ตำราฝึกงานในหน้าที่
จำพวกทหารสารสนเทศ
และสงครามอิเล็กทรอนิกส์

ลชทอ.๒๗๑๓๐

ลชทอ.๒๗๑๕๐

ลชทอ.๒๗๑๗๐

กองสงครามไซเบอร์

คำนำ

ตำราฝึกงานในหน้าที่เกี่ยวกับความรู้ทั่วไปด้านสงครามสารสนเทศและสงครามไซเบอร์นี้ จัดทำขึ้นเพื่อประกอบการฝึก ความชำนาญ ตามมาตรฐานการฝึกความชำนาญ (มฝช.) ของจำพวกทหารสารสนเทศและสงคราม อิเล็กทรอนิกส์ เนื้อหาของตำราเล่มนี้อธิบายในภาพรวมของสงครามสารสนเทศและสงครามไซเบอร์ กฎหมายคอมพิวเตอร์ พรบ.ที่เกี่ยวข้อง และระเบียบ ทอ.ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ เพื่อให้ผู้เข้ารับการฝึกงานในหน้าที่มีความรู้ ความเข้าใจในงานด้านสงครามสารสนเทศและสงครามไซเบอร์ สามารถนำไปปฏิบัติงานได้อย่างมีประสิทธิภาพ ตลอดจนสร้างจิตสำนึกต่อการปฏิบัติงานด้านเทคโนโลยีสารสนเทศและสงครามอิเล็กทรอนิกส์อย่างปลอดภัย ตามค่านิยมหลักของ ทอ. รวมทั้งตอบสนองต่อยุทธศาสตร์ของ ทอ.

กคซ.สบค.ทสส.ทอ.

กันยายน พ.ศ.๒๕๖๕

สารบัญ

สารบัญรูปภาพ

บทที่ ๑
สงครามสารสนเทศและสงครามไซเบอร์

ในช่วงหลายปีที่ผ่านมา แนวคิดหนึ่งที่เรียกว่า "สงครามสารสนเทศ (Information Warfare)" ได้กลายเป็นที่สนใจในหน่วยงานเกี่ยวกับการป้องกันประเทศสหรัฐอเมริกาและอีกหลายประเทศ เป็นแนวคิดที่ฝังรากในความเป็นจริงที่ปฏิเสธไม่ได้ว่า ข้อมูลและเทคโนโลยีสารสนเทศมีความสำคัญมากขึ้น ด้านความมั่นคงของชาติโดยทั่วไปและโดยเฉพาะการสงคราม ตามแนวคิดนี้ความขัดแย้งจะเป็นรูปแบบที่รุนแรงสูงมากขึ้น โดดเด่นด้วยการต่อสู้ที่ผ่านระบบสารสนเทศ โดยใช้ทุกรูปแบบของการต่อสู้ให้ได้เปรียบกว่าศัตรูที่ไม่ได้ทำ

๑. สงครามสารสนเทศ

ตามเอกสารของประธานคณะเสนาธิการร่วมสหรัฐฯ ค.ศ. 1996 ได้ให้คำจำกัดความของสงครามข่าวสารไว้ว่า “สงครามสารสนเทศ คือ การดำเนินการใด ๆ เพื่อครองความเหนือกว่าด้านสารสนเทศ ด้วยการกระทำต่อข้อมูลข่าวสาร กรรมวิธีข้อมูลข่าวสาร ระบบสารสนเทศ เครือข่ายคอมพิวเตอร์ ของฝ่ายตรงข้าม ในขณะเดียวกันก็ทำการป้องกันข้อมูลข่าวสาร กรรมวิธีข้อมูลข่าวสาร ระบบสารสนเทศ และเครือข่ายคอมพิวเตอร์ของตนเอง (Information Warfare (IW). Actions taken to achieve information superiority by affecting adversary information, information-base process, information system, and computer-base networks while defending one’s own information, information-base processes, information systems, and computer-base networks.)”

เป้าหมายของสงครามสารสนเทศ (Information Warfare) คือกระบวนการของข้อมูลสารสนเทศ ที่มีความเป็นอิสระไม่ว่าจะเป็นมนุษย์หรือเครื่องจักรต่างๆ การข่าวกรองและการสื่อสาร จะสนับสนุนสิ่งสำคัญเหล่านี้ ในการปฏิบัติ การรบด้วยวิธีรุก และการรบด้วยวิธีรับของสงครามสารสนเทศ การสงครามสารสนเทศจะสนับสนุนยุทธศาสตร์ทหารของชาติ แต่จะต้องได้รับการสนับสนุนในเรื่องเงื่อนไข และความร่วมมือของหน่วย และองค์กรต่างๆ ด้วย

สงครามสารสนเทศมีคุณลักษณะ คือ ไม่มีแนวรบชัดเจน, ลงทุนน้อยแต่ได้ผลมาก, เส้นพรมแดนไม่ชัดเจน และการหลอกลวงทำได้ง่าย

๑.๑ รูปแบบของสงครามสารสนเทศ

สงครามสารสนเทศ (Information Warfare) มี ๗ รูปแบบ คือ

๑.๑.๑ สงครามการบัญชาการและควบคุม (Command-and-Control Warfare) เป็นสงครามที่มุ่งการจู่โจมที่จุดสำคัญของการบัญชาการและควบคุมการรบของข้าศึก

๑.๑.๒ สงครามการข่าวกรอง (Intelligence-based Warfare) เป็นสงครามที่ใช้การออกแบบการป้องกัน และการปฏิเสธด้านการข่าวกรอง ที่แสวงหาความรู้ให้เพียงพอที่จะครองสนามรบ

๑.๑.๓ สงครามอิเล็กทรอนิกส์ (Electronic Warfare) เป็นสงครามที่ใช้ประโยชน์ของความถี่วิทยุ-อิเล็กทรอนิกส์หรือเทคนิคการเข้ารหัสลับ

๑.๑.๔ สงคราม จิตวิทยา (Psychological Warfare) เป็นสงครามที่ใช้ข้อมูลหรือสารสนเทศมุ่งเปลี่ยนจิตใจของกลุ่มคนทั้งที่เป็นมิตร ที่เป็นกลาง และที่เป็นศัตรู

๑.๑.๕ สงครามแฮ็กเกอร์(Hacker Warfare) เป็นสงครามที่ใช้ระบบคอมพิวเตอร์ในการโจมตี

๑.๑.๖ สงครามสารสนเทศทางเศรษฐกิจ (Economic Information Warfare) เป็นสงครามที่ใช้การปิดกั้น หรือเปลี่ยนช่องทางข้อมูลสารสนเทศ เพื่อสร้างความได้เปรียบหรือการครอบง าทางเศรษฐกิจ

๑.๑.๗ สงครามไซเบอร์ (Cyber Warfare) เป็นสงครามที่ใช้ทุกสถานการณ์เพื่อสร้างความได้เปรียบเหนือศัตรูทุกรูปแบบของสงครามสารสนเทศให้สอดคล้องสัมพันธ์เชื่อมโยงกันถูกกำหนดแล้ว

๒. สงครามไซเบอร์

สงครามไซเบอร์ คือ ความขัดแย้งที่มีพื้นที่ทำสงครามครอบคลุมในส่วนของคอมพิวเตอร์และอินเตอร์เน็ต โดยเป็นปฏิบัติการเพื่อขัดขวาง ทำลายระบบการข่าวและการสื่อสารของฝ่ายตรงข้าม และต้องทำให้ดุลแห่งข่าวสารและความรู้เอียงมาอยู่ฝ่ายเรา ส่วนมากจะมีแรงจูงใจทางการเมือง ทางเศรษฐกิจ หรือแม้กระทั่งความสัมพันธ์ระดับประเทศ หากจะกล่าวว่าเป็นวิธีการใดๆก็ตามที่ทำให้เราคาดว่าจะได้รับชัยชนะตามวัตถุประสงค์ส่วนบุคคล ส่วนองค์กร ผ่านการใช้อุปกรณ์เทคโนโลยีที่สามารถติดต่อสื่อสารได้ ก็คงไม่ผิดไปนัก

ไซเบอร์สเปซ (Cyber Space) คือ พื้นที่ทำการรบ หากเปรียบเทียบให้เห็นภาพกับสงครามโลกครั้งที่ ๒ การสู้รบด้วยทหารราบ รถถัง พื้นที่ทำการรบคือบนพื้น (Ground Space) เรือรบ เรือดำน้ำ เรือบรรทุกเครื่องบิน มีพื้นที่ทำการรบทางน้ำ (Sea Space) เครื่องบินลำเลียง เครื่องบินขับไล่ เครื่องบินทิ้งระเบิด มีพื้นที่ทางการรบทางอากาศ (Air Space) พื้นที่ทางการรบของไซเบอร์สเปซก็คือการติดต่อสื่อสาร แลกเปลี่ยนข้อมูล ในรูปแบบใดๆผ่านอุปกรณ์ต่างๆของทั้งการปฏิบัติการทางบก ทางเรือ ทางอากาศ นั่นเอง

รูปที่ ๑ ภาพประกอบพื้นที่ทำการรบในส่วนของไซเบอร์สเปซ

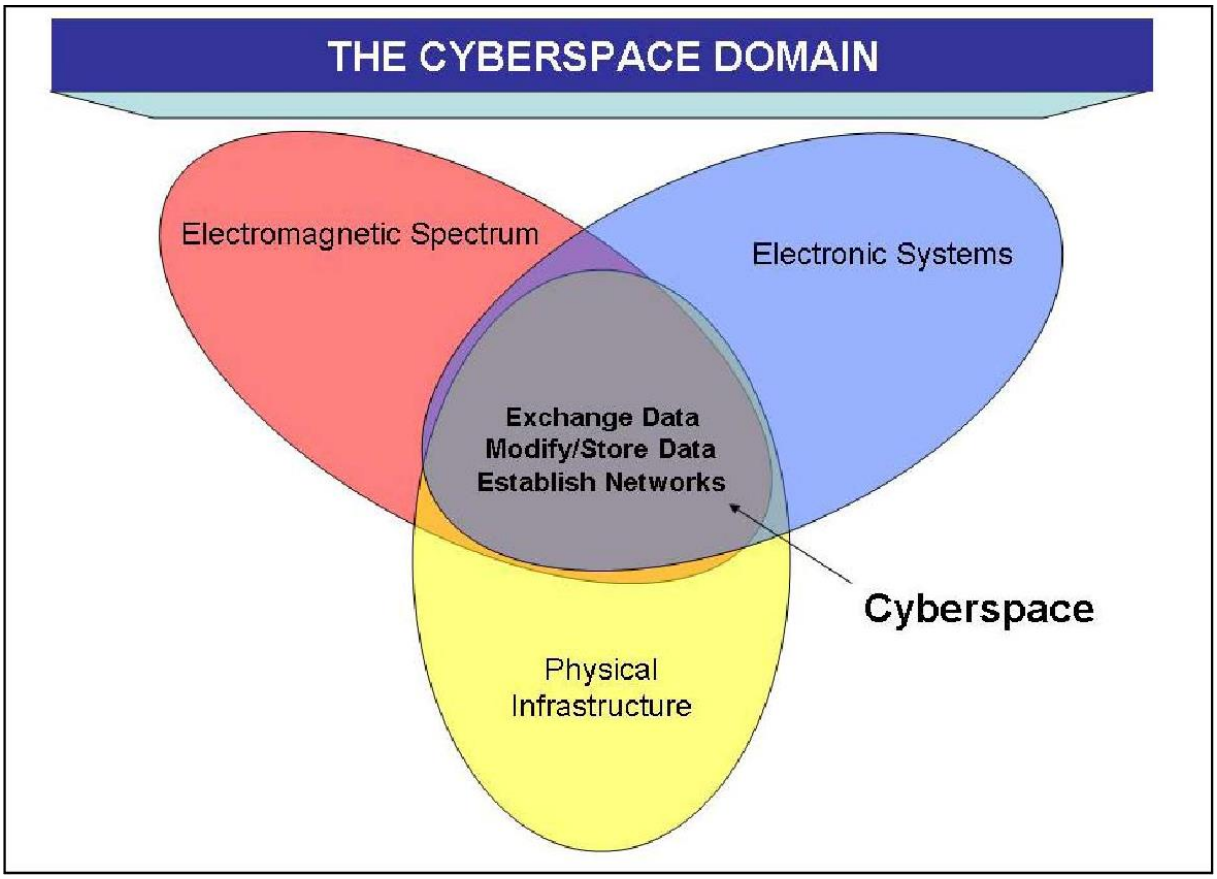
คุณลักษณะของไซเบอร์สเปซ

ลักษณะการทำงานในส่วนของไซเบอร์สเปซ ที่ใช้ในการแลกเปลี่ยนข้อมูลติดต่อสื่อสารผ่านกองกำลังทางบก ทางน้ำ ทางอากาศและอวกาศนั้น จะมีองค์ประกอบที่สำคัญๆอยู่สามอย่างด้วยกันคือ

๑. Electromagnetic Spectrum หรือ สเปกตรัมแม่เหล็กไฟฟ้า ประกอบไปด้วยคลื่นวิทยุ ทั้งระบบ A.M. ระบบ F.M. คลื่นโทรทัศน์ และไมโครเวฟ รังสีอินฟราเรด แสง รังสีอัลตร้าไวโอเลต รังสีเอกซ์ รังสีแกมมา

๒. Electronic Systems คือ การรวมกลุ่มของอุปกรณ์ วงจรอิเล็กทรอนิกส์ และส่วนประกอบต่างๆ ที่ถูกออกแบบมาสำหรับการทำงานของอุปกรณ์ที่มีฟังก์ชันการใช้งานที่ซับซ้อน ยกตัวอย่างเช่น ระบบสื่อสารโทรคมนาคม ระบบคอมพิวเตอร์ ระบบผลิตพลังงาน ระบบเรดาห์ ระบบเสียง เพลง อิเล็กทรอนิกส์ และอื่นๆอีกมาก

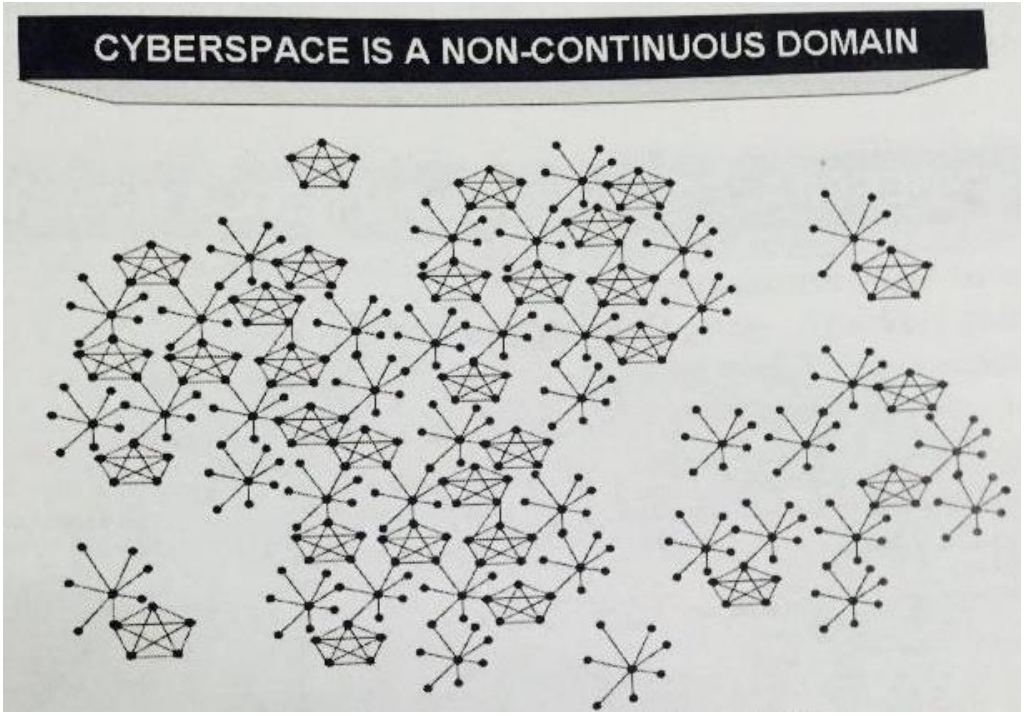
๓. Physical Infrastructure คือ โครงสร้างพื้นฐานทางกายภาพที่จับต้องได้ ไม่ว่าจะเป็นอุปกรณ์ที่เกี่ยวกับระบบธุรกิจ ระดับชาติ การขนส่ง การสื่อสาร ระบบการผลิตน้ำ กระแสไฟฟ้า ซึ่งโดยส่วนมากจะเป็นการลงทุนที่มีค่าใช้จ่ายค่อนข้างสูง



รูปที่ ๒ องค์ประกอบที่ทำให้เกิดไซเบอร์สเปซ

ไซเบอร์สเปซเป็นโดเมนที่ไม่ได้ต่อเนื่องกัน

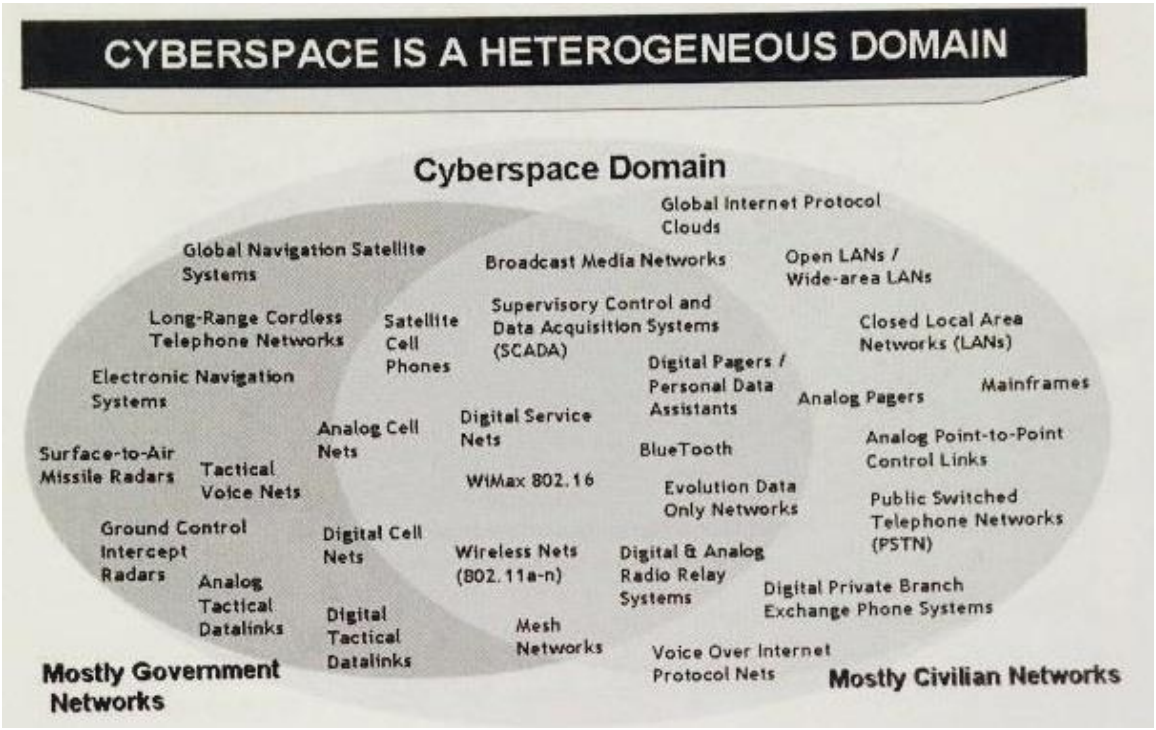
แม้ว่าไซเบอร์สเปซจะก่อให้เกิดการเชื่อมโยงกันอย่างมหาศาลมากขึ้นเรื่อยๆโดยเฉาพะการเชื่อมต่อระดับสากลหรือแทบจะทั้งโลก (Interconnected) แต่การเชื่อมต่อเน็ตเวิร์กในขอบเขตดังกล่าวนี้ได้ถูกแบ่งออกเป็นหลายๆส่วน ได้แก่ โปรโตคอล ไฟร์วอลล์ การเข้ารหัส และอุปกรณ์ที่ใช้งานผ่านเน็ตเวิร์กที่หลากหลาย ซึ่งทั้งหมดนี้ได้ถูกแยกออกจากกัน ตัวอย่างก็เช่นมีคอมพิวเตอร์อีกมากมายหลายเครื่องที่ไม่ได้เชื่อมต่อกับอินเตอร์เน็ต แต่ถูกแยกออกไปใช้เพื่อวัตถุประสงค์และมีการเชื่อมต่อเฉพาะทาง



รูปที่ ๓ แสดงให้เห็นภาพว่าไซเบอร์สเปซเป็นโดเมนที่ไม่ได้เชื่อมต่อกันทั้งหมด

ไซเบอร์สเปซเป็นโดเมนที่มีลักษณะเฉพาะต่างกัน

เนื่องจากมีหน่วยงานที่สร้างไซเบอร์สเปซของตัวเองโดยมีจุดมุ่งหมายและความต้องการที่ต่างกัน แท้ที่จริงแล้วมันคือการรวบรวมกลุ่มของระบบหลายๆระบบ โดยอีกนัยหนึ่ง ไซเบอร์สเปซก็คือการกำเนิดขึ้นของเน็ตเวิร์กที่มีชนิดแตกต่างกัน มีฟังก์ชันการใช้งานที่แตกต่างกัน ระดับการเชื่อมต่อ ความซับซ้อนของเทคโนโลยีและช่องโหว่ที่แตกต่างกัน จะเห็นจากรูปที่ ๔ ด้านล่างว่าไซเบอร์สเปซเหล่านั้นมีความสามารถในการแลกเปลี่ยนข้อมูลข่าวสารด้วยเทคโนโลยี อินเตอร์เฟซ และ โปรโตคอลที่ไม่เหมือนกันเลย ซึ่งจากกลุ่มไซเบอร์สเปซเหล่านี้ ได้ก่อให้เกิดนวัตกรรมขั้นสูงให้กับแวดวงอุตสาหกรรมการติดต่อสื่อสาร คอมพิวเตอร์ และอิเล็กทรอนิกส์เป็นอย่างมาก



รูปที่ ๔ ไซเบอร์สเปซที่มีความแตกต่างกันไปก่อให้เกิดนวัตกรรมใหม่ๆในแวดวงอุตสาหกรรม

ไซเบอร์สเปซมีการเปลี่ยนแปลงอย่างรวดเร็ว

ไซเบอร์สเปซส่วนมากจะถูกนำไปใช้และขับเคลื่อนในวงการพาณิชย์ ซึ่งโดเมนนี้มีวิวัฒนาการและสามารถขยายตัวด้วยความรวดเร็วดังที่เราเห็นเทคโนโลยีการติดต่อสื่อสารในปัจจุบัน สามารถพูดได้อีกนัยหนึ่งว่าส่วนของไซเบอร์สเปซมีส่วนในการผลักดันนวัตกรรมใหม่ๆออกมาอย่างต่อเนื่อง รวมถึงยังมีการแทนที่ปรับเปลี่ยน และอัพเดทโปรโตคอลอยู่ตลอดเวลา อาจจะเพราะเนื่องจากไซเบอร์สเปซเป็นปฏิบัติการที่มีความรวดเร็วมากเพราะอิเล็กตรอนนั้นเดินทางด้วยความเร็วแสงและก่อให้เกิดผลลัพธ์ทางการกระทำแทบจะทันทีทันใด ตัวอย่างเช่นประเทศสหรัฐอเมริกานั้นสามารถโจมตี และถูกโจมตีอย่างรวดเร็วจากโดเมนภายนอกผ่านการเชื่อมต่อเครือข่ายใหญ่ๆเช่นอินเตอร์เน็ต ซึ่งเรื่องนี้สามารถเกิดขึ้นได้ข้ามพรมแดนโดยผู้ที่โจมตีอาจจะอยู่คนละซีกโลกกันเลยทีเดียว

ไซเบอร์สเปซประกอบไปด้วยพื้นที่ทางการรบทั้งทางด้านตรรกะและกายภาพ

ในส่วนของไซเบอร์สเปซนั้นถูกเชื่อมโยงโดยโครงสร้างพื้นฐานทางกายภาพ ระบบอิเล็กทรอนิกส์ผ่านทางการใช้สเปกตรัมแม่เหล็กไฟฟ้า EMS (Electro-Magnetic Systems) ตามที่ได้กล่าวไปข้างต้น ซึ่งเมื่อมีการคิดค้นระบบและโครงสร้างพื้นฐานใหม่ๆ ก็จะทำให้เกิดการใช้ EMS ที่มากขึ้น ระบบอาจจะถูกออกแบบให้เปลี่ยนคลื่นความถี่เช่นเมื่อมีการส่งผ่านข้อมูล ส่งผลให้รูปแบบการรบเปลี่ยนแปลงไปแต่นั่นก็ยังอยู่ในรูปแบบการใช้งาน EMS ภายใต้ขอบเขตของไซเบอร์สเปซอยู่ดี

ระบบอิเล็กทรอนิกส์นั้นมีความสามารถในการเชื่อมกันระหว่างเทคนิคและโปรโตคอลซึ่งใช้ในการตรวจสอบได้หากมี “เอกลักษณ์”บางอย่างที่กำลังมองหาการเชื่อมต่อเข้าไปในระบบ ซึ่งการป้องกันเอกลักษณ์ที่ไม่พึงประสงค์เหล่านี้สามารถป้องกันได้โดยการเขียนโค้ดหรือการคิดเชิงตรรกะในระบบอิเล็คทรอนิกส์ เมื่อมีการเชื่อมต่อกันระหว่างระบบสองระบบเกิดขึ้น ผู้โจมตีก็จะใช้ประโยชน์จากความผิดพลาดทางการป้องกันเพื่อเข้าไปในอีกระบบ การเขียนโค้ดนั้นเป็นการคิดเชิงตรรกะผ่านทางไซเบอร์สเปซ ในเมื่อผู้โจมตีใช้ประโยชน์จากการเขียนโค้ดในการป้องกันที่มีช่องโหว่ ในฐานะฝ่ายป้องกันก้องระวังสิ่งผิดปกติในระบบของตัวเอง หรืออาจเขียนและปรับเปลี่ยนโค้ดเพื่อให้สามารถป้องกันช่องโหว่ในจุดนั้นได้ ซึ่งก็จะส่งผลให้ผู้โจมตีค้นหาวิธีการและช่องโหว่ใหม่ๆเสมอเป็นวัฏจักรที่ไม่มีวันจบสิ้นแม้ว่าภารกิจของผู้โจมตีจะลุล่วงหรือผู้ที่ทำการป้องกันไม่ต้องกังวลกับการโจมตีอีกแล้ว ทั้งนี้ก็เพื่อที่ต่างฝ่ายต่างก็ต้องการที่จะอยู่ในตำแหน่งที่มีความได้เปรียบตลอดไปในระยะยาวนั่นเอง

คอนเซปท์ของไซเบอร์สเปซ

ไซเบอร์สเปซนั้นมีจุดมุ่งหมายที่จะครอบครองชัยภูมิหรือตำแหน่งที่เหนือกว่าอีกฝ่ายหนึ่งโดยทำการปฏิการทางด้านไซเบอร์สเปซที่เชื่อมต่อกันอยู่ภายในเวลาที่จำกัดโดยที่ไม่ได้รับการอนุญาตอย่างถูกต้องจากอีกฝ่ายหนึ่ง พื้นฐานการออกแบบด้านการปฏิบัติการและปรัชญาการวางแผนเพื่อที่จะนำมาปรับใช้กับโดเมนนี้ โดยการปฏิบัติการนี้จะตสามารถครอบครองความได้เปรียบทางด้านไซเบอร์สเปซ ซึ่งจะมีศักยภาพมากที่สุดเมื่อนำมาปรับใช้กับศูนย์ปฏิบัติการทางอากาศและอวกาศ (Air and Space Operation Center) หรือ AOC โดยหน้าที่หลักๆก็คือการเตรียมตัวระวังป้องกันภัยทางไซเบอร์จากสถานการณ์รอบตัวที่อาจเกิดขึ้น

การตอบโต้กลับทางไซเบอร์ก็เป็นภารกิจอีกรูปแบบหนึ่งซึ่งเป็นการปฏิบัติการร่วมกันระหว่างการปฏิบัติการเชิงรุกและการปฏิบัติการเชิงรับ เพื่อรักษาความได้เปรียบทางด้านไซเบอร์ โดยภารกิจการตอบโต้กลับทางไซเบอร์จะจัดการมาตรการตอบโต้โดยอ้างอิงตามระดับของภัยคุกคามที่ได้ประสบ ซึ่งาจจะเป็นการเข้าควบคุมสถานการ์หรือรอจังหวะเพื่อโจมตีกลับ

๒.๑ การปฏิบัติการไซเบอร์เชิงรับ

มาตรการป้องกันทุกรูปแบบในการตรวจสอบ ทำลาย ลบล้าง หรือลดทอนกองกำลังของศัตรูซึ่งพยายามที่จะเจาะหรือการโจมตีผ่านโลกไซเบอร์ การป้องกันตอบโต้กลับไซเบอร์รวมถึง การปฏิบัติการไซเบอร์ป้องกันเชิงรุกและเชิงรวมทั้งหมด

มาตรการป้องกันออกแบบมาเพื่อทำลายกองกำลังฝ่ายตรงข้ามโจมตีหรือจะปฏิเสธหรือลดประสิทธิภาพขอฝ่ายตรงข้าม โดยการป้องกันและตอบโต้กลับทางไซเบอร์จะรวมถึงมาตรการที่จะรักษา ป้องกัน, การกู้คืนและ ความสามารถในการสร้างมิตรภาพกับโลกไซเบอร์ก่อนระหว่างและหลังจากการโจมตีฝ่ายตรงข้าม การป้องกันทางไซเบอร์จากฝ่ายตรงข้ามมีทั้งหมดสี่ขั้นตอนดังนี้

๒.๑.๑ สำรวจระบบเน็ตเวิร์ค

๒.๑.๒ พยายามค้นหาผู้บุกรุกและการกระทำอื่นๆที่อาจเกี่ยวข้อง

๒.๑.๓ อุดช่องโหว่ ป้องกันการบุกรุกและกิจกรรมอื่นๆ

๒.๑.๔ ทำการโจมตีตอบโต้กลับ

๒.๒ การปฏิบัติการไซเบอร์เชิงรุก

การปฏิบัติการเชิงรุกโดยการระงับ ลดทอน แทรกแซง ทำลาย หรือ หลอกล่อ ขโมยความสามารถของศัตรูที่ใช้ในไซเบอร์สเปซ รวมถึงการใช้งานอุปกรณ์อิเล็คทรอนิกส์ เน็ตเวิร์คและระบบอื่นๆ ซึ่งใช้ Electromagnetic Spectrum ในสภาพแวดล้อมทางไซเบอร์สเปซ โดยการปฏิบัติการเชิงรุกนั้นจะขึ้นตามรูปแบบหลักๆอยู่ ๘ ขั้นตอน ซึ่งการปฏิบัติการเชิงรุกจะประกอบไปด้วยขั้นตอนเหล่านี้เพียง ๑-๒ ขั้นตอนก็เป็นได้ แต่อย่างไรก็ตามจะต้องเป็นไปตามลำดับ ซึ่งขั้นตอนการปฏิบัติการเชิงรุกจะประกอบไปด้วย

๒.๒.๑ การตรวจสอบช่องโหว่

๒.๒.๒ ตรวจสอบเส้นทางที่เข้าถึง

๒.๒.๓ ทดสอบช่องโหว่และเส้นทางเชื่อมต่อโดยการปิดระบบหรือ ออฟไลน์

๒.๒.๔ ค้นหาข้อมูลและช่องทางที่เป็นประโยชน์ หรือการลองแหย่ฝั่งตรงข้ามดู

๒.๒.๕ สำรวจระบบเน็ตเวิร์คและสังเกตการณ์ปฏิบัติการของฝั่งตรงข้าม

๒.๒.๖ ดึงข้อมูลออกมา

๒.๒.๗ จำลองตัวอย่างการโจมตีทางเน็ตเวิร์ค แอพพลิเคชั่น และรายบุคคล

๒.๒.๘ ทำการโจมตีระบบเน็ตเวิร์ค แอพพลิเคชั่น และรายบุคคลจริงๆ

โดยขั้นตอนแรกๆของการปฏิบัติการไซเบอร์เชิงรุกก็คือ ทำการสำรวจช่องโหว่ในแอพพลิเคชั่นเครื่องเป้าหมาย หรือโครงสร้างของเครือข่ายและทดสอบเชื่อมต่อผ่านช่องโหว่เหล่านั้น ช่องโหว่ที่อยู่ภายในองค์ประกอบโครงสร้างหลายๆแอพพลิเคชั่นนั้น สามารถตรวจสอบได้เพราะแอพพลิเคชั่นเหล่านั้นมีขายอยู่ในท้องตลาดออนไลน์ และสามารถหาซื้อขายได้ทั่วไป เส้นทางที่เชื่อมต่อนั้น บ่อยครั้งจะถูกเปิดเผยโดยเทคโนโลยีที่สูงขึ้น ซึ่งวิศวกรทางด้านไอที ก็ต้องคอยดูแลระบบเฉพาะทางเหล่านั้นและพยายามจัดการปัญหาที่เกิดขึ้นมาใหม่ๆอยู่อย่างต่อเนื่อง

๒.๓ การข่าวกรองไซเบอร์

การข่าวกรองไซเบอร์ เป็นการประยุกต์ใช้กระบวนการข่าวเพื่อนำมาสนับสนุนการปฏิบัติการไซเบอร์ทั้งเชิงรุกและเชิงรับ ซึ่งเป็นการปฏิบัติการร่วมกันของกรมข่าวทหารอากาศ (ขว.ทอ.), กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ (ทสส.ทอ.), ศูนย์ไซเบอร์กองทัพอากาศ (ศซบ.ทอ.) และกรมสื่อสารอิเล็กทรอนิกส์ทหารอากาศ (สอ.ทอ.) โดยมีกระบวนการในการหาข่าวกรองไซเบอร์ ดังนี้

๒.๓.๑ ติดตามข้อมูลข่าวสารผ่านทางสื่อสังคมออนไลน์

๒.๓.๒ แลกเปลี่ยนข้อมูลข่าวสารกับหน่วยงานที่มีความรู้ความเชี่ยวชาญด้านไซเบอร์ทั้งภาครัฐและเอกชน ทั้งภายในและต่างประเทศ เช่น ศูนย์ไซเบอร์ทหาร (ศซบ.ทหาร), สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เป็นต้น

๒.๓.๓ ใช้อุปกรณ์ ซอฟต์แวร์หรือระบบสารสนเทศในการบริหารจัดการข่าวกรองไซเบอร์ (Cyber Threat Intelligence : CTI) เพื่อติดตามและประเมินผลพฤติกรรมจากผู้ใช้งานและผู้ไม่ประสงค์ดีที่อาจเป็นภัยคุกคามด้านไซเบอร์ต่อกองทัพอากาศได้

๓. บทบาทกองทัพอากาศกับสงครามไซเบอร์

พระราชบัญญัติจัดระเบียบราชการกระทรวงกลาโหม พ.ศ. ๒๕๕๑ มาตรา ๒๑ ระบุว่า “กองทัพอากาศมีหน้าที่เตรียมกำลังกองทัพอากาศ การปองกันราชอาณาจักร และดำเนินการเกี่ยวกับการใช้กำลังกองทัพอากาศตามอำนาจหน้าที่ของกระทรวงกลาโหม มีผู้บัญชาการทหารอากาศเปนผู้บังคับบัญชารับผิดชอบ” ซึ่งแต่เดิมกำลังกองทัพอากาศหมายถึงการปฏิบัติทางอากาศ (Air Power) ในมิติเดียวเท่านั้น กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ (ทสส.ทอ.) ในฐานะฝ่านอำนวยการและฝ่ายเสนาธิการด้านเทคโนโลยีสารสนเทศและการสื่อสารได้ดำเนินการเกี่ยวกับสงครามไซเบอร์ในด้านการปฏิบัติการไซเบอร์เชิงรับ (DCC) ให้ระบบสารสนเทศต่างๆ ของกองทัพอากาศมีความปลอดภัยและสามารถดำเนินการได้ตามปกติ เพื่อให้กองทัพอากาศสามารถดำรงขีดความสามารถการปฏิบติทางอากาศไว้ได้ โดยมีแผนกรักษาความปลอดภัยระบบสารสนเทศ กองสงครามอิเล็กทรอนิกส์ กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศรับผิดชอบ ตามโครงสร้าง อัตรา ทอ.๕๒

ต่อมาเมื่อสงครามไซเบอร์เริ่มเข้ามามีบทบาทในการสงครามระหว่างประเทศ ตามที่เทคโนโลยีสารสนเทศและการสื่อสารเข้ามามีบทบาทในการปฏิบัติการทางทหาร เมื่อกองทัพมีขีดความสามารถด้านสงครามไซเบอร์สูงกว่าข้าศึกศัตรู กองทัพสามารถใช้กำลังทางไซเบอร์สนับสนุนการปฏิบัติการทางทหารของตัวเองและขัดขวางการปฏิบัติการทางทหารของข้าศึกได้

กองทัพอากาศมีวิสัยทัศน์ มุ่งหวังพัฒนาสู่ “กองทัพอากาศชั้นนำในภูมิภาค” หรือ "One of the Best Air Forces in ASEAN" ซึ่งอีกนัยหนึ่ง คือ เป็นกองทัพอากาศที่มีขีดความสามารถในทุกมิติอยู่ในระดับ ๑ ใน ๓ ของภูมิภาคอาเซียนบนพื้นฐานของการพึ่งพาตนเอง ทั้งนี้ เพื่อให้มั่นใจว่าการก้าวไปสู่วิสัยทัศน์กองทัพอากาศอย่างเป็นระบบ เป็นรูปธรรม และมีความยั่งยืนกองทัพอากาศจึงได้กำหนดจุดเน้นของทิศทางการพัฒนาในแต่ละระยะดังนี้

กองทัพอากาศดิจิตอล (Digital Air Force : DAF) มีขีดความสามารถในการปฏิบัติการรบและการปฏิบัติการที่มิใช่การรบเพื่อตอบสนองต่อภัยคุกคามในทุกรูปแบบ โดยกองทัพอากาศต้องสามารถประยุกต์ใช้เทคโนโลยีดิจิตอลเป็นหลัก และบูรณาการเทคโนโลยีกำลังทางอากาศ เทคโนโลยีเครือข่าย และเทคโนโลยีสารสนเทศ เพื่อให้การปฏิบัติภารกิจของกองทัพอากาศเป็นไปอย่างรวดเร็ว เหมาะสม ทันตามความต้องการในทุกสถานการณ์ อันจะเป็นพื้นฐานการพัฒนาสู่การปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง (Network Centric Operations : NCO)

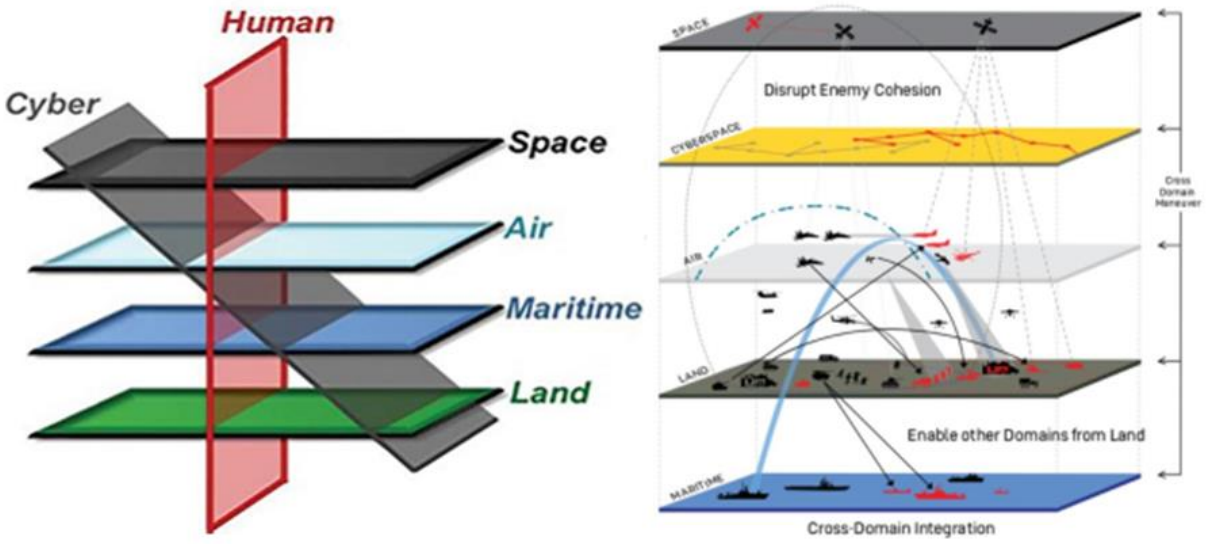
กองทัพอากาศที่ใช้เครือข่ายเป็นศูนย์กลาง (Network Centric Air Force : NCAF) มีขีดความสามารถในการปฏิบัติการรบและการปฏิบัติการที่มิใช่การรบ เพื่อตอบสนองต่อภัยคุกคามในทุกรูปแบบรวมถึงภัยคุกคามรูปแบบใหม่ในยุคสงครามที่ใช้เครือข่ายเป็นศูนย์กลาง (Network Centric Warfare : NCW) โดยกองทัพอากาศต้องสามารถประยุกต์แนวคิดการปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง (NCO) ได้อย่างสมบูรณ์ และต้องสามารถใช้เทคโนโลยีเครือข่ายและระบบเชื่อมโยงข้อมูลทางยุทธวิธี (Tactical Data Link) ได้บนพื้นฐานของการพึ่งพาตนเอง

กองทัพอากาศขับเคลื่อนไปสู่ "กองทัพอากาศชั้นนำในภูมิภาค" โดยสามารถใช้เทคโนโลยีดิจิตอลและแนวคิดการปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลาง (NCO) ในการปฏิบัติการรบ และการปฏิบัติการที่มิใช่การรบ เพื่อตอบสนองต่อภัยคุกคามในทุกรูปแบบ ได้อย่างมีประสิทธิภาพบนพื้นฐานของการพึ่งพาตนเองให้มากที่สุด

รูปที่ ๕ การพัฒนายุทธศาสตร์กองทัพอากาศ ๒๐ ปี (พ.ศ.๒๕๖๐ - ๒๕๗๙)

เพื่อให้เป็นไปตามวิสัยทัศน์กองทัพอากาศ และบทบาทของสงครามไซเบอร์ที่มากขึ้นในการปฏิบัติการสงครามระหว่างกองทัพ กรมเทคโนโลยีสารสนเทศและการสื่อสารจึงได้ปรับโครงสร้างตามอัตรา ทอ.๕๗ โดยมี กองสงครามไซเบอร์ สำนักระบบบัญชาการและควบคุม กรมเทคโนโลยีสารสนเทศและการสื่อสาร (กคซ.สบค.ทสส.ทอ.) เป็นผู้รับผิดชอบภารกิจเกี่ยวกับสงครามไซเบอร์ และเพื่อให้การใช้กำลังทางไซเบอร์ให้มีประสิทธิภาพมากยิ่งขึ้นจึงได้มีการตั้งศูนย์ไซเบอร์กองทัพอากาศ (ศซบ.ทอ.) ขึ้นเมื่อตุลาคม พ.ศ.๒๕๖๒ ตามโครงสร้างอัตรา ทอ.๖๒ โดยให้ กคซ.สบค.ทสส.ทอ. เป็นฝ่ายอำนวยการและฝ่ายเสนาธิการด้านสงครามไซเบอร์ และให้ ศซบ.ทอ.เป็นหน่วยปฏิบัติ (ส่วนกำลังรบ) มีหน้าที่ใช้กำลัง และเตรียมกำลังในยามปกติอีกด้วย

โดยปัจจุบันได้มีการนำแนวคิดการปฏิบัติการแบบการปฏิบัติการรบข้ามมิติ (Cross Domain Operation) ซึ่งเป็นการปฏิบัติการที่รวมเอาความสามารถจากการปฏิบัติการทั้ง ทางบก ทางทะเล ทางอากาศ ทางไซเบอร์ และทางอวกาศ มาผสมผสานกัน และเรียงลำดับการปฏิบัติการในแต่ละส่วนงานอย่างเป็นระบบเพื่อเอาชนะข้าศึกอย่างเด็ดขาด กองทัพอากาศที่มีขีดความสามารถทั้ง ๓ มิติ กล่าวคือ กำลังในมิติอากาศ (Air Domain), กำลังในมิติอวกาศ (Space Domain) และกำลังทางมิติไซเบอร์ (Cyber Domain) ได้จัดตั้งศูนย์ปฏิบัติการรบข้ามมิติ (Multi Domain Operation Center) เพื่อรวมการสั่งการกำลังรบทั้ง ๓ มิติให้สามารถปฏิบัติการรบได้อย่างสอดประสานและเกิดประสิทธิภาพสูงสุด



รูปที่ ๖ การปฏิบัติการรบข้ามมิติ (Multi Domain Operations)

บทที่ ๒
กฎหมายคอมพิวเตอร์และพรบ.ที่เกี่ยวข้อง

๑. พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

พระราชบัญญัตินี้ มาตรการหรือการดำเนินการที่กำหนดขึ้น เพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคาม ทางไซเบอร์ทั้งจากภายในและภายนอกประเทศ อันกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ ดังนั้นเพื่อให้สามารถป้องกัน รับมือและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงที จึงมีการกำหนดกฎหมายนี้ขึ้นมา ซึ่งการตราพระราชบัญญัตินี้ สอดคล้องกับเงื่อนไขที่บัญญัติไว้ในมาตรา ๒๖ ของรัฐธรรมนูญแห่งราชอาณาจักรไทย ที่บัญญัติไว้ว่า “การตรากฎหมายที่มีผลเป็นการจำกัดสิทธิหรือเสรีภาพของบุคคลต้องเป็นไปตามเงื่อนไขที่บัญญัติไว้ในรัฐธรรมนูญ ในกรณีที่รัฐธรรมนูญมิได้บัญญัติเงื่อนไขไว้ว่า กฎหมายดังกล่าว ต้องไม่ขัดต่อหลักนิติธรรม ไม่เพิ่มภาระหรือจำกัดสิทธิหรือเสรีภาพของบุคคลเกินสมควรแก่เหตุ และจะกระทบต่อศักดิ์ศรีความเป็นมนุษย์ของบุคคล มิได้ รวมทั้งต้องระบุเหตุผลความจำเป็นในการจำกัดสิทธิ และเสรีภาพไว้ด้วย กฎหมายตามวรรคหนึ่งต้องมีผลใช้บังคับเป็นการทั่วไป ไม่มุ่งหมายให้ใช้บังคับแก่กรณีใด กรณีหนึ่งหรือแก่บุคคลใดบุคคลหนึ่งเป็นการเจาะจง”

๑.๑ คณะกรรมการ

ในพระราชบัญญัตินี้ได้มีการจัดตั้งคณะกรรมการ ๓ คณะ ได้แก่

๑.๑.๑ คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ หรือ กมช. National Cyber Security Committee (NCSC) มีนายกรัฐมนตรีเป็นประธาน มีหน้าที่เสนอนโยบาย จัดทำแผนแม่บท กำหนดมาตรฐานและแนวทางส่งเสริมพัฒนา ยกระดับทักษะความรู้ของเจ้าหน้าที่ ประสานงานความร่วมมือกับหน่วยงานต่าง ๆ รวมไปถึงการติดตามและประเมินผลการปฏิบัติตามนโยบายที่ได้ถูกกำหนดแล้ว

๑.๑.๒ คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์

คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ หรือ กกม. มีรัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมเป็นประธาน มีหน้าที่ดูแลและดำเนินการเพื่อรับมือกับภัยคุกคามไซเบอร์ในระดับร้ายแรง กำหนดแนวทางปฏิบัติสำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานทางสารสนเทศ รวมทั้งกำหนดมาตรการในการประเมินความเสี่ยง การตอบสนองและรับมือกับภัยคุกคามที่เกิดขึ้น

๑.๑.๓ คณะกรรมการบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์

คณะกรรมการบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือ กบส. มีรัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมเป็นประธาน ทำหน้าที่ดูแลงานด้านการบริหารงานทั่วไป

๑.๒ ภัยคุกคามทางไซเบอร์

ทางคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์จะเป็นผู้กำหนดลักษณะของภัยคุกคามทางไซเบอร์ โดยแบ่งออกเป็น ๓ ระดับ ดังนี้

๑.๒.๑ ภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง

หมายถึง ภัยคุกคามทางไซเบอร์ในระดับที่ทำให้ระบบคอมพิวเตอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญของ ประเทศ หรือการให้บริการของรัฐ ด้อยประสิทธิภาพลง

๑.๒.๒ ภัยคุกคามทางไซเบอร์ในระดับร้ายแรง

หมายถึง ภัยคุกคามทางไซเบอร์ในระดับที่มีการโจมตีระบบคอมพิวเตอร์ หรือข้อมูลคอมพิวเตอร์ โดยมุ่งหมาย เพื่อ โจมตีและการโจมตีดังกล่าวมีผลทำให้ระบบคอมพิวเตอร์หรือโครงสร้างสำคัญทางสารสนเทศ ที่เกี่ยวข้องกับการให้บริการของโครงสร้างพื้นฐานสำคัญของ ประเทศ เสียหายจนไม่สามารถทำงานหรือให้บริการได้

๑.๒.๓ ภัยคุกคามทางไซเบอร์ในระดับวิกฤติ

หมายถึง ภัยคุกคามทางไซเบอร์ในระดับวิกฤติ ที่มีลักษณะ ล้มเหลวทั้งระบบจนรัฐไม่สามารถควบคุมการทำงานจาก ส่วนกลางของระบบคอมพิวเตอร์ของรัฐได้ หรือ ทำให้ประเทศหรือส่วนใดส่วนหนึ่งของประเทศตกอยู่ในภาวะคับขัน

๑.๓ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติได้มีประกาศ เรื่อง การกำหนดหลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและการมอบหมายการควบคุมและกำกับดูแล พ.ศ. ๒๕๖๔ โดยหน่วยงานที่ได้รับมอบหมายให้ดำเนินการควบคุมและกำกับดูแลด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แก่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศมี ๘ ด้าน ดังนี้

๑.๓.๑ ด้านความมั่นคงของรัฐ

ได้แก่ สำนักงานปลัดกระทรวงกลาโหม, สำนักงานตำรวจแห่งชาติ, สำนักงานสภาความมั่นคงแห่งชาติ

๑.๓.๒ ด้านบริการภาครัฐที่สำคัญ

ได้แก่ กระทรวงการคลัง, กรมศุลกากร, กรมการปกครอง, สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน), กรมชลประทาน

๑.๓.๓ ด้านการเงินการธนาคาร

ได้แก่ ธนาคารแห่งประเทศไทย, สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์

๑.๓.๔ ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม

ได้แก่ สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ

๑.๓.๕ ด้านการขนส่งและโลจิสติกส์

ได้แก่ สำนักงานตำรวจแห่งชาติ, กรมการขนส่งทางราง, สำนักงานปลัดกระทรวงคมนาคม, สำนักงานการบินพลเรือนแห่งประเทศไทย

๑.๓.๖ ด้านพลังงานและสาธารณูปโภค

ได้แก่ กระทรวงพลังงาน, การประปาส่วนภูมิภาค (เฉพาะบริการส่วนภูมิภาค)

๑.๓.๗ ด้านสาธารณสุข

ได้แก่ สำนักงานปลัดกระทรวงสาธารณสุข, สำนักงานคณะกรรมการอาหารและยา, สำนักงานปรมาณูเพื่อสันติ

๑.๓.๘ ด้านอื่น ๆ

ได้แก่ หน่วยงานด้านอื่น ๆ ที่คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติได้กำหนดเพิ่มเติม

๑.๔ การรับมือกับภัยคุกคามทางไซเบอร์

ในกรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ต่อระบบสารสนเทศซึ่งอยู่ในความดูแลรับผิดชอบของหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศใด ให้หน่วยงานนั้นดำเนินการตรวจสอบข้อมูลที่เกี่ยวข้อง ข้อมูลคอมพิวเตอร์ และระบบคอมพิวเตอร์ของหน่วยงานนั้น รวมถึงพฤติการณ์แวดล้อมของตน เพื่อประเมินว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้นหรือไม่ หากผลการตรวจสอบปรากฏว่าเกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ขึ้น ให้ดำเนินการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐาน ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานนั้น และแจ้งไปยังสำนักงานและหน่วยงานควบคุมหรือกำกับดูแลของตนโดยเร็ว ในกรณีที่หน่วยงานหรือบุคคลใดพบอุปสรรคหรือปัญหาในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ของตน หน่วยงานหรือบุคคลนั้นอาจร้องขอความช่วยเหลือไปยังสำนักงาน

๑.๕ บทลงโทษ

ในพระราชบัญญัตินี้มีบทลงโทษหลัก ๒ มาตรา ได้แก่

๑.๕.๑ มาตรา ๗๐

ห้ามมิให้พนักงานเจ้าหน้าที่ตามพระราชบัญญัตินี้เปิดเผยหรือส่งมอบข้อมูล คอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ หรือข้อมูล ของผู้ใช้บริการ ที่ได้มาตามพระราชบัญญัตินี้ให้แก่บุคคลใด ผู้ใดฝ่าฝืนต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาท หรือทั้งจำทั้งปรับ ความในวรรคหนึ่งมิให้ใช้บังคับกับการกระทำเพื่อประโยชน์ ในการดำเนินคดีกับผู้กระทำความผิด

ตามพระราชบัญญัตินี้หรือผู้กระทำความผิดตามกฎหมายอื่นหรือ เพื่อประโยชน์ในการดำเนินคดี กับพนักงานเจ้าหน้าที่เกี่ยวกับการใช้อำนาจหน้าที่โดยมิชอบ

๑.๕.๒ มาตรา ๗๒

ผู้ใดล่วงรู้ข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์ ข้อมูลของผู้ใช้บริการ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ที่พนักงานเจ้าหน้าที่ได้มาตามพระราชบัญญัตินี้ และเปิดเผยข้อมูลนั้นต่อผู้หนึ่งผู้ใดโดยมิชอบ ต้องระวางโทษจำคุกไม่เกิน ๒ ปี หรือปรับไม่เกิน ๔๐,๐๐๐ บาท หรือทั้งจำทั้งปรับ

นอกจากนี้นักศึกษายังสามารถศึกษาเพิ่มเติมได้จาก พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ตาม QR Code นี้

รูปที่ ๗ QR Code พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๒ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๕ หรือที่นิยมเรียกกันว่า PDPA ย่อมาจาก Personal Data Protection Act B.E. 2562 (2019) เป็นกฎหมายว่าด้วยการให้สิทธิ์กับเจ้าของข้อมูลส่วนบุคคล สร้างมาตรฐานการรักษาข้อมูลส่วนบุคคลให้ปลอดภัย และนำไปใช้ให้ถูกวัตถุประสงค์ตามคำยินยอมที่เจ้าของข้อมูลส่วนบุคคลอนุญาต โดยได้ประกาศไว้ในราชกิจจานุเบกษาเมื่อวันที่ ๒๔ พฤษภาคม ๒๕๖๒ และปัจจุบันได้ถูกเลื่อนให้มีผลบังคับใช้ในวันที่ ๑ มิถุนายน พ.ศ.๒๕๖๕

๒.๑ ความเป็นมาของพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๕

ประเทศไทยได้อ้างอิง PDPA มาจากกฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป General Data Protection Regulation (GDPR) โดยอยู่ในแผนพัฒนาดิจิทัลเพื่อเศรษฐกิจและสังคมภายใต้ยุทธศาสตร์ชาติ ๒๐ ปี

รูปที่ ๘ ยุทธศาสตร์ชาติ ๒๐ ปี

๒.๒ ข้อมูลส่วนบุคคล

ข้อมูลส่วนบุคคล คือ ข้อมูลเกี่ยวกับบุคคลที่สามารถระบุตัวบุคคลนั้นได้ ทั้งทางตรงหรือทางอ้อม แต่จะไม่นับรวมข้อมูลของผู้ที่เสียชีวิตไปแล้ว สามารถแบ่งได้ ๒ ประเภท ดังนี้

๒.๒.๑ ข้อมูลส่วนบุคคล

คือ ข้อมูลเกี่ยวกับบุคคลที่สามารถระบุตัวบุคคลนั้นได้ ทั้งทางตรงหรือทางอ้อม แต่จะไม่นับรวมข้อมูลของผู้ที่เสียชีวิตไปแล้ว เช่น ชื่อ ที่อยู่ บัตรประชาชน เบอร์โทรศัพท์ เลขที่บัญชีธนาคาร บัตรเครดิต เป็นต้น

๒.๒.๒ ข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Data)

คือ ข้อมูลที่เปลี่ยนยาก หรือ เปลี่ยนไม่ได้ เป็นข้อมูลที่จะทำให้เกิดอคติในสังคม ซึ่งจะเป็นข้อมูลที่จะทำให้เกิดความลำเอียง อาจจะทำให้เจ้าของข้อมูลนั้นสูญเสียโอกาสในการดำเนินชีวิตไป เช่น ข้อมูลลายนิ้วมือหรือข้อมูลใบหน้า ศาสนา ข้อมูลสุขภาพ รสนิยมทางเพศ ความคิดเห็นทางการเมือง ข้อมูลทางพันธุกรรม เป็นต้น

๒.๓ วัตถุประสงค์

PDPA มีวัตถุประสงค์ ดังนี้

๒.๓.๑ เพื่อให้การคุ้มครองข้อมูลส่วนบุคคลมีประสิทธิภาพ โดยกำหนดหน้าที่และความรับผิดชอบที่เหมาะสม

๒.๓.๒ เพื่อให้มีมาตรการเยียวยาจากการถูกละเมิดสิทธิในข้อมูลส่วนบุคคลที่มีประสิทธิภาพ

๒.๓.๓ เพื่อส่งเสริมการใช้ข้อมูลในการพัฒนานวัตกรรมอย่างมั่นคงปลอดภัย

๒.๓.๔ เพื่อสร้างความโปร่งใสและเป็นธรรม ในการใช้ข้อมูลส่วนบุคคล

๒.๔ ขอบเขตการบังคับใช้

PDPA ใช้บังคับแก่การเก็บรวบรวม การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคลโดยผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูล ส่วนบุคคลซึ่งอยู่ในราชอาณาจักร

มีผลใช้บังคับถึงกรณีผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคลที่อยู่นอกราชอาณาจักรหากมีกิจกรรม ดังนี้

๒.๔.๑ เสนอขายสินค้าหรือบริการแก่เจ้าของข้อมูลซึ่งอยู่ในราชอาณาจักรไม่ว่าจะมีการชำระเงินหรือไม่

๒.๔.๒ การเฝ้าติดตามพฤติกรรมของเจ้าของข้อมูลที่เกิดขึ้นในราชอาณาจักร

๒.๕ บทบาทและหน้าที่

ใน PDPA ได้แบ่งบทบาทและหน้าที่ของบุคคลแต่ละจำพวกไว้ ดังนี้

๒.๕.๑ เจ้าของข้อมูลส่วนบุคคล Data Subject (DS)

คือ ประชาชนทุกกคน หากเป็นหน่วยงานทั่วไปก็หมายถึง ลูกค้า พนักงาน รวมถึง Outsource ด้วย โดยมีหน้าที่ให้ความยินยอมหรือไม่ให้ความยินยอมในการเก็บรวบรวม การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคล

๒.๕.๒ ผู้ควบคุมข้อมูลส่วนบุคคล Data Controller (DC)

คือ หน่วยงาน องค์กร สถาบัน ที่ใช้ประโยชน์จากข้อมูลส่วนบุคคล บุคคลธรรมดาก็อาจเป็นผู้ควบคุมข้อมูลได้เช่นเดียวกัน โดยมีหน้าที่ตัดสินใจในการเก็บรวบรวม การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคลที่ได้มาจากเจ้าของข้อมูลส่วนบุคคล

๒.๕.๓ ผู้ประมวลผลข้อมูลส่วนบุคคล Data Processor (DP)

คือ ผู้ที่ทำตามคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคลโดยหลักคือ Outsource ที่รับจ้าง โดยมีหน้าที่ทำตามคำสั่งของผู้ควบคุมข้อมูลส่วนบุคคลในการเก็บรวบรวม การใช้ หรือการเปิดเผยข้อมูลส่วนบุคคลที่ได้มาจากเจ้าของข้อมูลส่วนบุคคล

๒.๕.๔ เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล Data Protection Officer (DPO)

คือ คนที่ได้รับมอบหมายเพื่อทำหน้าที่ให้คำแนะนำหรือตรวจสอบการคุ้มครองข้อมูลส่วนบุคคลของ หน่วยงาน องค์กร สถาบัน ให้เป็นไปตามกฎหมาย โดยมีหน้าที่ให้คำแนะนำหรือตรวจสอบการคุ้มครองข้อมูลส่วนบุคคลให้เป็นไปตามกฎหมาย

๒.๖ บทลงโทษ

ในพระราชบัญญัตินี้มีบทลงโทษแบ่งออกเป็น ๓ ประเภท ได้แก่

๒.๖.๑ ความรับผิดทางแพ่ง

กรณีผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลฝ่าฝืน หรือไม่ปฏิบัติตามบทบัญญัติแห่ง พ.ร.บ. นี้ ทำให้เกิดความเสียหายต่อเจ้าของข้อมูลส่วนบุคคล จะต้องจ่ายค่าสินไหมทดแทนจากความเสียหายที่ได้รับจริง และศาลสั่งลงโทษเพิ่มขึ้นได้แต่ไม่เกินสองเท่าของสินไหมทดแทนที่แท้จริง

๒.๖.๒ โทษทางปกครอง

แบ่งออกได้เป็น ๓ กรณี ดังนี้

๒.๖.๒.๑ กรณีผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลไม่ขอความยินยอมให้ถูกต้อง ไม่แจ้งรายละเอียดให้เจ้าของข้อมูลทราบ ไม่ให้เจ้าของข้อมูลเข้าถึงข้อมูลตามสิทธิ ไม่จัดทำบันทึกรายการ ไม่จัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล ไม่จัดให้มีการสนับสนุนการปฏิบัติหน้าที่ของ DPO มีโทษปรับไม่เกิน ๑,๐๐๐,๐๐๐ บาท

๒.๖.๒.๒ กรณีผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากฐานทางกฎหมาย ไม่ได้แจ้งวัตถุประสงค์การใช้งานใหม่ เก็บข้อมูลเกินความจำเป็น ขอความยินยอมที่เป็นการหลอกลวงให้เข้าใจผิด ไม่จัดให้มีมาตรการรักษาความปลอดภัยที่เหมาะสม ไม่แจ้งเหตุเมื่อมีการละเมิดข้อมูล โอนข้อมูลไปต่างประเทศโดยไม่ชอบด้วยกฎหมาย ไม่ตั้งตัวแทนในราชอาณาจักร มีโทษปรับไม่เกิน ๓,๐๐๐,๐๐๐ บาท

๒.๖.๒.๓ กรณีผู้ควบคุมข้อมูลส่วนบุคคลหรือผู้ประมวลผลข้อมูลส่วนบุคคลเก็บรวบรวม ใช้ เปิดเผยหรือโอนข้อมูลส่วนบุคคลอ่อนไหวโดยไม่ชอบด้วยกฎหมาย มีโทษปรับไม่เกิน ๕,๐๐๐,๐๐๐ บาท

๒.๖.๓ โทษทางอาญา

แบ่งออกได้เป็น ๓ กรณี ดังนี้

๒.๖.๓.๑ กรณีผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือเปิดเผยข้อมูลส่วนบุคคลอ่อนไหว โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล หรือผิดจากวัตถุประสงค์ที่ได้แจ้งไว้ หรือ โอนข้อมูลส่วนบุคคลอ่อนไหวไปยังต่างประเทศโดยไม่ชอบด้วยกฎหมาย “อันทำให้ผู้อื่นเกิดความเสียหาย เสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย” ต้องระวางโทษจำคุกไม่เกิน ๖ เดือน หรือ ปรับไม่เกิน ๕๐๐,๐๐๐ บาท หรือทั้งจำทั้งปรับ

๒.๖.๓.๒ กรณีผู้ควบคุมข้อมูลส่วนบุคคลใช้หรือเปิดเผยข้อมูลส่วนบุคคลอ่อนไหว โดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล หรือผิดจากวัตถุประสงค์ที่ได้แจ้งไว้ หรือ โอนข้อมูลส่วนบุคคลอ่อนไหวไปยังต่างประเทศโดยไม่ชอบด้วยกฎหมาย “เพื่อแสวงหาประโยชน์ที่มิควรได้โดยชอบด้วยกฎหมายสำหรับตนเองหรือผู้อื่น” ต้องระวางโทษจำคุกไม่เกิน ๑ ปี หรือ ปรับไม่เกิน ๑,๐๐๐,๐๐๐ บาท หรือทั้งจำทั้งปรับ

๒.๖.๓.๓ กรณีผู้ใดล่วงรู้ข้อมูลส่วนบุคคลของผู้อื่นเนื่องจากการปฏิบัติหน้าที่ ตาม พ.ร.บ. นี้ แล้วนำไปเปิดเผยแก่ผู้อื่น (เว้นแต่เข้าข้อยกเว้น) ต้องระวางโทษจำคุกไม่เกิน ๖ เดือน หรือ ปรับไม่เกิน ๕๐๐,๐๐๐ บาท หรือทั้งจำทั้งปรับ

นอกจากนี้นักศึกษายังสามารถศึกษาเพิ่มเติมได้จาก พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ตาม QR Code นี้

รูปที่ ๙ QR Code พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

๓ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๖๐ ได้แก้ไขเพิ่มเติมจากฉบับแรกที่บังคับใช้มาเมื่อ ๑๐ ปีที่แล้ว โดยมีเนื้อหาเข้มข้นขึ้น มุ่งหวังปกป้องคุ้มครองสิทธิ์ของประชาชน ไม่ให้ถูกคุกคามหรือล่วงละเมิด สิ่งที่แตกต่างจากเดิม คือเพิ่มการดูแลความเป็นส่วนตัวให้ประชาชนสามารถปฏิเสธจดหมายอิเล็กทรอนิกส์ที่เป็นสแปม ซึ่งไม่ต้องการรับได้ง่ายขึ้น โดยออกกฎเกณฑ์ควบคุมการส่งที่ชัดเจน และมีบทลงโทษปรับผู้ส่งสูงสุดถึง ๒ แสนบาท แต่ความผิดฐานแพร่ข้อมูลนั้น จะไม่ครอบคลุมถึงคดีการหมิ่นประมาท แต่เป็นการเอาผิดเฉพาะกับการฉ้อโกง ปลอม หรือเผยแพร่ข้อมูลที่เป็นเท็จเท่านั้น และไม่สามารถใช้กฎหมายฉบับนี้ เพียงฉบับเดียวฟ้องร้องได้

ที่สำคัญการเผยแพร่ภาพตัดต่อ จากเดิมมีความผิดเฉพาะภาพบุคคลที่ยังมีชีวิตเท่านั้น แต่กฎหมายฉบับนี้ให้ความคุ้มครองไปถึงภาพผู้ที่เสียชีวิตไปแล้วด้วย โดยเจ้าหน้าที่สามารถยึดและทำลายภาพตัดต่อได้ หากการเผยแพร่ภาพผู้เสียชีวิต ทำให้บิดามารดา คู่สมรส หรือบุตร เสื่อมเสียชื่อเสียงหรือได้รับความอับอาย ซึ่งสามารถฟ้องร้องดำเนินคดีได้ ไม่ว่าผู้กระทำผิดจะเป็นคนไทยหรือคนต่างชาติ จะต้องเข้ามารับโทษในประเทศไทยเท่านั้น

๓.๑ ตัวอย่างการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

หากเรามองถึงกองทัพอากาศแล้ว จะมองในด้านของการรักษาความมั่นคงปลอดภัยเป็นหลัก ดังนั้นนี่จึงเป็นตัวอย่างการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ในด้านความมั่นคงปลอดภัย

๓.๑.๑ มาตรา ๕ - ๘ การเข้าถึงระบบ ข้อมูล ของผู้อื่นโดยมิชอบ

๓.๑.๑.๑ เข้าถึงระบบคอมพิวเตอร์ ต้องระวางโทษจำคุกไม่เกิน ๖ เดือน หรือ ปรับไม่เกิน ๑๐,๐๐๐ บาท หรือทั้งจำทั้งปรับ

๓.๑.๑.๒ เข้าถึงข้อมูลคอมพิวเตอร์ ต้องระวางโทษจำคุกไม่เกิน ๒ ปี หรือ ปรับไม่เกิน ๔๐,๐๐๐ บาท หรือทั้งจำทั้งปรับ

๓.๑.๑.๓ ล่วงรู้มาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์และนำไปเปิดเผย ต้องระวางโทษจำคุกไม่เกิน ๑ ปี หรือ ปรับไม่เกิน ๒๐,๐๐๐ บาท หรือทั้งจำทั้งปรับ

๓.๑.๑.๔ ดักรับข้อมูลคอมพิวเตอร์ ต้องระวางโทษจำคุกไม่เกิน ๒ ปี หรือ ปรับไม่เกิน ๔๐,๐๐๐ บาท หรือทั้งจำทั้งปรับ

๓.๑.๒ มาตรา ๙ - ๑๐ แก้ไข ดัดแปลง ทำให้ข้อมูลเสียหาย

๓.๑.๒.๑ ทำให้ระบบคอมพิวเตอร์ของผู้อื่นไม่สามารถทำงานได้ตามปกติ ต้องระวางโทษจำคุกไม่เกิน ๕ ปี หรือ ปรับไม่เกิน ๑๐๐,๐๐๐ บาท หรือทั้งจำทั้งปรับ

๓.๑.๒.๒ กรณีเป็นการกระทำต่อระบบหรือข้อมูลคอมพิวเตอร์ตามมาตรา ๑๒ ต้องระวางโทษจำคุกสูงสุดไม่เกิน ๑๕ ปี และ ปรับสูงสุดไม่เกิน ๓๐๐,๐๐๐ บาท

๓.๑.๓ มาตรา ๑๑ ส่งข้อมูลหรืออีเมลล์ก่อกวนผู้อื่น

๓.๑.๓.๑ ส่งโดยปกปิดหรือปลอมแปลงแหล่งที่มา ต้องระวางโทษ ปรับไม่เกิน ๑๐๐,๐๐๐ บาท

๓.๑.๓.๒ ส่งโดยไม่เปิดโอกาสให้ปฏิเสธการคตอบรับได้โดยง่าย ต้องระวางโทษจำคุกไม่เกิน ๒ ปี หรือ ปรับไม่เกิน ๔๐,๐๐๐ บาท หรือทั้งจำทั้งปรับ

๓.๑.๔ มาตรา ๑๒ เข้าถึงระบบข้อมูลด้านความมั่นคงโดยมิชอบ

๓.๑.๔.๑ เข้าถึงระบบหรือข้อมูลคอมพิวเตอร์หรือล่วงรู้มาตรการการป้องกันการเข้าถึงระบบแบะนำไปเปิดเผย กรณีไม่เกิดความเสียหาย ต้องระวางโทษจำคุกสูงสุดไม่เกิน ๗ ปี และ ปรับสูงสุดไม่เกิน ๑๔๐,๐๐๐ บาท

๓.๑.๔.๒ เข้าถึงระบบหรือข้อมูลคอมพิวเตอร์หรือล่วงรู้มาตรการการป้องกันการเข้าถึงระบบแบะนำไปเปิดเผย กรณีเกิดความเสียหาย ต้องระวางโทษจำคุกสูงสุดไม่เกิน ๑๐ ปี และ ปรับสูงสุดไม่เกิน ๒๐๐,๐๐๐ บาท

๓.๑.๔.๓ เข้าถึงระบบหรือข้อมูลคอมพิวเตอร์หรือล่วงรู้มาตรการการป้องกันการเข้าถึงระบบแบะนำไปเปิดเผย กรณีเป็นเหตุให้ผู้อื่นถึงแก่ความตาย ต้องระวางโทษจำคุกสูงสุดไม่เกิน ๒๐ ปี และ ปรับสูงสุดไม่เกิน ๔๐๐,๐๐๐ บาท

๓.๑.๕ มาตรา ๑๕ ให้ความร่วมมือ ยินยอม รู้เห็นเป็นใจ

๓.๑.๕.๑ ผู้ให้บริการที่ให้ความร่วมมือ ยินยอม รู้เห็นเป็นใจให้มีการกระทำผิดต่อระบบคอมพิวเตอร์ ต้องระวางโทษเช่นเดียวกับผู้กระทำผิด ผู้ให้บริการมีหน้าที่เก็บข้อมูลการใช้งานไว้ไม่น้อยกว่า ๙๐ วัน กรณีจำเป็น ศาลอาจสั่งให้เก็บเพิ่มได้ไม่เกิน ๒ ปี

รูปที่ ๑๐ QR Code พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒)

พ.ศ. ๒๕๖๐

๔ พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔

หลักการและเหตุผล ในการประกาศใช้พระราชบัญญัติฉบับนี้ คือ โดยที่การทำธุรกรรมในปัจจุบันมีแนวโน้มที่จะปรับเปลี่ยนวิธีการในการติดต่อสื่อสารที่อาศัยการพัฒนาการเทคโนโลยีทางอิเล็กทรอนิกส์ซึ่งมีความสะดวก รวดเร็วและมีประสิทธิภาพ แต่เนื่องจากการทำธุรกรรมทางอิเล็กทรอนิกส์ดังกล่าวมีความแตกต่างจากวิธีการทำธุรกรรมซึ่งมีกฎหมายรองรับอยู่ในปัจจุบันเป็นอย่างมาก อันส่งผลให้ต้องมีกา รรองรับสถานะทางกฎหมายของข้อมูลทางอิเล็กทรอนิกส์ให้เสมอกับการทำเป็นหนังสือ หรือหลักฐานเป็นหนังสือ การรับรองวิธีการส่งและรับข้อมูลอิเล็กทรอนิกส์ การใช้ลายมือชื่ออิเล็กทรอนิกส์ ตลอดจนการรับฟังพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ เพื่อเป็นการส่งเสริมการทำธุร กรรมทางอิเล็กทรอนิกส์ให้น่าเชื่อถือ และมีผลในทางกฎหมายเช่นเดียวกับการทำธุรกรรมโดยวิธีการทั่วไปที่เคยปฏิบัติอยู่เดิม ควรกำหนดให้มีคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ทำหน้าที่วางนโยบายกำหนดหลักเกณฑ์เพื่อส่งเสริมการทำธุรกรรมทางอิเล็กทรอนิกส์ ติดตามดูแลการประกอบธุรกิจเกี่ยวกับ ธุรกรรมทางอิเล็กทรอนิกส์ รวมทั้งมีหน้าที่ในการส่งเสริมการพัฒนาการทางเทคโนโลยีเพื่อติดตามความก้าวหน้าของเทคโนโลยี ซึ่งมีการเปลี่ยนแปลงและพัฒนาศักยภาพตลอดเวลาให้มีมาตรฐานน่าเชื่อถือ ตลอดจนเสนอแนะแนวทางแก้ไขปัญหาและอุปสรรคที่เกี่ยวข้อง อันจะเป็นการส่งเสริมการใช้ธุรกรรมทางอิเล็กทรอนิกส์ทั้งภายในประเทศและระหว่างประเทศ ด้วยการมีกฎหมายรองรับในลักษณะที่เป็นเอกรูป และสอดคล้องกับมาตรฐานที่นานาประเทศยอมรับ

๔.๑ สาระสำคัญ

๔.๑.๑ ธุรกรรมทางอิเล็กทรอนิกส์

๔.๑.๑.๑ ในกรณีที่กฎหมายกำหนดให้การใดต้องทำเป็นหนังสือ มีหลักฐานเป็นหนังสือหรือมีเอกสารมาแสดง ถ้าได้มีการจัดทำข้อความขึ้นเป็นข้อมูลอิเล็กทรอนิกส์ที่สามารถเข้าถึงและนำกลับมาใช้ได้โดยความหมายไม่เปลี่ยนแปลง ให้ถือว่าข้อความนั้นได้ทำเป็นหนังสือ มีหลักฐานเป็นหนังสือ หรือมีเอกสารมาแสดงแล้ว และในกรณีที่บุคคลลงลายมือชื่อในหนังสือ ให้ถือว่าข้อมูลอิเล็กทรอนิกส์นั้นมีการลงลายมือชื่อแล้ว ถ้าบุคคลนั้นใช้วิธีการที่สามารถระบุตัวเจ้าของลายมือชื่อได้และสามารถจะแสดงได้ว่าเจ้าของลายมือชื่อนั้น

รับรองข้อความในข้อมูลอิเล็กทรอนิกส์ว่าเป็นของตน โดยวิธีดังกล่าวจะต้องเป็นวิธีการที่เชื่อถือได้โดยเหมาะสมกับวัตถุประสงค์ของการสร้างหรือส่งข้อมูลอิเล็กทรอนิกส์โดยคำนึงถึงพฤติการณ์แวดล้อมหรือข้อตกลงของคู่กรณี

๔.๑.๑.๒ ในกรณีที่กฎหมายกำหนดให้นำเสนอหรือเก็บรักษาข้อความใดในสภาพที่เป็นมาแต่เดิมอย่างเอกสารต้นฉบับ ถ้าได้นำเสนอหรือเก็บรักษาในรูปข้อมูลอิเล็กทรอนิกส์โดยใช้วิธีการที่เชื่อถือได้ในการรักษาความถูกต้องของข้อความ ความครบถ้วนและไม่มีการเปลี่ยนแปลงใดๆ ของข้อความ เว้นแต่การรับรองหรือบันทึกเพิ่มเติมหรือการเปลี่ยนแปลงใดๆ และสามารถที่จะแสดงข้อความนั้นในภายหลังได้แล้ว ให้ถือว่าได้มีการนำเสนอหรือเก็บรักษาเป็นเอกสารต้นฉบับตามกฎหมายแล้ว

๔.๑.๑.๓ ห้ามไม่ให้ปฏิเสธการรับฟังข้อมูลอิเล็กทรอนิกส์เป็นพยานหลักฐานในกระบวนการพิจารณาตามกฎหมายเพียงเพราะเหตุว่าเป็นข้อมูลอิเล็กทรอนิกส์ โดยการพิเคราะห์ถึงความน่าเชื่อถือของข้อมูลดังกล่าวจะพิเคราะห์ถึงลักษณะหรือวิธีการที่ใช้สร้าง เก็บรักษา หรือสื่อสารข้อมูลอิเล็กทรอนิกส์ ลักษณะหรือวิธีการรักษาความครบถ้วนและไม่มีการเปลี่ยนแปลงของข้อความ ลักษณะหรือวิธีการที่ใช้ในการระบุหรือแสดงตัวผู้ส่งข้อมูล รวมทั้งพฤติการณ์ที่เกี่ยวข้องทั้งปวง

๔.๑.๒ ลายมือชื่ออิเล็กทรอนิกส์

๔.๑.๒.๑ ลายมือชื่ออิเล็กทรอนิกส์ หมายความว่า อักษร อักขระ ตัวเลข เสียงหรือสัญลักษณ์อื่นใดที่สร้างขึ้นให้อยู่ในรูปแบบอิเล็กทรอนิกส์ซึ่งนำมาใช้ประกอบกับข้อมูลอิเล็กทรอนิกส์เพื่อแสดงความสัมพันธ์ระหว่างบุคคลกับข้อมูลอิเล็กทรอนิกส์ โดยมีวัตถุประสงค์เพื่อระบุตัวบุคคลผู้เป็นเจ้าของลายมือชื่ออิเล็กทรอนิกส์ที่เกี่ยวข้องกับข้อมูลอิเล็กทรอนิกส์นั้นและเพื่อแสดงว่าบุคคลดังกล่าวยอมรับข้อความในข้อมูลอิเล็กทรอนิกส์นั้น

ลายมือชื่ออิเล็กทรอนิกส์ที่มีลักษณะดังนี้ให้ถือว่าเป็นลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้ เช่น ข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์นั้นได้เชื่อมโยงไปยังเจ้าของลายมือชื่อโดยไม่เชื่อมโยงไปยังบุคคลอื่นภายใต้สภาพที่นำมาใช้,ในขณะสร้างลายมือชื่ออิเล็กทรอนิกส์นั้น ข้อมูลสำหรับใช้สร้างลายมือชื่ออิเล็กทรอนิกส์อยู่ภายใต้การควบคุมของเจ้าของลายมือชื่อโดยไม่มีการควบคุมของบุคคลอื่น,การเปลี่ยนแปลงใดๆ ที่เกิดแก่ลายมือชื่ออิเล็กทรอนิกส์ นับแต่เวลาที่ได้สร้างขึ้นสามารถจะตรวจพบได้ และในกรณีที่กฎหมายกำหนดให้การลงลายมือชื่ออิเล็กทรอนิกส์เป็นไปเพื่อรับรองความครบถ้วนและไม่มีการเปลี่ยนแปลงของข้อความ การเปลี่ยนแปลงใดแก่ข้อความนั้นสามารถตรวจพบได้นับแต่เวลาที่ลงลายมือชื่ออิเล็กทรอนิกส์ เป็นต้น ซึ่งก็อาจยังมีวิธีการอื่นอีกที่แสดงได้ว่าเป็นลายมือชื่ออิเล็กทรอนิกส์ที่เชื่อถือได้

๔.๑.๓ บทกำหนดโทษ

ผู้ใดประกอบธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์โดยไม่แจ้งหรือขึ้นทะเบียนต่อพนักงานเจ้าหน้าที่ตามที่กำหนดในพระราชกฤษฎีกาหรือฝ่าฝืนคำสั่งห้ามการประกอบธุรกิจของคณะกรรมการหรือประกอบธุรกิจบริการเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์โดยไม่ได้รับใบอนุญาต ต้องได้รับโทษตามที่กฎหมายกำหนด โดยความผิดดังกล่าวนี้ รวมถึงการกระทำโดยนิติบุคคล ผู้จัดการหรือผู้แทนนิติบุคคล

หรือผู้ซึ่งมีส่วนร่วมในการดำเนินงานของนิติบุคคลด้วย เว้นแต่จะพิสูจน์ได้ว่าตนมิได้รู้เห็นหรือมีส่วนร่วมในการกระทำความผิดนั้น

รูปที่ ๑๑ QR Code พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔

บทที่ ๓
ระเบียบกองทัพอากาศว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ

๑. หลักการอ้างอิงในการจัดทำระเบียบ ทอ.ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ

ภายใต้โครงสร้างกองทัพอากาศ กำหนดให้ กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศทสส.ทอ. เป็นหน่วยงานฝ่ายเสนาธิการ รับผิดชอบเกี่ยวกับงานเชิงนโยบายด้านเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งการปฏิบัติการไซเบอร์และการปฏิบัติการสงครามอิเล็กทรอนิกส์ของกองทัพอากาศ มีกองสงครามไซเบอร์เป็นหน่วยงานรับผิดชอบด้านสงครามไซเบอร์ โดยมีหน่วยงานที่เกี่ยวข้อง คือ กรมสื่อสารอิเล็กทรอนิกส์ทหารอากาศ (สอ.ทอ.) เป็นหน่วยงานสนับสนุนและซ่อมบำรุงที่รับผิดชอบเกี่ยวกับงานด้านระบบคอมพิวเตอร์ ระบบเครือข่าย ระบบโทรคมนาคม และการติดต่อสื่อสารเชิงปฏิบัติ มีศูนย์คอมพิวเตอร์และกองสื่อสารโทรคมนาคมเป็นหน่วยงานรับผิดชอบ รวมถึงมีหน่วยขึ้นตรงของกองทัพอากาศที่จะต้องรับผิดชอบดูแลระบบเทคโนโลยีสารสนเทศและการสื่อสารที่มีใช้งานด้วย

กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ (ทสส.ทอ.) มีหน้าที่พิจารณา เสนอนโยบาย วางแผน อำนวยการ ประสานงาน ควบคุม กำกับ การพัฒนา และดำเนินการด้านระบบบัญชาการและควบคุม ระบบเครือข่าย เทคโนโลยีสารสนเทศและการสงครามสารสนเทศ การสื่อสารอิเล็กทรอนิกส์ ปฏิบัติการสงครามอิเล็กทรอนิกส์ และปฏิบัติการสงครามไซเบอร์ กับมีหน้าที่จัดการความรู้ ควบคุม ประเมินผล และตรวจตรากิจการด้านสารสนเทศสงครามอิเล็กทรอนิกส์ และสงครามไซเบอร์ รวมถึงบริหารจัดการในฐานะหัวหน้าสายวิทยาการสารสนเทศและสงครามอิเล็กทรอนิกส์ เกี่ยวกับ การจัดการความรู้ การบริหารการฝึกและศึกษาการบริหารกำลังพลจำพวกทหารสารสนเทศและสงครามอิเล็กทรอนิกส์ ภายใต้โครงสร้างหน่วยของ ทสส.ทอ.

มีหน่วยรับผิดชอบที่เกี่ยวข้อง คือ กองสงครามไซเบอร์ สำนักระบบบัญชาการและควบคุม กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ (กคช.สบค.ทสส.ทอ.) มีหน้าที่พิจารณา เสนอนโยบาย วางแผน อำนวยการ ประสานงาน ควบคุม กำกับการ พัฒนา และดำเนินการด้านสงครามสารสนเทศและสงครามไซเบอร์ กำหนดแนวทางและ มาตรการในการป้องกัน และการรักษาความปลอดภัยปลอดภัยระบบสารสนเทศ มีโครงสร้างประกอบด้วย แผนกสงครามไซเบอร์แผนกกรรมวิธีข้อมูลสงครามไซเบอร์ แผนกรักษาความปลอดภัยระบบสารสนเทศ แผนกปฏิบัติการสงครามไซเบอร์ และแผนกประเมินผลการสงครามไซเบอร์

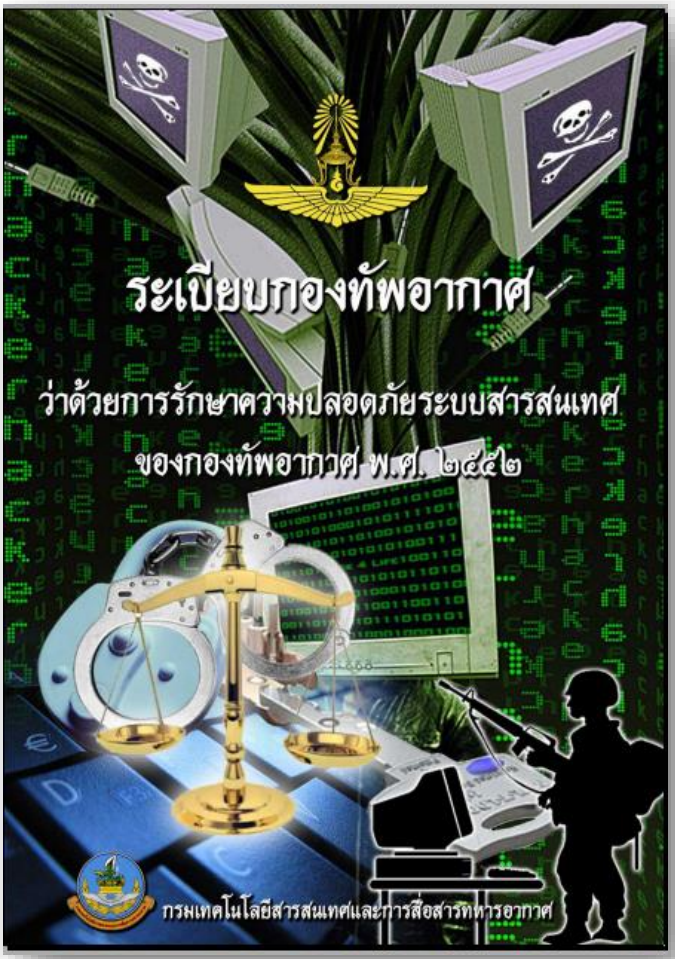
กรมสื่อสารอิเล็กทรอนิกส์ทหารอากาศ (สอ.ทอ.) มีหน้าที่วางแผนการปฏิบัติ อำนวยการ ประสานงาน ติดตาม กำกับการ พัฒนา และ ดำเนินการเกี่ยวกับกิจการสื่อสารอิเล็กทรอนิกส์ กิจการกระจายเสียงและกิจการโทรทัศน์ มาตรวิทยา และการพัสดุสื่อสารอิเล็กทรอนิกส์ กับมีหน้าที่จัดการความรู้ ควบคุม ประเมินผล และตรวจตรา กิจการ ในสายวิทยาการด้านสื่อสารอิเล็กทรอนิกส์ มีหน้าที่ที่สำคัญ คือ ดำเนินกิจการสื่อสารอิเล็กทรอนิกส์ให้พร้อมในขอบเขตเกี่ยวกับการเตรียมกำลังตามยุทธศาสตร์กองทัพอากาศ แผนการใช้กำลังทางอากาศ การจัดทำแผนงาน โครงการ งบประมาณ ด้านสื่อสารอิเล็กทรอนิกส์ การกำหนดมาตรฐานข้อมูลคุณลักษณะเฉพาะ กรรมวิธีการปฏิบัติของพัสดุอุปกรณ์สายสื่อสารอิเล็กทรอนิกส์ การปฏิบัติการสื่อสารอิเล็กทรอนิกส์ เครือข่ายสื่อสารและสารสนเทศ โทรคมนาคม และสนับสนุนการปฏิบัติการสงครามอิเล็กทรอนิกส์และสารสนเทศ การส่งกำลังและการพัสดุสื่อสารอิเล็กทรอนิกส์ คอมพิวเตอร์ และการภาพ การ

พัฒนากิจการสื่อสารอิเล็กทรอนิกส์ รวมทั้งประสานการซ่อมบำรุงและให้คำแนะนำทางเทคนิค ภายใต้โครงสร้างหน่วยของ สอ.ทอ.มีหน่วยรับผิดชอบที่เกี่ยวข้อง คือ ศูนย์คอมพิวเตอร์มีหน้าที่ดำเนินการและปฏิบัติการเกี่ยวกับกิจการเทคโนโลยีสารสนเทศ การกรรมวิธีข้อมูล การสื่อสารข้อมูล การสงครามสารสนเทศ และการซ่อม สร้าง ผลิต ประกอบติดตั้ง ดัดแปลงบริภัณฑ์คอมพิวเตอร์ บริภัณฑ์เครือข่ายสื่อสารข้อมูลของกองทัพอากาศ ตลอดจนการควบคุมสถานภาพเครือข่ายสื่อสารข้อมูลและระบบสารสนเทศ ซึ่งศูนย์คอมพิวเตอร์นี้มีงานหลักด้านไซเบอร์ คือ การควบคุม กำกับดูแลการบริการ ระบบอุปกรณ์คอมพิวเตอร์และเครือข่ายสื่อสารข้อมูลของกองทัพอากาศ โดยจะต้องเฝ้าตรวจและเฝ้าระวังตรวจจับสิ่งแปลกปลอมเพื่อเฝ้าระวังโปรแกรมหวังร้ายที่จะเข้ามาในระบบของกองทัพอากาศและหาทางช่วยเหลือและแก้ไขเมื่อถูกโจมตีทางไซเบอร์จากผู้ไม่หวังดี

หน่วยขึ้นตรงของกองทัพอากาศ (นขต.ทอ.) มีนายเทคโนโลยีสารสนเทศเป็นผู้กำกับดูแลการใช้งานระบบสานสนเทศและการสื่อสาร รวมถึงหน่วยขึ้นตรงของกองทัพอากาศ ที่จะต้องรับผิดชอบดูแลระบบเทคโนโลยีสารสนเทศและการสื่อสารที่มีใช้งานด้วย มิติไซเบอร์ (Cyber Domain) เทคโนโลยีสารสนเทศและการสื่อสารได้รับการพัฒนาอย่างรวดเร็ว รวมทั้ง การเกิดขึ้นของภัยคุกคามในมิติไซเบอร์ทั้งในรูปแบบการจารกรรมข้อมูลและการโจมตีเพื่อทำลายล้าง ล้วนก่อให้เกิดผลกระทบและความเสียหายในวงกว้างหลายประเทศมี การจัดตั้งหน่วยงานรับผิดชอบโดยตรง และกำหนดเป็นมิติหนึ่งในการปฏิบัติการ ด้านความมั่นคงของชาติโดยยุทธศาสตร์ไซเบอร์ เพื่อการป้องกันประเทศ และยุทธศาสตร์ ด้านสงครามไซเบอร์กองทัพไทย กำหนดให้เหล่าทัพต้องมีขีดความสามารถ ดังนี้ การป้องกันภัยคุกคามทางไซเบอร์ พัฒนาและใช้ประโยชน์จากขีดความสามารถทางไซเบอร์ในการปฏิบัติการทางทหาร ร่วมมือกับหน่วยงานภายในเพื่อการผนึกกำลังป้องกันประเทศ กองทัพอากาศจำเป็นต้องพัฒนาขีดความสามารถด้านไซเบอร์ให้มี ความพร้อมในการเผชิญกับภัยคุกคามด้านไซเบอร์ รวมทั้งการพัฒนาระบบเครือข่ายให้มี ความแข็งแกร่ง (Robustness) และปลอดภัย (Security) จะต้องจัดทำนโยบายด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ โดยมีวัตถุประสงค์เพื่อให้การรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศของกองทัพอากาศ เป็นไปอย่างเหมาะสม มีประสิทธิภาพ และมีความมั่นคงปลอดภัย

รวมทั้งสอดคล้องกับกฎหมาย และกฎระเบียบที่เกี่ยวข้องด้านเทคโนโลยีสารสนเทศและด้านการประกอบธุรกรรมทางอิเล็กทรอนิกส์ ด้วยการสร้างความมั่นคงปลอดภัยด้านบริหาร การสร้างความมั่นคงปลอดภัยด้านบุคลากร โดยมีการจัดทำระเบียบกองทัพอากาศ ว่าด้วยการรักษาความปลอดภัยระบบ สารสนเทศกองทัพอากาศ พ.ศ.๒๕๕๒ โดยอ้างอิงจากมาตรฐาน (ISO/IEC27001:2005) ซึ่งระเบียบนี้ ให้ใช้บังคับข้าราชการ

พนักงานราชการ ลูกจ้าง ที่มีการปฏิบัติเกี่ยวกับระบบสารสนเทศ รวมถึง บุคคลภายนอกที่เข้ามาดำเนินการเกี่ยวกับระบบสารสนเทศของกองทัพอากาศ มีความมุ่งหมายเพื่อ กำหนดหลักการและมาตรการการป้องกันระบบสารสนเทศ รวมถึงให้แต่งตั้งคณะกรรมการรักษาความ ปลอดภัยระบบสารสนเทศและนายทหารรักษาความปลอดภัยของหน่วยเพื่อดำเนินการอีกด้วย จึงเป็นที่มาของการจัดทำระเบียบ ทอ.ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศของกองทัพอากาศ พ.ศ.๒๕๕๒



รูปที่ ๑๒ ระเบียบ ทอ.ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศของกองทัพอากาศ พ.ศ.๒๕๕๒

๒ เหตุผลความจำเป็นของการปรับปรุงระเบียบ ทอ.ฯ (ฉบับ พ.ศ.๒๕๕๒)

ตามแผนการปฏิบัติงานของ กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ (ทสส.ทอ.) ปี ๒๕๖๓ กำหนดให้มีการจัดทำร่างระเบียบ ทอ. ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศของ ทอ. พ.ศ.๒๕๖๓ เพื่อปรับปรุงแก้ไขระเบียบ ทอ.ฯ (ฉบับ พ.ศ.๒๕๕๒) เนื่องด้วยการใช้เนื้อหา แนวทาง กระบวน การดำเนินการในด้านการรักษาความปลอดภัยระบบสารสนเทศนั้น อ้างอิงตามกรอบมาตรฐาน ISO/IEC 27001:2005 (Information Security Management System Implementation) ซึ่งเป็นเวอร์ชันที่ถูกยกเลิกการใช้งานไปแล้ว จึงมีแนวทางในการจัดทำร่างระเบียบ ทอ.ฯ ฉบับใหม่ โดยให้ใช้ มาตรฐาน ISO/IEC 27001(Information Security Management System: ISMS) คือ มาตรฐานสากลด้านการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ เพื่อให้สารสนเทศมีคุณสมบัติ CIA การรักษาความลับ (Confidentiality), การรักษาความถูกต้องครบถ้วน (Integrity), สภาพความพร้อมใช้ (Availability) และเน้นความสำคัญด้านระบบการบริหารจัดการ (Management System) โดยให้ใช้มาตรฐาน (ISO/IEC 27001:2013, 2560) ซึ่งเป็นเวอร์ชันปัจจุบัน และถูก

นำมาใช้งานกันอย่างแพร่หลายในหลายประเทศ โดยมีข้อกำหนดต่าง ๆ ที่หน่วยงานพึงปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ ให้พ้นจากภัยคุกคาม และความเสี่ยงในหลากหลายรูปแบบ รวมถึงเป็นกรอบเนื้อหาในการกำหนดให้มีการจัดทำเอกสาร แนวทาง กระบวน การดำเนินการ แผนรับมือเหตุฉุกเฉินที่อาจเกิดขึ้น ลดความสูญเสีย และคงไว้ซึ่งความสามารถในการดำเนินงานในด้านการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศในด้านต่าง ๆ ได้อย่างต่อเนื่อง

รูปที่ ๑๓ มาตรฐาน ISO/IEC27001:2013

โดยการปรับแก้ร่างระเบียบ ทอ.ฯ ให้มีความทันสมัยสอดคล้องกับมาตรการและกฎหมายต่าง ๆ ที่เกี่ยวข้อง เช่น บทบาทหน้าที่ของหน่วยเกี่ยวข้อง ความเหมาะสมในการกำหนดให้มีคณะกรรมการต่าง ๆ ในร่างระเบียบ ทอ.ฯ เป็นต้น เพื่อให้การดำเนินการรักษาความปลอดภัยตามร่างระเบียบนี้ รองรับการบังคับใช้กฎหมายที่เกี่ยวข้อง ได้แก่ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร พ.ศ.๒๕๖๒, พระราชบัญญัติคุ้มครองข้อมูลสวนบุคคล พ.ศ.๒๕๖๒, ระเบียบสำนักนายกรัฐมนตรีวาด้วยการรักษาความปลอดภัยแหงชาติ พ.ศ.๒๕๕๒, และฉบับแกไข เพิ่มเติม ระเบียบวาด้วยการรักษาความลับของทางราชการ พ.ศ.๒๕๔๔, และฉบับแกไขเพิ่มเติม และระเบียบ กองทัพอากาศวาด้วยการรักษาการณพ.ศ.๒๕๖๐ รวมทั้งให้สอดประสานการปฏิบัติด้านไซเบอร์กับ ศซบ.ทอ.ซึ่งเป็นหน่วยที่ได้รับอมุมัติให้จัดตั้ง เมื่อ ๑ ต.ค.๖๒ และเพื่อสอดคล้องกับอนุมัติ ผบ.ทอ.ในเรื่องของแนวทาง มาตรการ ระเบียบ ข้อบังคับต่าง ๆ ที่เกี่ยวข้องกับการรักษาความปลอดภัยระบบสารสนเทศของ ทอ.จึงเป็นเหตุผลความจำเป็นของการปรับปรุงระเบียบ ทอ.ฯ (ฉบับ พ.ศ.๒๕๕๒)

และเมื่อดำเนินการปรับปรุงระเบียบ ทอ.ฯ เสร็จสิ้นกระบวนการเรียบร้อยแล้ว ได้มีการขออนุมัติใช้ระเบียบ ทอ.ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๖๓ เมื่อ ๓๑ สิงหาคม ๒๕๖๓

http://dict.km.rtaf.mi.th/Home/Page/19?menuID=4736&contentID=30257

รูปที่ ๑๔ ระเบียบ ทอ.ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๖๓

๓. หน่วยงานที่เกี่ยวข้องของ ทอ. ในการกำหนดโครงสร้างการบริหารจัดการความมั่นคงปลอดภัย บทบาทและหน้าที่ความรับผิดชอบด้านการรักษาความมั่นคงปลอดภัย

๓.๑ กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ (ทสส.ทอ.)

เป็นหน่วยงานฝ่ายเสนาธิการ มีหน้าที่พิจารณา เสนอนโยบาย วางแผน อำนวยการ ประสานงาน ควบคุม กำกับการ พัฒนาและดำเนินการด้านระบบบัญชาการและควบคุม ข่าย เครือข่ายเทคโนโลยีสารสนเทศและการสงครามสารสนเทศ การสื่อสารอิเล็กทรอนิกส์และการสงครามอิเล็กทรอนิกส์ กับมีหน้าที่จัดการความรู้ ควบคุม ประเมินผล และตรวจตรากิจการด้านสารสนเทศและสงครามอิเล็กทรอนิกส์ มีเจ้ากรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศเป็นผู้บังคับบัญชารับผิดชอบ มีหน่วยรับผิดชอบที่เกี่ยวข้อง คือ กองสงครามไซเบอร์ สำนักระบบบัญชาการและควบคุม กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ (กคช.สบค.ทสส.ทอ.) มีหน้าที่พิจารณา เสนอนโยบาย วางแผน อำนวยการ ประสานงาน ควบคุม กำกับการ พัฒนา และดำเนินการด้านสงครามสารสนเทศและสงครามไซเบอร์ กำหนดแนวทางและ มาตรการในการป้องกัน และการรักษาความปลอดภัยปลอดภัยระบบสารสนเทศ มีผู้อำนวยการกองสงครามไซเบอร์เป็นผู้บังคับบัญชารับผิดชอบ ซึ่งในระเบียบ ทอ.ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๖๓ มีการกำหนดโครงสร้างการบริหารจัดการความมั่นคงปลอดภัย บทบาทและหน้าที่ความรับผิดชอบด้านการรักษาความมั่นคงปลอดภัย เพื่อให้การดำเนินงานในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของ

กองทัพอากาศเป็นไปอย่างมีประสิทธิภาพ จึงแบ่งมอบบทบาทและหน้าที่ความรับผิดชอบไว้ ดังนี้ กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ มีหน้าที่รับผิดชอบ กำหนดมาตรการ แนวทางปฏิบัติ ประเมิน ตรวจสอบการรักษาความมั่นคงปลอดภัยระบบสารสนเทศและไซเบอร์ของกองทัพอากาศ ให้เป็นไปตามความมุ่งหมายของระเบียบนี้ และเป็นหน่วยงานในการประสานการดำเนินการด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศและไซเบอร์ กับหน่วยงานภายนอกที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยระบบสารสนเทศและไซเบอร์ รวมทั้งให้มีหน้าที่ดังต่อไปนี้

๓.๑.๑ ประเมินความมั่นคงปลอดภัยของระบบสารสนเทศและการดำเนินการกับสารสนเทศเพื่อระบุภัยที่จะเกิดกับระบบสารสนเทศของกองทัพอากาศ

๓.๑.๒ พัฒนาหลักการ และกระบวนการด้านการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ และส่งเสริมความร่วมมือกับหน่วยงานภายนอกที่เกี่ยวข้อง

๓.๑.๓ สนับสนุนและส่งเสริมให้มีการศึกษาหลักสูตรการรักษาความมั่นคงปลอดภัยระบบสารสนเทศและไซเบอร์ อย่างต่อเนื่อง

๓.๑.๔ ให้มีการฝึกอบรม สัมมนาและดูงาน เกี่ยวกับงานด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศและไซเบอร์

๓.๑.๕ ตรวจสอบให้มีการปฏิบัติตามระเบียบนี้

๓.๑.๖ แจ้งผลการตรวจสอบความมั่นคงปลอดภัยระบบสารสนเทศ (Information System Security Audit) รวมทั้งพิจารณาให้คำแนะนำ ติดตามและประเมินผลตามนโยบาย และระเบียบนี้

๓.๒ ศูนย์ไซเบอร์กองทัพอากาศ (ทสส.ทอ.)

มีหน้าที่ วางแผน เตรียมการ ประสานงาน ควบคุม กำกับการ พัฒนา และดำเนินการด้านไซเบอร์ของกองทัพอากาศ มีผู้อำนวยการศูนย์ไซเบอร์กองทัพอากาศ เป็นผู้บังคับบัญชารับผิดชอบ

ศูนย์ไซเบอร์กองทัพอากาศขึ้น โดยจัดตั้งเป็น ศูนย์ไซเบอร์กองทัพอากาศ (เพื่อพลาง) เพื่อทดลองปฏิบัติงานตั้งแต่ ๑ ม.ค.๖๒ และได้รับการอนุมัติจัดตั้งเป็นหน่วยขึ้นตรงกองทัพอากาศ ในส่วนบัญชาการ
เมื่อ ๑ ต.ค.๖๒ ศูนย์ไซเบอร์กองทัพอากาศ มีหน้าที่ วางแผน เตรียมการ ประสานงาน ควบคุม กำกับการ พัฒนาและดำเนินการด้านไซเบอร์ของกองทัพอากาศ โดยมีขอบเขตความรับผิดชอบเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์, การปฏิบัติการไซเบอร์ และการฝึกและพัฒนาทางไซเบอร์เพื่อเป็นการตอบโจทย์ของการพัฒนาขีดความสามารถในมิติไซเบอร์ หรือ Cyber Domain ให้มีศักยภาพและความเข้มแข็งสามารถสนับสนุนการปฏิบัติการในมิติทางอากาศ หรือ Air Domain ทั้งนี้ ยังเป็นการเตรียมความพร้อมในการป้องกันภัยคุกคามทั้งในปัจจุบันและในอนาคต ซึ่งหากศูนย์ไซเบอร์กองทัพอากาศสามารถพัฒนาขีดความสามารถด้านไซเบอร์ได้อย่างมีประสิทธิภาพ จะมั่นได้ได้ว่ากองทัพอากาศจะสามารถบรรลุวิสัยทัศน์ที่กำหนดในการเป็น "กองทัพอากาศชั้นนำในภูมิภาค One of the Best Air Forces in ASEAN" โดยเป็นที่ยอมรับจากนานาประเทศอย่างแท้จริง ซึ่งในระเบียบ ทอ.ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๖๓ มีการกำหนดโครงสร้างการบริหารจัดการความมั่นคงปลอดภัย บทบาทและหน้าที่ความรับผิดชอบด้านการรักษาความมั่นคงปลอดภัย เพื่อให้การ

ดำเนินงานในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของกองทัพอากาศเป็นไปอย่างมีประสิทธิภาพ จึงแบ่งมอบบทบาทและหน้าที่ความรับผิดชอบไว้ ดังนี้ ศูนย์ไซเบอร์กองทัพอากาศ มีหน้าที่รับผิดชอบ ปฏิบัติการตามกระบวนการป้องกัน ป้องปราม และตอบสนองต่อภัยคุกคามทางไซเบอร์ รวมถึงการปฏิบัติอื่น ๆ ที่กำหนดไว้ในระเบียบนี้

ประวัติความเป็นมา ศูนย์ไซเบอร์กองทัพอากาศ

ตามยุทธศาสตร์กองทัพอากาศ ๒๐ ปี ได้ให้ความสำคัญกับการพัฒนากองทัพอากาศในทุกด้านอย่างเป็นระบบโดยยกระดับให้การปฏิบัติการครอบคลุมทุกมิติ รวมถึง**มิติไซเบอร์**ในการสนับสนุนการปฏิบัติการทางอากาศ เพื่อมุ่งสู่การเป็นกองทัพอากาศที่ใช้เครือข่ายเป็นศูนย์กลาง ซึ่งต้องใช้ระบบสารสนเทศเป็นปัจจัยหลักในการบัญชาการและควบคุม จึงมีความจำเป็นอย่างยิ่งในการที่จะต้องป้องกันภัยคุกคามทางไซเบอร์ ทั้งในรูปแบบของการโจมตีที่อาจจะส่งผลให้เกิดความเสียหายต่อระบบ รวมถึงการรั่วไหลของข้อมูลชั้นความลับ เพื่อดำรงไว้ซึ่งเสถียรภาพในการบัญชาการรบ รวมทั้งความมั่นคงของประเทศ

กองทัพอากาศจึงได้จัดตั้งศูนย์ไซเบอร์กองทัพอากาศขึ้น **โดยจัดตั้งเป็น ศูนย์ไซเบอร์กองทัพอากาศ (เพื่อพลาง) เพื่อทดลองปฏิบัติงานตั้งแต่ ๑ ม.ค.๖๒ และได้รับการอนุมัติจัดตั้งเป็นหน่วยขึ้นตรงกองทัพอากาศในส่วนบัญชาการ เมื่อ ๑ ต.ค.๖๒** ศูนย์ไซเบอร์กองทัพอากาศ มีหน้าที่ วางแผน เตรียมการ ประสานงาน ควบคุม กำกับการ พัฒนา และดำเนินการด้านไซเบอร์ของกองทัพอากาศ โดยมีขอบเขตความรับผิดชอบเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ , การปฏิบัติการไซเบอร์ และ การฝึกและพัฒนาทางไซเบอร์เพื่อเป็นการตอบโจทย์ของการพัฒนาขีดความสามารถในมิติไซเบอร์ หรือ Cyber Domain ให้มีศักยภาพและความเข้มแข็ง สามารถสนับสนุนการปฏิบัติการในมิติทางอากาศ หรือ Air Domain ทั้งนี้ ยังเป็นการเตรียมความพร้อมในการป้องกันภัยคุกคามทั้งในปัจจุบันและในอนาคต ซึ่งหากศูนย์ไซเบอร์กองทัพอากาศสามารถพัฒนาขีดความสามารถด้านไซเบอร์ได้อย่างมีประสิทธิภาพ จะมั่นใจได้ว่ากองทัพอากาศจะสามารถบรรลุวิสัยทัศน์ที่กำหนดในการเป็น**"กองทัพอากาศชั้นนำในภูมิภาค** One of the Best Air Forces in ASEAN" โดยเป็นที่ยอมรับจากนานาประเทศอย่างแท้จริง

รูปที่ ๑๕ ประวัติความเป็นมา ศูนย์ไซเบอร์กองทัพอากาศ

๓.๓ กรมสื่อสารอิเล็กทรอนิกส์ทหารอากาศ (สอ.ทอ.)

มีหน้าที่ วางแผนการปฏิบัติ อำนวยการ ประสานงาน ติดตาม กำกับการ พัฒนา และดำเนินการเกี่ยวกับกิจการสื่อสารอิเล็กทรอนิกส์ กิจการกระจายเสียงและกิจการโทรทัศน์ มาตรวิทยา และการพัสดุสื่อสารอิเล็กทรอนิกส์ กับมีหน้าที่จัดการความรู้ ควบคุมประเมินผล และตรวจตรากิจการในสายวิทยาการสื่อสารอิเล็กทรอนิกส์ มีเจ้ากรมสื่อสารอิเล็กทรอนิกส์ทหารอากาศ เป็นผู้บังคับบัญชารับผิดชอบ มีหน่วยรับผิดชอบที่เกี่ยวข้อง คือ ศูนย์คอมพิวเตอร์ มีหน้าที่ ดำเนินการและปฏิบัติการเกี่ยวกับกิจการเทคโนโลยีสารสนเทศ การกรรมวิธีข้อมูล การสื่อสารข้อมูล การสงครามสารสนเทศ และการซ่อม สร้าง ผลิต ประกอบ ติดตั้ง ดัดแปลง บริภัณฑ์คอมพิวเตอร์ บริภัณฑ์เครือข่ายสื่อสารข้อมูลของกองทัพอากาศ ตลอดจนการควบคุมสถานภาพเครือข่ายสื่อสารข้อมูลและระบบสารสนเทศมีผู้อำนวยการศูนย์คอมพิวเตอร์ เป็นผู้บังคับบัญชารับผิดชอบ ซึ่ง

ในระเบียบ ทอ.ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๖๓ มีการกำหนดโครงสร้างการบริหารจัดการความมั่นคงปลอดภัย บทบาทและหน้าที่ความรับผิดชอบด้านการรักษาความมั่นคงปลอดภัย เพื่อให้การดำเนินงานในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของกองทัพอากาศเป็นไปอย่างมีประสิทธิภาพ จึงแบ่งมอบบทบาทและหน้าที่ความรับผิดชอบไว้ ดังนี้ กรมสื่อสารอิเล็กทรอนิกส์ทหารอากาศ มีหน้าที่รับผิดชอบ ดำรงรักษาสถานภาพการใช้งานระบบสารสนเทศและการสื่อสาร และสนับสนุนระบบรวมถึงอุปกรณ์ที่เกี่ยวข้องกับการปฏิบัติการด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศและไซเบอร์ของกองทัพอากาศ ให้เป็นไปตามความมุ่งหมายของระเบียบนี้

๓.๔ หน่วยขึ้นตรงกองทัพอากาศ (นขต.ทอ.)

มีนายเทคโนโลยีสารสนเทศเป็นผู้กำกับดูแลการใช้งานระบบสารสนเทศและการสื่อสาร ภายในหน่วยงาน ซึ่งในระเบียบ ทอ.ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๖๓ มีการกำหนดโครงสร้างการบริหารจัดการความมั่นคงปลอดภัย บทบาทและหน้าที่ความรับผิดชอบด้านการรักษาความมั่นคงปลอดภัย เพื่อให้การดำเนินงานในการรักษาความมั่นคงปลอดภัยระบบสารสนเทศของกองทัพอากาศเป็นไปอย่างมีประสิทธิภาพ จึงแบ่งมอบบทบาทและหน้าที่ความรับผิดชอบไว้ ดังนี้ ให้หน่วยขึ้นตรงกองทัพอากาศดำเนินการจัดโครงสร้างบริหารจัดการความมั่นคงปลอดภัยระบบสารสนเทศภายในหน่วยงาน ดังนี้

๓.๔.๑ แต่งตั้งนายทหารรักษาความมั่นคงปลอดภัยระบบสารสนเทศ

๓.๔.๒ แต่งตั้งคณะกรรมการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ ประกอบด้วย

๓.๔.๒.๑ หัวหน้า หรือรองหัวหน้าหน่วยขึ้นตรงกองทัพอากาศเป็นประธาน

๓.๔.๒.๒ หัวหน้าส่วนราชการของหน่วย เป็นกรรมการ

๓.๔.๒.๓ นายทหารรักษาความมั่นคงปลอดภัยระบบสารสนเทศเป็นกรรมการและเลขานุการ

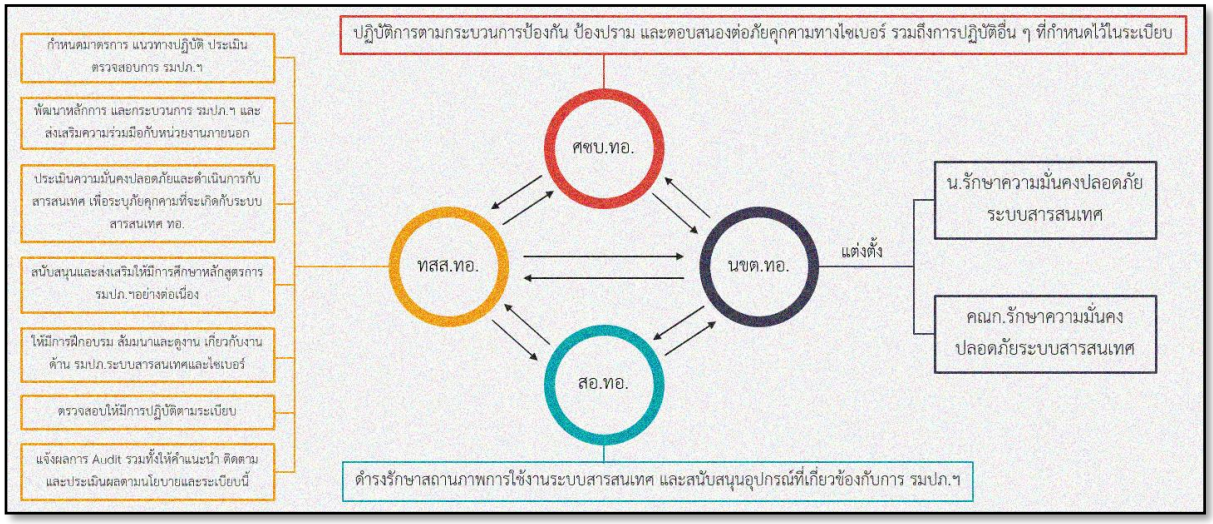
๓.๔.๒.๔ ผู้ดูแลระบบ ได้แก่ ผู้ดูแลเครือข่ายสารสนเทศ ผู้ดูแลระบบสารสนเทศของหน่วย (กรณีหน่วยขึ้นตรงมีระบบสารสนเทศภายในหน่วย) และผู้ดูแลระบบสารสนเทศของระบบงานของกองทัพอากาศ (กรณีหน่วยขึ้นตรงรับผิดชอบระบบงานของกองทัพอากาศ) เป็นกรรมการ

๓.๔.๒.๕ ผู้เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ และบุคคลตามผนวก ก ตามความเหมาะสม เป็นกรรมการ

๓.๔.๑ ประเมินความมั่นคงปลอดภัยของระบบสารสนเทศและการดำเนินการกับสารสนเทศเพื่อระบุภัยที่จะเกิดกับระบบสารสนเทศของกองทัพอากาศ

๓.๔.๑ ประเมินความมั่นคงปลอดภัยของระบบสารสนเทศและการดำเนินการกับสารสนเทศเพื่อระบุภัยที่จะเกิดกับระบบสารสนเทศของกองทัพอากาศ

๓.๔.๑ ประเมินความมั่นคงปลอดภัยของระบบสารสนเทศและการดำเนินการกับสารสนเทศเพื่อระบุภัยที่จะเกิดกับระบบสารสนเทศของกองทัพอากาศ



รูปที่ ๑๖ หน่วยงานที่เกี่ยวข้องของ ทอ. ในการกำหนดโครงสร้างการบริหารจัดการความมั่นคงปลอดภัย

บทบาทและหน้าที่ความรับผิดชอบด้านการรักษาความมั่นคงปลอดภัย

๔. โครงสร้างระเบียบ ทอ.ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๖๓

หมวด ๑ กล่าวทั่วไป

ส่วนที่ ๑ ความมุ่งหมาย

ระเบียบนี้มีความมุ่งหมายเพื่อ กำหนดหลักการ และมาตรการป้องกันระบบสารสนเทศของกองทัพอากาศ เพื่อรักษาไว้ซึ่งคุณสมบัติที่มั่นคงปลอดภัยของระบบสารสนเทศ ได้แก่ การรักษาความลับ (Confidentiality) ความครบถ้วนสมบูรณ์ (Integrity) และความพร้อมใช้งาน (Availability) ของสารสนเทศ

รูปที่ ๑๗ หลักการการรักษาความปลอดภัยของข้อมูล (Principles of Information Security)

ส่วนที่ ๒ แนวทางการบริหารจัดการความมั่นคงปลอดภัย

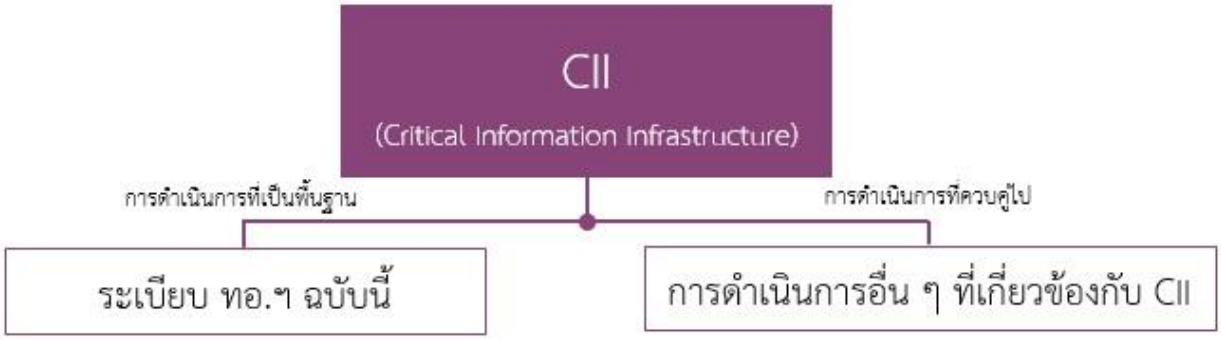
การกำหนดมาตรการ หรือระบบบริหารจัดการความมั่นคงปลอดภัยระบบสารสนเทศนั้น ระบบสารสนเทศและการดำเนินการกับสารสนเทศที่เกี่ยวข้องต้องผ่านการประเมินความเสี่ยง (Risk Assessment) ช่องโหว่ (Vulnerability) ภัยคุกคาม (Threat) เพื่อให้ได้มาตรการป้องกันที่เหมาะสมกับระบบสารสนเทศ โดยการจัดทำแผนบริหารจัดการความเสี่ยง (Risk Management Plan) รองรับเพื่อมุ่งเน้นให้มีแผนปฏิบัติการที่สามารถแปลงเป็นมาตรการป้องกันที่มีความเข้มแข็ง (Robustness) ต่อภัยคุกคามทางไซเบอร์ได้อย่างแท้จริง และกำหนดให้มีการปรับปรุงให้ทันสมัยอยู่เสมอ

รูปที่ ๑๘ ระบบบริหารจัดการความมั่นคงปลอดภัยระบบสารสนเทศ

โดยมีหัวข้อสำคัญอ้างตามระเบียบทอ.ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๖๓ หลัก ๆ ๒ ข้อ ดังนี้

หมวด ๑ ส่วนที่ ๒ ข้อ ๑๑ ต้องดำเนินการตรวจสอบ ทบทวน และประเมินแนวทางบริหารความมั่นคงปลอดภัยตามระยะเวลาที่กำหนดไว้ หรืออย่างน้อย ๑ ครั้งต่อปี หรือเมื่อมีการเปลี่ยนแปลงสำคัญที่มีผลกระทบต่อระบบสารสนเทศ

หมวด ๑ ส่วนที่ ๒ ข้อ ๑๒ การรักษาความมั่นคงปลอดภัยโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องดำเนินการตามระเบียบนี้เป็นพื้นฐาน ควบคู่กับการดำเนินการด้านความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศของกองทัพอากาศ เพื่อรักษาความมั่นคงปลอดภัยของโครงสร้างพื้นฐานให้สามารถสนับสนุนการปฏิบัติภารกิจของกองทัพอากาศได้อย่างต่อเนื่อง



รูปที่ ๑๙ การรักษาความมั่นคงปลอดภัยโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

หมวด ๒ โครงสร้างการบริหารความมั่นคงปลอดภัยสารสนเทศและไซเบอร์

ส่วนที่ ๑ บทบาทและหน้าที่ความรับผิดชอบด้านการรักษาความมั่นคงปลอดภัย

โดยกองทัพอากาศได้มีการวางโครงสร้างการบริหารจัดการความมั่นคงปลอดภัยไว้ดังต่อไปนี้

ทสส.ทอ. มีหน้าที่

กำหนดมาตรการ แนวทางปฏิบัติ ประเมิน ตรวจสอบการรักษาความมั่นคงปลอดภัยระบบสารสนเทศและไซเบอร์ของกองทัพอากาศ ให้เป็นไปตามความมุ่งหมายของระเบียบนี้ และเป็นหน่วยงานในการประสานการดำเนินการด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศและไซเบอร์ กับหน่วยงานภายนอกที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยระบบสารสนเทศและไซเบอร์

ประเมินความมั่นคงปลอดภัยของระบบสารสนเทศและการดำเนินการกับสารสนเทศเพื่อระบุภัยที่จะเกิดกับระบบสารสนเทศของกองทัพอากาศ

พัฒนาหลักการ และกระบวนการด้านการรักษาความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ และส่งเสริมความร่วมมือกับหน่วยงานภายนอกที่เกี่ยวข้อง

สนับสนุนและส่งเสริมให้มีการศึกษาหลักสูตรการรักษาความมั่นคงปลอดภัยระบบสารสนเทศและไซเบอร์ อย่างต่อเนื่อง

ให้มีการฝึกอบรม สัมมนาและดูงาน เกี่ยวกับงานด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศและไซเบอร์

แจ้งผลการตรวจสอบความมั่นคงปลอดภัยระบบสารสนเทศ (Information System Security Audit) รวมทั้งพิจารณาให้คำแนะนำ ติดตามและประเมินผลตามนโยบาย และระเบียบนี้

ศซบ.ทอ. มีหน้าที่

ปฏิบัติการตามกระบวนการป้องกัน ป้องปราม และตอบสนองต่อภัยคุกคามทางไซเบอร์ รวมถึงการปฏิบัติอื่น ๆ ที่กำหนดไว้ในระเบียบนี้

สอ.ทอ. มีหน้าที่

ดำรงรักษาสถานภาพการใช้งานระบบสารสนเทศและการสื่อสาร และสนับสนุนระบบรวมถึงอุปกรณ์ที่เกี่ยวข้องกับการปฏิบัติการด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศและไซเบอร์ของกองทัพอากาศ ให้เป็นไปตามความมุ่งหมายของระเบียบนี้

นขต.ทอ. มีหน้าที่

แต่งตั้งนายทหารรักษาความมั่นคงปลอดภัยระบบสารสนเทศ โดยมีหน้าที่ดำเนินการให้เป็นไปตามระเบียบนี้และมาตรการที่กำหนด

แต่งตั้งคณะกรรมการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ โดยมีหน้าที่จัดทำแผนบริหารจัดการความเสี่ยงการดำเนินการเกี่ยวกับสารสนเทศและระบบสารสนเทศของหน่วย และของระบบงานของกองทัพอากาศ และจัดทำแผนที่เกี่ยวข้องดังต่อไปนี้

แผนการสำรองข้อมูลและสารสนเทศ

แผนฟื้นฟูระบบสารสนเทศ

แผนป้องกันภัยธรรมชาติ

แผนป้องกันอัคคีภัย

แผนเผชิญเหตุ (Contingency Plan)

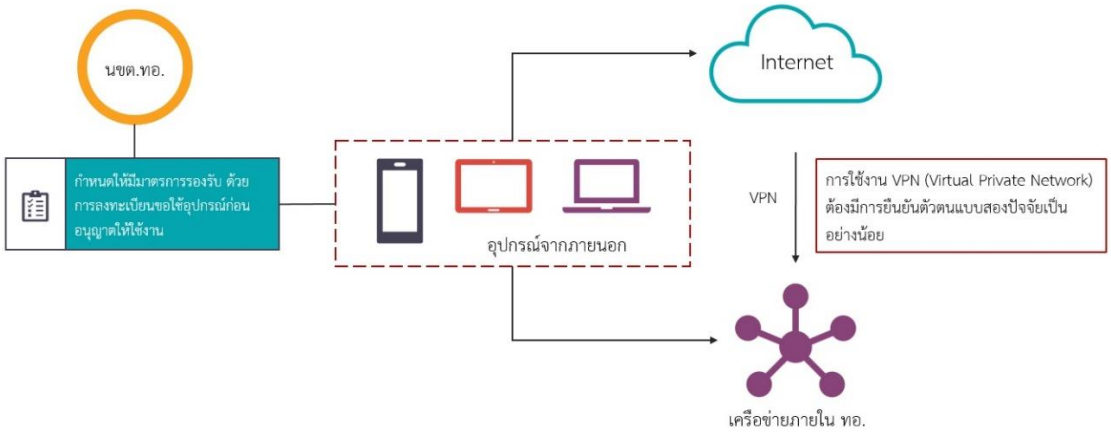
แผนป้องกันภัยที่หน่วยงานนั้นพิจารณาว่าควรจัดทำตามสภาพแวดล้อม

ส่วนที่ ๒ อุปกรณ์พกพาและการปฏิบัติงานจากระยะไกล

เพื่อรักษาความมั่นคงปลอดภัยระบบสารสนเทศในการปฏิบัติงานจากภายนอกกองทัพอากาศและการใช้งานของอุปกรณ์คอมพิวเตอร์แบบพกพา จึงมีข้อกำหนดไว้ในส่วนนี้ โดยอ้างตามระเบียบทอ.ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๖๓ หลัก ๆ ๒ ข้อ ดังนี้

หมวด ๒ ส่วนที่ ๒ ข้อ ๑๕ กำหนดให้มีมาตรการรองรับด้วยการลงทะเบียนขอใช้อุปกรณ์ก่อนอนุญาตให้ใช้งาน

หมวด ๒ ส่วนที่ ๒ ข้อ ๑๖ การใช้งาน VPN (Virtual Private Network) ต้องมีการยืนยันตัวตนแบบสองปัจจัย (Two Factor Authentication) เป็นอย่างน้อย



รูปที่ ๒๐ การรักษาความมั่นคงปลอดภัยอุปกรณ์พกพาและการปฏิบัติงานจากระยะไกล

หมวด ๓ การรักษาความมั่นคงปลอดภัยด้านบุคคล

แบ่งออกเป็น ๓ ส่วน ดังนี้

ส่วนที่ ๑ ก่อนการบรรจุเข้าปฏิบัติงาน

นขต.ทอ.จะต้องตรวจสอบความไว้วางใจบุคคลโดยละเอียดผาน ขว.ทอ.

ส่วนที่ ๒ ระหว่างดำรงสถานภาพการปฏิบัติงาน

น.รมปภ.ฯ ต้องผ่านการอบรมความรู้เกี่ยวกับการรักษาความมั่นคงปลอดภัยระบบสารสนเทศและไซเบอร์

น.รมปภ.ฯ ชี้แจงโทษและทัณฑ์ทางวินัย ให้บุคคลที่ได้รับมอบหมายให้ปฏิบัติหน้าที่เกี่ยวกับสารสนเทศทราบ

ให้มีการกำหนดมาตรการ ควบคุม ดูแล และตรวจสอบสิทธิ์การเข้าถึงระบบสารสนเทศ

หากบุคคลมีพฤติการณ์ไม่น่าไว้วางใจหรืออาจเป็นภัยต่อระบบสารสนเทศ ให้ผู้ดูแลรับผิดชอบที่เกี่ยวข้อง รายงาน น.รมปภ.ฯ ทันที

ส่วนที่ ๓ การสิ้นสุดสถานภาพและการเปลี่ยนหน้าที่ปฏิบัติงาน

ให้ตัดชื่อออกจากทะเบียนความไว้วางใจของบุคคลที่ปฏิบัติหน้าที่เกี่ยวกับระบบสารสนเทศ

หมวด ๔ การบริหารจัดการทรัพย์สิน

ส่วนที่ ๑ ความรับผิดชอบต่อทรัพย์สิน

จัดทำบัญชีหรือทะเบียนเฉพาะทรัพย์สินประเภทอุปกรณ์คอมพิวเตอร์ รวมถึงอุปกรณ์อื่นที่เกี่ยวข้องกับการประมวลผลสารสนเทศของหน่วยหรือของระบบงาน มีป้ายชื่อ ระบุผู้ถือครอง และมีหลักฐานการรับไปถือครอง

การเคลื่อนย้ายเข้า-ออก พื้นที่ของหน่วยงาน หรือการเคลื่อนย้ายที่มีผลทำให้สภาวะแวดล้อมการใช้งานทรัพย์สินเปลี่ยนแปลงไปจะต้องแจ้งและขออนุญาตต่อนายทหารรักษาความมั่นคงปลอดภัยระบบสารสนเทศก่อนการเคลื่อนย้ายทุกครั้ง

ส่วนที่ ๒ การจัดชั้นความลับของสารสนเทศ

กำหนดชั้นความลับให้เป็นไปตามกฎหมายที่เกี่ยวข้อง และมีการจัดทำป้ายชื่อของข้อมูล

ส่วนที่ ๓ การจัดการสื่อบันทึกข้อมูล

สามารถใช้สื่อบันทึกข้อมูลแบบถอดย้ายได้ในระบบสารสนเทศที่มีชั้นความลับได้โดยต้องแสดงชั้นความลับไว้บนสื่อบันทึกข้อมูลนั้น และให้เก็บในกล่อง หรือหีบห่อ ซึ่งมีเครื่องหมายแสดงชั้นความลับนั้น ๆ

ไม่สามารถใช้สื่อบันทึกข้อมูลแบบถอดย้ายได้ในพื้นที่ใช้งานระบบสารสนเทศที่มีชั้นความลับ และที่เกี่ยวข้องกับงานด้านยุทธการ

ต้องมีการกำจัดหรือทำลายทิ้งโดยปฏิบัติตามกระบวนการทำลายข้อมูลของทางราชการ เมื่อหมดความต้องการในการใช้งานสื่อบันทึกข้อมูลที่มีชั้นความลับ

หมวด ๕ การควบคุมการเข้าถึง

ส่วนที่ ๑ หลักการควบคุมการเข้าถึง

อ้างตามระเบียบทอ.ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๖๓ หมวด ๕ ส่วนที่ ๑ ข้อ ๔๒ มีใจความสำคัญ ดังนี้

กำหนดนโยบายควบคุมการเข้าถึง การใช้งานระบบสารสนเทศ มีการทำบันทึกติดตาม และเฝ้าระวัง

การเข้าถึงเครือข่ายและบริการเครือข่าย ผู้ใช้งานต้องได้รับสิทธิ์การเข้าถึงเฉพาะเครือข่ายและบริการของเครือข่ายตามที่ตนได้รับอนุมัติการเข้าถึงเท่านั้น

ส่วนที่ ๒ การจัดการเข้าถึงระบบของผู้ใช้งาน

อ้างตามระเบียบทอ.ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๖๓ หมวด ๕ ส่วนที่ ๒ ข้อ ๔๓ ๔๔ และ ๔๕ มีใจความสำคัญ ดังนี้

การลงทะเบียนผู้ใช้ใหม่ ต้องกำหนดให้มีระเบียบปฏิบัติเป็นทางการ รวมทั้งระเบียบปฏิบัติสำหรับการยกเลิกสิทธิ์

กำหนดสิทธิ์ในการเข้าถึงระบบสารสนเทศ และมีการยืนยันตัวตนทุกครั้ง

กำหนดให้มีปฏิเสธการให้บริการเมื่อใส่รหัสผ่านผิดเกิน ๓ ครั้ง และควบคุมดูแลให้ผู้ใช้งานเปลี่ยนรหัสผ่านทุก ๆ ๑๘๐ วัน หรือเมื่อมีการแจ้งเตือน

ส่วนที่ ๓ หน้าที่ความรับผิดชอบของผู้ใช้งาน

อ้างตามระเบียบทอ.ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๖๓ หมวด ๕ ส่วนที่ ๓ ข้อ ๔๙ มีใจความสำคัญ ดังนี้

ต้องเก็บ username password เป็นความลับ

กำหนดให้มีการเปลี่ยนรหัสเริ่มต้นเป็นของผู้ใช้งานทันที

ส่วนที่ ๔ การควบคุมการเข้าถึงระบบและแอปพลิเคชัน

อ้างตามระเบียบทอ.ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๖๓ หมวด ๕ ส่วนที่ ๔ ข้อ ๕๐ และ ๕๑ มีใจความสำคัญ ดังนี้

มีการควบคุมโดยกำหนดสิทธิ์ กำหนดกลุ่ม บัญชีที่มีสิทธิ์ admin ต้องได้รับมอบหมายและมีเวลากำหนด

บุคคลภายนอกต้องแสดงความยินยอมในการปฏิบัติตามระเบียบนี้

การใช้โปรแกรมประยุกต์ที่อาจละเมิดมาตรการความมั่นคงปลอดภัยระบบสารสนเทศ ต้องมีการจำกัดและควบคุมการใช้อย่างใกล้ชิด

หมวด ๖ การเข้ารหัสสารสนเทศ

อ้างตามระเบียบทอ.ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๖๓ หมวด ๖ ข้อ ๕๓ ๕๔ ๕๕ และ ๕๖ มีใจความสำคัญ ดังนี้

สารสนเทศที่มีชั้นความลับต้องได้รับอนุมัติจากเจ้าของ ผู้มีสิทธิ์และอำนาจในสายงาน โดยสารสนเทศนั้นต้องถูกส่งด้วยการเข้ารหัส ตามมาตรฐานที่ได้รับการรับรองแล้ว จาก ทสส.ทอ.

หากมีการใช้เครือข่ายไร้สายทั้งด้านยุทธการและธุรการต้องมีการป้องกันทั้งการพิสูจน์ทราบและเข้ารหัสที่ได้รับการยืนยันจาก ทสส.ทอ.

ข้อมูล ข่าวสาร สารสนเทศทุกประเภท ที่จัดเก็บในระบบฐานข้อมูลต้องได้รับการจัดระดับการป้องกัน

กุญแจเพื่อเข้ารหัสและถอดรหัส ต้องจำกัดการเข้าถึงเท่าที่จำเป็น

หมวด ๗ ความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม

ส่วนที่ ๑ พื้นที่คุมความมั่นคงปลอดภัย

อ้างตามระเบียบทอ.ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๖๓ หมวด ๗ ส่วนที่ ๑ มีใจความสำคัญ ดังนี้

กำหนดอาคาร สถานที่ซึ่งเป็นที่ตั้งระบบสารสนเทศ เป็นพื้นที่หวงห้าม

จัดทำแผนผังแสดงตำแหน่ง และชนิดพื้นที่ให้ชัดเจน

ดูแลรักษาสภาพแวดล้อมให้คงสภาพพร้อมใช้

ควบคุมการเข้า-ออกบริเวณพื้นที่ ตามสิทธิ์ที่กำหนด

จัดให้มีมาตรการในการรักษาความมั่นคงปลอดภัยให้สำนักงานและเครื่องมือต่าง ๆ

ข้อมูล สื่อบันทึก วัสดุ และอุปกรณ์ต้องจัดเก็บโดยเหมาะสม

ไม่อนุญาตให้ถ่ายภาพหรือบันทึกวิดีโอ และต้องมีป้ายประกาศข้อความพื้นที่หวงห้าม

เตรียมพร้อมรับมือสถานการณ์ฉุกเฉินต่าง ๆ และกำหนดมาตรการป้องกัน

เมื่อเกิดเหตุร้ายแรงจนไม่สามารถพิทักษ์รักษาระบบสารสนเทศได้ ให้เคลื่อนย้ายและทำลายตามขั้นตอนปฏิบัติ

ส่วนที่ ๒ ความมั่นคงปลอดภัยของอุปกรณ์

อ้างตามระเบียบทอ.ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๖๓ หมวด ๗ ส่วนที่ ๒ มีใจความสำคัญ ดังนี้

ต้องกำหนดให้มีระบบกระแสไฟฟ้าสำรองและต้องมีการตรวจสอบระบบไฟฟ้าสำรอง อย่างน้อยปีละ ๒ ครั้ง

ต้องมีการวางแผนจัดการขีดความสามารถของระบบสารสนเทศ อย่างน้อย ปีละ ๑ ครั้ง

ต้องมีการแยกเครื่องมือในการประมวลผลสารสนเทศ ในการพัฒนาและทดสอบระบบ รวมทั้งควรแยกระบบเครือข่ายของการพัฒนาออกจากระบบที่ใช้งานจริง

หมวด ๘ ความมั่นคงปลอดภัยสำหรับการปฏิบัติงาน

ส่วนที่ ๑ ขั้นตอนการปฏิบัติงานและหน้าที่ความรับผิดชอบ

อ้างตามระเบียบทอ.ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๖๓ หมวด ๘ ส่วนที่ ๑ ข้อ ๗๔ ๗๕ ๗๖ และ ๗๗ มีใจความสำคัญ ดังนี้

มีการจัดทำคู่มือ และ/หรือขั้นตอนการปฏิบัติงานสารสนเทศ

เมื่อมีการเปลี่ยนแปลงระบบสารสนเทศ ต้องบันทึกการเปลี่ยนแปลงทุกครั้ง

จัดการขีดความสามารถเพื่อใช้ในการพยากรณ์ให้รองรับความต้องการในอนาคต

แยกเครื่องมือในการประมวลผล ในการพัฒนาและทดสอบ

ส่วนที่ ๒ การป้องกันโปรแกรมประสงค์ร้าย (Malware)

อ้างตามระเบียบทอ.ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๖๓ หมวด ๘ ส่วนที่ ๒ ข้อ ๗๘ ๗๙ ๘๓ และ ๘๔ มีใจความสำคัญ ดังนี้

เครื่องลูกข่ายต้องได้รับการติดตั้งซอฟต์แวร์ป้องกันโปรแกรมประสงค์ร้าย

ต้องมีการปรับปรุงข้อมูลล่าสุดอยู่เสมอ

ห้าม สร้าง จัดเก็บ หรือเผยแพร่โปรแกรมประสงค์ร้าย

ห้าม ผู้ใช้งานสร้างหรือรบกวนการทำงานของซอฟต์แวร์ป้องกันโปรแกรมประสงค์ร้าย

ส่วนที่ ๓ การสำรองข้อมูล

อ้างตามระเบียบทอ.ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๖๓ หมวด ๘ ส่วนที่ ๓ มีใจความสำคัญ ดังนี้

กำหนดความถี่ ระยะเวลา อุปกรณ์ เอกสารของการสำรองข้อมูล

ทดสอบข้อมูลสำรองตามห้วงเวลาเพื่อให้มั่นใจ

ส่วนที่ ๔ การบันทึกข้อมูลล็อกและการเฝ้าระวัง (Logging and Monitoring)

อ้างตามระเบียบทอ.ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๖๓ หมวด ๘ ส่วนที่ ๔ ข้อ ๙๐ และ ๙๓ มีใจความสำคัญ ดังนี้

บันทึกข้อมูลเหตุการณ์ การใช้งาน หรือการปฏิเสธการให้บริการของระบบ และเหตุการณ์ที่เกี่ยวข้อง

ต้องตั้งเวลาของเครื่องอุปกรณ์ของหน่วยงานให้ตรงกัน

ส่วนที่ ๕ การควบคุมการติดตั้งซอฟต์แวร์บนระบบให้บริการ

อ้างตามระเบียบทอ.ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๖๓ หมวด ๘ ส่วนที่ ๕ มีใจความสำคัญ ดังนี้

ผู้พัฒนาระบบสารสนเทศต้องมีการควบคุมการติดตั้งซอฟต์แวร์ต่าง ๆ โดยต้องผ่านการทดสอบการใช้งานมาเป็นอย่างดี

ส่วนที่ ๖ การบริหารจัดการช่องโหว่ทางเทคนิค

อ้างตามระเบียบทอ.ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๖๓ หมวด ๘ ส่วนที่ ๖ ข้อ ๙๖ และ ๙๗ มีใจความสำคัญ ดังนี้

ติดตามข้อมูลข่าวสารที่เกี่ยวข้องกับช่องโหว่ในระบบ

ผู้ใช้งานต้องปฏิบัติตามข้อกำหนดทางลิขสิทธิ์

หมวด ๙ ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล

ส่วนที่ ๑ การบริหารจัดการการรักษาความปลอดภัยระบบเครือข่าย

อ้างตามระเบียบทอ.ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๖๓ หมวด ๙ ส่วนที่ ๑ ข้อ ๙๙ ๑๐๐ และ ๑๐๑ มีใจความสำคัญ ดังนี้

ต้องกำหนดผู้รับผิดชอบเครือข่าย รวมทั้งวิธีปฏิบัติเมื่อมีเหตุการณ์ผิดปกติ หรือการละเมิดการรักษาความมั่นคงปลอดภัย และดำเนินการตรวจสอบผู้กระทำการละเมิด

ห้ามติดตั้งอุปกรณ์เครือข่ายโดยไม่ได้รับอนุญาต

ต้องจำกัดจำนวนการเชื่อมต่อจากเครือข่ายภายนอก ทอ.

ห้ามเชื่อมต่อเครือข่ายด้านยุทธการกับเครือข่ายอินเทอร์เน็ต ยกเว้นได้รับการตรวจสอบและเห็นชอบจาก ทสส.ทอ.

ออกแบบเครือข่ายสารสนเทศตามกลุ่มของการให้บริการของระบบสารสนเทศ

ต้องจัดทำแผนผังเครือข่าย พร้อมทั้งปรับปรุงให้เป็นปัจจุบัน

ออกแบบเครือข่ายสารสนเทศตามกลุ่มของการให้บริการของระบบสารสนเทศ

ส่วนที่ ๒ การถ่ายโอนสารสนเทศ (Information Transfer)

อ้างตามระเบียบทอ.ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๖๓ หมวด ๙ ส่วนที่ ๒ มีใจความสำคัญ ดังนี้

หากมีการแลกเปลี่ยนสารสนเทศกับหน่วยงานนอกกองทัพอากาศ ต้องได้รับการตรวจสอบระดับความปลอดภัยที่เหมาะสมจาก ทสส.ทอ.

ต้องมีการจัดทำข้อตกลงในการถ่ายโอนแลกเปลี่ยนสารสนเทศ

หมวด ๑๐ การจัดหา การพัฒนา และการบำรุงรักษาระบบ

ส่วนที่ ๑ การกำหนดความต้องการด้านความมั่นคงปลอดภัยระบบสารสนเทศ

อ้างตามระเบียบทอ.ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๖๓ หมวด ๑๐ ส่วนที่ ๑ มีใจความสำคัญ ดังนี้

ต้องวิเคราะห์และกำหนดมาตรการปฏิบัติก่อนที่จะเกิดความเสียหาย

ต้องวิเคราะห์และกำหนดมาตรการปฏิบัติหลังที่จะเกิดความเสียหาย

ส่วนที่ ๒ ความมั่นคงปลอดภัยสำหรับกระบวนการในการสนับสนุนและการพัฒนาระบบ

อ้างตามระเบียบทอ.ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๖๓ หมวด ๑๐ ส่วนที่ ๒ มีใจความสำคัญ ดังนี้

กำหนดหลักเกณฑ์ในการพัฒนาซอฟต์แวร์ และปฏิบัติตามนโยบายหรือข้อกำหนดของ ทอ.

ทบทวนทางเทคนิค และทดสอบด้านความมั่นคงปลอดภัย

หมวด ๑๑ ความสัมพันธ์กับผู้ให้บริการภายนอก

ส่วนที่ ๑ ความมั่นคงปลอดภัยสารสนเทศด้านความสัมพันธ์กับผู้ให้บริการภายนอก

อ้างตามระเบียบทอ.ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๖๓ หมวด ๑๑ ส่วนที่ ๑ มีใจความสำคัญ ดังนี้

ต้องจัดทำข้อกำหนด หรือสัญญาร่วมกันระหว่างหน่วยงานกับผู้ให้บริการภายนอก และต้องจัดทำเป็นลายลักษณ์อักษร

ส่วนที่ ๒ การบริหารจัดการการให้บริการโดยผู้ให้บริการภายนอก

อ้างตามระเบียบทอ.ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๖๓ หมวด ๑๑ ส่วนที่ ๒ มีใจความสำคัญ ดังนี้

การติดตามและทบทวนบริการของผู้ให้บริการภายนอก ต้องจัดทำข้อตกลง กำหนดสิทธิ์สำหรับกองทัพอากาศ

จัดทำเอกสารวิธีปฏิบัติงาน กำกับดูแลการเปลี่ยนแปลงรายละเอียดการให้บริการ

หมวด ๑๒ การบริหารจัดการสถานการณ์ (Incident) ความมั่นคงปลอดภัยสารสนเทศ

อ้างตามระเบียบทอ.ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๖๓ หมวด ๑๒ มีใจความสำคัญ ดังนี้

ทสส.ทอ. มีหน้าที่

ควบคุม กำกับ และกำหนดหน้าที่รับผิดชอบในการดำเนินการ

ศซบ.ทอ. มีหน้าที่

เฝ้าระวังสถานการณ์

ต้องมีการกำหนดขั้นตอนไว้รองรับกรณีเกิดสถานการณ์ความไม่มั่นคงปลอดภัย

การตอบสนองต่อสถานการณ์ความมั่นคงปลอดภัยระบบต้องปฏิบัติตามขั้นตอนปฏิบัติที่จัดทำไว้เป็นลายลักษณ์อักษร

ต้องบันทึกสถานการณ์ละเมิดความมั่นคงปลอดภัยระบบ

ต้องรวบรวมและจัดเก็บหลักฐานตามกฎหมาย

น.รมปภ มีหน้าที่

.ต้องบันทึกช่องโหว่ที่สังเกตพบหรือเกิดความสงสัยในระบบและรายงาน ศซบ.ทอ.

บุคคลใน ทอ. มีหน้าที่

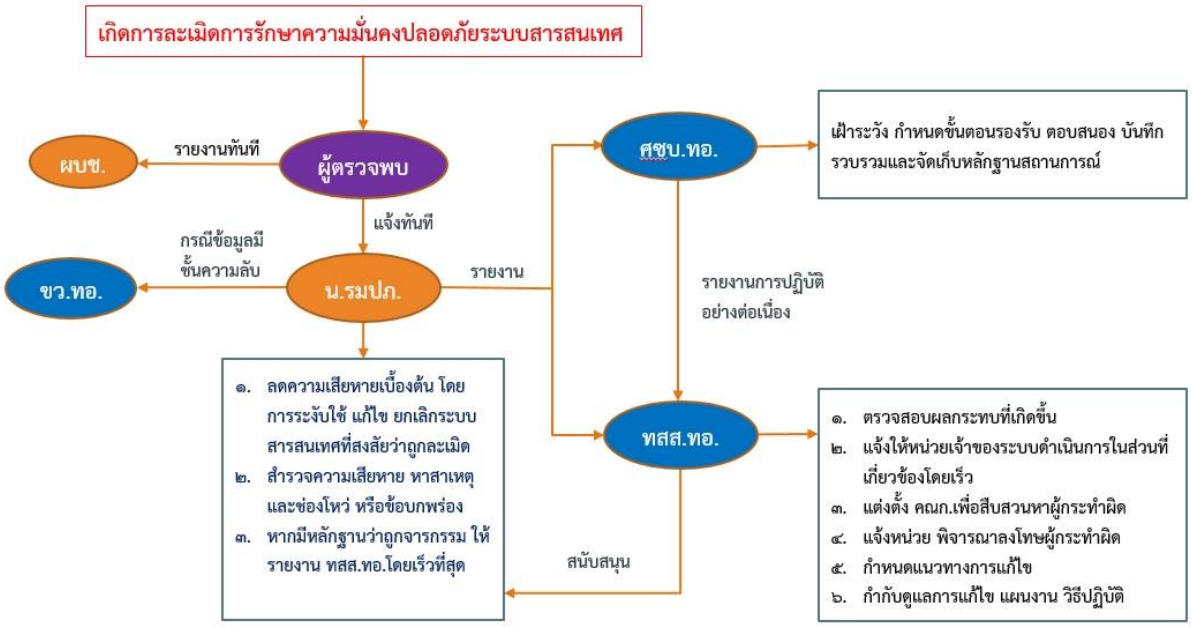
รายงานเหตุละเมิดความมั่นคงปลอดภัย

รายงานการทำงานที่ผิดปกติ

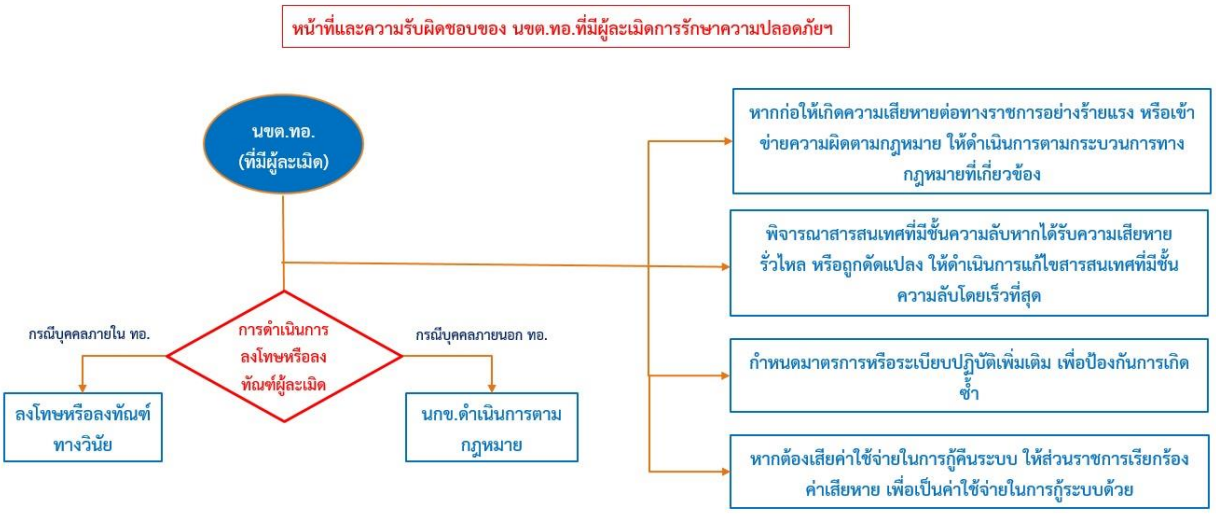
รายงานเหตุฯ และห้ามดำเนินการใด ๆ ที่เกี่ยวข้องกับหลักฐานด้วยตนเอง

หมวด ๑๓ การปฏิบัติเมื่อเกิดการละเมิดการรักษาความปลอดภัยสารสนเทศ

เมื่อเกิดเหตุการณ์การละเมิดการรักษาความปลอดภัยสารสนเทศขึ้น แต่ละหน่วยที่เกี่ยวข้องจะต้องปฏิบัติตามระเบียบนี้ โดยมีรายระเอียดสรุปดับรูปต่อไปนี้



รูปที่ ๒๑ การปฏิบัติเมื่อเกิดการละเมิดการรักษาความปลอดภัยสารสนเทศ



รูปที่ ๒๒ การปฏิบัติเมื่อเกิดการละเมิดการรักษาความปลอดภัยสารสนเทศ (ต่อ)

ผนวก ก หน้าที่การรักษาความปลอดภัยระบบสารสนเทศแบ่งตามบทบาท

ผู้บริหาร หรือผู้ดูแลระบบ มีหน้าที่

บริหารและดูแลอุปกรณ์คอมพิวเตอร์

ควบคุมและตรวจสอบการใช้งานระบบ

ตรวจสอบ ควบคุม ดูแล และบำรุงรักษาระบบ

รักษาความปลอดภัยระบบ

ผู้บริหารฐานขอมูล มีหน้าที่

ควบคุมดูแลฐานข้อมูล

เลือก ตัดตอน และกำหนดรูปแบบขอมูลที่เก็บในแฟ้มขอมูล

รักษาความปลอดภัยฐานข้อมูล

ตรวจสอบฐานข้อมูล และวิเคราะห์ขอมูล

ควบคุม และบริการการใช้งานฐานขอมูล

ผู้ดูแลเครือขาย มีหน้าที่

กำหนด IP ให้คอมพิวเตอร์

กำหนด Account และ Password ของผูใชภายในเครือขายที่รับผิดชอบ

ดูแลการใช้เครือขายคอมพิวเตอร์

ดูแลโครงสร้างพื้นฐานและอุปกรณ์ที่เกี่ยวกับระบบเครือข่าย

รักษาความปลอดภัยระบบเครือข่าย

นักเขียนโปรแกรม มีหน้าที่

เขียนและพัฒนาโปรแกรมที่ไดรับมอบหมาย

จัดหาข้อมูลเพื่อทดสอบโปรแกรม

ดูแลบำรุงรักษาโปรแกรมที่พัฒนา

รักษาความปลอดภัยโปรแกรม

ผนวก ข คำศัพท์คอมพิวเตอร์ที่เกี่ยวข้อง

สามารถศึกษารายละเอียดเพิ่มเติมได้ตาม QR Code ต่อไปนี้

รูปที่ ๒๓ QR Code ระเบียบกองทัพอากาศว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๖๓

บทที่ ๔
ความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร ทอ.

การบริหารความเสี่ยง (Risk Management) เป็นสิ่งที่มีความสำคัญและยากจะหลีกเลี่ยงได้ เนื่องจากภัยคุกคามด้านความมั่นคงปลอดภัยข้อมูลและระบบสารสนเทศได้ทวีความรุนแรง และได้สร้างความเสียหายมากขึ้นไปตามแนวโน้มของการใช้งานระบบสารสนเทศและอินเทอร์เน็ตของหน่วยงานที่เพิ่มขึ้น ทำให้ระบบต่าง ๆ เหล่านี้ล้วนแล้วแต่มีความเสี่ยงที่จะถูกโจมตีผ่านช่องโหว่ (Vulnerability) เพื่อทำลายคุณสมบัติทั้ง ๓ ด้านของความมั่นคงปลอดภัยข้อมูลและระบบสารสนเทศ ได้แก่ ความลับ ความถูกต้อง และความพร้อมใช้งาน ไม่ว่าข้อมูลนั้นอยู่ระหว่างการประมวลผล ระหว่างที่มีการส่งผ่านเครือข่าย หรือจัดเก็บในอุปกรณ์ ภัยคุกคาม (Threat) ต่อข้อมูลนั้นอาจรวมถึงการโจมตีทางไซเบอร์ ภัยธรรมชาติ ความผิดพลาดจากผู้ใช้งานหรือเครื่อง หรือแม้กระทั่งสภาพแวดล้อมด้านอาคารสถานที่ ดังนั้น จึงมีความจำเป็นอย่างยิ่งที่หน่วยงานต้องตระหนักถึงความสำคัญ และรับผิดชอบต่อการบริหารความเสี่ยงที่เกี่ยวข้องกับระบบสารสนเทศ โดยเฉพาะระบบที่มีความสำคัญต่อการสนับสนุนภารกิจของหน่วยงาน ตลอดจนการกำหนดกฎระเบียบ ข้อบังคับ และกฎหมายต่าง ๆ ที่กำหนดให้หน่วยงานต้องปฏิบัติตาม ล้วนแล้วแต่ต้องมีความเกี่ยวข้องกับการบริหารความเสี่ยงระบบสารสนเทศในหน่วยงานแทบทั้งสิ้น

การรักษาความปลอดภัยของข้อมูลนั้น เป็นกระบวนในเชิงรุกเพื่อบริหารความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ แต่ที่ผ่านมาโดยส่วนใหญ่การรักษาความปลอดภัยจะเป็นแบบเชิงรับ กล่าวคือ หน่วยงานจะรอให้มีเหตุการณ์เกิดขึ้นก่อนแล้วจึงหาวิธีการที่จะป้องกันเหตุการณ์นั้น ซึ่งอาจจะก่อให้ผลกระทบและเกิดความเสียหายต่อหน่วยงานมากกว่าที่คาดไว้ได้ การจัดการในเชิงรุกนั้นเป็นขั้นตอนที่ทำก่อนที่จะเกิดเหตุการณ์ จึงทำให้หน่วยงานสามารถประเมินความเสียหายและประเมินงบประมาณสำหรับการจัดความเสี่ยงได้

เนื่องจากภารกิจของกองทัพอากาศโดยส่วนใหญ่ ได้นำเอาระบบเทคโนโลยีสารสนเทศและการสื่อสารเข้ามามีบทบาทสำคัญต่อการปฏิบัติงานของหน่วยงาน ฉะนั้นเพื่อให้การนำระบบเทคโนโลยีสารสนเทศมาสนับสนุนการปฏิบัติงานเกิดประโยชน์สูงสุด และลดโอกาสความเสียหายที่อาจเกิดขึ้น จึงจำเป็นต้องมีการบริหารจัดการความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ เพื่อให้มีขีดความสามารถในการปฏิบัติการที่ใช้เครือข่ายเป็นศูนย์กลางตามยุทธศาสตร์กองทัพอากาศได้

๑. ทรัพยากรด้านเทคโนโลยีและการสื่อสาร (ICT Resources)

๑.๑ ระบบงาน (Application System) ได้แก่ ขั้นตอนและกระบวนการปฏิบัติงาน

๑.๒ เทคโนโลยี (Technology) ได้แก่ เครื่องคอมพิวเตอร์ (Hardware) โปรแกรมระบบ (Operating System) ระบบบริหารฐานข้อมูล (Database Management System) ระบบเครือข่าย (Network) และระบบมัลติมีเดีย

๑.๓ องค์ประกอบ (Facilities) ได้แก่ ทรัพยากรต่าง ๆ ที่ใช้เป็นสถานที่ติดตั้งหรือจัดวาง ตลอดจนสาธารณูปโภคที่จำเป็น เพื่อการปฏิบัติงานของระบบสารสนเทศ

๑.๔ บุคลากร (People) ได้แก่ บุคลากรที่มีความรู้ความชำนาญในการบริหารและปฏิบัติงานสำหรับการดูแลและจัดการระบบ รวมถึงผู้ใช้งานทั่วไป

๑.๕ ข้อมูล (Data) ได้แก่ ข้อมูลในรูปแบบต่าง ๆ ทั้งที่มีโครงสร้างและไม่มีโครงสร้าง ข้อมูลด้านกราฟิกและข้อมูลที่เป็นมัลติมีเดีย

๒. การวิเคราะห์ความเสี่ยง

ก่อนที่จะประเมินความเสี่ยงนั้นจำเป็นอย่างยิ่งที่ต้องทำความเข้าใจว่าความเสี่ยงคืออะไร มีสาเหตุมาจากอะไร การวิเคราะห์ความเสี่ยงจนทำให้เข้าใจปัจจัยหรือสาเหตุที่ทำให้เกิดความเสี่ยงนั้น จะนำไปสู่การหาวิธีในการป้องกันหรือแก้ไขได้ต่อไป

ความเสี่ยง (Risk) คือ เหตุการณ์หรือการกระทำใด ๆ ที่อาจเกิดขึ้นภายใต้สถานการณ์ที่ไม่แน่นอน และจะส่งผลกระทบหรือสร้างความเสียหาย ก่อให้เกิดการลดทอน ขัดขวาง ทำลายต่อทรัพย์สิน หรือลดโอกาสที่จะบรรลุเป้าหมายตามภารกิจของหน่วยงาน ความเสี่ยงนั้นเกิดจากปัจจัยเสี่ยง (Risk Factor) ซึ่งหมายถึง ต้นเหตุหรือสาเหตุที่มาของความเสี่ยง ที่ทำให้ไม่บรรลุตามวัตถุประสงค์ที่กำหนดไว้ โดยต้องระบุได้ด้วยว่าเหตุการณ์นั้นเกิดที่ไหน เกิดขึ้นเมื่อใด และเกิดขึ้นได้อย่างไร เพื่อจะได้นำไปวิเคราะห์และกำหนดมาตรการลดความเสี่ยงในภายหลังได้อย่างถูกต้อง

การวิเคราะห์ความเสี่ยง ประกอบด้วย ๓ กระบวนการ คือ

๑. การชี้ระบุความเสี่ยง (Risk identification) เป็นการชี้ให้เห็นถึงความเสี่ยงที่หน่วยงานเผชิญอยู่ กระบวนการนี้จำเป็นต้องอาศัยความรู้ความเข้าใจหน่วยงาน ภารกิจและกิจกรรมสิ่งแวดล้อมด้านกฎหมาย สังคมการเมืองและวัฒนธรรม พัฒนาการและปัจจัยที่มีต่อความสำเร็จของหน่วยงาน รวมทั้งโอกาสและภัยคุกคามที่มีต่อหน่วยงาน การชี้ระบุความเสี่ยงควรได้ดำเนินการอย่างทั่วถึงครอบคลุมกิจกรรมในทุก ๆ ด้านของหน่วยงาน สาเหตุสำคัญของความเสี่ยงคือการมีภัยคุกคาม (Threat) ที่อาจส่งผลให้เกิดการละเมิดความมั่นคงสารสนเทศและส่งผลเสียตามมา

การชี้ระบุความเสี่ยง (Risk Identification) อาจพิจารณาถึงเหตุการณ์หรือสิ่งที่เคยเกิดขึ้นมาแล้วในอดีตกับหน่วยงานนั้นหรือหน่วยงานอื่นใด หรืออาจเป็นสิ่งที่มีความเป็นไปได้ว่าจะเกิดขึ้นแม้ไม่เคยเกิดขึ้นมาก่อนก็ได้ กระบวนการในการชี้ระบุความเสี่ยงอาจใช้วิธีการต่าง ๆ ร่วมกันได้ เช่น

- การระดมสมอง (Brain Storming)
- การออกแบบสอบถาม (Questionnaire)
- การวิเคราะห์กระบวนการทำงานหรือกิจกรรมในภารกิจ (Business Process Analysis)
- การวิเคราะห์สภาพการณ์เหตุการณ์ละเมิดความมั่นคง (Scenario Analysis)
- การประชุมเชิงปฏิบัติการด้านการประเมินความเสี่ยง (Risk Assessment Workshop)
- การสืบสวนเหตุการณ์ละเมิดความมั่นคงสารสนเทศ (Incident Investigation)
- การตรวจสอบและการตรวจสภาพระบบ (Auditing and Operability Studies)
- การวิเคราะห์สถานการณ์ (SWOT Analysis)

๒. ลักษณะรายละเอียดของความเสี่ยง (Description of Risk) เมื่อชี้ระบุความเสี่ยงได้แล้ว และนำมาบรรยายรายละเอียดและลักษณะของความเสี่ยงนั้น ได้แก่

- ชื่อความเสี่ยง (Name)
- ขอบเขต (Scope)
- ลักษณะความเสี่ยง (Nature)
- ผู้ที่มีผลกระทบ
- ลักษณะเชิงประมาณ
- การยอมรับความเสี่ยง
- การบำบัดและการควบคุม
- แนวทางการปรับปรุง
- การพัฒนากลยุทธ์และนโยบาย

๓. การประมาณความเสี่ยง (Risk Estimation) ขั้นตอนนี้เป็นการดูปัญหาความเสี่ยงในแง่ของโอกาสการเกิดเหตุหรือเหตุการณ์ว่ามีมากน้อยเพียงไรและผลกระทบที่เกิดขึ้นว่ามีความรุนแรงหรือก่อให้เกิดความเสียหายมากน้อยเพียงใด

ระดับโอกาส (Likelihood) ที่จะเกิดเหตุการณ์ภัยคุกคามที่มีผลต่อความมั่นคงปลอดภัยของทรัพย์สิน จะพิจารณาจากสถิติที่เกิดขึ้นในอดีต แนวโน้มในปัจจุบันและอนาคต มาตรการควบคุมหรือการป้องกันไม่ให้เกิดเหตุการณ์เหล่านั้น รวมถึงการประเมินฝ่ายตรงข้ามหรือศัตรูว่ามีแรงจูงใจมากน้อยแค่ไหน ที่จะเข้ามาทำให้เกิดเหตุการณ์ด้านความมั่นคงเหล่านั้น โอกาสจะเกิดขึ้นนั้นสามารถกำหนดได้สองแบบคือ แบบเชิงปริมาณและเชิงคุณภาพ เชิงปริมาณจะกำหนดเป็นตัวเลขหรือร้อยละ เช่น ถ้าระบุว่าเหตุการณ์นี้จะเกิดขึ้นแน่นอนก็เป็นระดับ ๕ ไล่เรียงไปตามระดับ ส่วนการกำหนดโอกาสที่จะเกิดในเชิงคุณภาพนั้น นิยมกำหนดเป็นห้าระดับ เช่น สูงมาก สูง ปานกลาง น้อย น้อยมาก

ค่าเชิงคุณภาพ	ค่าเชิงปริมาณ	คำอธิบาย
สูงมาก	๕	เหตุการณ์ภัยคุกคามมีโอกาสที่จะเกิดขึ้นเกือบจะแน่นอน
สูง	๔	เหตุการณ์ภัยคุกคามมีโอกาสที่จะเกิดสูง
ปานกลาง	๓	เหตุการณ์ภัยคุกคามมีโอกาสที่จะเกิดปานกลาง
น้อย	๒	เหตุการณ์ภัยคุกคามมีโอกาสที่จะเกิดน้อย
น้อยมาก	๑	เหตุการณ์ภัยคุกคามแทบจะไม่มีโอกาสที่จะเกิด

ระดับผลกระทบ (Impact) เป็นการกำหนดระดับความรุนแรงของผลกระทบ ที่เกิดจากภัยคุกคามที่มีผลต่อความมั่นคงปลอดภัยของทรัพย์สิน สามารถกำหนดได้สองแบบคือ แบบเชิงปริมาณและเชิงคุณภาพ เชิงปริมาณจากกำหนดเป็นตัวเลขหรือร้อยละ เช่น ถ้าระบุว่าเหตุการณ์นี้ส่งผลกระทบอย่างร้ายแรงมากก็เป็นระดับ ๕ โอกาสที่จะเกิดเชิงในคุณภาพนั้น นิยมกำหนดเป็น ๕ ระดับ เช่น สูงมาก สูง ปานกลาง ต่ำ ต่ำมาก

ค่าเชิงคุณภาพ	ค่าเชิงปริมาณ	คำอธิบาย
สูงมาก	๕	เหตุการณ์ภัยคุกคาม สามารถสร้างความเสียหายร้ายแรงมากหลายด้าน หรือสร้างความหายนะต่อการดำเนินงานของหน่วยงาน ทรัพย์สิน บุคลากร หน่วยงานอื่น หรือต่อประเทศชาติ
สูง	๔	เหตุการณ์ภัยคุกคาม สามารถสร้างความเสียหายร้ายแรงมาก หรือสร้างความหายนะต่อการดำเนินงานของหน่วยงาน ทรัพย์สิน บุคลากร หน่วยงานอื่น หรือต่อประเทศชาติ
ปานกลาง	๓	เหตุการณ์ภัยคุกคาม สามารถสร้างความเสียหายร้ายแรงต่อการดำเนินงานของหน่วยงาน ทรัพย์สิน หรือหน่วยงานอื่น
ต่ำ	๒	เหตุการณ์ภัยคุกคาม สามารถสร้างความเสียหายบางส่วน ต่อการดำเนินงานของหน่วยงาน ทรัพย์สิน หรือหน่วยงานอื่น
ต่ำมาก	๑	เหตุการณ์ภัยคุกคามที่สร้างความเสียหายน้อยมาก จนสามารถละเลยได้ต่อการดำเนินงานของหน่วยงาน ทรัพย์สิน หรือบุคลากร

๓. การบริหารความเสี่ยง

การบริหารความเสี่ยง (Risk Management) คือ กระบวนการที่ใช้ในการบริหารจัดการ ให้โอกาสที่จะเกิดเหตุการณ์ความเสี่ยงลดลง หรือผลกระทบของความเสียหายจากเหตุการณ์ความเสี่ยงลดลงอยู่ในระดับที่หน่วยงานยอมรับได้

๓.๑ วัตถุประสงค์ของการบริหารจัดการความเสี่ยง

๓.๑.๑ เพื่อเตรียมความพร้อมและรองรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบสารสนเทศของหน่วยงาน

๓.๑.๒ เพื่อให้สามารถวางแผนควบคุมและแก้ไขความเสี่ยงต่อระบบสารสนเทศ

๓.๑.๓ เพื่อนำระบบสารสนเทศมาสนับสนุนการดำเนินงานของหน่วยงานให้เกิดประสิทธิภาพสูงสุด และลดโอกาสที่อาจเกิดความเสียหาย

๓.๑.๔ เพื่อเป็นแนวทางการดำเนินการ กำกับดูแล และตรวจสอบเกี่ยวกับการบริหารจัดการความเสี่ยงที่อาจมีผลกระทบต่อการดำเนินงาน

๓.๑.๕ เพื่อช่วยเพิ่มประสิทธิภาพในการตัดสินใจ โดยคำนึงถึงปัจจัยเสี่ยงและความเสี่ยงในด้านต่าง ๆ ที่อาจจะมีผลกระทบกับการดำเนินงาน วัตถุประสงค์ และนโยบาย แล้วพิจารณาหาแนวทางในการป้องกันหรือจัดการกับความเสี่ยงเหล่านั้น ทั้งก่อนที่จะเริ่มปฏิบัติงาน ระหว่างปฏิบัติงาน และสิ้นสุดการปฏิบัติงาน

๓.๒ กระบวนการในการบริหารความเสี่ยงของระบบสารสนเทศ

ขั้นที่ ๑ การระบุความเสี่ยง และผลกระทบที่มีต่อระบบสารสนเทศ

ขั้นที่ ๒ ประเมินถึงโอกาสที่จะเกิดขึ้นของความเสี่ยงและความรุนแรงของผลกระทบ ซึ่งแต่ละความเสี่ยงจะมีความรุนแรงแตกต่างกัน ทั้งนี้การควบคุมความเสี่ยงหรือหลีกเลี่ยงความเสี่ยงนั้น ก็จะขึ้นอยู่กับมาตรการควบคุมความเสี่ยงของแต่ละหน่วยงาน

ขั้นที่ ๓ มีการวางแผนโดยกำหนดมาตรการเพื่อควบคุมผลกระทบของความเสี่ยง เพื่อให้สามารถบรรลุเป้าหมายหรือใกล้เคียงกับเป้าหมายที่กำหนดไว้ จะต้องมีการกำหนดกลยุทธ์ในการควบคุมผลกระทบของความเสี่ยงที่อาจเกิดขึ้นเพื่อที่จะลดและตรวจหาความเสี่ยงที่ได้ประเมินเอาไว้ โดยให้มีการแต่งตั้งเจ้าหน้าที่ผู้รับผิดชอบของแต่ละหน่วยงานเป็นผู้ดูแลรักษาความมั่นคงปลอดภัยของระบบ และป้องกัน/แก้ไข/ควบคุมความเสี่ยงไม่ให้มีผลกระทบ โดยสามารถดำเนินการตามแผนได้

ขั้นที่ ๔ การประเมินแผนเพื่อทราบความเสี่ยงที่เหลืออยู่ เจ้าหน้าที่ผู้รับผิดชอบจะต้องมีการรวบรวมและรายงานข้อมูลของความเสี่ยงที่ยอมรับได้ และข้อมูลที่เกี่ยวข้องเพื่อนำเสนอให้ผู้บังคับบัญชาทราบและบันทึกไว้เป็นหลักฐาน

ขั้นที่ ๕ การติดตาม กำกับ และตรวจสอบ การปฏิบัติการควบคุมความเสี่ยงตามแผนที่ดำเนินการไว้ในขั้นที่ ๓ มีการตรวจสอบการทำงานของเจ้าหน้าที่ที่ได้รับมอบหมายให้ดูแลรักษาความมั่นคงปลอดภัยของระบบโดยมีหลักฐานประกอบการปฏิบัติหน้าที่ตามระยะเวลาที่กำหนด

๔. มาตรฐานการบริหารความเสี่ยง

มาตรฐานสากลต่าง ๆ ที่กล่าวถึงการบริหารความเสี่ยงมีอยู่ด้วยกันหลายมาตรฐาน ซึ่งแต่ละมาตรฐานก็มีข้อแตกต่างกันตั้งแต่วัตถุประสงค์ ขั้นตอนการปฏิบัติ ดังนั้น หน่วยงานควรต้องพิจารณาเลือกมาตรฐานที่เหมาะสมกับลักษณะการดำเนินการและภารกิจของหน่วยงานนั้น ๆ หรือหากเป็นเรื่องเฉพาะด้านการรักษาความมั่นคงปลอดภัยข้อมูลและระบบสารสนเทศ ผู้บริหารหรือผู้บังคับบัญชาด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศขององค์กร ต้องเลือกมาตรฐานหรือกรอบการปฏิบัติมาใช้ให้เหมาะสมกับการบริหารความเสี่ยงระบบสารสนเทศในหน่วยงานของตน

มาตรฐาน	ชื่อมาตรฐาน
ISO 31000:2018	Risk Management
ISO/IEC 27005:2018	Information technology - Security techniques - Information Security Risk Management
NIST SP 800-30 Rev1	Guide for Conducting Risk Assessments

๕. การประเมินความเสี่ยง

การประเมินความเสี่ยง จะพิจารณาจากปัจจัยของขั้นตอนที่ผ่านมา ได้แก่ โอกาสที่ภัยคุกคามที่เกิดขึ้นทำให้ระบบขาดความมั่นคงปลอดภัย ระดับผลกระทบหรือความรุนแรงของภัยคุกคามที่มีต่อระบบ และประสิทธิภาพของแผนการควบคุมความปลอดภัยของระบบ การวัดความเสี่ยงมีการกำหนดแผนภูมิความเสี่ยงที่ได้จากการ

พิจารณาจัดระดับความสำคัญของความเสี่ยงจากการคำนวณระดับความเสี่ยง การคำนวณระดับความเสี่ยง (Degree of Risk) จะได้จากผลคูณของระดับโอกาส (Likelihood) กับระดับผลกระทบ (Impact) ดังนี้

ระดับความเสี่ยง = ระดับโอกาส x ระดับผลกระทบ

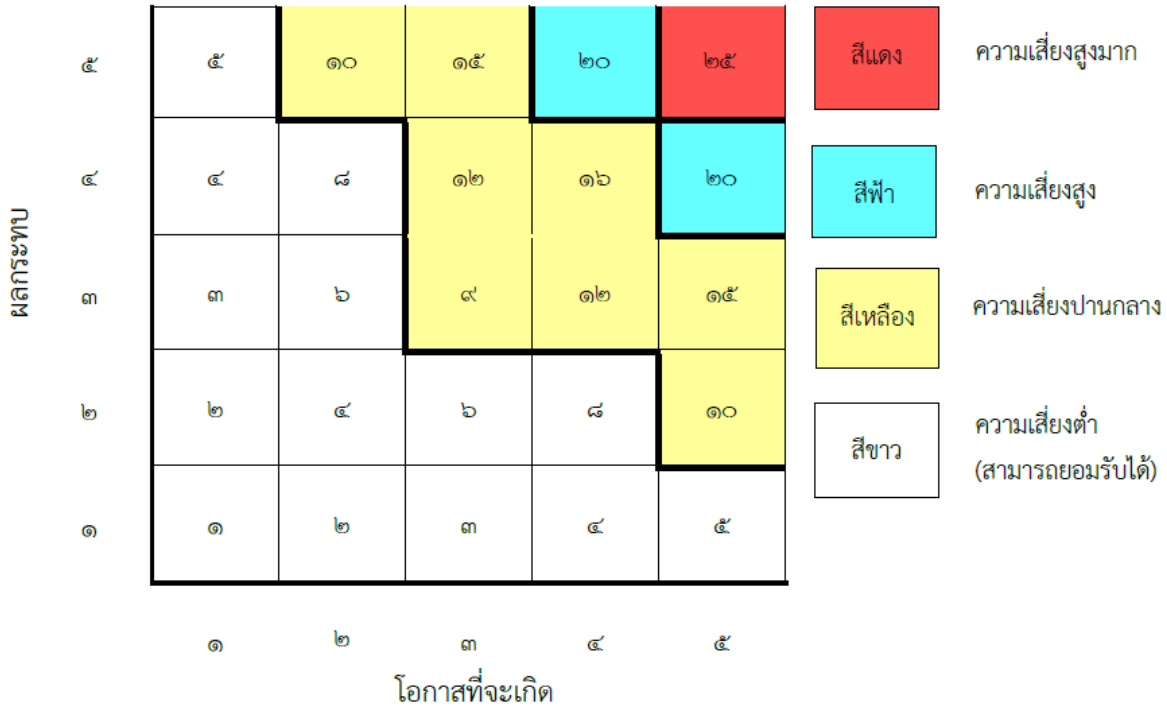
ระดับคะแนนความเสี่ยงใช้เกณฑ์ในการจัดแบ่ง ดังนี้

ระดับค่าความเสี่ยง	ระดับความเสี่ยง	สีที่แสดง
๑ – ๘	ความเสี่ยงต่ำ (สามารถยอมรับได้)	ขาว
๙ – ๑๖	ความเสี่ยงปานกลาง	เหลือง
๒๐	ความเสี่ยงสูง	ฟ้า
๒๕	ความเสี่ยงสูงมาก	แดง

แผนภูมิความเสี่ยง (Risk Map)

การวัดระดับความเสี่ยงโดยจัดลำดับจากผลกระทบและความเป็นไปได้ที่จะเกิดขึ้น

รูปที่ ๒๔ แผนภาพแสดงความเสี่ยงตามผลกระทบและโอกาสที่จะเกิด



รูปที่ ๒๕ แผนภาพแสดงความเสี่ยงตามผลกระทบและโอกาสที่จะเกิด

ปัญหาและอุปสรรคที่สำคัญที่พบเจอในการบริหารจัดการความเสี่ยง คือ ปัญหาในขั้นตอนการประเมินความเสี่ยง เนื่องจากการประเมินความเสี่ยงเป็นขั้นตอนที่สำคัญมาก หากมีการประเมินความเสี่ยงที่ไม่ครบถ้วนและไม่ครอบคลุมจะทำให้กระบวนการในการบริหารจัดการความเสี่ยงนั้นมีช่องโหว่โดยคาดไม่ถึง ซึ่งอาจก่อให้เกิดความเสียหายและกระทบต่อการดำเนินงานของหน่วยงานได้ ดังนั้น การประเมินความเสี่ยงให้ถูกต้องอาจต้องอาศัยคำแนะนำและความช่วยเหลือจากผู้เชี่ยวชาญ

๖. การจัดการความเสี่ยง

ผลที่ได้จากการประเมินความเสี่ยง คือ ระดับความเสี่ยงของหน่วยงาน จากนั้นจะเป็นขั้นตอนในการพิจารณาว่าระดับความเสี่ยงดังกล่าวอยู่ในระดับที่ยอมรับได้หรือไม่ หากอยู่ในระดับที่ยอมรับได้ก็ไม่จำเป็นต้องดำเนินการอะไรนอกเหนือจากการเฝ้าระวังเหตุการณ์ แต่หากระดับความเสี่ยงนั้นอยู่ในระดับที่ยอมรับไม่ได้จะต้องมีการจัดการความเสี่ยง

การบรรเทาความเสี่ยง (Risk Mitigation) เกี่ยวข้องกับการจัดลำดับ การคำนวณความเสี่ยง และการลงมือควบคุมลดความเสี่ยงอย่างเหมาะสมตามแนวทางที่มาจากการประเมินความเสี่ยง เนื่องจากการที่จะกำจัดความเสี่ยงในระบบทั้งหมดนั้นเป็นเรื่องที่ทำได้ยาก ผู้บังคับบัญชาของหน่วยจะต้องเป็นผู้รับผิดชอบการทำงานในส่วนนี้ด้วย เงื่อนไขในการใช้งบประมาณที่สมดุล เพื่อให้เกิดประสิทธิภาพสูงสุด และใช้วิธีการควบคุมที่เหมาะสมที่สุด

เพื่อลดระดับความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ โดยส่งผลกระทบต่อภารกิจและทรัพยากรของหน่วยให้น้อยที่สุด

กลยุทธ์เพื่อการบรรเทาความเสี่ยง สามารถแบ่งออกเป็น ๔ ประเภท ดังนี้

๑. การลดความเสี่ยง (Risk Reduction) คือ การพิจารณาจำกัดความเสี่ยงให้ผลกระทบลดลงมาอยู่ในระดับที่หน่วยงานสามารถยอมรับได้ เช่น การใช้งานการเข้ารหัสข้อมูล และการใช้งานไฟล์วอล เป็นต้น

๒. การยอมรับความเสี่ยง (Risk Acceptance) คือ การยอมรับความเสี่ยงในระดับที่เป็นอยู่และให้ระบบสารสนเทศดำเนินงานไปตามปกติ ซึ่งเป็นการยอมรับผลกระทบจากความเสี่ยงที่เกิดขึ้นนั้น เนื่องจากพิจารณาแล้วว่า การดำเนินการจัดการความเสี่ยงอาจมีค่าใช้จ่ายสูงไม่คุ้มค่า หน่วยงานอาจยอมรับความเสี่ยงและปรับปรุงเมื่อมีโอกาส

๓. การหลีกเลี่ยงความเสี่ยง (Risk Avoidance) คือ การหลีกเลี่ยงความเสี่ยงด้วยการกำจัดสาเหตุของความเสี่ยง เพื่อลดข้อผิดพลาด ลดช่องโหว่ และโอกาสที่จะเกิดความเสี่ยงขึ้นต่อการดำเนินงานของหน่วยงาน

๔. การถ่ายโอนความเสี่ยง (Risk Transfer) คือ การพิจารณาถ่ายโอนความเสี่ยงไปให้ผู้อื่นรับผิดชอบแทน เช่น การซื้อประกันภัย เป็นต้น

มาตรการควบคุมและแก้ไขความเสี่ยง อาจแบ่งออกเป็น ๓ ประเภท ดังนี้

๑. มาตรการควบคุมทางด้านกายภาพ คือ การจัดให้มีสภาพแวดล้อมทางกายภาพที่เหมาะสม เช่น

- การจัดให้มีระบบควบคุมการเข้าออกสถานที่สำคัญ (Access Control)
- การจัดแบ่งพื้นที่สำคัญ เช่น การแยกศูนย์ข้อมูลออกจากพื้นที่ปฏิบัติงานปกติ
- การจัดระเบียบสายเคเบิลสื่อสารต่าง ๆ ให้เรียบร้อย

๒. มาตรการควบคุมทางด้านเทคนิค คือ การใช้ซอฟต์แวร์หรืออุปกรณ์ฮาร์ดแวร์มาช่วยควบคุมและจัดการด้านการรักษาความมั่นคงปลอดภัย เช่น

- การเข้ารหัสข้อมูล (Encryption)
- การใช้ซอฟต์แวร์ป้องกันและกำจัดไวรัส
- การใช้ไฟล์วอลควบคุมทราฟฟิกเข้าออกเครือข่าย
- การใช้ระบบตรวจจับและป้องกันการบุกรุก (Intrusion Detection System (IDS), Intrusion Prevention System (IPS))

๓. มาตรการควบคุมทางด้านนโยบาย แนวทาง แผน และระเบียบปฏิบัติ คือ การจัดให้มีนโยบาย แนวทางการปฏิบัติ แผนการปฏิบัติ และระเบียบปฏิบัติที่เกี่ยวข้องกับการดำเนินงานของหน่วยงาน ให้บุคลากรของหน่วยงานยึดถือปฏิบัติ และสร้างความตระหนักรู้แก่บุคลากร

บทที่ ๕
การรักษาความปลอดภัยของข้อมูล

การรักษาความปลอดภัยของข้อมูล

เมื่อมีการนำคอมพิวเตอร์และระบบข้อมูลสารสนเทศเข้ามาใช้ การเก็บรวบรวมข้อมูลสารสนเทศของหน่วยงานก็เปลี่ยนรูปแบบไป ข้อมูลและสารสนเทศจะถูกเก็บเป็นไฟล์ และมีการจัดทำระบบข้อมูลส่วนกลางของหน่วยงาน เพื่อให้การนำข้อมูลไปใช้งานง่าย และสะดวกมากขึ้น

เมื่อระบบเสียหายหรือไม่สามารถทำงานได้ตามปกติ เวลาและค่าใช้จ่ายที่ต้องใช้ในการแก้ปัญหาก็สูงตามไปด้วย นอกจากนี้เมื่อทุกคนทั้งในและนอกหน่วยงานสามารถเข้าถึงระบบข้อมูลได้ โดยผ่านทางระบบเครือข่ายคอมพิวเตอร์ เป็นเหตุให้ระบบข้อมูลถูกบุกรุกจากผู้ไม่ประสงค์ดีได้ง่าย นอกจากนี้ระบบคอมพิวเตอร์ยังต้องเผชิญกับภัยคุกคาม (Threat) ต่าง ๆ ได้ง่ายกว่าข้อมูลในรูปแบบเอกสารอีกด้วย

๑ ประเภทของภัยคุกคามต่อความปลอดภัยของข้อมูล

๑.๑ ผู้บุกรุก (Hacker)

หมายถึง ผู้ที่ไม่ได้รับอนุญาตในการใช้งานระบบ แต่พยายามลักลอบเข้ามาใช้งานด้วยวัตถุประสงค์ต่าง ๆ ไม่ว่าจะเพื่อโจรกรรมข้อมูล ผลกำไร หรือความพอใจส่วนบุคคลก็ตาม ความเสียหายจากผู้บุกรุกเป็นภัยคุกตามที่หนัก ดังนั้น หน่วยงานส่วนใหญ่ที่ใช้อินเทอร์เน็ตจึงให้ความสำคัญกับมาตรการป้องกัน Hacker

๑.๒ ไวรัสคอมพิวเตอร์ (Computer Virus)

เป็นซอฟต์แวร์ประเภทที่มีเจตนาร้ายแฝงเข้ามาในระบบคอมพิวเตอร์โดยจะตรวจพบได้ยากไวรัสคอมพิวเตอร์มีหลายประเภทและก่อให้เกิดความเสียหายต่อระบบได้หลายรูปแบบ ตั้งแต่สร้างความรำคาญมีข้อความแปลก ๆปรากฏขึ้นมาเรื่อย ๆ บนหน้าจอ หรือแม้กระทั่งทำลายไฟล์ข้อมูลต่าง ๆ ให้ได้รับความเสียหาย

- ไวรัสเลียนแบบ (Companion Virus) จะแอบแฝงตามไฟล์ต่าง ๆ และคอยสร้างไฟล์ขึ้นมาใหม่ โดยเลียนแบบไฟล์ในระบบเดิม แล้วหลอกให้ระบบเรียกไฟล์ที่สร้างเลียนแบบขึ้นมาใช้งานแทนไฟล์จริง

- ไวรัสโปรแกรม (Program Virus) ถ้ามีการเรียกใช้ไฟล์ที่ติดไวรัสประเภทนี้ ก็จะทำให้ไวรัสแพร่เชื้อไปยังทุกไฟล์ที่สามารถติดต่อไปได้

- ไวรัสบู๊ต (Boot Virus) เป็นไวรัสที่คอยก่อกวนไฟล์สำคัญ ๆ ที่สำหรับเปิดเครื่องในตอนแรก ทำให้เราไม่สามารถบู๊ตเข้าสู่วินโดว์ได้

- ไวรัสหลบหลีก (Stealth Virus) จะหลบหลีกการตรวจจับจากโปรแกรมป้องกันไวรัส โดยจะขัดขวางการทำงานของโปรแกรมบางประเภทที่มีการป้องกันไวรัสด้วยการ copy ข้อมูลเดิมไว้ก่อน โดยไวรัสจะทำการแก้ไขชื่อไฟล์และไดเร็กทอรีที่ติดเชื้อ ทำให้โปรแกรมป้องกันไวรัสตรวจหาไฟล์ไม่เจอ

- ไวรัสหลอกลวง (Polymorphic Virus) จะแพร่กระจายเชื้อไปตามไฟล์ต่าง ๆ แล้วแสดงผลหลอกเหมือนว่ามีไวรัสหลายตัวในเครื่อง เพื่อให้โปรแกรมป้องกันไวรัสตรวจจับได้ยาก

- ไวรัสสองหน้า (Multipartite Virus) สามารถติดเชื้อได้ทั้งโปรแกรมและบู๊ตเซ็กเตอร์ได้พร้อม ๆ กัน ถือเป็นไวรัสที่มีความสามารถสูง

- ไวรัสมาโคร (Macro Virus) ทำการแพร่กระจายเชื้อเฉพาะไฟล์ที่เป็นเอกสารเท่านั้น เพื่อทำให้ข้อมูลที่เก็บไว้ในไฟล์เกิดความเสียหายหรือเปลี่ยนแปลงไป

๑.๓ ความผิดพลาดของซอฟต์แวร์ (Bug)

ความผิดพลาดนั้นหมายถึง การทำงานในบางส่วนที่ไม่เป็นไปตามความต้องการหรือไม่ถูกต้อง

๑.๔ อุบัติภัย (Disaster)

อุบัติภัยประเภทไฟไหม้ แหล่งจ่ายไฟล้มเหลว หรือภัยพิบัติอื่น ๆ ย่อมเกิดความเสียหายอย่างหลีกเลี่ยงไม่ได้ ดังนั้น จึงควรวางมาตรการป้องกันอุบัติภัยให้กับระบบคอมพิวเตอร์เป็นอย่างดี

๑.๕ ความผิดพลาดในขั้นตอนการทำงานของระบบคอมพิวเตอร์

เนื่องจากระบบคอมพิวเตอร์มีโอกาสที่จะรับความเสียหายเข้ามาได้หลายทาง ตั้งแต่ส่วนการรับข้อมูลเข้ามาในระบบ เช่น การรับข้อมูลที่มีไวรัสคอมพิวเตอร์เข้ามา ส่วนของการทำงาน เช่น โปรแกรมทำงานในส่วนที่เกิด Bug พอดีหรือปัญหาจากฮาร์ดแวร์ ซึ่งความเสียหายของระบบเหล่านี้สามารถก่อความเสียหายให้กับหน่วยงานได้

๒ หลักการการรักษาความปลอดภัยข้อมูล

๒.๑ หลักสำคัญของการรักษาความปลอดภัยของข้อมูล คือ การปกป้องข้อมูล หรือสารสนเทศ ตามสภาพแวดล้อมของหน่วยงาน การสร้างความตระหนักรู้เกี่ยวกับความจำเป็น และความสำคัญในการ**รักษาความปลอดภัยของข้อมูล**การกำหนดความรับผิดชอบ และนโยบายสำหรับการ**รักษาความปลอดภัยของข้อมูล** ความต่อเนื่องในการให้บริการข้อมูล สารสนเทศ ระบบ และทรัพย์สินสารสนเทศ พร้อมทั้งประสิทธิผลของมาตรการควบคุม ทั้งมาตรการด้านบริหารจัดการ (Administrative security) มาตรการด้านเทคนิค (Technical security) และมาตรการทางกายภาพ (Physical security) ตอบสนองความต้องการของหน่วยงานและกลุ่มผู้มีส่วนได้เสีย และภายใต้การบริหารจัดการความเสี่ยงตามระดับความเสี่ยงที่ยอมรับได้ของหน่วยงาน โดยมีหลักการการรักษาความปลอดภัยข้อมูล ดังนี้

๒.๑.๑ การรักษาความลับ (Confidentiality) ข้อมูล สารสนเทศ เข้าถึงได้เฉพาะผู้ที่มีสิทธิ์ หรือได้รับอนุญาตเท่านั้น จะต้องไม่มีการเปิดเผยโดยมิชอบ หรือโดยบุคคลที่ไม่มีสิทธิ์ หรือไม่ได้รับอนุญาต มาตรการที่นำมาใช้ เช่น การกำหนดการเข้าถึงข้อมูล (Data/information classification) การตั้งค่ารหัสไฟล์/แฟ้มข้อมูล (Password)

๒.๑.๒ การรักษาความถูกต้องครบถ้วน (Integrity) ข้อมูล สารสนเทศ มีความถูกต้อง จะมีการแก้ไขเปลี่ยนแปลง ได้เฉพาะผู้ที่มีสิทธิ์หรือได้รับอนุญาตเท่านั้นมาตรการที่นำมาใช้ เช่น การจัดการสิทธิ์ (access rights)

๒.๑.๓ สภาพความพร้อมใช้ (Availability) ข้อมูล สารสนเทศ มีความพร้อมในการใช้งานอยู่เสมอ สามารถเข้าถึงได้เมื่อต้องการ เฉพาะผู้มีสิทธิ์ หรือได้รับอนุญาต มาตรการที่นำมาใช้ เช่น การควบคุมการเข้าถึง (Access control)

รูปที่ ๒๖ หลักการการรักษาความปลอดภัยของข้อมูล (*Principles of Information Security)*

นอกจากหลักการฯ ทั้ง ๓ ด้านแล้ว ยังมีหลักการอื่นที่เกี่ยวข้องกับด้านการรักษาความปลอดภัยข้อมูล ดังนี้

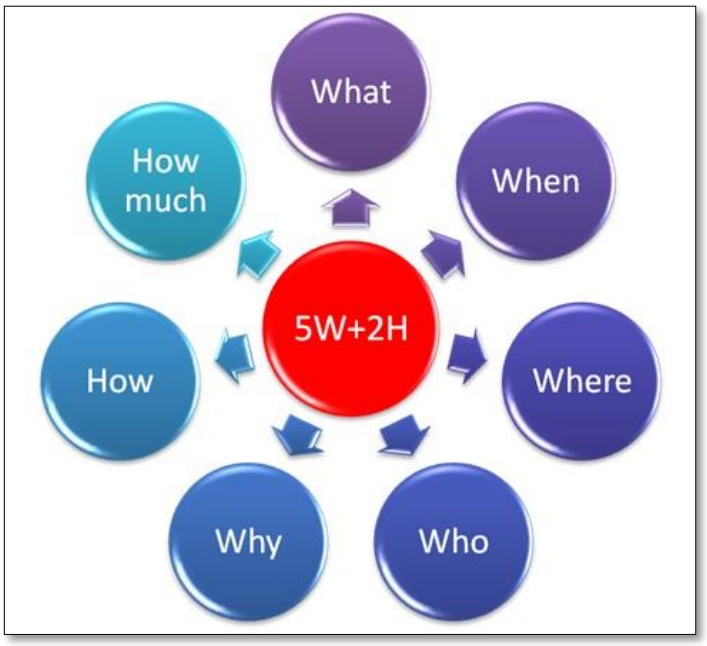
- การพิสูจน์ทราบตัวตน (Authentication) การพิสูจน์ทราบตัวตนเป็นการระบุตัวตน (Identification) ต้องสามารถระบุตัวตนของผู้ใช้งานของแต่ละคนที่ใช้งานข้อมูลได้การระบุตัวตนเป็นขั้นตอนแรกในการเข้าถึงข้อมูล หรือข้อมูลที่มีชั้นความลับ ในการเข้าถึงข้อมูล เช่น การใช้ Username Password, การนำรูปแบบไบโอเมตริกส์ (Biometrics) เช่น การประทับลายนิ้วมือ การตรวจจับม่านตา หรือเสียงพูด เป็นต้น

- การอนุญาตใช้งาน (Authorization) ภายหลังจากได้รับการ Authentication แล้ว ขั้นตอนต่อไป คือ การตรวจสอบสิทธิ์ของผู้ใช้งานนั้น ว่าได้มีการกำหนดสิทธิ์ให้เข้าข้อมูลได้ในระดับไหน ซึ่งสิทธินั้นประกอบด้วย การเข้าถึงหรืออ่าน การแก้ไข และการลบข้อมูล เพื่อป้องกันการนำข้อมูลไปใช้งานเกินสิทธิน้าที่รับผิดชอบ

- การตรวจสอบการใช้งาน (Accountability) มุ่งเน้นการเก็บข้อมูลรายละเอียดเหตุการณ์ที่เกิดขึ้นตามเวลา การเกี่ยวเนื่องของการดำเนินการต่าง ๆ เพื่อตรวจสอบเหตุการณ์หรือความเสียหายต่าง ๆ ที่เกิดขึ้นต่อข้อมูลในระบบสารสนเทศ จะต้องสามารถตรวจสอบได้ เพื่อตรวจสอบการทำงานของข้อมูลในระบบสารสนเทศว่าอยู่ในภาวะการให้บริการโดยปกติหรือไม่ ข้อมูลที่ได้รับความปลอดภัยนั้น จะต้องสามารถตรวจสอบได้ เมื่อเกิดเหตุการณ์ด้านการปลอดภัยข้อมูลขึ้น จะต้องสามารถตรวจพิสูจน์ได้ องค์ประกอบของ 5W2H

- Who ใคร คือ ต้องรู้ว่า ใครรับผิดชอบ ใครเกี่ยวข้อง ใครได้รับผลกระทบ ในเรื่องนั้นมีใครบ้าง
- What ทำอะไร คือ ต้องรู้ว่า เราจะทาอะไร แต่ละคนทำอะไรบ้าง
- Where ที่ไหน คือ ต้องรู้ว่า สถานที่ที่เราจะทาว่าจะทำที่ไหน เหตุการณ์หรือสิ่งที่ทานั้นอยู่ที่ไหน
- When เมื่อไหร่ คือ ต้องรู้ว่า ระยะเวลาที่จะทาจนถึงสิ้นสุด เหตุการณ์หรือสิ่งที่ทานั้นทำเมื่อวัน เดือน ปี ใด
- Why ทำไม คือ ต้องรู้ว่า สิ่งที่เราจะทำนั้น ทำด้วยเหตุผลใด เหตุใดจึงด้ทำสิ่งนั้น หรือเกิดเหตุการณ์นั้นๆ

- How อย่างไร คือ ต้องรู้ว่า เราจะสามารถทำทุกอย่างให้บรรลุผลได้อย่างไร เหตุการณ์หรือสิ่งที่ทำนั้นทำอย่างไรบ้าง
- How Much เท่าไร คือ การวิเคราะห์ค่าใช้จ่าย งบประมาณเท่าไหร่



รูปที่ ๒๗ องค์ประกอบของ 5W2H

- การไม่สามารถปฏิเสธการกระทำ (Non-Repudiation) วิธีการสื่อสารซึ่งผู้ส่งข้อมูลได้รับหลักฐานว่าได้มีการส่งข้อมูลแล้ว และผู้รับก็ได้รับการยืนยันว่าผู้ส่งเป็นใครดังนั้น เช่น ลายเซ็นอิเล็กทรอนิกส์ (Digital Signature), กุญแจสาธารณะ, (Public-Key Infrastructure) โดยประเทศไทยได้มีพระราชบญัญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.๒๕๔๔

- ความเป็นส่วนตัว (Privacy) ข้อมูลที่องค์กร รวบรวม จัดเก็บ และใช้งานนั้นควรถูกใช้ เพื่อจุดประสงค์ที่เจ้าของข้อมูลระบุตอนที่เก็บรวบรวม แต่ถ้าใช้เพื่อจุดประสงค์อื่นก็แสดงว่า เป็นการละเมิดสิทธิส่วนบุคคลของเจ้าของข้อมูลนั้น เช่น พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

– การห้ามปฏิเสธความรับผิดชอบ (Non-repudiation) การทำให้มั่นใจว่าผู้มีส่วนร่วม (parties) ที่เกี่ยวข้องในการทำธุรกรรมไม่สามารถปฏิเสธได้ ว่าไม่มีส่วนเกี่ยวข้องกับการทำธุรกรรมที่เกิดขึ้น การรักษาความปลอดภัยข้อมูลอย่างมีประสิทธิภาพ จำเป็นต้องมีข้อตกลงร่วมกัน (MOU) โดยประกอบด้วย

– การรักษาความปลอดภัยถือว่าเป็นหน้าที่ของบุคคลและบุคคลภายนอกทุกคน

– การบริหาร และการปฏิบัติในด้านการรักษาความปลอดภัยข้อมูลเป็นกระบวนการ ที่ต้องกระทำอย่างต่อเนื่องอยู่ตลอดเวลา

– การมีจิตสำนึก รู้จักหน้าที่ มีความรับผิดชอบ และใส่ใจที่จะกระทำตามข้อปฏิบัติที่กำหนดไว้ในนโยบาย มาตรฐาน กรอบการดำเนินงาน ขั้นตอนการปฏิบัติงาน คำแนะนำ และกระบวนการต่างๆ ถือเป็นสิ่งสำคัญที่สุดในกระบวนการรักษาความมั่นคงปลอดภัย การอธิบายให้พนักงานและบุคคลภายนอกทราบอย่างชัดเจนเพื่อให้มีความเข้าใจในหน้าที่และความรับผิดชอบในการรักษาความปลอดภัยที่ตนเองรับผิดชอบเป็นสิ่งที่จะทำให้การรักษาความมั่นคงปลอดภัยดำเนินไปอย่างมีประสิทธิผล

๒.๒ ลักษณะของภัยคุกคามทางไซเบอร์

ภัยคุกคามด้านความมั่นคงปลอดภัยไซเบอร์ หรือ ภัยคุกคามทางไซเบอร์ หมายถึง การกระทำหรือการดำเนินการใด ๆ โดยมิชอบโดยใช้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือโปรแกรมไม่พึงประสงค์ โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึง ทั้งนี้ ลักษณะของภัยคุกคามทางไซเบอร์ (อ้างอิงตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒) แบ่งออกเป็น ๓ ระดับ ดังนี้

๒.๒.๑ ภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง

ภัยคุกคามทางไซเบอร์ที่มีความเสี่ยงอย่างมีนัยสำคัญถึงระดับที่ทำให้ระบบคอมพิวเตอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศ (CII) หรือการให้บริการของรัฐด้อยประสิทธิภาพลง

๒.๒.๒ ภัยคุกคามทางไซเบอร์ในระดับร้ายแรง

ภัยคุกคามที่มีลักษณะการเพิ่มขึ้นอย่างมีนัยสำคัญของการโจมตีระบบคอมพิวเตอร์ หรือข้อมูลคอมพิวเตอร์ โดยมุ่งหมายเพื่อโจมตีโครงสร้างพื้นฐานสำคัญของประเทศ และการโจมตีดังกล่าวมีผลทำให้ระบบคอมพิวเตอร์หรือโครงสร้างสำคัญทางสารสนเทศที่เกี่ยวข้องกับการให้บริการของโครงสร้างพื้นฐานสำคัญของประเทศ ความมั่นคงของรัฐ ความสัมพันธ์ระหว่างประเทศ การป้องกันประเทศ เศรษฐกิจ การสาธารณสุข ความปลอดภัยสาธารณะ หรือความสงบเรียบร้อยของประชาชนเสียหาย จนไม่สามารถทำงาน หรือให้บริการได้

๒.๒.๓ ภัยคุกคามทางไซเบอร์ในระดับวิกฤติ

๒.๒.๓.๑ เป็นภัยคุกคามทางไซเบอร์ที่เกิดจากการโจมตีระบบคอมพิวเตอร์ คอมพิวเตอร์ข้อมูลคอมพิวเตอร์ในระดับที่สูงขึ้นกว่าภัยคุกคามทางไซเบอร์ในระดับร้ายแรง โดยส่งผลกระทบรุนแรงต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศในลักษณะที่เป็นวงกว้าง จนทำให้การทำงานของหน่วยงานรัฐหรือการให้บริการของโครงสร้างพื้นฐานสำคัญของประเทศที่ให้กับประชาชนล้มเหลวทั้งระบบ จนไม่สามารถควบคุมการทำงานส่วนกลางของระบบคอมพิวเตอร์ของได้

๒.๒.๓.๒ เป็นภัยคุกคามทางไซเบอร์อันกระทบ หรืออาจกระทบต่อความสงบเรียบร้อยของประชาชน หรือเป็นภัยต่อความมั่นคงของรัฐ หรืออาจทำให้ประเทศ หรือส่วนใดส่วนหนึ่งของประเทศตกอยู่ในภาวะคับขันหรือมีการกระทำความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา การรบ หรือการสงคราม ซึ่งจำเป็นต้องมีมาตรการเร่งด่วน เพื่อรักษาไว้ซึ่งการปกครองระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุขตามรัฐธรรมนูญแห่งราชอาณาจักรไทย เอกราชและบูรณภาพแห่งอาณาเขต ผลประโยชน์ของชาติ การปฏิบัติตามกฎหมาย ความปลอดภัยของประชาชน การดำรงชีวิตโดยปกติสุขของประชาชน การ

คุ้มครองสิทธิเสรีภาพ ความสงบเรียบร้อย หรือประโยชน์ส่วนรวม หรือการป้องปัด หรือแก้ไขเยียวยาความเสียหายจากภัยพิบัติสาธารณะอันมีมาอย่างฉุกเฉินและร้ายแรง

หมายเหตุ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ **(Critical information infrastructure: CII)** จะต้องมีการประเมิน และตรวจสอบว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้น หรือคาดว่าจะเกิดขึ้นหรือไม่ให้ดำเนินการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ตามประมวลแนวทางปฏิบัติ และกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน

๓. มาตรการในการรักษาความปลอดภัยของข้อมูล

ในยุคปัจจุบัน ข้อมูลข่าวสารไม่ได้อยู่เพียงในกระดาษหรือสื่อสิ่งพิมพ์แต่ยังมีการบันทึกไว้ในรูปแบบอื่นๆ ภายในระบบคอมพิวเตอร์ ซึ่งจะต้องมีวิธีการหรือมาตรการในการรักษาความปลอดภัยเช่นเดียวกัน

มาตรการในการรักษาความปลอดภัยสามารถแบ่งออกเป็น ๓ มาตรการใหญ่ คือ

๓.๑ มาตรการรักษาความปลอดภัยทางกายภาพ (Physical Security) เป็นมาตรการรักษาความปลอดภัยทั่วไปให้กับบุคคล สถานที่ และอุปกรณ์ ตลอดจนสื่อต่าง ๆ ที่บันทึกข้อมูลข่าวสาร เพื่อป้องกันไม่ให้ผู้บุกรุกเข้าถึงแหล่งข้อมูลได้ทางกายภาพ เช่น การสร้างรั้ว การเฝ้ายาม และการดำเนินงานด้านเอกสาร เป็นต้น ทั้งนี้รวมถึงการป้องกันการแพร่กระจายของคลื่นแม่เหล็กไฟฟ้าไม่ให้เล็ดลอดไปในสถานที่ที่ไม่เหมาะสม

๓.๒ มาตรการรักษาความปลอดภัยทางระบบคอมพิวเตอร์ (Computing Security) เป็นมาตรการรักษาความปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสารโดยตรง เน้นในการเข้าถึงและการใช้งานข้อมูลที่อยู่ในระบบสารสนเทศ ซึ่งจะต้องดำรงไว้ใน ๓ ลักษณะ คือ การรักษาความลับ (Confidential), การคงสภาพ (Integrity) และความพร้อมในการใช้งาน (Availability)

๓.๒.๑ การรักษาความลับ (Confidential) เป็นการดำเนินการเพื่อให้สาระของข้อมูลข่าวสารได้ถูกเปิดเผยต่อบุคคล หรือ process ที่ได้รับอนุญาตเท่านั้น มาตรการนี้จะทำได้โดยวิธีการเข้ารหัส (Cryptography)

๓.๒.๒ การคงสภาพ (Integrity) เป็นการยืนยันว่าข้อมูลที่ต้องการรักษาไม่ถูกเปลี่ยนแปลงไปจากของเดิมโดยผู้ที่ไม่ได้รับอนุญาต เนื่องจากในบางกรณีผู้บุกรุกไม่มีความประสงค์ที่จะรู้สาระของข้อมูลข่าวสาร แต่ต้องการทำให้ข่าวสารนั้นผิดไปจากสาระเดิม ซึ่งจะใช้การ Error Correction Code หรือ Integrity Check Sum เป็นต้น

๓.๒.๓ ความพร้อมในการใช้งาน (Availability) เป็นการรักษาความพร้อมในการใช้งานของข้อมูล เช่น ข้อมูลบัญชีเงินฝากของลูกค้าธนาคาร หรือข้อมูลสำคัญต่าง ๆ ที่ต้องพร้อมใช้งานในเวลาที่ต้องการ ซึ่งในบางครั้งเป็นข้อมูลที่สามารถเปิดเผยให้สาธารณชนรับทราบได้ เพื่อประโยชน์ในการประชาสัมพันธ์ หรือการเผยแพร่ในวงกว้าง เช่น ข้อมูลการท่องเที่ยว การแบ่งปันข้อมูล หรือการติดต่อแบบ Social Network เป็นต้น โดยใช้วิธีการ Back Up ต่าง ๆ หรือการทำ Redundant Array of Independent Disk : RIAD รวมทั้งการเตรียมที่ตั้งสำรองในยามฉุกเฉิน

๓.๓ มาตรการรักษาความปลอดภัยทางระเบียบกฎเกณฑ์ (Rule and Regulations) ในโลกแห่งความเป็นจริงแล้ว ไม่มีอุปกรณ์ หรือสิ่งกีดขวางใด ๆ จะสามารถรักษาความปลอดภัยของข้อมูลข่าวสารได้สมบูรณ์ หากไม่ได้ควบคุมการใช้งานของมนุษย์ การละเมิดในระบบรักษาความปลอดภัยนั้นส่วนมากจะมีคนใน

หน่วยงานมีส่วนเกี่ยวข้องโดยเสมอ ดังนั้นจึงขาดไม่ได้ที่จะต้องมีมาตรการทางด้านระเบียบกฎเกณฑ์มารองรับหรือควบคุม

การใช้งาน (Authentication) ของบุคลากรภายในหน่วยงาน ตลอดถึงการออกกฎหมาย (Law) ด้านการรักษาความปลอดภัยของประเทศ เพื่อป้องกันอาชญากรรมคอมพิวเตอร์ที่จะเกิดขึ้นในสังคมปัจจุบัน อีกทั้งต้องกำหนดให้มีการบันทึกการใช้งาน (Log) ของระบบสารสนเทศ เพื่อใช้ในการตรวจสอบ (Audit) และหาผู้ละเมิดมาลงโทษ

๔ การรักษาความปลอดภัยฐานข้อมูล (Database Security)

การรักษาความปลอดภัยฐานข้อมูล มีความมุ่งหมาย เพื่อกำหนดมาตรการป้องกันฐานข้อมูลจากการเข้าถึงการเปลี่ยนแปลง การโอนถ่ายข้อมูล หรือการกระทำใด ๆ โดยผู้ไม่เกี่ยวข้อง ตลอดจนการเตรียมระบบสำรองและการฟื้นฟูระบบ

๔.๑ ข้อมูล ข่าวสาร สารสนเทศทุกประเภท ในฐานข้อมูลต้องได้รับการจัดระดับการป้องกันผู้มีสิทธิเข้าใช้หรือดำเนินการ รวมทั้งรายละเอียดอื่น ๆ ที่จำเป็นต่อมาตรการรักษาความปลอดภัยและหากเป็นข้อมูลที่มีชั้นความลับ ต้องมีการเข้ารหัสในการจัดเก็บที่เหมาะสม โดยใช้รูปแบบการเข้ารหัสตามมาตรฐานที่กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศกำหนด

๔.๒ ส่วนราชการเจ้าของฐานข้อมูล ผู้มีสิทธิและอำนาจในสายงาน เป็นผู้พิจารณาคุณสมบัติของผู้ใช้และโปรแกรมที่ได้รับอนุญาตให้กระทำการใด ๆ กับข้อมูลนั้นได้ตามสิทธิและจัดให้มีแฟ้มลงบันทึกเข้าออกและการใช้งาน (Audit Log) การใช้งานสำหรับฐานข้อมูลตามความจำเป็น เพื่อประโยชน์ในการตรวจสอบความถูกต้องของการใช้งานฐานข้อมูล

๔.๓ ในกรณีฐานข้อมูลที่มีการใช้ร่วมกันระหว่างราชการให้จัดทำข้อตกลงการใช้

๔.๔ ต้องมีการจัดทำแผนสำรองและกู้ข้อมูลที่เหมาะสม และหากเป็นข้อมูลเกี่ยวกับงานด้านยุทธการต้องมีการสำรองข้อมูลอย่างน้อย ๒ ชุด โดยเก็บไว้ในพื้นที่ปฏิบัติงาน ๑ ชุด และเก็บไว้ห่างจากจุดที่มีการติดตั้งใช้อีก ๑ ชุด สำหรับระบบอื่น ๆ ให้กำหนดตามความเหมาะสม

๕. การเข้ารหัสข้อมูล

๕.๑ การรักษาความปลอดภัยข้อมูลเครือข่ายไร้สาย

หากมีการใช้เครือข่ายไร้สายทั้งในด้านยุทธการ และธุรการต้องมีการป้องกันทั้งการพิสูจน์ทราบและการเข้ารหัส โดยต้องมีการขึ้นทะเบียนอุปกรณ์ (WiFi Access Point) เพื่อตรวจสอบและยืนยันความปลอดภัยจากกรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศเพื่อป้องกันการลักลอบใช้งานจากผู้ที่ไม่ได้รับอนุญาต ทำให้ความลับทางราชการรั่วไหล

๕.๒ วิธีการป้องกันภัยจากการใช้งานระบบเครือข่ายไร้สาย

หลักการในการใช้ระบบเครือข่ายไร้สายให้สะดวกและปลอดภัย

๕.๒.๑ ต้องมีการเข้ารหัสข้อมูล เช่น WEP, WPA, WPA version 2

๕.๒.๒ ต้องรีบเปลี่ยนรหัส (Default Password) ที่มากับอุปกรณ์ทั้งหมดให้เป็นของตนเองและต้องเก็บเป็นความลับ

๕.๒.๓ กำหนดระดับความแรงสัญญาณให้เหมาะสมกับพื้นที่ ๆ เปิดใช้งาน

๕.๒.๔ การแชร์ข้อมูลต้องมีการใช้รหัสผ่านเพื่อเข้าถึงข้อมูล

๕.๓ ระบบเข้าระหัส WEP กับ WPA

การเข้ารหัสข้อมูลมีอยู่ด้วยกันหลากหลายรูปแบบ เพื่อเพิ่มความปลอดภัยและความเหมาะสมในการใช้งาน โดยจะขอย่อ ๆ อธิบายดังนี้

๕.๓.๑ WEP คือ ใช้หลักการเข้ารหสและถอดรหัสแบบ Symmetrical key มีความยาว 64 หรือ 128 บิต อย่างไรก็ตามกลไกการเข้ารหัสแบบ WEP นี้มีช่องโหว่อยู่มาก เพราะรหัสที่ใช้สามารถถูกถอดรหัสได้จากผู้ใช้งานโดยตรง นอกจากนี้ key ที่ใช้ในการเข้ารหัสก็ไม่มีการเปลี่ยนแปลงตลอดการใช้งาน

๕.๓.๒ WPA (Wi-Fi Protected Access) คือ รูปแบบการเข้ารหัสที่มีความปลอดภัยสูงกว่าแบบ WEP เพราะใช้กลไกการเข้ารหัสและถอดรหัสแบบ TKIP (Temporal Key Integrity) ซึ่งเป็น key ชั่วคราวที่จะเปลี่ยนอยู่เรื่อย ๆ ร่วมกับ MIC (Message Integrity Code) เพื่อทำให้แน่ใจว่าข้อมูลที่อยู่ระหว่างการสื่อสารจะไม่ถูกปลอมแปลงจากผู้บุกรุก ทำให้ยากแก่การคาดเดาถอดรหัส

๕.๓.๓ WPA2 คือ การรักษาความปลอดภัยระดับสูงสุดในปัจจุบันที่ถูกพัฒนาขึ้นโดยใช้กลไกการเข้ารหัสและถอดรหัสแบบ AES (Advanced Encryption Standard)

ระบบป้องกันมีหลายแบบดังที่กล่าวมาข้างต้น แต่ปัจจุบันแนะนำให้ใช้ WPA version 2 with AES (Advance Encryption Standard) ซึ่งเป็นระบบที่มีประสิทธิภาพมากที่สุด

นอกจากเทคนิคที่กล่าวมาข้างต้นนี้แล้ว ปัจจุบันยังมีวิธีการรักษาความปลอดภัยของระบบเครือข่ายไร้สายอีกหลายวิธีด้วยกัน ซึ่งจะต้องเลือกวิธีการให้เหมาะกับลักษณะและงบประมาณของหน่วยงานของตนเองเพื่อให้เกิดประโยชน์และความคุ้มค่าสูงสุด

๕.๔ ข้อปฏิบัติและดำเนินการของผู้ได้รับอนุญาตให้เข้าถึงระบบสารสนเทศ

๕.๔.๑ ดำเนินการใด ๆ กับข้อมูลเฉพาะที่ได้รับอนุญาตแล้วเท่านั้นและต้องปฏิบัติตามระเบียบว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศอย่างเคร่งครัด

๕.๔.๒ ใช้ระบบสารสนเทศอย่างระมัดระวัง ถูกต้องตามกระบวนการรักษาความปลอดภัย และใช้ในกิจการงานที่ได้รับอนุญาต หรือได้รับมอบหมายเท่านั้น

๕.๔.๓ ตรวจสอบโปรแกรมประสงค์ร้ายก่อนนำมาใช้งานในระบบ

๕.๔.๔ ไม่นำโปรแกรมที่ไม่ได้รับอนุญาตหรือไม่เกี่ยวข้องกับภารกิจหน้าที่ ที่ได้รับมอบหมายเข้าสู่ระบบสารสนเทศ

๕.๔.๕ เก็บรักษาและใช้งานบัญชีผู้ใช้ (User Account) ซึ่งประกอบด้วยชื่อผู้ใช้ (user name) และรหัสผ่าน (Password) ให้เหมาะสม และเก็บรักษารหัสผ่าน (Password) ให้เป็นไปด้วยความปลอดภัยไม่รั่วไหลถึงบุคคลอื่น

๕.๕ ข้อกำหนดขั้นต่ำของการกำหนดรหัสผ่าน (Password) ที่เหมาะสม

๕.๕.๑ มีความยาวอย่างน้อย ๘ ตัวอักษร

๕.๕.๒ ประกอบไปด้วยตัวอักษรพิมพ์เล็ก พิมพ์ใหญ่ ตัวเลขและอักขระพิเศษ

๕.๕.๓ จะต้องไม่มีข้อมูลเกี่ยวกับผู้ใช้ เช่น วันเกิด ชื่อเล่น หมายเลขโทรศัพท์จดจำรหัสผ่านแทนการเขียนบันทึก หากเจ้าของรหัสผ่านลืมรหัสผ่าน หรือต้องการแก้ไขให้เจ้าของรหัสผ่านแจ้งผู้ดูแลระบบให้ดำเนินการ

๕.๕.๔ ต้องเปลี่ยนรหัสผ่านตามช่วงเวลาที่กำหนด หรือตามความเหมาะสม สำหรับระบบที่มีความสำคัญ

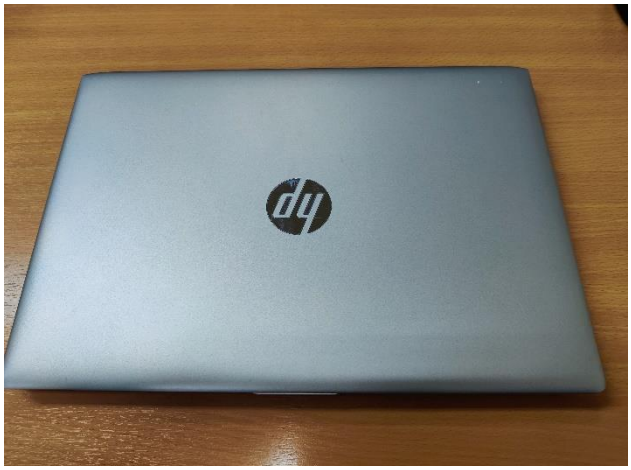
๕.๕.๕ ความรับผิดชอบในการใช้งาน Username และ Password เป็นของเจ้าของผู้ใช้งานต้องไม่โอนสิทธิหรือยินยอมให้ผู้อื่นใช้รหัสผ่านของตน ต้องไม่เปิดเผยรหัสผ่านให้แก่ผู้ใดทั้งสิ้น รวมถึงผู้ดูแลระบบสารสนเทศ

บทที่ ๖
การฝึกปฏิบัติด้านการรักษาความปลอดภัยระบบสารสนเทศ

๑. การตรวจสอบระบบเครือข่ายทางสาย (LAN)

ตรวจการแชร์ข้อมูล โดยใช้โปรแกรม network scanner ค้นหาหมายเลข ip address ที่ต้องการค้นหา หรือจากการแจกจ่าย ip

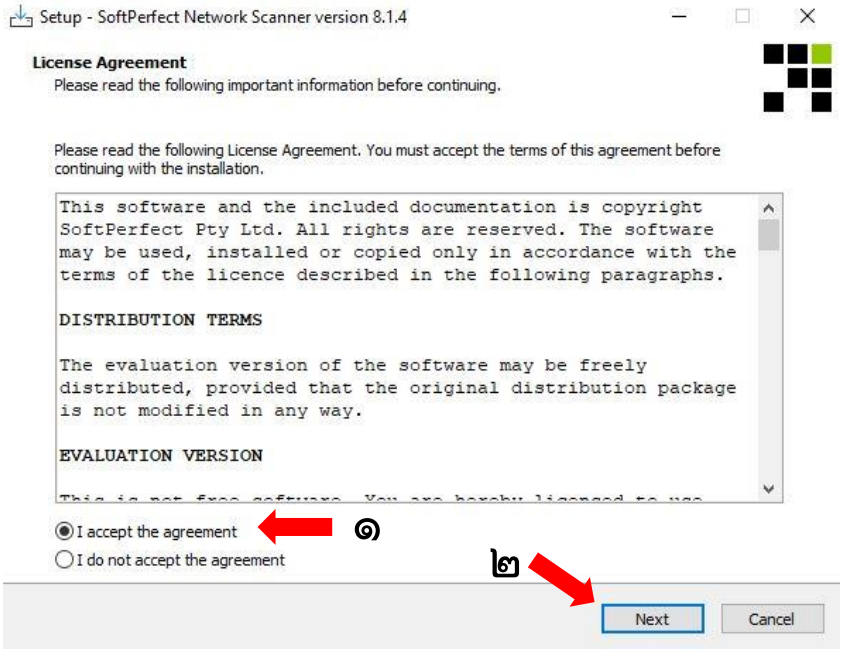
๑.๑ อุปกรณ์ที่ใช้ในการตรวจ



รูปที่ ๒๘ คอมพิวเตอร์โน้ตบุค

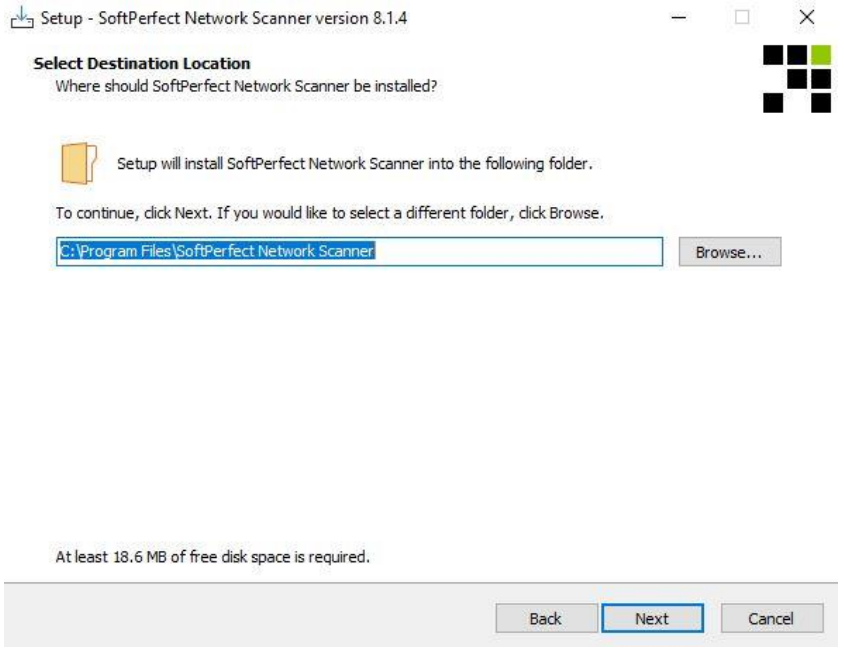
๑.๒ ขั้นตอนการติดตั้งโปรแกรม

๑.๒.๑ คลิ๊กที่หมายเลข ๑ ตามด้วยหมายเลข ๒



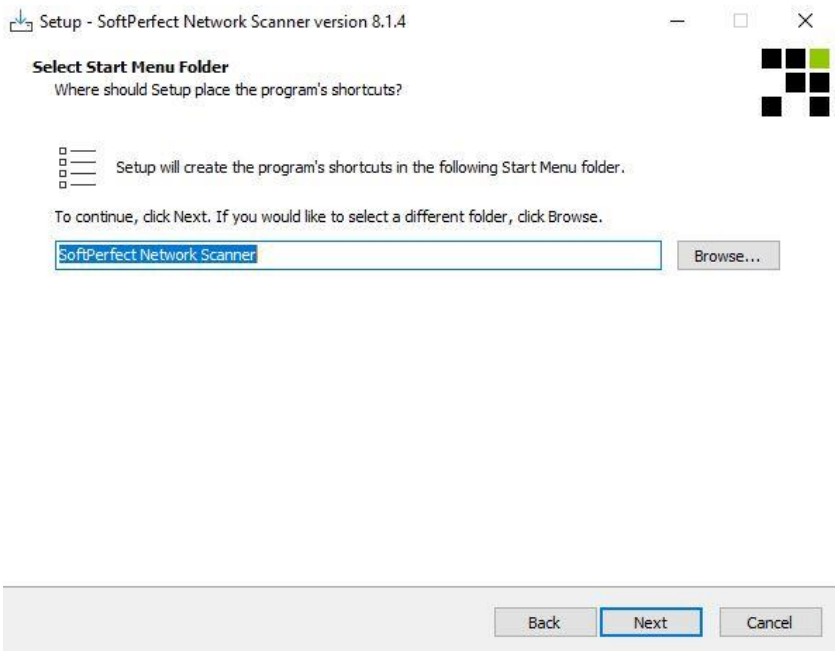
รูปที่ ๒๙ การติดตั้งโปรแกรม ขั้นตอนที่ ๑

๑.๒.๒ กด Next



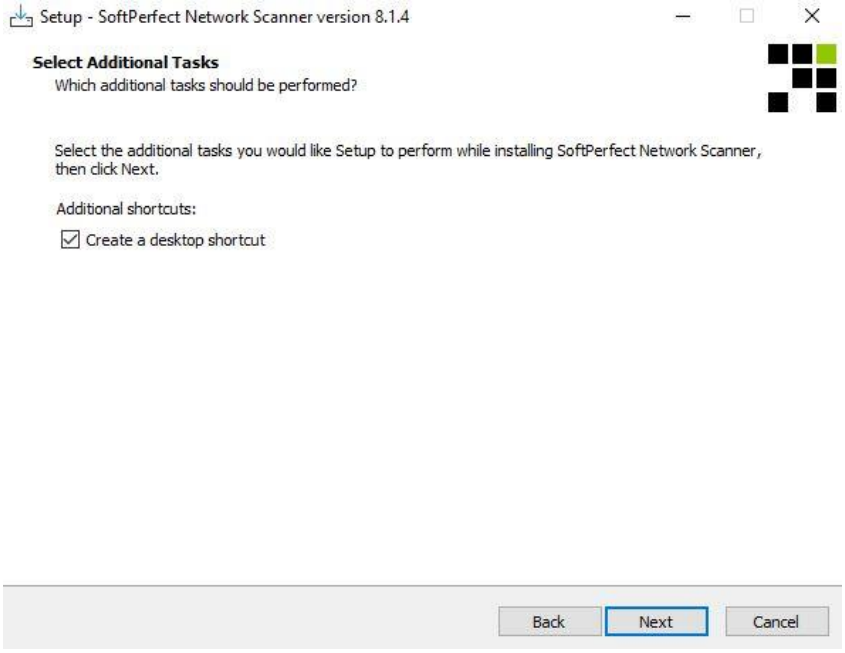
รูปที่ ๓๐ การติดตั้งโปรแกรม ขั้นตอนที่ ๒

๑.๒.๓ กด Next



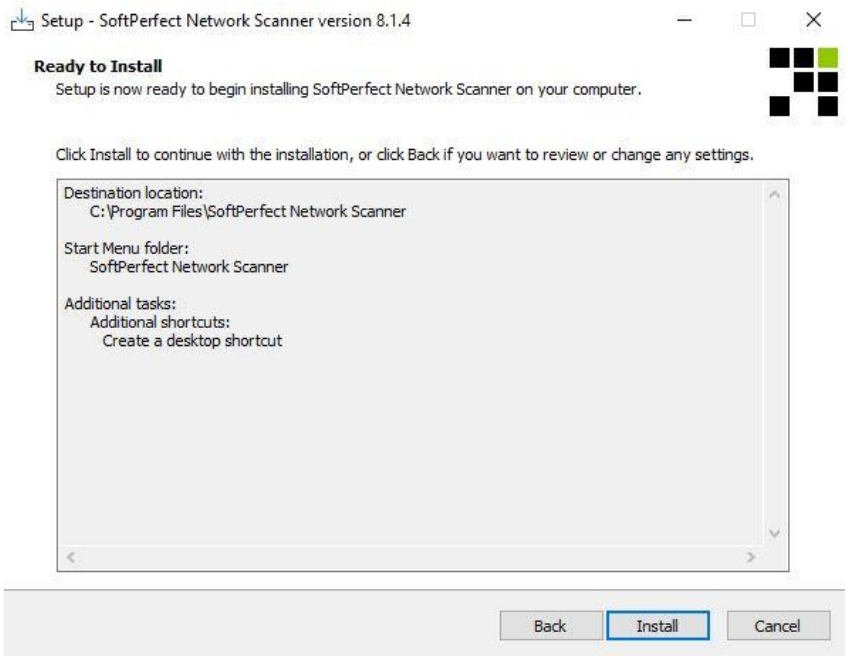
รูปที่ ๓๑ การติดตั้งโปรแกรม ขั้นตอนที่ ๓

๑.๒.๔ กด Next



รูปที่ ๓๒ การติดตั้งโปรแกรม ขั้นตอนที่ ๔

๑.๒.๕ กด Install



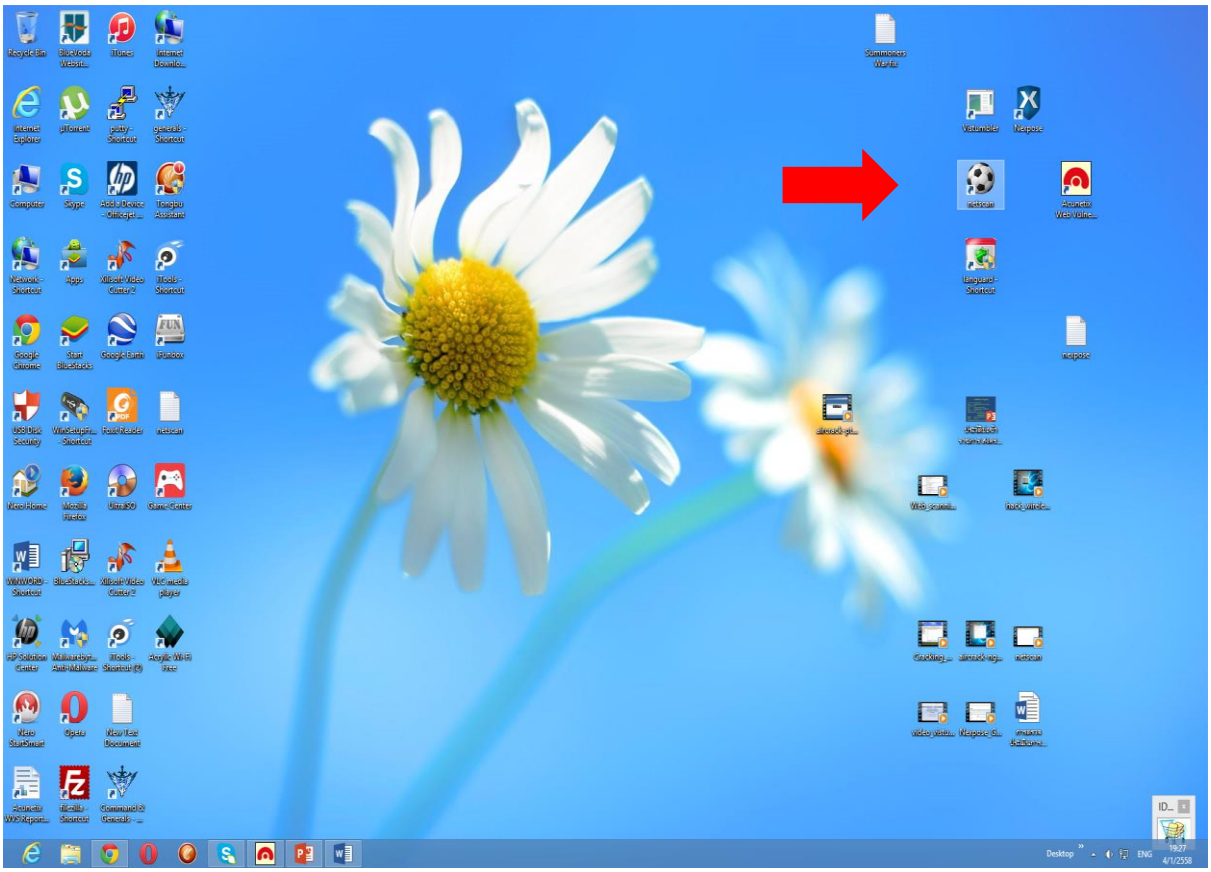
รูปที่ ๓๓ การติดตั้งโปรแกรม ขั้นตอนที่ ๕

๑.๒.๖ กด Finish

รูปที่ ๓๔ การติดตั้งโปรแกรม ขั้นตอนที่ ๖

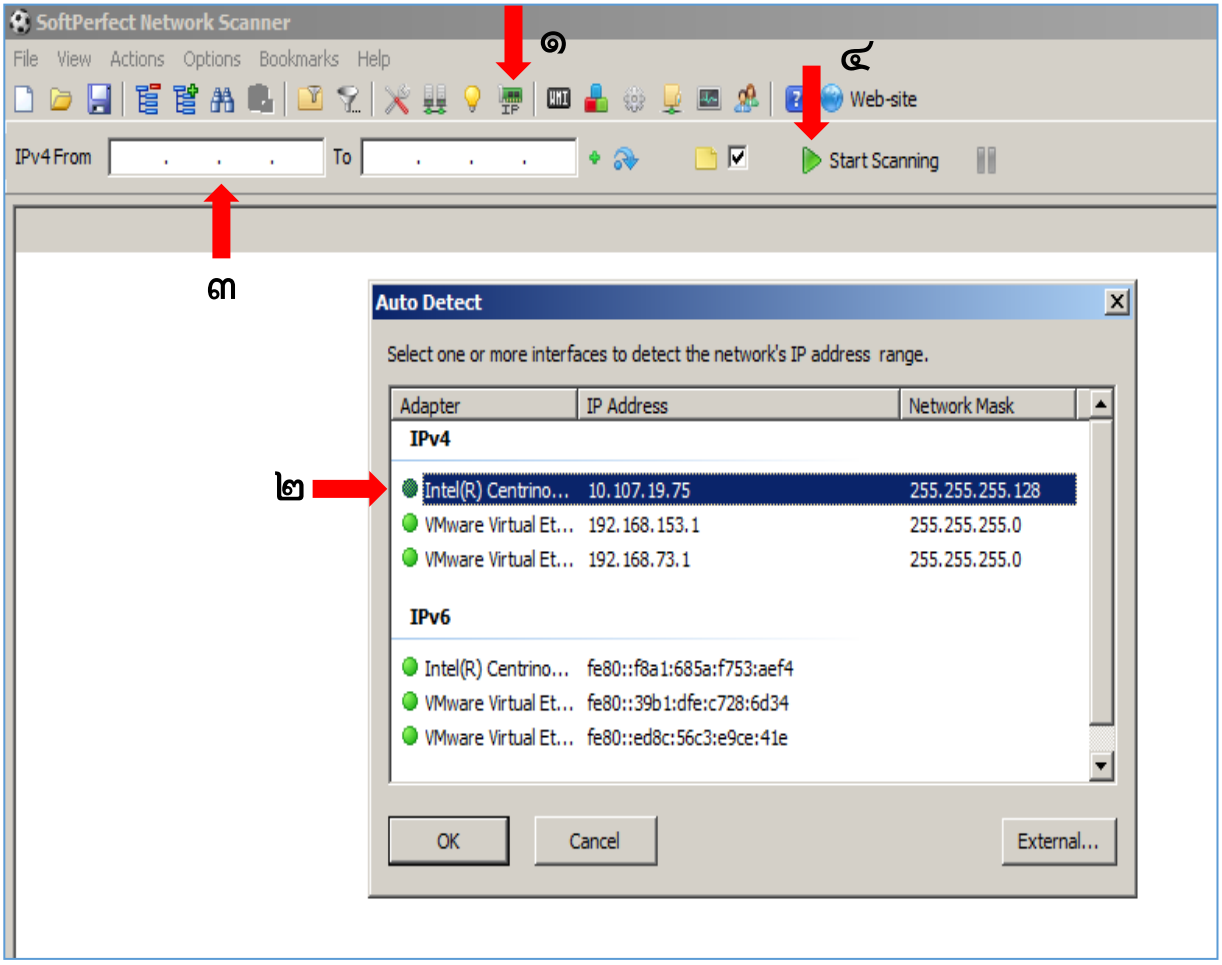
๑.๓ การตรวจสอบระบบเครือข่ายทางสาย (LAN)

๑.๓.๑ ดับเบิ้ลคลิกที่ netscan



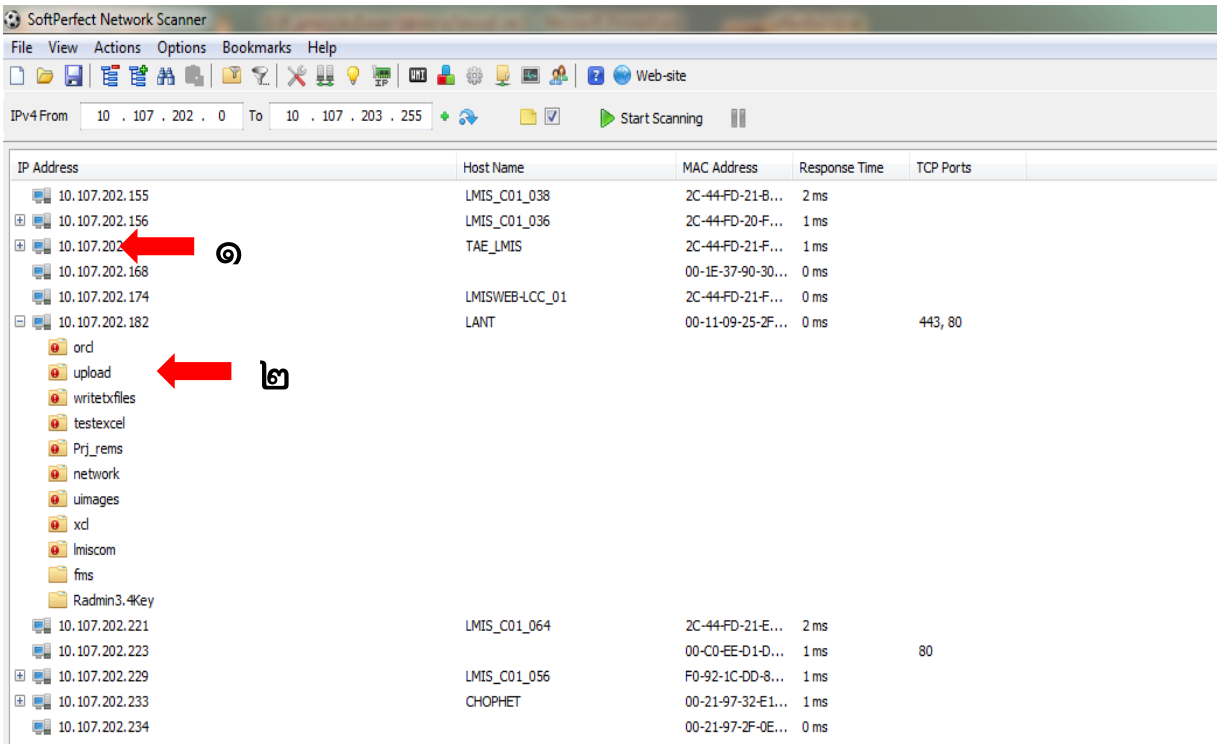
รูปที่ ๓๕ การตรวจสอบระบบเครือข่ายทางสาย (LAN) ขั้นตอนที่ ๑

๑.๓.๒ หลังจากเปิดโปรแกรมขึ้นมาแล้วให้คลิ๊กที่หมายเลย ๑ แล้วตามด้วยหมายเลข ๒ เพื่อเลือกเครือข่าย (ip) ที่ต้องการใช้งาน แต่ถ้าทราบแล้วให้กรอกตามหมายเลข ip ที่หมายเลข ๓ ได้เลย หลังจากนั้นให้กดเริ่มตามหมายเลข ๔ start scanning



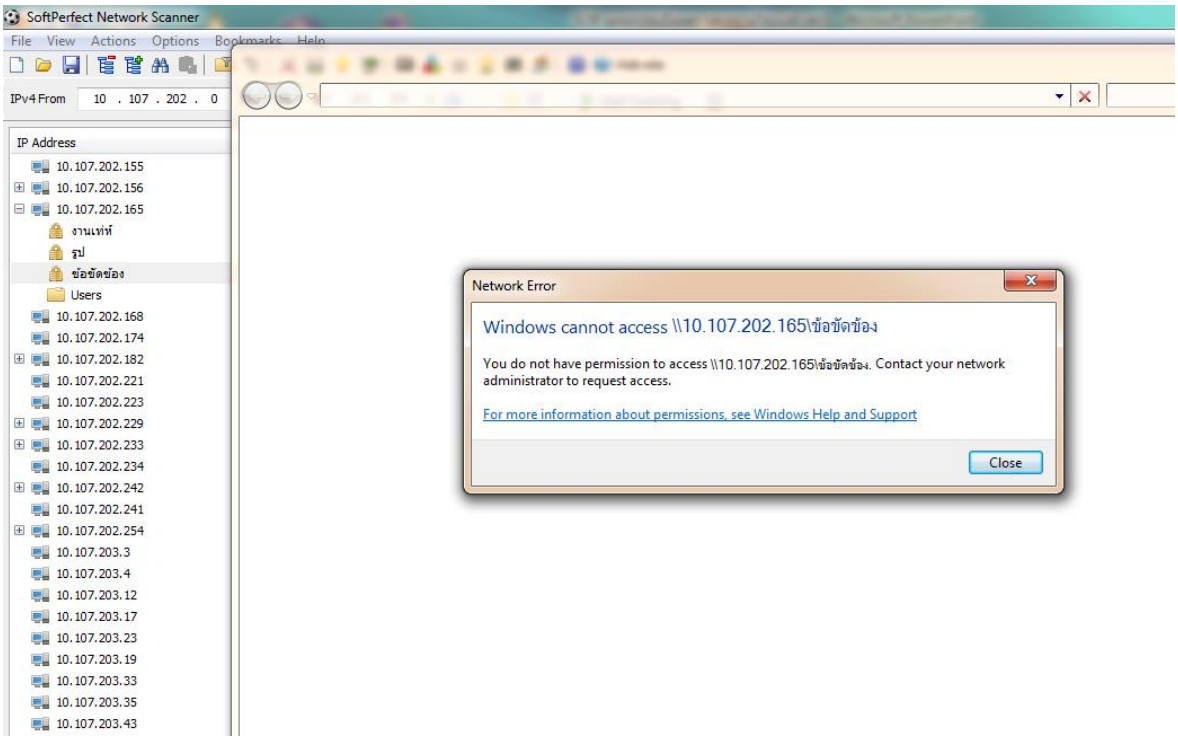
รูปที่ ๓๖ การตรวจสอบระบบเครือข่ายทางสาย (LAN) ขั้นตอนที่ ๒

๑.๓.๓ ผลการสแกนเครื่องที่อยู่ในชุดหมายเลข ip โดยที่จะสามารถค้นหาเครื่องคอมพิวเตอร์ที่ได้มีการเปิดการ share file โดยคลิ๊กที่เครื่องหมาย+หน้า ip ว่าแชร์ข้อมูลหรืออุปกรณ์อะไรบ้าง (๑) โฟลเดอร์แชร์ที่มีเครื่องหมายสีแดง สามารถเขียน ลบ แก้ไขเปลี่ยนแปลงข้อมูลได้ (๒)



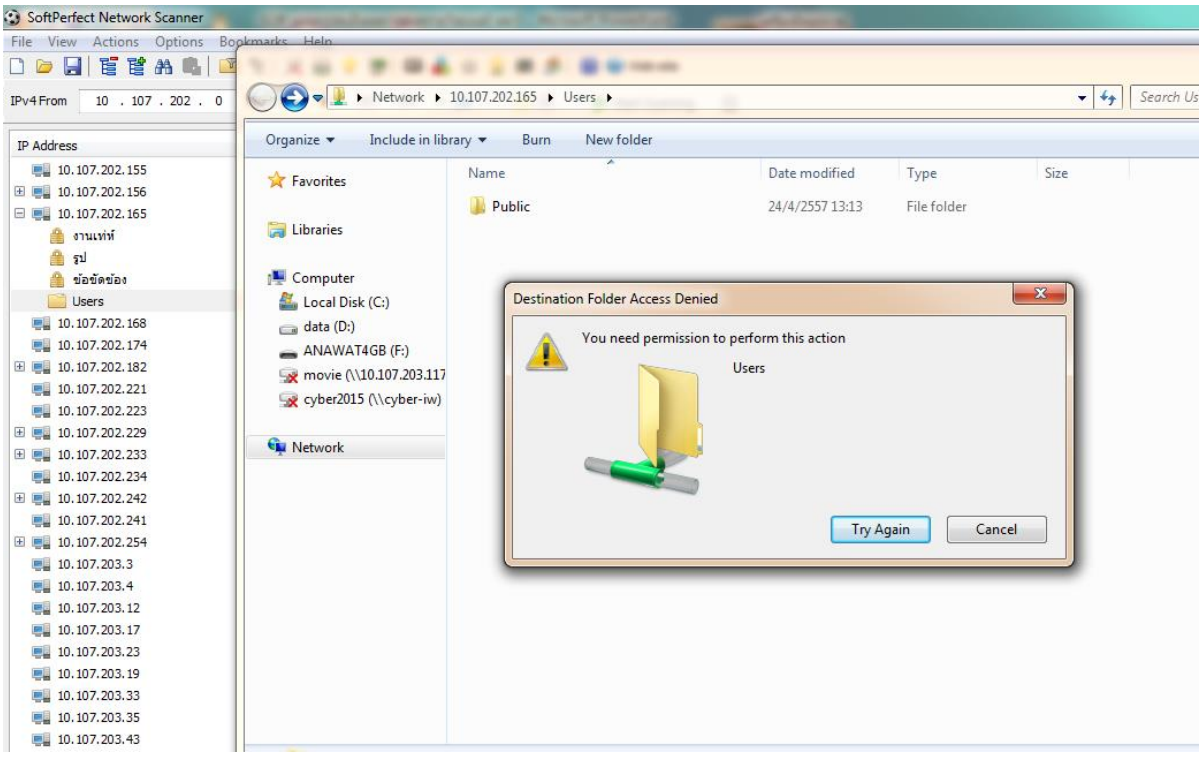
รูปที่ ๓๗ การตรวจสอบระบบเครือข่ายทางสาย (LAN) ขั้นตอนที่ ๓

๑.๓.๔ แชร์ไว้ แต่ได้กำหนดสิทธิการเข้าถึง จะมีรูปเครื่องหมายกุญแจ ดังรูป



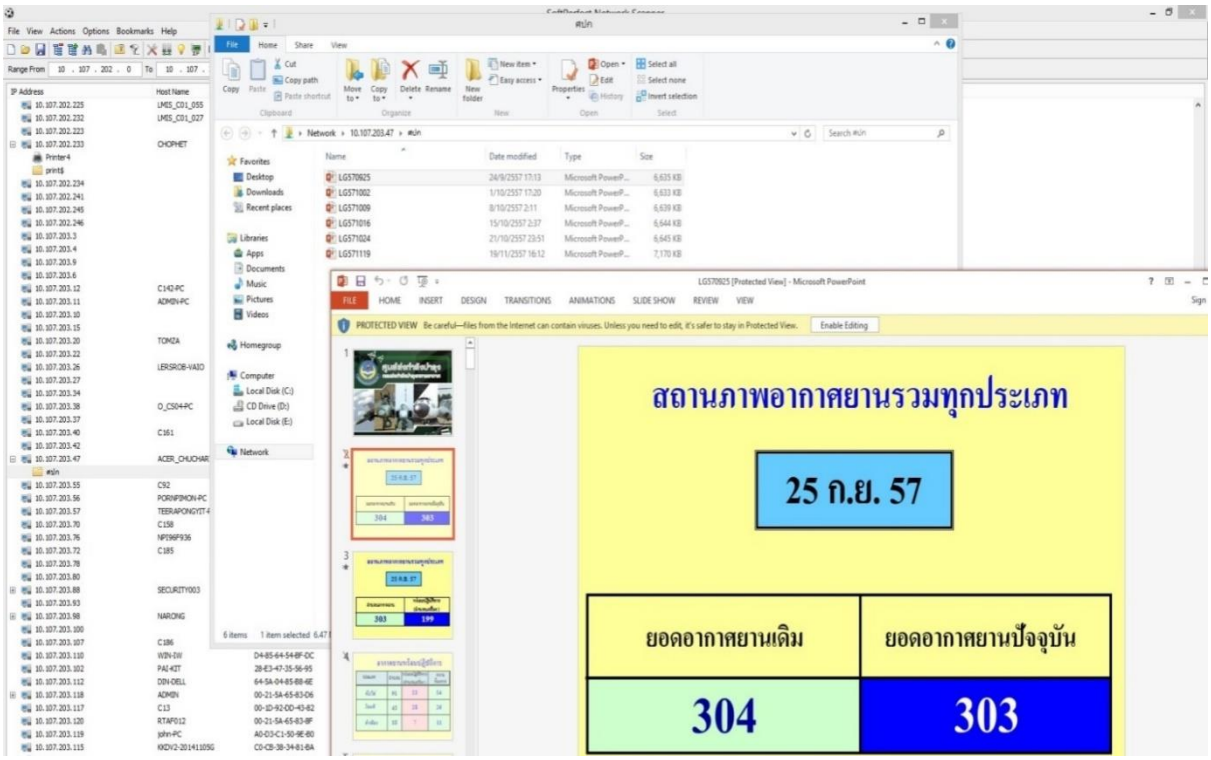
รูปที่ ๓๘ การตรวจสอบระบบเครือข่ายทางสาย (LAN) ขั้นตอนที่ ๔

๑.๓.๕ แชร์ธรรมดา สามารถอ่านได้อย่างเดียว



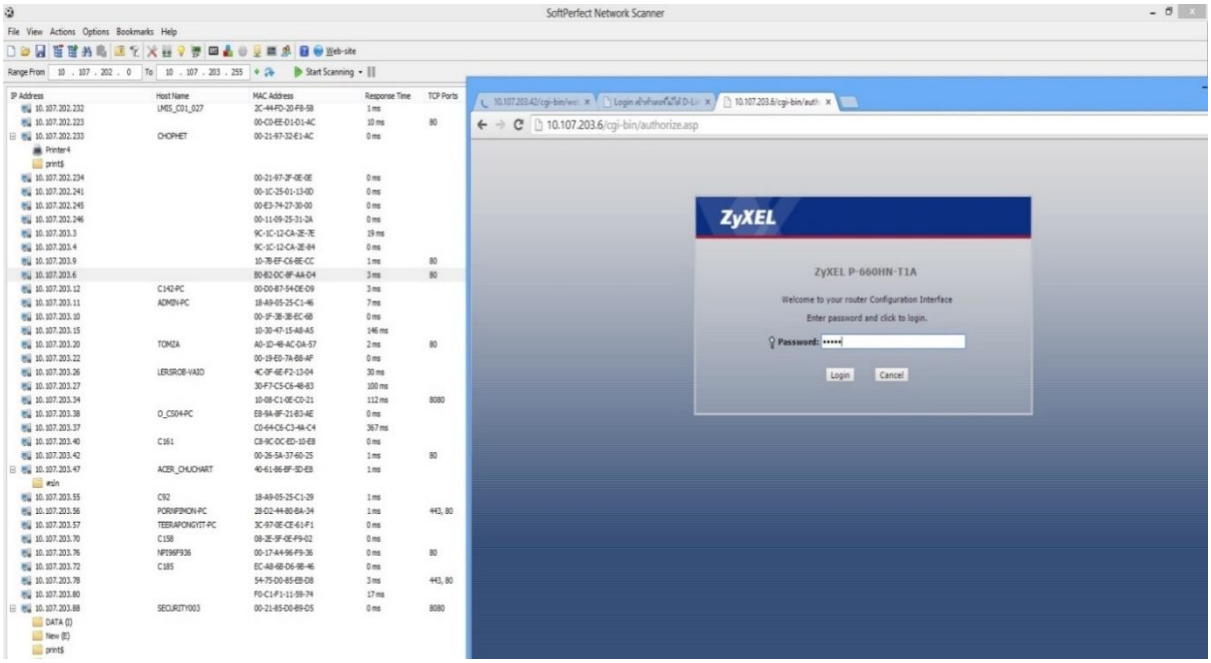
รูปที่ ๓๙ การตรวจสอบระบบเครือข่ายทางสาย (LAN) ขั้นตอนที่ ๕

๑.๓.๖ คลิ๊กเข้าไป จะเห็นไฟล์ภายใน สามารถเปิดมาดูได้ และ save เก็บเข้าไปยัง hard disk ของเราได้



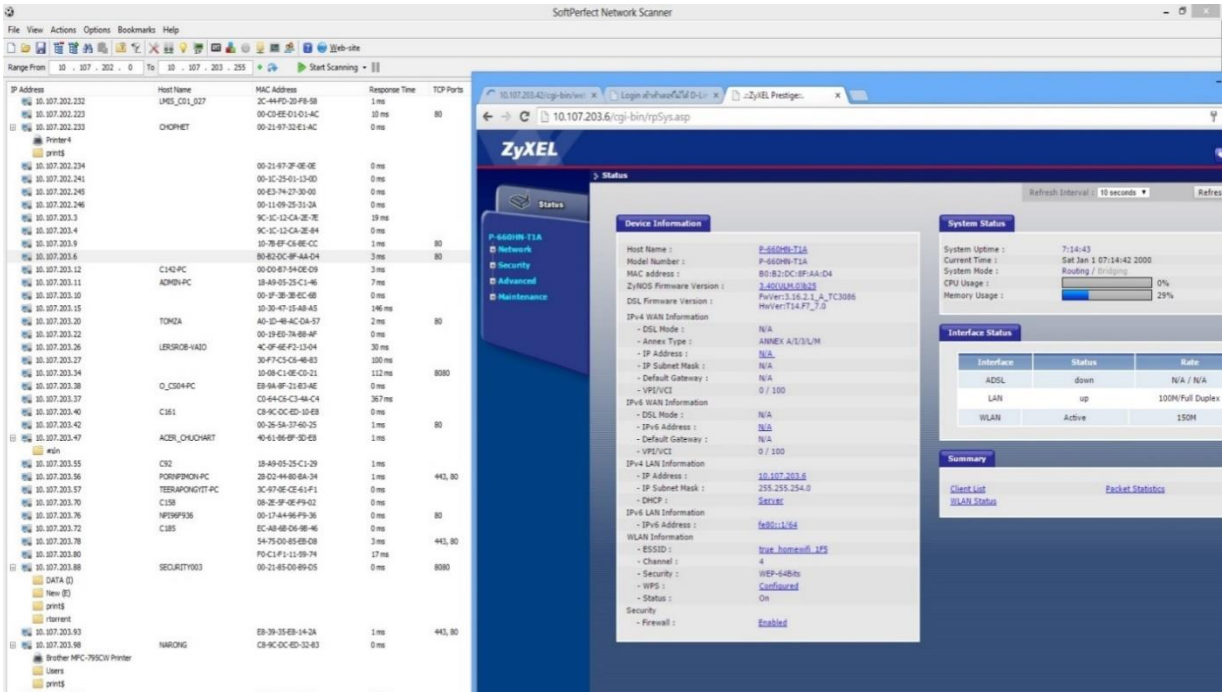
รูปที่ ๔๐ การตรวจสอบระบบเครือข่ายทางสาย (LAN) ขั้นตอนที่ ๖

๑.๓.๗ จากรูปเราสามารถเห็นการเปิดการให้บริการรูปแบบอื่น ๆ (port) ทำให้สามารถรู้ service ที่เปิด และสามารถเข้าไปดูได้



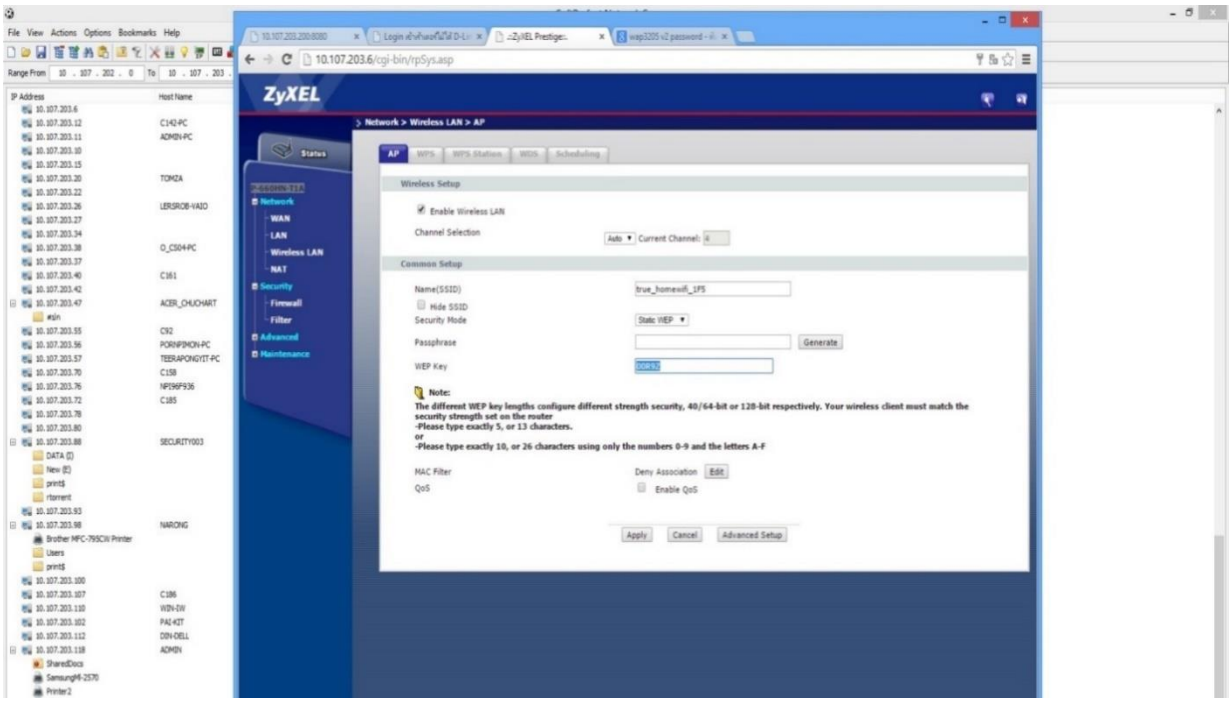
รูปที่ ๔๑ การตรวจสอบระบบเครือข่ายทางสาย (LAN) ขั้นตอนที่ ๗

๑.๓.๘ สามารถแก้ไขค่าสิทธิต่าง ๆ ได้



รูปที่ ๔๒ การตรวจสอบระบบเครือข่ายทางสาย (LAN) ขั้นตอนที่ ๘

๑.๓.๙ เข้าไปดูรายละเอียด อาทิเช่นเห็นรหัสการเข้าใช้งานอุปกรณ์พร้อมชื่อ SSID : Service Set Identifier (ชื่อของ Wireless Lan)



รูปที่ ๔๓ การตรวจสอบระบบเครือข่ายทางสาย (LAN) ขั้นตอนที่ ๙

๒ ตรวจสอบเครือข่ายไร้สาย

ตรวจสอบจุดที่ตั้งของอุปกรณ์ด้วยวิธีการ war driving โดยใช้โปรแกรม vistumbler พร้อมกับใช้อุปกรณ์บอกพิกัด หรือที่เราเรียกว่า GPS

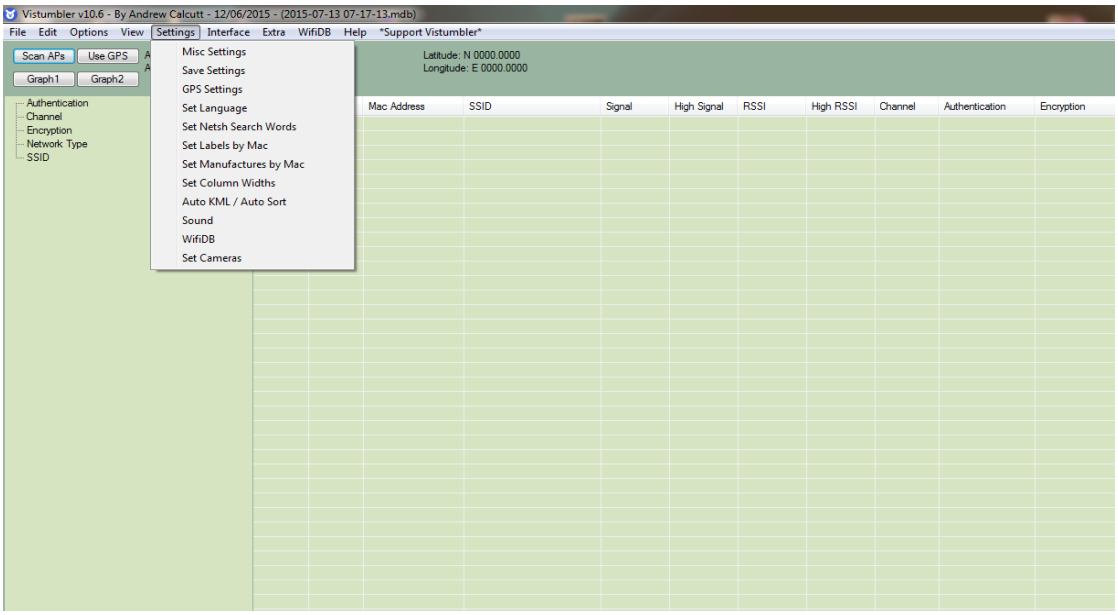
๒.๑ อุปกรณ์ที่ใช้ในการตรวจ

รูปที่ ๔๔ คอมพิวเตอร์โน้ตบุค

รูปที่ ๔๕ อุปกรณ์ระบุพิกัด (GPS)

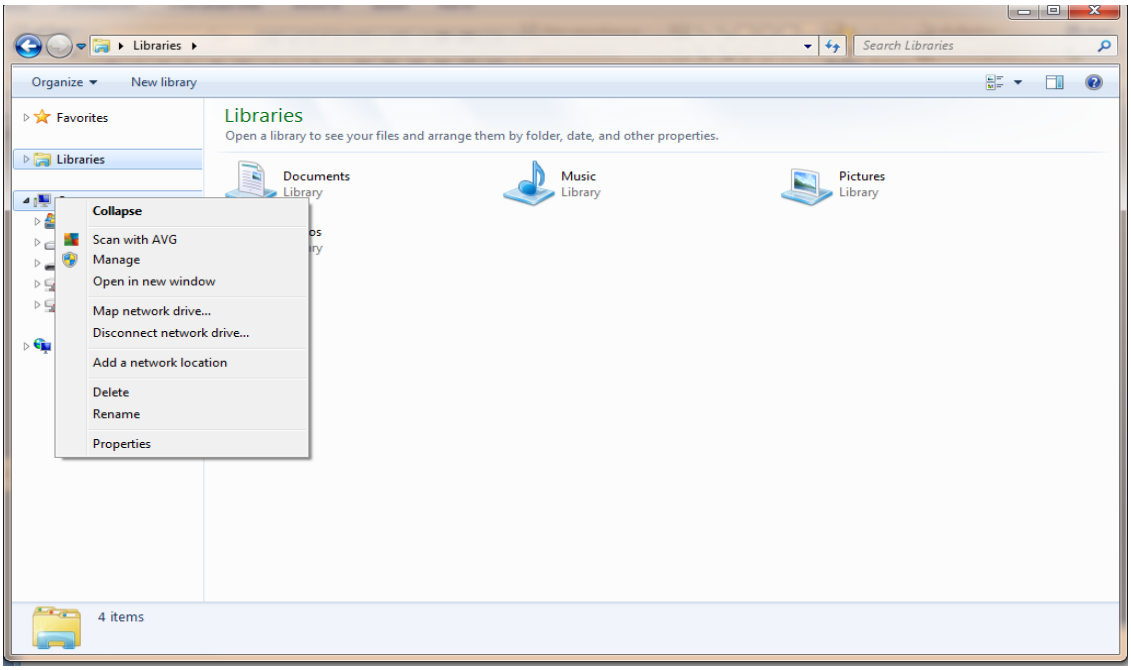
๒.๒ ตรวจสอบระบบไร้สายด้วย Vistumbler

๒.๒.๑ เสียบ usb GPS แล้วเปิดโปรแกรม vistumbler แล้วจะพบหน้าต่าง เลือกการตั้งค่า gps ก่อนการใช้งาน



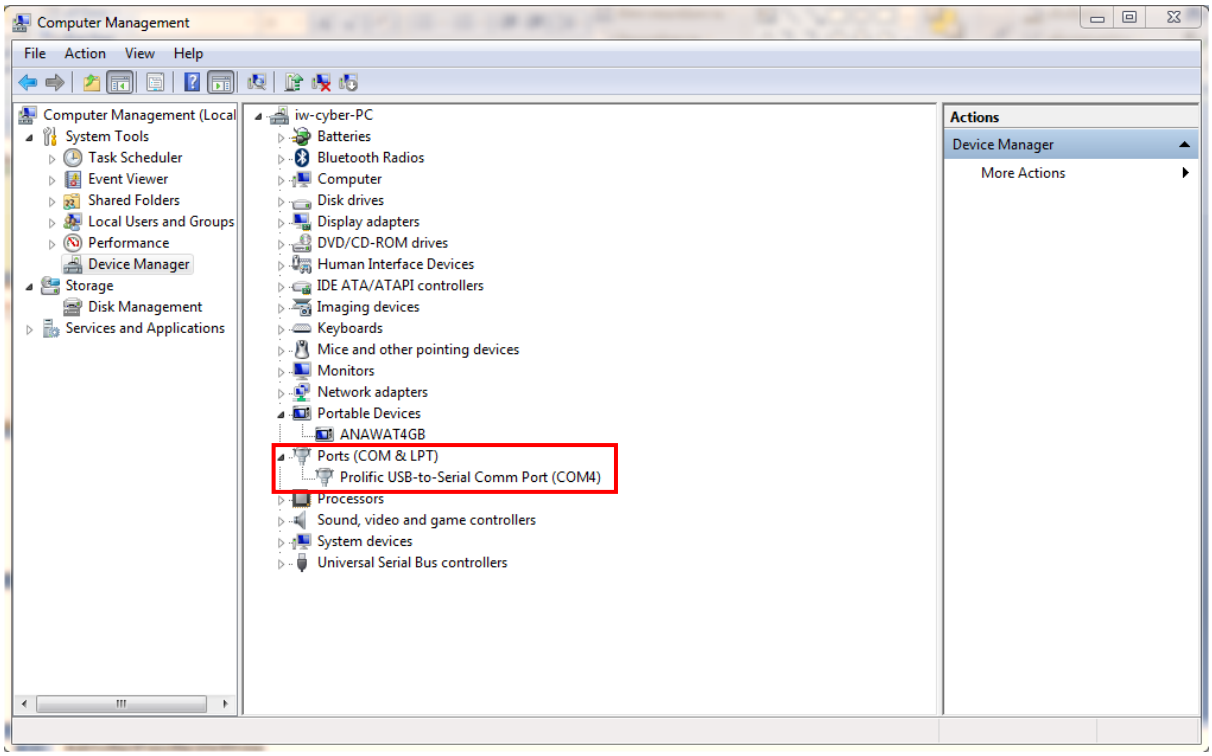
รูปที่ ๔๖ ตรวจสอบระบบไร้สายด้วย Vistumbler ขั้นตอนที่ ๑

๒.๒.๒ หาค่าพอร์ต GPS ได้จาก windows explorer คลิ๊กขวาที่ computer เลือก manage



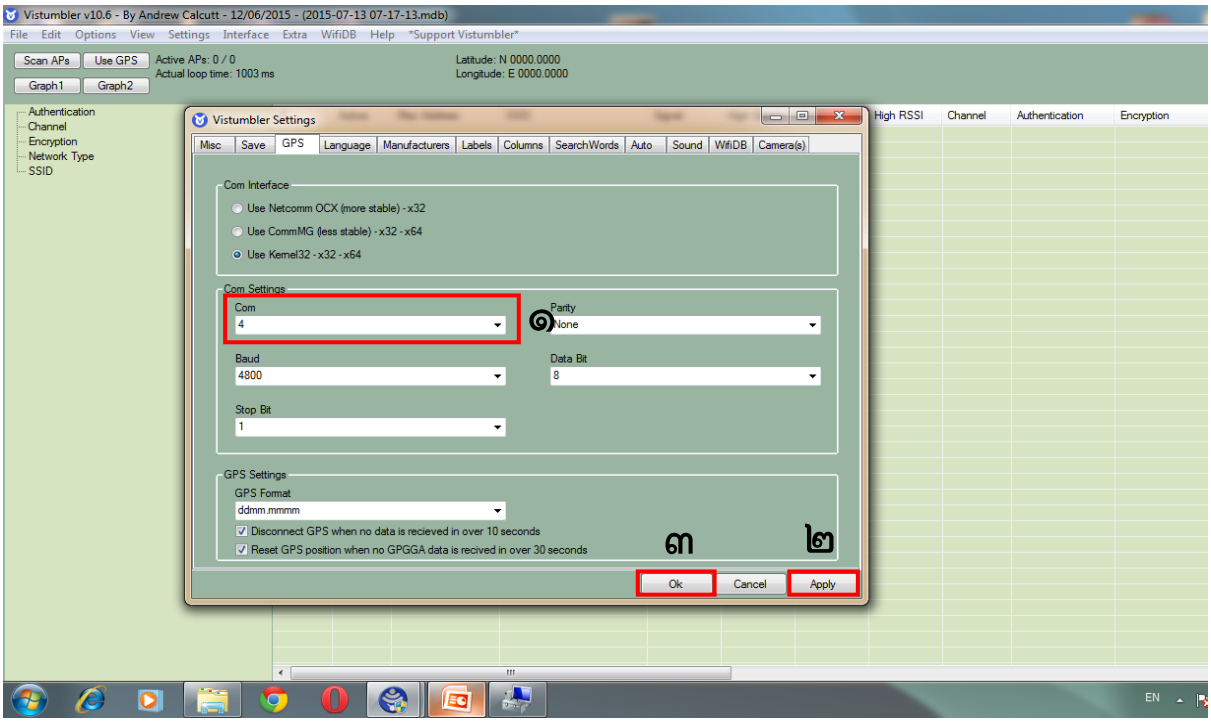
รูปที่ ๔๗ ตรวจสอบระบบไร้สายด้วย Vistumbler ขั้นตอนที่ ๒

๒.๒.๒ เช็คดูพอร์ตคอม โดยคลิ๊กที่เครื่องหมาย +



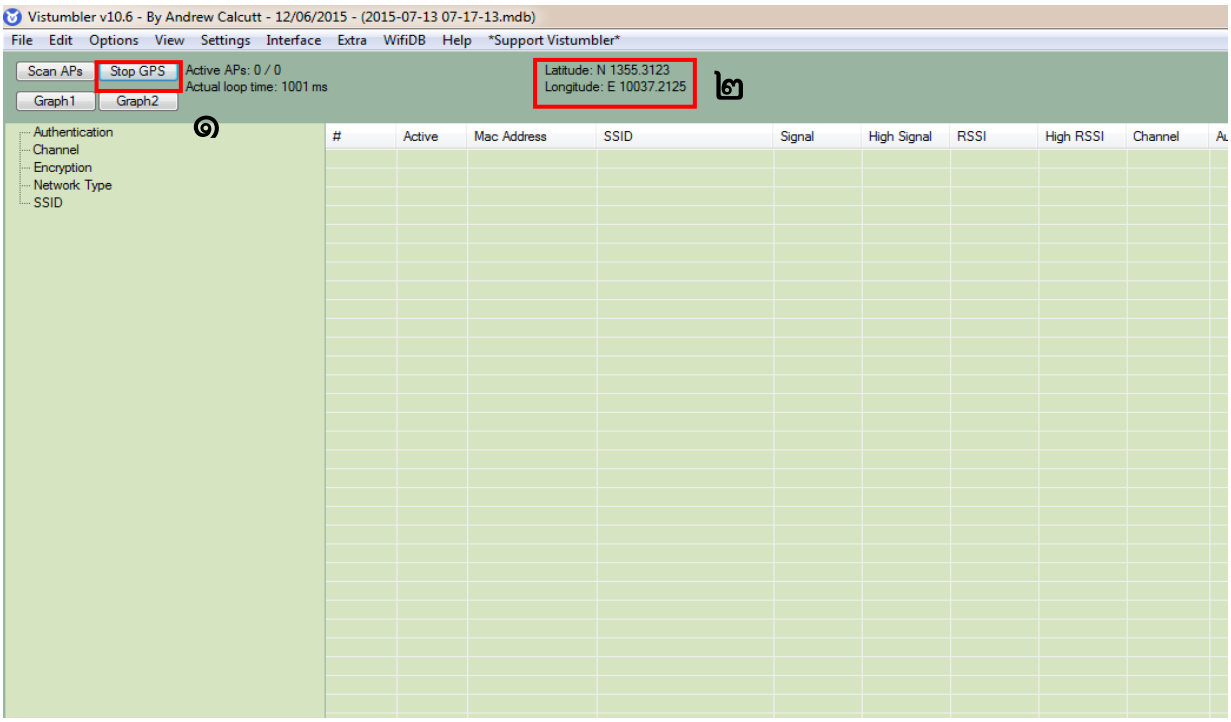
รูปที่ ๔๘ ตรวจสอบระบบไร้สายด้วย Vistumbler ขั้นตอนที่ ๓

๒.๒.๒ นำค่าที่ได้ไปเปลี่ยนค่าพอร์ตของ Gps ให้ตรงกัน (๑) จากนั้นกด apply (๒) แล้วตามด้วย ok (๓)



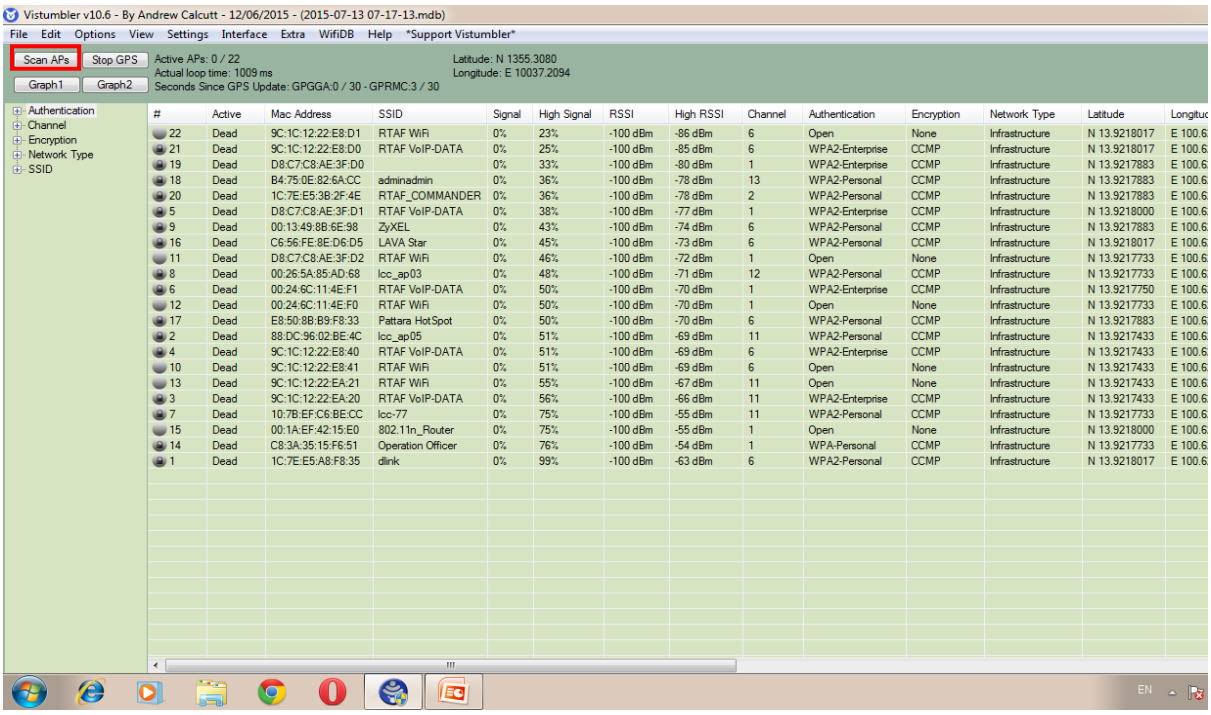
รูปที่ ๔๙ ตรวจสอบระบบไร้สายด้วย Vistumbler ขั้นตอนที่ ๔

๒.๒.๒ กด use gps (๑) จะเห็นการรับค่าต่าง ๆ ของดาวเทียม (๒) รอจนมีค่าพิกัดดาวเทียมขึ้นทางด้านขวามือ



รูปที่ ๕๐ ตรวจสอบระบบไร้สายด้วย Vistumbler ขั้นตอนที่ ๕

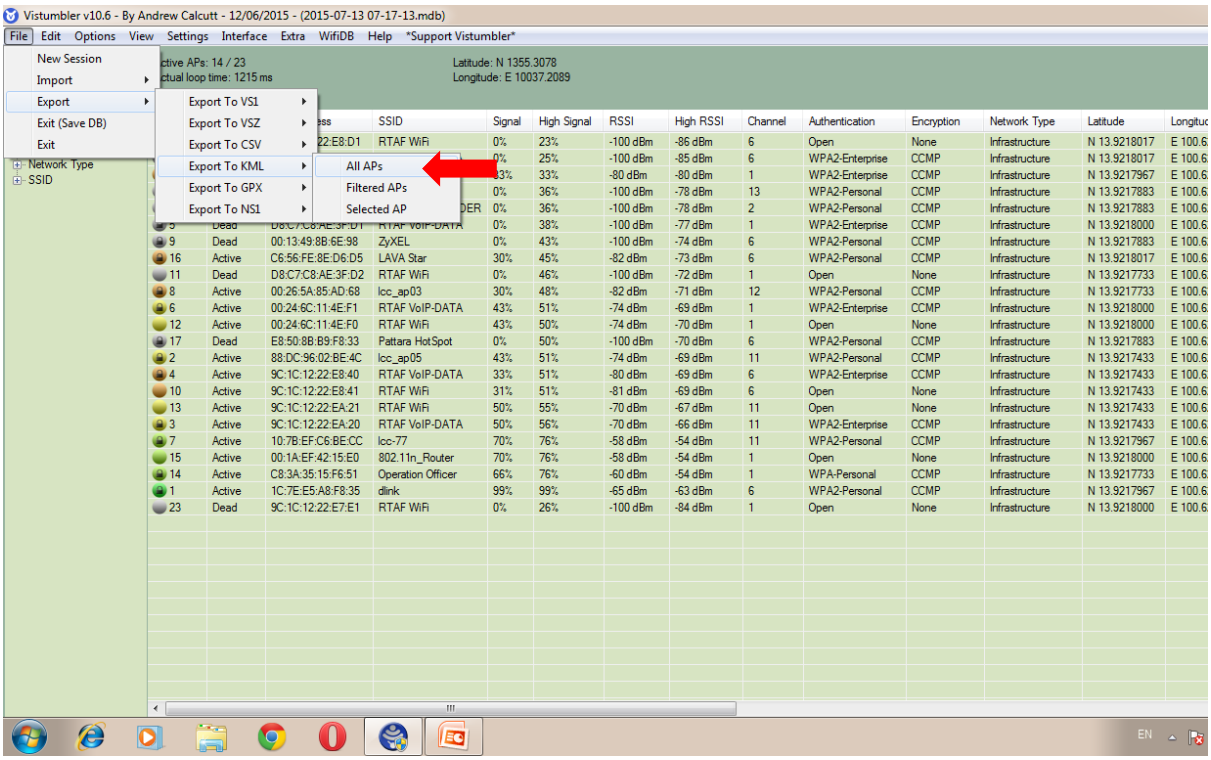
๒.๒.๒ จากนั้นกด Scan APs แล้วทำการตรวจสอบเครือข่ายไร้สาย ด้วยการขับรถ หรืออื่น ๆ ตามสะดวก



#	Active	Mac Address	SSID	Signal	High Signal	RSSI	High RSSI	Channel	Authentication	Encryption	Network Type	Latitude	Longitud
22	Dead	9C:1C:12:22:E8:D1	RTAF WiFi	0%	23%	-100 dBm	-86 dBm	6	Open	None	Infrastructure	N 13.9218017	E 100.6
21	Dead	9C:1C:12:22:E8:D0	RTAF VoIP-DATA	0%	25%	-100 dBm	-85 dBm	6	WPA2-Enterprise	CCMP	Infrastructure	N 13.9218017	E 100.6
19	Dead	D8:C7:C8:AE:3F:D0		0%	33%	-100 dBm	-80 dBm	1	WPA2-Enterprise	CCMP	Infrastructure	N 13.9217883	E 100.6
18	Dead	B4:75:0E:82:6A:CC	adminadmin	0%	36%	-100 dBm	-78 dBm	13	WPA2-Personal	CCMP	Infrastructure	N 13.9217883	E 100.6
20	Dead	1C:7E:E5:3B:2F:4E	RTAF_COMMANDER	0%	36%	-100 dBm	-78 dBm	2	WPA2-Personal	CCMP	Infrastructure	N 13.9217883	E 100.6
5	Dead	D8:C7:C8:AE:3F:D1	RTAF VoIP-DATA	0%	38%	-100 dBm	-77 dBm	1	WPA2-Enterprise	CCMP	Infrastructure	N 13.9218000	E 100.6
9	Dead	00:13:49:8B:6E:98	ZyXEL	0%	43%	-100 dBm	-74 dBm	6	WPA2-Personal	CCMP	Infrastructure	N 13.9217883	E 100.6
16	Dead	C6:56:FE:8E:D6:D5	LAVA Star	0%	45%	-100 dBm	-73 dBm	6	WPA2-Personal	CCMP	Infrastructure	N 13.9218017	E 100.6
11	Dead	D8:C7:C8:AE:3F:D2	RTAF WiFi	0%	46%	-100 dBm	-72 dBm	1	Open	None	Infrastructure	N 13.9217733	E 100.6
8	Dead	00:26:5A:85:AD:68	Icc_ap03	0%	48%	-100 dBm	-71 dBm	12	WPA2-Personal	CCMP	Infrastructure	N 13.9217733	E 100.6
6	Dead	00:24:6C:11:4E:F1	RTAF VoIP-DATA	0%	50%	-100 dBm	-70 dBm	1	WPA2-Enterprise	CCMP	Infrastructure	N 13.9217750	E 100.6
12	Dead	00:24:6C:11:4E:F0	RTAF WiFi	0%	50%	-100 dBm	-70 dBm	1	Open	None	Infrastructure	N 13.9217733	E 100.6
17	Dead	E8:50:8B:B9:F8:33	Pattara HotSpot	0%	50%	-100 dBm	-70 dBm	6	WPA2-Personal	CCMP	Infrastructure	N 13.9217883	E 100.6
2	Dead	88:DC:96:02:BE:4C	Icc_ap05	0%	51%	-100 dBm	-69 dBm	11	WPA2-Personal	CCMP	Infrastructure	N 13.9217433	E 100.6
4	Dead	9C:1C:12:22:E8:40	RTAF VoIP-DATA	0%	51%	-100 dBm	-69 dBm	6	WPA2-Enterprise	CCMP	Infrastructure	N 13.9217433	E 100.6
10	Dead	9C:1C:12:22:E8:41	RTAF WiFi	0%	51%	-100 dBm	-69 dBm	6	Open	None	Infrastructure	N 13.9217433	E 100.6
13	Dead	9C:1C:12:22:EA:21	RTAF WiFi	0%	55%	-100 dBm	-67 dBm	11	Open	None	Infrastructure	N 13.9217433	E 100.6
3	Dead	9C:1C:12:22:EA:20	RTAF VoIP-DATA	0%	56%	-100 dBm	-66 dBm	11	WPA2-Enterprise	CCMP	Infrastructure	N 13.9217433	E 100.6
7	Dead	10:7B:EF:C6:BE:CC	Icc-77	0%	75%	-100 dBm	-55 dBm	11	WPA2-Personal	CCMP	Infrastructure	N 13.9217733	E 100.6
15	Dead	00:1A:EF:42:15:E0	802.11n_Router	0%	75%	-100 dBm	-55 dBm	1	Open	None	Infrastructure	N 13.9218000	E 100.6
14	Dead	C8:3A:35:15:F6:51	Operation Officer	0%	76%	-100 dBm	-54 dBm	1	WPA-Personal	CCMP	Infrastructure	N 13.9217733	E 100.6
1	Dead	1C:7E:E5:A8:F8:35	dlink	0%	99%	-100 dBm	-63 dBm	6	WPA2-Personal	CCMP	Infrastructure	N 13.9218017	E 100.6

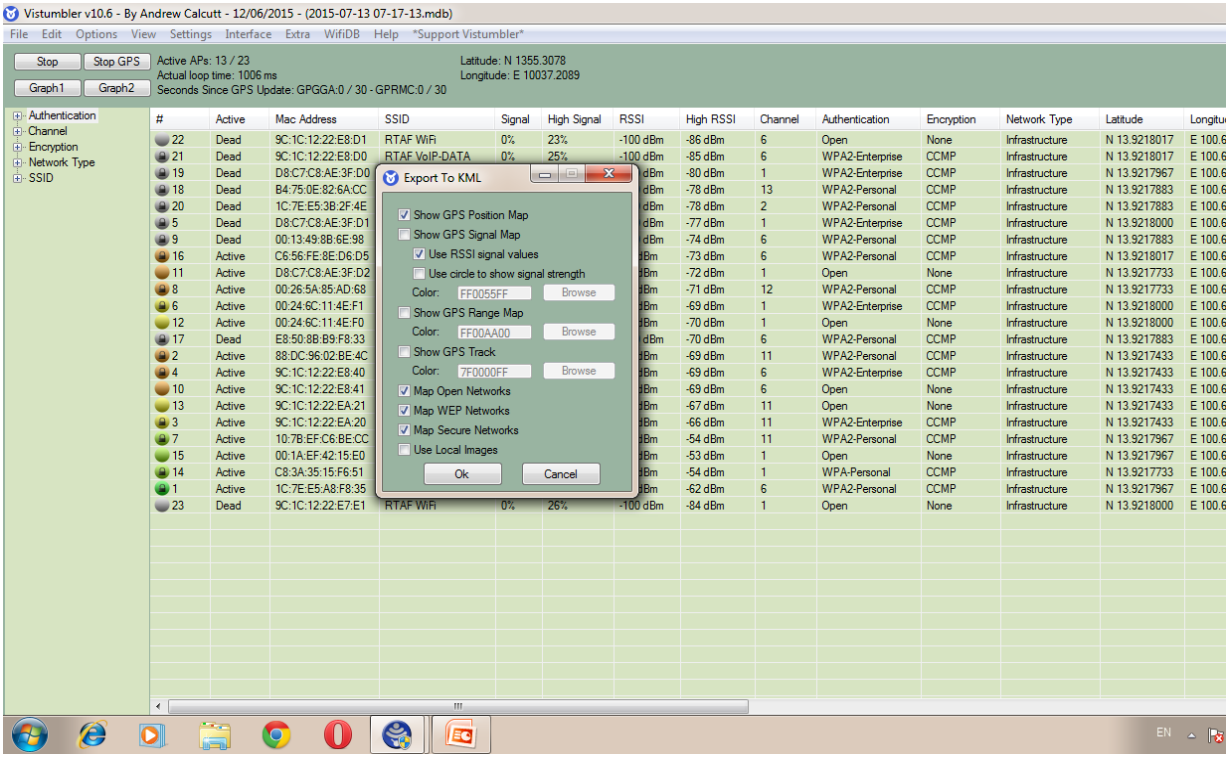
รูปที่ ๕๑ ตรวจสอบระบบไร้สายด้วย Vistumbler ขั้นตอนที่ ๖

๒.๒.๒ เมื่อเสร็จการตรวจสอบระบบไร้สายแล้ว ให้ทำการเซฟไฟล์เป็น vs1 ในเมนู Export



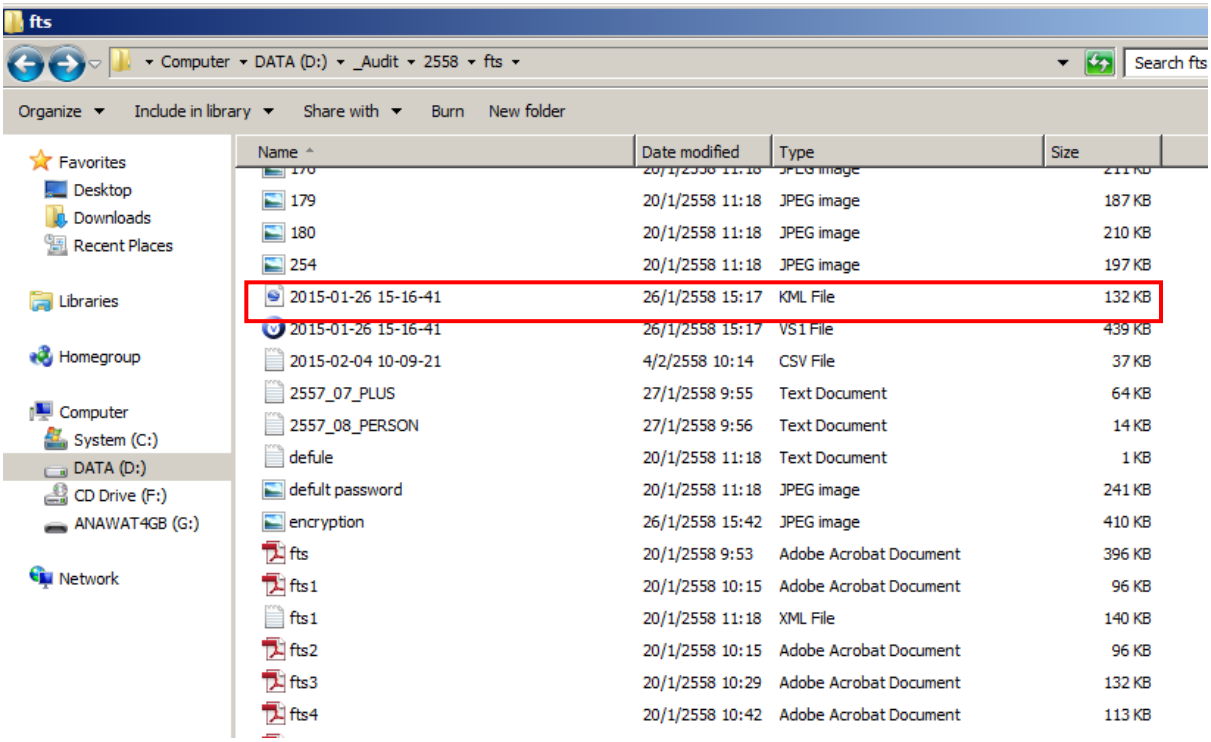
รูปที่ ๕๒ ตรวจสอบระบบไร้สายด้วย Vistumbler ขั้นตอนที่ ๗

๒.๒.๒ หลังจากนั้นก็เลือก Export เป็น kml อีกครั้งหนึ่ง



รูปที่ ๕๓ ตรวจสอบระบบไร้สายด้วย Vistumbler ขั้นตอนที่ ๘

๒.๒.๒ เลือกที่เก็บไฟล์ไว้

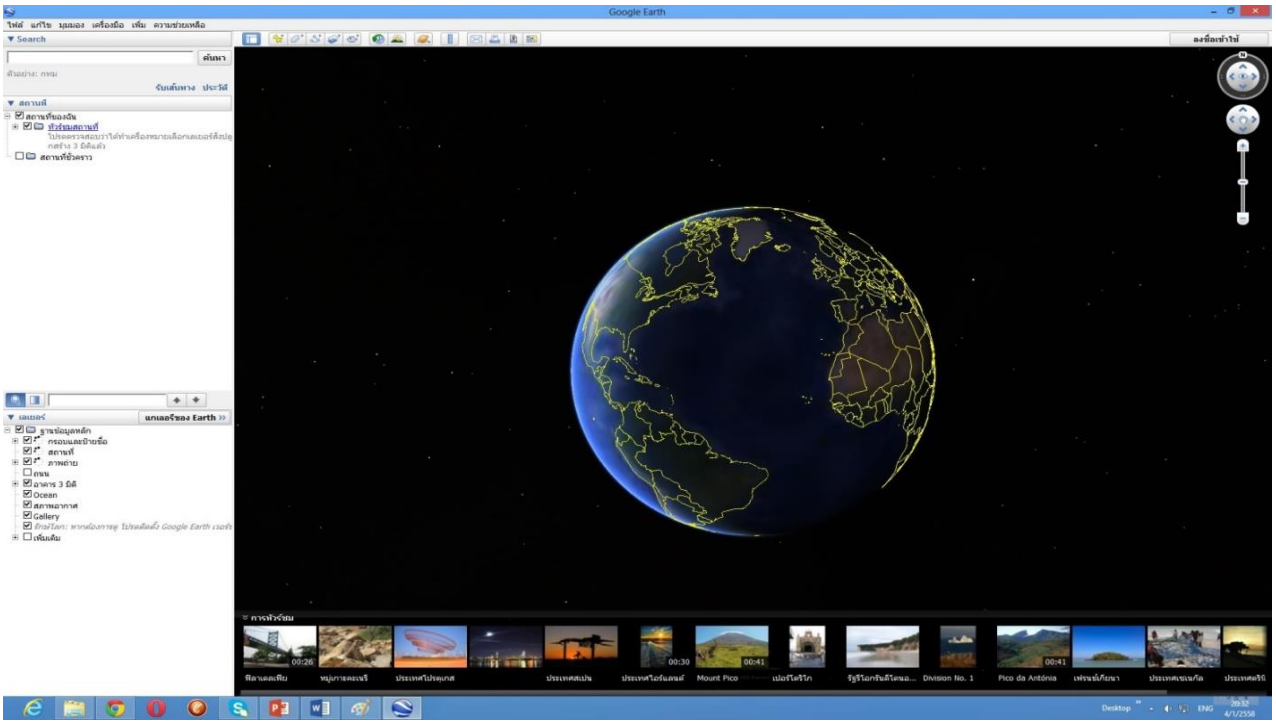


รูปที่ ๕๔ ตรวจสอบระบบไร้สายด้วย Vistumbler ขั้นตอนที่ ๙

๒.๒.๑ จากนั้นไปที่โฟลเดอร์ที่เก็บ ให้ดับเบิลคลิ๊กที่ไฟล์นามสกุล kml :ต่อ internet ให้เรียบร้อยด้วย

๒.๓ การใช้โปรแกรมเสริมเพื่อเปิดดูไฟล์ KML : google earth

๒.๓.๑ เปิดโปรแกรม google earth ขึ้นมา หากไม่มีให้ไปดาวโหลดและติดตั้งก่อน

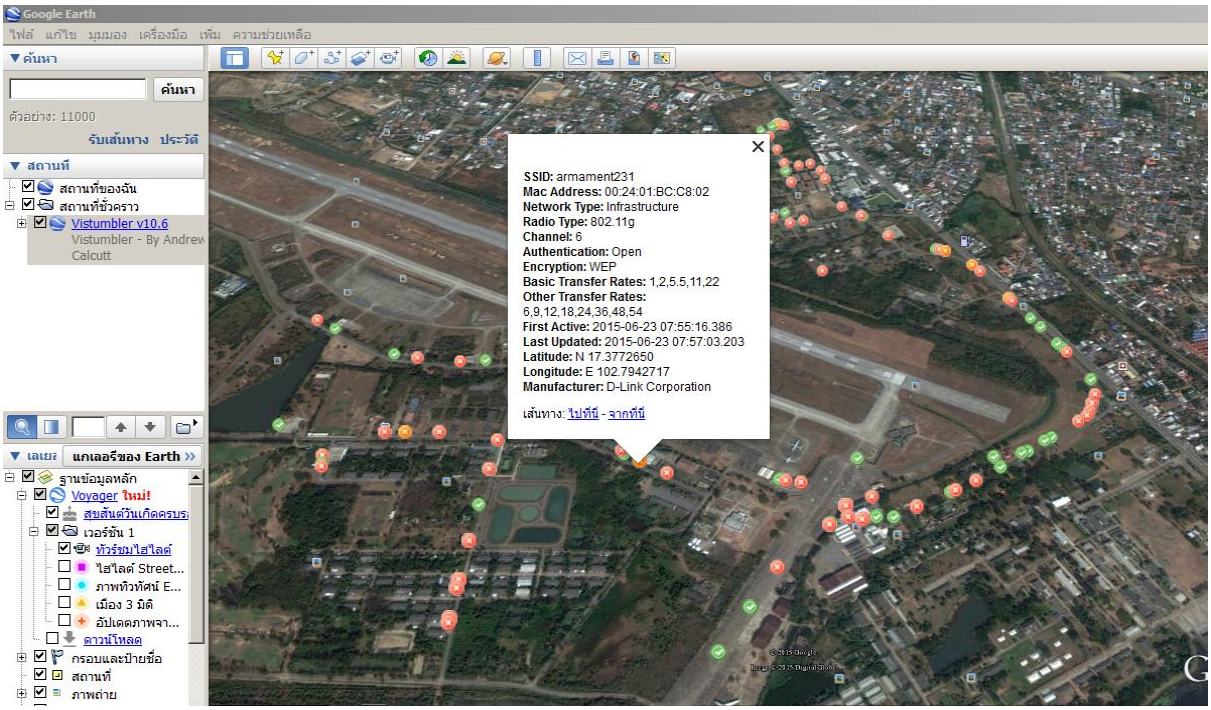


รูปที่ ๕๕ การใช้โปรแกรมเสริมเพื่อเปิดดูไฟล์ KML ขั้นตอนที่ ๑

๒.๒.๒ แสดงตำแหน่งที่อยู่ของอุปกรณ์ไร้สาย

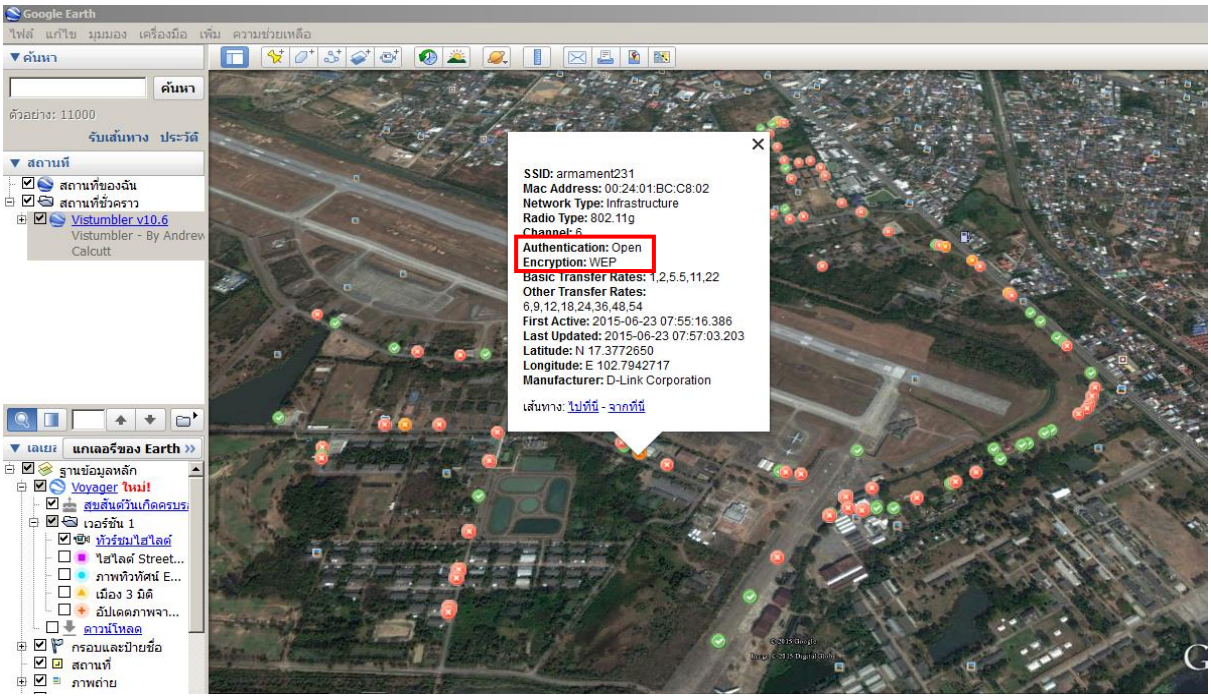
รูปที่ ๕๖ การใช้โปรแกรมเสริมเพื่อเปิดดูไฟล์ KML ขั้นตอนที่ ๒

๒.๒.๑ สามารถคลิ๊กเข้าไปดูได้ตามจะสีต่าง ๆ ในที่นี้สีแดงหมายถึงปลอดภัย สีส้มหมายถึงไม่ปลอดภัย สีเขียวหมายถึงเข้าถึงได้โดยไม่ต้องใส่รหัส



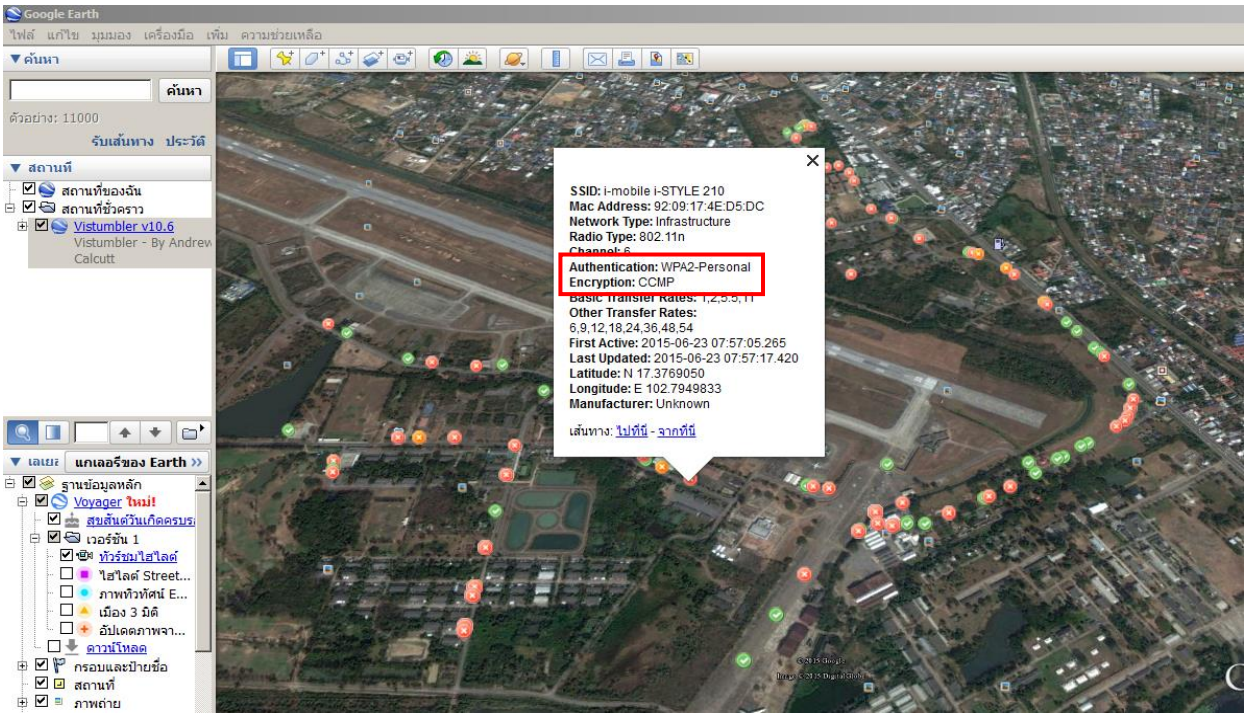
รูปที่ ๕๗ การใช้โปรแกรมเสริมเพื่อเปิดดูไฟล์ KML ขั้นตอนที่ ๓

๒.๒.๒ คลิ๊กเข้าไปดูได้ตามจุดสีต่าง ๆ จะแสดงรายละเอียดที่ตรวจพบ ในที่นี้เป็นการเข้ารหัสแบบไม่ปลอดภัย สามารถถอดรหัสได้ง่าย



รูปที่ ๕๘ การใช้โปรแกรมเสริมเพื่อเปิดดูไฟล์ KML ขั้นตอนที่ ๔

๒.๒.๑ คลิ๊กเข้าไปดูได้ตามจุดสีแดง จะแสดงรายละเอียดที่ตรวจพบ ในที่นี้เป็นการเข้ารหัสแบบปลอดภัย WPA หรือ WPA2



รูปที่ ๕๙ การใช้โปรแกรมเสริมเพื่อเปิดดูไฟล์ KML ขั้นตอนที่ ๕

บทที่ ๗

การปฏิบัติการไซเบอร์เชิงรุก

๑. การปฏิบัติการทางทหารในมิติไซเบอร์

การปฏิบัติการทางทหารในมิติไซเบอร์ (Military Cyber Operation) เป็นการดำเนินการโดยใช้ขีดความสามารถทางไซเบอร์ (Cyber Capabilities) ในมิติไซเบอร์ทั้งปวง เพื่อให้บรรลุวัตถุประสงค์ทางทหาร ได้แก่ การได้มาซึ่งความได้เปรียบในมิติไซเบอร์ (Cyberspace Superiority) หรือการครองมิติไซเบอร์ (Cyberspace Control) ซึ่งหมายถึงสภาวะที่ฝ่ายเรามีความได้เปรียบหรือมีอิสระในการปฏิบัติการในมิติไซเบอร์ได้อย่างปลอดภัย (Secure) เชื่อถือได้ (Reliable) ในช่วงเวลาและสถานที่ที่ต้องการ โดยปราศจากการขัดขวางจากฝ่ายตรงข้าม

๒. การปฏิบัติการไซเบอร์เชิงรุก

การปฏิบัติการทางไซเบอร์เชิงรุก เป็นการปฏิบัติการในมิติไซเบอร์โดยมีวัตถุประสงค์เพื่อนำไปสู่การโจมตีทางไซเบอร์ต่อฝ่ายตรงข้าม ซึ่งการโจมตีทางไซเบอร์นั้นมีวัตถุประสงค์เพื่อขัดขวาง (Disrupt) ทำลาย (Destroy) หรือควบคุม (Control) การใช้งานในมิติไซเบอร์ของฝ่ายตรงข้าม โดยรวมถึงการทำลาย เปลี่ยนแปลง หรือจารกรรมข้อมูลสำคัญ

การปฏิบัติการทางทหารเชิงรุกในมิติไซเบอร์ มีเป้าหมายอยู่ที่การใช้ยุทธภัณฑ์ทางไซเบอร์ (Cyber Weapon) ซึ่งหมายถึงชุดคำสั่งทางคอมพิวเตอร์ที่ถูกออกแบบมาเพื่อใช้ในการโจมตีระบบสารสนเทศหรืออุปกรณ์อิเล็กทรอนิกส์ โดยเฉพาะระบบหรืออุปกรณ์ที่มีความสำคัญสูงของฝ่ายตรงข้าม เพื่อหวังผลให้เกิดความเสียหายทางกายภาพ ทางกระบวนการทำงาน หรือทางจิตใจของผู้ปฏิบัติงาน ดังนี้

๒.๑ การปฏิเสธการใช้งาน (Deny) มีวัตถุประสงค์เพื่อสร้างผลกระทบให้เกิดขึ้นต่อความพร้อมใช้งานระบบเป้าหมายของฝ่ายตรงข้ามในระดับที่ต้องการในห้วงเวลาที่ต้องการ เพื่อเป็นการลด/ขัดขวาง/ทำลาย ขีดความสามารถในการใช้ทรัพยากรทางไซเบอร์ของฝ่ายตรงข้าม แบ่งออกเป็น ๓ ระดับ คือ

๒.๑.๑ ระดับลดขีดความสามารถ (Degrade) เป็นลักษณะของการพยายามลดขีดความสามารถในการเข้าถึง (Access) และปฏิบัติการ (Operation) ของเป้าหมายให้ไปอยู่ในระดับที่ต้องการ โดยระบุเป็นค่าเปอร์เซ็นต์ของขีดความสามารถ (Percentage of Capacity) โดยระดับของการลดขีดความสามารถจะต้องกำหนดให้ชัดเจน และหากมีความต้องการระบุห้วงเวลา ให้กำหนดห้วงเวลาด้วย

๒.๑.๒ ระดับขัดขวางขีดความสามารถ (Disrupt) เป็นลักษณะของการพยายามทำลายขีดความสามารถทั้งมวลในการเข้าถึง (Access) และปฏิบัติการ (Operations) ของเป้าหมายแบบชั่วคราวเฉพาะระหว่างห้วงเวลาที่ต้องการ โดยระบุเวลาเริ่มและเวลาสิ้นสุด ทั้งนี้ การขัดขวางขีดความสามารถอาจพิจารณา

เป็นรูปแบบของการลดขีดความสามารถ (Degrade) ที่กำหนดระดับของการลดขีดความสามารถเท่ากับ ๑๐๐ เปอร์เซ็นต์ได้

๒.๑.๓ ระดับทำลายขีดความสามารถ (Destroy) เป็นลักษณะของการพยายามทำลายขีดความสามารถทั้งมวลในการเข้าถึง (Access) และปฏิบัติการ (Operations) ของเป้าหมายแบบถาวร (กำหนดให้ค่าเปอร์เซ็นต์เป้าหมายของขีดความสามารถและห้วงเวลาที่ต้องการมีค่าสูงสุด)

๒.๒ การเข้าควบคุม (Manipulate) เป็นการเข้าควบคุมหรือเปลี่ยนแปลงแก้ไขข้อมูล/สารสนเทศตลอดจนระบบเครือข่าย/ระบบสารสนเทศของเป้าหมาย ให้เป็นไปตามเจตนารมณ์/วัตถุประสงค์/การสั่งการของผู้บังคับบัญชาฝ่ายเรา

๓. กระบวนการ และกรอบการปฏิบัติการไซเบอร์เชิงรุก

๓.๑ Cyber Kill Chain เผยแพร่โดยบริษัท Lockheed Martin เป็นกระบวนการที่ระบุสิ่งที่ต้องดำเนินการเพื่อให้บรรลุวัตถุประสงค์ของปฏิบัติการทางไซเบอร์เชิงรุก โดยเฉพาะอย่างยิ่งการโจมตีที่เรียกว่า Advanced Persistent Threats (APTs) โดยแบ่งออกเป็น ๗ ขั้นตอน ดังนี้

๓.๑.๑ Reconnaissance การสอดส่องเพื่อเก็บข้อมูลของเป้าหมายให้มากที่สุด เพื่อหาโอกาสและจุดอ่อนก่อนเริ่มโจมตีเป้าหมาย ซึ่งอาจจะใช้เครื่องมือในการหาข้อมูลต่าง ๆ หรือการสืบค้นผ่านอินเทอร์เน็ต

๓.๑.๒ Weaponization เป็นการเตรียมหาวิธีเพื่อเจาะระบบ และเลือกเครื่องมือที่เหมาะสมกับเป้าหมาย โดยพิจารณาและวิเคราะห์จากช่องโหว่ที่ตรวจพบ

๓.๑.๓ Delivery ส่ง Payload ที่เตรียมไว้ไปยังเหยื่อผ่านช่องทางต่างๆ เช่น ไฟล์แนบอีเมล เว็บไซต์ หรือ USB Drive

๓.๑.๔ Exploitation: แฮกเกอร์ทำการเจาะระบบของเหยื่อผ่านช่องโหว่ต่างๆ

๓.๑.๕ Installation: ติดตั้งชุดโปรแกรมประสงค์ร้ายบนเครื่องเป้าหมาย เพื่อคอยรับคำสั่งจากฝั่งเรา

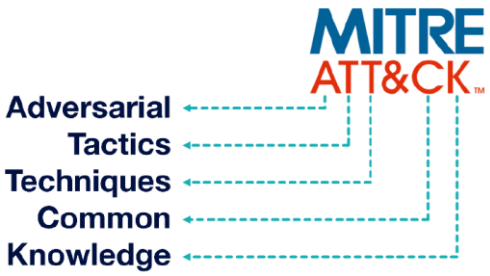
๓.๑.๖ Command & Control สร้างช่องทางรับส่งคำสั่งกับชุดคำสั่งที่ติดตั้งไว้ เพื่อสั่งการและควบคุมเครื่องเป้าหมาย

๓.๑.๗ Action on Objectives ดำเนินการติดตามเป้าหมายเพื่อให้บรรลุวัตถุประสงค์ เช่น ขโมยข้อมูล หรือขัดขวางการทำงานของระบบ เป็นต้น

รูปที่ ๖๐ กรอบการปฏิบัติการไซเบอร์เชิงรุก

กระบวนการต่าง ๆ นั้น มีลักษณะเกี่ยวข้องกันและต่อเนื่องกันในลักษณะลูกโซ่ (Chain) หากเกิดการยับยั้งในขั้นตอนใดขั้นตอนหนึ่งได้สำเร็จ ก็จะส่งผลให้โจมตีทางไซเบอร์ต่อเป้าหมายนั้นไม่ประสบผลความสำเร็จได้

๓.๒ MITRE ATT&CK Framework เป็นกรอบการปฏิบัติการไซเบอร์เชิงรุกที่พัฒนาโดย MITRE เพื่อระบุรายการ จัดหมวดหมู่ และอธิบายกลยุทธ์ กระบวนการ และเทคนิคการโจมตีที่พบได้ในมิติไซเบอร์ปัจจุบัน



รูปที่ ๖๑ กรอบการปฏิบัติการไซเบอร์เชิงรุกของ MITRE

MITRE ATT&CK แบ่งเป็นหมวดหมู่เทคนิคการโจมตีครอบคลุมทั้งการเตรียมโจมตี (PRE-Attack) รูปแบบการโจมตีต่อองค์กร (Enterprise) รูปแบบการโจมตีต่ออุปกรณ์เคลื่อนที่ (Mobile) และรูปแบบการโจมตีต่อระบบควบคุมอุตสาหกรรม (Industrial Control System) ซึ่งกลยุทธ์ในการโจมตีต่อองค์กรประกอบไปด้วย ๑๒ กลยุทธ์ ดังนี้

๓.๒.๑ Initial Access เป็นกลยุทธ์ที่ฝ่ายโจมตีพยายามที่จะเข้าถึงระบบ หรือหาช่องทางในการโจมตีเป้าหมาย

๓.๒.๒ Execution เป็นกลยุทธ์ที่ฝ่ายโจมตีพยายามเรียกใช้งานชุดคำสั่ง/โปรแกรมประสงค์ร้ายที่ได้ลักลอบติดตั้งไว้ที่เครื่องเป้าหมาย

๓.๒.๓ Persistence เป็นกลยุทธ์ที่ฝ่ายโจมตีพยายามให้ชุดคำสั่ง/โปรแกรมประสงค์ร้ายสามารถพร้อมรับคำสั่งจากฝ่ายโจมตีอยู่ตลอดเวลาที่ต้องการ

๓.๒.๔ Privilege Escalation เป็นกลยุทธ์ที่ฝ่ายโจมตีพยายามยกระดับสิทธิ์ให้สูงขึ้น เพื่อเอื้อประโยชน์ในการเข้าสั่งการและควบคุมเป้าหมาย

๓.๒.๕ Defense Evasion เป็นกลยุทธ์ที่ฝ่ายโจมตีใช้เพื่อพยายามหลบเลี่ยงการตรวจจับจากระบบการรักษาความปลอดภัย

๓.๒.๖ Credential Access เป็นกลยุทธ์ที่ฝ่ายโจมตีพยายามโจรกรรมข้อมูลสำหรับใช้ยืนยันตัวตน ที่มีใช้งานอยู่บนระบบเป้าหมาย

๓.๒.๗ Discovery เป็นกลยุทธ์ที่ฝ่ายโจมตีพยายามใช้ตรวจสอบข้อมูล การเชื่อมต่อ หรือช่องโหว่ของเป้าหมาย เพื่อสนับสนุนการโจมตี

๓.๒.๘ Lateral Movement เป็นกลยุทธ์ที่ฝ่ายโจมตีพยายามเคลื่อนย้ายตัวเองไปสู่เป้าหมายอื่น ๆ ที่อยู่ในระบบ

๓.๒.๙ Collection เป็นกลยุทธ์ที่ฝ่ายโจมตีพยายามเก็บรวบรวมข้อมูลที่สนใจ หรือข้อมูลที่มีความละเอียดอ่อนของเป้าหมาย

๓.๒.๑๐ Command & Control เป็นกลยุทธ์ที่ฝ่ายโจมตีพยายามติดต่อสื่อสารกับเครื่องเป้าหมายที่สามารถควบคุมได้สำเร็จแล้ว เพื่อใช้สั่งการให้กระทำการสิ่งอื่นต่อไป

๓.๒.๑๑ Exfiltration เป็นกลยุทธ์ที่ฝ่ายโจมตีพยายามขโมยข้อมูลสำคัญออกไป

๓.๒.๑๒ Impact เป็นกลยุทธ์ที่ฝ่ายโจมตีพยายามลดทอน ขัดขวาง หรือทำลายต่อข้อมูลและระบบเป้าหมาย

๔. ขั้นตอนและวิธีการปฏิบัติการไซเบอร์เชิงรุก

๔.๑ การสอดส่อง และรวบรวมข้อมูลเป้าหมาย (Reconnaissance and Information Gathering)

เป็นการปฏิบัติการข่าว สอดส่อง และเฝ้าตรวจในมิติไซเบอร์ เพื่อรวบรวมข้อมูลข่าวกรองซึ่งคาดว่าจะมีความจำเป็นต่อการสนับสนุนการปฏิบัติการเชิงรุก เช่น การรวบรวมข้อมูลเป้าหมายเกี่ยวกับโครงสร้างสถาปัตยกรรมระบบ ลักษณะอุปกรณ์และเครื่องมือที่ใช้ วิธีการใช้งานและข้อมูลของบุคคล โดยทำการสืบค้นข้อมูลจากกระบวนการทางเทคนิค รวมถึงการใช้วิธีวิศวกรรมสังคม (Social Engineering) ร่วมด้วย

๔.๑.๑ Passive Information Gathering คือ รูปแบบการหาข่าวที่ปฏิบัติโดยไม่มีการปฏิสัมพันธ์กับข้อมูลหรือระบบเป้าหมาย เป็นประโยชน์เมื่อฝ่ายโจมตีไม่ต้องการให้เป้าหมายรับรู้และตรวจจับการปฏิบัติได้ การใช้ OSINT หรือ Open Source Intelligence เพื่อการค้นหาและวิเคราะห์ข้อมูลเป้าหมายจากแหล่งข้อมูลเปิดทั่วไปที่สามารถเข้าถึงได้โดยสาธารณะ ตัวอย่างเครื่องมือและซอฟต์แวร์ที่ใช้ คือเครื่องมือสืบค้น (Search Engines) เช่น Google Bing หรือ DuckDuckGo ซึ่งเป็นเครื่องมือ OSINT ที่ใช้งานได้ฟรีและมีประสิทธิภาพ สามารถใช้งานฟังก์ชันการสืบค้นขั้นสูงโดยใช้ตัวกรองได้ วิธีการนี้เรียกว่า Google Dorking หรือ Google Hacking เพื่อใช้งานการสืบค้นข้อมูลทั่วไปที่ตรงตามเงื่อนไขหรือเฉพาะเจาะจง เช่น การสืบค้นข้อมูลตามนามสกุลไฟล์ที่ระบุ การสืบค้นข้อมูลจากเว็บไซต์ที่ระบุ หรือการสืบค้นข้อมูลตามช่วงเวลา

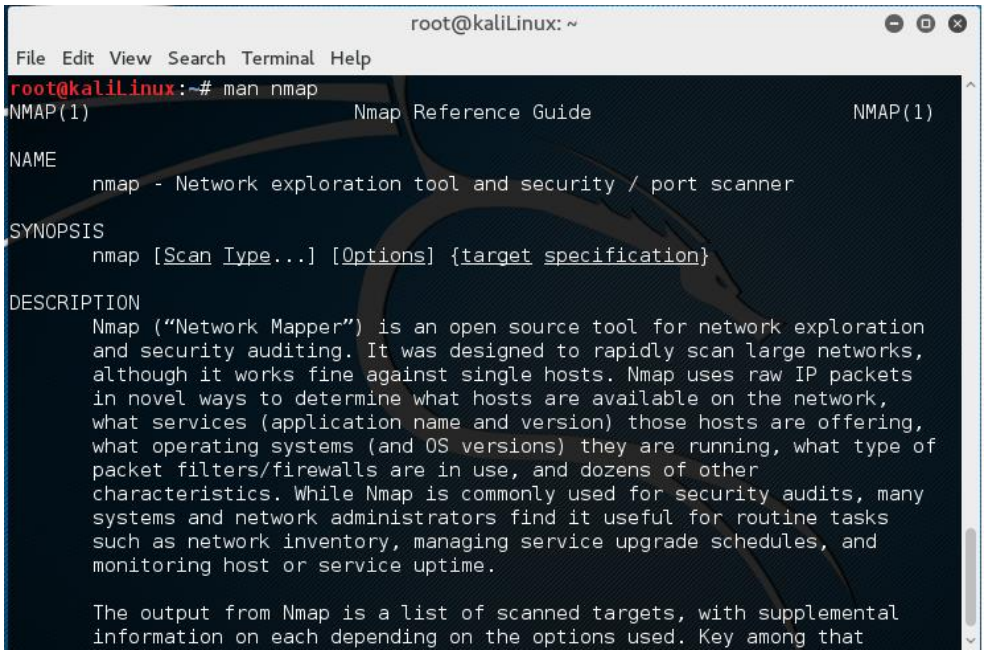
๔.๑.๒ Active Information Gathering คือ รูปแบบการหาข่าวที่ปฏิบัติโดยมีการปฏิสัมพันธ์กับข้อมูลหรือระบบเป้าหมาย การหาข่าวด้วยวิธีนี้อาจทำให้ระบบรักษาความปลอดภัยบนเป้าหมายสามารถตรวจจับการปฏิบัติได้ เช่น DNS Enumeration, Port Scanning และการหา OS Fingerprinting เป็นต้น

๔.๒ การตรวจสอบและประเมินช่องโหว่ (Scanning and Vulnerability Assessment)

เป็นการตรวจสอบหรือการวิเคราะห์ช่องโหว่ เพื่อโอกาสในการใช้ช่องโหว่นั้นโจมตีต่อเป้าหมาย ช่องโหว่ที่อาจตรวจพบ เช่น การใช้งาน Service ที่ล้าสมัยและมีช่องโหว่ เป็นต้น การปฏิบัติในขั้นตอนนี้อาจมีข้อบังคับทางกฎหมายมาเกี่ยวข้องหากการปฏิบัตินั้นกระทำโดยไม่ได้รับอนุญาตจากเจ้าของระบบ

๔.๒.๑ Port Scanning ด้วย Nmap/Zenmap

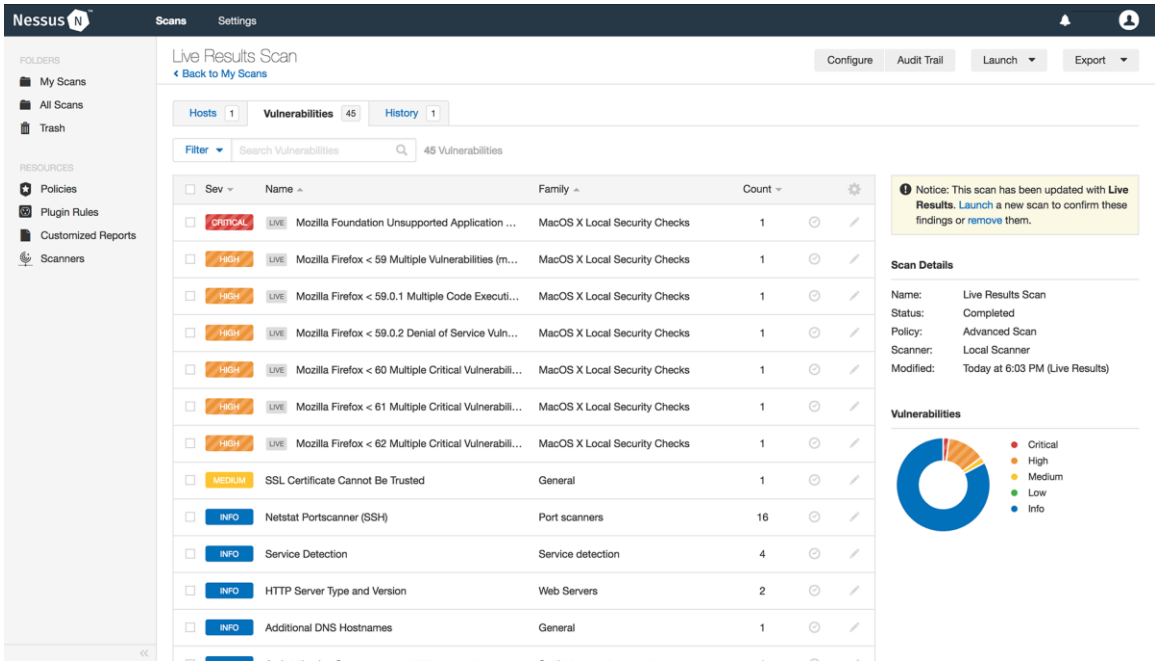
Nmap และ Zenmap เป็นเครื่องมือการสำรวจระบบที่ได้รับความนิยมและสามารถใช้งานได้ฟรี มีความสามารถในการสำรวจเครือข่าย อุปกรณ์ บริการ รวมถึงการตรวจสอบช่องโหว่ได้



รูปที่ ๖๒ เครื่องมือสำรวจระบบ nmap

๔.๒.๒ Vulnerability Scanning ด้วย Nessus

Nessus เป็นเครื่องมือที่ใช้สำรวจ ตรวจสอบ และประเมินช่องโหว่ในระบบ ซึ่งสามารถให้รายละเอียดอุปกรณ์ รายละเอียดช่องโหว่ และวิธีการจัดการช่องโหว่ โดยจะจัดระดับความรุนแรงของช่องโหว่ไว้เป็น ๔ ระดับ คือ ระดับวิกฤต (Critical) ระดับสูง (High) ระดับกลาง (Medium) และระดับต่ำ (INFO)

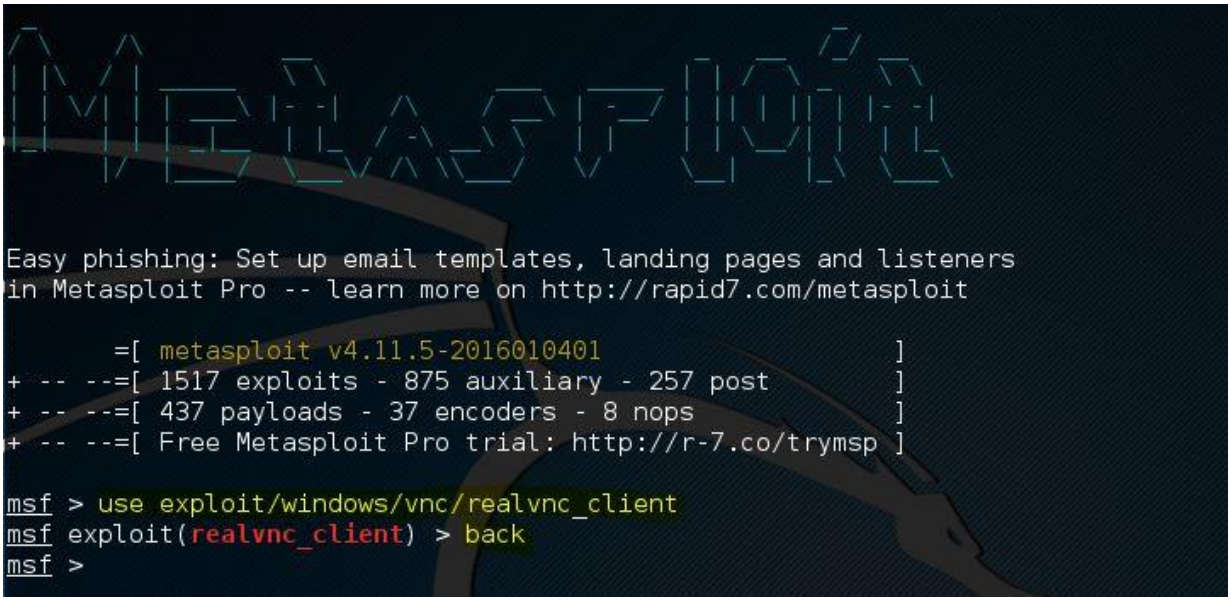


รูปที่ ๖๓ เครื่องมือสำรวจ ตรวจสอบ และประเมินช่องโหว่ในระบบ Nessus

๔.๓ การแสวงประโยชน์จากช่องโหว่ (Exploitation)

เป็นการใช้อาวุธทางด้านไซเบอร์ทุกรูปแบบในการเข้าโจมตีต่อระบบเป้าหมาย โดยแสวงประโยชน์จากช่องโหว่ทางไซเบอร์เพื่อเจาะระบบให้เกิดผลตามที่คาดหวัง

Metasploit Framework เป็นเครื่องมือที่ใช้ Exploit ระบบเป้าหมายจากช่องโหว่ต่าง ๆ ที่ตรวจพบ มีฟังก์ชันการใช้งานหรือโมดูลที่หลากหลาย และสามารถสร้างเครื่องมือที่เฉพาะเจาะจงสำหรับการโจมตีระบบเป้าหมายได้



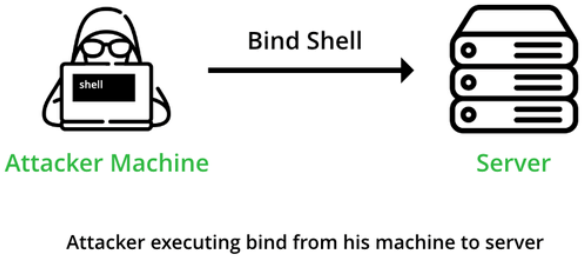
รูปที่ ๖๔ เครื่องมือที่ใช้ Exploit ระบบเป้าหมายจากช่องโหว่ต่าง ๆ

๔.๔ การรักษาช่องทางเข้าถึง (Maintaining Access)

เป็นการเปิดช่องโหว่ทิ้งไว้ในระบบเป้าหมาย เพื่อใช้เป็นช่องทางสำหรับสร้างโอกาสการเข้าปฏิบัติการครั้งต่อไป ด้วยวิธีการฝังทางลับ (Backdoor) ไว้ในระบบที่เป็นเป้าหมาย เช่น การทำ Bind Shell หรือ Reverse Shell

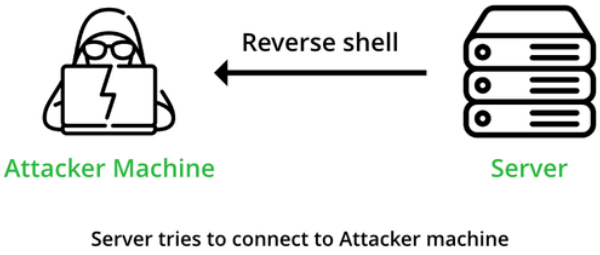
Shell เป็นโปรแกรมเพื่อสั่งการระบบปฏิบัติการ โดยจะทำหน้าที่ในลักษณะเป็นส่วนต่อประสานระหว่างผู้ใช้งานกับระบบปฏิบัติการ โดยสามารถเรียกใช้งานและสั่งการได้ผ่าน Terminal หรือ Command Line ตัวอย่างรูปแบบ Shell ที่เป็นที่นิยม เช่น Windows PowerShell Windows Command Prompt bash sh dash Born และ Korn เป็นต้น

๔.๔.๑ Bind Shell ลักษณะของการทำ Bind Shell นั้น เป้าหมายจะทำการเปิดช่องทางติดต่อไว้เพื่อให้ฝ่ายโจมตีติดต่อเข้าไปเพื่อทำการสั่งการและควบคุม



รูปที่ ๖๕ ภาพแสดงการทำ Bind Shell

๔.๔.๒ Reverse Shell เป็นลักษณะของการเปิดช่องทางการติดต่อไว้ที่เครื่องสั่งการและควบคุม เมื่อเป้าหมายได้เรียกใช้คำสั่ง ระบบเป้าหมายจะพยายามติดต่อกลับไปหาเครื่องสั่งการและควบคุม



รูปที่ ๖๖ ภาพแสดงการทำ Reverse shell

ข้อแตกต่างระหว่าง Bind Shell และ Reverse Shell

	Bind Shell	Reverse Shell
๑	ทำการเปิดช่องทางการติดต่อไว้ที่เครื่องเป้าหมาย เพื่อให้ผู้โจมตีติดต่อเข้าไปทำการสั่งการและควบคุมได้	ทำการเปิดช่องทางการติดต่อไว้ที่เครื่องผู้โจมตี เพื่อให้เป้าหมายติดต่อกลับไป ทำให้สามารถสั่งการและควบคุมได้
๒	ผู้โจมตีพบพอร์ตที่เปิดอยู่บน เครื่องเป้าหมาย จากนั้นพยายามติดต่อกับพอร์ตนั้น	ผู้โจมตีจะเปิดพอร์ตการเชื่อมต่อ เพื่อให้เป้าหมายสามารถเชื่อมต่อกับพอร์ตนั้น
๓	ผู้โจมตีต้องทราบข้อมูลหมายเลข Ip Address ของเป้าหมาย	ผู้โจมตีไม่จำเป็นต้องทราบหมายเลข Ip Address ของเป้าหมาย
๔	มีโอกาสที่จะโจมตีไม่สำเร็จ เนื่องจากไฟล์วอลสมัยใหม่มักจะมีมาตรการป้องกันการติดต่อจากภายนอก	มีโอกาสที่จะโจมตีสำเร็จ เนื่องจากวิธีนี้สามารถ bypass ผ่านการป้องกันของไฟล์วอลได้

๔.๕ การลบร่องรอยการโจมตี (Covering Tracks)

เป็นการลบร่องรอยของการโจมตี หรือการกลบเกลื่อนบิดเบือนร่องรอยของการเข้าโจมตีระบบ เพื่อไม่ให้ฝ่ายตรงข้ามทราบว่าถูกโจมตี และทำให้ไม่สามารถสืบย้อนกลับมาถึงผู้โจมตีได้

บรรณานุกรม

“พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒” (๒๗ พฤษภาคม ๒๕๖๒). ราชกิจจานุเบกษา, เล่ม ๑๓๖ ตอนที่ ๖๙ ก, น. ๒๐.

“พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒” (๒๗ พฤษภาคม ๒๕๖๒). ราชกิจจานุเบกษา, เล่ม ๑๓๖ ตอนที่ ๖๙ ก, น. ๕๒.

กองทัพอากาศ. หลักนิยมกองทัพอากาศ พ.ศ.๒๕๖๒ (2562). ไทย. สืบค้น ๑๔ กันยายน ๒๕๖๓ จาก https://www.rtaf.mi.th/th/Documents/Publication/RTAF_Doctrine_2020.pdf

กองทัพอากาศ กรมเทคโนโลยีสารสนเทศและการสื่อสารทหารอากาศ. ระเบียบ ทอ. ว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พ.ศ.๒๕๖๓ (2563). ไทย. สืบค้น ๑๔ กันยายน ๒๕๖๓ จาก http://dict.km.rtaf.mi.th/Home/Page/19?menuID=4736&contentID=30257