ปัจจัยที่มีผลต่อการตระหนักถึงภัยคุกคามทางไซเบอร์ของชุมชน ตำบลบ้านโปร่ง อำเภอหนองโดน จังหวัดสระบุรี

Factors affecting the awareness of cyber threats in Ban Prong Subdistrict, Nong Don District, Saraburi Province

รุ่งเรืองกิจ วงษ์ที
Rungruangkit Wongtee
มหาวิทยาลัยราชภัฏเทพสตรี
Thepsatri Rajabhat University
Email: wongtee @gmail.com
Received February 15, 2022 & Revise April 20, 2022 & Accepted June 30, 2022

บทคัดย่อ

การศึกษาวิจัยนี้ มีวัตถุประสงค์เพื่อศึกษาปัญหาของภัยคุกคามทางไซเบอร์ของชุมชน ตำบลบ้านโปร่ง อำเภอหนองโดน จังหวัดสระบุรี โดยผู้วิจัยรวบรวมความเห็นจากกลุ่มตัวอย่างจำนวน 180 คน และนำกลับมาวิเคราะห์ผลด้วยสถิติวิเคราะห์ค่าความถี่ ร้อยละ ผลวิจัยพบว่า การศึกษาปัญหาของภัยคุกคามทางไซเบอร์ของชุมชน ตำบลบ้านโปร่ง อำเภอหนองโดน จังหวัดสระบุรี ค่าเฉลี่ยอยู่ในระดับมากทุกองค์ประกอบ ทั้งในด้านความปลอดภัยการเข้าใช้งานอินเตอร์เน็ต ด้านการป้องกันข้อมูล

คำสำคัญ ปัจจัยที่มีผลต่อการตระหนักถึงภัยคุกคามทางไซเบอร์, ชุมชน ตำบลบ้านโปร่ง อำเภอหนองโดน จังหวัดสระบุรี

Abstract

This research aimed to study the problem of cyber threats in Ban Prong Sub-district, Nong Don District, Saraburi Province. The researcher collected opinions from 180 sample groups and analyzed the results using statistics to analyze frequency, percentage, mean, The research results found that the study of the problem of cyber threats in Ban Prong Sub-district, Nong Don District, Saraburi Province showed that the mean was at a high level in all components, both in terms of internet access security and data protection.

Keywords Factors affecting awareness of cyber threats, Ban Prong Sub-district Community, Nong Don District, Saraburi Province

บทนำ

ในปัจจุบันที่อินเทอร์เน็ต (Internet) เป็นเสมือนปัจจัยที่ 5 ของการดำเนินชีวิตของ มนุษย์ทั่วโลกไม่เว้นแม้แต่คนไทย ทั้งนี้ผลการสำรวจล่าสุดของ We Are Social (2016) ดิจิทัลเจน ชื่อดังของประเทศสิงค์โปร ได้ออกรายงานชื่อ Digial in 2016 ซึ่งมีสถิติเกี่ยวกับพฤติกรรมการใช้อินเทอร์เน็ตของคนไทยพบว่า ในกลุ่มประชากรคนไทยทั้งหมด 68.05 ล้านคนนั้น เป็นผู้ใช้อินเทอร์เน็ตมากกว่าครึ่งหนึ่ง หรือประมาณ 38 ล้านคน โดยทั้งหมดนั้นใช้สื่อสังคมออนไลน์ (Social Media) โดยมีจำนวนหมายเลขโทรศัพท์เคลื่อนที่ซึ่งเปิดใช้งานถึง 82.78 ล้านคนซึ่งมากกว่าจำนวน ประชากรทั้งหมด และมีผู้ใช้สื่อสังคมออนไลน์ผ่านโทรศัพท์เคลื่อนที่ถึง 34 ล้านคน

เครือข่ายอินเทอร์เน็ตและเครือข่ายสื่อสังคมออน ไลน์ทั่วโลกและในประเทศไทยพบการกระทำที่เป็นการคุกคามมากมาย เช่น การปลอมอินสตราแกรม ของ หญิง รฐา โพธิ์งามและแตงโม นิดา พัชรวีระพงษ์เพื่อนำไปขายสินค้าหรือรับงานโชว์ตัวโดยหลอกผู้เสียหายมากมาขถึงพันกว่ารายรวมมูลค่าความเสียหายหลายรายหลายล้านบาท (ไทยรัฐออนไลน์, 2560) นอกจากนั้นยังมีการขโมยตัวตน (dentity Thet) ซึ่งการขโมยตัวตนในโลกออนไลน์นั้นมักจะทำร่วมกับสิ่งที่ไม่ชอบมาพากลอื่น ๆ เช่น การปลอมแปลงเว็บไซต์เพื่อที่จะหลอกคักข้อมูลชื่อผู้ใช้และรหัสผ่านจากผู้ใช้แล้วนำข้อมูลที่ได้มาปลอมแปลงอีกครั้ง เพื่อนำไปหลอกลวงผู้ใช้งานอื่น ๆ อีกทอดหนึ่งไปจนถึงการทำให้ได้รับความเสื่อมเสียชื่อเสียง อับอาย และเสียทรัพย์สินหรือตกเป็นผู้ต้องสงสัยในคดีอาญา บางกรณีบรรดาแฮกเกอร์ก็ใช้วิธีการคาดเคารหัสผ่านที่มีคาดเดาได้ง่าย ซึ่งก็เป็นอีกวิธีที่ทำให้ผู้ใช้บริการถูกขโมยตัวตนทางออนไลน์ไปใช้แบบไม่รู้ตัว เช่น ตั้งรหัสจากตัวเลข วัน/เดือน/ปีเกิดหรือจะเป็นกรณีการละเลยจากตนเองปล่อยให้มีการเข้าสู่ระบบ (Login)คอมพิวเตอร์ในเว็บไซต์ต่าง ๆ ทิ้งไว้ในร้านคอมพิวเตอร์หรือคอมพิวเตอร์สาธารณะ โทรศัพท์มือถือและเมื่อมีผู้ไม่ประสงค์ดีมาพบข้อมูลของเราก็จะถูกขโมยไปต่อเนื่องไปจนถึงการถูกสวมรอยเพื่อเข้าถึงบัญชีธนาคารหรือการทำธุรกรรมที่ผิดกฎหมาย

ปัจจุบันจำนวนประชากรของชุมชน ตำบลบ้านโปร่ง อำเภอหนองโดน จังหวัดสระบุรี ทั้งหมด2,377 คน แยกเป็นชาย 1,137 คนคิดเป็นร้อยละ 47.83 หญิง 1,240 คน คิดเป็นร้อยละ 52.17จำนวนครัวเรือนทั้งหมด 1,047 ครัวเรือนคิดเป็นร้อยละ 52.17 หญิง 1,240 คน ความหนาแน่นเฉลี่ย 1,225.26 คน/ตารางกิโลเมตร ยังมีที่ผู้ที่ตกเป็นเหยื่อ (Victims) จากการ ถูกโจมตีหรือจากภัยคุกคามเหล่านั้นเพิ่มขึ้นอย่างรวดเร็วเพราะขังขาดความรู้และวิธีป้องกันภัยคุกคามทางไซเบอร์ การโจมตีบนโลกไซเบอร์ถูกออกแบบมาเพื่อสร้างความเสียหายในการแสวงหาผลประโชชน์จากการคุกคามเป็นหลัก ซึ่งรูปแบบการโจมตีที่หลากหลายบวกกับการพัฒนาของเทคโนโลยีขั้นสูง จึงก่อให้เกิดอาชญากรรมไซเบอร์ (Cyber Crime) และอาชญากรรมอื่นๆ ที่เชื่อมโยงออกไปไม่จบไม่สิ้น

ดังนั้นผู้วิจัยจึงศึกษาปัจจัยที่มีผลต่อการตระหนักถึงภัยคุกคามทางไซเบอร์ของชุมชน ตำบลบ้านโปร่ง อำเภอหนองโดน จังหวัดสระบุรี การกำหนดกรอบทิศทาง หลักการใน การบริหารจัดการเพื่อให้เกิดความมั่นคงปลอดภัยไซเบอร์และแนวปฏิบัติที่ดี (Best Practice) อย่างมี ประสิทธิภาพ ตลอดจนกระบวนการหรือการกระทำทั้งหมดที่จำเป็นเพื่อทำให้ประชากรของชุมชน ตำบลบ้านโปร่ง อำเภอหนองโดน จังหวัดสระบุรี

ปราศจากความเสี่ยง และความเสียหายจากการแฮกข้อมูล โดยเลือกศึกษาภัยการคุกคามทางไซเบอร์เพื่อนำไปวิเคราะห์เตรียมแผนการรับมือและเฝ้าระวังภัยคุกคามทางไซเบอร์ในองค์กร

วัตถุประสงค์ของการวิจัย

1. เพื่อให้เกิดความมั่นคงปลอดภัยไซเบอร์และแนวปฏิบัติที่ดี
2. เพื่อนำไปวิเคราะห์เตรียมแผนการรับมือและเฝ้าระวังภัยคุกคามทางไซเบอร์ในองค์กร

สมมุติฐานการวิจัย

1. เพื่อทำความเข้าใจเกี่ยวกับปัญหาของภัยคุกคามทางไซเบอร์ของชุมชน ตำบลบ้านโปร่งอำเภอหนองโดน จังหวัดสระบุรี

2. ปัญหาในช่วงการคุกคามทางไซเบอร์ของชุมชน ตำบลบ้านโปร่งอำเภอหนองโดน จังหวัดสระบุรี

3. วิธีการดูแลรักษาความปลอดภัยของระบบให้มีประสิทธิภาพภายในชุมชน ตำบลบ้านโปร่งอำเภอหนองโดน จังหวัดสระบุรี

เอกสารและงานวิจัยที่เกี่ยวข้อง

การศึกษา เรื่อง การศึกษาปัจจัยที่มีผลต่อการตระหนักถึงภัยคุกคามทางไซเบอร์ของชุมชน ตำบลบ้านโปร่งอำเภอหนองโดน จังหวัดสระบุรี ผู้วิจัยได้แนวคิดทฤษฎีและงานวิจัยที่เกี่ยวข้องต่างๆ มาใช้เป็นแนวทางในการศึกษาวิจัยดังต่อไปนี้

แนวคิดเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security)

สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช. หรือ NSTDA) ให้ความหมายของ ไซเบอร์ (Cyber) ว่าเป็น คำที่กร่อนมาจากคำว่าไซเบอร์เนติกส์ (Cybernetics) และมีความหมายว่าเกี่ยวข้องกับระบบเครือข่ายและสังคมเครือข่ายสากลทั่วโลก เช่น ระบบอินเทอร์เน็ต(Internet) และยังมีการให้ความหมาย "สารสนเทศ (Virtual) เสมือนจริงที่ถูกสร้างขึ้นหรือเกิดขึ้นเอง" (www.nstda.or.th, 2557)

โดยรวมแล้ว Cyber- จึงเป็นความหมายในเชิงนามธรรม หมายถึง ขอบเขตที่เกี่ยวข้องกับการใช้งานของระบบเครือข่ายคอมพิวเตอร์หรือระบบอิเล็กทรอนิกส์ ซึ่งจะครอบคลุมมากกว่าคอมพิวเตอร์ ซึ่งมีความหมายในเชิงรูปธรรมของอุปกรณ์ระบบคอมพิวเตอร์หัวเตอร์ที่ไป

ตามพจนานุกรม Cyberspace Operations Lexicon ของกระทรวงกลาโหมสหรัฐอเมริกา กำหนดให้ Cyber Security คือ กระบวนการหรือการกระทำทั้งหมดที่จำเป็น เพื่อทำให้องค์กรปราศจากความเสี่ยง และความเสียหายที่มีผลต่อความมั่นคงปลอดภัยของข้อมูลข่าวสารในทุกรูปแบบ (ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ) ความมั่นคงปลอดภัยของระบบและเครือข่ายที่ใช้ในการเก็บ เข้าถึง ประมวลผล และกระจายข้อมูล ทั้งนี้ Cyber Security ยังรวมถึงการระวังป้องกันต่อการอาชญากรรม การโจมตี การบ่อนทำลาย การจารกรรม อุบัติเหตุ และความผิดพลาดต่าง ๆ(www.enwikipedia.org, 2557)

ความเสี่ยงของ Cyber Security อาจรวมถึงสิ่งต่าง ๆ ที่ทำลายความเชื่อมั่นและความไว้วางใจของผู้มีส่วนได้เสีย (Stakeholder) ผลกระทบที่มีต่อการเก็บรักษาและการเติบโตของกลุ่มลูกค้า การละเมิดการป้องกันข้อมูลส่วนตัวของกลุ่มลูกค้าและผู้ถือหุ้น การรบกวนการทำงานหรือการดำเนินธุรกรรม ผลกระทบที่เป็นปฏิปักษ์ต่อชีวิตและสุขภาพของผู้ปฏิบัติงาน และผลกระทบที่ส่งผลต่อโครงสร้างระบบสาธารณูปโภคที่สำคัญของชาติ

แนวคิดเกี่ยวกับการคุกคามทางไซเบอร์ (Cyber Threat)

การคุกคามทางไซเบอร์สามารถเกิดขึ้นได้หลายรูปแบบ แต่ละรูปแบบสามารถสร้างความเสียหายให้แก่บุคคล เศรษฐกิจ ไปจนถึงโครงสร้างพื้นฐานของประเทศต่าง ๆ ภัยคุกคามอาจเป็นการก่อวินาศกรรม การจารกรรมข้อมูลหรือรหัสสำคัญ การปล่อยข้อมูลมูลวง การทำลายชื่อเสียงของของประเทศ องค์กร หรือบุคคล การเผยแพร่ข่าวสารอันเป็นเท็จ รวมถึงการทำลายระบบปฏิบัติการของเซิร์ฟเวอร์ คอมพิวเตอร์ส่วนบุคคล และอุปกรณ์เคลื่อนที่ เช่น แท็บเล็ต หรือโทรศัพท์แบบสมาร์ตโฟนเป็นต้น

1 ประเภทของการเกิดภัยคุกคามทางไซเบอร์

ภัยคุกคามทางไซเบอร์ สามารถแบ่งออกเป็น 5 กลุ่ม ดังนี้

1. ภัยคุกคามที่เกิดจากการใช้โปรแกรมประยุกต์โปรมภรมประยุกต์ (application-based threats) ที่ถูกดาวรโหลดดดมาเพื่อตั้งบคอมพิวเตอร์ หรืออุปกรณ์เคลื่อนที่ อาจจะถูกแอบแฝงมาด้วยโปรแกรมที่เป็นภัยคุกคาม ภัยคุกคามประเภทนี้เรียกว่า มัลแวร์ (malware) ซึ่งเป็นโปรแกรมที่ถูกออกแบบมาเพื่อทำอันตรายต่อข้อมูลในคอมพิวเตอร์ หรืออุปกรณ์เคลื่อนที่ ทำให้เกิดความขัดข้องหรือเสียหายกับระบบปฏิบัติการ นอกจากนี้โปรแกรมที่ติดมัลแวร์ยังส่งข้อความที่ไม่พึงประสงค์ออกไปยังผู้อื่น หรือขโมยข้อมูลสำคัญออกไปตัวอย่างโปรแกรมในกลุ่มนี้ ได้แก่ Virus, Worm, Trojan, Botnet หรือ Spyware เป็นต้น

2. ภัยคุกคามที่เกิดจากการใช้งานเว็บไซต์ภัยคุกคามที่เกิดจากการใช้งานเว็บไซต์ (web-based threats) เป็นภัยคุกคามที่เกิดจากการที่ผู้ใช้คอมพิวเตอร์ หรืออุปกรณ์พกพา เปิดเว็บไซต์ขึ้นมาใช้งาน ซึ่งเว็บไซต์ที่เรียกมาใช้อาจเป็นเว็บไซต์ฟิชชิ่ง (Phishing) ซึ่งถูกออกแบบให้มีลักษณะคล้ายคลึงกับเว็บไซต์จริงเพื่อหลอกให้ผู้ใช้กรอกข้อมูลเข้าสู่ระบบของผู้ไม่หวังดี เช่น หลอกให้ผู้ใช้งานล็อกอินเข้าอีเมล เฟซบุ๊ก หรือเว็บไซต์ที่เกี่ยวข้องกับธุรกรรมทางการเงิน ซึ่งจะคอยดักจับรหัสล็อกอินของผู้ใช้งานนั้น ๆ ทำให้ข้อมูลหรือบัญชีการใช้งานนั้น ๆ มีความเสี่ยงที่จะโดนขโมยข้อมูลออก

3. ภัยคุกคามจากการใช้งานเครือข่ายไร้สายปัจจุบันมีผู้ให้บริการเครือข่ายไร้สายเป็นจำนวนมาก มีทั้งที่น่าเชื่อถือและที่ไม่น่าเชื่อถือรวมถึงผู้ที่แอบแฝงเพื่อวัตถุประสงค์อื่น ดังนั้นผู้ใช้คอมพิวเตอร์ หรืออุปกรณ์เคลื่อนที่เชื่อมต่อระบบเครือข่ายไร้สายต่าง ๆ อาจได้รับผลกระทบโดยตรง รวมถึงยังสามารถเป็นต้นตอของผลกระทบไปยังอุปกรณ์คอมพิวเตอร์ หรืออุปกรณ์เคลื่อนที่ของผู้อื่นด้วยเช่นกัน โดยผู้ใช้เครือข่ายไร้สายอาจถูกโจมตีด้วยมัลแวร์ผ่านข้อบกพร่องของระบบปฏิบัติการ และถูกเปลี่ยนสถานะมาเป็นผู้โจมตีโดยการส่งต่อหรือแพร่กระจายมัลแวร์เหล่านี้ไปยังอุปกรณ์อื่นผ่านเครือข่ายไร้สาย หรือบลูทูธ นอกจากนี้การใช้เครือข่ายไร้สายยังเปิดโอกาสให้ผู้ไม่ประสงค์ดีดักจับข้อมูลสำคัญ หรือรหัสผ่านบนเครือข่ายไร้สายได้อีกด้วย

4. ภัยคุกคามที่เกิดจากการถูกโจมตีแบบเจาะจงเป้าหมายภัยคุกคามที่เกิดการโจมตีแบบเจาะจงเป้าหมาย (targeted attack) ที่มาจากหลายประเทศมีมากขึ้น ผู้โจมตี หรือแฮกเกอร์ (hackers) ในประเทศต่าง ๆ จะใช้การโจมตีแบบเจาะจงเป้าหมายอย่างต่อเนื่อง สร้างความเสียหายให้แก่โครงสร้างพื้นฐาน สถาบันการเงิน และองค์กรอื่น ๆของภาครัฐ และภาคเอกชนในหลายประเทศ อาชญากรไซเบอร์เหล่านี้จะใช้มาตรการที่รวดเร็วและรุนแรงในการโจรกรรมข้อมูล ภัยคุกคามประเภทนี้จัดว่า เป็นภัยคุกคามที่กระทบต่อความมั่นคงของประเทศเป็นอย่างยิ่ง

2.3.2 ประเภทของผู้คุกคามทางไซเบอร์

ผู้คุกคามทางโซเบอร์ หรือกลุ่มบุคคลและ/หรือองค์กรที่มีความชำนาญในกรปฏิปฏิบัติการภัยใซเบอร์สามารถแบ่งออกเป็น 5 กลุ่ม (นงรัตน์ สายเพชร, 2556) ดังนี้

1. ประเทศที่มีความประสงค์ร้ายกลุ่มนี้ ได้แก่ รัฐบาลของบางประเทศที่มุ่งโจมตีกลุ่มงานความมั่นคงหรือกองทัพ โดยมีจุดมุ่งหมายที่จะสร้างความเสียหายให้เกิดขึ้น กับประเทศเป้าหมาย ซึ่งอาจเป็นการก่อกวนเว็บไซต์ของหน่วยงานต่าง ๆ การจารกรรมข้อมูลสำคัญ รวมถึงการสร้างความเสียหายให้กับโครงสร้างพื้นฐานของประเทศเป้าหมาย

2. ผู้ก่อการร้ายกลุ่มนี้ ได้แก่ ผู้ก่อการร้ายหรือผู้ไม่หวังดี ซึ่งมีจุดประสงค์ที่จะทำลายผลประโยชน์ของชาติเป้าหมาย กลุ่มผู้ก่อการร้ายเหล่านี้ใช้ไซเบอร์เป็นช่องทางการสื่อสาร โดยจะสร้างแบบแผนเพื่อหาเงินทุนหรือเพื่อเผยแพร่แนวความคิดที่เป็นภัยต่อประเทศเป้าหมาย

3. สายลับภาคเอกชน/องค์กรอาชญากรรมกลุ่มนี้ ได้แก่ สายลับภาคเอกชน หรือองค์กรอาชญากรรมซึ่งมีการใช้เบอร์เป็นช่องทางในการบุกรุก และโจมตีระบบ โดยมีเป้าหมายเพื่อจารกรรมข้อมูลสำคัญ รวมถึงทรัพย์สินจากองค์กรภาครัฐ และภาคเอกชนต่าง ๆ กลุ่มนี้อาจเป็นกลุ่มปฏิบัติการของหน่วยงานความมั่นคงของบางประเทศ หรืออาจเป็นเพียงอาชญากรที่ต้องการนำช้อสำชัลสำคัญไปหารายได้

4. แฮกเกอร์กลุ่มแฮกเกอร์ (hackers) คือ กลุ่มผู้ที่พยายามหาช่องโหว่ของระบบ ลักลอบเจาะเข้าสู่ระบบเพื่ออ่านข้อมูลข่าวสาร เพื่อขโมย หรือเพื่อทำลายข้อมูลข่าวสารสำคัญเหล่านั้น ซึ่งจะทำให้เกิดความเสียหายแก่องค์กรเป้าหมาย แฮกเกอร์สามารถมาได้จากประเทศต่าง ๆ ทั่วโลก การป้องกัน หรือการสืบหาตัวผู้กระทำความผิดค่อนข้างยาก

5. แฮกทิวิสกลุ่มแฮกทิวิส (hacktivists) คือ กลุ่มแฮกเกอร์ที่มีแรงจูงใจทางการเมือง เป็นกลุ่มที่ต้องการผลักดันให้เกิดความเปลี่ยนแปลงทางการเมือง กลุ่มนี้มุ่งเน้นที่จะนำเสนอแนวคิดผ่านทางไซเบอร์ และสร้างมูลเหตุที่ส่งผลต่อการเมืองและสังคมมากกว่าการสร้างความเสียหายให้กับโครงสร้างพื้นฐาน

2.3.3 ประเภทของภัยคุกคามทางไซเบอร์

หน่วยงาน The European Computer Security Incident Response Team (eCSIRT)ซึ่งเป็นเครือข่ายความร่วมมือของหน่วยงาน CSIRT ในสหภาพยุโรปได้จำแนกตามประเภทของภัยคุกคามทางไซเบอร์

ออกเป็น 10 ประเภท ดังนี้ (ไทยเซิร์ต, "การตรวจจับภัยคุกคามและอาชญากรรมไซเบอร์ในประเทศไทย", 2556)

1. บอตเน็ต (Botnet) คือ โปรมไม่ไม่พึงประสงค์ติดตั้งอยู่ในคอมพิวมพิวเตอร์ซึ่งสามารถโจมตีได้โดยอัตโนมัติ หรือรับคำสั่งจากผู้ควบคุมผ่านเครือข่ายอินเทอร์เน็ตได้จากระยะไกล

2. สแปม (Spam)) คือ การส่งจดหมายอิเล็กทรอนิกส์ออกไปยังผู้รับจำนวนมากโดยผู้ที่ได้รับจดหมายเหล่านั้น ไม่ได้มีความประสงค์ที่จะได้รับ ส่วนมากเป็นการโฆษณาสินค้าและบริการ

3. โอเพ่นดีเอ็นเอสรีโซลเวอร์ (Open DNS Resolver) คือ การตั้งค่าเครื่องให้บริการดีเอ็นเอส (DNS) อย่างไม่เหมาะสม ทำให้ผู้อื่นสามารถส่งข้อมูลโดเมนเนมหลอกลวงให้กับเครื่องบริการดีเอ็นเอส เพื่อใช้หลอกลวงผู้ใช้งาน

4. บรูตฟอร์ช (Brute Force) คือ โปรแกรมที่เจาะระบบบเป้าหมายด้วยวิธีการสุ่มช้อมูลตามอัลกอริทีมที่ผู้โจมตีคิดค้น เพื่อให้ได้ข้อมูลสำคัญหรือข้อมูลลับของระบบเป้าหมาย เช่นบัญชีชื่อผู้ใช้งาน และรหัสผ่าน

5. มัลแวร์ยูอาร์แอล (Malware UPL) คือ การที่ผู้ไม่ประสงค์ดีบุกรุกเข้าไปยังไซต์ของผู้อื่น และใช้พื้นที่ของเว็บไซต์นั้นในการแยแพรโปรแกรมไม่พึงประสงค์

6. สแกนนิ่ง (Scanning) คือ การตรวจสอบข้อมูลของบริการของเครื่องแม่ข่ายโดยใช้วิธีส่งข้อมูลไปสู่ระบบที่เป็นเป้าหมาย และรวบรวมข้อมูลที่ได้จากการสแกนนิ่ง เพื่อใช้เป็นข้อมูลในการเจาะระบบ

7. โอเพ่นพร็อกซี่เซิร์ฟเวอร์ (Open Proxy Server) คือ การตั้งค่าบริการเว็บพร็อกซี่(web proxy) ไม่เหมาะสมที่ยินยอมให้ผู้ใช้งานทั่วไปเรียกใช้งาน เพื่อเข้าถึงบริการเว็บในเครือข่ายอินเทอร์เน็ตได้โดยไม่มีระบบยืนยันตัวตน (authentication)

8. พีชชิ่ง (Prishing) คือ เว็บไซต์ปลอมที่องการหลอกลวงเพื่อขโมยซัลสำคัญของผู้ใช้งาน เช่น บัญชีผู้ใช้หรือรหัสผ่าน เป็นต้น

9. สตอร์มเวิร์ม (Storm Worm) คือ โปรแกรมไม่พึ่งประสงค์ในลักษณะเวิร์ม (Worm)ซึ่งสามารถแพร่กระจายได้ด้วยตัวเอง สตอร์มเวิร์มมีลักษณะการทำงานในรูปแบบบอตเน็ต ต่างกันที่บอตเน็ตทั่วไปมีใครงสร้างการทำงานที่มีเครื่องที่ทำหน้าที่ควบคุม

10. ดีดอส (DDoS) คือ โปรแกรมที่โจมตีสภาพความพร้อมใช้งานของระบบเพื่อทำให้บริการต่าง ๆ ของระบบไม่สามารถให้บริการได้ตามปกติจนกระทั่งระบบไม่สามารถให้บริการต่อไปได้

2.3.4 ลักษณะและผลของภัยคุกคามทางไซเบอร์

เอกสาร Cyber Security Articles 2012 ของไทยเซิร์ต ได้จำแนกลักษณะและผลของภัยคุกคามทางไซเบอร์ไว้ 8 ด้าน ดังนี้ (สรณันท์ จิวะสุรัตน์ และชัยชนะ มิตรพันธ์, 2555)

1. เนื้อหาที่เป็นภัยคุกคาม (abusive conten) เป็นการใช้ข้อมูล หรือแอมแพร่ข้อมูลที่ไม่เป็นจริงหรือไม่เหมาะสม เพื่อทำลายความน่าเชื่อถือของบุคคลหรือสถาบัน เพื่อก่อให้เกิดความไม่สงบหรือข้อมูลที่ไม่ถูกต้องตามกฎหมาย การหมิ่นประมาท และรวมถึงการโฆษณาขายสินค้าต่าง ๆทางอีเมลที่ผู้รับไม่ได้มีความประสงค์จะรับข้อมูลโฆษณานั้น ๆ

2. การโจมตีสภาพความพร้อมใช้งานของระบบ (availability) เป็นการโจมตีสภาพความพร้อมใช้งานของระบบ เพื่อสร้างความเสียหายให้แก่ระบบให้บริการต่าง ๆ เช่น ทำให้เกิดความล่าช้า จนถึงขั้นที่ระบบไม่สามารถให้บริการต่อไปได้ อาจเป็นการโจมตีระบบโดยตรง เช่น การโจมตีประเภท DoS (Denial of Service) หรือเป็นการโจมตีโครงสร้างพื้นฐาน เช่น การให้บริการระบบไฟฟ้า น้ำประปา หรือระบบโทรศัพท์ เป็นต้น

3. การฉ้อฉล ฉ้อโกง หรือหลอกลวง เพื่อผลประโยชน์ (fraud) เป็นความพยามที่จะหาผลประโยชน์ด้วยการฉ้อโกง หรือหลอกลวง สามารถเกิดได้ในหลายลักษณะ เช่น การลักลอบใช้งานระบบ หรือทรัพยากรทางสารสนเทศที่ไม่ได้รับอนุญาต เพื่อแสวงหาผลประโยชน์ของตนเอง หรือการขายสินค้า หรือซอฟต์แวร์ที่ละเมิดลิขสิทธิ์

4. ความพยายามรวบรวมข้อมูลของระบบ (information gathering) เป็นความพยายามในการรวบรวมข้อมูลระบบของผู้ไม่ประสงค์ดีด้วยการเรียกใช้บริการต่าง ๆ ที่อาจจะเปิดไว้บนระบบ เช่น ข้อมูลเกี่ยวกับระบบปฏิบัติการระบบซอฟต์แวร์ที่ติดตั้งหรือใช้งาน ข้อมูลบัญชีชื่อผู้ใช้งาน ชื่ออีเมล รวมถึงการเก็บรวบรวมหรือตรวจสอบข้อมูลจราจรบนระบบเครือข่าย (sniffing)และการล่อลวงต่างๆ เพื่อให้ผู้ใช้งานเปิดเผยข้อมูลที่มีความสำคัญของระบบ

5. การเจาะระบบได้สำเร็จ (intrusions) เป็นความพยายามที่สามารถเจาะเข้าระบบได้สำเร็จ และระบบถูกครอบครองโดยผู้ที่ไม่ได้รับอนุญาต

6. ความพยายามจะบุกรุกเข้าระบบ (intrusion attempts) เป็นความพยายามจะเจาะเข้าระบบผ่านจุดอ่อน หรือช่องโหว่ที่เป็นที่รู้จักในสาธารณะ (Common Vulnerabilities andทExposures: CVE) หรือผ่านจุดอ่อนหรือช่องโหวใหม่ที่ยังไม่เคยพบมาก่อน เพื่อการเข้าครอบครองหรือทำให้เกิดความขัดข้องกับบริการต่าง ๆ ของระบบ รวมถึงความพยายามจะเจาะระบบผ่านช่องทางการตรวจสอบบัญชีชื่อผู้ใช้งานและรหัสผ่าน ด้วยวิธีการสุ่มข้อมูล หรือวิธีการทดสอบรหัสผ่านทุกค่า (brute force)

7. โค้ดมุ่งร้าย (malicious code or malware) คือ โค้ดมุ่งร้ายหรือเป็นอันตรายต่อระบบ ขโมยข้อมูล และ/หรือยังส่งต่อไปยังเครื่องผู้อื่น ตัวอย่างโปรแกรมในกลุ่มนี้ ได้แก่ Virus,Worm, Trojan, Botnet, Horse, Spyware who Web Scripts เป็นต้น

8. การเข้าถึง/เปลี่ยนแปลงแก้ไขข้อมูลโดยไม่ได้รับอนุญาต (information security)เป็นภัยคุกคามที่เกิดจากการที่ผู้ไม่ได้รับอนุญาตสามารถเข้าถึงข้อมูลสำคัญ (unauthorized access)หรือเปลี่ยนแปลงแก้ไขข้อมูล (unauthorized modification) ได้

วิธีดำเนินการวิจัย

การศึกษาปัจจัยที่มีผลต่อการตระหนักถึงภัยคุกคามทางไซเบอร์ของชุมชน ตำบลบ้านโปร่งอำเภอหนองโดน จังหวัดสระบุรี โดยผู้วิจัยได้ค้นคว้าและดำเนินการ

ขอบเขตของการวิจัย

จำนวนประชากรที่เกิดปัญหาภัยคุกคามทางไซเบอร์ของชุมชน ตำบลบ้านโปร่งอำเภอหนองโดน จังหวัดสระบุรี

ขอบเขตด้านเนื้อหา การวิจัยครั้งนี้ทำการศึกษาปัจจัยที่มีผลต่อการตระหนักถึงภัยคุกคามทางไซเบอร์ของชุมชน ตำบลบ้านโปร่งอำเภอหนองโดน จังหวัดสระบุรี

ขอบเขตด้านพื้นที่ การทำวิจัยครั้งนี้ทำการศึกษาปัจจัยที่มีผลต่อการตระหนักถึงภัยคุกคามทางไซเบอร์ของชุมชน ตำบลบ้านโปร่งอำเภอหนองโดน จังหวัดสระบุรี

ประชากรและกลุ่มตัวอย่าง ผู้ที่อาศัยอยู่ในของชุมชน ตำบลบ้านโปร่งอำเภอหนองโดน จังหวัดสระบุรี มีจำนวน 2,377 คน

สถิติที่ใช้ในการวิเคราะห์ข้อมูล

ในการวิเคราะห์ข้อมูลครั้งนี้ ผู้วิจัยได้นำหลักสถิติมาใช้ในการวิเคราะห์จากแบบสอบถามประกอบด้วย

1.การวิเคราะห์ข้อมูลพื้นฐานทั่วไปของผู้ตอบแบบสอบถาม สถิติที่ใช้ ได้แก่ การแจกแจงความถี่และร้อยละ

ผลการวิจัย

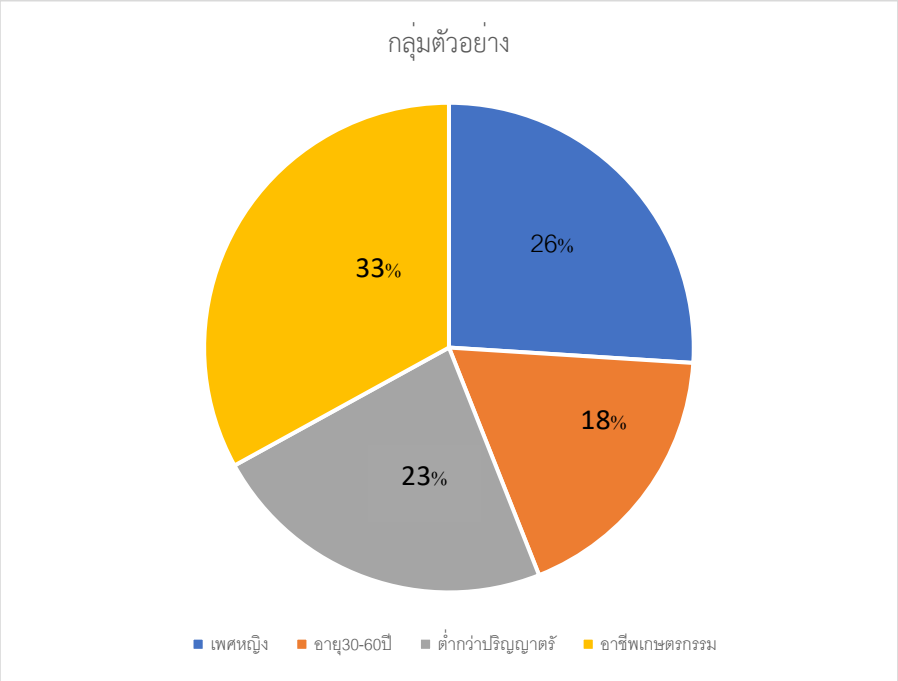
1) จากผลการศึกษาพบว่า ประชากรของชุมชน ตำบลบ้านโปร่งอำเภอหนองโดน จังหวัดสระบุรี อยู่ในระดับมากทุกๆของหมู่บ้านในด้านความปลอดภัยการเข้าใช้งานอินเตอร์เน็ต ด้านการป้องกันข้อมูลเกิดความมั่นคงปลอดภัยไซเบอร์และแนวปฏิบัติที่ดี โดยมีผลการวิเคราะห์ลักษณะกลุ่มตัวอย่าง ดังตารางที่ 1

ตารางที่ 1 ผลการวิเคราะห์ลักษณะกลุ่มตัวอย่าง

ตัวแปร	รายการ	ความถี่	ร้อยละ
เพศ	ชาย	86	47.77
	หญิง	94	52.23
	รวม	**180**	**100.0**
อายุ	ต่ำกว่า 20 ปี	15	8.34
	21 - 30 ปี	20	11.11
	30 -60 ปี	80	44.44
	60 ปีขึ้นไป	65	36.11
	รวม	**180**	**100.0**
สถานภาพ	โสด	35	19.56
	สมรส	114	63.55

	หย่าร้าง	30	16.89
	รวม	**180**	**100.0**

ตัวแปร	รายการ	ความถี่	ร้อยละ
การศึกษา	ต่ำกว่า ป.ตรี	172	95.55
	ป.ตรี	8	4.45
	สูงกว่า ป.ตรี	0	0.00
	รวม	**180**	**100.0**
อาชีพ	ค้าขาย	27	15.12
	พนักงานราชการ	0	0.00
	นักเรียน นักศึกษา	2	1.54
	พนักงานบริษัท	8	4.45
	พนักงานรัฐ	**0**	0.00
	เกษตรกร	142	78.89
	รวม	**180**	**100.0**



ภาพที่ 1 แสดงกลุ่มตัวอย่าง

อภิปรายผล

การศึกษาปัญหาของภัยคุกคามทางไซเบอร์ของชุมชน ตำบลบ้านโปร่ง อำเภอหนองโดน จังหวัดสระบุรี ค่าเฉลี่ยอยู่ในระดับมากทุกองค์ประกอบ ทั้งในด้านความปลอดภัยการเข้าใช้งานอินเตอร์เน็ต ด้านการป้องกันข้อมูล 1) เกิดความมั่นคงปลอดภัยไซเบอร์และแนวปฏิบัติที่ดี สอดคล้องกับเมธาพร ธรรมศิริ และ ศิรภัสสรศ์ วงศ์ทองดี,(2565) ที่ได้ศึกษาความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ของบุคลากรในบริษัทเอกชนแห่งหนึ่งในเขตกรุงเทพมหานคร พบว่า บุคลากรในบริษัทเอกชนแห่งหนึ่งในเขตกรุงเทพมหานคร มีความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์อยู่ในระดับมาก โดยเมื่อจำแนกตามปัจจัยส่วนบุคคลพบว่าบุคลากรในบริษัทเอกชนแห่งนี้ที่มี เพศ อายุ และประสบการณ์การทำงาน (อายุงาน) ที่ต่างกันมีระดับความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ที่ไม่แตกต่างกัน และในส่วนบุคลากรที่มีระดับการศึกษาสูงสุด แผนกที่สังกัด และประสบการณ์เกี่ยวกับความมั่นคง

และ2) นำข้อมูลที่ได้จากการศึกษาเรื่องนี้ไปรับปรุงและและพัฒนาเพื่อเพิ่มประสิทธิภาพองค์ความรู้ในการเฝ้าระวังภัยคุกคามทางไซเบอร์ในองค์กรทำงานต่อไป

ข้อเสนอแนะจากการวิจัย

1) ควรจัดการอบรมการเตือนภัยบนโลกออนไลน์ เตือนภัย เช่น ความรู้เกี่ยวกับข้อมูลเกี่ยวกับระบบปฏิบัติการระบบซอฟต์แวร์ที่ติดตั้งหรือใช้งาน ข้อมูลบัญชีชื่อผู้ใช้งาน ชื่ออีเมล รวมถึงการเก็บรวบรวมหรือตรวจสอบข้อมูลจราจรบนระบบเครือข่าย (sniffing)และการล่อลวงต่างๆ เพื่อให้ผู้ใช้งานเปิดเผยข้อมูลที่มีความสำคัญของระบบ

เอกสารอ้างอิง

จิตารีย์ จันทพันธ์. (2559). วิจัย เรื่อง "*การศึกษาผลกระทบการรับรู้ความเสี่ยงในการใช้งานการขอระบุตำแหน่ง (Location - Based Services: LBS) บนสื่อสังคมออนไลน์ ต่อความเป็นส่วนตัวของผู้ใช้งานในเขตกรุงเทพมหานคร*" มหาวิทยาลัยกรุงเทพ.

เมธาพร ธรรมศิริ และ ศิรภัสสรศ์ วงศ์ทองดี,(2565)ความตระหนักรู้ด้านภัยคุกคามทางไซเบอร์ของบุคลากรในบริษัทเอกชนแห่งหนึ่งในเขตกรุงเทพมหานคร, *วารสารวิชาการไทยวิจัยและการจัดการ*, 3(2).1-17

ศิวลีย์ สิริโรจน์บริรักษ์. (2558). วิจัยเรื่อง *การพัฒนามาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์(Cyber Security) ของกระทรวงกลาโหม ศูนย์ศึกษายุทธศาสตร์* สถาบันวิชาการป้องกันประเทศ.

อรรถพล ป้อมสถิต. (2559). *การเพิ่มประสิทธิภาพระบบตรวจจับการบุกรุกในการรักษาความมั่นคงทางไซเบอร์ด้วยฮันนี่พอท* มหาวิทยาลัยราชภัฏพระนคร.

อุบลวรรณ ภีระเป็ง. (2558). *การโจมตีทางไซเบอร์ในสถานการณ์การขัดกันทางอาวุธ : ศึกษาการบังคับใช้กฎหมายมนุษยธรรมระหว่างประเทศ*"คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย.

We Are Social (2016). สืบค้นเมื่อ 10 กุมภาพันธ์ 2565 จาก https://datareportal.com/reports/digital-2016-global-digital-overview