แนวทางการพัฒนาความมั่นคงปลอดภัยเครือข่ายไร้สาย ในเขตพื้นที่พุทธสถานโดยใช้แนวทางของโรงแรม

A Guidelines for Developing the Cyber Security on Wireless Security at the Buddhist Places According to Hotel Guidelines

คริชณะ ฉิมมณี*

Krishna Chimmanee

เดชพสิษฐ์ นาคประพันธุ์

Dejpasit Narkpraphan

วิทยาลัยนวัตกรรมดิจิทัลเทคโนโลยี มหาวิทยาลัยรังสิต, ประเทศไทย

College of Digital Innovation Technology, Rangsit University, Thailand

Email: sanon.s@rsu.ac.th

Received : February 17, 2021

Revised : August 3, 2021

Accepted : August 10, 2021

บทคัดย่อ

บทความวิจัยนี้มีวัตถุประสงค์เพื่อ (๑) เพื่อศึกษาแนวทางความมั่นปลอดภัยไร้สายจากมาตรฐานเอ็นไอเอส (๒) เพื่อศึกษารูปแบบการโจมตีผ่านระบบเครือข่ายไร้สายและแนวทางการป้องกัน (๓) เพื่อศึกษาหาแนวทางการพัฒนาการรักษาความมั่นคงปลอดภัยในเครือข่ายไร้สายในเขตพื้นที่พระพุทธสถานใช้รูปแบบการวิจัยเชิงคุณภาพ ประชากรและกลุ่มตัวอย่าง ได้แก่ ผู้เชี่ยวชาญทางด้านโทรคมนาคมที่ทำงานอยู่ในบริษัททางด้านเครือข่ายคอมพิวเตอร์ และผู้มีประสบการณ์ด้านเครือข่ายคอมพิวเตอร์โดยเป็นผู้ติดตั้งระบบเครือข่าย เครื่องมือที่ใช้ คือ แบบสอบถาม โดยสัมภาษณ์ ผู้เชี่ยวชาญจำนวน ๘ ท่าน แบ่งเป็น ๒ กลุ่ม

ผลการศึกษาพบว่า (๑) แนวทางความมั่นปลอดภัยไร้สายจากมาตรฐาน National Institute of Standard and Technology (NIST) ควรดำเนินการ ดังนี้ (๑.๑) การกำหนดสิทธิ์ เช่น โอทีพี เอ็มเอฟเอ (๑.๒) อุปกรณ์ที่ควรติดตั้งได้แก่ ดับเบิลยูไอดีเอส ไอดีเอส/ไอพีเอส และเอสไออีเอ็มด้วยฟังก์ชันยูอีบีเอ (๑.๓) การตรวจสอบช่องโหว่และอัพเดทแพท (๑.๔) ระบบเฝ้าระวัง (๒) ศึกษารูปแบบการโจมตีผ่านระบบเครือข่ายไร้สายและแนวทางการป้องกัน โดยคลอบคลุมทั้ง ๘ ด้านได้แก่ (๒.๑) การรักษาความลับ (๒.๒) ด้านความคงสภาพ (๒.๓) ด้านความพร้อมใช้งาน (๒.๔) ด้านการควบคุมการเข้าถึง (๒.๕) แนวทาง

---

* รศ.ดร.คริชณะ ฉิมมณี Assoc. Prof. Dr.Krishna Chimmanee

ในการป้องกันการถูกโจมตีผ่านเครือข่ายไร้สายทำการติดตั้งระบบดับเบิลยูไอดีเส การติดตั้งเอพี ต้องพยายามกำจัดสัญญานออกนอกพื้นที่ให้น้อยที่สุด เพิ่มการติดตั้งระบบระบุตัวตนผู้ใช้งานและปิดการมองเห็นระหว่างไคเอนต์ เป็นต้น (๒.๖) ตรวจสอบการถูกโจมตีและแสวงหาประโยชน์ผ่านช่องโหว่อย่างต่อเนื่อง ซึ่งอาจใช้เซียมช่วยในการตรวจสอบหรือดูจากรายงานในไอดีเอส ไอพีเอส (๒.๗) แนวทางในการทดสอบการเจาะระบบและตรวจสอบช่องโหว่ด้านความปลอดภัยเป็นที่ทราบโดยทั่วกันคือ ตรวจสอบความผิดปกติของอุปกรณ์ ตรวจสอบอุปกรณ์ไร้สายใกล้เคียง ตรวจสอบจุดเชื่อมต่อภายใน ทดสอบอุปกรณ์ภายใน ทดสอบพื้นฐานของเครือข่าย (๒.๘) การตรวจสอบการถูกโจมตีและแสวงหาผลประโยชน์อยู่เป็นประจำและประเมินเป็นระยะ โดยทำรายงานเป็น วัน, สัปดาห์ และเดือน เพื่อวิเคราะห์ดูว่ามีแนวทางป้องกันปัญหาได้อย่างเพียงพอ (๓) แนวทางการพัฒนาการรักษาความมั่นคงปลอดภัยในเครือข่ายไร้สายในเขตพื้นที่พระพุทธสถาน เพื่อความมั่นคงปลอดภัยในการติดตั้งระบบเครือข่ายไร้สาย ควรแบ่งโซนไฟร์วอลล์ และวีแลน เพื่อแยกเครือข่ายออกเป็นส่วน ๆ รวมทั้งกำหนดสิทธิ์การเข้าถึงตามหน้าที่และการรับบริการ ในโซนต่อไปนี้ (๓.๑) กุฏิหรือห้องพักในเขตพุทธสถาน (๓.๒) พื้นที่ส่วนกลางในเขตพุทธสถาน (๓.๓) ห้องประชุม (๓.๔) สำนักงาน (๓.๕) กล้องวงจรปิด (๓.๖) อุปกรณ์ ไอโอที

คำสำคัญ: การโจมตีเครือข่าย; เครือข่ายไร้สาย; ความมั่นคงปลอดภัยไซเบอร์

Abstract

This research article objectives are (1) to study the guidelines for wireless security from the NIS standard; (2) to study the patterns of attacks via wireless network systems and prevention methods; (3) to study and find guidelines for the development of security in wireless networks in the area of the Buddhasthan. Apply pattern qualitative research the population and samples are Atelecommu-nication specialist working in a computer network company and who have experience in computer networking by being a network installer The instrument used was a question-naire by interviewing 8 experts, divided into 2 groups.

The results of the study found that (1) wireless security guidelines from the National Institute of Standards and Technology (NIST) should proceed as follows: (1.1) Assigning rights such as OTP, MFA (1.2) Equipment that should be installed are: WIDS IDS/IPS and SIEM with UEBA function (1.3) Vulnerability check and patch update (1.4) Surveillance system (2) to study the patterns of attacks via wireless network systems and methods of prevention It covers all 8 areas as follows: (2.1) Confidentiality (2.2) Integrity (2.3) Availability (2.4) Access Control (2.5) Guidelines for preventing attacks

via wireless networks by installing a WIDS system. The installation of APs must try to eliminate the signal from outside the area to a minimum. Added installation of user identification system and disable visibility between clients, etc. (2.6) Continuously monitor attacks and exploits through vulnerabilities. This may be used to help check or look at the reports in the IDS IPS (2.7) Guidelines for penetration testing and detection of security vulnerabilities are widely known. Check for device malfunctions Check nearby wireless devices. Check the internal access point. internal device test network fundamentals (2.8) Regular monitoring of attacks and exploitation and periodic assessment by making reports in days, weeks and months to analyze whether there are adequate preventive measures (3) guidelines for the development of security in wireless networks in the area of the Buddhasthan for consideration is for security in wireless network installations Firewall and WLAN should be zoned to separate the network into sections. including assigning access rights according to functions and receiving services in the following zones (3.1) A cubicle or room in a Buddhasthan area (3.2) a common area in a Buddhasthan area (3.3) a meeting room (3.4) an office (3.5) CCTV (3.6) A IOT device

Keywords: Cyber-attacks; Wireless network; Cyber security

บทนำ

โดยทั่วไปการใช้งานระบบไร้สายนำไปสู่อันตรายที่แอบแฝงมากับจุดเชื่อมต่อของเครือข่ายไร้สายนั้น ๆ ผ่านตัวกลางที่เป็นคลื่นวิทยุ (Radio Wave) ซึ่งไม่สามารถระบุได้ว่ามีใครบ้างที่กำลังดำเนินการทำอะไรกับเครือข่ายไร้สาย รวมถึงการตรวจสอบว่า ผู้ที่กำลังเชื่อมต่ออยู่กับเครือข่ายไร้สายนั้นอยู่ที่พิกัดไหน ซึ่งไม่เหมือนการเชื่อมต่อสัญญาณผ่านสายแลน (Local Area Network: LAN) ที่จะรู้ต้นสายปลายทางจากการเชื่อมต่อนั้น ๆ ได้ง่าย เพราะฉะนั้นการคิดจะจัดตั้งจุดเชื่อมเครือข่ายไร้สาย ควรต้องศึกษาข้อมูลให้ละเอียดถึงการทำงานในส่วนต่าง ๆ ทั้งข้อดีและข้อเสียของอุปกรณ์แต่ละชนิด นอกจากนี้จำเป็นต้องรู้เท่าทันเหตุการณ์ภัยคุกคามไซเบอร์ที่อาจจะเกิดขึ้นในอนาคต เพื่อเตรียมพร้อมรับมือและทำให้เครือข่ายไร้สายมีความมั่นคงปลอดภัยมากที่สุด ซึ่งปัจจุบันนี้พระภิกษุสงฆ์ได้ใช้อินเทอร์เน็ตในการเผยแพร่พุทธศาสนาอย่างแพร่หลายโดยเฉพาะสื่อสังคมออนไลน์[๑]

[๑] พระมหาเอก เมธิกญาโณ เจตสลัน, “พฤติกรรมการใช้สื่อสังคมออนไลน์ ของพระนิสิตระดับปริญญาตรี มหาวิทยาลัยมหาจุฬาลงกรณราชวิทยาลัย อำเภอวังน้อย จังหวัดพระนครศรีอยุธยา”, **วารสารมหาจุฬาวิชาการ**, ปีที่ ๗ ฉบับที่ ๒ (๒๗ สิงหาคม ๒๕๖๓) : ๑๗๙-๑๙๐.

สถาบันมาตรฐานและเทคโนโลยีแห่งชาติแห่งชาติกระทรวงพานิชย์ สหรัฐฯ หรือเรียกว่า เอ็นไอเอสที (NIST: National Institute of Standards and Technology) ได้ออกแนวทางความมั่นคงปลอดภัยของระบบไร้สายในปี พ.ศ. ๒๕๕๐ เรื่อง “A Guide to IEEE 802.11i, Special Publication 800-97[๒] และถัดมา พ.ศ. ๒๕๕๕ เรื่อง Guidelines for Securing Wireless Local Area Networks (WLANs); Special Publication 800-153[๓] เพื่อเป็นแนวทางในการพัฒนาระบบเครือข่ายไร้สาย จากการทบทวนวรรณกรรมงานวิจัยที่เกี่ยวข้องในปี พ.ศ. ๒๕๖๒ เช่น ราจีฟ ซิงห์[๔] ได้อธิบายถึงการรักษาความมั่นคงปลอดภัยในระบบเครือข่ายไร้สาย โดยได้แสดงการเปรียบเทียบวิธีการต่าง ๆ ซารีมาร์ แบนดาล่าและคณะ[๕] ได้ระบุผลการสำรวจพบว่าโดยทั่วไป ความตระหนักถึงภัยคุมคามในการใช้เครือข่ายไร้สายค่อนข้างต่ำ ซึ่งสอดคล้องกับงานวิจัยของ อตาวิน่า วี และคณะ[๖] ที่ระบุว่าการใช้ไวไฟในเขตพื้นที่สาธารณะยังคงขาดความมั่นคงปลอดภัยในการใช้งาน และ สมญา คิเตอร์ มอมแมส อเทลมาเนจ[๗] ได้ระบุว่า ความเสี่ยงและภัยคุกคามจากการใช้เครือข่ายไร้สายยังคงมีอยู่ และยากที่จะแก้ไขปัญหานี้ได้อย่างสมบูรณ์ แต่ขั้นตอนการใช้ที่ดีจะช่วยบรรเทาปัญหาได้ โดยทั่วไปการใช้งานตามที่พักอาศัยจะมีโอกาสเสี่ยงต่อการโจมตีที่น้อยกว่า และมีการป้องกันที่ไม่ซับซ้อน เมื่อเทียบกับองค์กรขนาดใหญ่ โรงแรม เขตพื้นที่พุทธสถาน หรืออินเทอร์เน็ตไร้สายสำหรับพื้นที่ให้บริการ เช่น ห้องประชุม ห้องพักผ่อน ห้องสัมมนา เป็นต้น โดยปกติผู้ใช้บริการจะมีความคาดหวังเป็นอย่างมากในเรื่องของความสะดวกต่อการเข้าใช้งาน และความเร็ว

---

[๒] Frankel Sheila, Eydt Bernard, Owens Les, Scarfone Karen, “**Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i”**, Special Publication 800-97, National Institute of Standards and Technology (NIST) [February 2007].

[๓] Souppaya Murugiah, Scarfone Karen, **“Guidelines for Securing Wireless Local Area Networks (WLANs)”,** Special Publication 800-153, National Institute of Standards and Technology (NIST) [February 2012].

[๔] Singh Rajeev and Parval Sharma Teek, **“Security in Wireless Local Area Networks (WLANs)”,** [Online], Available: https://www.intechopen.com/books/computer-and-network-security/security-in-wireless-local-area-networks-wlans- [2019].

[๕] Benqdara Salima, Mahmoud Abdelfattah, “Wireless Security in Libya: A Survey Paper”, **International Journal of Computer Applications**, 181 (35) (January 2019) 26-31.

[๖] Anastasia Atavina V., Zareshin Sergei V., Rumyantseva Irina S., Ivanenko Vitaliy G. Analysis of Security of Public Access to Wi–Fi Networks on Moscow Streets. Russian: **IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus),** (2017) 105-110.

[๗] Mohmmed Somya Khidir, Al Mostafa Ahmed Hassan, “A review of threats, protocols, and solutions to enhance the security of wireless networks”, **IJCSNS International Journal of Computer Science and Network Security**, 19 (4) (2019): 108-115.

ของอินเทอร์เน็ตไร้สาย ยิ่งไปกว่านั้น สิ่งหนึ่งที่ผู้ใช้บริการคาดหวังเป็นอย่างยิ่ง คือ ความปลอดภัยของการเข้าใช้งานในเขตพื้นที่พุทธสถานนั้น ๆ ซึ่งถ้าสถานที่ได้มีการวางระบบเรื่องความมั่นคงปลอดภัย และมีการตรวจสอบที่ดีมีประสิทธิภาพ มีประสิทธิผล และมีการแก้ไขปัญหาอย่างรวดเร็ว ก็จะทำให้ผู้ใช้บริการมีความมั่นคงปลอดภัยต่อการใช้งาน และมีความเชื่อมั่นต่อการใช้บริการมากขึ้น ในปี พ.ศ. ๒๕๖๑ แดนนี่ มารีโค[๘] ได้นำเสนอแนวทางในการป้องกันความมั่นคงปลอดภัยของระบบไร้สายในโรงแรมอย่างคร่าว ๆ ดังนั้น ขั้นตอนการรักษาความมั่นคงปลอดภัยของเครือข่ายไร้สายยังคงเป็นที่ต้องการโดยเฉพาะในโรงแรมและพื้นที่ในเขตพุทธสถาน

วัตถุประสงค์ของการวิจัย

๑. เพื่อศึกษาหลักความมั่นคงปลอดภัยไร้สายจากมาตรฐานเอ็นไอเอสที

๒. เพื่อศึกษารูปแบบการโจมตีผ่านระบบเครือข่ายไร้สายและแนวทางการป้องกัน

๓. เพื่อเสนอแนวทางการพัฒนาความมั่นคงปลอดภัยในเครือข่ายไร้สายในเขตพื้นที่พระพุทธสถาน

แนวคิดและทฤษฎีที่เกี่ยวข้อง

ผู้วิจัยศึกษาแนวคิด และทฤษฎีที่เกี่ยวข้อง จำนวน ๒ ฉบับ ได้แก่

๑. จากมาตรฐานที่ได้กำหนดแนวทางไว้โดย เอ็นไอเอสที 800-97

(๑) การรักษาความลับ (Confidentiality) ต้องแน่ใจว่าผู้ไม่ได้รับสิทธิ์การเข้าถึง จะไม่สามารถเชื่อมต่อเข้าระบบได้

(๒) ความสมบูรณ์ (Integrity) ต้องตรวจสอบการเปลี่ยนแปลงของการใช้งานทั้งหมดที่เกิดขึ้นไม่มีการเปลี่ยนแปลงข้อมูล

(๓) ความพร้อมใช้งาน (Availability) ตรวจสอบให้แน่ใจว่าอุปกรณ์และบุคคลสามารถเข้าถึงเครือข่ายและทรัพยากรได้สะดวกและมั่นคงปลอดภัย

(๔) การควบคุมการเข้าถึง (Access Control) จำกัดสิทธิ์ของอุปกรณ์หรือบุคคลในการเข้าถึงเครือข่ายหรือทรัพยากรภายในเครือข่าย

๒. จากมาตรฐานที่ได้กำหนดแนวทางไว้โดย เอ็นไอเอสที 800-153

(๑) การเฝ้าระวังการโจมตี (Attack Monitoring)

(๑.๑) การโจมตีแบบพาสซีฟ (Passive attack) คือ การโจมตีที่พยายามอ่านหรือใช้ประโยชน์จากข้อมูลภายในที่เจาะเข้าไป แต่ไม่ส่งผลกระทบต่อระบบ โดยแบ่งออกเป็นสองประเภท

---

[๘] Mareco Danny, **"6 Ways Hotel Wi-Fi Is About More than Providing In-Room Guest Access"**, [Online], Available: https://www.securedgenetworks.com/blog/hotel-wifi-is-about-more-than-in-room-guest-access [23 March 2018].

(๑.๑.๑) การแอบดูข้อมูล (Eavesdropping) ผู้โจมตีดักดูข้อมูล เนื้อหาและข้อความของการสื่อสารบนเครือข่ายไร้สาย

(๑.๑.๒) การวิเคราะห์การจราจร (Traffic analysis) หรือการวิเคราะห์การไหลของข้อมูล ผู้โจมตีจะทำการตรวจสอบข้อมูลในระบบเพื่อนำมาวิเคราะห์ว่าข้อมูลไหนที่ต้องการ และเข้าโจมตีต่อไป

(๑.๒) การโจมตีที่แอคทีฟ (Active attack) คือ การโจมตีที่พยายามเปลี่ยนข้อมูลหรือส่งผลต่อการทำงานของระบบ การโจมตีที่แอ็คทีฟอาจเป็นหนึ่งในประเภทดังต่อไปนี้

(๑.๒.๑) การโจมตีโดยการปลอมตัว (Masquerading attack) ผู้โจมตีต้องการไม่ให้ใครรู้ตัวตนที่แท้จริงว่าใครเป็นผู้ส่งข้อมูล โดยการส่งข้อมูลปลอมเพื่อให้ผู้ใช้งานใส่ข้อมูลยืนยันตนเอง (False identity) และหลอกล่อเข้าไปในเครือข่ายปลอมที่สร้างไว้ซึ่งเป็นสาเหตุที่ทำให้เกิดความเสียหายได้

(๑.๒.๒) การโจมตีแบบทวนซ้ำข้อความ (Replay attack) ผู้โจมตีใช้ข้อมูลที่เก็บมาได้ เช่น การเก็บบัญชีรายชื่อผู้ใช้งานและรหัสผ่าน เพื่อนำไปล็อคอินเข้าสู่ระบบได้

(๑.๒.๓) ข้อความเท็จ (Bogus messages of Fake message) ผู้โจมตีอาจทำการส่งข้อมูลที่มีข้อความเท็จเข้าไปในเครือข่ายแล้วส่งผลกระทบกับผู้ใช้คนอื่น ๆ

(๑.๒.๔) การโจมตีเพื่อทำลายหรือหยุดการให้บริการ (Denial of service: DoS) ผู้โจมตีอาจทำการส่งข้อมูลที่ไม่เกี่ยวข้องกับการทำงานของเครือข่ายจนทำให้แบนด์วิชท์ เครือข่ายถูกใช้งานจนเต็ม และไม่สามารถให้บริการผู้ใช้งานต่อไปได้

(๑.๒.๕) การลักลอบ (Misappropriation) ผู้โจมตีขโมยข้อมูลหรือใช้บริการเครือข่ายไร้สายโดยไม่ได้รับอนุญาต

(๒) การตรวจสอบช่องโหว่ (Vulnerability Monitoring)

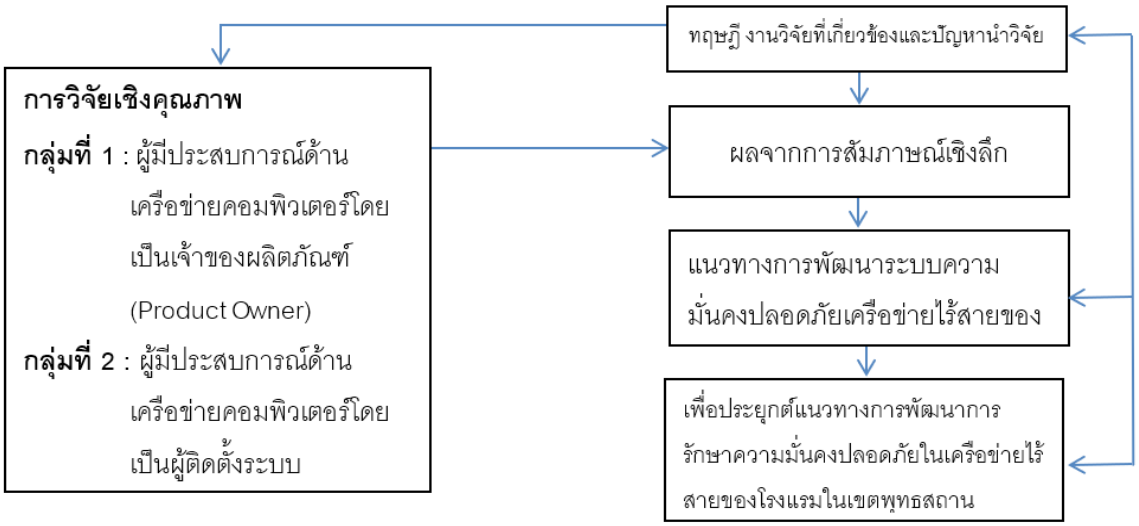
(๒.๑) องค์กรควรทำการตรวจสอบช่องโหว่เพื่อตั้งค่าความมั่นคงปลอดภัยและปรับปรุง แก้ไขอยู่เป็นประจำ

(๒.๒) การตรวจสอบช่องโหว่ของเครือข่ายไร้สายช่วยป้องกันการโจมตีจากผู้บุกรุกซึ่งอาจจะพัฒนาโปโตคอลหรือโปรแกรมโดยเฉพาะ เพื่อนำมาใช้กับอุปกรณ์ต่าง ๆ ทั้งภายในและภายนอกเครือข่าย

วิธีการดำเนินการวิจัย

๑. กรอบแนวคิดการวิจัย

กรอบแนวคิดการวิจัยซึ่งแบ่งออกได้เป็น ๔ ขั้นตอน และสามารถอธิบายในรายละเอียดได้แสดงในภาพที่ ๑



ภาพที่ ๑ แสดงกรอบแนวคิดการวิจัย

ระเบียบวิธีวิจัย

ขอบเขตในการดำเนินการงานวิจัยดังนี้

ขั้นตอนที่ ๑ คือ ศึกษาแนวคิด ทฤษฎี งานวิจัยที่เกี่ยวข้อง และมาตรฐานความมั่นคงปลอดภัยของระบบไร้สายจากสถาบันมาตรฐานและเทคโนโลยีแห่งชาติของสหรัฐฯ (NIST) โดยได้เลือกใช้มาตรฐานจำนวนสองฉบับ ได้แก่ แนวทางความมั่นคงปลอดภัยของระบบไร้สาย ในปี พ.ศ. ๒๕๕๐ เรื่อง “A Guide to IEEE 802.11i, Special Publication 800-97 (Sheila Frankel et al., 2007) และ พ.ศ. ๒๕๕๕ เรื่อง “Guidelines for Securing Wireless Local Area Networks (WLANs); Special Publication 800-153 (Murugiah Souppaya et al., 2012) เพื่อเป็นแนวทางในการสร้างเครื่องมือแบบสอบถามสำหรับศึกษาแนวทางการพัฒนาระบบความมั่นคงปลอดภัยเครือข่ายไร้สายสำหรับโรงแรม

ขั้นตอนที่ ๒ คือ สร้างเครื่องมือ แบบสอบถามสำหรับการสัมภาษณ์เชิงลึก โดยส่งให้ผู้เชี่ยวชาญจำนวน ๓ ท่าน สำหรับตรวจสอบความเหมาะสมถูกต้อง และได้แก้ไขตามคำแนะนำเรียบร้อยแล้ว โดยแบบสอบถามแบ่งเป็น ๒ ส่วน ได้แก่

ส่วนที่ ๑ เป็นแบบสอบถามสัมภาษณ์เชิงลึกอ้างอิงจาก NIST ในขั้นตอนที่ ๑

ส่วนที่ ๒ เป็นแบบสอบถามสัมภาษณ์เชิงลึกสำหรับแนวทางป้องกันระบบเครือข่ายไร้สายในโรงแรม

ขั้นตอนที่ ๓ คือ การสัมภาษณ์เชิงลึกผู้เชี่ยวชาญซึ่งเลือกวิธีแบบเฉพาะเจาะจงจำนวน ๘ คน ซึ่งแบ่งออกเป็นสองกลุ่ม ได้แก่

กลุ่มที่ ๑ มีประสบการณ์ด้านเครือข่ายคอมพิวเตอร์โดยเป็นเจ้าของผลิตภัณฑ์ (Product Owner) จำนวน ๒ คน

กลุ่มที่ ๒ มีประสบการณ์ด้านเครือข่ายคอมพิวเตอร์โดยเป็นผู้ติดตั้งระบบ (System Integrator : SI) จำนวน ๖ คน

ขั้นตอนที่ ๔ คือ วิเคราะห์ผลที่ได้จากการสัมภาษณ์เชิงลึก และการรวบรวมข้อมูลจากงานวิจัยที่เกี่ยวข้อง

ขั้นตอนที่ ๕ คือ ได้แนวทางในการดำเนินการพัฒนาระบบความมั่นคงปลอดภัยเครือข่ายไร้สายสำหรับโรงแรม

การเก็บรวบรวมข้อมูล

ผู้วิจัยได้สัมภาษณ์เชิงลึกจากผู้เชี่ยวชาญจำนวน ๘ ท่าน แบ่งเป็น ๒ กลุ่ม ได้แก่ กลุ่มที่ ๑ ซึ่งคือ ผู้เชี่ยวชาญทางด้านโทรคมนาคมที่ทำงานอยู่ในบริษัททางด้านเครือข่ายเน็ตเวิร์ค (Vendor) กลุ่มที่ ๒ ซึ่งคือ เจ้าหน้าที่เกี่ยวข้องกับเครือข่ายไร้สายโดยตรงของโรงแรมที่ทำการทดสอบ

ผลการสัมภาษณ์เชิงลึก

สรุปผลการวิจัย

ในบทนี้ได้แสดงผลการสัมภาษณ์เชิงลึกจากผู้เชี่ยวชาญทั้งหมดจำนวน ๘ ท่านโดยใช้แบบสอบถามตามภาคผนวก ก. ซึ่งได้แบ่งออกเป็น ๒ หัวข้อหลัก ได้แก่ ผลสัมภาษณ์เชิงลึกอ้างอิงจากทฤษฎีของ NIST โดยผลลัพธ์การสัมภาษณ์เชิงลึกได้แสดงในตาราง ๑ และผลสัมภาษณ์เชิงลึกอ้างอิง โดยผลลัพธ์การสัมภาษณ์เชิงลึกได้แสดงในตาราง ๒

ตารางที่ ๑ ผลสัมภาษณ์เชิงลึกอ้างอิงจากทฤษฎีของ NIST โดยผลลัพธ์การสัมภาษณ์เชิงลึกได้สรุปประเด็นสำคัญ ๆ ไว้ในตาราง

คำถาม	สรุปคำตอบแบบสอบถาม
๑. ท่านมีแนวทางในการกำหนดสิทธิ์การเข้าถึงเครือข่ายอย่างไร	กำหนดสิทธิ์ประเภทผู้ใช้งานในการเข้าถึงที่แน่นอนชัดเจน โดยจัดทำระบบยืนยันตัวตนในองค์กรของแต่ละแผนก ส่วนงาน หรือแขกที่ใช้งาน และกำหนดช่วงเวลาในการเข้าถึง โดยใช้การแก้ปัญหา ทางด้านไอทีในการกำหนดสิทธิ์ เช่น วิวอะบิลลิที (Viewability), เอ็มเอฟเอ(MFA), เรเดียส และโปรโตคอล เอเอเอ (RADIUS-AAA)
๒. ท่านมีแนวทางในการตรวจสอบความผิดปกติของการให้บริการในระบบเครือข่ายอย่างไร	โดยปกติจะนิยมใช้โปรโทคอล เอสเอ็นเอ็มพี (SNMP) เพื่อแจ้งเตือนหากเกิดข้อผิดพลาดขึ้นในระบบเครือข่ายนอกจากนี้ในระบบสมัยใหม่จำเป็นต้องมีระบบ ไอดีเอส (IDS) / ไอพีเอส (IPS) และ เซียม ซึ่งปัจจุบันนี้ได้มีเทคโนโลยีเรียกว่า ยูอีบีเอ (UEBA) ในการวิเคราะห์พฤติกรรรมของผู้ใช้งานและอุปกรณ์ โดยใช้ปัญญาประดิษฐ์เพื่อแจ้งเตือนความผิดปกติที่เกิดจากพฤติกรรมการใช้งานที่เปลี่ยนไป
๓. ท่านมีแนวทางในการดำเนินการด้านความปลอดภัยระบบสารสนเทศและเครือข่ายดังต่อไปนี้	แยกเป็นหัวข้อย่อย ๓.๑ - ๓.๔
๓.๑ การรักษาความลับ (Confidentiality)	ต้องมีการพิสูจน์ตัวตนด้วยอุปกรณ์ที่ได้มาตรฐาน เช่น เอดี (AD) / เรเดียส (RADIUS) และควรมีการใช้วิธีเปิดใช้งานทูเอฟเอ (2FA) และนอกจากนี้ต้องมีการเข้ารหัส (Data Encryption)
๓.๒ ความคงสภาพ (Integrity)	โดยกำหนด เพื่อกำหนดสิทธิ์ในการเปิดข้อมูล (Data permission) และเพื่อป้องกันการเปลี่ยนแปลงข้อมูล (Data hashing) ด้วยวิธีการดังกล่าวจะทำให้ข้อมูลมีความปลอดภัยและป้องกันไม่ให้ใครมาแทรกหรือเปลี่ยนแปลงข้อมูลในระหว่างทาง นอกจากนี้ต้องมีการเก็บข้อมูลให้ปลอดภัยโดยจะมีเพียงหน่วยงานที่มีสิทธิ์เท่านั้นที่จะสามารถเข้าถึงหรือแก้ไขข้อมูล
๓.๓ ความพร้อมใช้งาน (Availability)	ต้องจัดทำให้ระบบสามารถให้บริการได้ตลอดเวลาเรียกว่า เอชเอ (HA) และการวางแผนต่อเนื่องทางธุรกิจ (Business Continuity Planning) ถ้าระบบล้มเหลวเราสามารถทำตามแผนที่ได้วางไว้เพื่อกู้ข้อมูลหรือให้ระบบสามารถกลับมาดำเนินการได้
๓.๔ การควบคุมการเข้าถึง (Access Control)	ใช้แนค (NAC) เข้ามาช่วยควบคุมผู้ใช้งานและอุปกรณ์ ที่ใช้งานเครือข่ายอัจฉริยะ และ การจัดการอุปกรณ์ไร้สาย (Mobile management) เพื่อการยืนยันตัวบุคคลก่อนเข้าสู่ระบบที่สามารถระบุตัวบุคคลได้ และควรกำหนดสิทธิ์ผู้ที่ใช้งานแบบจำกัดโซนนิ่ง (Zoning) นอกจากนี้เพื่อความปลอดภัยมั่นคงมากขึ้นควรใช้วิธีการทูเอฟเอ

๔. ท่านมีแนวทางในการทดสอบการเจาะระบบ (Penetration Testing) และตรวจสอบช่องโหว่ของระบบ (Vulnerability Assessment) อย่างไรบ้าง	การทดสอบการโจมตี (Penetration Testing) คือ ทดสอบการเจาะระบบเครือข่ายโดยการตรวจสอบช่องโหว่ของระบบ (Vulnerability Assessment) เพื่อการประเมินหาความเสี่ยงที่เกิดจากช่องโหว่ที่ค้นพบ และผลกระทบจากการโดนโจมตี โดยทั่วไปการทดสอบการโจมตี จะใช้ความเสี่ยงที่ปรากฏต่อสาธารณะ เช่น ซีวีอี (CVE) ซึ่งเป็นดัชนีที่รวบรวมรายชื่อช่องโหว่ด้านความปลอดภัยที่เป็นที่ทราบโดยทั่วกัน ขั้นตอนการหาช่องโหว่ของระบบโดยผู้ดูแลระบบไร้สายมีดังต่อไปนี้ (๑) ตรวจสอบอุปกรณ์แปลกปลอม (Investigate rogue devices) (๒) ค้นหาอุปกรณ์ไร้สายใกล้เคียง (Discover nearby wireless devices) (๓) ทดสอบอุปกรณ์กระจายสัญญาณของคุณ (Test your own access points) (๔) ทดสอบอุปกรณ์ภายใน (Test your own stations) (๕) ทดสอบโครงสร้างพื้นฐานวีแลน (Test your WLAN infrastructure)
๕. ท่านมีคำแนะนำเกี่ยวกับเครื่องมือที่ใช้ในการทดสอบการเจาะระบบและตรวจสอบช่องโหว่ของระบบอย่างไรบ้าง	ทำตามกฎของความปลอดภัยพื้นฐาน (Baseline Security) ด้านไวไฟ โดยใช้เครื่องมือวิเคราะห์ เช่น ไวร์ชาร์ก (Wireshark), เอ็นเอ็มเอพี (NMAP) หรือใช้กาลีลินุกซ์ (Kali Linux) ซึ่งจะมีเครื่องมือต่าง ๆ ที่เกี่ยวข้องในการทดสอบการเจาะระบบและตรวจสอบช่องโหว่
๖. ท่านมีคำแนะนำในการเฝ้าระวังการถูกโจมตี และแสวงประโยชน์ผ่านช่องโหว่อย่างต่อเนื่อง (Continuous Monitoring) อย่างไร	การโจมตีในลักษณะเอพีที (APT) จะตรวจสอบได้ค่อนข้างลำบาก ดังนั้นจึงนิยมใช้อุปกรณ์เซียมเพื่อคอยตรวจสอบไฟล์เก็บประวัติ (ล็อกไฟล์) จากอุปกรณ์เครือข่าย และแจ้งเตือนโดยอัตโนมัติ หรือตรวจสอบจากรายงานของอุปกรณ์ไอดีเอส/ไอพีเอส สำหรับในกรณีที่ต้องการป้องกันข้อมูลควรจะมีอุปกรณ์ที่ทำหน้าที่ในการป้องกันข้อมูล (Data Protection)
๗. ถ้าหากมีการเฝ้าระวังการถูกโจมตีและแสวงหาประโยชน์ (Exploits) ผ่านช่องโหว่อยู่เป็นประจำแล้ว ท่านมีข้อแนะนำในการประเมินผลเป็นระยะอย่างไร (Periodic Assessment Recommendations)	ต้องมีการตรวจสอบอยู่เป็นประจำโดยทำรายงานเป็นรายวัน รายสัปดาห์ รายเดือน เพื่อวิเคราะห์ดูว่าการแก้ปัญหาเพียงพอหรือไม่ หลังจากรวบรวมข้อมูลที่ได้มาจากการโจมตีและแสวงหาประโยชน์แล้ว การตรวจสอบมักจะใช้รายการตรวจสอบ (check list) ตามมาตรฐาน หรือใช้เครื่องมือในการตรวจสอบ สิ่งที่ตรวจสอบ ได้แก่ (๑) ข้อมูลรั่วไหล (Information leak) จากการใช้งานอินเทอร์เน็ต เช่น ฟิชชิ่ง (Phishing) เป็นเทคนิคการหลอกลวงทางอินเทอร์เน็ตประเภทหนึ่ง ซึ่งมักจะมาในรูปแบบของการปลอมแปลงอีเมล หรือข้อความที่สร้างขึ้น เพื่อหลอกให้เหยื่อเปิดเผยข้อมูลทางด้านการเงินหรือข้อมูลส่วนตัวต่าง ๆ เช่น บัญชีผู้ใช้งานและรหัสผ่านของหมายเลขบัตรเครดิตหรือหมายเลขบัตรประชาชน นอกจากนี้การรั่วของดีเอ็นเอส (DNS) ทำให้แฮกเกอร์สามารถทราบข้อมูลเว็บไซต์ที่คุณเข้าชม หรือ การเรียกใช้งานอินเทอร์เน็ตของคุณ (DNS log) และใช้เพื่อการโจมตีแบบฟิชชิ่งได้ ซึ่งอาจจะปลอมแปลงการเข้าถึงข้อมูลได้ (Hijack) หรือ Redirect เพื่อไปยังที่อื่นที่ไม่ใช่ตัวจริง (๒) รายการตรวจสอบเว็บแอปพลิเคชั่น (Web Application checklist) โดยใช้มาตรฐานโอดับเบิลยูเอเอสพี (OWASP) เป็นต้นเพื่อตรวจสอบช่องโหว่ในการเข้าถึงระบบผ่านเว็บแอปพลิเคชั่น (๓) รายชื่อโดเมน (DNS server checklist) ตรวจสอบค่าที่แสดงข้อมูลสาธารณะเลือกใช้ดีเอ็นเอส เซิร์ฟเวอร์ ที่มีความน่าเชื่อถือสูง เพื่อหลีกเลี่ยงปัญหาของการรั่วของดีเอ็นเอส (๔) การทำรายการอีเมลที่ไม่น่าเชื่อถือเพื่อป้องกันไม่ให้เข้าถึง (E-mail Server checklist) เพื่อป้องกันจดหมายขยะ มัลแวร์ และไวรัส ที่จะ

	เข้ามาทางช่องทางนี้ (๕) การตรวจสอบโครงสร้างเครือข่าย (Network Topology checklist) คือ การตรวจสอบการเชื่อมต่อกับอินเทอร์เน็ต และเครือข่ายภายในเพื่อวิเคราะห์จุดอ่อน หรือช่องโหว่ของเครือข่ายสำหรับการรักษาความมั่นคงปลอดภัย การเชื่อมต่อกับอินเทอร์เน็ต ได้แก่ เส้นทาง (route) เชื่อมต่อไปยังไอเอสพีที่ให้บริการ ได้ผ่านผู้ให้เช่าโครงข่ายอย่างไร และข้อมูลเส้นทาง จำนวนลิงค์ของไอเอสพี ซึ่งส่วนนี้จะเน้นไปถึงการประเมินประสิทธิภาพการป้องกันการโจมตีแบบดีดีโอเอส/ดีโอเอส (DDoS/DoS) การเชื่อมต่อเครือข่ายภายใน ต้องมีแนวทางการป้องกันการโจมตีแบบดีดีโอเอส/ดีโอเอส ซึ่งจะสะท้อนให้เห็นถึงความพร้อมโครงสร้างเครือข่ายของบริษัทว่าได้มีการจัดเตรียมเทคโนโลยีด้านความมั่นคงปลอดภัยครบถ้วน อุปกรณ์เราเตอร์ควรมีการจัดทำเอซีแอล (ACL) นอกจากนี้อุปกรณ์ไฟร์วอลล์ควรกำหนดค่าแบล็คลิสต์ และสามารถทำงานในระดับ stateful inspection ได้ (๖) ตรวจสอบพอร์ตที่เปิดให้บริการจากข้อมูลในขั้นตอนสำรวจพอร์ตที่เปิดใช้บริการจาก ไอพีแอดเดรสของเว็บไซต์บริษัท อีเมล ดีเอ็นเอส เซิร์ฟเวอร์ เราเตอร์ และอื่น ๆ ที่ทำการเปิดบริการไว้ เพื่อจะทำการขยายผลหาช่องโหว่จากการโจมตีในขั้นตอนต่อไป

ตารางที่ ๒ แบบสอบถามสัมภาษณ์เชิงลึกสำหรับแนวทางป้องกันระบบเครือข่ายไร้สายในโรงแรม ได้สรุปประเด็นสำคัญ ๆ ไว้ในตาราง

คำถาม	สรุปคำตอบแบบสอบถาม
๑. ท่านช่วยอธิบายวิธีการโจมตีผ่านระบบเครือข่ายไร้สาย	นำอุปกรณ์เอพีเข้ามาติดตั้งใช้งานโดยไม่ได้กำหนดค่าเกี่ยวกับความปลอดภัย ทำให้เกิดช่องโหว่ของระบบเครือข่ายเป็นการเปิดช่องทางให้ผู้บุกรุกสามารถเข้าใช้งานระบบเครือข่ายได้ แฮกเกอร์ที่นั่งอยู่นอกอาคารสำนักงานสามารถเข้าถึงเน็ตเวิร์คของเราผ่านทางเครือข่ายไร้สาย ที่ไม่ได้เข้ารหัสหรือตั้งค่าเกี่ยวกับการตรวจสอบสิทธิ์ไว้ จากนั้นแฮกเกอร์สามารถเข้าถึง Share Folder ที่เราเผลอเปิดไว้โดยไม่ได้ตั้งรหัสผ่าน และในนั้นก็อาจมีข้อมูลสำคัญด้วย เป็นต้น นอกจากนี้วิธีการที่ถูกพบในปัจจุบัน ได้แก่ แมกแอดเดรสปลอม โรกเอพี โดยการปลอมเอสเอสไอดี (SSID) เพื่อดักรอข้อมูลชื่อผู้ใช้และรหัสผ่านที่ได้ จากนั้นนำไปล็อกอินเข้ากับระบบของโรงแรม และติดอุปกรณ์แจมเมอร์ (Jammer) ทำให้คลื่นเต็มจนทำให้ไม่สามารถเข้าใช้งานได้
๒. ท่านช่วยอธิบายแนวทางในการป้องกันการถูกโจมตีผ่านเครือข่ายระบบไร้สาย	(๑) การติดตั้งเอพีต้องพยายามกำจัดสัญญาณออกนอกพื้นที่ให้น้อยที่สุด เพื่อป้องกันผู้ไม่หวังดีจากภายนอกเข้ามาเจาะระบบ (๒) ควรกำหนดให้ใช้ระบบรักษาความปลอดภัยแบบดับเบิลยูพีเอสอง (WPA2) เป็นอย่างน้อย (๓) ควรมีระบบที่สามารถมอนิเตอร์ (Monitor) ผู้ใช้งานเพื่อตรวจสอบว่ามีการเข้าถึงจากอุปกรณ์ใดร่วมกับการตรวจสอบจากเอพี (๔) หากต้องการรักษาความมั่นคงปลอดภัยเพิ่มขึ้นอาจกำหนดให้เข้าถึงได้เฉพาะแมกแอดเดรสที่ลงทะเบียน (๕) กำหนดช่วงไอพีแอดเดรส (IP Address) ใหม่และอย่าใช้ ดีฟอลต์พาสเวิร์ด (Default Password) กับอุปกรณ์ต่าง ๆ (๖) การติดตั้งอุปกรณ์ดับเบิลยูไอดีเอส (WIDS) เพื่อตรวจสอบว่ามีโรกเอพีที่ไม่ได้รับการอนุญาตอยู่หรือไม่ (๗) attack surface นั่นคือช่องทางหรือพื้นที่ แฮกเกอร์สามารถทำงานได้

	กล่าวคือ ยิ่งมีบริการออนไลน์หลายรูปแบบ ยิ่งมีโอกาสเกิดช่องโหว่ได้มากขึ้นตาม สถาปัตยกรรมซีโร่ทรัสต์ (zero trust architecture) ยึดหลักการนี้ว่าต้องยืนยันตัวตนจนกว่าจะมั่นใจถึงจะยอมให้เข้าระบบได้ โดยอย่าเชื่ออะไรที่ยังไม่มีการตรวจสอบ (๘) การติดตั้งระบบระบุตัวตนของผู้ใช้งานควรใช้วิธีการยืนยันตัวตนด้วยระบบโอทีพี (OTP) ซึ่งจะส่งรหัสอ้างอิงไปที่เบอร์โทรศัพท์ก่อนเข้าใช้งานทุกครั้ง โดยมีระบบอ้างอิงเบอร์การโทรจากฐานข้อมูลลูกค้าที่ลงทะเบียนไว้ก่อนแล้ว (๙) อุปกรณ์สวิทช์ที่มีอุปกรณ์เอพีเชื่อมต่ออยู่ควรใช้ฟังก์ชั่นพอร์ตไอซะเลท (Port Isolation) สำหรับแยกไวไฟไคลเอนต์ (WiFi Client) ออกจากเน็ตเวิร์คหลักที่ใช้สายแลน
๓. ท่านเคยมีประสบการณ์ที่เกี่ยวข้องกับการถูกโจมตีผ่านระบบเครือข่ายไร้สายหรือไม่ เช่น Data Diddling (เป็นการปลอมแปลงเอกสารหรือปรับ เปลี่ยนเนื้อหาเอกสาร เพื่อประโยชน์ส่วนตน โดยไม่ได้รับอนุญาต)	(๑) ปัญหาการล๊อคอินเข้าเครือข่ายไร้สายไม่ได้ เกิดขึ้นโดยไม่ได้ตั้งใจจากลูกค้าซึ่งได้ทำการติดตั้งฟรีแอปพลิเคชั่น และมีมัลแวร์แฝงอยู่ในมือถือทำให้ไม่สามารถเชื่อมต่ออินเทอร์เน็ตของโรงแรมได้ (๒) ปัญหาหน้าล๊อคอินเข้าระบบเครือข่ายไร้สายไม่ปรากฏที่อุปกรณ์ของลูกค้า ซึ่งเกิดจากเกิดปัญหาแชนเนล (Chanel) ของเอพีชนกันเนื่องจากการติดตั้งเอพีในระบบเครือข่ายซึ่งมีคอนโทรลเลอร์ (Controller) คนละตัวกัน
๓.๑. จากข้อ ๓ ถ้าท่านมีประสบการณ์ดังกล่าว ท่านมีแนวทางในการป้องกันการถูกโจมตีอย่างไร	เพื่อแก้ไขปัญหาใช้งานไม่ได้เพราะเป็นแชนเนลเดียวกัน เจ้าของสถานที่ต้องเรียกประชุมผู้ให้บริการเช่น เอไอเอส ทรู ภายในพื้นที่มาร่วมกันออกแบบการกำหนดค่าของเอพีใหม่ทั้งหมด รวมถึงอุปกรณ์อื่น ๆ ที่เกี่ยวข้อง
๓.๒. จากข้อ ๓ ถ้าท่านมีประสบการณ์ดังกล่าว ท่านมีวิธีการ ปรับปรุง แก้ไข กู้คืนระบบติดตั้งระบบใหม่ หรือดำเนินการอย่างไร	ให้เจ้าของสถานที่ (Landlord) บริหารจัดการ และดำเนินการกับบริษัทที่ดูแลแต่ละอุปกรณ์เครือข่ายที่นำมาติดตั้ง เพื่อไม่ให้เกิดปัญหา
๔. หน่วยงานของท่านเคยประสบปัญหาถูกโจมตีผ่านระบบเครือข่ายไร้สายหรือไม่ ถ้ามีช่วยอธิบายเพิ่มเติม (ตัวอย่างการถูกโจมตีผ่านระบบเครือข่ายไร้สาย)	(๑) ลูกค้าพบการทำโรกเอพี จากผู้ไม่หวังดี และปัญหาแชนเนลของสัญญาณซ้ำกัน (๒) พนักงานนำอุปกรณ์ของบริษัทไปใช้ภายนอกสำนักงานทำให้มีความเสี่ยงต่อการติดไวรัสและทำให้องค์กรอาจถูกโจมตีได้ (๓) ปัญหาเกิดจากผู้ใช้งานขาดความตระหนักในด้านความมั่นคงปลอดภัย เช่น เข้าถึงไวไฟปลอม ผู้ใช้งานเปิดไวไฟฮอตสปอตทำให้แชนเนลชนกัน (๔) การทำแมคสปูฟิงแอทแทค (Mac spoofing attack) เพื่อแอบใช้ไวไฟฟรี
๔.๑. จากข้อ ๔ เมื่อเกิดปัญหาดังกล่าว หน่วยงานของท่านมีแนวทางในการป้องกันการถูกโจมตีอย่างไร	ให้ความรู้ และจัดทำข้อตกลง (Awareness) ในองค์กร เพื่อมีความพร้อมในการป้องกันในอนาคต โดยจัดทำระบบยืนยันตัวตนก่อนเข้าใช้งานไวไฟพร้อมทั้งจัดทำเอ็มเอฟเอ

๔.๒. จากข้อ ๔ เมื่อเกิดปัญหาดังกล่าว หน่วยงานของท่านมีการดำเนินการอย่างไรบ้าง	เปลี่ยนจากคาเปก (Capex) เป็นโอเปก (Opex) ถ้ามีผู้ใช้งานอุปกรณ์เคลื่อนที่เป็นจำนวนมากต้องมีการป้องกันให้ทั่วถึงโดยวิธีการการพิสูจน์ตัวตนการเข้าถึงระบบเครือข่ายหากพนักงานนำอุปกรณ์ของบริษัทไปใช้ที่บ้านวิธีการง่าย ๆ ควรเลือกใช้คลาวด์โซลูชั่น เนื่องจากยังไม่พบผลกระทบที่ร้ายแรง การดำเนินการจึงทำโดยให้ความรู้กับผู้ใช้ เพื่อให้เกิดความตระหนักถึงผลกระทบที่เกิดขึ้น
๕. ท่านมีคำแนะอื่นเพิ่มเติมอย่างไร?	การโจมตีเป็นสิ่งที่ควบคุมไม่ได้ แต่เราสามารถควบคุมช่องโหว่โดยดำเนินการตั้งแต่เลเยอร์ ๑-๗ และทำประจำอย่างต่อเนื่องพร้อมทั้งมีการตรวจสอบและทดสอบผลด้วย ปัจจุบันอุปกรณ์ไอโอที (IoT) เข้ามามีบทบาทต่อการใช้งานภายในองค์กรมากขึ้น จึงต้องปรับเปลี่ยนระบบไอที จากเดิมที่เป็นสายแลนเปลี่ยนเป็นไวไฟ เพื่อที่สามารถทำงานได้ทุกพื้นที่ภายในองค์กร โดยพนักงานสามารถทำงานจากที่บ้านได้อีกด้วย แต่ยังต้องคำนึงถึงความปลอดภัยในการใช้งานระบบเครือข่าย เพื่อให้อุปกรณ์เหล่านั้นสามารถใช้งานได้อย่างปลอดภัยและระบบยังสามารถทำงานได้อย่างมีประสิทธิภาพสิ่งสำคัญที่สุด คือ ผู้ใช้ต้องตระหนักช่วยป้องกันภัยคุกคามด้านความมั่นคงปลอดภัยไซเบอร์ได้พอสมควร ซึ่งการยืนยันตัวตนคนที่จะเข้าใช้งานจึงเป็นสิ่งที่ควรให้ความสำคัญเพื่อป้องกันคนที่ไม่มีสิทธิ์เข้าถึงระบบเครือข่าย การรักษาความปลอดภัยในการใช้งานด้านเครือข่ายต้องบริหารความสมดุลให้กับผู้ใช้และผู้ให้บริการบนพื้นฐานของซีไอเอ (CIA) นอกจากนี้ ไม่มีระบบความปลอดภัยใดดีที่สุด ดังนั้นจึงควรเรียนรู้ปรับปรุงระบบความปลอดภัยตลอดเวลาตามมาตรฐานของเอ็นไอเอสทีและมีระบบแบ็คอัพที่เหมาะสม

สรุปผลการวิจัย การอภิปรายผลการวิจัยและข้อเสนอแนะ

การสรุปผล

งานวิจัยนี้เป็นงานวิจัยเชิงคุณภาพโดยใช้การสัมภาษณ์เชิงลึกบนพื้นฐานแนวทางของเอ็นไอเอสทีและแดนนี่ มารีโค (๒๕๖๒) มาเป็นข้อคำถามในการสัมภาษณ์เชิงลึก เพื่อรวบรวมแนวทางป้องกันการโจมตีของเครือข่ายไร้สายของโรงแรม เพื่อนำมาเป็นแนวทางในการศึกษา ในปัจจุบันนี้สถานที่เกี่ยวข้องกับพระพุทธศาสนาได้ให้บริการระบบเครือข่ายไร้สายสำหรับพระและฆราวาส เพื่อนำมาสนับสนุนกิจกรรมทางด้านพระพุทธศาสนา และจากการทบทวนวรรณกรรมที่ผ่านมา เช่น ประชา เทศพานิช[๙] ยังไม่พบงานวิจัยที่กล่าวถึงการรักษาความมั่นคงปลอดภัยของเครือข่ายไร้สายในเขตพื้นที่พระพุทธสถาน ดังนั้นบทความวิจัยฉบับนี้ จึงได้นำเสนอแนวทางการป้องเครือข่ายไร้สายของโรงแรมเพื่อนำมาประยุกต์ใช้กับเขตพื้นที่พุทธสถานต่อไป โดยแบ่งออกเป็น

[๙] ประชา เทศพานิช, “แนวทางการพัฒนาจริยธรรมของผู้ประกอบกิจการโทรทัศน์ดาวเทียมในประเทศไทยเชิงพุทธบูรณาการ”, **วารสารบัณฑิตศึกษาปริทรรศน์,** ปีที่ ๑๖ ฉบับที่ ๒ (พฤษภาคม-สิงหาคม ๒๕๖๓) : ๑๔๐.

๑. แนวทางในการรักษาความมั่นคงปลอดภัยในเครือข่ายไร้สายคลอบคลุมทั้งหมด ๘ ด้าน ได้แก่

(๑) การรักษาความลับ (Confidentiality) โดยการกำหนดสิทธิ์ผู้ที่จะสามารถเข้าถึง และ พิสูจน์ตัวตนพร้อมทั้งกำหนดระดับการเข้ารหัส (Data Encryption) มีการใช้ทูเอฟเอและจำกัดโซนนิ่ง

(๒) ด้านความคงสภาพ (Integrity) โดยกำหนด Data permission, Data hashing มีสิทธิ์ในการเปิดข้อมูล ออกแบบให้ปลอดภัยและป้องกันไม่ให้ใครมาแทรกหรือเปลี่ยนแปลงข้อมูลในระหว่างทาง มีการเก็บข้อมูลให้ปลอดภัยในหน่วยงานที่มีสิทธิ์แก้ไข

(๓) ด้านความพร้อมใช้งาน (Availability) โดยข้อมูลต้องเข้าถึงได้ตลอดเวลาจากบุคคลที่มีสิทธิ์เท่านั้นผ่าน เอดี/เรเดียส ต้องจัดทำเอชเอ และถ้าระบบล้มเหลวเราสามารถทำตามแผนที่ได้วางไว้เพื่อกู้ข้อมูลหรือให้สามารถดำเนินการระบบต่อไปได้

(๔) ด้านการควบคุมการเข้าถึง (Access Control) โดยใช้แนคเข้ามาช่วยควบคุมผู้ใช้หรืออุปกรณ์โดยเปิดใช้งานเครือข่ายอัจฉริยะและการจัดการอุปกรณ์ไร้สาย ใช้การยืนยันตัวบุคคลก่อนเข้าสู่ระบบที่สามารถระบุตัวบุคคลได้ เพื่อความปลอดภัยควรใช้ทูเอฟเอ

(๕) แนวทางในการป้องกันการถูกโจมตีผ่านเครือข่ายระบบไร้สายทำการติดตั้งระบบดับเบิลยูไอดีเอส เพื่อตรวจสอบว่ามีการ Access package ที่ไม่ได้รับการอนุญาตอยู่หรือไม่ การติดตั้งเอพีต้องพยายามกำจัดสัญญาณออกนอกพื้นที่ให้น้อยที่สุดเพื่อป้องกันผู้ไม่หวังดีจากภายนอกเข้ามาเจาะระบบ และการทำตามสถาปัตยกรรมซีโร่ทรัสต์ยึดหลักการนี้ว่าต้องยืนยันตัวตนจนกว่าจะมั่นใจถึงจะยอมให้เข้าระบบได้ และสองเมื่อถูกโจมตีแล้วต้องจำกัดพื้นที่ (Attack Surface) ให้มากที่สุดเพื่อลดผลกระทบให้เล็กที่สุด เพิ่มการติดตั้งระบบระบุตัวตนของผู้ใช้งานและปิดการมองเห็นระหว่างไคเอนต์ (Client Isolate) ทำระบบยืนยันตัวตนที่เข้ามาใช้งานผ่านแนคและสามารถระบุชื่อผู้ใช้งานและอุปกรณ์ที่สามารถใช้งานในระบบได้ ซึ่งต้องมีระบบยืนยันตัวตันด้วยระบบโอทีพีส่งรหัสอ้างอิงไปที่เบอร์โทรศัพท์ก่อนเข้าใช้งานทุกครั้ง โดยมีระบบอ้างอิงเบอร์โทรจากฐานข้อมูลลูกค้าที่ลงทะเบียนไว้ ๑) ควรกำหนดให้ใช้ระบบรักษาความปลอดภัยแบบดับเบิลยูพีเอสเป็นอย่างน้อย ๒) ควรมีระบบที่สามารถเฝ้าระวังผู้ใช้งานเพื่อตรวจสอบว่ามีการเข้าถึงจากอุปกรณ์ใดร่วมกับการตรวจสอบจากเอพี ๓) หากต้องการความปลอดภัยเพิ่มขึ้นอาจกำหนดให้เข้าถึงได้เฉพาะแมกที่ลงทะเบียน ๔) กำหนดช่วงไอพีแอดเดรสใหม่และอย่าใช้ดีฟอลต์พาสเวิร์ดกับอุปกรณ์ต่าง ๆ เพิ่มเติมทำ Trust Device, เอ็มเอฟเอ, ทูเอ็มเอ

(๖) คำแนะนำในการตรวจสอบการถูกโจมตีและแสวงประโยชน์ผ่านช่องโหว่อย่างต่อเนื่อง โดยปกติแล้วหากเป็นการโจมตีทั่ว ๆ ไปเราจะทราบว่าถูกโจมตีเมื่อพบสิ่งผิดปกติ ซึ่งกรณีนี้เราสามารถกู้คืนระบบได้และคนโจมตีอาจไม่ได้สนใจถึงผลประโยชน์ในเชิงลึก แต่หากเป็นการโจมตีในลักษณะเอพีที่กรณีแบบนี้เรามักตรวจสอบลำบากหากไม่มีเครื่องมือคอยช่วยตรวจสอบ ซึ่งอาจใช้เซียมช่วยได้หรือ

หากเกี่ยวข้องกับข้อมูลควรมีเครื่องมือที่ช่วยทำ Data Protection หรือตรวจสอบจากรายงานจากในไอดีเอส/ไอพีเอส

(๗) แนวทางในการทดสอบการเจาะระบบและตรวจสอบช่องโหว่ของระบบ คือ การทดสอบเจาะระบบเหมือนกับการดำเนินการโดยแฮกเกอร์เพื่อประเมินความปลอดภัยความยากง่ายของการเจาะระยะเวลาและผลกระทบจากการโดนโจมตีพร้อมตรวจสอบช่องโหว่ของระบบเป็นการประเมินหาความเสี่ยงที่เกิดจากช่องโหว่ที่ค้นพบตามช่องโหว่ที่มีความเสี่ยง ซึ่งส่วนใหญ่แล้วเป็นความเสี่ยงที่ปรากฏต่อสาธารณะแล้วตามด้วยซีวีอี ซึ่งเป็นดัชนีที่รวบรวมรายชื่อช่องโหว่ด้านความปลอดภัยที่เป็นที่ทราบโดยทั่วกันซึ่งมี ๕ ขั้นตอนคือ (๑) ตรวจสอบความผิดปกติของอุปกรณ์ (๒) ตรวจสอบอุปกรณ์ไร้สายใกล้เคียง (๓) ตรวจสอบจุดเชื่อมต่อภายใน (๔) ทดสอบอุปกรณ์ภายใน (๕) ทดสอบพื้นฐานของเครือข่าย

(๘) การตรวจสอบการถูกโจมตีและแสวงหาประโยชน์ผ่านช่องโหว่อยู่เป็นประจำแล้วการประเมินผลเป็นระยะ โดยทำรายงานเป็น วัน, สัปดาห์ และเดือน เพื่อวิเคราะห์ดูว่ามีแนวทางป้องกันปัญหาเพียงพอหรือไม่เมื่อรวบรวมข้อมูลที่ได้มาจากการโจมตีและแสวงหาประโยชน์นั้นการตรวจสอบมักจะใช้รายการตรวจสอบตามมาตรฐาน หรือใช้เครื่องมือหรือสิ่งที่ควรตรวจสอบ ได้แก่ Information leak, Web Application, checklist DNS server, checklist E-mail Server, checklist Network Topology และ checklist Port services

๒. แนวทางในการรักษาความมั่นคงปลอดภัยในระบบเครือข่ายไร้สายในบริเวณเขตพื้นที่ใช้งานดังต่อไปนี้

(๑) ห้องพัก : นอกจากในห้องพักของโรงแรมมักจะมีการแบ่งโซนโดยใช้ไฟร์วอลล์แล้วควรมีการแบ่งวีแลนเพิ่มเติมเพื่อป้องกันการดักจับข้อมูลจากห้องพักใกล้เคียง ดังนั้น กุฏิหรือห้องพักในเขตพุทธสถานก็ควรมีการแบ่งวีแลนเช่นกัน และสิทธิ์การใช้งานควรอยู่ในแค่ในระดับผู้ใช้บริการ

(๒) พื้นที่ส่วนกลาง : ในเขตโรงแรมพื้นที่ส่วนนี้ควรที่จะถูกแบ่งให้อยู่ในโซนพื้นที่ส่วนกลาง (Public zone) ของไฟร์วอลล์ นอกจากนี้มีความจำเป็นต้องติดตั้งอุปกรณ์กระจายสัญญานให้คลอบคลุมพื้นที่ (Coverage Area) เพื่อรองรับการให้บริการแก่ลูกค้าอย่างทั่วถึง แต่ในเขตพุทธสถานควรจะมีเพียงแค่บางพื้นที่ตามความเหมาะสม สำหรับการพิสูจน์ตัวตนควรอนุญาตให้ทุกบัญชีรายชื่อสามารถใช้บริการได้ตามสิทธิ์ที่เหมาะสม

(๓) ห้องประชุม : ในเขตโรงแรมพื้นที่ส่วนนี้ควรที่จะถูกแบ่งให้อยู่ในโซนห้องประชุมของไฟร์วอลล์ นอกจากนี้มีความจำเป็นต้องออกแบบการติดตั้งอุปกรณ์กระจายสัญญานให้สามารถรองรับจำนวนผู้ใช้บริการ (High capacity) ได้อย่างเพียงพอ และวิธีการลงทะเบียนเพื่อสมัครใช้บริการต้องมีความสะดวกกว่าการใช้ในห้องพัก เช่น เป็นบัตรหรือคูปองที่กำหนดระยะเวลาการใช้งานในช่วงสั้น ๆ ห้องประชุมในเขตพุทธสถานก็ควรจะใช้แนวทางเดียวกัน

(๔) สำนักงาน : ในเขตโรงแรมพื้นที่ส่วนนี้ควรที่จะถูกแบ่งให้อยู่ในโซนสำนักงานของไฟร์วอลล์ และควรใช้ไฟร์วอลล์เพิ่มเติมเพื่อแยกระบบเครือข่ายออกเป็นส่วนอื่น ๆ นอกจากนี้ควรมีการแบ่งวีแลนของแต่ละแผนกเพิ่มเติมเพื่อป้องกันการดักจับข้อมูลจากแผนกอื่น สำหรับเรื่องของสิทธิ์ก็ควรมีเพียงแค่ผู้ดูแลและเจ้าหน้าที่ที่สามารถใช้งานในพื้นที่นี้ได้

(๕) กล้องวงจรปิด : ความปลอดภัยของแขกเป็นสิ่งสำคัญสูงสุดสิ่งหนึ่งสำหรับโรงแรม ซึ่งนอกเหนือจากการปกป้องและตรวจสอบทรัพย์สินแล้วกล้องวงจรปิดและระบบต่าง ๆ ที่เชื่อมต่อกับไวไฟ จำเป็นต้องมีการออกแบบอย่างเหมาะสม เพื่อความมั่นคงปลอดภัยของระบบกล้องวงจรปิดควรที่จะแยกเครือข่ายออกจากระบบเครือข่ายไร้สายที่ให้บริการแก่ผู้พักทั่วไปโดยการแบ่งวีแลนที่อุปกรณ์สวิทซ์ สำหรับเรื่องของสิทธิ์ก็ควรมีเพียงแค่ผู้ดูแลและเจ้าหน้าที่ที่สามารถใช้งานในพื้นที่นี้ได้ ซึ่งในเขตพุทธสถานก็ต้องคำนึงถึงเช่นกันเพื่อความปลอดภัย

(๖) อุปกรณ์ ไอโอที : ปัจจุบันนี้ลูกค้านิยมนำอุปกรณ์ไอโอทีมาเชื่อมต่อผ่านเครือข่ายไร้สายกับอุปกรณ์ในโรงแรม ซึ่งอาจจะเป็นจุดอ่อนในการถูกโจมตีจากภายนอก ดังนั้นทางโรงแรมจึงต้องคำนึงถึงการออกแบบระบบการเชื่อมต่อให้มีความปลอดภัยมั่นคง เพื่อสามารถอำนวยความสะดวกให้กับลูกค้าได้อย่างปลอดภัย เนื่องจากอุปกรณ์เหล่านี้ส่วนใหญ่แล้วจะมีการอนุญาตให้เข้าใช้ระบบเครือข่ายผ่านการใช้หมายเลขแมคแอดเดรสทำให้ไม่การพิสูจน์ตัวตนในระบบแอพพลิเคชั่น ดังนั้นจึงมีความเสี่ยงแต่ถ้าได้มีการแบ่งวีแลนในห้องพักอาศัยแล้วก็จะลดความเสี่ยงลงได้ ซึ่งในเขตพุทธสถานก็ควรที่จะใช้แนวทางในการป้องกันเหมือนกัน

การอภิปรายผลการวิจัย

จากตารางที่ ๒ ในข้อที่ ๒ ผู้เชี่ยวชาญได้ให้คำแนะนำว่าให้ติดตั้งระบบดับเบิลยูไอดีเอส ซึ่งสอดคล้องกับมาตรฐานของโฮมแลนด์ ซีคิวริตี้[๑๐] โดยทำหน้าที่เฝ้าระวังรวมถึงการตรวจสอบโรกเอพี และการเชื่อมต่อที่ไม่ผ่านการระบุตัวตน นอกจากนี้การใช้ฟังก์ชันพอร์ตไอโซเลชั่น (Port Isolation) ตามคำแนะนำของผู้เชี่ยวชาญได้สอดคล้องกับ ศุภเดช สุทธิพงศ์คณาสัย[๑๑] เพื่อความมั่นคงปลอดภัย และลดบรอดแคสต์แพ็คเก็ต (Broadcast Packet) สำหรับสถาปัตยกรรมซีโร่ทรัสตามคำแนะนำของผู้เชี่ยวชาญได้สอดคล้องกับ วิโรจน์ จ้อยประเสริฐ[๑๒] เป็นการออกแบบระบบเครือข่ายโดยยึดข้อมูลเป็นศูนย์กลาง (Data-centric

---

[๑๐] Homeland Security, “A Guide to Securing Networks for Wi-Fi (IEEE 802.11 Family)”, **Department of Homeland Security Cybersecurity Engineering**, Version 1.0 (2017) : 4-5.

[๑๑] ศุภเดช สุทธิพงศ์คณาสัย, **Rogue AP..Access Point จำแลงแปลงกายมาดักข้อมูล,** [ออนไลน์], แหล่งที่มา: https://www.catcyfence.com/it-security/article/rogue-access-point/ [๒๔ มกราคม ๒๕๖๐].

[๑๒] วิโรจน์ จ้อยประเสริฐ, **๕ ข้อหลัก Zero Trust ต้องไม่เชื่อและตรวจสอบก่อนเสม,** [ออนไลน์], แหล่งที่มา: https://www.catcyfence.com/it-security/article/5-element-of-zero-trust [๑๒ พฤษภาคม ๒๕๖๓].

Network) และมีการวางมาตรการควบคุมโดยรอบข้อมูลหรือทรัพย์สินสารสนเทศเหล่านั้น เพื่อให้สามารถกำหนดและบังคับใช้นโยบายด้านความมั่นคงปลอดภัยในการเข้าถึงข้อมูลได้ทั้งหมด แนวคิดนี้ช่วยให้สามารถตรวจจับและป้องกันแฮกเกอร์ที่แทรกซึมเข้ามายังระบบเครือข่ายและป้องกันข้อมูลรั่วไหลสู่ภายนอกได้ดียิ่งขึ้นกว่าในอดีต โดยกูลเกิ้ล (Google) ได้เสนอแนวคิดการรักษาความมั่นคงปลอดภัยในปัจจุบันมาทั้งหมด ๕ รูปแบบ ดังนี้ (๑) ความน่าเชื่อถือของอุปกรณ์ (๒)ความน่าเชื่อถือของผู้ใช้ (๓) การอนุญาตให้มีสิทธิ์เข้าถึงทรัพยากรให้น้อยที่สุด (Transport / Session Trust) (๔) ความน่าเชื่อถือของแอปพลิเคชั่น (๕) ข้อมูลเป็นสิ่งที่มีความสำคัญสูงสุด (Data Trust)

จากตารางที่ ๒ ในข้อที่ ๔ ผู้เชี่ยวชาญได้ให้คำแนะนำว่าควรมีการฝึกอบรม หรือสัมมนาเพื่อให้คนในองค์กรเกิดความตระหนักรู้ถึงอันตรายจากภัยคุกคามไซเบอร์ (Cyber Awareness) ในองค์กร เพื่อมีความพร้อมในการป้องกันในอนาคต โดยจัดทำระบบยืนยันตัวตนก่อนเข้าใช้งานไวไฟพร้อมทั้งจัดทำเอฟเอ็มเอ[๑๓]

ข้อเสนอแนะสำหรับการวิจัยครั้งต่อไป

ควรมีการสัมภาษณ์เชิงลึกจากกลุ่มผู้ดูแลระบบความมั่นคงปลอดภัยกับในโรงแรมเพิ่มเติมและควรมีการจัดกลุ่มสนทนาเฉพาะประเด็น (Focus Group) เพิ่มเติม เพื่อต่อยอดแนวทางการนำเสนอให้กลายเป็นกรอบแนวคิดที่สมบูรณ์ (Framework) เพื่อนำแนวทางไปพัฒนากับเขตพื้นที่พุทธสถานต่อไป

บรรณานุกรม

ประชา เทศพานิช. “แนวทางการพัฒนาจริยธรรมของผู้ประกอบกิจการโทรทัศน์ดาวเทียมใน ประเทศไทยเชิงพุทธบูรณาการ”. **วารสารบัณฑิตศึกษาปริทรรศน์.** ปีที่ ๑๖ ฉบับที่ ๒ (พฤษภาคม - สิงหาคม ๒๕๖๓) : ๑๔๐.

พระมหาเอก เมธิกญาโณ เจตสลัน. “พฤติกรรมการใช้สื่อสังคมออนไลน์ ของพระนิสิตระดับปริญญาตรี มหาวิทยาลัยมหาจุฬาลงกรณราชวิทยาลัย อำเภอวังน้อย จังหวัดพระนครศรีอยุธยา”. **วารสารมหาจุฬาวิชาการ**. ปีที่ ๗ ฉบับที่ ๒ (พฤษภาคม-สิงหาคม ๒๕๖๓) : ๑๗๙-๑๙๐.

Anastasia Atavina V., Zareshin Sergei V., Rumyantseva Irina S., Ivanenko Vitaliy G. “Analysis of Security of Public Access to Wi–Fi Networks on Moscow Streets”**.** Russian: **IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus)**. (2017). 105-110.

[๑๓] Optimus Thailand, **ทำความรู้จัก Multi-factor Authentication หรือ AuthPoint Mobile App,** [ออนไลน์], แหล่งที่มา: https://optimus.co.th/multi-factor-authentication-authpoint-mobile-app [16 July 2020].

Benqdara Salima, Mahmoud Abdelfattah. “Wireless Security in Libya: A Survey Paper”. **International Journal of Computer Applications**. Vol. 181 No. 35 (2019) : 26-31.

Frankel Sheila, Eydt Bernard, Les Owens, Scarfone Karen. **Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i.** Special Publication 800-97. National Institute of Standards and Technology (NIST). 2007.

Homeland Security. **A Guide to Securing Networks for Wi-Fi (IEEE 802.11 Family).** Department of Homeland Security Cybersecurity Engineering. Version 1.0, (2017) : 4-5.

Murugiah Souppaya, Karen Scarfone. **Guidelines for Securing Wireless Local Area Networks (WLANs).** Special Publication 800-153. National Institute of Standards and Technology (NIST). (February 2012) : 1-12.

Mohmmed Somya Khidir, Al Mostafa Ahmed Hassan. “A review of threats, protocols, and solutions to enhance the security of wireless networks”. **IJCSNS International Journal of Computer Science and Network Security**. Vol.19 No.4 (2019) : 108-115.

วิโรจน์ จ้อยประเสริฐ. **๕ ข้อหลัก Zero Trust ต้องไม่เชื่อและตรวจสอบก่อนเสมอ.** [ออนไลน์]. แหล่งที่มา: https://www.catcyfence.com/it-security/article/5-element-of-zero-trust. [๑๒ พฤษภาคม ๒๕๖๓].

ศุภเดช สุทธิพงศ์คณาสัย. **Rogue AP..Access Point จำแลงแปลงกายมาดักข้อมูล.** [ออนไลน์]. แหล่งที่มา: https://www.catcyfence.com/it-security/article/rogue-access-point/ [๒๔ มกราคม ๒๕๖๐].

Mareco Danny. **6 Ways Hotel Wi-Fi Is About More than Providing In-Room Guest Access.** [Online]. Available: https://www.securedgenetworks.com/blog/hotel-wifi-is-about-more-than-in-room-guest-access. [23 March 2018].

Optimus Thailand. **ทำความรู้จัก Multi-factor Authentication หรือ AuthPoint Mobile App.** [ออนไลน์]. แหล่งที่มา: https://optimus.co.th/multi-factor-authentication-auth-point-mobile-app, [16 July 2020].

Singh Rajeev and Parval Sharma Teek. **Security in Wireless Local Area Networks (WLANs).** [Online]. Available: https://www.intechopen.com/books/computer-and-network-security/security-in-wireless-local-area-networks-wlans- [2019].