำหรับแนวทางปฏิบัติในการออกแบบ และวางกลยุทธ์ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ แบ่งเป็น 5 ฟังก์ชันหลัก แต่ละฟังก์ชันหลักจะแบ่งออกเป็นฟังก์ชันย่อยเพื่อนำกระบวนตอบสนองต่อเหตุการณ์โจมตีจากมัลแวร์เรียกค่าไถ่ (Stouffer et al., 2023, pp.90-138)

3) งานวิจัยที่เกี่ยวกับระบบควบคุมอุตสาหกรรม (ICS)

ในหัวข้อนี้จะกล่าวถึงสามงานวิจัยที่เกี่ยวข้องกับระบบควบคุมอุตสาหกรรม (ICS) จากภัยคุกคามไซเบอร์ (Cyber Threats) ที่เกิดจากมัลแวร์เรียกค่าไถ่ และการนำเสนอแนวทางการป้องกันภัยจากมัลแวร์เรียกค่าไถ่ ในงานวิจัยของ You et al. (2018, pp. 1-6) ได้กล่าวถึงการบริหารจัดการควบคุมความปลอดภัยความมั่นคงปลอดภัยทางไซเบอร์สำหรับระบบควบคุมอุตสาหกรรมมีหลายมาตรฐาน โดยงานวิจัยได้วิเคราะห์

สถานการณ์ของระบบควบคุมอุตสาหกรรมที่ใช้ในโครงสร้างพื้นฐาน และนำเสนอแนวทางปฏิบัติ โดยได้เปรียบเทียบพร้อมวิเคราะห์ในแต่ละมาตรฐานโดยใช้เมทริกซ์ (Matrix) ซึ่งหนึ่งในมาตรฐานเป็นกรอบแนวทางของเอ็นไอเอสที เวอร์ชัน (Version) SP 800-53 ซึ่งเป็นหนึ่งมาตรฐานเพื่อใช้สำหรับการจัดการป้องกันความปลอดภัยของข้อมูล โดยมีขอบเขตการดำเนินงานดังนี้ 1) ในส่วนการสื่อสารระหว่างมนุษย์และเครื่องจักร (Human-Machine Interface: HMI) คือฮาร์ดแวร์ หรือซอฟต์แวร์ ที่ผู้ปฏิบัติงานทำงานของระบบควบคุมอุตสาหกรรม 2) ในส่วนอุปกรณ์ควบคุม (Controller) คืออุปกรณ์ หรือโปรแกรมที่ทำหน้าที่เป็นศูนย์ควบคุมกระบวนการ 3) ในส่วนสั่งการ (Actuator) คืออุปกรณ์ที่ควบคุมกระบวนการโดยตรงตามคำสั่งของอุปกรณ์ควบคุม และ 4) ในเซ็นเซอร์ (Sensor) คืออุปกรณ์ที่วัดปริมาณทางกายภาพและแปลงเป็นสัญญาณ เพื่อจัดการรักษาความปลอดภัย ผลการวิจัยนำไปใช้เป็นตัวชี้วัดที่มีประสิทธิภาพในการเลือกใช้มาตรฐานที่เหมาะสมเพื่อเป็นแนวทางของการเพิ่มระดับการป้องกันที่เหมาะสมนำไปใช้กับระบบควบคุมอุตสาหกรรมได้

ในงานวิจัยของ AlMedires & AlMaiah (2021, pp. 640-647) ได้กล่าวถึงภาพรวมของความปลอดภัยของระบบควบคุมอุตสาหกรรม โดยเน้นที่ระบบควบคุม การออกแบบระบบการป้องกันให้มีความน่าเชื่อถือและปลอดภัย โดยโปรแกรมที่ใช้ควบคุมการทำงานของฮาร์ดแวร์ในระบบควบคุมดูแลประมวลผลข้อมูลและบันทึกข้อมูล เช่น ระบบควบคุมดูแลและเก็บข้อมูล (SCADA) ระบบควบคุมแบบกระจาย (DCS) และส่วนต่อประสานระหว่างมนุษย์กับเครื่องจักร (HMI) เป็นต้น เหล่านี้มีความซับซ้อนสูง ประกอบด้วยอุปกรณ์และซอฟต์แวร์จำนวนมากจากผู้ขายในการเชื่อมต่อในระบบเครือข่าย เพื่อการส่งผ่านข้อมูลจากเครื่องสู่เครื่อง การรักษาและป้องกันด้านความมั่นคงปลอดภัยทางไซเบอร์ ซึ่งเป็นเครื่องมือสำคัญนำไปสู่การพัฒนาระบบควบคุมอุตสาหกรรม งานวิจัยได้ให้คำอธิบายเกี่ยวกับพัฒนาการในการรักษาความปลอดภัยระบบควบคุมอุตสาหกรรมที่ครอบคลุมพร้อมได้ระบุฟังก์ชันเฉพาะของระบบรักษาความปลอดภัยไซเบอร์ที่มีความสำคัญต่อโครงสร้างพื้นฐานระบบควบคุมอุตสาหกรรม ได้ให้ประเด็นสำคัญในการผสมผสานระหว่างสามส่วน เทคโนโลยีสารสนเทศ (IT) และเทคโนโลยีปฏิบัติการ (OT) และระบบควบคุมอุตสาหกรรม (ICS)

งานวิจัยของ Wiboonrat (2022, pp. 1-6) ศึกษาความมั่นคงปลอดภัยทางไซเบอร์ในระบบควบคุมอุตสาหกรรม โดยเน้นที่การผสมผสานระหว่าง เทคโนโลยีสารสนเทศ เทคโนโลยีเชิงปฏิบัติการ และระบบควบคุม ได้กล่าวถึงระบบควบคุมอุตสาหกรรม ซึ่งประกอบด้วยระบบควบคุมกระบวนการ (PCS) ระบบควบคุมแบบกระจาย และระบบควบคุมดูแลและบันทึกข้อมูล มีความเสี่ยงสูงต่อการถูกโจมตี ซึ่งสามารถเกิดขึ้นได้พร้อมกันในหลายระบบ ซึ่งอาจส่งผลกระทบต่อการดำเนินงานของอุตสาหกรรม เพื่อป้องกันภัยคุกคามดังกล่าว ได้นำเสนอมาตรฐานที่เป็นที่ยอมรับมาใช้เป็นแนวทางปฏิบัติ ได้แก่ มาตรฐานเอ็นไอเอสที (NIST) เวอร์ชัน (Version) SP 800-61r2 และ SP 800-82r2 กำหนดแนวทางปฏิบัติที่เหมาะสมสำหรับการบริหารจัดการความเชื่อมโยงระหว่างระบบด้วย (Purdue Enterprise Reference Architecture: PERA) ใช้เป็นแนวคิดในการแบ่งส่วนเครือข่าย (Network Segmentation) ในระบบควบคุมอุตสาหกรรม ซึ่งเป็นแนวทางสำคัญในการปกป้องและจำกัดการแพร่กระจายของภัยคุกคามทางไซเบอร์ โดยเน้นการศึกษาจุดอ่อนด้านความปลอดภัยหลัก 4 ประเภท ได้แก่ จุดอ่อนของเครือข่าย ระบบปฏิบัติการ บุคลากร และกระบวนการ

4) งานวิจัยที่เกี่ยวกับเอ็นไอเอสที (NIST)

ในหัวข้อนี้จะกล่าวถึงงานวิจัยที่กับเอ็นไอเอสที (NIST) หลายงานวิจัยชี้ให้เห็นว่าเอ็นไอเอสที เป็นกรอบการทำงานที่มีประสิทธิภาพสำหรับการจัดการและลดความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ องค์กรที่ใช้แนวทางปฏิบัตินี้สามารถลดความเสี่ยงต่อข้อมูล สินทรัพย์ และปรับปรุงการป้องกันด้านความปลอดภัยเพื่อเพิ่มความมั่นใจของลูกค้าและพันธมิตร และตอบสนองต่อข้อกำหนดทางกฎหมาย ในงานวิจัยของ Udroiu et al. (2022, pp. 1-7) ได้กล่าวถึงเอ็นไอเอสที เป็นแนวทางการรักษาความปลอดภัยไซเบอร์สำหรับระบบควบคุมอุตสาหกรรม เป็นเฟรมเวิร์ก (Framework) ที่อิงตามการวิเคราะห์ความเสี่ยงและการรักษา สร้างขึ้นจากมาตรฐาน คำแนะนำ แนวทางปฏิบัติที่ดีที่สุด โดยแนวทางการใช้งานในระบบควบคุมอุตสาหกรรมที่ใช้กันทั่วไปสามารถปรับใช้เพื่อประเมินความพร้อมปรับปรุงความปลอดภัยขององค์กร พร้อมให้คำแนะนำในแต่ละขั้นตอนด้านการดูแลความมั่นคงปลอดภัยทางไซเบอร์ที่เป็นมาตรฐาน เพื่อให้แน่ใจว่าการรักษาความปลอดภัยทางไซเบอร์ในภาคส่วนสำคัญได้ครอบคลุม และแนวปฏิบัติที่ดีที่สุดไว้อย่างหลากหลาย

งานวิจัยของ Goodwin (2022, pp. 89-95) ได้กล่าวถึงสถาบันมาตรฐานและเทคโนโลยีแห่งชาติ เอ็นไอเอสที ได้เผยแพร่กรอบงานสำหรับการปรับปรุงความปลอดภัยโครงสร้างพื้นฐานที่สำคัญทางความมั่นคงปลอดภัยไซเบอร์ของปี ค.ศ. 2014 ตามด้วยเวอร์ชันที่อัปเดตในปี ค.ศ. 2017 และอย่างต่อเนื่องจนถึงปี ค.ศ. 2022 กรอบงานดังกล่าวได้รับการพัฒนาขึ้นจากความร่วมมือระหว่างรัฐบาลกลางของสหรัฐอเมริกาและภาคเอกชน ทำหน้าที่เป็นแนวทางเท่านั้นซึ่งไม่ได้รับคำสั่งจากผู้มีอำนาจทางกฎหมายใด ๆ ปัจจุบัน การยอมรับกรอบงานเป็นไปด้วยความสมัครใจ กรอบความมั่นคงปลอดภัยทางไซเบอร์ของเอ็นไอเอสที ได้รับการพิสูจน์แล้วว่าประสบความสำเร็จในการป้องกันเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ตามที่กำหนด การนำกรอบการทำงานเอ็นไอเอสทีไปใช้ในกรณีศึกษาหลายกรณี ซึ่งได้พิสูจน์แล้วว่าสามารถบรรเทาหรือลดผลกระทบด้านความเสี่ยงไซเบอร์ รวมถึงเสริมสร้างโครงสร้างพื้นฐานด้านความปลอดภัยไซเบอร์ขององค์กรได้ ในงานวิจัยของ Stouffer et al. (2023) ได้กล่าวถึงเอ็นไอเอสที เวอร์ชัน (Version) ล่าสุด (SP 800-82 Rev. 3) ซึ่งเป็นเฟรมเวิร์ก มุ่งเน้นไปที่การแนะนำแนวทางปฏิบัติสำหรับการรักษาความปลอดภัยเทคโนโลยีเชิงปฏิบัติการ (OT) เฟรมเวิร์กนี้อธิบายถึงวิธีการรักษาความปลอดภัยเทคโนโลยีเชิงปฏิบัติการ โดยพิจารณาข้อกำหนดด้านประสิทธิภาพ ความน่าเชื่อถือ และความปลอดภัยที่เหมาะสม เฟรมเวิร์กได้ครอบคลุมระบบและอุปกรณ์ที่ติดตั้งโปรแกรมได้หลากหลาย ซึ่งสื่อสารระหว่างกันในสภาพแวดล้อมเชิงปฏิบัติการ และได้กล่าวถึงเพอร์ดูโมเดล (Purdue Model) เป็นแนวทางจัดหมวดหมู่และกำหนดระดับการป้องกันของระบบควบคุมอุตสาหกรรมที่มีความซับซ้อน (Stouffer et al., 2023, pp. 71-75) ซึ่งทำให้เจ้าหน้าที่ดูแลระบบสารสนเทศสามารถทำความเข้าใจและป้องกันอุปสรรคทางความปลอดภัยได้อย่างเหมาะสม

ระเบียบวิธีวิจัย

การศึกษาวิจัยในครั้งนี้เป็นงานวิจัยเชิงคุณภาพเพื่อหาแนวทางป้องกันมัลแวร์เรียกค่าไถ่ตลอดจนข้อปฏิบัติในการรับมือการโจมตีจากมัลแวร์เรียกค่าไถ่ภายในระบบควบคุมในโรงงานอุตสาหกรรม มีแนวทางการคัดเลือกผู้เข้าร่วมการสนทนากลุ่ม คือ ต้องสำเร็จการศึกษาในระดับปริญญาตรีขึ้นไป และมีประสบการณ์ใน

ด้านการรักษาความมั่นคงปลอดภัยอย่างน้อย 1 ปี มีผู้เข้าร่วมการสนทนากลุ่มทั้งหมดจำนวน 44 คน แบ่งออกเป็น 2 กลุ่ม ได้แก่

(1) ตัวแทนจำหน่ายผลิตภัณฑ์ด้านไอทีหรือผู้ติดตั้งระบบ มีจำนวน 13 คน

(2) ผู้ดูแลระบบหรือภาคการศึกษา มีจำนวน 31 คน

1) แนวคำถาม

ถามความเห็นและข้อแนะนำเกี่ยวกับแนวทางการปฏิบัติการ และการบริหารจัดการ เพื่อการรักษาความมั่นคงปลอดภัยจากมัลแวร์เรียกค่าไถ่ และการป้องกันโจมตี แบ่งออกเป็น 5 คำถามตามขั้นตอนของเอ็นไอเอสที (NIST) ได้แก่

(1) การกำหนดมาตรการความมั่นคงปลอดภัยไซเบอร์ (Identify)

(2) การปกป้องดูแลทรัพย์สินสารสนเทศ (Protect)

(3) ความสามารถในการตรวจพบเหตุภัยคุมคามไซเบอร์ (Detect)

(4) การรับมือภัยคุกคาม (Respond)

(5) การกู้คืนข้อมูล และ ระบบหลังเหตุภัยคุกคามไซเบอร์ (Recover)

2) การเก็บรวบรวมข้อมูล

ในการศึกษาวิจัยในครั้งนี้ได้จัดเก็บข้อมูลในการสนทนากลุ่มด้วยกูเกิลฟอร์ม (Google Form) และบันทึกวิดีโอในส่วนสำคัญ เพื่อได้ข้อมูลครบถ้วนพร้อมความคิดเห็นและข้อเสนอแนะเฉพาะจากมุมมองที่หลากหลายในส่วนของระบบควบในโรงงานอุตสาหกรรม (ICS) ตามแนวทางปฏิบัติของเอ็นไอเอสที (NIST) ทั้ง 5 ส่วน เพื่อนำมาทำการวิเคราะห์ข้อมูลและสรุปผลเป็นตาราง

3) การวิเคราะห์ข้อมูล

เมื่อได้ข้อสรุปจากการประชุมทางวิชาการกลุ่มเป้าหมายที่กำหนดหรือสนทนากลุ่ม พร้อมทั้งได้ข้อมูลความคิดเห็นและการตอบข้อคำถามจากผู้เข้าร่วมสนทนากลุ่มผ่านกูเกิลฟอร์ม ซึ่งได้ข้อมูลครบถ้วน จากมุมมองที่หลากหลายของผู้เชี่ยวชาญ เพื่อนำไปวิเคราะห์หาแนวทางการป้องกัน

ผลการวิจัย

คุณสมบัติและความเชี่ยวชาญของผู้เข้าร่วมการสนทนากลุ่มทั้งหมด 44 คน ได้แสดงดังตารางที่ 1

ตารางที่ 1 แสดงข้อมูลผู้มีประสบการณ์เชี่ยวชาญเข้าร่วมสนทนากลุ่ม

ผู้มีประสบการณ์เชี่ยวชาญ (P=44)	ระดับการศึกษาปริญญา			ผู้มีประสบการณ์เชี่ยวชาญในส่วน		ใบรับรองความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity Certifications)	
	ตรี	โท	เอก	กลุ่ม 1	กลุ่ม 2		
P1-P3	-	-	3	-	3	3	CompTIA Security+ (Plus), ECSS, PECB DPO, CCDP, and CEH

ผู้มีประสบการณ์เชี่ยวชาญ (P=44)	ระดับการศึกษาปริญญา			ผู้มีประสบการณ์เชี่ยวชาญในส่วน		ใบรับรองความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity Certifications)	
	ตรี	โท	เอก	กลุ่ม 1	กลุ่ม 2		
P4-P18	-	15	-	5	10	9	AZ-500, AZ-900, SC-200, SC-300, SC-400, SC-900, DP-900, AI-900, CompTIA Security+ (Plus), AZ-104, CISSP, and CEHv11
P19-P44	26	-	-	8	18	14	VCP, CHFI, CompTIA Security+ (Plus), CompTIA Pen Test+, EICSS, ACE, ISC, PEN Test+, CCNA CEH, CASP, CHFI, and ECSS

จากการสนทนากลุ่มผู้วิจัยได้เก็บรวบรวมข้อมูลมาทำการการวิเคราะห์ข้อมูลแบบเชิงคุณภาพจากหลักการแนวทางปฏิบัติของเอ็นไอเอสที (NIST) ทั้ง 5 ส่วน โดยได้ข้อสรุปเนื้อหาในแต่ละขั้นตอนแนวการป้องกันภัยจากมัลแวร์เรียกค่าไถ่ภัยในระบบควบคุมอุตสาหกรรมเป็นตาราง ดังนี้

ตารางที่ 2 สรุปการสนทนากลุ่ม (Focus Group) โดยใช้แนวทางปฏิบัติของเอ็นไอเอสที (NIST)

สรุปการสนทนากลุ่ม (Focus Group) โดยใช้แนวทางปฏิบัติของเอ็นไอเอสที (NIST)	
แนวคำถามสนทนากลุ่ม	**สรุปข้อมูลจากการสนทนากลุ่ม**
1) การระบุความเสี่ยงที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สิน และชีวิตร่างกายของบุคคล (Identify) 1.1 การบริหารจัดการทรัพย์สิน (Asset Management: AM) 1.2 การดำเนินการตรวจสอบสภาพแวดล้อม (Business Environment: BE) 1.3 การกำกับดูแล (Governance: GV) 1.4 การตรวจสอบและประเมินความเสี่ยงด้านเครือข่าย (Risk Assessment: RA)	1. ต้องมีการจัดการระบบทะเบียนทรัพย์สิน (Inventory) ในส่วนเทคโนโลยีสารสนเทศ (IT) เทคโนโลยีเชิงปฏิบัติการ (OT) และระบบควบคุมอุตสาหกรรม (ICS) ที่ระบุทรัพย์สินของบริการที่สำคัญ ควรมีการตรวจสอบทะเบียนทรัพย์สิน และต้องประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ 1 ครั้ง 2. ระบุความเสี่ยงที่อาจจะเกิดขึ้นในแต่ละโซน เช่น ส่วนไอที (IT) ส่วนออฟฟิศ (Office) เทคโนโลยีเชิงปฏิบัติการ และระบบควบคุมอุตสาหกรรม ได้แก่ เครือข่าย (Network) เซิร์ฟเวอร์ (Server) เดสก์ท็อป (Desktop) แล็ปท็อป (Laptop) อุปกรณ์ในเทคโนโลยีเชิงปฏิบัติการ ร่วมถึงผู้ใช้งานภายในและภายนอก 3. มีการประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing) ตัวอย่าง เช่น เครื่องมือชื่อว่าอัปการ์ด (Up-Guard) ในการสแกนตรวจจับช่องโหว่ พร้อมแนะนำแนวทางการแก้ไขที่ละขั้นตอน 4. มีการจัดการผู้ให้บริการภายนอก (Third Party Management) รวมถึงการนำอุปกรณ์ต่าง ๆ ที่นำเข้าถึงในแต่ละโซนภายในบริษัท และส่วนเทคโนโลยีเชิงปฏิบัติการ และระบบควบคุมอุตสาหกรรม พร้อมบันทึกเหตุการณ์ไว้ทั้งหมด 5. การจัดการการเข้าถึงที่ปลอดภัยจากภายนอกทั้งภายในไอทีโซน ออฟฟิศโซน และโอทีโซน เช่น การเชื่อมต่อคอมพิวเตอร์ระบบเครือข่ายแบบแลน (LAN) หรือวายฟาย (Wi-Fi) การเข้าถึงอินเทอร์เน็ต (Internet) แอปพลิเคชัน (Application) อีเมล (Email) ยูเอสบีแฟลชไดรฟ์ (USB Flash Drive) บลูทูธ (Bluetooth) เครือข่ายเสมือนส่วนตัววีพีเอ็น (Virtual Private Network: VPN) และผู้ให้บริการภายนอกมีข้อตกลงระดับการให้บริการ (Service Level Agreement) หรือเงื่อนไขของสัญญากับผู้ให้บริการภายนอกให้ปฏิบัติตามสัญญาอย่างเคร่งครัด 6. การบริหารจัดการ (Governance) การกำหนดนโยบาย (Policy Setting) การกำหนดนโยบายที่ชัดเจน และเหมาะสมสำหรับองค์กร ข้อเสนอแนะการป้องกันภัยจากมัลแวร์เรียกค่าไถ่

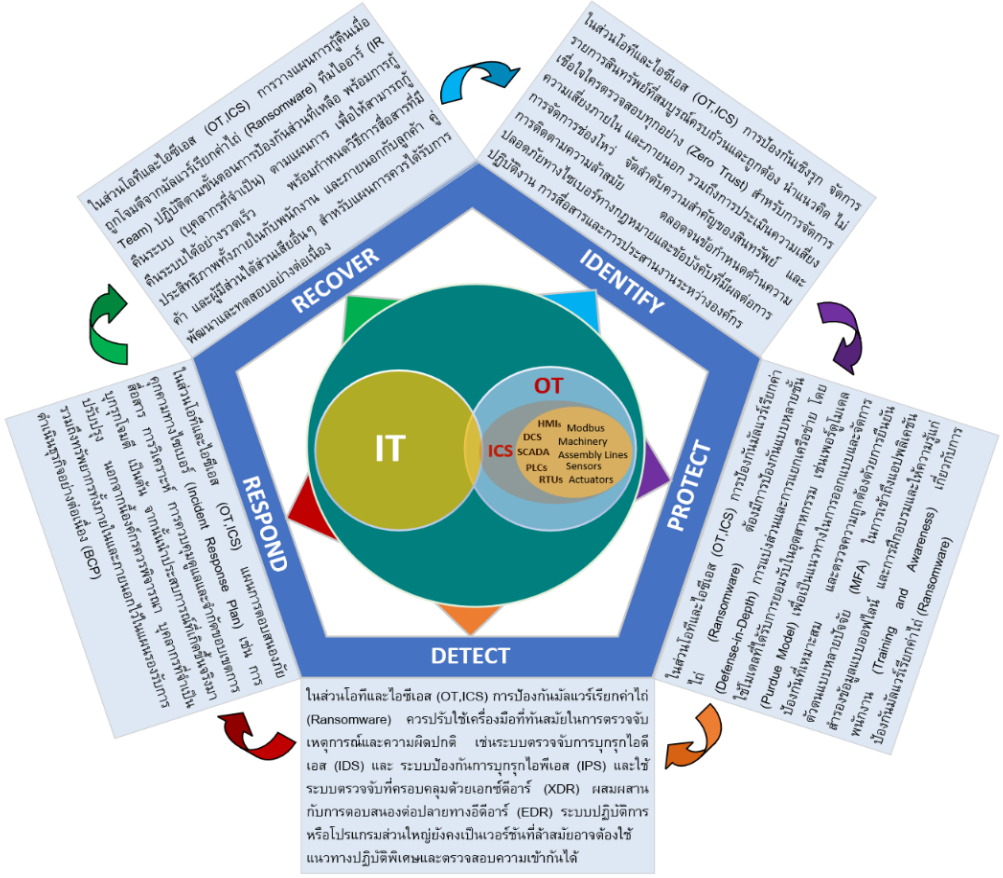
สรุปการสนทนากลุ่ม (Focus Group) โดยใช้แนวทางปฏิบัติของเอ็นไอเอสที (NIST)	
แนวคำถามสนทนากลุ่ม	**สรุปข้อมูลจากการสนทนากลุ่ม**
1.5 การกำหนดกลยุทธ์บริหารจัดการความเสี่ยง (Risk Management Strategy: RM) 1.6 การบริหารจัดการความเสี่ยงห่วงโซ่อุปทาน (Supply Chain Risk Management: SC)	สำหรับระบบควบคุมอุตสาหกรรม (ICS) จากกรณีการโจมตีที่เกิดขึ้นจริงจากมัลแวร์เรียกค่าไถ่คริปโทล็อกเกอร์ (CryptoLocker) องค์กรได้พิจารณาถึงความสำคัญของรายการสินทรัพย์ให้สมบูรณ์ครบถ้วนและถูกต้องสำหรับการจัดการความเสี่ยงภายในสภาพแวดล้อมในส่วนเทคโนโลยีเชิงปฏิบัติการ และระบบควบคุมอุตสาหกรรม การป้องกันเชิงรุก รวมถึงนำแนวคิดไม่เชื่อใจใครตรวจสอบทุกอย่าง (Zero Trust) ในการประเมินความเสี่ยง การจัดการช่องโหว่ และการติดตามความล้าสมัย และเพิ่มในเนื้อหาการฝึกอบรมบุคลากรประจำไตรมาส ในส่วนไอทีตลอดจนข้อกำหนดด้านความปลอดภัยไซเบอร์ทางกฎหมาย และข้อบังคับที่มีผลต่อการปฏิบัติงาน เช่น จากเหตุการโจมตีของมัลแวร์เรียกค่าไถ่คริปโทล็อกเกอร์ (CryptoLocker) เพื่อลดความเสี่ยงการเกิดซ้ำ ได้ออกข้อบังคับอย่างเคร่งครัดในการใช้ยูเอสบีแฟลชไดรฟ์ (USB Flash Drive) และเพิ่มนโยบายป้องกันความเสี่ยงในขั้นตอนปฏิบัติงานอย่างเคร่งครัด พร้อมตรวจสอบความปลอดภัยในการนำเครื่องจักรเข้าออกภายในระบบควบคุมอุตสาหกรรม
2. มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect) 2.1 กำหนดมาตรการควบคุมการเข้าถึง (Access Control: AC) 2.2 การสร้างความตระหนักและการฝึกอบรม (Awareness and Training: AT) 2.3 การกำหนดความมั่นคงปลอดภัยของข้อมูล (Data Security: DS) 2.4 กระบวนการบำรุงรักษา (Maintenance: MA) 2.5 จัดหาเทคโนโลยีการป้องกัน (Protective Technology: PT)	1. การควบคุมการเข้าถึงองค์กรต้องจัดหาระบบสำหรับป้องกันและการรักษาความมั่นคงปลอดภัยเพื่อเพิ่มประสิทธิภาพในการจัดการความมั่นคงปลอดภัย ต้องมีการเก็บรักษาบันทึกเหตุการ์ของการเข้าถึงทั้งหมด 2. การสร้างความตระหนักผ่านข่าวสาร และการฝึกอบรม การจำลองเหตุการณ์เสมือนถูกโจมตีด้วยเทคนิคต่าง ๆ ไซเบอร์เอ็กเซอร์ไซส์ (Cyber Exercise) สำหรับเจ้าหน้าที่ไอที ไซเบอร์ดริล (Cyber Drill) สำหรับเจ้าหน้าที่ปฏิบัติการในออฟฟิศ และในส่วนของเทคโนโลยีเชิงปฏิบัติการและระบบควบคุมอุตสาหกรรม อย่างน้อยปีละ 1 ครั้ง 3. การกำหนดความมั่นคงปลอดภัยของข้อมูล มีการจัดการสำรองข้อมูล สาม-สอง-หนึ่ง รวมถึงสำรองข้อมูลอุปกรณ์ในส่วนของเทคโนโลยีเชิงปฏิบัติการ และระบบควบคุมอุตสาหกรรม จัดทำกระบวนการจัดการเปลี่ยนแปลง (Change Management Process) เพื่ออนุญาตและตรวจสอบความถูกต้องของการเปลี่ยนแปลงระบบไอทีทั้งหมด 4. การบำรุงรักษา การปรับปรุงซอฟต์แวร์ และการอัปเดตความปลอดภัยปิดช่องโหว่ที่เกิดขึ้นทันที 5. จัดหาเทคโนโลยีการป้องกันที่ทันสมัยอย่าง เช่น การเข้ารหัสข้อมูล (Data Encryption) ระบบตรวจจับและป้องกันการบุกรุก (Intrusion Detection and Prevention Systems: IDPS) ไฟร์วอลล์รักษาความปลอดภัยที่ช่วยปกป้องเว็บแอปพลิเคชัน (Web Application) จากการโจมตีทางไซเบอร์ (Web Application Firewall: WAF) ระบบจัดการข้อมูลและเหตุการณ์ความปลอดภัย ตรวจจับ วิเคราะห์ และตอบสนองต่อภัยคุกคามด้านความปลอดภัยได้อย่างมีประสิทธิภาพ (Security Information and Event Management: SIEM) ระบบป้องกันการสูญหายของข้อมูล (Data Loss Prevention: DLP), และการปกป้องอุปกรณ์ปลายทาง (Endpoint Detection and Response: EDR) ข้อเสนอแนะการป้องกันภัยจากมัลแวร์เรียกค่าไถ่ (Ransomware) สำหรับระบบควบคุมอุตสาหกรรม (ICS) การออกแบบสถาปัตยกรรมระบบโดยมีการป้องกันในเชิงลึกได้แบ่งออกเป็น 5 ชั้นดังนี้ 1) การจัดการความปลอดภัย (Security Management) 2) ความปลอดภัยทางกายภาพ (Physical Security) 3) ความปลอดภัยเครือข่าย (Network Security) 4) ความปลอดภัยของฮาร์ดแวร์ (Hardware Security) 5) ความปลอดภัยของซอฟต์แวร์ (Software Security) ในการป้องกันในเชิงลึกชั้นที่ 3 ความปลอดภัยเครือข่าย (Network Security) องค์กรอาจพิจารณา การแบ่งส่วนและการแยกเครือข่ายในด้านความปลอดภัยเครือข่าย เช่น เพอร์ดูโมเดล (Purdue Model) เพื่อเป็นแนวทางในกระบวนการออกแบบและจัดการป้องกันที่เหมาะสม สามารถช่วยป้องกันและลดความเสี่ยงจากการโจมตี ตรวจจับการเข้าถึงที่ผิดปกติด้วยระบบการยืนยันตัวตนแบบหลายปัจจัย (Multi-

สรุปการสนทนากลุ่ม (Focus Group) โดยใช้แนวทางปฏิบัติของเอ็นไอเอสที (NIST)	
แนวคำถามสนทนากลุ่ม	**สรุปข้อมูลจากการสนทนากลุ่ม**
	Factor and Password Authentication: MFA) ในการเข้าถึงแอปพลิเคชัน (Application) ส่วนเทคโนโลยีเชิงปฏิบัติการ (OT) และระบบควบคุมอุตสาหกรรม (ICS) พร้อมป้องกันการสูญเสียข้อมูลด้วยการสำรองข้อมูลแบบออฟไลน์ตามหลักการสาม-สอง-หนึ่ง 3-2-1
3. มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect) 3.1 การตรวจจับเหตุการณ์ และความผิดปกติ (Anomalies and Events: AE) 3.2 การตรวจสอบด้านความมั่นคงปลอดภัยอย่างต่อเนื่อง (Security Continuous Monitoring: CM) 3.3 กระบวนการตรวจจับ (Detection Processes: DP)	1. การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring) ต้องสร้างกลไกและกระบวนการเพื่อตรวจจับเหตุการณ์ การจัดประเภทและวิเคราะห์เหตุการณ์ การระบุว่ามีภัยคุกคามทางไซเบอร์ หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ทั้งหมด 2. การตรวจสอบด้านความมั่นคงปลอดภัยต้องดำเนินการทบทวนกลไกและกระบวนการอย่างน้อยปีละ 1 ครั้ง 3. กระบวนการตรวจจับ ปรับใช้เครื่องมือที่ทันสมัยอย่าง เช่นเอสไออีเอ็ม (SIEM) เอกซ์ดีอาร์ (XDR) อีดีอาร์ (EDR) และเอสโอเออาร์ (SOAR) พร้อมเจ้าหน้าที่ตรวจสอบและแก้ไขได้ตามแผนที่กำหนดไว้ ข้อเสนอแนะการป้องกันภัยจากมัลแวร์เรียกค่าไถ่ (Ransomware) สำหรับระบบควบคุมอุตสาหกรรม ในส่วนของระบบปฏิบัติการ (Operating system: OS) หรือ โปรแกรมส่วนใหญ่ยังคงล้าสมัยในการใช้โปรแกรมป้องกันไวรัส การตรวจจับอาจต้องใช้แนวทางปฏิบัติพิเศษ และต้องตรวจสอบความเข้ากันได้ อย่างเช่น เครื่องมือเอกซ์ดีอาร์ที่ให้บริการสนับสนุนป้องกันเฉพาะของระบบควบคุมอุตสาหกรรม ชื่อว่าทีเอ็กซ์วัน สเตลลาร์ (TXOne Stellar) ของเทรนด์ไมโคร (Trend Micro) (Kobialka, 2023)
4. มาตรการเผชิญเหตุเมื่อตรวจพบภัยคุกคามทางไซเบอร์ (Respond) 4.1 การวางแผนการตอบสนอง (Response Planning: RP) 4.2 การสื่อสาร (Communications: CO) 4.3 การวิเคราะห์ (Analysis: AN) 4.4 การควบคุมดูแลและจำกัด (Mitigation: MI) 4.5 การปรับปรุง (Improvements: IM)	1. แผนรับมือเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Incident Response Plan) ทีมมีจัดทำขั้นตอน สื่อสาร ฝึกซ้อม ทบทวนและปรับปรุงปีละ 1 ครั้งหรือมากกว่า 2. แผนการสื่อสารในภาวะวิกฤต ต้องจัดทำแผนการสื่อสารในภาวะวิกฤตเพื่อตอบสนองต่อวิกฤตที่เกิดจากเหตุการณ์ได้ 3. ฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise) ทบทวน และปรับปรุงอย่างน้อยปีละ 1 ครั้ง 4. การตรวจสอบและการตอบสนองต่อเหตุการณ์ทางไซเบอร์และไม่ใช่ทางไซเบอร์ (Cyber and Non-Cyber Event Handling) ระบุและจำแนกเหตุการณ์ที่เกิดขึ้นที่ส่งผลกระทบต่อระบบควบคุมอุตสาหกรรม ตามแผนเผชิญเหตุ ข้อเสนอแนะการป้องกันภัยจากมัลแวร์เรียกค่าไถ่ (Ransomware) สำหรับระบบควบคุมอุตสาหกรรม (ICS) และแผนการตอบสนองภัยคุกคามทางไซเบอร์ (Incident Response Plan) เช่น การสื่อสาร การวิเคราะห์ การควบคุมดูแลและจำกัดขอบเขตการบุกรุกโจมตี เป็นต้น จากนั้นนำประสบการณ์ที่เกิดขึ้นจริงมาปรับปรุง นอกจากนี้องค์กรควรพิจารณา บุคลากรที่จำเป็น รวมถึงทรัพยากรทั้งภายในและภายนอกไว้ในแผนรองรับการดำเนินธุรกิจอย่างต่อเนื่อง (BCP)
5. มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover) 5.1 การวางแผนการกู้คืน (Recovery Planning: RP) 5.2. การปรับปรุง (Improvements: IM)	1.จัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP) ตรวจสอบให้แน่ใจว่าฝึกซ้อมอย่างน้อยปีละ 1 ครั้ง เพื่อประเมินประสิทธิภาพของแผนตามที่กำหนดไว้ 2. แหล่งกู้ภัยสำรอง (Disaster Recovery Site: DR) ทำการสำรองข้อมูลสถานที่อื่นโดยสิ้นเชิงและสำรองข้อมูลตามหลักการ สาม-สอง-หนึ่ง ในการกู้คืนสภาพข้อมูล ต้องมีการกำหนดระยะเวลาที่สำคัญของระยะเวลาหยุดชะงักที่ยอมรับได้ (Tolerable Period of Disruption: TPD) ช่วงเวลาการหยุดชะงักที่ยอมรับได้สูงสุด (Maximum Tolerable Period of Disruption: MTPD) กำหนดเป้าหมายเวลาสำหรับการกู้คืนระบบให้กลับมาใช้งานได้ (Recovery Time Objective: RTO) พร้อมกำหนดจุดเวลาสำคัญสำหรับแผนการกู้คืนระบบ (Recovery Point Objective: RPO) เป็นต้น ควรมีแผนการทดสอบกู้ข้อมูลอย่างน้อยปีละ 1 ครั้ง

สรุปการสนทนากลุ่ม (Focus Group) โดยใช้แนวทางปฏิบัติของเอ็นไอเอสที (NIST)	
แนวคำถามสนทนากลุ่ม	**สรุปข้อมูลจากการสนทนากลุ่ม**
5.3 สื่อสาร (Communications: CO)	3. แผนกู้คืนสภาพคอมพิวเตอร์ควบคุมเทคโนโลยีเชิงปฏิบัติการ (OT) และระบบควบคุมอุตสาหกรรม (ICS) ควรสำรองข้อมูลของค่าติดตั้งอุปกรณ์ในระบบควบคุมปีละ 1 ครั้ง 4. การจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ (Information Security Incident Management) มีการกำหนดข้อตกลงระดับสัญญาการให้บริการ (Service Level Agreement: SLA) ในกระบวนการบริหารจัดการเหตุการณ์ที่ผิดปกติ เพื่อความรวดเร็วในการแก้ปัญหาตามแผนงานที่กำหนดไว้ได้ 5. มีกระบวนการดำเนินการเหตุการณ์ที่มีผลกระทบร้ายแรงต่อการดำเนินงานธุรกิจในส่วนระบบควบคุมอุตสาหกรรม ข้อเสนอแนะการป้องกันภัยจากมัลแวร์เรียกค่าไถ่ (Ransomware) ของระบบควบคุมอุตสาหกรรม ได้แก่ 1) การวางแผนการกู้คืนรายการทรัพยากรภายในและภายนอก ควรมีแผนการทดสอบการกู้ข้อมูลคืนจากการสำรองข้อมูลแบบออฟไลน์ อย่างน้อยปีละ 1 ครั้ง 2) แผนการสื่อสารที่มีประสิทธิภาพทั้งภายในและภายนอก

อภิปรายผล

จากตารางที่ 2 ได้นำเสนอแผนภาพแนวทางการป้องกันภัยจากมัลแวร์เรียกค่าไถ่ในระบบควบคุมอุตสาหกรรมในโรงงานแสดงถึงความสัมพันธ์ระหว่างเทคโนโลยีสารสนเทศ (IT), เทคโนโลยีเชิงปฏิบัติการ (OT) และระบบควบคุมอุตสาหกรรม (ICS) บนพื้นฐาน 5 ขั้นตอนของแนวทางของเอ็นไอเอสที (NIST) ดังนี้



ภาพที่ 4 แนวทางป้องกันมัลแวร์เรียกค่าไถ่ในระบบควบคุมอุตสาหกรรมบนพื้นฐานจากแนวทางปฏิบัติของเทคโนโลยีเชิงปฏิบัติการ (OT) และระบบควบคุมอุตสาหกรรม (ICS) เฉพาะจุดเด่นที่เพิ่มเติมจากเอ็นไอเอสที

ภาพที่ 4 ที่ได้นำเสนอในในงานวิจัยฉบับนี้ เป็นแผนภาพแนวทางการป้องกันภัยจากมัลแวร์เรียกค่าไถ่ในระบบควบคุมอุตสาหกรรมในโรงงานในภาพรวม สำหรับในภาพที่ 5 เป็นโมเดลในการใช้งานจริงระหว่างไอทีโซน (IT Zone) และโอทีโซน (OT Zone) ในระบบควบคุมอุตสาหกรรมในโรงงานเขตพื้นที่พระนครศรีอยุธยา เพื่อป้องกันภัยจากมัลแวร์เรียกค่าไถ่คริปโทล็อกเกอร์

ภาพที่ 4 ได้ใช้แนวทางเดียวกันกับงานวิจัยของ Chimmanee & Chotrungrat (2021, pp. 104-118) ที่ได้นำเสนอการแนวทางการป้องกันมัลแวร์เรียกค่าไถ่บนพื้นฐานของไอเอสที (NIST) เวอร์ชัน (Version) 8374 (Draft) ฉบับร่าง แต่ยังไม่ได้ออกแบบมาสำหรับส่วนเทคโนโลยีเชิงปฏิบัติการ (OT) และระบบควบคุมอุตสาหกรรม (ICS) นอกจากนี้ยังสอดคล้องกับงานวิจัยของ Wiboonrat (2022, pp. 1-6) ซึ่งได้นำเสนอแนวทางการป้องกันมัลแวร์เรียกค่าไถ่บนเอ็นไอเอสที เวอร์ชัน (Version) SP 800-82r2 ซึ่งเป็นเกี่ยวกับระบบควบคุมอุตสาหกรรมโดยเฉพาะ แต่อย่างไรก็ตามยังเป็นฉบับร่างอยู่ ดังนั้น แผนภาพที่ 4 จึงเป็นแนวทางการป้องกันภัยจากมัลแวร์เรียกค่าไถ่ในระบบควบคุมอุตสาหกรรมในโรงงานที่ได้รวมองค์ประกอบของเทคโนโลยีเชิงปฏิบัติการ, ระบบควบคุมอุตสาหกรรมและเอ็นไอเอสทีเวอร์ชัน (Version) SP 800-82r3 เข้าด้วยกัน

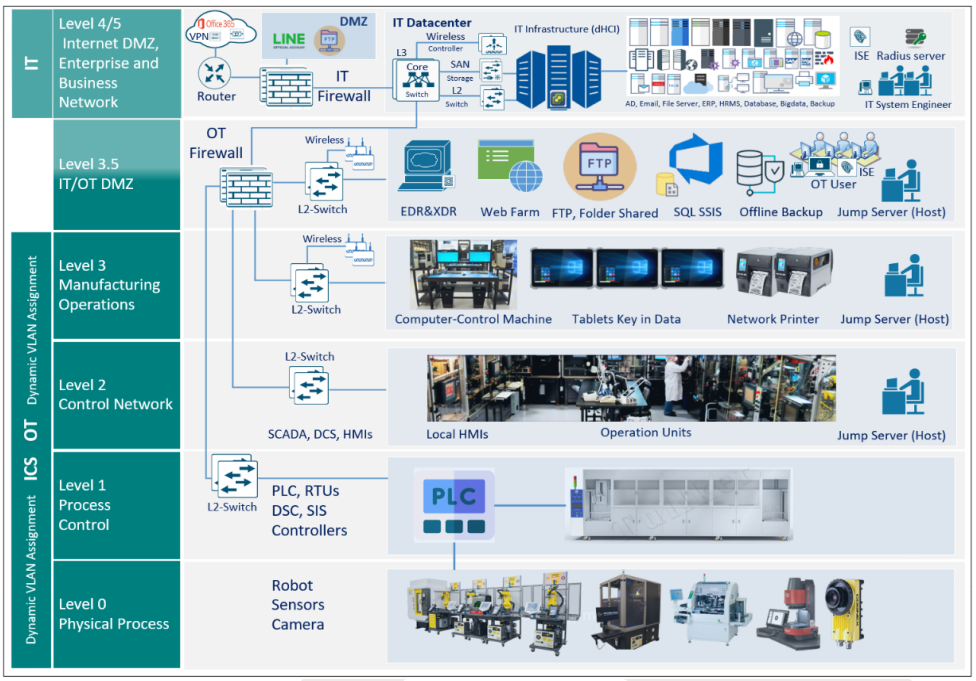
เพื่อเป็นการพิสูจน์ว่า แนวคิดที่นำเสนอในภาพที่ 4 สามารถนำมาประยุกต์ใช้งานจริงในการป้องกันมัลแวร์เรียกค่าไถ่ในระบบควบคุมอุตสาหกรรม ดังนั้น ในภาพที่ 5 ได้แสดงโมเดล (Model) ในการป้องกัน ลดความเสี่ยงและจำกัดขอบเขตพื้นที่ได้รับความเสียหายจากการถูกโจมตี โดยเป็นเชื่อมต่อระหว่างส่วนงานเทคโนโลยีสารสนเทศ (IT), ส่วนงานเทคโนโลยีเชิงปฏิบัติการ (OT) และระบบควบคุมอุตสาหกรรม (ICS) ซึ่งเป็นกรณีศึกษาจริงในโรงงานอุตสาหกรรมขนาดใหญ่ในพื้นที่พระนครศรีอยุธยา โดยการแบ่งส่วนและการแยกเครือข่าย (Network Segmentation and Isolation) ได้พิจารณาใช้เพอร์ดูโมเดล (Purdue Model) เพื่อป้องกันและลดความเสี่ยงจากการโจมตีทางไซเบอร์จากมัลแวร์เรียกค่าไถ่ (Ransomware) ซึ่งให้ความสำคัญหัวข้อดังต่อไปนี้

1. การไหลของข้อมูล (Data Flow Model) ข้อมูลจากระบบควบคุมอุตสาหกรรม (ICS) ในภาพที่ 5 จากระดับชั้น 1 การนำข้อมูลออกในทิศทางเดียวเท่านั้นไปยังระดับชั้น 3.5 ฐานข้อมูลระดับย่อย (Database) และฐานข้อมูลระดับย่อยจะทำการรวมข้อมูลด้วยเอสคิวเอล เอสเอสไอเอส (SQL Server Integration Services: SSIS) ส่งผ่านในแต่ละระดับชั้นไปยังระดับชั้น 4 ฐานข้อมูลเอสคิวแอลหลักระบบคลังข้อมูล (Data Warehouse) โดยการกำหนดนโยบายเอซีเอล (ACLs) อนุญาตโพรโทคอลทีซีพีพอร์ต (TCP Ports) 1433, 4022, 135, 1434, และยูดีพีพอร์ต (UDP Port) 1434 เท่านั้น พร้อมมีการตรวจสอบและควบคุมการเข้าถึงข้อมูล ซึ่งมีเพียงผู้ที่ได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงข้อมูลได้ เพื่อป้องกันการโจมตีโดยใช้เทคนิค T1071 ซึ่งถูกใช้โดยมัลแวร์เรียกค่าไถ่คริปโทล็อกเกอร์ (CryptoLocker) ในภาพที่ 2

2. การพิสูจน์ตัวตนของแต่ละระดับชั้น ในภาพที่ 5 ระหว่างระดับชั้น 3.5 กับระดับชั้น 4 และ 5 ซึ่งเป็นจุดอ่อนในปัจจุบัน จากรูปภาพจะเห็นได้ว่าโมเดล (Model) นี้มุ่งเน้นไปที่การจัดการเครือข่าย และการพิสูจน์ตัวตน (Authentication) การป้องกันด้วยการจัดการข้อมูลประจำตัวและการเข้าถึง (Identity and Access Management) ระบบจะมีการยืนยันตัวตนที่มอบสิทธิ์ในการใช้งานแก่ผู้ใช้เข้าถึงระบบหรือข้อมูลที่จำ

เป็นได้เท่านั้น เพื่อเพิ่มความน่าเชื่อถือด้วยการกำหนดการเข้าถึงแอปพลิเคชัน (Application) ด้วยการยืนยันตัวตนโดยใช้หลายปัจจัย (Multi-Factor Authentication: MFA) การยืนยันตัวตนผู้ใช้จะต้องระบุข้อมูลจากอย่างน้อย 2 ปัจจัยที่แตกต่างกัน (2FA) เช่น ชื่อผู้ใช้พร้อมทั้งรหัสผ่านที่มีความซับซ้อนที่ปลอดภัยตามนโยบายกำหนด และป้อนรหัสโอทีพี (OTP) ยืนยันตัวตนจากแอปพลิเคชัน (Application) ที่สร้างรหัสโอทีพี (OTP) บนโทรศัพท์มือถือ เพื่อป้องกันการโจมตีโดยใช้เทคนิค T1199 ซึ่งถูกใช้โดยมัลแวร์เรียกค่าไถ่คริปโทล็อกเกอร์ (CryptoLocker) ในภาพที่ 2 ร่วมถึงการเข้าถึงระบบจากเครือข่ายเสมือนส่วนตัววีพีเอ็น (Virtual Private Network: VPN) เพื่อป้องกันการโจมตีโดยใช้เทคนิค T1133 ซึ่งถูกใช้โดยมัลแวร์เรียกค่าไถ่คริปโทล็อกเกอร์ (CryptoLocker) ในภาพที่ 2

3. การควบคุมการเข้าถึง (Access Control) และเพิ่มความปลอดภัยในระหว่างโซน ซึ่งได้ติดตั้งไฟร์วอลล์ (Firewall) เพื่อแยกส่วนในการควบคุมการเข้าถึงระหว่างเทคโนโลยีสารสนเทศ (IT), เทคโนโลยีเชิงปฏิบัติการ (OT) และระบบควบคุมอุตสาหกรรม (ICS) โดยทำการกรองแพ็กเก็ต (Packet Filtering) จากไฟร์วอลล์ (Firewall) ตรวจจับสถานะ ป้องกันการโจมตี และลดความเสี่ยงการโจมตีจากมัลแวร์เรียกค่าไถ่ (Ransomware) (Belev, 2022 p. 1-4) โดยจัดการเครือข่าย (Network) นั้นได้กำหนดไดนามิควีแลนแอสซายเม้นท์ (Dynamic VLAN Assignment) และมีระบบพิสูจน์ตัวตนจากเรเดียสเซิร์ฟเวอร์ (Radius Server) ซึ่งจะทำงานร่วมกับกลุ่มผู้ใช้ในแอคทีฟไดเร็กทอรี (Active Directory: AD) สามารถกำหนดนโยบายเน็ตเวิร์กในการเข้าถึงที่ปลอดภัยให้กับเครื่องไคลเอนต์ (Client) ในแต่ละระดับชั้นโดยให้ความสำคัญในส่วนระบบควบคุมอุตสาหกรรม ยึดตามหมายเลขวีแลน (VLAN) แต่ในส่วนของอุปกรณ์ระบบปฏิบัติการ หรือโปรแกรมที่ยังคงเป็นเวอร์ชันที่ล้าสมัย ที่ยังคงต้องการเชื่อมต่อเข้าในระบบเครือข่ายของเทคโนโลยีเชิงปฏิบัติการ และระบบควบคุมอุตสาหกรรมจะกำหนดการอนุญาตหรือปฏิเสธการเข้าถึงระบบเครือข่ายด้วย (Media Access Control Address: MAC Address) ดังกล่าวข้างต้นเพื่อกำหนดนโยบาย (Dynamic Access Control List: ACL) พร้อมทำการกรองแพ็กเก็ต (Packet Filtering) และตรวจจับสถานะ ที่ส่งข้อมูลผ่านไฟร์วอลล์ให้เป็นไปตามเงื่อนไข ในภาพที่ 5 ระหว่างระดับชั้น 3.5 กับระดับชั้น 4 และ 5 โดยใช้นโยบายที่สร้างขึ้นมาเป็นเงื่อนไขเพื่อระบุสิทธิในการอนุญาตหรือปฏิเสธการเข้าถึงทรัพยากรข้อมูลระหว่างเครื่องคอมพิวเตอร์ หรือระหว่างระดับชั้นเครือข่าย พร้อมทั้งให้ความสำคัญอย่างละเอียดในการอนุญาตพอร์ตของโพรโทคอลทีซีพี (Transmission Control Protocol: TCP) และยูดีพี (User Datagram Protocol: UDP) ที่จำเป็นต้องใช้งานเชื่อมถึงกันในแต่ละระดับชั้นเครือข่าย ตัวอย่าง เช่น ในภาพที่ 5 ระหว่างระดับชั้น 3 กับระดับชั้น 3.5 การเข้าถึงไฟล์ข้อมูลการอนุญาตเข้าถึงด้วยพอร์ตโพรโทคอลทีซีพี 445, 139, 138, และ 137 เท่านั้น และที่สำคัญในการถึงข้อมูลจากเทคโนโลยีเชิงปฏิบัติการ และระบบควบคุมอุตสาหกรรม เช่น ซีเอสวีไฟล์ (CSV) จากเครื่องมือวัดทั้งหมดดังกล่าว ตามความสำคัญของข้อมูลการอนุญาตหรือปฏิเสธการเข้าถึงในแต่ระดับชั้น โดยการกำหนดนโยบายเอซีเอล (ACLs) อย่างเคร่งครัดเพื่อป้องกันลดความเสี่ยงและพื้นที่การโจมตีจากจากมัลแวร์เรียกค่าไถ่ (Ransomware) เพื่อป้องกันการโจมตีโดยใช้เทคนิค T1071 ซึ่งถูกใช้โดยมัลแวร์เรียกค่าไถ่คริปโทล็อกเกอร์ (CryptoLocker) ในภาพที่ 2



ภาพที่ 5 โมเดลการนำไปใช้งานจริงระหว่างเทคโนโลยีเชิงปฏิบัติการ (OT) และระบบควบคุมอุตสาหกรรม (ICS) กรณีศึกษาโรงงานอุตสาหกรรมขนาดใหญ่ ที่มีเงินทุนกว่า 200 ล้านบาท และคนงานกว่า 200 คนขึ้นไป ในเขตพื้นที่พระนครศรีอยุธยา

4. การตรวจจับภัยคุกคาม (Threat Detection) โดยใช้เครื่องมืออีดีอาร์ (Endpoint Detection and Response: EDR) ในภาพที่ 5 ในระดับชั้น 2 และ 3 ต้องมีการตรวจจับภัยคุกคามที่หลากหลาย (Threat Detection) และใช้นโยบายควบคุมอย่างเคร่งครัดของคอมพิวเตอร์ควบคุมเครื่องจักร (Computer-Controlled Machine) ในการควบคุมการเข้าถึงของพอร์ตยูเอสบีแฟลชไดรฟ์ (USB Flash drive) และบลูทูธ (Bluetooth) เพื่อป้องกันการโจมตีโดยใช้เทคนิค T1091 ซึ่งถูกใช้โดยมัลแวร์เรียกค่าไถ่คริปโทล็อกเกอร์ (CryptoLocker) ตามภาพที่ 2

บทสรุป

งานวิจัยนี้ดำเนินการศึกษาการป้องกันมัลแวร์เรียกค่าไถ่คริปโทล็อกเกอร์ (CryptoLocker) สำหรับระบบควบคุมอุตสาหกรรม (ICS) จากกรณีศึกษาโรงงานอุตสาหกรรมขนาดใหญ่ และได้นำแนวคิดไม่เชื่อใจใครตรวจสอบทุกอย่าง (Zero Trust) ซึ่งเป็นแนวคิดด้านความมั่นคงปลอดภัยทางไซเบอร์ โดยเน้นที่การป้องกันการเข้าถึงระบบควบคุมอุตสาหกรรมตั้งแต่เริ่มต้น และการสร้างความสามารถในการกู้คืนระบบอย่างรวดเร็วหากเกิดการโจมตี ซึ่งได้สอดคล้องกับผลจากการสนทนากลุ่มบนพื้นฐานของเอ็นไอเอสที (NIST) การจัดการในส่วนเทคโนโลยีเชิงปฏิบัติการ (OT) และระบบควบคุมอุตสาหกรรม โดยในงานวิจัยฉบับนี้ได้ นำเสนอแผนภาพแสดงความสัมพันธ์ของแนวทางป้องกันมัลแวร์เรียกค่าไถ่สำหรับระบบควบคุมอุตสาหกรรมตามแนวทางของมาตรฐานเอ็นไอเอสที ทั้ง 5 ขั้นตอน และโมเดล (Model) ในการใช้งานจริงระหว่างเทคโนโลยีเชิงปฏิบัติการและระบบควบคุมอุตสาหกรรม เพื่อป้องกันภัยจากมัลแวร์เรียกค่าไถ่คริปโทล็อกเกอร์

ข้อเสนอแนะ

การศึกษาวิจัยในอนาคตควรจะมีกรณีศึกษาเพิ่มเติมจากการโจมตีด้วยมัลแวร์เรียกค่าไถ่ชนิดอื่น ซึ่งจะทำให้ได้มีการวิเคราะห์เทคนิคการโจมตีอื่นเพิ่มเติม เพื่อจะได้นำมาออกแบบโมเดล (Model) ในการป้องกันภัยจากมัลแวร์เรียกค่าไถ่ได้ครอบคลุมมากยิ่งขึ้น นอกจากนี้การวิเคาระห์การโจมตีด้วยมัลแวร์เรียกค่าไถ่ควรจะใช้จากกรอบแนวคิดของเฟรมเวิร์กทูเอสเมทริกซ์ (2S Matrix for Ransomware Attack) ที่จัดทำโดย Chimmanee & Jantavongso (2024, pp. 1-17) ซึ่งวิเคราะห์การโจมตีจากมัลแวร์เรียกค่าไถ่ใหม่ล่าสุด

เอกสารอ้างอิง

Alamri, A. (2023). *Dragos Industrial Ransomware Analysis: Q2 2023.* Retrieved August 9, 2023. from https://www.dragos.com/blog/dragos-industrial-ransomware-attack-analysis-q2-2023.

AlMedires, M., & AlMaiah, M. (2021). Cybersecurity in industrial control system (ICS). *IEEE 2021 International Conference on Information Technology (ICIT),* 640-647.

Belev, B. C. (2022). Purdue Model Implementation in the Shipping Control Systems. *IEEE In 2022 10th International Scientific Conference on Computer Science (COMSCI)*, 1-4.

Chimmanee, K., & Chotrungrat, M. (2021). A Guideline for Ransomware Detection and Prevention at the Buddhist Places: A Case Study of Maze Gang. *Mahachula Academic Journal, 8(3), 104-118.* (In Thai).

Chimmanee, K., & Jantavongso, S. (2024). Digital forensic of Maze ransomware: A case of electricity distributor enterprise in ASEAN. *Expert Systems with Applications*, 1-17.

Goodwin, S. (2022). The need for a financial sector legal standard to support the NIST Cybersecurity Framework. *IEEE SoutheastCon 2022*, 89-95.

Kobialka, D. (2023). *Stellar Cyber now offers XDR for Operational Technology (OT) Environments.* Retrieved August 9, 2023. from https://www.msspalert.com/news/stellar-cyber-now-offers-xdr-for-operational-technology-ot-environments

Microsoft Threat Intelligence. (2020). *Ransomware groups continue to target healthcare critical services*. Retrieved August 9, 2023. from https://www.microsoft.com/en-us/security/blog/2020/04/28/ransomware-groups-continue-to-target-healthcare-critical-services-heres-how-to-reduce-risk.

Nakhonthai, P., & Chimmanee, K. (2022). Digital Forensic Analysis of Ransomware Attacks on Industrial Control Systems: A Case Study in Factories*, IEEE 2022 6th International Conference on Information Technology (InCIT),* 416-421.

Rajesh, P., Alam, M., Tahernezhadi, M., Monika, A., & Chanakya, G. (2022). Analysis of cyber threat detection and emulation using mitre attack framework. *IEEE 2022 International Conference on Intelligent Data Science Technologies and Applications (IDSTA),* 4-12.

Stouffer, K., Pease, M., Tang, C., Zimmerman, T., Pillitteri, V., Lightman, S., Hahn, A., Saravia, S., Sherule, A., & Thompson, M. (2023). *NIST SP 800-82r3 Guide to Operational Technology (OT) Security.* Retrieved September 10, 2023. from https://csrc.nist.gov/pubs/sp/800/82/r3/final.

Udroiu, A. M., Dumitrache, M., & Sandu, I. (2022, June). Improving the cybersecurity of medical systems by applying the NIST framework. *IEEE 2022 14th International Conference on Electronics, Computers and Artificial Intelligence (ECAI),* 1-7.

Wiboonrat, M. (2022). Cybersecurity in Industrial Control Systems: An integration of information technology and operational technology, *IEEE IECON 2022 – 48th Annual Conference of the IEEE Industrial Electronics Society,* 1-6.

You, Y., Lee, J., Oh, J., & Lee, K. (2018). A review of cyber security controls from an ICS perspective. *IEEE 2018 International Conference on Platform Technology and Service (PlatCon),* 1-6.