วารสารปราชญ์ประชาคม
ปีที่ 1 ฉบับที่ 6 พฤศจิกายน-ธันวาคม 2566
Journal of Scholar Community
Vol.1 No.6 November-December 2023

มหา ยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์ประเทศไทยของ สกมช.

ธวัชชัย สุขสาย [1*]
วสันต์ เกิดสวัสดิ์ [2]

รับบทความ: 12 พฤศจิกายน 2566 แก้ไขบทความ: 14 ธันวาคม 2566 ตอบรับบทความ: 22 ธันวาคม 2566

บทคัดย่อ

บทความวิชาการนี้มุ่งนำเสนอการดำเนินงานในการรักษาความมั่นคงปลอดภัยไซเบอร์ของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ มีตัวย่อว่า สกมช. มีชื่อภาษาอังกฤษ “National Cyber Security Agency (NCSA)” เป็นหน่วยงานของรัฐในรูปแบบองค์การมหาชน ตามที่พระราชบัญญัติบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ให้จัดตั้ง สกมช. เป็นหน่วยงานของรัฐที่กำหนดนโยบาย มาตรการ แนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานภาครัฐและภาคเอกชนที่เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์มิให้เกิดผลกระทบและสร้างความเดือดร้อนต่อประชาชน ซึ่ง สกมช. มีหน้าที่รับผิดชอบงานตามพระราชบัญญัติ ประสานงานร่วมกันทั้งภาครัฐและเอกชน รวมถึงกำหนดนโยบาย ระเบียบ มาตรฐานขั้นต่ำ แนวทางความปลอดภัยสำหรับหน่วยงานภาครัฐ ป้องกันรับมือภัยคุกคามไซเบอร์ ตลอดจนความมั่นคงของรัฐและความสงบเรียบร้อยของประเทศ โดยมหายุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์ ประกอบด้วย การขับเคลื่อนนโยบายและแผนด้านความมั่นคงปลอดภัยไซเบอร์ การจัดทำกฎหมายลำดับรองประกาศระเบียบที่เกี่ยวข้อง การส่งเสริมความร่วมมือกับหน่วยงาน การเฝ้าระวังตอบโต้ภัยคุกคามทางไซเบอร์ และการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ ด้วยการกำหนดมหายุทธศาสตร์ดังกล่าวจะสามารถนำพาองค์การสู่เป้าหมายและเกิดความมั่นคงปลอดภัยทางไซเบอร์ยั่งยืนได้

คำสำคัญ: ความมั่นคงปลอดภัยไซเบอร์ สกมช. ยุทธศาสตร์ด้านไซเบอร์

[1-2] นักศึกษาปริญญาโท สาขาวิชาการจัดการความปลอดภัย คณะตำรวจศาสตร์ โรงเรียนนายร้อยตำรวจ
[*] อีเมล: np2915@gmail.com

NCSA's Great Strategy for Cybersecurity in Thailand

Thawatchai Suksai [1*]
Vasan Kirdsawasd [2]

Abstract

This academic article aims to present the operations in maintaining cyber security of the office of the National Cyber Security Commission, abbreviated as NCSA. Its name in English is "National Cyber Security Agency (NCSA)". Government agencies in the form of public organizations according to the cybersecurity act of 2019, the NCSA is established as a government agency that sets policies, measures, and guidelines for maintaining cybersecurity for government agencies and the private sector that are important infrastructure. information in preventing, dealing with, and reducing risks from cyber threats in order not to have an impact and cause distress to the people, the NCSA is responsible for the work according to the act. Coordinate together with both the public and private sectors. Including setting policies, regulations, minimum standards, and safety guidelines for government agencies. Protect against cyber threats as well as the security of the state and peace and order of the country the grand strategy for maintaining cybersecurity consists of driving cybersecurity policies and plans. Preparation of secondary laws, announcements of relevant regulations promoting cooperation with agencies surveillance and response to cyber threats and development of cybersecurity personnel by setting such a strategic strategy, the organization will be able to lead the organization towards its goals and achieve sustainable cybersecurity.

Keywords: Cybersecurity, NCSA, Cyber Strategy

[1-2] M.P.A. (Security Management) Faculty of Police Science Royal Police Cadet Academy
[*] Email: np2915@gmail.com

บทนำ

ปัจจุบันเทคโนโลยีไซเบอร์ นั้นมีอยู่ในอุปกรณ์หรือผลิตภัณฑ์เครื่องมือเครื่องใช้แทบทุกอย่าง และแนวโน้มของการสร้างสรรค์สิ่งต่าง ๆ ได้ถูกแปลงให้อยู่ในรูปแบบดิจิทัลที่มีความต้องการเชื่อมต่อทางอินเตอร์เน็ตมากขึ้น เพื่อที่จะทำให้เกิดการบูรณาการเทคโนโลยีสารสนเทศดังกล่าว เข้าไปเป็นส่วนหนึ่งของผลิตภัณฑ์ต่าง ๆ ซึ่งแต่เดิมในอดีตสามารถใช้งานได้โดยไม่จำเป็นต้องมีการเชื่อมต่ออินเตอร์เน็ตเช่น สาธารณูปโภคต่าง ๆ รวมทั้งปฏิบัติการทางทหารและการขนส่ง ฯลฯ การเติบโตของสังคมข้อมูลข่าวสารในปัจจุบันทำให้ด้านสาธารณูปโภคที่สำคัญเช่น ประปา ไฟฟ้า ระบบควบคุมการจราจร หรือระบบโทรคมนาคม ต้องพึ่งพาการเชื่อมต่อหรือดำเนินการของเทคโนโลยีไซเบอร์ เพื่อความมีเสถียรภาพ แต่อย่างไรก็ดี เทคโนโลยีไซเบอร์ ดังกล่าวนี้ก็มาพร้อมกับภัยอันตรายที่ร้ายแรงรูปแบบใหม่ ดังนั้นหากมีการจู่โจมโครงสร้างพื้นฐานสำคัญทางสารสนเทศและบริการ จึงเป็นการสั่นคลอนความมั่นคงของสังคมและถือว่าเป็นอาชญากรรมทางไซเบอร์

ภัยคุกคามทางไซเบอร์ (Cyber Threat) เกิดขึ้นในหลายรูปแบบ และถูกสร้างขึ้นใหม่ในทุกวัน เช่น 1) โปรแกรมหรือซอฟต์แวร์ (Malicious Code) เพื่อทำให้เกิดความขัดข้องหรือเสียหายกับระบบที่โปรแกรม หรือซอฟต์แวร์ที่มีมัลแวร์ติดตั้งอยู่ เช่น Virus, Worm, Trojan หรือ Spyware ต่าง ๆ ส่งผลให้อาจเผลอดาวน์โหลดมัลแวร์เข้าสู่ระบบจนทำให้ระบบสารสนเทศเกิดความเสียหาย เช่น ถูกเรียกค่าไถ่ข้อมูล ไฟล์ข้อมูลรั่วไหล ไปจนถึงใช้งานระบบไม่ได้ 2) Availability ได้แก่ DDoS (Distributed Denial of Service) Attack คือ การที่ผู้ไม่ประสงค์ดีใช้เครื่องมือเพื่อสร้างปริมาณ Traffic/Packet ที่ผิดปกติส่งเข้ามาก่อกวนในระบบ Network (Flood Network) จนส่งผลกระทบให้ระบบตอบสนองได้ช้าลงหรือหยุดทำงาน โดยมีสาเหตุมาจากผู้ไม่ประสงค์ดี สามารถเข้าถึงเครื่องดังกล่าว และใช้เป็นเครื่องมือในการโจมตี ส่วนใหญ่เริ่มมาจากการติดมัลแวร์และถูก compromised ผ่านช่องโหว่ (Vulnerability) และ 3) Intrusion Attempt การบุกรุกหรือเจาะระบบผ่านช่องทางการตรวจสอบบัญชีชื่อผู้ใช้งานและรหัสผ่าน (Login) ด้วยวิธีการเดาสุ่มข้อมูล หรือวิธีการทดสอบรหัสผ่านทุกค่า (Brute Force) ตัวอย่างของภัยคุกคามในรูปแบบนี้ ได้แก่ Web exploit, SQL-injection, Cross Site Scripting (XSS) และ Brute Force Attacks (ศูนย์ CSOC NT, 2565)

ในขณะที่ภัยคุกคามไซเบอร์ มีรูปแบบที่เปลี่ยนแปลงไปจากอดีตและมีแนวโน้มขยายตัวอย่างรวดเร็วและทวีความรุนแรงมากขึ้นเรื่อย ๆ สกมช. ซึ่งเป็นหน่วยงานหลักของประเทศที่มีหน้าที่เสนอแนะและขับเคลื่อนนโยบาย แผน ยุทธศาสตร์ และปรับปรุงกฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมทั้ง ศึกษาวิจัย กำหนดแนวทางมาตรฐาน มาตรการที่เกี่ยวข้องให้สอดคล้องกับสถานการณ์ทั้งในปัจจุบันและอนาคต จึงมอบหมายภารกิจสำคัญให้กับ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (Thailand Computer Emergency Response Team - ThaiCERT) ซึ่งเป็นหน่วยงานในสังกัด ให้ทำงานเชิงรุกเพื่อเป็นกลไกสำคัญของประเทศด้านความมั่นคงปลอดภัยไซเบอร์ ทั้งการตอบสนองและจัดการกับสถานการณ์ด้านความมั่นคงปลอดภัยการสนับสนุนที่จำเป็นและให้คำแนะนำในการแก้ไข

ภัยคุกคามแก่หน่วยงานต่าง ๆ รวมทั้งติดตามและเผยแพร่ข่าวสารและเหตุการณ์ทางด้านความมั่นคงปลอดภัยไซเบอร์ต่อสาธารณชน ตลอดจนทำการศึกษาและพัฒนาเครื่องมือและแนวทางต่าง ๆ ในการปฏิบัติเพื่อเพิ่มความมั่นคงปลอดภัยในการใช้ระบบสารสนเทศและเครือข่ายอินเทอร์เน็ต (Thailand Computer Emergency Response Team, ม.ป.ป.)

นอกจากนี้ Thai CERT ได้เผยแพร่ผลจากการแจ้งเหตุและสถิติภัยด้านความมั่นคงปลอดภัยไซเบอร์ในปี พ.ศ. 2565 เพื่อวิเคราะห์สถานการณ์ อุปสรรค และการรับมือภัยคุกคามไซเบอร์ของประเทศในภาพรวม พบว่าการรับมือภัยคุกคามไซเบอร์ จึงมีความจำเป็นในการวางนโยบายสนับสนุนเพื่อเสริมสร้างศักยภาพในด้านนี้อย่างเข็มแข็ง รายละเอียดตามตารางที่ 1

ตารางที่ 1 สถิติภัยคุกคามประจำปี พ.ศ. 2565

ประเภทภัยคุกคาม	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	ต.ค.	พ.ย.	ธ.ค.	รวม
Abusive Content	7	0	1	1	4	6	4	6	6	3	3	0	41
Availability	0	0	0	0	0	0	0	3	7	2	2	0	14
Fraud	6	9	10	6	9	1	0	0	3	3	3	0	44
Information Gathering	0	9	4	1	0	0	0	0	2	2	0	0	14
Information Security	1	6	1	0	1	0	1	2	1	0	0	0	13
Intrusion Attempts	17	7	6	22	6	29	33	18	18	26	25	0	207
Intrusions	23	4	13	4	1	2	0	17	24	17	17	0	122
Malicious Code	111	66	201	126	136	151	50	79	94	52	121	0	1187
Vulnerability	55	52	106	80	45	48	24	43	57	60	67	0	637
Other	0	0	0	0	0	0	0	0	0	0	0	0	0

จากสถิติภัยคุกคาม ดังตารางที่ 1 ซึ่งเคยส่งผลกระทบ เช่น ปี 2563 โรงพยาบาลสระบุรี โดนโจรไซเบอร์แฮกข้อมูล พร้อมเรียกค่าไถ่ข้อมูลคนไข้ชื่อ voidcrypt/spade ทำให้ระบบการจัดการและรักษาพยาบาล รวมถึงข้อมูลระบบสนับสนุนบริการทั้งหมดได้รับความเสียหาย การโจมตีโรงไฟฟ้าในยูเครนผ่าน Phishing Email ทำให้ประชาชนกว่า 2 แสนคน ไม่มีไฟฟ้าใช้นานถึง 6 ชั่วโมง (BBC NEWS ไทย, 2022) และการโจมตีเรียกค่าไถ่ Colonial Pipeline บริษัทท่อส่งน้ำมันรายใหญ่ในสหรัฐอเมริกา ทำให้การส่งน้ำมัน

ทางท่อต้องหยุดชะงักลง (แมรี-แอนน์ รัสสัน, 2021) สอดคล้องกับการรายรายของ แคสเปอร์สกี้ ตรวจพบคอมพิวเตอร์จำนวนเกือบครึ่งในระบบ ICS องค์กรด้านพลังงาน โดนคุกคามทางไซเบอร์ โดยภัยร้าย 3 อันดับแรกที่โจมตี คือ เวิร์ม สปายแวร์ และการขุดเงินคริปโต ในช่วงหกเดือนแรกของปี 2562 โซลูชั่นของแคสเปอร์สกี้ ตรวจพบว่า เครื่องคอมพิวเตอร์ในระบบการควบคุมอุตสาหกรรม (Industrial Control System หรือ ICS) จำนวน 41.6% ในภาคพลังงานโดนคุกคามทางไซเบอร์ (Kaspersky Industrial Control Systems Cyber Emergency Response Team, 2019)

ดังนั้นรัฐบาลตระหนักถึงภัยคุกคามทางไซเบอร์เพื่อเตรียมความพร้อมรับมือกับภัยคุกคาม จึงได้บัญญัติ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 เพื่อรับมือ ป้องกัน และลดความเสี่ยงภัยคุกคามทางไซเบอร์ ที่จะกระทบหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ อันจะส่งผลกระทบต่อการให้บริการประชาชนในวงกว้างได้ สกมช. เป็นหน่วยงานกลางที่ขับเคลื่อนการทำงานด้านการดูแลและรับมือภัยคุกคามทางไซเบอร์ รวมทั้งให้ความช่วยเหลือสนับสนุนหน่วยงานภาครัฐ และหน่วยงานที่เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศเพื่อลดความเสี่ยงและบรรเทาความเสียหายจากภัยคุกคามดังกล่าว

บทความเรื่อง มหายุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์ประเทศไทยของ สกมช. เป็นการศึกษาเชิงเอกสาร เรียบเรียง สังเคราะห์ และนำเสนอบทบาท สกมช. ในปฏิบัติการ เพื่อป้องกัน รับมือและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์โดยมีการดำเนินการ ดังนี้ การขับเคลื่อนนโยบายและแผนด้านความมั่นคงปลอดภัยไซเบอร์ การจัดทำกฎหมายลำดับรอง ภายใต้พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 การส่งเสริมความร่วมมือกับหน่วยงานองค์การทั้งภายในประเทศและระหว่างประเทศ การเฝ้าระวัง รับมือภัยคุกคามทางไซเบอร์ และการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์และสร้างการตระหนักรู้ให้กับประชาชน

มหายุทธศาสตร์ที่ 1 การขับเคลื่อนนโยบายและแผนด้านความมั่นคงปลอดภัยไซเบอร์

การขับเคลื่อนนโยบายแลแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 – 2570) นโยบายบริการจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ (ราชกิจจานุเบกษา,2564, 1-48) เป็นแนวทางสำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยมีประสิทธิภาพและเป็นไปในทิศทางเดียวกัน ดังนี้

1. สร้างขีดความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ (บุคลากร องค์ความรู้ และเทคโนโลยี) เพื่อเสริมสร้างขีดความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ ของประเทศ โดยบูรณาการ บุคลากร องค์ความรู้ และเทคโนโลยี นำไปสู่การพัฒนาผลิตภัณฑ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่เป็นนวัตกรรมของประเทศ มีเป้าหมาย 1) พัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์เพื่อรองรับความต้องการของประเทศ 2) ส่งเสริมให้บุคลากรทุกภาคส่วนมีความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ 3)

ส่งเสริมให้เกิดการมีส่วนร่วมในการสร้างความแข็งแกร่งด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศ และ 4) ส่งเสริมการพัฒนาผลิตภัณฑ์ด้านความมั่นคงปลอดภัยไซเบอร์ให้เป็นนวัตกรรมของประเทศ กลยุทธ์ที่ 1 เพิ่มบุคลากรที่มีความสามารถด้านความมั่นคงปลอดภัยไซเบอร์ พัฒนาหลักสูตรการเรียนการสอนด้านความมั่นคงปลอดภัยไซเบอร์ทั้งภาคทฤษฎีและภาคปฏิบัติ เป็นสาขาเฉพาะทางในระดับอุดมศึกษา รองรับความต้องการของภาคอุตสาหกรรมที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ พัฒนาทักษะและฝึกอบรมบุคลากรด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ทั้งในระดับผู้บริหารและผู้ปฏิบัติงาน กลยุทธ์ที่ 2 สร้างความตระหนักรู้และทักษะด้านความมั่นคงปลอดภัยไซเบอร์ สร้างความตระหนักและการรู้เท่าทัน ด้านความมั่นคงปลอดภัยไซเบอร์ ส่งเสริมให้เกิดการบูรณาการหลักสูตรเกี่ยวกับการตระหนักรู้และทักษะด้านความมั่นคงปลอดภัยไซเบอร์ในระบบการศึกษาทุกระดับชั้น กลยุทธ์ที่ 3 ส่งเสริมการวิจัยและพัฒนาและนวัตกรรมด้านความมั่นคงปลอดภัยไซเบอร์ ส่งเสริมการศึกษา วิจัย พัฒนาและสร้างนวัตกรรมด้านความมั่นคงปลอดภัยไซเบอร์ ส่งเสริมความร่วมมือด้านวิจัยและพัฒนา ระหว่างหน่วยงานวิจัยในประเทศและต่างประเทศ ส่งเสริมการลงทุนด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ส่งเสริมการพัฒนาผลิตภัณฑ์ด้านความมั่นคงปลอดภัยไซเบอร์ให้เป็นนวัตกรรม และสามารถต่อยอดเชิงพาณิชย์ได้

2. บูรณาการความร่วมมือเพื่อเตรียมความพร้อมในการรับมือทางไซเบอร์และฟื้นคืนสู่สภาพปกติได้ (Partnership) เพื่อบูรณาการความร่วมมือในการเตรียมความพร้อมสำหรับการรับมือภัยคุกคามทางไซเบอร์และการฟื้นคืนบริการที่สำคัญสู่สภาพปกติได้อย่างรวดเร็วกับทุกภาคส่วนทั้งภายในประเทศและระหว่างประเทศ กลยุทธ์ที่ 1 ส่งเสริมและสนับสนุนความร่วมมือระหว่างภาครัฐและภาคเอกชน ระบุถึงการมีส่วนร่วมของผู้มีส่วนได้ส่วนเสีย เพื่อสร้างความร่วมมือระหว่างหน่วยงานภาครัฐและภาคเอกชน กำหนดโครงสร้างการกำกับดูแลที่ชัดเจน และกำหนดกลไกที่ทำหน้าที่สร้างความร่วมมือและประสานงานระหว่างหน่วยงานภาครัฐและภาคเอกชน สร้างความร่วมมือระหว่างหน่วยงานภาครัฐ รักษาสมดุลระหว่างความมั่นคงปลอดภัยทางไซเบอร์และการคุ้มครองข้อมูลส่วนบุคคล สนับสนุนการพัฒนาศักยภาพบุคลากรภาครัฐที่เกี่ยวข้องกับการบังคับใช้กฎหมายด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ กลยุทธ์ที่ 2 ประสานความร่วมมือระหว่างประเทศเพื่อรับมือภัยคุกคาม กำหนดให้การรักษาความมั่นคงปลอดภัยไซเบอร์เป็นประเด็นสำคัญ ในการกำหนดนโยบายด้านการต่างประเทศ มีส่วนร่วมในเวทีการประชุมระหว่างประเทศด้านความมั่นคงปลอดภัยไซเบอร์ สร้างความร่วมมือด้านความมั่นคงปลอดภัยไซเบอร์ระหว่างประเทศในทุกมิติ พัฒนายุทธศาสตร์ของประเทศให้สอดคล้องตามแนวปฏิบัติสากล สนับสนุนการพัฒนาศักยภาพบุคลากรภาครัฐที่เกี่ยวข้องกับการบังคับใช้กฎหมายระหว่างประเทศด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และกฎหมายอื่นที่เกี่ยวข้องเพื่อให้สามารถปฏิบัติงานร่วมกับหน่วยงานที่เกี่ยวข้องในระดับนานาชาติได้อย่างมีประสิทธิภาพ

3. สร้างบริการภาครัฐ และโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้มีความมั่นคงปลอดภัยไซเบอร์และฟื้นคืนสู่สภาพปกติได้ (Resilience) เพื่อส่งเสริมบริการภาครัฐและโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้มีความมั่นคงปลอดภัยไซเบอร์ และสามารถฟื้นคืนบริการที่สำคัญสู่สภาพปกติได้ มีเป้าหมาย 1) มีการ

กำหนดโครงสร้างการกำกับดูแลและกรอบกฎหมายสำหรับหน่วยงานภาครัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ 2) มีการกำหนดมาตรการการรักษาความมั่นคงปลอดภัยขั้นต่ำสำหรับหน่วยงานภาครัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ 3) มีการปกป้องระบบข้อมูลและเครือข่ายของหน่วยงานภาครัฐ กลยุทธ์ที่ 1 กำหนดมาตรการการรักษาความมั่นคงปลอดภัยขั้นต่ำสำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (Critical Information Infrastructure : CII) ปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยระบุถึงประเภทของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และกำหนดมาตรการลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ กำหนดหลักเกณฑ์การรักษาความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำ ส่งเสริมและสนับสนุนหลักการออกแบบระบบอย่างมั่นคงปลอดภัย (Security By Design) ส่งเสริมและสนับสนุนให้บุคลากรทุกระดับมีความตระหนักรู้ในการรักษาความมั่นคงปลอดภัยไซเบอร์ กลยุทธ์ที่ 2 กำหนดโครงสร้างการกำกับดูแลและกรอบกฎหมายสำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ กำหนดวิธีการบริหารจัดการความเสี่ยงเพื่อปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พัฒนากลไกแนวทางการกำกับดูแลของหน่วยงานโครงสร้างพื้นฐาน สำคัญทางสารสนเทศ และพิจารณากำหนดให้ ข้อมูลและบริการคลาวด์ (Data & Cloud Computing) เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่ต้องมีการกำกับดูแลในระยะต่อไป พัฒนากฎหมาย กฎระเบียบที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ให้ทันสมัย กลยุทธ์ที่ 3 ปกป้องระบบข้อมูลและเครือข่ายของหน่วยงานภาครัฐ กำหนดให้หน่วยงานภาครัฐปฏิบัติตามนโยบายมาตรฐานการรักษาความมั่นคงปลอดภัยขั้นต่ำ กำหนดให้มีการประเมินความเสี่ยงจากการใช้เทคโนโลยีเพื่อให้เกิดความมั่นคงปลอดภัยตั้งแต่เริ่มต้นการใช้งาน กำหนดมุมมองการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ร่วมกัน เตรียมความพร้อมด้านบุคลากร ข้อมูล เทคโนโลยี และกระบวนการเพื่อรับมือภัยคุกคามไซเบอร์สมัยใหม่

4. สร้างศักยภาพของหน่วยงานระดับชาติให้มีคุณภาพและมาตรฐาน (Standard) วัตถุประสงค์มุ่งสร้างศักยภาพของหน่วยงานระดับชาติให้มีคุณภาพและมาตรฐาน เพื่อให้การบริหารจัดการด้านความมั่นคงปลอดภัยไซเบอร์เป็นไปอย่างมีประสิทธิภาพ มีเป้าหมาย 1) มีการบริหารจัดการการรักษาความมั่นคงปลอดภัยไซเบอร์แบบบูรณาการในระดับชาติ 2) มีหน่วยงานหลักและหน่วยงานรองที่มีคุณภาพและมาตรฐาน สามารถทำงานร่วมกันแบบบูรณาการได้ 3) มีมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์มีการแบ่งปันข้อมูลภัยคุกคามทางไซเบอร์อย่างมีประสิทธิภาพ และ 4) หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศมีมาตรการการรักษาความมั่นคงปลอดภัยไซเบอร์ที่เข้มแข็ง กลยุทธ์ที่ 1 เพิ่มขีดความสามารถในการรับมือและตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ พิจารณาศึกษาและทบทวนนโยบาย กฎหมาย และขีดความสามารถด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีอยู่ในปัจจุบัน เพื่อกำหนดแนวทางการพัฒนาการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ กำหนดกลไกการขับเคลื่อนยุทธศาสตร์ กระบวนการตัดสินใจ การแบ่งหน้าที่ความรับผิดชอบ การประสานความร่วมมือกับหน่วยงานที่เกี่ยวข้อง แนวทางการดำเนินการและการติดตามประเมินผลการปฏิบัติงาน ส่งเสริมบุคลากร

(People) กระบวนการ (Process) และเทคโนโลยี(Technology) ให้มีการพัฒนาศักยภาพ คุณภาพ และมาตรฐาน เพื่อสร้างความเชื่อมั่นให้กับผู้มีส่วนได้เสียและนำมาตรฐานและแนวปฏิบัติที่ดีมาใช้ในการปฏิบัติงาน โดยอาจดำเนินการเพื่อให้ได้รับใบรับรอง(Certification) และการรับรอง (Accreditation) กลยุทธ์ที่ 2 ส่งเสริมและสนับสนุนการแบ่งปันข้อมูลภัยคุกคาม สร้างกลไกการแลกเปลี่ยนข้อมูล ข่าวกรอง และองค์ความรู้ด้านภัยคุกคามทางไซเบอร์ สร้างกลไกการรายงานเหตุการณ์ภัยคุกคามทางไซเบอร์ สร้างการมีส่วนร่วมของทุกภาคส่วนในการแบ่งปันข้อมูลภัยคุกคามทางไซเบอร์ กลยุทธ์ที่ 3 ส่งเสริมและสนับสนุนความมั่นคงปลอดภัยทางไซเบอร์ สร้างความเชื่อมั่นให้กับทุกภาคส่วนในการรักษาความมั่นคงปลอดภัยไซเบอร์ ยกระดับการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานที่ให้บริการที่สำคัญ ส่งเสริมและสนับสนุนให้เกิดบริการด้านความมั่นคงปลอดภัยไซเบอร์

มหายุทธศาสตร์ที่ 2 การจัดทำกฎหมายลำดับรอง ภายใต้พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

1. ประกาศ กมช. เรื่อง การกำหนดหลักเกณฑ์ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (ราชกิจจานุเบกษา, 2564) โดยหน่วยงานที่มีภารกิจหรือให้บริการที่เข้าลักษณะเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการควบคุมหรือกำกับดูแล มีดังนี้ 1) ด้านความมั่นคงของรัฐ มีภารกิจเกี่ยวข้องกับการป้องกันประเทศ ภารกิจเกี่ยวข้องกับการบังคับใช้กฎหมาย ภารกิจเกี่ยวข้องกับความมั่นคงอื่น ๆ 2) ด้านบริการภาครัฐที่สำคัญ บริการด้านการเงิน บริการโดยตรงแก่ประชาชน บริการที่เกี่ยวข้องกับการแจ้งเตือน 3) ด้านการเงินการธนาคาร การให้บริการทางการเงิน บริการที่เกี่ยวข้องกับตลาดทุน 4) ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม การให้บริการโทรคมนาคม 5) ด้านการขนส่งและโลจิสติกส์ การให้บริการขนส่งทางบก การให้บริการขนส่งทางราง การให้บริการขนส่งทางน้ำ การให้บริการขนส่งทางอากาศ 6) ด้านพลังงานและสาธารณูปโภค การให้บริการด้านไฟฟ้า การให้บริการด้านปิโตรเลียมและก๊าซ การให้บริการด้านประปา 7) ด้านสาธารณสุข การให้บริการสุขภาพในโรงพยาบาล การให้บริการสุขภาพระหว่างโรงพยาบาล การให้บริการด้านยา เวชภัณฑ์ และเครื่องมือแพทย์ มีการให้บริการตรวจวิเคราะห์ทางการแพทย์และรังสีวิทยา การให้บริการข้อมูลสุขภาพดิจิทัล

2. ประกาศ กมช. เรื่องลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ (ราชกิจจานุเบกษา, 2564) ในการพิจารณาระบุระดับของภัยคุกคามทางไซเบอร์ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศควรพิจารณาจากเหตุการณ์ต่าง ๆ ที่เป็นพฤติการณ์แวดล้อมผลกระทบที่เกิดขึ้น ความเสี่ยงหรือแนวโน้มที่อาจเกิดขึ้นจากภัยคุกคามทางไซเบอร์ในกรณีต่าง ๆ เพื่อพิจารณาว่าลักษณะของภัยคุกคามทางไซเบอร์นั้นอยู่ในระดับใด โดยการจำแนกหมวดหมู่ของภัยคุกคามทางไซเบอร์ หมวด 0 เหตุการณ์จำลอง และ การฝึกจู่โจม ของหน่วยงานเอง (Training and Exercises) หมวด 1 การพยายามเข้าถึงระบบที่ไม่สำเร็จ (Unsuccessful Activity Attempt) หมวด 2 การ

พยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance) หมวด 3 การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยที่หน่วยงานกำหนด (Non-Compliance Activity) หมวด 4 การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic) หมวด 5 การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion) หมวด 6 การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion) หมวด 7 การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service) หมวด 8 เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating) และ หมวด 9 เหตุการณ์ผิดปกติที่ได้รับการวิเคราะห์แล้วว่าไม่ใช่เหตุการณ์ที่เป็นภัยคุกคาม (Explained Anomaly)

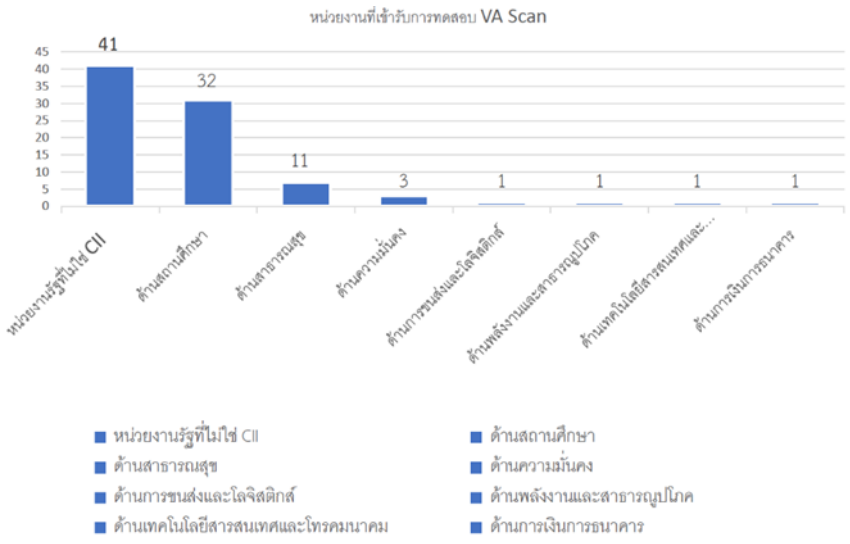
3. ประกาศ กมช. เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (ราชกิจจานุเบกษา, 2564) โดยกำหนดกรอบและวิธีปฏิบัติสำหรับการทำงานด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Framework) ดังนี้ 1) Identify คือ การระบุและเข้าใจถึงบริบทต่าง ๆ เพื่อการบริหารจัดการความเสี่ยง ที่จะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล 2) Protect คือ การวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน 3) Detect คือ มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ และ 4) Response คือ มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์5) Recover คือ มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์

มหายุทธศาสตร์ที่ 3 การส่งเสริมความร่วมมือกับหน่วยงานองค์การทั้งภายในประเทศและระหว่างประเทศ

สกมช มีการดำเนินงาน ดังนี้ 1) การดำเนินงานภายใต้กรอบความร่วมมือทวิภาคและพหุภาคี โดยการส่งเสริมความร่วมมือระหว่างประเทศ ทั้งสิ้น 13 ประเทศ ได้แก่ สาธารณรัฐเช็ก สหราชอาณาจักร สหรัฐอเมริการ อิสราเอล อินเดีย ออสเตรเลีย สหรัฐอาหรับเอมิเรตส์ สิงคโปร์ นิวซีแลนด์ สาธารณรัฐประชาชาจีน ญี่ปุ่น สาธารณรัฐเกาหลี รัสเซีย เข้าร่วมประชุมหารือ ประชุมเชิงปฏิบัติการ อบรม สัมมนา เพื่อส่งเสริมและสนับสนุนความร่วมมือระหว่างประเทศด้านความมั่นคงความปลอดภัยไซเบอร์ จำนวน 197 ครั้ง 2) การสนับสนุนการแถลงผลสัมฤทธิ์คณะกรรมาธิการการทหารและความมั่นคงของรัฐ วุฒิสภา และสำนักงานสภาความมั่นคงแห่งชาติ 3) การสร้างเครือข่ายสื่อมวลชนผสานความร่วมมือด้านการรักษาความมันคงปลอดภัยไซเบอร์ร่วมกับชมรมเครือข่ายนักสื่อสารข้อมูลเชิงลึกแห่งประเทศไทย และ 4) การแต่งตั้งคณะทำงานจัดทำแผนรับมือเหตุภัยคุกคามทางโซเบอร์

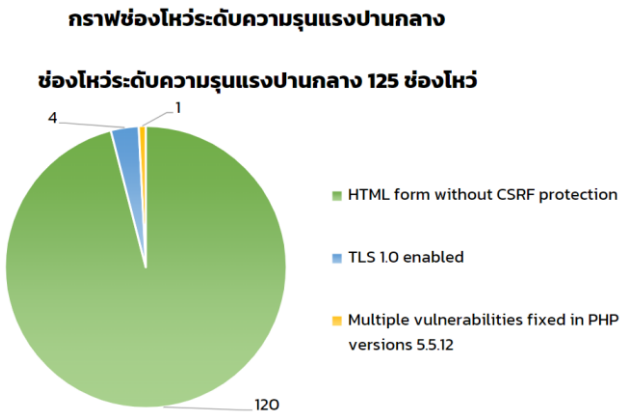
มหายุทธศาสตร์ที่ 4 การเฝ้าระวัง รับมือภัยคุกคามทางไซเบอร์

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ศปช.) ภายใต้ (สกมช.) มีหน้าที่เฝ้าระวังความเสี่ยงในการเกิดภัยคุกคามทางไซเบอร์ ติดตาม วิเคราะห์และประมวลผลข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ และการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์ให้กับหน่วยงานต่าง ๆ อย่างเป็นทางการ โดยมีการแจ้งเตือนข้อมูลข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์การเผยแพร่ข้อมูลภัยคุกคามทางไซเบอร์และข่าวสารที่เป็นประโยชน์ต่อสาธารณะ การทดสอบความมั่นคงปลอดภัยของระบบเครื่องแม่ข่ายและเว็บไซต์ การแจ้งเตือนเหตุการณ์และให้คำแนะนำไปแก้ปัญหา การตอบสนองและรับมือภัยคุกคามไซเบอร์ และประสานงานเพื่อระงับการเผยแพร่เว็บไซต์ปลอมหรือเลียนแบบ เช่น VA Scan (Vulnerability Assessment) คือ วิธีการตรวจสอบ ค้นหาช่องโหว่ต่าง ๆ ด้านความปลอดภัยอย่างเป็นระบบ ทำให้เราสามารถประเมินวิเคราะห์ได้ว่าระบบของเรานั้นจะถูกโจมตีผ่านช่องทางใด ในรูปแบบใดได้บ้าง ดังภาพที่ 1 และ การวิเคราะห์รูปแบบ Vulnerability Assessment นั้นจะดำเนินการสแกนตรวจสอบตั้งแต่การทำงานของ System, Server, ระบบ Network ต่าง ๆ ระบบ หรือ อุปกรณ์รักษาความปลอดภัย จนไปถึง แอปพลิเคชันต่าง ๆ ที่สร้างขึ้น หรือ ที่ใช้งานว่ามีช่องโหว่อะไรบ้าง ดังภาพที่ 2



ภาพที่ 1 ระดับความรุนแรงของช่องโหว่ ต.ค. 65 - ก.ย. 66

ที่มา: https://drive.ncsa.or.th/s/Fi5sYPYCocsOOoT



ภาพที่ 2 ระดับความรุนแรงของช่องโหว่

ที่มา: https://drive.ncsa.or.th/s/FPYgMpAxzFAqzrN

มหายุทธศาสตร์ที่ 5 การพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์และสร้างการตระหนักรู้ให้กับประชาชน

1. การเร่งรัดการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ ระยะที่ 1 (Intensive Cybersecurity Capacity Building Program) โดยมีเป้าหมายในการพัฒนาศักยภาพบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อยกระดับการพัฒนาบุคลากรด้านไซเบอร์ของประเทศไทย โดยกำหนดกลุ่มเป้าหมายเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศทั้งภาครัฐและเอกชน รายละเอียดหลักสูตรมีดังนี้

หลักสูตรระดับพื้นฐาน รายวิชาในหลักสูตร หน่วยที่ 01 หลักการพื้นฐานด้านความมั่นคงปลอดภัยสารสนเทศ หน่วยที่ 02 ภัยคุกคามและการโจมตีด้านความมั่นคงปลอดภัยสารสนเทศ หน่วยที่ 03 วิศวกรรมทางสังคม (การหลอกลวงทางไซเบอร์) หน่วยที่ 04 ระบบแฟ้มข้อมูล หน่วยที่ 05 วิทยาการเข้ารหัสลับ หน่วยที่ 06 วิทยาการอำพรางข้อมูล หน่วยที่ 07 จริยธรรมและกฎหมาย หน่วยที่ 08 หลักการพื้นฐานด้านเครือข่ายสื่อสาร หน่วยที่ 09 โปรโตคอลการเชื่อมต่อเครือข่ายที่ปลอดภัย หน่วยที่ 10 อุปกรณ์ความปลอดภัยเครือข่าย หน่วยที่ 11 ระบบการตรวจจับการบุกรุก หน่วยที่ 12 เครือข่ายส่วนตัวแบบเสมือน หน่วยที่ 13 ความมั่นคงปลอดภัยของเครือข่ายไร้สาย หน่วยที่ 14 การระบุตัวตน การพิสูจน์ตัวตน และการให้สิทธิ หน่วยที่ 15 ศูนย์ข้อมูลและการสำรองข้อมูล หน่วยที่ 16 การตอบสนองต่อเหตุขัดข้อง หน่วยที่ 17 การวิเคราะห์ข้อมูลบันทึกกิจกรรม หน่วยที่ 18 กระบวนการทดสอบเจาะระบบ หน่วยที่ 19 การเจาะระบบและการทดสอบเจาะระบบทางเทคนิค หน่วยที่ 20 ความมั่นคงปลอดภัยซอฟต์แวร์และระบบเว็บ หน่วยที่ 21 หลักการพื้นฐานด้านนิติคอมพิวเตอร์ หน่วยที่ 22 หลักฐานดิจิทัล หน่วยที่ 23 นิติวิทยาระบบปฏิบัติการวินโดว์ หน่วยที่ 24 นิติวิทยาระบบเครือข่าย

หน่วยที่ 25 อาชญากรรมทางจดหมายอิเล็กทรอนิกส์และนิติคอมพิวเตอร์ และ หน่วยที่ 26 การจัดทำรายงานการตรวจพิสูจน์หลักฐาน

หลักสูตรระดับผู้เชี่ยวชาญ เฉพาะด้าน รายวิชาในหลักสูตร Domain 1 Security and Risk Management Domain 2 Asset Security Domain 3 Security Architecture and Engineering Domain 4 Communication and Network Security Domain 5 Identity and Access Management (IAM) Domain 6 Security Assessment and Testing Domain 7 Security Operations Domain และ 8 Software Development Security

หลักสูตรระดับผู้เชี่ยวชาญ รายวิชาในหลักสูตร Lesson 1: Comparing Security Roles and Security Controls Lesson 2: Explaining Threat Actors and Threat Intelligence Lesson 3: Performing Security Assessments Lesson 4: Identifying Social Engineering and Malware Lesson 5: Summarizing Basic Cryptographic Concepts Lesson 6: Implementing Public Key Infrastructure Lesson 7: Implementing Authentication Controls Lesson 8: Implementing Identity and Account Management Controls Lesson: Implementing Secure Networking Designs Lesson 10: Implementing Network Security Appliances Lesson 1: Implementing Secure Network Protocols Lesson 12: Implementing Host Security Solutions Lesson 13: Implementing Secure Mobile Solutions Lesson 14: Analyze Indicators of Application Attacks Lesson 15: Implementing Secure Cloud Solutions Lesson 16: Explaining Data Privacy and Protection Concepts Lesson 17: Performing Incident Response Lesson 18: Explaining Digital Forensic Lesson 19: Summarizing Risk Management Concepts Lesson 20: Implementing Cybersecurity Lesson 21: Explaining Physical Security

2. จัดอบรมเพื่อสร้างความตระหนักรู้ให้กับประชาชนทั่วไป Cybersecurity Knowledge Sharing โดยมีหลักสูตรอบรม ดังนี้ 1) หลักสูตรภัยไซเบอร์จากระบบ Remote Working 2) หลักสูตรวัยเกษียณยุคใหม่ห่างไกลภัยไซเบอร์ 3) หลักสูตรรู้เท่าทันภัยคุกคามไซเบอร์ ฉบับพนักงานมืออาชีพ : Cybersecurity for professional employee 4) หลักสูตรการยกระดับมาตรฐาน CII ตาม พ.ร.บ. ไซเบอร์ 5) หลักสูตร Data Layer Protection 6) หลักสูตร Infrastructure ในรูปแบบ Multi-Cloud กับความสัมพันธ์ด้าน Cybersecurity และ 7) ควอนตัมคอมพิวเตอร์ – ประโยชน์ ภัยคุกคาม และการรับมือ

3. การอบรมหลักสูตรเร่งรัดเพื่อแต่งตั้งเป็นพนักงานเจ้าหน้าที่ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 เป็นหลักสูตรเร่งรัด (Intensive Course) ที่มุ่งหมายพัฒนา 3 ด้าน ดังนี้ 1) ด้านการอบรมจริยธรรม/จรรยาบรรณที่พึงมีในบทบาทและอำนาจหน้าที่เป็นพนักงานเจ้างหน้าที่ 2) ด้านความรู้พื้นฐานการสืบสวนและสอบสวนเพื่อการบังคับใช้กฎหมาย (Law Enforcement) และ 3) ด้านการบริหารเหตุภัยคุกคาม (Incident Handling) และการพิสูจน์หลักฐานดิจิทัล (Digital Forensics) พนักงาน

เจ้าหน้าที่ หมายความว่า ผู้ซึ่งรัฐมนตรีแต่งตั้งให้ปฏิบัติการตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

รัฐมนตรี หมายความว่า นายกรัฐมนตรี

พนักงานเจ้าหน้าที่ต้องมีคุณสมบัติ ดังต่อไปนี้

1. มีคุณสมบัติอย่างหนึ่งอย่างใด ดังต่อไปนี้

(1) รับราชการ หรือเคยรับราชการ หรือเป็นบุคคลที่ทำงานเกี่ยวกับการสืบสวนสอบสวนหรือวิเคราะห์ข้อมูล (Data Analyst) ไม่น้อยกว่า 2 ปี ในตำแหน่งที่เกี่ยวข้องกับด้านความมั่นคงปลอดภัยสารสนเทศ (information Security) ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity) ด้านการบริหารเหตุภัยคุกคามไซเบอร์ (Incident Handling) หรือด้านการพิสูจน์หลักฐานทางดิจิทัล (Digital Forensics) หรือ

(2) สำเร็จการศึกษาไม่น้อยกว่าระดับปริญญาตรี หรือเทียบเท่าทางวิศวกรรมศาสตร์ วิทยาศาสตร์ วิทยาการคอมพิวเตอร์ เทคโนโลยีสารสนเทศ สถิติศาสตร์ นิติศาสตร์ รัฐศาสตร์ รัฐประศาสนศาสตร์

2. มีความรู้ความชำนาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

3. ผ่านการอบรมด้านจริยธรรม สืบสวน สอบสวน ความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security) การบริหารจัดการเหตุภัยคุกคามไซเบอร์ (Incident Handling) หรือการพิสูจน์หลักฐานทางดิจิทัล (Digital Forensics) ทั้งนี้บุคคลที่ได้รับการยกเว้นคุณสมบัติดังกล่าว ต้องผ่านการอบรมหลักสูตรเร่งรัด ดังนี้ ประกอบด้วย ด้านที่ 1 การอบรมด้านจริยธรรม/จรรยาบรรณที่พึงมีในบทบาทแลอำนาจหน้าที่เป็นพนักงานเจ้าหน้าที่ ด้านที่ 2 ความรู้พื้นฐานด้านการสืบสวนและสอบสวนเพื่อการบังคับใช้กฎหมาย ดังตารางที่ 2

ตารางที่ 2 หลักสูตรพื้นฐานด้านการสืบสวนสอบสวน

ลำดับที่	เนื้อหาหลักสูตร
1	กฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์
2	กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
3	กฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล
4	กฎหมายอาญาและวิธีพิจารณาความอาญาที่เกี่ยวข้องกับการกระทาความผิดเกี่ยวกับคอมพิวเตอร์
5	รูปแบบการกระทำความผิดและกรณีศึกษา (Case Studies)
6	แนวทางปฏิบัติในการดำเนินคดี/การทาสำนวนคดี เช่น การร้องทุกข์กล่าวโทษ (การแจ้งความ) การประสานความร่วมมือกับหน่วยงานที่เกี่ยวข้อง การรวบรวมพยานหลักฐาน และแสวงหาข้อเท็จจริง การตรวจสถานที่เกิดเหตุ การยื่นคาร้องต่อศาล การยึดอายัดและคืนพยานหลักฐาน

ลำดับที่	เนื้อหาหลักสูตร
	การเก็บรักษา พยานหลักฐานให้คงความน่าเชื่อถือในกระบวนการเปรียบเทียบปรับและการดำเนินคดี เป็นต้น
7	การบริหารจัดการคดีให้เป็นไปอย่างมีประสิทธิภาพ

ด้านที่ 3 การบริหารจัดการเหตุภัยคุกคามไซเบอร์ (Incident Handling) และการพิสูจน์หลักฐานทางดิจิทัล (Digital forensics) ดังตารางที่ 3

ตารางที่ 3 หลักสูตรการบริหารจัดการเหตุภัยคุกคามไซเบอร์

ลำดับที่	เนื้อหาหลักสูตร
1	Fundamentals of Incident Management
2	Incident Handling and Response Program Planning
3	Anti-forensics Techniques
4	Malware Incident Handling and Response
5	Email Security Incident Handling and Response
6	Network Security Incident Handling and Response
7	Web Security Incident Handling and Response
8	Cloud Security Incident Handling and Response
9	Insider Threat-related Incident Handling and Response
10	Fundamentals of Computer Forensics
11	Computer Forensics Investigation Process
12	Investigative Reports

กล่าวโดยสรุป มหายุทธศาสตร์ทั้ง 6 ด้าน เป็นยุทธศาสตร์ในการป้องกัน รับมือ ลดความเสี่ยงจากภัยคุกคามไซเบอร์ ของ สกมช. ทำให้การปฏิบัติการ ประสานงาน สนับสนุน และการให้ความช่วยเหลือหน่วยงานที่เกี่ยวข้องในการปฏิบัติตามนโยบายและแผน เฝ้าระวัง ความเสี่ยง ติดตาม วิเคราะห์และประมวลผลข้อเกี่ยวกับภัยคุกคามทางไซเบอร์ ทำให้เกิดความร่วมมือระหว่างหน่วยงานภาครัฐและเอกชน ใช้แก้ปัญหาเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีลักษณะและเป็นปัจจุบัน

สรุป

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือ สกมช. หรือ NCSA เป็นองค์การมหาชนที่จัดตั้งขึ้นตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 เพื่อกำหนดนโยบาย มาตรการ แนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและเอกชนที่เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ มิให้กระทบต่อความมั่นคงของรัฐ และความสงบเรียบร้อยภายในประเทศ ผลการปฏิบัติงานตามยุทธศาสตร์ ทำให้ทุกมิติของประเทศมีความมั่นคงปลอดภัยไซเบอร์สูงขึ้นกว่าทุกปีที่ผ่านมา โดยการวัดจากรายงาน Global Cybersecurity Index (GCI) ปี 2563 ซึ่งเป็นรายงานที่แสดงถึงความเข้มข้นในการจัดการด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศต่าง ๆ โดยสหภาพโทรคมนาคมระหว่างประเทศหรือ International Telecommunication Union (ITU) ประเมินค่าคะแนนความพร้อมด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศไทยคิดเป็น 86.5 และอยู่อันดับ 44 จาก 182 ประเทศ มีความตระหนักรู้และองค์ความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ขยายวงกว้างมากขึ้น มีขีดความสามารถในการป้องกันภัยคุกคามทางไซเบอร์สูงขึ้น ซึ่งส่งผลให้ความเสี่ยงภัยคุกคามทางไซเบอร์ลดน้อยลง โดยได้มีแนวทางการจัดทำและทบทวนการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ การจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP) จัดทำแผนการสื่อสารในภาวะวิกฤติเพื่อตอบสนองต่อเหตุการณ์ทางไซเบอร์ และมีกระบวนการจัดทำมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

บรรณานุกรม

ประกาศ กมช. เรื่อง นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 - 2570). (9 ธันวาคม 2564). *ราชกิจจานุเบกษา.* เล่ม 139 ตอนพิเศษ 288 ง หน้า 1-48.

_____ . เรื่อง การกำหนดระดับความรู้ความชำนาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อแต่งตั้งเป็นพนักงานเจ้าหน้าที่ พ.ศ. 2564. (7 ธันวาคม 2564). *ราชกิจจานุเบกษา.* เล่ม 138 ตอนพิเศษ 299 ง หน้า 21-23.

_____ . เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564. (6 กันยายน 2564). *ราชกิจจานุเบกษา.* เล่ม 138 ตอนพิเศษ 208 ง หน้า 9-15.

_____. เรื่อง การกำหนดหลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการมอบหมายการควบคุมและกำกับดูแล พ.ศ. 2564. (23 สิงหาคม 2564). *ราชกิจจานุเบกษา.* เล่ม 138 ตอนพิเศษ 194 ง หน้า 14-15.

แมรี-แอนน์ รัสสัน. (10 พฤษภาคม 2021). สหรัฐฯ ประกาศภาวะฉุกเฉินหลัง บ.ท่อส่งน้ำมันรายใหญ่โดนมัลแวร์เรียกค่าไถ่โจมตี. *BBC NEWS ไทย*. https://www.bbc.com/thai/international-57052951#:~:text=10%20พฤษภาคม%202021,ท่อต้องหยุดชะงักลง.

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ. (ม.ป.ป.). *กฎหมาย ข้อบังคับ และประกาศ.* http://www.ncsa.or.th/กฎหมาย-ข้อบังคับ-และประก.html.

BBC NEWS ไทย. (27 พฤศจิกายน 2022). รัสเซีย ยูเครน: รัสเซียสร้างความเสียหายต่อระบบไฟฟ้าของยูเครนมากแค่ไหน. *BBC NEWS ไทย.* https://www.bbc.com/thai/international-63767411 27 พฤศจิกายน 2022

Kaspersky Industrial Control Systems Cyber Emergency Response Team. (30 September 2019). *Threat landscape for industrial automation systems, H1 2019.* https://ics-cert.kaspersky.com/publications/reports/2019/09/30 /threat-landscape-for-industrial-automation-systems-h1-2019/

Thailand Computer Emergency Response Team. (ม.ป.ป.). *ผลรวมระดับความรุนแรงของช่องโหว่.* https://www.thaicert.or.th/กฎหมาย-ข้อบังคับ-ประกาศ/.