ESTABLISHING A COMPUTER SECURITY INCIDENT RESPONSE TEAM
คู่มือการจัดตั้งศูนย์ประสานการรับมือภัยคุกคามความมั่นคงปลอดภัยคอมพิวเตอร์

คู่มือการจัดตั้งซีเซิร์ต

ESTABLISHING A CSIRT

ThaiCERT
Thailand Computer Emergency Response Team
a member of ETDA

ETDA
สพธอ
www.etda.or.th

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
Ministry of Digital Economy and Society

ESTABLISHING A CSIRT

คู่มือการจัดตั้งซีเซิร์ต

ชื่อเรื่อง : **คู่มือการจัดตั้งซีเซิร์ต (Establishing a CSIRT)**

เรียบเรียงโดย : ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (Thailand Computer Emergency Response Team)

พิมพ์ครั้งที่ 1 : มกราคม 2561

พิมพ์จำนวน : 500 เล่ม

จัดพิมพ์และเผยแพร่โดย:

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (Thailand Computer Emergency Response Team)

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

อาคารเดอะ ไนน์ ทาวเวอร์ แกรนด์ พระรามเก้า (อาคารบี) ชั้น 20
เลขที่ 33/4 ถนนพระราม 9 แขวงห้วยขวาง เขตห้วยขวาง กรุงเทพมหานคร 10310

โทรศัพท์: 0 2123 1234 โทรสาร: 0 2123 1200

อีเมล: office@thaicert.or.th

เว็บไซต์ไทยเซิร์ต: www.thaicert.or.th

เว็บไซต์สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน): www.etda.or.th

เว็บไซต์กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม: www.mdes.go.th

ESTABLISHING A COMPUTER SECURITY INCIDENT RESPONSE TEAM

คู่มือการจัดตั้งศูนย์ประสานการรับมือภัยคุกคามความมั่นคงปลอดภัยคอมพิวเตอร์

คู่มือการจัดตั้งซีเซิร์ต

ESTABLISHING A CSIRT

ThaiCERT
Thailand Computer Emergency Response Team
a member of ETDA

ETDA
สพธอ
www.etda.or.th

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
Ministry of Digital Economy and Society

สารบัญ

บทนำ

ปัจจุบัน เสถียรภาพ ความมั่นคง และความพร้อมใช้งานของอินเทอร์เน็ตนั้นสำคัญยิ่งต่อการทำงานของหน่วยงานและองค์กรต่าง ๆ โดยเฉพาะที่เป็นโครงสร้างพื้นฐานสำคัญ อาทิ ภาคการเงิน ภาคพลังงาน ภาคการขนส่ง หรือภาครัฐ ซึ่งจะให้บริการได้อย่างเต็มที่นั้น ประชาชนจะต้องสามารถเข้าถึงอินเทอร์เน็ตได้ ส่วนผู้ดูแลระบบโครงสร้างพื้นฐานเองก็ต้องพึ่งพาอินเทอร์เน็ตมากขึ้นเรื่อย ๆ เพื่อให้บริการและติดต่อสื่อสารระหว่างกัน

เวลานี้ หากการเชื่อมต่ออินเทอร์เน็ตขัดข้องเพียงไม่กี่นาทีคงเป็นเรื่องที่รับไม่ได้ และหากการเชื่อมต่อขัดข้องเป็นเวลานานก็อาจส่งผลกระทบต่อเสถียรภาพของระบบเศรษฐกิจ โดยเฉพาะองค์กรต่าง ๆ ที่ใช้ประโยชน์จากเว็บไซต์ในการทำธุรกรรมซื้อขาย ย่อมจะได้รับผลกระทบที่รุนแรง แม้อินเทอร์เน็ตจะไม่สามารถให้บริการไปเพียงระยะเวลาสั้น ๆ ก็ตาม ดังเช่นการหยุดให้บริการของ Facebook ที่เคยปรากฏเป็นข่าวใหญ่โตมาแล้ว

นอกจากกรณีข้างต้นแล้ว ก็ยังมีรายงานข้อมูลรั่วไหลที่เกิดขึ้นกับองค์กรต่าง ๆ ทั่วโลกอยู่ทุกวัน ในหลายกรณีก็พบว่าข้อมูลหรือทรัพย์สินทางปัญญาถูกขโมย ซึ่งการกระทำเหล่านี้ถือว่าเป็นการจารกรรมระดับองค์กร

หากพูดถึงความเสียหายที่เกิดจากเหตุภัยคุกคามอาจแบ่งออกเป็น 2 ลักษณะคือ (1) ความเสียหายทางตรงที่เกี่ยวข้องกับรายได้และกำไรที่สูญเสียไป รวมถึงค่าใช้จ่ายในการจำกัดขอบเขตความเสียหายและแก้ปัญหาที่เกิดจากเหตุภัยคุกคามนั้น และ (2) ความเสียหายทางอ้อมที่เกิดต่อภาพลักษณ์ การสูญเสียลูกค้า หรือค่าปรับจากองค์กรกำกับดูแล

ที่ผ่านมา มีกรณีศึกษาให้เห็นอยู่หลายกรณีที่เหตุภัยคุกคามด้านความมั่นคงปลอดภัยทำให้องค์กรล้มละลาย เพราะไม่สามารถฟื้นตัวให้กลับมาเหมือนเดิมได้ภายหลังเกิดเหตุ ดังนั้น จึงต้องมีการรับมือที่เหมาะสมและทันท่วงทีเมื่อมีเหตุภัยคุกคามไซเบอร์เกิดขึ้น และนี่คือเหตุผลที่ต้องจัดตั้ง CSIRT

CSIRT คือทีมผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยไซเบอร์ที่สามารถรับมือและแก้ไขเหตุภัยคุกคาม

ประกอบด้วยบุคลากรที่มีความรู้และทักษะในการรับมือเหตุภัยคุกคาม ให้ความช่วยเหลือผู้รับบริการในการฟื้นตัวจากการเจาะระบบ นอกจากนี้ในการดำเนินการเชิงรุก CSIRT ให้บริการตรวจสอบและประเมินช่องโหว่ของระบบสารสนเทศและความเสี่ยงต่าง ๆ รวมทั้งสร้างความตระหนักและให้ความรู้แก่ผู้เกี่ยวข้องในการพัฒนาและปรับปรุงการบริการเพื่อให้เกิดความมั่นคงปลอดภัยบนโลกไซเบอร์

สุรางคณา วายุภาพ
ผู้อำนวยการสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)

อภิธานศัพท์

คำศัพท์เฉพาะที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์ที่ควรรู้จัก มีดังนี้

CERT หรือ Computer Emergency Response Team

คำว่า "CERT" เป็นเครื่องหมายการค้าจดทะเบียนของ CERT Coordination Center (CERT/CC)[1] หมายถึงหน่วยงานรับมือเหตุภัยคุกคามที่อยู่ภายใต้สถาบันวิศวกรรมซอฟต์แวร์ (Software Engineering Institute – SEI) แห่งมหาวิทยาลัย Carnegie Mellon ในสหรัฐอเมริกา และเนื่องจาก CERT เป็นเครื่องหมายการค้าจดทะเบียน ดังนั้น ศูนย์ที่ทำหน้าที่ประสานและรับมือเหตุภัยคุกคามด้านความมั่นคงทางไซเบอร์ที่จัดตั้งขึ้นใหม่และต้องการใช้ชื่อที่มีคำว่า CERT จะต้องยื่นขอใบอนุญาตเสียก่อน[2] ทั้งนี้ CERT แห่งแรกจัดตั้งขึ้นเพื่อรับมือและแก้ไขเหตุการเชื่อมต่ออินเทอร์เน็ตขัดข้องที่มีผลกระทบในวงกว้างซึ่งเกิดจาก worm ชื่อ Morris[3] ในปี พ.ศ. 2531

CSIRT หรือ Computer Security Incident Response Team

เป็นศัพท์ทั่วไปที่ใช้เรียกทีมรับมือเหตุภัยคุกคามและมีภารกิจเช่นเดียวกับ CERT อย่างไรก็ดี เนื่องจาก CERT เป็นเครื่องหมายการค้าจดทะเบียน ในเอกสารฉบับนี้จึงใช้คำว่า CSIRT แทน

---

1 CERT/CC: <https://www.cert.org/>
2 รายละเอียดเพิ่มเติมและขั้นตอนการยื่นขอใบอนุญาต สามารถศึกษาได้ที่ <https://www.cert.org/incident-management/csirt-development/cert-authorized.cfm>
3 The Morris Worm: <https://en.wikipedia.org/wiki/Morris_worm>

ISAC หรือ Information Sharing and Analysis Center

คือศูนย์แลกเปลี่ยนและวิเคราะห์ข้อมูล ที่มีหน้าที่สร้างความร่วมมือระหว่างทีมด้านความมั่นคงปลอดภัยทางไซเบอร์ที่มีลักษณะคล้ายคลึงกันหรืออยู่ในภาคส่วนเดียวกัน ซึ่งศูนย์แลกเปลี่ยนและวิเคราะห์ข้อมูลนี้อาจมีหน้าที่ความรับผิดชอบคล้ายกับ CSIRT เพียงแต่จะขาดภารกิจในการรับมือและแก้ไขเหตุภัยคุกคาม

SOC หรือ Security Operating Center

คือศูนย์ปฏิบัติการทางไซเบอร์ ซึ่งเป็นพื้นที่หรือห้องในอาคารที่เป็นศูนย์กลางสำหรับการเฝ้าระวังเหตุภัยคุกคามแบบเรียลไทม์ การส่งทีมรับมือและแก้ไขเหตุภัยคุกคามไปยังที่เกิดเหตุ และการประสานงานเพื่อรับมือและแก้ไขเหตุภัยคุกคาม คล้ายกับที่บริษัทผู้ให้บริการอินเทอร์เน็ต (ISPs) มี NOC หรือ Network Operating Centers ซึ่งเป็นศูนย์ปฏิบัติการสำหรับดูแลเครือข่าย แต่ความแตกต่างคือ SOC จัดตั้งขึ้นเพื่อรับมือเหตุภัยคุกคามโดยเฉพาะ โดยปกติแล้ว มีเพียง CSIRT ชั้นแนวหน้าหรือองค์กรใหญ่ ๆ ที่มีระบบเทคโนโลยีสารสนเทศกระจายอยู่หลายพื้นที่เท่านั้น ที่จำเป็นต้องมี SOC

การดำเนินงานของ CSIRT และ SOC ไม่แตกต่างกันมากนักเพราะมีภารกิจที่คล้ายคลึงและทับซ้อนกันอยู่มาก ในบางกรณีอาจพบ CSIRT ตั้งอยู่ใน SOC ในขณะที่ CSIRT บางแห่งก็กำหนดให้ SOC เป็นเสมือนทีมหน้าด่านในการรับมือเมื่อเกิดเหตุภัยคุกคาม ซึ่งรายละเอียดและความสัมพันธ์ระหว่าง CSIRT และ SOC จะปรากฏในบทที่ 6

ทั้งนี้ ไม่ว่าจะใช้คำว่าอะไร หรือศูนย์ที่จัดตั้งขึ้นจะได้ชื่อว่าอะไร ท้ายที่สุดแล้วสิ่งที่สำคัญสำหรับองค์กรที่เกี่ยวข้องก็คือขีดความสามารถในการรับมือเหตุภัยคุกคาม

โครงสร้างเนื้อหาของเอกสาร

บทที่ 1 อธิบายวงจรการทำงานและขีดความสามารถของ CSIRT

บทที่ 2-4 รายละเอียดขั้นตอนต่าง ๆ ที่จำเป็นในการจัดทำแผน การขอให้ผู้บริหารอนุมัติจัดตั้ง CSIRT

บทที่ 5 รายละเอียดการให้บริการรับมือและแก้ไขเหตุภัยคุกคาม

บทที่ 6 อธิบายบริการอื่น ๆ ที่ CSIRT อาจมี

หมายเหตุ เพื่อประโยชน์ต่อผู้อ่านในการทำความเข้าใจกับคำแนะนำในคู่มือฉบับนี้ จึงได้ยกตัวอย่างของไทยเซิร์ต เป็นข้อความในกล่องสี่เหลี่ยม

ตัวอย่างไทยเซิร์ต

ผู้ที่จะได้รับประโยชน์จากเอกสารฉบับนี้

คู่มือฉบับนี้ได้รับการออกแบบมาสำหรับองค์กรต่าง ๆ ที่ต้องการจะเรียนรู้เพิ่มเติมเกี่ยวกับ CSIRT และต้องการจัดตั้ง CSIRT ขึ้นมาภายในองค์กร โดยคู่มือจะมีรายละเอียดเกี่ยวกับกระบวนการจัดตั้ง CSIRT และข้อกำหนดต่าง ๆ รวมทั้งสอดแทรกตัวอย่าง เพื่อให้เข้าใจและเห็นภาพว่าจะดำเนินการตามขั้นตอนแต่ละขั้นให้สำเร็จได้อย่างไร เอกสารฉบับนี้เหมาะสำหรับเจ้าหน้าที่ในระดับบริหาร แต่เจ้าหน้าที่ด้านเทคนิคก็สามารถใช้ประโยชน์ในการอ้างอิงจากคู่มือฉบับนี้ได้เช่นกัน

คำชี้แจงทางกฎหมาย

คู่มือนี้มีจุดประสงค์เพื่อช่วยองค์กรในการจัดตั้ง CSIRT ตั้งแต่เริ่มต้นจนถึงขั้นที่สามารถปฏิบัติงานได้ เนื้อหาที่ปรากฏในเล่มนี้มาจากทั้งองค์ความรู้และประสบการณ์ของไทยเซิร์ต และสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) และจากเครือข่าย CSIRT อื่น ๆ ทั้งนี้เนื้อหาของคู่มือเป็นเนื้อหาที่รวบรวม ณ เวลาที่จัดทำ ไม่ได้เป็นคู่มือที่สมบูรณ์แบบที่สุด อาจจำเป็นต้องปรับปรุงให้ทันสมัยเหมาะสมตามกาลเวลา

คู่มือนี้อ้างอิงเนื้อหาจากแหล่งข้อมูลต่าง ๆ ซึ่งไทยเซิร์ตขอสงวนสิทธิ์ในการรับผิดชอบต่อเนื้อหาดังกล่าว รวมถึงรับรองว่าเว็บไซต์ที่ได้อ้างอิงหรือระบุไว้ในคู่มือนี้จะยังสามารถเข้าถึงได้ และหากเนื้อหาส่วนใดมีการระบุถึงชื่อผลิตภัณฑ์ ไม่ได้หมายความว่าไทยเซิร์ตสนับสนุนผลิตภัณฑ์ดังกล่าว เพียงแต่เป็นการยกตัวอย่างเท่านั้น

คู่มือนี้จัดทำขึ้นเพื่อการศึกษาและอ้างอิงเท่านั้น ไทยเซิร์ตหรือบุคคลใด ๆ ที่ปฏิบัติหน้าที่ในนามไทยเซิร์ตจะไม่รับผิดชอบต่อผลลัพธ์ของการใช้งานข้อมูลที่ปรากฏในคู่มือนี้ ข้อมูลทุกอย่างที่ปรากฏในคู่มือนี้อาจเปลี่ยนแปลงไปตามกาลเวลา จึงขอสงวนสิทธิ์เกี่ยวกับความถูกต้องของข้อมูลต่าง ๆ

[4] Creative Commons License: <https://creativecommons.org/licenses/by-nc-sa/4.0/>

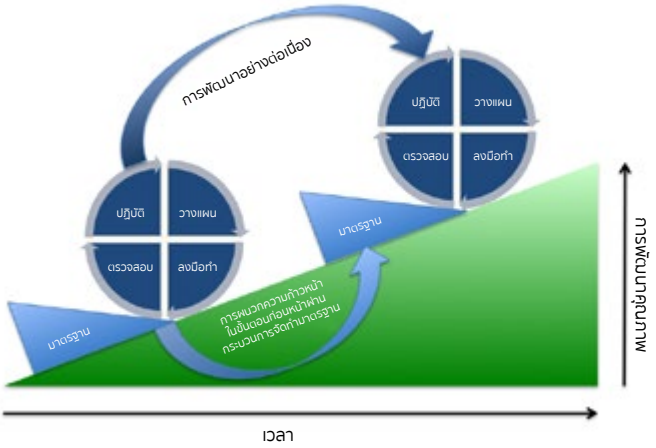
กิตติกรรมประกาศ

ไทยเซิร์ตขอขอบคุณสถาบันและบุคคลต่าง ๆ ที่ให้ความอนุเคราะห์จนประสบความสำเร็จในการจัดทำคู่มือฉบับนี้ โดยขอแสดงความขอบคุณเป็นพิเศษแด่

- CERT/CC โดยเฉพาะอย่างยิ่งทีมพัฒนา CSIRT ซึ่งให้ข้อมูลประกอบในบทที่ 6
- ENISA สำหรับข้อมูลเชิงลึกเกี่ยวกับบุคคล กฎหมายและกฎระเบียบ
- TRANSITS สำหรับข้อเสนอในกระบวนการรับมือและแก้ไขเหตุภัยคุกคาม
- ผู้ที่ได้กรุณาตรวจสอบการแปลและความถูกต้องของคู่มือนี้

1. การบริหารจัดการวงจรการทำงานของทีมและขีดความสามารถ

การจัดตั้ง CSIRT มีหลายองค์ประกอบและปัจจัยที่ต้องคำนึงถึง ดังนั้น จึงควรนำวงจร วางแผน-ลงมือทำ -ตรวจสอบ-ปฏิบัติ (Plan-Do-Check-Act หรือ PDCA[5] มาปรับใช้เพื่อให้การจัดตั้งและการทำงานเป็นไปอย่างราบรื่น มีการพัฒนาปรับปรุงอย่างต่อเนื่องสม่ำเสมอ



รูปภาพที่ 1: แสดงวงจร PDCA (หรือวงจร Deming) เป็นแนวทางช่วยให้การดำเนินการมีการพัฒนาคุณภาพอย่างต่อเนื่อง

[5] วงจร PDCA : <https://en.wikipedia.org/wiki/PDCA>

ในการจัดตั้งและดำเนินภารกิจของ CSIRT ควรจะมีที่ปรึกษาระดับสูงที่มีประสบการณ์ในการบริหารองค์กร ในระดับสูงสุด มีประสบการณ์กับการกำหนดเป้าหมายและยุทธศาสตร์ทางธุรกิจ รวมทั้งสามารถสนับสนุน แผนงานต่าง ๆ เข้ามามีบทบาทให้คำแนะนำด้วย นอกจากนี้ ยังมี CSIRT ที่พร้อมแบ่งปันประสบการณ์และองค์ความรู้รวมทั้งตัวอย่างต่าง ๆ เพื่อสนับสนุนการจัดตั้ง CSIRT ใหม่ ๆ

- AusCERT[6]
- สถาบันการเงิน[7]
- CERT Polska[8]

วางแผน (Plan)

การจัดทำกรอบงาน CSIRT

- คำอธิบายโดยละเอียดจะปรากฏในบทที่ 2 และในภาคผนวก ก: แม่แบบกรอบงาน CSIRT

การกำหนดงบประมาณ

- กำหนดงบประมาณสำหรับการดำเนินการต่อเนื่องเป็นเวลาหลายปี โดยต้องแยกงบประมาณด้านการปฏิบัติการและงบประมาณที่ใช้สำหรับการลงทุนออกจากกัน

---

6 AusCERT: <https://www.auscert.org/au/render.html?it=2252>
7 สถาบันการเงิน: <http://www.cert.org/incident-management/publications/case-studies/afi-case-study.cfm>
8 CERT Polska: <https://www.terena.org/activities/tf-csirt/meeting9/jaroszewski-assistance-csirt.pdf>

- ไม่ควรกำหนดงบประมาณในลักษณะที่เป็นการผูกมัดจนเกินไป และไม่ควรประเมินงบประมาณสูงกว่าความเป็นจริง
- จัดทำงบประมาณให้กระชับที่สุดเท่าที่จะกระทำได้และควรชี้แจงเกี่ยวกับสิ่งที่เป็นรูปธรรม และนามธรรมในข้อเสนออย่างตรงไปตรงมา

การจัดทำแผนธุรกิจ แผนประกอบการ

- ศึกษาจากตัวอย่างและเว็บไซต์ที่ให้คำแนะนำเกี่ยวกับแผนธุรกิจต่าง ๆ
- ขอรับการสนับสนุนจากที่ปรึกษาระดับสูง
- แผนธุรกิจ แผนประกอบการควรสะท้อนเป้าหมายของ CSIRT ที่มีต่อองค์กร และความเชื่อมโยงระหว่างเป้าหมายกับงบประมาณ
- ควรระบุผลตอบแทนจากการลงทุนในแผนฯ ด้วย (Return on Investment : ROI)

การนำเสนองบประมาณและแผนงาน

- คำอธิบายปรากฏในบทที่ 3
- ศึกษาอย่างรอบคอบเพื่อให้สามารถอธิบายและชี้แจงเหตุผลความจำเป็นของงบประมาณแต่ละรายการได้
- นำเสนอแผนต่อที่ปรึกษาระดับสูงก่อนเพื่อรับฟังข้อคิดเห็นและข้อเสนอแนะ
- จากนั้นจึงนำเสนอต่อบุคคลที่มีอำนาจอนุมัติแผนและค่าใช้จ่ายต่าง ๆ ในการจัดตั้ง CSIRT

ลงมือทำ (Do)

การดำเนินการตามแผน

- คำอธิบายปรากฏในบทที่ 4
  - สรุปข้อมูลภาพรวมเกี่ยวกับแหล่งข้อมูล
  - ร่างนโยบายการรับมือและแก้ไขเหตุภัยคุกคาม
  - ร่างนโยบายการจัดการและแลกเปลี่ยนข้อมูล
  - ประเมินขีดความสามารถพื้นฐานของผู้รับบริการ
  - ประชาสัมพันธ์การจัดตั้ง CSIRT
  - สร้างเครือข่ายความร่วมมือจากการเข้าร่วมการประชุมและการเสวนาต่าง ๆ
  - ซ้อมรับมือเหตุภัยคุกคาม
- ดำเนินการรับมือและแก้ไขเหตุภัยคุกคาม (บทที่ 5) รวมทั้งให้บริการตามภารกิจหลักอื่น ๆ (บทที่ 6)

ตรวจสอบ (Check)

วิเคราะห์การทำงานของ CSIRT

- ให้ความสำคัญกับผังขั้นตอนการทำงาน (workflow) กระบวนการและภารกิจที่สำคัญ
  - การดำเนินการไม่ต่อเนื่อง ไม่สม่ำเสมอหรือไม่
  - การดำเนินการต่าง ๆ สามารถที่จะพัฒนาและปรับปรุงได้ดียิ่งขึ้นได้อย่างไร

- ใช้วิธีการประเมินผลที่เหมาะสม
- ให้บุคลากรเข้ามามีส่วนร่วม
  - การมีส่วนร่วมนำไปสู่ความมุ่งมั่นและพันธกิจร่วมกัน
  - แลกเปลี่ยนในสิ่งที่ดำเนินการได้ดีแล้วและสิ่งที่ยังปรับปรุงได้อีก
  - ทำงานร่วมกับส่วนตรวจสอบคุณภาพในองค์กร (หากมี)
  - อาจพิจารณาจ้างที่ปรึกษาจากภายนอกเข้ามาช่วย
- สัมภาษณ์ผู้รับบริการ เกี่ยวกับ
  - สิ่งที่ CSIRT ดำเนินการได้ดีอยู่แล้ว
  - ช่องทางในการปรับปรุงและพัฒนา
- บริหารจัดการคุณภาพทั่วไป
  - CSIRT ทำงานตามกระบวนการและมาตรฐานที่วางไว้หรือไม่
  - ได้มีการบันทึกการปฏิบัติงานเป็นลายลักษณ์อักษรหรือไม่
  - ทุกคนทราบว่าเอกสารที่เกี่ยวข้องอยู่ที่ใดหรือไม่
  - มีผลการประชุมทุกอย่างที่เกี่ยวข้องเก็บไว้เพื่อการอ้างอิงในภายหลังหรือไม่
  - ทุกคนทำงานร่วมกันอย่างไร ทุกคนแบ่งปันข้อมูลเกี่ยวกับเหตุภัยคุกคามที่ดำเนินอยู่ได้ทราบอย่างไร
  - วางแผนให้บุคลากรในทีมเข้าร่วมการฝึกอบรม การประชุมและการสัมมนาต่าง ๆ

ปฏิบัติ (Act)

ตัดสินใจเกี่ยวกับภารกิจ บริการเพิ่มเติมและการพัฒนาปรับปรุง

- นำผลที่ได้จากขั้นการตรวจสอบ (check) ไปปรับปรุงการปฏิบัติงาน
- เมื่อ CSIRT มีขีดความสามารถเพิ่มขึ้น ก็อาจให้บริการอื่น ๆ เพิ่มเติม ดังรายละเอียดที่ปรากฏ ในบทที่ 6
- เริ่มต้นจากขั้นการวางแผนใหม่และดำเนินการตามขั้นตอนและวงจรจากนั้นจึงดำเนินการตามวงจรเพื่อให้มีการพัฒนาและปรับปรุงอย่างต่อเนื่องสม่ำเสมอ

หลังจากจัดตั้ง CSIRT แล้ว การดำเนินการตามวงจรมักใช้เวลาประมาณหนึ่งปี ซึ่งจะพอดีกับปีงบประมาณขององค์กร ทั้งนี้ เพื่อให้สามารถบรรจุความจำเป็นหรือความต้องการต่าง ๆ ของ CSIRT ในการหารือเพื่อกำหนดหรือยกร่างข้อเสนองบประมาณได้ตามกรอบเวลา

ปัจจัยการพิจารณาการให้บริการของ CSIRT ประการหนึ่งคือระดับขีดความสามารถของ CSIRT ซึ่งมีตั้งแต่ระดับที่จำกัดเพียงการรับมือเหตุภัยคุกคามจนถึงการให้บริการเชิงรุกเพื่อป้องกันและการบริหารจัดการคุณภาพ ในคู่มือฉบับนี้ CSIRT ขั้นต่ำสุดที่จะกล่าวถึงคือ CSIRT ที่มีขีดความสามารถระดับ 2 (พื้นฐาน)

ระดับขีดความสามารถ (Maturity Level)	คำอธิบาย
1. ระดับเบื้องต้น	CSIRT ตั้งขึ้นเพื่อเป็นผู้ติดต่อ (Point of Contact: POC) สำหรับประสานแจ้งเหตุและแก้ไขเหตุภัยคุกคาม มีกฎ ระเบียบ และข้อบังคับสำหรับการแจ้งเตือนและรายงานไปยังองค์กรที่เกี่ยวข้องต่าง ๆ
2. ระดับพื้นฐาน	ระดับที่ 1 + มีกระบวนการรับมือเหตุภัยคุกคามรูปแบบใหม่ และใช้ระบบสำหรับรับแจ้งเหตุและติดตามการดำเนินการ (ticketing system) รวมถึงให้คำแนะนำด้านความมั่นคงปลอดภัยแก่องค์กร
3. ระดับพร้อมรับมือ	ระดับที่ 2 + มีเครื่องมือวิเคราะห์เหตุภัยคุกคามและมีกระบวนการจัดประเภทและจัดการข้อมูล
4. ระดับเชิงรุก	ระดับที่ 3 + เผยแพร่ข้อมูลข่าวสารเกี่ยวกับความมั่นคงปลอดภัย ใช้เครื่องมือตรวจสอบและเฝ้าระวังเหตุภัยคุกคามอย่างสม่ำเสมอ รวมถึงวางแผนการฝึกอบรมแก่บุคลากร
5. ระดับครบวงจร	ระดับที่ 4 + เฝ้าระวังและตรวจจับเหตุภัยคุกคามแบบเรียลไทม์ รวมถึงเมื่อพบเหตุภัยคุกคามประเภทใหม่ จะมีการร่างคู่มือป้องกันเหตุภัยคุกคามและแบ่งปันแก่ทั้งภายในและภายนอกองค์กร

2. การร่างกรอบงาน CSIRT

กรอบงานของ CSIRT กำหนดรายละเอียดเกี่ยวกับภารกิจของ CSIRT ไม่ว่าจะเป็นจำนวน และประเภทภารกิจของ CSIRT ผู้ได้รับประโยชน์จากการทำงานของ CSIRT และทรัพยากรที่ต้องใช้ในการดำเนินภารกิจ ซึ่งสามารถนำมาปรับใช้กับ CSIRT แต่ละแห่งได้ เพราะแม้ว่าจะมีความแตกต่างกัน แต่ CSIRT ทุกแห่งก็มีองค์ประกอบพื้นฐานที่คล้ายคลึงกัน ตัวอย่างของกรอบงานที่จะช่วยให้เห็นภาพชัดขึ้นนั้นปรากฏอยู่ใน ภาคผนวก ก: แม่แบบกรอบงาน CSIRT (CSIRT framework template)

ข้อมูลเกี่ยวกับการจัดตั้ง CSIRT ในเอกสารฉบับนี้อ้างอิงมาจากแนวปฏิบัติที่ได้รับการยอมรับในระดับนานาชาติ หากปฏิบัติตามกรอบงานดังกล่าว จะช่วยให้เข้าเป็นสมาชิกของเครือข่ายความร่วมมือต่าง ๆ ได้ง่ายขึ้น เพราะข้อกำหนดของการเข้าเป็นสมาชิกเครือข่ายความร่วมมือต่าง ๆ ล้วนสอดคล้องกับแนวปฏิบัติที่ได้รับการยอมรับ

องค์กรสามารถนำ CSIRT framework ไปใช้ประชาสัมพันธ์การจัดตั้ง CSIRT ให้ผู้มีส่วนเกี่ยวข้อง ผู้รับบริการ และสาธารณชนรับทราบ (โปรดอ่านข้อ 4.5 ประกอบ) เพื่อให้เห็นภาพ เอกสารฉบับนี้จะยกตัวอย่างไทยเซิร์ตประกอบในส่วนประกอบของ CSIRT framework ที่จะอธิบายถัดไป

2.1 พันธกิจ

เมื่อจัดตั้ง CSIRT ควรบันทึกพันธกิจ (mission statement) ของ CSIRT ไว้เป็นลายลักษณ์อักษร โดยพันธกิจจะต้องกำหนดวัตถุประสงค์และหน้าที่ของ CSIRT ให้ชัดเจนและควรระบุในภาพรวมเกี่ยวกับเป้าหมายระยะยาวและเป้าหมายหลักของ CSIRT ด้วย

พันธกิจควรกระชับ (2-3 ประโยค) แต่ก็ไม่ควรสั้นเกินไปจนทำให้เกิดความคลุมเครือเมื่อคำนึงว่า พันธกิจนี้จะไม่เปลี่ยนแปลงไปอีกหลายปี

ไทยเซิร์ตเป็น CSIRT ระดับประเทศของไทยที่จัดตั้งขึ้นเพื่อส่งเสริมให้ธุรกรรมทางอิเล็กทรอนิกส์ มีความมั่นคงปลอดภัย โดยเป็นหน่วยงานกลางในการรับแจ้ง ประสานเพื่อรับมือและแก้ไขเหตุ ภัยคุกคามในขอบเขตครอบคลุมระบบเครือข่ายอินเทอร์เน็ตภายในประเทศไทย และระบบคอมพิวเตอร์ภายใต้โดเมนเนมประเทศไทย (.th)

2.2 ผู้รับบริการ

การทำความเข้าใจกับขอบเขต (scope) ผู้รับบริการ จะช่วยให้ CSIRT สามารถกำหนดความต้องการพื้นฐาน เช่น สินทรัพย์ที่ต้องได้รับการปกป้องและรูปแบบการให้บริการ

CSIRT ของแต่ละองค์กรจะต้องกำหนดขอบเขตของผู้รับบริการให้ชัดเจน ในกรณีที่ขอบเขตผู้รับบริการคาบเกี่ยวกับ CSIRT ขององค์กรอื่น จะต้องกำหนดให้ชัดเจนและแจ้งให้ทราบโดยทั่วกันว่า เมื่อเกิดเหตุภัยคุกคาม ทีมใดที่จะต้องดำเนินการและผู้รับบริการต้องติดต่อใคร

ทั้งนี้ ENISA[9] ได้จำแนกประเภทของ CSIRT ตามขอบเขตผู้รับบริการไว้ ดังนี้

ภาคส่วน	เป้าหมาย	ผู้รับบริการ
CSIRT ภาคการศึกษา	สถาบันวิชาการและการศึกษา เช่น มหาวิทยาลัย หรือหน่วยงานวิจัย	บุคลากรของมหาวิทยาลัยหรือโรงเรียน นักเรียน นักศึกษา
CSIRT ภาคการพาณิชย์	องค์กรด้านการพาณิชย์ ซึ่งอาจเป็นบริษัทต่าง ๆ ผู้ให้บริการอินเทอร์เน็ต (ISP) หรือผู้ให้บริการอื่น ๆ	ลูกค้าที่ชำระเงินเพื่อรับบริการ
CSIRT ภาคโครงสร้างพื้นฐานสำคัญของประเทศ/โครงสร้างพื้นฐานทางสารสนเทศที่สำคัญของประเทศ	การปกป้องข้อมูลสำคัญและระบบเทคโนโลยีสารสนเทศของโครงสร้างพื้นฐานสำคัญต่าง ๆ ในประเทศ	รัฐบาล ภาคส่วนสำคัญและพลเมือง
CSIRT องค์กรภาครัฐ	รัฐบาล	องค์กรภาครัฐ
CSIRT ภายในองค์กร	องค์กรหรือหน่วยงานนั้น ๆ	บุคลากรภายในและส่วนงานด้านเทคโนโลยีสารสนเทศ ขององค์กร

[9] ศึกษาเพิ่มเติมได้ที่ "A Step-by-step approach on how to set up a CSIRT" ปรากฏในหน้าเว็บไซต์ ENISA หน้า 8

ภาคส่วน	เป้าหมาย	ผู้รับบริการ
CSIRT ทหาร	หน่วยงานทหารที่รับผิดชอบโครงสร้างด้านสารสนเทศ	บุคลากรของสถาบันทหารและหน่วยงานใกล้ชิด อาทิ กระทรวงกลาโหม
CSIRT ระดับประเทศ	เน้นการบริการระดับประเทศ โดยถือว่าเป็นผู้ประสานงานเพื่อรับมือและแก้ไขเหตุภัยคุกคาม	ไม่มีผู้รับบริการโดยตรง อย่างไรก็ดี CERT ระดับประเทศอาจมีบทบาทในฐานะองค์กรรัฐที่ดูแลและให้บริการภาครัฐด้วย
CSIRT ภาค SME	จัดตั้งขึ้นเพื่อให้บริการแก่สาขาธุรกิจขององค์กร	SME และเจ้าหน้าที่
CSIRT/ PSIRT[10] ของ vendor	เน้นไปที่ผลิตภัณฑ์เฉพาะของ vendor ส่วนมากมักจะเป็นการแก้ไขช่องโหว่ หรือให้คำแนะนำเพื่อลดผลกระทบกรณีพบการโจมตีผลิตภัณฑ์	เจ้าของผลิตภัณฑ์

ไทยเซิร์ตเป็น CERT ระดับประเทศของไทยและยังปฏิบัติหน้าที่เป็น CSIRT ที่ให้บริการองค์กรภาครัฐอีกด้วย ดังนั้น ผู้รับบริการจึงประกอบด้วยประชาชน เครือข่ายและองค์กรต่าง ๆ ภายในประเทศไทย[10]

[10] ย่อมาจาก Product Security Incident Response Team

2.3 อำนาจหน้าที่

อำนาจหน้าที่ (authority) ของ CSIRT เป็นสิ่งที่กำหนดว่า CSIRT ได้รับอนุญาตให้ทำอะไรได้บ้าง ซึ่งมีตั้งแต่การมีอำนาจเพียงการให้คำแนะนำ จนถึงหยุดบริการที่พบว่ามีช่องโหว่หรือถูกเจาะระบบแล้ว โดยทั่วไป CSIRT ควรมีหน้าที่รับผิดชอบในด้านเทคนิคและไม่ควรมีอำนาจในการปราบปรามหรือลงโทษ เนื่องจากผู้ที่เกี่ยวข้องกับเหตุภัยคุกคามอาจเกรงกลัวและไม่ยอมแจ้งเหตุ

ไทยเซิร์ตทำหน้าที่ประสานเกี่ยวกับเหตุภัยคุกคามกับผู้ที่เกี่ยวข้อง และไม่มีอำนาจหน้าที่อื่น

2.4 ความรับผิดชอบ

โดยปกติความรับผิดชอบของ CSIRT ครอบคลุมการให้บริการต่าง ๆ ซึ่งรายการบริการของ CSIRT จะระบุในบทที่ 6 ทั้งนี้ CSIRT อาจมีหน้าที่เพิ่มเติม เช่น ทำงานร่วมกับองค์กรกำกับดูแลหรือหน่วยงานบังคับใช้กฎหมาย

เมื่อมีหน้าที่เพิ่มเติม CSIRT จะต้องระมัดระวังอย่างยิ่งไม่ให้เกิดผลประโยชน์ทับซ้อน เช่น กรณีที่ CSIRT ได้รับมอบหมายหน้าที่ในการปฏิบัติการควบคู่กับการกำกับดูแลภารกิจ นอกจากนี้ หากเป็น CSIRT ระดับประเทศหรือ CSIRT ภาครัฐ ก็ควรมีการกำหนดบทบาทความรับผิดชอบของหน่วยงานดังกล่าวในกฎหมายให้ชัดเจนด้วย

ไทยเซิร์ตรับมือกับเหตุภัยคุกคามไซเบอร์ต่าง ๆ นอกจากนั้น ยังให้บริการปรึกษา ให้คำแนะนำเชิงเทคนิค สร้างความตระหนักรู้และจัดการฝึกอบรม

2.5 โครงสร้างบริหาร

โครงสร้างบริหารของ CSIRT ภายในองค์กรมักจะขึ้นอยู่กับองค์กรหลักที่กำกับดูแล เช่น CSIRT ระดับชาติมักจะอยู่ภายใต้องค์กรภาครัฐ โดย CSIRT อาจจัดตั้งตามโครงสร้างรูปแบบต่าง ๆ ดังนี้

2.5.1 รูปแบบธุรกิจอิสระ (independent business model)

CSIRT เป็นองค์กรอิสระในตัวเอง มีส่วนบริหารจัดการ ลูกจ้าง และเจ้าหน้าที่สนับสนุนของตนเอง โดยรูปแบบนี้อาจใช้สำหรับ CSIRT ในภาคการพาณิชย์

2.5.2 รูปแบบฝังตัว (embedded model)

CSIRT ภายในองค์กรมักได้รับการกำหนดให้อยู่ในส่วนงานด้านเทคโนโลยีสารสนเทศขององค์กรนั้น ซึ่งก็นับว่าสมเหตุสมผล เนื่องจาก CSIRT มีภารกิจเกี่ยวข้องโดยตรงกับระบบเทคโนโลยีสารสนเทศ อย่างไรก็ดี ในกรณีที่เป็นองค์กรขนาดใหญ่ อาจพิจารณาแยกส่วน CSIRT ออกมาเพื่อให้สามารถดูแลความมั่นคงปลอดภัยของระบบและข้อมูลขององค์กรอย่างทั่วถึง

หาก CSIRT ได้รับการกำหนดให้อยู่ในโครงสร้างองค์กรที่ "ต่ำเกินไป" CSIRT ก็อาจเป็นหน่วยงานที่โดดเดี่ยว กลายเป็น "ของเล่น IT" ที่ไม่มีความสำคัญและไม่ได้รับการสนับสนุนจากหน่วยงานอื่นในองค์กร ในขณะเดียวกัน หาก CSIRT อยู่ในโครงสร้างองค์กรที่ "สูง" พนักงานและเจ้าหน้าที่ขององค์กรนั้นอาจเห็น CSIRT เป็นหอคอยงาช้างและไม่มีปฏิสัมพันธ์กับ CSIRT ในระยะหลัง CSIRT เริ่มได้รับการยอมรับและได้รับการปรับให้ขึ้นไปอยู่ในโครงสร้างองค์กรที่สูงขึ้นเพื่อให้สามารถให้บริการองค์กรได้สะดวก รวดเร็ว และมีประสิทธิภาพ

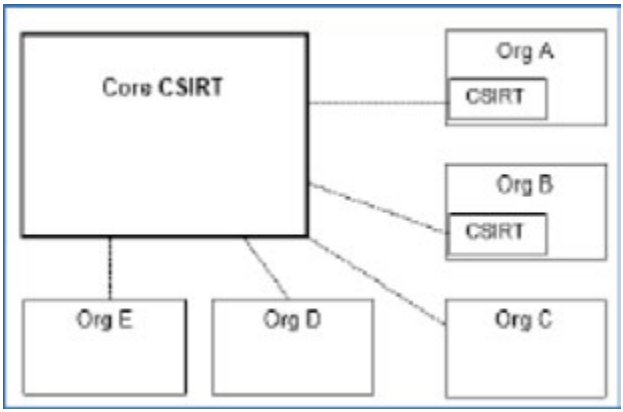
การออกแบบตำแหน่งที่ตั้งของ CSIRT อาจทำได้หลายรูปแบบขึ้นอยู่กับโครงสร้างขององค์กรนั้น โดยสามารถจำแนกตามลักษณะดังนี้

- รูปแบบรวมศูนย์: บุคลากรของ CSIRT ทั้งหมดอยู่ในสำนักงานเดียวกัน
- รูปแบบกระจาย: บุคลากรของ CSIRT กระจายตามสำนักงานต่าง ๆ ในกรณีที่มีองค์กรหลายสาขา โดยรูปแบบนี้อาจจำเป็นต้องทำงานร่วมกันและมีการประสานงานกันเป็นประจำ
- รูปแบบกระจายตามเขตเวลา: เป็นรูปแบบที่พัฒนามาจากรูปแบบกระจาย บางครั้งก็เรียกว่าเป็น "รูปแบบตามพระอาทิตย์" (follow the sun) กล่าวคือ เมื่อพระอาทิตย์ตกในประเทศหนึ่งและ CSIRT ในประเทศนั้นเลิกงาน CSIRT ในอีกประเทศหนึ่งก็จะรับช่วงทำงานต่อ ดังนั้น CSIRT แต่ละแห่งจึงไม่จำเป็นต้องทำงานเป็นกะ

2.5.3 รูปแบบแคมปัส (CSIRT หลัก/ รอง)

สถาบันวิชาการ เช่น มหาวิทยาลัย นิยมใช้รูปแบบนี้ แต่ก็อาจนำมาปรับใช้กับ CSIRT ในหน่วยงานทหารและ SME ได้

รูปแบบมีลักษณะตามรูปภาพที่ 2 องค์กรที่อยู่ในภาคส่วนเดียวกันจัดตั้ง CSIRT กลางเพื่อให้บริการองค์กรสมาชิก และเป็นหน่วยงานกลางประสานกับองค์กรภายนอก อาจอยู่ในรูปแบบขององค์กรอิสระหรือรูปแบบฝังตัว ส่วนองค์กรสมาชิกอาจมีหรือไม่มี CSIRT เป็นของตัวเอง



รูปภาพที 2: โครงสร้างรูปแบบแคมปัส

ไทยเซิร์ตเป็นส่วนหนึ่งขององค์กรรัฐ ปฏิบัติงานตามภารกิจของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) ดังนั้น ไทยเซิร์ตจึงมีรูปแบบฝังตัวและรวมศูนย์

2.6 ความพร้อมในการให้บริการ

ความพร้อมในการให้บริการ (availability) ของ CSIRT ส่วนใหญ่จะขึ้นอยู่กับชั่วโมงการทำงานขององค์กรหลักที่ CSIRT ตั้งอยู่ด้วย โดยหาก CSIRT ไม่ทำงานตลอดยี่สิบสี่ชั่วโมงทุกวันก็จะต้องมีแนวปฏิบัติในการจัดการเหตุภัยคุกคามที่ได้รับแจ้งนอกเวลาทำงาน ซึ่งอาจเป็นแนวทางง่าย ๆ อาทิ การกำหนดให้บุคลากร CSIRT เปิดอ่านข้อความในอีเมลที่ส่งเข้ามาในแต่ละวันให้หมดภายในวันทำการถัดไป นอกจากนั้น อาจกำหนดให้มีบุคลากรเข้าเวรเฝ้าระวังเหตุภัยคุกคาม ซึ่งมีอำนาจตัดสินใจว่าในกรณีเกิดเหตุภัยคุกคาม จะรอถึงวัน

ทำการถัดไปได้หรือไม่ หรือจำเป็นต้องดำเนินการทันที

การกำหนดช่วงเวลาให้บริการของ CSIRT ควรต้องพิจารณาสภาพแวดล้อมขององค์กรด้วย เช่น หากส่วนงานด้านเทคโนโลยีสารสนเทศขององค์กรเปิดทำการในเวลาทำการเท่านั้น การที่ CSIRT จะให้บริการตลอด 24 ชั่วโมงทุกวันก็อาจไม่เกิดประโยชน์ เพราะปัญหาต่าง ๆ ที่เกิดขึ้นไม่ได้รับ การแก้ไขนอกเวลางาน

ทั้งนี้ การให้บุคลากรทำงานนอกเวลางานอาจทำให้มีต้นทุนเพิ่มขึ้นในรูปแบบค่าล่วงเวลา

> ในอดีต ไทยเซิร์ตเปิดทำการระหว่าง 08:30–17:30 วันจันทร์ถึงศุกร์ จนกระทั่งเมื่อต้นปี 2558 ไทยเซิร์ตเริ่มเปิดให้บริการตลอด 24 ชั่วโมงทุกวัน

2.7 บริการหลัก

CSIRT สามารถให้บริการได้หลากหลาย แต่ในช่วงเริ่มต้น อาจจำกัดการให้บริการอยู่เพียง 1 ถึง 2 รายการ และเพิ่มตามความจำเป็นในอนาคต โดยจะกล่าวถึงอย่างละเอียดในบทที่ 6 อย่างไรก็ตาม หัวใจหลักของบริการ CSIRT คือการรับมือและแก้ไขปัญหาเหตุภัยคุกคาม (จะได้กล่าวถึงต่อไปในบทที่ 5) ในขณะที่บริการที่สำคัญรองลงมาคือบริการแจ้งเตือน และเผยแพร่ข้อมูลข่าวสาร

> ไทยเซิร์ตให้บริการเกือบทุกรายการที่ระบุในบทที่ 6

2.8 ข้อกำหนดด้านบุคลากร

2.8.1 อัตราเจ้าหน้าที่

CSIRT ไม่ได้กำหนดตายตัวว่า ควรมีบุคลากรทางเทคนิคจำนวนเท่าใด เพราะ CSIRT แต่ละแห่งย่อมมีความแตกต่างทั้งในเรื่องสภาพแวดล้อมในการทำงาน ผู้รับบริการ และผู้ที่มีส่วนเกี่ยวข้องต่าง ๆ อย่างไรก็ดี อาจใช้แนวทางต่อไปนี้เป็นแนวทางเบื้องต้นในการกำหนดจำนวนบุคลากร

- เพื่อให้ CSIRT สามารถให้บริการภารกิจหลัก 2 รายการ ได้แก่ (1) การรับมือและแก้ไขเหตุ ภัยคุกคามและ (2) การแจ้งเตือนและเผยแพร่ข้อมูลข่าวสาร CSIRT ควรมีพนักงานเต็มเวลา อย่างน้อย 4 คน
- สำหรับ CSIRT ที่ให้บริการมากกว่า 2 รายการและปฏิบัติงานเฉพาะในเวลาทำการและดูแลระบบของตนเอง ควรมีเจ้าหน้าที่เต็มเวลาอย่างน้อย 6-8 คน
- สำหรับ CSIRT ครบวงจรที่บุคลากรทำงานตลอดยี่สิบสี่ชั่วโมงโดยไม่มีวันหยุด (3 กะต่อวัน) ควรมีพนักงานเต็มเวลาอย่างน้อย 12 คน

แนวทางข้างต้นได้พิจารณาครอบคลุมถึงสิทธิประโยชน์เรื่องวันลาป่วยและวันลาพักผ่อนของพนักงานแล้ว

ไทยเซิร์ตมีบุคลากรทั้งสิ้น 43 คน

2.8.2 ความสามารถ

ENISA[11] กำหนดความสามารถหลัก (key competencies) สำหรับผู้เชี่ยวชาญทางเทคนิคใน CSIRT ไว้หลายประการ โดยในการรับบุคคลเข้าทำงานอาจต้องตรวจสอบคุณวุฒิทางเทคนิค จากใบประกาศนียบัตรและวุฒิการศึกษา นอกจากนี้ บุคลากรของ CSIRT ยังอาจจำเป็นต้องมีทักษะเฉพาะด้านอื่น ๆ เพื่อให้บริการด้านอื่น ๆ ของ CSIRT ด้วย

ความสามารถสำหรับเจ้าหน้าที่ด้านเทคนิคทั่วไป ประกอบด้วย

<u>ขีดความสามารถส่วนบุคคล</u>

- มีความยืดหยุ่น สร้างสรรค์ และสามารถทำงานเป็นทีม
- มีทักษะการคิดวิเคราะห์
- สามารถสื่อสารเรื่องเทคนิคที่ยากให้เป็นเรื่องง่าย
- สามารถรักษาความลับและทำงานอย่างเป็นระบบ
- มีทักษะในการบริหารจัดการ
- สามารถทำงานในสภาวะกดดันได้
- มีทักษะในการเขียนและการสื่อสาร
- เปิดใจแจะพร้อมเรียนรู้สิ่งใหม่ ๆ

<u>ขีดความสามารถเชิงเทคนิค</u>

- มีความรู้พื้นฐานเกี่ยวกับอินเทอร์เน็ตและโปรโตคอลต่าง ๆ
- มีความรู้เกี่ยวกับระบบ Linux และ Unix (ขึ้นอยู่กับระบบปฏิบัติการและเครื่องมือที่องค์กรใช้)

---

[11] ศึกษาเพิ่มเติมได้ที่ "A Step-by-step approach on how to set up a CSIRT" ปรากฏในหน้าเว็บไซต์ ENISA หน้า 25

- มีความรู้เกี่ยวกับระบบ Windows
(ขึ้นอยู่กับระบบปฏิบัติการและเครื่องมือที่องค์กรใช้)
- มีความรู้เกี่ยวกับอุปกรณ์เครือข่ายต่าง ๆ
(router, switches, DNS, Proxy, Mail และอื่น ๆ)
- มีความรู้เกี่ยวกับ internet applications
(SMTP, HTTP(S), FTP, telnet, SSH และอื่น ๆ)
- มีความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์
(DDoS, Phishing, Defacement, Sniffing และอื่น ๆ)
- มีความรู้เกี่ยวกับการประเมินความเสี่ยงและการนำองค์ความรู้ไปใช้ปฏิบัติงาน

ขีดความสามารถอื่น ๆ

- สามารถทำงานในรูปแบบตลอด 24 ชั่วโมง หรือพร้อมปฏิบัติการเมื่อมีเหตุฉุกเฉิน หรือสถานการณ์ (ขึ้นอยู่กับหน้าที่ความรับผิดชอบ)
- ระยะทางและเวลาที่ใช้เดินทางมาทำงานในกรณีฉุกเฉินอยู่ในเกณฑ์ที่ยอมรับได้
- ระดับการศึกษา
- ประสบการณ์การทำงานด้านความมั่นคงปลอดภัยทางไซเบอร์

2.8.3 แนวปฏิบัติ แนวทางการดำเนินงาน จรรยาบรรณ

แนวปฏิบัติ แนวทางการดำเนินงาน จรรยาบรรณเป็นระเบียบหรือแนวทางสำหรับเจ้าหน้าที่ใน CSIRT ให้ทำงานอย่างเป็นมืออาชีพโดยอาจครอบคลุมถึงการปฏิบัติตนเมื่ออยู่นอกเวลางาน ซึ่งมีความสำคัญไม่น้อยไปกว่ากันเนื่องจากอาจส่งผลกระทบต่อความมั่นคงปลอดภัยของข้อมูลและระบบที่ดูแล ทั้งนี้ CSIRT อาจนำแนวปฏิบัติที่

จัดทำขึ้นโดย Trusted Introducer[12] มาปรับใช้ได้

เจ้าหน้าที่ของ CSIRT ต้องมีความน่าเชื่อถือ องค์กรควรหลีกเลี่ยงการว่าจ้างผู้ที่มีประวัติไม่ดี เช่น เคยเจาะระบบหรือขโมยข้อมูลองค์กร เนื่องจากการสร้างความไว้เนื้อเชื่อใจให้ CSIRT อาจใช้เวลาหลายปี แต่ความน่าเชื่อถือนั้นอาจหายไปในชั่วข้ามคืนก็ได้ ดังนั้นแนวปฏิบัติจึงให้ความสำคัญกับการคัดกรองบุคลากรที่จะเข้ามาทำงาน

ไทยเซิร์ตใช้แนวปฏิบัติ CSIRT จาก Trusted Introducer

2.8.4 การฝึกอบรม

มี 2 รูปแบบ: (1) การฝึกอบรมภายในสำหรับเจ้าหน้าที่ CSIRT บรรจุใหม่เพื่อแนะนำ ให้ทราบว่า CSIRT ทำงานอย่างไร และ (2) การฝึกอบรมภายนอกสำหรับเจ้าหน้าที่ประจำเพื่อพัฒนาทักษะอย่างต่อเนื่อง และเรียนรู้พัฒนาการทางเทคโนโลยี รวมถึงภัยคุกคามใหม่ ๆ

องค์กรต่อไปนี้มีหลักสูตรการฝึกอบรมที่มีคุณภาพสำหรับเจ้าหน้าที่ของ CSIRT

- TRANSITS[13]
- CERT/CC[14]

---

[12] Trusted Introducer CSIRT Code of Practice: <https://www.trusted-introducer.org/CCoPv21.pdf>
[13] TRANSITS: <https://www.terena.org/activities/transits/>
[14] CERT/CC: <http://cert.org/training/>

- SANS[15]
- FIRST[16]

ทั้งนี้ CSIRT ควรพิจารณาจัดสรรงบประมาณไว้จำนวนหนึ่งสำหรับการเข้าร่วมการประชุมและการสัมมนาต่าง ๆ ซึ่งถือเป็นส่วนหนึ่งของการฝึกอบรมต่อเนื่องเช่นกัน (ศึกษาเพิ่มเติมได้ที่ข้อ 4.6)

ไทยเซิร์ตใช้ประโยชน์จากการอบรมขององค์กรทั้งหมดที่กล่าวมาข้างต้น

2.9 โครงสร้างพื้นฐานและเครื่องมือ

สถานที่ สิ่งอำนวยความสะดวก เครือข่ายและโครงสร้างพื้นฐานด้านโทรคมนาคมของ CSIRT ควรออกแบบอย่างรอบคอบเพื่อปกป้องข้อมูลสำคัญที่จัดเก็บ และเพื่อคุ้มครองความปลอดภัย ของเจ้าหน้าที่ ดังนั้น CSIRT ควรสร้างพื้นที่จัดเก็บข้อมูลและพื้นที่ใช้สอยของเจ้าหน้าที่ให้มีระบบป้องกันที่เป็นไปตามข้อกำหนดเดียวกันกับศูนย์ข้อมูล (data center)

ข้อควรพิจารณาด้านความมั่นคงปลอดภัยทางกายภาพ

- มีพื้นที่ปฏิบัติงานที่ปลอดภัยหรือมีศูนย์ปฏิบัติการด้านความมั่นคงปลอดภัย (SOC) เป็นที่ตั้งเซิร์ฟเวอร์ของ CSIRT และสำหรับ
  จัดเก็บข้อมูล
- มีห้องปฏิบัติงานที่ปลอดภัยและเก็บเสียงสำหรับการสืบสวนและ

[15] SANS Institute: <https://www.sans.org/>
[16] FIRST: <https://www.first.org/>

หารือเกี่ยวกับการดำเนินงานของ CSIRT

- มีห้องที่สามารถเก็บรักษาข้อมูลและเอกสารในรูปแบบที่ไม่ใช่อิเล็กทรอนิกส์
- มีเครื่องทำลายเอกสารและมีอุปกรณ์ที่สามารถทำลายสื่อเก็บข้อมูลที่ไม่ใช้แล้ว
- ควรแยกบุคลากรของ CSIRT ออกจากส่วนอื่น ๆ ขององค์กร และควบคุมพื้นที่เข้าออก
- มีนโยบายเกี่ยวกับผู้เข้ามาเยี่ยมชม โดยอาจกำหนดรวมเป็นนโยบายควบคุมพื้นที่เข้าออก

ข้อควรพิจารณาเกี่ยวกับอุปกรณ์ด้านเทคโนโลยีสารสนเทศ

- มีกลไกการสื่อสารที่มีความมั่นคงปลอดภัย เช่น โทรศัพท์ โทรสาร และอีเมล
- มีการตั้งค่าเพื่อเพิ่มความมั่นคงปลอดภัย (hardening) แก่ระบบต่าง ๆ รวมถึงเครื่องคอมพิวเตอร์ที่ใช้ในการทำงาน
- มีเครือข่าย CSIRT แยกจากเครือข่ายของสำนักงานอื่น ๆ ในองค์กร
- มีเครื่องมือช่วยติดตั้งโปรแกรมและระบบต่าง ๆ ในอุปกรณ์ได้อย่างรวดเร็ว ในกรณีที่ต้องติดตั้งระบบและโปรแกรมใหม่เนื่องจาก นำอุปกรณ์ออกไปนอกพื้นที่มั่นคงปลอดภัยหรือนำไปใช้ในการวิเคราะห์มัลแวร์ เพื่อให้มั่นใจว่าไม่มีมัลแวร์อยู่ในเครื่องหลังเสร็จสิ้นการวิเคราะห์

ข้อควรพิจารณาเกี่ยวกับอุปกรณ์เฉพาะทางของ CSIRT

- มีระบบสำหรับรับแจ้งเหตุและติดตามการดำเนินการ (ticketing system)

- มีฐานข้อมูลการติดต่อของบุคลากร ผู้ที่มีส่วนเกี่ยวข้อง ผู้รับบริการและผู้ติดต่ออื่น ๆ
- มีอุปกรณ์อื่น ๆ ที่ CSIRT จำเป็นต้องใช้ในการให้บริการ
- มีอุปกรณ์ตาม ภาคผนวก ค: อุปกรณ์ด้านความมั่นคงปลอดภัยที่ใช้ทั่วไป

ทั้งนี้ บริการของ CSIRT บางประเภท เช่น การตรวจพิสูจน์พยานหลักฐานดิจิทัลอาจต้องมีข้อกำหนดเพิ่มเติมเกี่ยวกับพื้นที่ปฏิบัติการและเทคโนโลยีสารสนเทศที่ใช้งาน

ไทยเซิร์ตดำเนินการตามองค์ประกอบทุกข้อข้างต้น

2.10 ความสัมพันธ์ภายในและภายนอกองค์กร

CSIRT ควรสร้างความสัมพันธ์ที่ดีเพื่อให้ได้รับการสนับสนุนและการยอมรับจากองค์กรที่กำกับดูแล เมื่อมีเหตุภัยคุกคามเกิดขึ้น ทั้ง CSIRT และองค์กรเหล่านี้จะต้องร่วมมือกันเพื่อแก้ไขปัญหา หารือถึงการดำเนินการต่าง ๆ ความสัมพันธ์ที่ดีจะช่วยให้การทำงานเป็นไปอย่างรวดเร็วและราบรื่น ทั้งนี้ CSIRT ควรมีความสัมพันธ์ที่ดี ไม่เฉพาะต่อส่วนงานสารสนเทศขององค์กร แต่ยังต้องไม่ลืมส่วนงานด้านอื่น ๆ เช่น ด้านความมั่นคงปลอดภัยทางกายภาพ ด้านการสื่อสาร ด้านกฎหมาย และด้านบุคลากร

ความสัมพันธ์ภายนอกที่เป็นประโยชน์ต่อ CSIRT ได้แก่ ความสัมพันธ์กับ CSIRT ระดับประเทศ ผู้บังคับใช้กฎหมาย และหน่วยงาน

กำกับดูแล หากมีเครือข่าย CSIRT ขององค์กรที่อยู่ในภาคส่วนเดียวกัน (sector-based CSIRT) หรือเครือข่าย ISAC ในภาคส่วนที่ CSIRT ปฏิบัติงานอยู่[17] ก็ควรพิจารณาเข้าร่วมเป็นสมาชิกเครือข่ายเหล่านี้ด้วย

ทั้งนี้ โปรดศึกษาเพิ่มเติมในข้อ 4.6 สำหรับตัวอย่างความร่วมมือระหว่างประเทศที่อาจเป็นประโยชน์ต่อ CSIRT ขององค์กร

ไทยเซิร์ตสร้างความสัมพันธ์ทั้งภายในและภายนอกกับหน่วยงานต่าง ๆ ตามที่ระบุข้างต้น

2.11 รูปแบบการรับเงินทุนสนับสนุนค่าใช้จ่าย

องค์กรต้องมีแนวทางชัดเจนในการสนับสนุนด้านงบประมาณแก่ CSIRT เพื่อสามารถให้บริการในระยะยาวได้อย่างราบรื่น ควรมีแผนจัดสรรงบประมาณสำหรับจัดตั้งทีม และการปฏิบัติงาน ซึ่งจำแนกเป็น ค่าใช้จ่าย
ด้านบุคลากร สถานที่ สิ่งอำนวยความสะดวก ซอฟต์แวร์ ฮาร์ดแวร์ ตลอดจนต้นทุนในการให้บริการต่าง ๆ

รูปแบบการสนับสนุนงบประมาณ:

- องค์กรหรือหน่วยงานที่ CSIRT อยู่ภายใต้ เป็นผู้รับผิดชอบค่าใช้จ่ายทั้งหมดและ CSIRT ไม่มีรายได้ใด ๆ

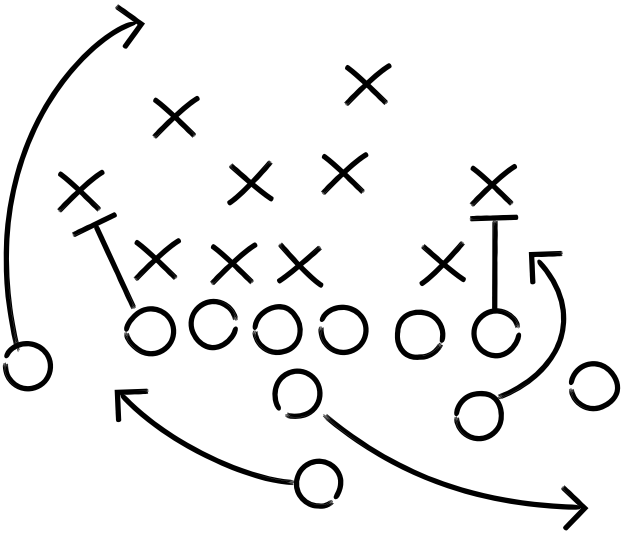
[17] ศึกษาเพิ่มเติมจาก "Establishing a Sector-based ISAC" โดย ThaiCERT

- CSIRT อาจได้รับการสนับสนุนจากองค์กรอื่นเต็มจำนวนหรือบางส่วนแบบให้เปล่า โดยหากเป็นเช่นนั้น ต้องพิจารณาว่า
  - ใครเป็นผู้สนับสนุน
  - จุดประสงค์ของการสนับสนุนคืออะไร
  - การสนับสนุนมีมูลค่าเท่าใดและจะครอบคลุมการปฏิบัติการมากน้อยเพียงใด
  - แหล่งทุนมีความมั่นคงเพียงใด
  - การสนับสนุนจากแหล่งทุนมีระยะเวลานานเท่าใด

CSIRT ควรระบุรายละเอียดเกี่ยวกับการสนับสนุนงบประมาณแบบให้เปล่า โดยมีข้อมูลต่าง ๆ อาทิ ผู้ให้และแหล่งทุน จุดประสงค์ จำนวนเงิน ระยะเวลาของการสนับสนุน

- CSIRT อาจคิดค่าบริการจากการให้บริการทั้งภายในและภายนอกองค์กร หรือได้รับการสนับสนุนผ่านสมาคมขององค์กรต่าง ๆ เช่น มหาวิทยาลัยในเครือข่ายการวิจัย หรือช่องทางการสนับสนุนทางการเงินที่ผสมผสานระหว่างรูปแบบใดรูปแบบหนึ่งดังที่ได้กล่าวมาแล้ว

ไทยเซิร์ตได้รับการสนับสนุนทางการเงินทั้งหมดจากรัฐบาลและยังมีรายได้บางส่วนจากการให้บริการเฉพาะด้าน



3. การขออนุมัติจัดตั้ง CSIRTจากผู้บริหารระดับสูง

การจัดตั้ง CSIRT ควรได้รับการสนับสนุนจากผู้บริหารระดับสูงสุดในหน่วยงาน (สำหรับวิสาหกิจเชิงพาณิชย์ ภาคเอกชน ผู้บริหารดังกล่าวอาจเป็นคณะกรรมการบริษัท และสำหรับ CSIRT ภาครัฐ ผู้บริหารดังกล่าวหมายถึงคณะรัฐมนตรี) ทั้งนี้ การสนับสนุนดังกล่าวมีความจำเป็นเพื่อให้

- นโยบายที่เกี่ยวข้องต่าง ๆ มีผลบังคับใช้และปฏิบัติทั่วทั้งองค์กร
- ได้รับการสนับสนุนในการดำเนินการสำคัญหรือมีค่าใช้จ่ายสูง
- เกิดความต่อเนื่องในการปฏิบัติการต่าง ๆ แม้ในช่วงที่มีการเปลี่ยนโครงสร้างองค์กรหรือการตัดงบประมาณ

ผู้บริหารขององค์กรจะมองส่วนงานด้านเทคโนโลยีสารสนเทศแตกต่างออกไปจากบุคลากรที่ทำงานด้านเทคนิค การโน้มน้าวให้ผู้บริหารระดับสูงเชื่อว่า CSIRT จะช่วยให้องค์กรบรรลุเป้าหมายขององค์กร จำเป็นต้องปรับการใช้ภาษา โดยหลีกเลี่ยงการใช้ศัพท์ และการอธิบายทางเทคนิค

ตัวอย่างของเหตุผลต่าง ๆ ที่ควรนำมาใช้เพื่อโน้มน้าวผู้บริหารระดับสูง ได้แก่

- ข้อกำหนดด้านกฎหมายหรือสัญญาที่กำหนดให้ระบบขององค์กรต้องมีความมั่นคงปลอดภัยในระดับหนึ่ง

- CSIRT ที่ได้รับการฝึกอบรมและมีอุปกรณ์พร้อมจะช่วยลดความเสียหายที่อาจเกิดขึ้นจากเหตุภัยคุกคาม (ทั้งในแง่ของความเสียหายจากการหยุดทำงานและในแง่ของความเสียหายต่อภาพลักษณ์ ชื่อเสียง) เนื่องจากองค์กรสามารถจำกัดขอบเขตความเสียหายและฟื้นตัวจากการโจมตีได้อย่างรวดเร็ว ดังนั้น CSIRT จะช่วยประหยัดงบประมาณขององค์กรได้
- บริการเชิงป้องกันของ CSIRT อาจช่วยลดช่องโหว่และความเสี่ยงในการเกิดเหตุภัยคุกคามก่อนที่จะระบบขององค์กรจะถูกโจมตี
- การรวมงานด้านความมั่นคงปลอดภัยไซเบอร์ใน CSIRT จะช่วยลดความซ้ำซ้อนของงานด้านนี้ในส่วนงานต่าง ๆ ขององค์กร รวมทั้งยังช่วยให้องค์กรมีมาตรฐานด้านความมั่นคงปลอดภัยเพิ่มขึ้น
- การมี CSIRT อาจเป็นจุดเด่นที่เป็นเอกลักษณ์ขององค์กร โดยแสดงให้เห็นถึงความมุ่งมั่นขององค์กรในการรักษาความมั่นคงปลอดภัย (ช่วยให้สามารถประชาสัมพันธ์ได้ว่า “ข้อมูลของคุณปลอดภัยเมื่ออยู่กับเรา")
- ใช้คำพูดโน้มน้าวง่าย ๆ แต่ส่งผลกระทบทางจิตวิทยา เช่น “คู่แข่งของเราก็ทำแบบนี้เหมือนกัน"

3.1 รูปแบบการรายงานผลการปฏิบัติงานของ CSIRT

การรายงานผลการปฏิบัติงานขององค์กร โดยทั่วไปมักอยู่ในรูปแบบการจัดประชุมอย่างสม่ำเสมอ หรือการจัดทำรายงานรายไตรมาสหรือรายปี อย่างไรก็ดี CSIRT มักถูกมองว่าใช้ต้นทุนใน

การดำเนินงานสูง ซึ่งแท้จริงแล้ว CSIRT อาจช่วยองค์กรประหยัดงบประมาณได้ ดังนั้น CSIRT จึงไม่เพียงแค่ใช้รูปแบบการรายงานผลการปฏิบัติงานตามปกติ แต่ควรเพิ่มตัวเลขมูลค่าความเสียหายที่ลดลงจากการดำเนินการรับมือ หรือป้องกันไม่ให้เกิดความเสียหายลงในรายงานด้วยเพื่อแสดงให้เห็นว่า CSIRT มีส่วนช่วยในเรื่องงบประมาณขององค์กรเพียงใด

ไทยเซิร์ตยึดหลักการความโปร่งใสของหน่วยงานภาครัฐ จึงจัดทำรายงานสถิติเหตุภัยคุกคามที่ได้รับแจ้งประจำเดือนและเผยแพร่บนเว็บไซต์ อีกทั้งยังได้นำสถิติมาวิเคราะห์ เผยแพร่เป็นรายงานประจำปีทั้งในรูปแบบอิเล็กทรอนิกส์และรูปแบบเอกสาร

4. การจัดตั้ง CSIRT และสภาวะแวดล้อมในการทำงาน

4.1 รวบรวมและจัดทำรายการแหล่งข้อมูลด้านต่าง ๆ

รวบรวมแหล่งข้อมูลด้านต่าง ๆ เช่น ข้อมูลที่เกี่ยวกับภัยคุกคาม ข้อมูลติดต่อองค์กร ซึ่งเป็นประโยชน์ต่อภารกิจดังนี้

- การเฝ้าระวังเหตุภัยคุกคามด้วยระบบที่รวบรวมข้อมูลอัตโนมัติ
- การแจ้งเตือนเหตุภัยคุกคามจากแหล่งอื่น ๆ (อาทิ อีเมล โทรศัพท์ แบบฟอร์มบนเว็บไซต์)
- การรับข้อมูลเกี่ยวกับภัยคุกคามและช่องโหว่ต่าง ๆ
- การสื่อสารทางตรงกับผู้มีส่วนเกี่ยวข้อง ผู้รับบริกา/ องค์กร ในระหว่างเกิดเหตุภัยคุกคาม (การจัดทำบัญชีผู้ติดต่อ)
- การสื่อสารทั่วไปกับผู้มีส่วนเกี่ยวข้อง ผู้รับบริการ องค์กร (การสร้างความตระหนักรู้และการประชาสัมพันธ์)

4.2 จัดทำนโยบายรับมือและแก้ไขเหตุภัยคุกคาม

นโยบายรับมือและแก้ไขเหตุภัยคุกคามควรระบุผู้รับผิดชอบในการรับมือเหตุภัยคุกคามแต่ละรูปแบบ และระบุองค์กรภายนอกที่สามารถช่วยเหลือ

รายละเอียดที่ควรกำหนดในนโยบาย มีดังนี้

- ประเภทเหตุภัยคุกคามที่อยู่ภายใต้ขอบเขตบริการรับมือของ CSIRT
- ผู้ที่ทำหน้าที่วิเคราะห์ รับมือเหตุภัยคุกคาม
- สิ่งต้องดำเนินการด้านกฎหมาย
- การรายงานและการปฏิบัติที่อยู่นอกเหนือขอบเขตของ CSIRT

นโยบายควรมีรายละเอียดพื้นฐานในการรับมือและแก้ไขปัญหาเหตุภัยคุกคามโดยครอบคลุมถึงประเด็นต่อไปนี้

- กรอบเวลาในการรับมือและแก้ไขปัญหา
- แนวทางสำหรับการยกระดับการรับมือ
- การจัดหมวดหมู่และการจัดลำดับความสำคัญของเหตุภัยคุกคาม
- การติดตามและเก็บข้อมูลเหตุภัยคุกคาม
- การจบการรับมือเหตุภัยคุกคาม
- การแสวงหาความช่วยเหลือเพิ่มเติมเพื่อประโยชน์ในการวิเคราะห์หรือเพื่อฟื้นฟูระบบภายหลังเกิดเหตุภัยคุกคาม

ภาพรวมขั้นตอนการรับมือและแก้ไขเหตุภัยคุกคามที่สมบูรณ์จะกล่าวถึงต่อไปในบทที่ 5

4.3 จัดทำนโยบายการจัดการและแลกเปลี่ยนข้อมูล

กำหนดชั้นความลับของข้อมูลทั้งที่อยู่ในรูปแบบอิเล็กทรอนิกส์และเอกสาร โดยอาจแบ่งเป็น ข้อมูลที่มีความละเอียดอ่อน (sensitive information) ข้อมูลลับ หรือข้อมูลที่เปิดเผยต่อสาธารณชน รวมถึงกำหนดวิธีการจัดการข้อมูลเหล่านั้นทั้งในแง่ของการจัดเก็บ การรับส่ง การเข้าถึง ฯลฯ ทั้งนี้ รูปแบบชั้นความลับของข้อมูลที่นิยมใช้คือ traffic light protocol[18]

นโยบายการจัดการและแลกเปลี่ยนข้อมูลควรกำหนด (1) ประเภทของข้อมูลที่ไม่ควรเผยแพร่ออกไปนอก CSIRT (2) ประเภทของข้อมูลที่สามารถเก็บบนอุปกรณ์สื่อสารเคลื่อนที่หรืออุปกรณ์ที่ไม่ปลอดภัย (3) ประเภทของข้อมูลที่ต้องรับส่งและจัดเก็บอย่างมั่นคงปลอดภัย รวมถึงไม่ควรนำมาแบ่งปันกับบุคคลที่ไม่ได้รับอนุญาต และ (4) การจัดการและแบ่งปันข้อมูลที่ได้รับจาก CSIRT อื่น ภายใน CSIRT และภายในองค์กร

4.3.1 กฎหมายและกฎระเบียบต่าง ๆ

เนื่องจากอินเทอร์เน็ตเป็นสภาพแวดล้อมที่มีพัฒนาการไปอย่างรวดเร็วในขณะที่กฎหมายยังคงค่อย ๆ ปรับตัวตามหลังเทคโนโลยีในหลาย ๆ ประเด็นจึงยังไม่มีกฎหมายใดรองรับ และแม้จะมีกฎหมาย

[18] traffic light protocol : <http://www.us-cert.gov/>

ครอบคลุมในบางประเด็นแล้วก็ยังไม่เคยนำข้อบทกฎหมายนั้นมาใช้ในกระบวนการยุติธรรม นอกจากนั้น ยังอาจมีกรณีที่เนื้อความในกฎหมายบางฉบับขัดแย้งกับกฎหมายอื่น ๆ อีกด้วย

CSIRT มีหน้าที่ปฏิบัติตามกฎหมายของประเทศและความตกลงระหว่างประเทศ รวมถึงมาตรฐานต่าง ๆ ที่รัฐบาลแนะนำหรือบังคับใช้ และมาตรฐานที่กำหนดในสัญญากับลูกค้า บางประเทศมีกฎหมายที่ต้องแจ้งองค์กรกำกับดูแลในกรณีที่เกิดเหตุภัยคุกคามที่ส่งผลกระผลกับข้อมูล ซึ่งการแจ้งควรอยู่ในกระบวนการรับมือเหตุภัยคุกคาม (ศึกษาเพิ่มเติมได้ที่ข้อ 2.4)

มิติด้านกฎหมายไม่เพียงจะมีผลบังคับใช้กับการจัดการข้อมูลภายในประเทศเท่านั้น แต่ยังรวมถึงการแลกเปลี่ยนข้อมูลระหว่างประเทศด้วย อีกทั้งยังอาจจำกัดสิ่งที่ CSIRT สามารถดำเนินการได้ในระหว่างการรับมือและแก้ไขเหตุภัยคุกคาม (เช่น อาจไม่อนุญาตให้ดักรับข้อมูลเพื่อนำไปวิเคราะห์การโจมตีเนื่องจากเหตุผลด้านสิทธิส่วนบุคคล)

องค์กรควรปรึกษาผู้เชี่ยวชาญทางกฎหมายและตรวจสอบว่าการดำเนินการของ CSIRT นั้นสอดคล้องกับกฎหมายทั้งในระดับชาติและระดับนานาชาติหรือไม่

กฎหมายและนโยบายที่เกี่ยวข้องอาจประกอบด้วย:[19]

<u>กฎหมายระดับประเทศ</u>

- กฎหมายที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ การโทรคมนาคม และสื่อมวลชน

[19] ดูเพิ่มเติมได้ที่ "A Step-by-step approach on how to set up a CSIRT" ปรากฏในหน้าเว็บไซต์ ENISA หน้า 25

- กฎหมายเกี่ยวกับการปกป้องคุ้มครองข้อมูลและสิทธิส่วนบุคคล
- กฎหมายและกฎระเบียบเกี่ยวกับการเก็บรักษา/ ถือครองข้อมูล
- กฎหมายเกี่ยวกับการเงิน การบัญชี และการบริหารองค์กร
- แนวปฏิบัติและหลักการเกี่ยวกับบรรษัทภิบาลและการอภิบาลเทคโนโลยีสารสนเทศ
- สำหรับประเทศไทย: พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์และพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (มาตรา 35)[20]

<u>กฎหมายและสัญญาระหว่างประเทศ</u>

- ความตกลง Basel II โดยเฉพาะส่วนที่เกี่ยวกับการจัดการความเสี่ยงในการปฏิบัติการ (Basel II Agreement)
- อนุสัญญาว่าด้วยอาชญากรรมทางไซเบอร์โดยคณะมนตรีแห่งสหภาพยุโรป (Council of Europe - Convention on Cybercrime)
- อนุสัญญาว่าด้วยสิทธิมนุษยชนโดยคณะมนตรีแห่งสหภาพยุโรป ส่วนมาตรา 8 เกี่ยวกับสิทธิส่วนบุคคล (Council of Europe - Convention on Human Rights)
- มาตรฐานการบัญชีระหว่างประเทศ (International Accounting Standards หรือ IAS มีส่วนที่กล่าวถึงการควบคุมด้านเทคโนโลยีสารสนเทศ)

[20] ศึกษาเพิ่มเติมเกี่ยวกับแนวทางการบังคับใช้ พ.ร.บ. ว่าด้วยการทำธุรกรรมทางอิเล็กทรอนิกส์ ได้ที่ https://www.etda.or.th/publishing-detail/information-technology-law-7-edition.html

มาตรฐานต่าง ๆ

- มาตรฐานสหราชอาณาจักร (British Standard) BS7799 ส่วนความมั่นคงปลอดภัยทางสารสนเทศ
- มาตรฐานระหว่างประเทศ ISO2700x เกี่ยวกับระบบการบริหารจัดการความมั่นคงปลอดภัยทางสารสนเทศ (ISMS - Information Security Management Systems)
- มาตรฐานเยอรมนี IT-Grundschutzbuch มาตรฐานฝรั่งเศส EBIOS และมาตรฐานระดับชาติของประเทศอื่น ๆ

4.3.2 การสื่อสารอย่างมั่นคงปลอดภัยด้วย PGP

PGP (Pretty Good Privacy) หรือ GPG (GNU Privacy Guard) เป็นโปรแกรมที่ CSIRT นิยมใช้เพื่อรักษาความความมั่นคงปลอดภัยในการรับส่งข้อมูลประเภทต่าง ๆ โดยเฉพาะอีเมล ด้วยการเข้ารหัสลับ (encryption) ถอดรหัสลับ (decryption) และลงลายมือชื่อ (sign) กระบวนการทั้ง 3 อาศัยชุดรหัสที่เรียกว่ากุญแจสาธารณะ (public key) และกุญแจส่วนตัว (private key) ซึ่งกุญแจส่วนตัวผู้ใช้งาน PGP ควรเก็บเป็นความลับ[21]

PGP ถือเป็นเครื่องมือที่สำคัญ CSIRT ที่ต้องการเข้าเป็นสมาชิก FIRST หรือ Trusted Introducer จำเป็นต้องสามารถใช้งานโปรแกรมดังกล่าวในการสื่อสาร

ในการนำ PGP มาใช้งานในทีมควรพิจารณาประเด็นต่าง ๆ ดังนี้

- ผู้ที่เก็บรักษากุญแจส่วนตัว (private key) อาจเป็นผู้บริหาร หรือ เจ้าหน้ารับมือเหตุภัยคุกคาม

[21] ศึกษาการใช้งาน PGP เพิ่มเติมได้ที่ https://www.thaicert.or.th/papers/general/2011/pa2011ge002.html

- การดำเนินการเกี่ยวกับกุญแจ ตั้งแต่การสร้าง การจัดเก็บ และการเผยแพร่
- ประเด็นสำคัญในจัดการกุญแจ เช่น
  - ใครจะเป็นผู้สร้างกุญแจ
  - ควรสร้างกุญแจประเภทใด
  - กุญแจควรมีขนาดเท่าใด
  - กุญแจควรมีอายุการใช้งานนานเท่าใด
  - ควรมี revocation certificate หรือไม่ เพื่อประกาศหยุดการใช้งานกุญแจในกรณีที่กุญแจส่วนตัวถูกขโมย
  - ควรเก็บกุญแจและ revocation certificate ไว้ที่ใด
  - ใครเป็นผู้ลงลายมือชื่อ (sign) กุญแจ
  - นโยบายในการจัดการรหัสผ่านและระบบเก็บรหัสผ่าน
  - ใครเป็นผู้บริหารจัดการกุญแจ รวมถึงนโยบายและกระบวนการที่เกี่ยวข้องในการบริหารจัดการกุญแจ

4.4 การสำรวจซอฟต์แวร์และฮาร์ดแวร์ที่ใช้งานในองค์กร

CSIRT สำรวจและจัดทำข้อมูลสรุปเกี่ยวกับผลิตภัณฑ์ซอฟต์แวร์และฮาร์ดแวร์พร้อมเวอร์ชันที่ใช้งานในองค์กร เพื่อให้คำแนะนำเกี่ยวกับผลิตภัณฑ์ได้อย่างเหมาะสม

นอกจากนั้น หาก CSIRT ให้บริการแจ้งเตือนและเผยแพร่ข้อมูลข่าวสารด้วย ก็อาจขอให้พนักงานในองค์กรสมัครรับข่าวสารแจ้งเตือนโดยระบุรายการผลิตภัณฑ์ใช้งานอยู่เพื่อรับคำแนะนำที่เกี่ยวกับผลิตภัณฑ์เหล่านั้น

4.5 การประชาสัมพันธ์

เมื่อจัดตั้ง CSIRT เรียบร้อยแล้ว ควรแจ้งให้ผู้มีส่วนเกี่ยวข้องและผู้รับบริการทราบถึงแนวทางการติดต่อและบริการ และหาก CSIRT จะเป็นผู้ติดต่อ (Point of Contact) หลักในการรับแจ้งและประสานงาน เพื่อรับมือเหตุภัยคุกคาม CSIRT ควรแจ้งให้ผู้รับบริการและผู้มีส่วนเกี่ยวข้องทั้งหมดให้ทราบว่าต้องรายงานเหตุภัยคุกคามไปที่ CSIRT โดยตรง

รูปแบบการประชาสัมพันธ์โดยทั่วไปคือการจัดทำเอกสารข้อมูลและบริการต่าง ๆ ของ CSIRT และเผยแพร่บนอินทราเน็ต (สำหรับ CSIRT ภายในองค์กร) หรือบนอินเทอร์เน็ต โดยตัวอย่างรูปแบบเอกสารดังกล่าวสามารถศึกษาจาก RFC2350[22]

ในการปฏิบัติงานได้อย่างมีประสิทธิภาพจำเป็นต้องอาศัยความไว้เนื้อเชื่อใจและความเคารพจากผู้รับบริการ โดยความไว้เนื้อเชื่อใจอาจเริ่มต้นจากสิ่งเล็ก ๆ และขยายผลต่อไป เมื่อ CSIRT เริ่มได้รับความเชื่อมั่น และไว้วางใจ ผู้รับบริการเหล่านั้นก็จะเริ่มตระหนักและสนับสนุน CSIRT มากขึ้น

นอกจากนี้ CSIRT อาจเผยแพร่ข่าวสารเป็นประจำหรือตามโอกาส

---

[22] RFC2350 <https://www.ietf.org/rfc/rfc2350.txt>

เกี่ยวกับเหตุภัยคุกคามที่ได้รับแจ้ง บทเรียนที่ได้จากการรับมือ รวมถึงหัวข้อน่าสนใจต่าง ๆ เพื่อสร้างความตระหนักด้านความมั่นคงปลอดภัยไซเบอร์ให้กับผู้รับบริการในองค์กร

4.6 การสร้างเครือข่าย

แต่ละองค์กรส่วนใหญ่เผชิญกับเหตุภัยคุกคามลักษณะคล้าย ๆ กัน และสามารถ แลกเปลี่ยน เรียนรู้จากเหตุภัยคุกคามต่าง ๆ ที่เกิดขึ้น การแบ่งปันประสบการณ์และบทเรียนที่ได้รับจะเป็นประโยชน์สำหรับทุกฝ่ายในการพัฒนาแนวปฏิบัติ ปรับปรุงความมั่นคงปลอดภัยของระบบ

น้อยครั้งนักที่เหตุภัยคุกคามจะเกี่ยวข้องกับองกรค์เดียว ส่วนมากเหตุภัยคุกคามมักจะเชื่อมโยงกับที่อื่น ๆ โดยผู้อยู่เบื้องหลังการโจมตีมักจะอยู่คนละที่ อยู่คนละประเทศ และยิ่งไปกว่านั้น การโจมตีครั้งหนึ่งอาจมีที่มาจากหลายแห่งในเวลาเดียวกัน เช่น การโจมตีแบบ DDoS ดังนั้น ในการรับมือและแก้ปัญหาเหตุภัยคุกคามลักษณะนี้ CSIRT จะต้องทำงานร่วมกับทีมอื่น ๆ โดยเฉพาะทีมที่ดูแลเครือข่ายที่เป็นแหล่งที่มาของการโจมตี

ปัจจุบัน มีหลายเครือข่ายที่ร่วมมือในด้านต่าง ๆ เช่น การอบรม การรับมือเหตุภัยคุกคาม ตัวอย่างที่เห็นได้ชัดคือ FIRST[23] (Forum of Incident Response and Security Teams) ซึ่งมี CSIRT หลายร้อยแห่งทั่วโลกเป็นสมาชิก APCERT[24] (Asia Pacific CERT) ซึ่งเป็นเครือข่ายความร่วมมือสำหรับ CSIRT ระดับประเทศในภูมิภาคเอเชีย

[23] FIRST: <http://www.first.org/>
[24] APCERT: <http://www.apcert.org>

แปซิฟิก Trusted Introducer[25] สำหรับ CSIRT ทั้งหมดในยุโรป หรือ Africa CERT[26] เครือข่าย CSIRT ในทวีปแอฟริกา ซึ่งการเป็นสมาชิกในเครือข่ายเหล่านี้ล้วนเป็นประโยชน์อย่างมาก

เครือข่ายเหล่านี้ รวมถึง CSIRT ที่มีขนาดใหญ่ยังจัดการประชุมและสัมมนาที่เปิดให้ผู้สนใจเข้าร่วมเป็นประจำเพื่อฝึกอบรมและยังเป็นโอกาสอันดีที่บุคลากรของ CSIRT จะสร้างเครือข่ายและความสัมพันธ์กับเจ้าหน้าที่ CSIRT อื่น ๆ ด้วย

4.7 การซ้อมรับมือเหตุภัยคุกคาม

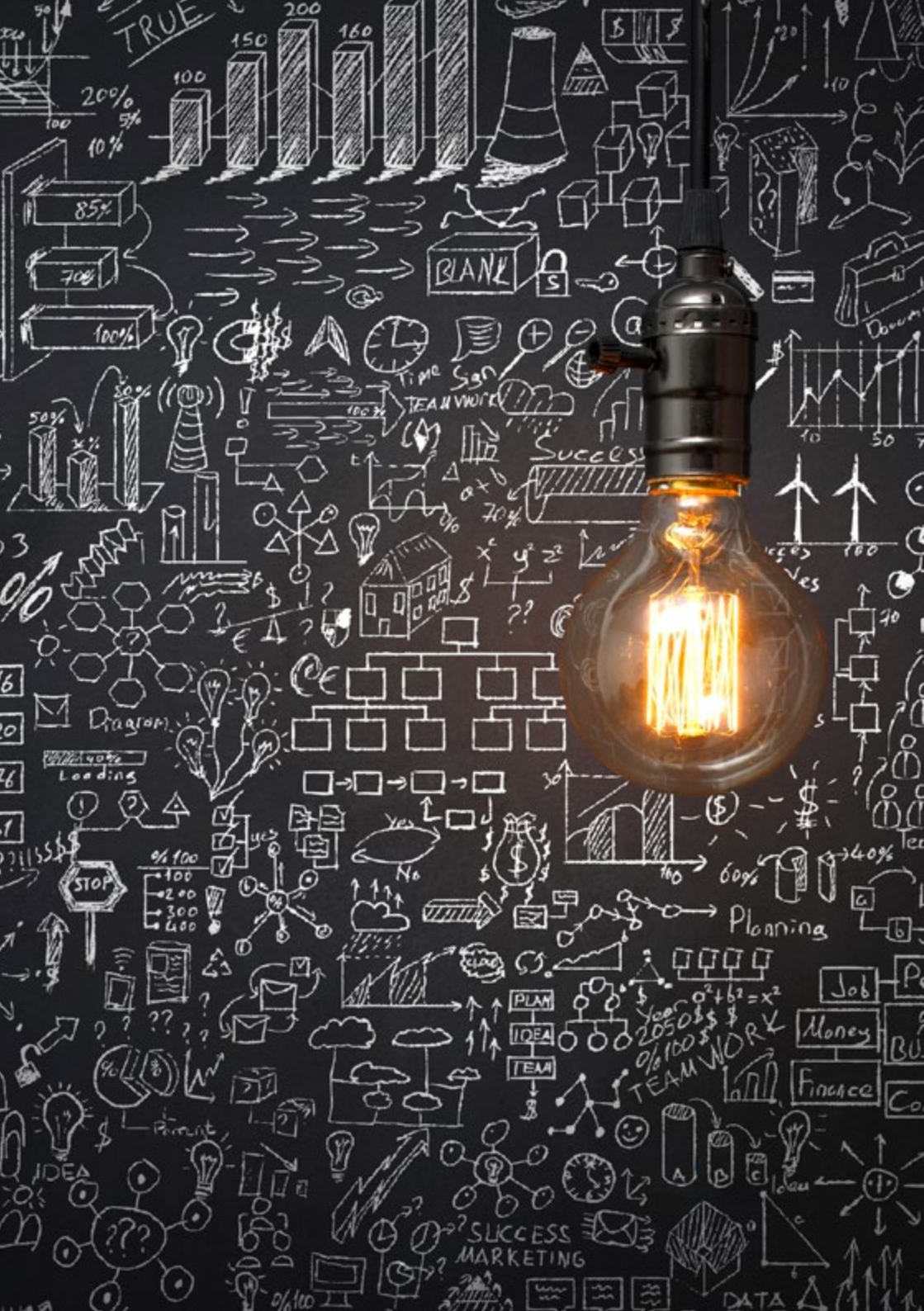
เนื่องจากเหตุภัยคุกคามขนาดใหญ่ไม่ได้เกิดขึ้นเป็นประจำ CSIRT จึงอาจยังไม่มีประสบการณ์เพียงพอในการดำเนินการตามขั้นตอนและกระบวนการที่วางไว้ เมื่อเกิดเหตุภัยคุกคามขึ้นจริงอาจเป็นปัญหาได้

CSIRT ควรจัดการซ้อมรับมือเหตุภัยคุกคามในลักษณะ table-top exercise ซึ่งเป็นการจำลองสถานการณ์เกิดเหตุภัยคุกคาม ผู้เข้าร่วมการซ้อมจะได้รับบทบาทสมมติและต้องแก้ไขเหตุการณ์ การซ้อมรับมือจะช่วยให้เกิดความชำนาญ และเห็นช่องทางในการปรับปรุงกระบวนการให้มีประสิทธิภาพยิ่งขึ้น

ทั้งนี้ ENISA ได้เผยแพร่เอกสารและเครื่องมือที่จำเป็นสำหรับการซ้อมรับมือโดยไม่เสียค่าใช้จ่ายบนเว็บไซต์ ผู้ที่สนใจสามารถดาวน์โหลดได้ที่ https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material

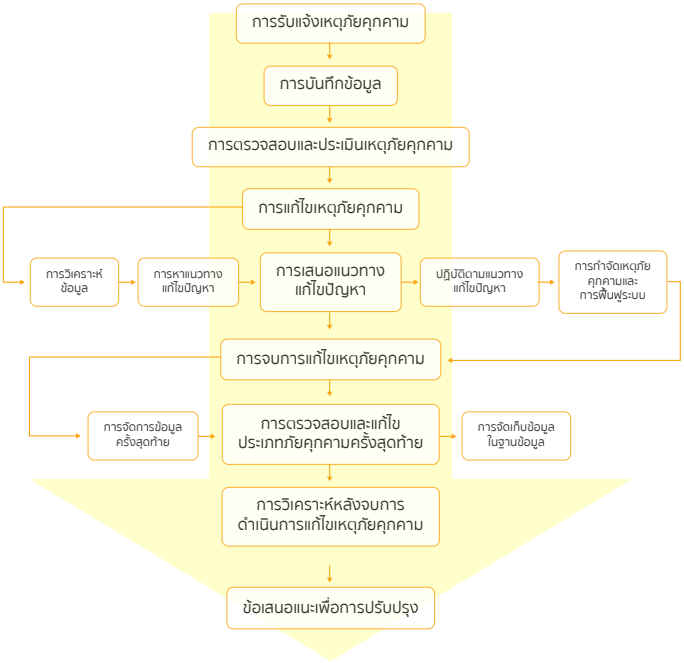
---

[25] Trusted Introducer: <https://www.trusted-introducer.org/>
[26] AfricaCERT: <http://www.africacert.org/>


TRUE
BLANK
Time
Sign
TEAMWORK
Success
Diagram
Loading
STOP
Planning
PLAN
IDEA
TEAM
Job
Money
Finance
IDEA
SUCCESS
MARKETING
DATA

5. กระบวนการรับมือและแก้ไขเหตุภัยคุกคาม

ในบทที่ 5 จะอธิบายกระบวนการพื้นฐานที่จำเป็นในการรับมือและแก้ไขเหตุภัยคุกคามโดยมีแผนผังขั้นตอนตามรูปภาพที่ 3 ส่วนเครื่องมือแนะนำที่อาจพิจารณานำมาใช้ จะระบุไว้ใน ภาคผนวก ค: เครื่องมือด้านความมั่นคงปลอดภัย



รูปภาพที่ 3: แผนผังขั้นตอนการรับมือและแก้ไขเหตุภัยคุกคาม

5.1 การรับแจ้งเหตุภัยคุกคาม

5.1.1 การแจ้งเตือน

CSIRT ได้รับแจ้งเหตุภัยคุกคาม ซึ่งมีที่มาจากหลายแหล่งโดยอาจมาจากการพบเองหรือแหล่งอื่น ๆ แจ้งมา เช่น

- การแจ้งโดยระบบเฝ้าระวังเครือข่าย
- สมัครเพื่อรับข่าวสารทางอีเมลกลุ่มเครือข่ายด้านความมั่นคงปลอดภัยไซเบอร์
- การสมัครเพื่อรับข้อมูลในรูปแบบ automatic feed โดยสามารถศึกษาเพิ่มเติมที่ ภาคผนวก ง: แหล่งข้อมูล
- วิทยุ โทรทัศน์ และหนังสือพิมพ์

CSIRT สามารถศึกษาภาคผนวก ข: ตัวอย่างแบบฟอร์มการรายงานเหตุภัยคุกคาม ซึ่งจะระบุข้อมูลต่าง ๆ ที่จำเป็นในการรายงานเหตุภัยคุกคาม และเพื่อให้การติดต่อเป็นไปอย่างสะดวกและคล่องตัว CSIRT อาจสร้างช่องทางติดต่อรับแจ้งเหตุภัยคุกคาม ได้แก่

- อีเมล
- โทรศัพท์
- แบบฟอร์มติดต่อทางเว็บไซต์
- สื่อสังคมออนไลน์

อย่างไรก็ดี ช่องทางการติดต่อที่เหล่านี้เกือบทั้งหมดต้องใช้อินเทอร์เน็ต โดยเฉพาะหากใช้ VoIP ในการติดต่อทางโทรศัพท์ ซึ่งหากการเชื่อมต่ออินเทอร์เน็ตมีปัญหาก็อาจส่งผลให้ไม่สามารถติดต่อ CSIRT ดังนั้นจึงต้องคำนึงถึงช่องทางการติดต่อสำรองไว้ด้วย

5.1.2 การบันทึกข้อมูล

เหตุภัยคุกคามทั้งหมดที่ได้รับแจ้งควรจะได้รับการบันทึกใน ticketing system ซึ่งเป็นระบบสำหรับรับแจ้งเหตุและติดตามการดำเนินการ โดยจะมีการระบุหมายเลข ticket สำหรับแต่ละเหตุภัยคุกคามที่ได้รับแจ้ง เพื่อใช้อ้างอิงเวลาติดต่อสื่อสาร

ticket system จากผู้พัฒนาบางรายสามารถรับแจ้งเหตุภัยคุกคามทางอีเมล โดยจะสร้างหมายเลข ticket ให้กับอีเมลที่เข้ามาโดยอัตโนมัติ

ข้อมูลเหตุภัยคุกคามที่ได้รับแจ้งควรจัดการให้อยู่ในที่เดียวกัน เนื่องจากข้อมูลอาจมีความสัมพันธ์กับข้อมูลที่ได้รับแจ้งก่อนหน้า เช่น การแพร่กระจายของมัลแวร์ในส่วนงานขององค์กรโดยก่อนหน้านี้ได้รับแจ้งการแพร่ระบาดของมัลแวร์เดียวกันจากอีกส่วนงาน จะเห็นได้ว่าเป็นเหตุการณ์ที่ความสัมพันธ์กัน และอาจจัดให้อยู่ใน ticket หมายเลขเดียวกัน

ข้อดีอีกอย่างของการมีศูนย์กลางในการจัดการข้อมูลคือ ในกรณีที่พบว่าเหตุภัยคุกคามที่ได้รับแจ้งมีความคล้ายคลึงกับที่ได้รับแจ้งก่อนหน้า ก็อาจนำช่องทางการติดต่อหรือวิธีการจัดการเดิมมาใช้งานได้

ticket system ที่ CSIRT นิยมใช้และไม่เสียค่าใช้จ่าย ได้แก่ RITR (Request Tracker for Incident Response)[27] และ OTRS (Open Technology Real Services)[28]

---

[27] RITR: <https://bestpractical.com/>
[28] OTRS: <https://www.otrs.com/>

ไทยเซิร์ตใช้ระบบ ticket system ที่ชื่อ RTIR

5.2 การตรวจสอบและประเมินเหตุภัยคุกคาม

ขั้นตอนนี้ถือว่าเป็นหนึ่งในขั้นตอนที่สำคัญที่สุดในกระบวนการรับมือและแก้ไขเหตุภัยคุกคามเพราะเป็นขั้นตอนที่ต้องมีการตัดสินใจสำคัญ อันดับแรก CSIRT ต้องตรวจสอบว่าเหตุภัยคุกคามที่ได้รับแจ้งเป็นเหตุภัยคุกคามจริงหรือไม่ แหล่งที่มาของรายงานเชื่อถือได้มากน้อยเพียงใด จากนั้นควรพิจารณา ดังนี้

- เหตุภัยคุกคามที่เกิดขึ้นอยู่ใต้ขอบเขตการทำงานและความรับผิดชอบของ CSIRT หรือไม่มีความเกี่ยวข้องกับผู้รับบริการหรือไม่
- เกิดผลกระทบอะไรบ้าง
- เกิดความเสียหายร้ายแรงเพียงใด
- มีความเร่งด่วนมากน้อยแค่ไหน ความเสียหายจะเพิ่มขึ้นตามเวลาที่ดำเนินไปหรือไม่ จะลุกลามไปยังผู้รับบริการ ผู้มีส่วนเกี่ยวข้องอื่น ๆ หรือไม่

หลังจากตรวจสอบ เป็นการตอบสนองต่อผู้แจ้ง โดยมีเนื้อหาดังนี้

- ตอบรับทราบการแจ้งเตือน
- อธิบายสิ่งที่จะดำเนินการ
- สิ่งที่ผู้แจ้งควรกระทำในระหว่างรอ CSIRT รับมือและแก้ปัญหาเหตุภัยคุกคามจนสำเร็จ

CSIRT อาจพิจารณาจัดทำ template ข้อความที่ใช้ในการตอบสนองผู้แจ้งเพื่อช่วยประหยัดเวลาของผู้ปฏิบัติ

5.2.1 การระบุประเภทและความเร่งด่วนของเหตุภัยคุกคาม

เป็นการระบุเบื้องต้นว่าเหตุภัยคุกคามที่ได้รับแจ้งว่าอยู่ในประเภทใด สามารถกลับมาแก้ไขเมื่อมีข้อมูลเพิ่มเติม และเมื่อพิจารณาประเภทของเหตุภัยคุกคามร่วมกับประเภทผู้แจ้ง จะสามารถระบุความเร่งด่วนในการดำเนินการรวมถึงทรัพยากรที่จำเป็นในการรับมือเหตุภัยคุกคาม

ตัวอย่าง การกำหนดความรุนแรงและความเร่งด่วนของเหตุภัยคุกคามที่ใช้โดยหน่วยงานภาครัฐและองค์กรขนาดใหญ่บางแห่ง ดังตารางที่ 1 เช่น หากได้รับรายงานการแพร่ระบาดของ trojan โดยหน่วยงานภาครัฐถือว่ามีความเร่งด่วนเป็นอันดับ 2 ในขณะที่หากผู้แจ้งเป็นองค์กรลูกค้าถือว่ามีความเร่งด่วนเป็นอันดับ 1

กลุ่มสี	ความรุนแรง	ตัวอย่าง
แดง	สูงมาก	DDoS, เว็บไซต์ Phishing
ส้ม	สูง	Trojan การเข้าถึงโดยไม่ได้รับอนุญาต
เหลือง	ปกติ	Spam ประเด็นการละเมิดลิขสิทธิ์

ลำดับความเร่งด่วน	ภาครัฐ	ลูกค้า SLA	อื่น ๆ
สีแดง	1	1	2
สีส้ม	2	1	3
สีเหลือง	3	2	3

ตารางที่ 1: ตัวอย่างการกำหนดความรุนแรงและความเร่งด่วนของเหตุภัยคุกคามที่ใช้โดยหน่วยงานภาครัฐและองค์กรขนาดใหญ่บางแห่ง

การจัดประเภทเหตุภัยคุกคามยังมีประโยชน์เชิงสถิติอีกด้วย โดยช่วยให้ CSIRT สามารถ

- ระบุแนวโน้มของเหตุภัยคุกคามแต่ละประเภท
- จัดทำสถิติรายงานผู้บริหาร
- เปรียบเทียบกับข้อมูลของ CSIRT อื่น ๆ

การจัดประเภทเหตุภัยคุกคามที่นิยมใช้ ได้แก่

- ประเภทเหตุภัยคุกคามโดย LatvianCERT[29]
- ประเภทเหตุภัยคุกคามโดย eCSIRT.net[30]
- กำหนดโดย CSIRT เอง

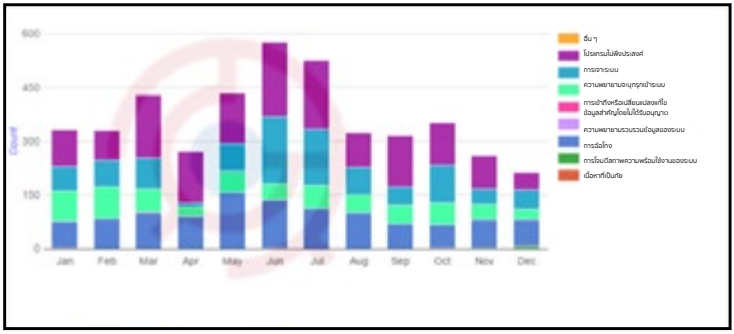
ทั้งนี้ แม้การกำหนดประเภทเหตุภัยคุกคามด้วยตนเองอาจเหมาะสมกับองค์กร แต่อาจมีปัญหาในการนำข้อมูลไปเปรียบเทียบกับ CSIRT ขององค์กรอื่น

หากต้องการกำหนดเอง ไม่ควรสร้างประเภทที่ซับซ้อนหรือละเอียดเกินไป (เช่น กำหนดประเภทของเหตุภัยคุกคามสำหรับมัลแวร์ทุกชนิด) เนื่องจากถึงแม้จะช่วยให้สามารถมองภาพรวมประเภทของเหตุภัยคุกคามที่ CSIRT รับมือได้อย่างละเอียดมาก แต่ก็หมายความว่าต้องใช้เวลาอย่างมากในการกำหนดประเภทของเหตุภัยคุกคามแทนที่จะใช้เวลานั้นมาแก้ไขปัญหา

---

[29] <https://www.enisa.europa.eu/topics/csirt-cert-services/community-projects/existing-taxonomies>
[30] <https://www.enisa.europa.eu/topics/csirt-cert-services/community-projects/existing-taxonomies>

ไทยเซิร์ตใช้ประเภทเหตุภัยคุกคามของ eCSIRT.net และเผยแพร่สถิติเหตุภัยคุกคามที่ได้รับแจ้งรายเดือนบนเว็บไซต์[31]



รูปภาพที่ 4: สถิติเหตุภัยคุกคามรายเดือนที่ไทยเซิร์ตได้รับแจ้งในปี 2558

ขั้นตอนสุดท้ายในส่วนนี้ คือการกำหนดผู้รับผิดชอบเหตุภัยคุกคาม ซึ่งจะเป็นผู้ดำเนินการต่อไป

5.3 การแก้ไขเหตุภัยคุกคาม

5.3.1 การวิเคราะห์ข้อมูล

สิ่งที่สำคัญในขั้นตอนนี้คือการรวบรวมข้อมูลให้ได้มากที่สุดเท่าที่จะทำได้จากรายงานและระบบที่ได้รับผลกระทบ เพื่อให้ทีมได้ภาพรวมเกี่ยวกับเหตุภัยคุกคามและสาเหตุการเกิดเหตุภัยคุกคามที่สมบูรณ์ที่สุด ตัวอย่างข้อมูลที่รวบรวม เช่น

[31] สถิติรายเดือนของ ThaiCERT: <https://www.thaicert.or.th/statistics/statistics-en.html>

- ข้อมูลติดต่อโดยละเอียด
- รายละเอียดของเหตุภัยคุกคามที่เกิด
- ประเภทของเหตุภัยคุกคามที่เสนอโดยผู้แจ้งเหตุภัยคุกคาม
- ข้อมูลเกี่ยวกับระบบปฏิบัติการและเครือข่ายที่เกี่ยวข้อง
- ข้อมูลเวลาและเขตเวลาของเหตุภัยคุกคาม
- ข้อมูลระบบรักษาความมั่นคงปลอดภัยที่ติดตั้ง
- ความรุนแรงของเหตุภัยคุกคาม
- ไฟล์ล็อกที่แนบมากับรายงานแจ้งเหตุภัยคุกคาม

นอกจากนี้ อาจหาข้อมูลที่เกี่ยวข้องกับเหตุภัยคุกคามจากฐานข้อมูลของระบบหรืออุปกรณ์ต่าง ๆ เช่น

- Netflow data
- ล็อกในเราเตอร์
- ล็อกใน proxy server
- ล็อกในเว็บแอปพลิเคชัน
- ล็อกในเมลเซิร์ฟเวอร์
- ล็อกใน DHCP เซิร์ฟเวอร์
- ล็อกในเซิร์ฟเวอร์ที่ให้บริการยืนยันตัวตน (authentication server)
- ฐานข้อมูลต่าง ๆ ที่เกี่ยวข้อง
- อุปกรณ์เกี่ยวกับความมั่นคงปลอดภัย เช่น Firewall หรือ IDS (Intrusion Detection System)

เมื่อแหล่งที่มาของการโจมตีทางไซเบอร์อยู่นอกขอบเขต นอกองค์กร หรือหน่วยงาน CSIRT อาจจำเป็นต้องใช้ข้อมูลจากแหล่งอื่น ๆ มาประกอบการวิเคราะห์ด้วย ในการขอข้อมูลเพิ่มเติม CSIRT ต้อง

- ระบุแหล่งข้อมูล
- ติดต่อประสานงานแหล่งข้อมูล เพื่อขอข้อมูลที่จำเป็น

แม้การหาข้อมูล รายละเอียดให้ได้มากที่สุดนั้นเป็นสิ่งสำคัญ แต่ก็ต้องคำนึงถึงความเป็นไปได้ในทางปฏิบัติด้วยโดยไม่ควรรอข้อมูลจากแหล่งอื่นนานจนเกินไป เนื่องจากเหตุภัยคุกคามอาจดำเนินไปเรื่อย ๆ และความล่าช้าที่เกิดจากการรอข้อมูลจนครบถ้วนก็อาจกลายเป็นปัญหาหรือทำให้ผู้บุกรุกมีเวลาเพิ่มขึ้นในการปกปิดร่องรอย โดยทั่วไปแล้ว ข้อมูลที่หาได้เพียงร้อยละ 20 ถือเป็นสี่ในห้าขององค์ความรู้ที่จำเป็นต้องใช้ในการแก้ไขเหตุภัยคุกคาม

5.3.2 การหาแนวทางแก้ไขปัญหา

ภายหลังจากที่ได้ข้อมูลทั้งหมดจากขั้นตอนก่อนหน้านี้ จะเป็นการหาแนวทางแก้ไขปัญหาที่ดีที่สุดจากทางเลือกต่าง ๆ โดยพิจารณาข้อสังเกตและข้อสรุปจากการวิเคราะห์ข้อมูลที่รวบรวมหรือจากการหารือระดมสมอง ตัวอย่างผลลัพธ์อาจเป็นแนวทางการตั้งค่าอุปกรณ์หรือเครื่องมือเพื่อแก้ไขหรือลดผลกระทบของปัญหา

5.3.3 การเสนอแนวทางปฏิบัติ

ในการแก้ไขเหตุภัยคุกคาม CSIRT อาจต้องเสนอแนวทางปฏิบัติหนึ่งหรือสองแนวทาง ทั้งนี้ ขึ้นอยู่กับความซับซ้อนของเหตุภัยคุกคามนั้น ๆ ด้วย ในการนำเสนอ จะต้องคำนึงถึงผู้ฟัง บุคลากรด้านเทคนิคย่อมเข้าใจแนวทางแก้ปัญหาเชิงเทคนิค แต่หากจำเป็นต้องดำเนินการอื่น ๆ หรือหากแนวทางปฏิบัติมีค่าใช้จ่ายสูง ก็อาจต้อง

ปรับเนื้อหานำเสนอให้ฝ่ายบริหารหรือฝ่ายการเงินเข้าใจด้วย

ตัวอย่างของแนวทางปฏิบัติ เช่น

- การยุติการให้บริการชั่วคราว
- การตรวจหามัลแวร์ในเครือข่าย
- การแก้ไขช่องโหว่ในระบบ
- การตั้งค่าระบบเพื่อเพิ่มความมั่นคงปลอดภัย
- การแยกระบบออกจากเครือข่าย
- การตรวจสอบระบบ
- การหาข้อมูลเพิ่มเติม (อาจว่าจ้างบุคคลภายนอก)
- การซื้อบริการเสริม เช่น บริการป้องกันจากการโจมตี DDoS
- การยกระดับการแก้ปัญหาให้ผู้บริหารหรือคณะกรรมการด้านกฎหมายร่วมตัดสินใจ
- การร่วมมือแก้ไขปัญหากับฝ่ายสื่อสารองค์กรหรือฝ่ายประชาสัมพันธ์
- การร่วมมือกับหน่วยงานบังคับใช้กฎหมายในกระบวนการสืบสวนอาชญากรรม
- หากระบบหรือแอปพลิเคชันที่องค์กรใช้งาน มีการดูแลโดยองค์กรภายนอก เช่น ระบบบนคลาวด์ CSIRT ก็อาจจำเป็นต้องส่งคำแจ้งเตือนหรือทำงานร่วมกับองค์กรเหล่านั้น

5.3.4 ปฏิบัติตามแนวทางแก้ไขปัญหา

ประเด็นที่ควรพิจารณาหลังจากปฏิบัติตามแนวทางแก้ไขปัญหาที่ดำเนินการเสร็จสิ้นแล้ว

- ระบบสามารถให้บริการตามปกติได้หรือไม่
- การปฏิบัตินั้นสามารถแก้ไขปัญหาได้เสร็จสิ้นหรือไม่
- ทราฟฟิกในเครือข่ายได้รับการเฝ้าระวังอย่างเหมาะสมหรือไม่

หากส่วนที่ตกเป็นเป้าหมายของการโจมตียังมีช่องโหว่หรือแนวทางการแก้ไขปัญหาไม่สามารถแก้ไขเหตุภัยคุกคามอย่างสมบูรณ์ ต้องทำตามขั้นตอนก่อนหน้าอีกครั้งเพื่อหาแนวทางการแก้ไขปัญหาที่เหมาะสมต่อไป

5.3.5 การกำจัดปัญหาและการฟื้นฟูระบบ

หลังจากที่แก้ไขต้นตอปัญหาที่สร้างความเสียหายให้กับระบบเรียบร้อย เป็นการฟื้นฟูระบบให้สามารถให้บริการตามปกติ อย่างไรก็ตาม ในบางกรณี อาจต้องใช้เวลาเพิ่มเติมพอสมควร เช่น กรณีที่มีการดำเนินการทางกฎหมายเพื่อสืบสวนทางอาญา นอกจากนี้ ส่วนงานที่รับผิดชอบด้านการสื่อสารองค์กรหรือการประชาสัมพันธ์อาจเข้ามามีส่วนร่วมประชาสัมพันธ์ข้อมูลให้สาธารณชนทราบความคืบหน้าของการดำเนินการอย่างต่อเนื่อง

5.4 การจบการแก้ไขเหตุภัยคุกคาม

CSIRT ควรมีนโยบายที่ชัดเจนว่าจะจบการดำเนินการรับมือและแก้ไขเหตุภัยคุกคามเมื่อใดและอย่างไร เนื่องจากระยะเวลาที่เหตุภัยคุกคามดำเนินไปมักมีการใช้เป็นปัจจัยในการประเมินการทำงานด้วย

CSIRT บางแห่งเลือกที่จะปล่อยให้สถานะ ticket ของเหตุภัยคุกคามที่ได้รับแจ้งใน ticket system คงสถานะเป็น open หรือ “ระหว่างการดำเนินการ” มีการอัปเดตสถานะเพิ่มรายละเอียดการดำเนินการเรื่อย ๆ จนกว่าเหตุภัยคุกคามจะได้รับการแก้ไขโดยสมบูรณ์ บางแห่งตัดสินใจจบการดำเนินการปิด ticket (เปลี่ยนสถานะเป็น closed) เมื่อได้รับการแก้ไขในเชิงเทคนิคตามขั้นตอนที่กำหนด ซึ่งอาจเลือกดำเนินการถึงการติดตามประเมินผล (follow-up) แล้วจึงจบการดำเนินการ

5.4.1 การจัดการข้อมูลครั้งสุดท้าย

แนบเอกสารที่เกี่ยวข้องทุกอย่างเข้าไปใน ticket จากนั้นจึงดำเนินการแจ้งฝ่ายต่าง ๆ ที่เกี่ยวข้องตามประเด็น ดังนี้

- คำอธิบายสั้น ๆ เกี่ยวกับเหตุการณ์
- ผลลัพธ์จากการดำเนินการรับมือและแก้ไขเหตุภัยคุกคาม
- สิ่งที่พบและข้อเสนอแนะ

5.4.2 การตรวจสอบและแก้ไขประเภทภัยคุกคามครั้งสุดท้าย

เมื่อมีข้อมูลเกี่ยวกับเหตุภัยคุกคามที่ได้รับแจ้งครบถ้วนแล้ว ควรตรวจสอบความถูกต้องของประเภทภัยคุกคามที่ได้ระบุไว้ หากไม่ถูกต้องให้แก้ไขและปรับปรุงการระบุประเภทภัยคุกคามให้แม่นยำยิ่งขึ้น

5.4.3 การจัดเก็บข้อมูลในฐานข้อมูล

ในการจัดเก็บข้อมูลที่อยู่ใน ticket ที่มีสถานะ “closed” หรือจบการดำเนินการ หลังการดำเนินการรับมือเหตุภัยคุกคามเสร็จสิ้น ควรเก็บในลักษณะที่สามารถสืบค้นได้ในภายหลัง เพื่อใช้อ้างอิงวิธีการรับมือกรณีที่เกิดเหตุภัยคุกคามลักษณะใกล้เคียงกันในอนาคต

5.5 การวิเคราะห์หลังจบการดำเนินการแก้ไขเหตุภัยคุกคาม

ควรเรียนรู้จากบทเรียนที่ได้รับจากเหตุภัยคุกคามที่เกิดขึ้นเพื่อป้องกันไม่ให้เกิดเหตุเช่นนี้ขึ้นอีกในอนาคตหรือปรับปรุงกระบวนการให้รับมือและแก้ไขเหตุภัยคุกคามต่าง ๆ ได้รวดเร็วขึ้น

ตัวอย่างของบทเรียนที่ได้และข้อเสนอแนะเพื่อนำไปปรับปรุงและพัฒนา ได้แก่

- การเพิ่มเติมเนื้อหาหรือคำอธิบายในนโยบายความมั่นคงปลอดภัยขององค์กร
- การพัฒนาปรับปรุงโครงสร้าง สถาปัตยกรรมของเครือข่าย
- การพัฒนาปรับปรุงกลไกการตรวจจับเหตุภัยคุกคาม
- การจัดหาเครื่องมือเพื่อเพิ่มความสามารถวิเคราะห์
- การได้เรียนรู้วิธีรับมือเหตุภัยคุกคามรูปแบบใหม่ ๆ

CSIRT อาจแบ่งปันบทเรียนที่ได้รับแก่เครือข่ายความร่วมมือเพื่อให้สมาชิกได้รับประโยชน์จากองค์ความรู้ใหม่ ๆ ด้วย (ศึกษาเพิ่มเติมที่ข้อ 4.6)

6. บริการเพิ่มเติม

ตารางด้านล่างแสดงบริการต่าง ๆ ที่ CSIRT มักให้บริการ ทั้งนี้ตามที่ CERT/CC[32] ระบุไว้

บริการเชิงรับ เพื่อตอบสนองภัยคุกคาม	บริการเชิงรุก เพื่อป้องกันภัยคุกคาม	บริการบริหารคุณภาพทางด้านความมั่นคงปลอดภัย
• **การแจ้งเหตุภัยคุกคาม** • **การรับมือและแก้ไขเหตุภัยคุกคาม** **- การวิเคราะห์เหตุภัยคุกคาม** **- การรับมือและแก้ไขเหตุภัยคุกคาม ณ สถานที่เกิดเหตุ (on site)** **- การสนับสนุนการรับมือและแก้ไขเหตุภัยคุกคาม** **- การประสานงานเพื่อรับมือและแก้ไขเหตุภัยคุกคาม** • การจัดการกับช่องโหว่ด้านความมั่นคงปลอดภัย - การวิเคราะห์ช่องโหว่ - การแก้ไขช่องโหว่ - การประสานงานเพื่อแก้ไขช่องโหว่ • การจัดการกับ artifact - การวิเคราะห์ artifact - การดำเนินการต่อ artifact - การประสานงานเพื่อจัดการกับ artifact	• **การแจ้งเตือนและเผยแพร่ข้อมูลข่าวสาร** • การเฝ้าติดตามพัฒนาการทางเทคโนโลยี • การตรวจสอบและประเมินด้านความมั่นคงปลอดภัย • การตั้งค่าและดูแลเครื่องมือด้านความมั่นคงปลอดภัย แอปพลิเคชัน โครงสร้างและบริการด้านสารสนเทศ • การพัฒนาเครื่องมือด้านความมั่นคงปลอดภัย • การบริการตรวจจับการบุกรุก • การเผยแพร่ข้อมูลที่เกี่ยวข้องกับความมั่นคงปลอดภัย	• การวิเคราะห์ความเสี่ยง • การวางแผนความต่อเนื่องทางธุรกิจและการฟื้นตัวจากเหตุภัยพิบัติ • การให้คำปรึกษาด้านความมั่นคงปลอดภัย • การสร้างความตระหนักเรื่องความมั่นคงปลอดภัย • บริการวิชาการด้านความมั่นคงปลอดภัย • การประเมินผลิตภัณฑ์หรือการออกใบรับรองประกาศนียบัตร

[32] อ้างอิงจาก.. "Handbook for Computer Security Incident Response Teams (CSIRTs), 2nd edition" หน้า 25

การบริการที่เป็นตัวอักษรสีแดงคือบริการขั้นพื้นฐานที่ CSIRT ที่จัดตั้งขึ้นใหม่ควรมีพร้อมให้บริการ ส่วนบริการอื่น ๆ อาจเพิ่มเติมได้ในอนาคตตามความจำเป็น

CSIRT ควรตัดสินใจอย่างรอบคอบในการวางแผนการให้บริการเพื่อให้สอดคล้องกับเป้าหมายขององค์กรภายใต้งบประมาณที่ได้รับจัดสรร ทั้งนี้ เนื่องจากการให้บริการที่เพิ่มขึ้นจำเป็นต้องใช้ทรัพยากร ทักษะ และความร่วมมือจาก CSIRT อื่น การให้บริการที่จำกัดแต่มีคุณภาพย่อมดีกว่ามีบริการมากมายแต่ไม่มีคุณภาพ

ในบางกรณี อาจพิจารณา outsource บริการบางอย่างให้กับหน่วยงานที่มีภารกิจ ในด้านนั้น ๆ โดยเฉพาะ เนื่องจากบริการเหล่านั้นอาจมีต้นทุนสูงและมีการใช้งานน้อย เช่น การตรวจพิสูจน์พยานหลักฐานดิจิทัล (digital forensics) ซึ่ง CSIRT สามารถทำหน้าที่เป็นผู้ประสานงานในการจัดหาบริการดังกล่าวได้

อนึ่ง ในปัจจุบัน ยังไม่พบ CSIRT ใดที่ให้บริการตามรายการข้างต้นครบทั้งหมด

6.1 คำอธิบายบริการต่าง ๆ ของ CSIRT[33]

6.1.1 บริการเชิงรับเพื่อตอบสนองภัยคุกคาม

บริการที่จะช่วยให้หน่วยงานสามารถรับมือและแก้ไขเหตุภัยคุกคามที่

[33] อ้างอิงจาก.. "Handbook for Computer Security Incident Response Teams (CSIRTs), 2nd edition" หน้า 25-34

ส่งผลกระทบต่อระบบสารสนเทศต่าง ๆ ทั้งขององค์กรหรือของ CSIRT เอง โดยอาจได้รับแจ้งเหตุจากการเฝ้าติดตาม การแจ้งเตือนจาก IDS logs และหน่วยงานภายนอกอื่น ๆ

6.1.1.1 การแจ้งเหตุภัยคุกคาม

ประกอบด้วยการแจ้งข้อมูลต่าง ๆ เช่น ข้อมูลการโจมตี ช่องโหว่ด้านความมั่นคงปลอดภัย การถูกเจาะระบบ มัลแวร์ หรือข้อความหลอกลวง CSIRT มีหน้าที่แจ้งเตือนเหตุภัยคุกคาม ให้คำแนะนำแนวทางปฏิบัติเบื้องต้นแก่ผู้รับบริการเพื่อแก้ไขปัญหาที่เกิดขึ้น โดย CSIRT อาจเป็นผู้จัดทำข้อมูลเองหรือนำข้อมูลจากผู้เชี่ยวชาญ vendors หรือ CSIRT อื่น ๆ มาเผยแพร่

6.1.1.2 การรับมือและแก้ไขเหตุภัยคุกคาม

ประกอบด้วย การรับแจ้งเหตุภัยคุกคาม การตรวจสอบและประเมินเหตุภัยคุกคามการตอบกลับต่อผู้แจ้ง การวิเคราะห์เหตุภัยคุกคาม โดย CSIRT อาจดำเนินการต่าง ๆ เช่น

- ปกป้องระบบและเครือข่ายที่ได้รับผลกระทบหรือถูกข่มขู่โดยผู้ประสงค์ร้าย
- เตรียมมาตรการรับมือเหตุภัยคุกคามตามคำแนะนำหรือการแจ้งเตือนที่ได้รับ
- การตรวจสอบร่องรอยการถูกเจาะระบบในส่วนอื่น ๆ ของเครือข่าย
- การตรวจสอบและบล็อก traffic ที่ผิดปกติ
- การล้างข้อมูลในเครื่องและติดตั้งระบบใหม่
- การแพตช์หรือการซ่อมแซมระบบ

- การพัฒนาแนวทางการรับมืออื่น ๆ ในกรณีที่ไม่มีวิธีการแก้ไขโดยตรงก็จำเป็นต้องหาแนวทางการรับมือทางอ้อม (workaround)

การบริการนี้สามารถแบ่งย่อยออกไปได้อีก ดังนี้

o <u>การวิเคราะห์เหตุภัยคุกคาม</u>

การวิเคราะห์เหตุภัยคุกคามเองก็อาจแบ่งได้หลายระดับ แต่หัวใจสำคัญคือการตรวจสอบข้อมูล หลักฐานสนับสนุนหรือ artifact ทั้งหมดที่เกี่ยวข้องกับเหตุภัยคุกคามเพื่อให้สามารถระบุขอบเขต ระดับความเสียหาย ลักษณะของเหตุภัยคุกคาม และแนวทางการรับมือหรือ workaround ได้ โดย CSIRT อาจใช้ผลลัพธ์ที่ได้จากการวิเคราะห์ช่องโหว่และ artifact เพื่อช่วยทำความเข้าใจและวิเคราะห์สิ่งที่เกิดขึ้นกับระบบนั้น ๆ นอกจากนี้ ในกระบวนการวิเคราะห์เหตุภัยคุกคาม CSIRT ควรหาความเชื่อมโยง แนวโน้มการเกิดเหตุภัยคุกคาม แบบแผน หรือร่องรอยของผู้บุกรุกโดยการเทียบเคียงระหว่างเหตุภัยคุกคามหนึ่งกับอีกเหตุหนึ่ง

ทั้งนี้ มีบริการย่อยสองประเภทที่ CSIRT อาจดำเนินการโดยถือเป็นส่วนหนึ่งของการวิเคราะห์เหตุภัยคุกคาม ได้แก่

- การจัดเก็บหลักฐานดิจิทัล

จัดเก็บ บันทึก และวิเคราะห์หลักฐานที่ได้จากคอมพิวเตอร์ที่ถูกเจาะระบบซึ่งครอบคลุมถึงการทำสำเนาฮาร์ดดิสก์ในลักษณะ copy ข้อมูลแบบบิตต่อบิต ตลอดจนการตรวจสอบความเปลี่ยนแปลงที่เกิดขึ้นกับระบบ เช่น พบโปรแกรม ไฟล์ บริการ และบัญชีผู้ใช้ที่ผิดปกติ การตรวจสอบการทำงานของระบบและพอร์ตที่เปิดอยู่ การตรวจหา trojan

การจัดเก็บข้อมูลและหลักฐานต่าง ๆ จะต้องกระทำอย่างระมัดระวังและรอบคอบเพื่อให้ตรวจพิสูจน์ได้และเป็นที่ยอมรับในชั้นศาล ทั้งนี้ บุคลากรของ CSIRT ที่รับผิดชอบบริการนี้อาจต้องพร้อมปฏิบัติหน้าที่เป็นพยานผู้เชี่ยวชาญ (expert witness) ในกระบวนการพิจารณาของศาลด้วย

- การติดตามหรือสืบหาร่องรอย

ติดตามหรือสืบหาร่องรอยว่าผู้ประสงค์ร้ายเข้าถึงระบบที่ได้รับผลกระทบและเครือข่ายที่เกี่ยวข้องได้อย่างไร ใช้วิธีการหรือเครื่องมือใดจึงสามารถเข้าถึงระบบได้ การโจมตีเกิดขึ้นจากที่ใด และระบบหรือเครือข่ายอื่นใดบ้างที่ถูกใช้เป็นส่วนหนึ่งของการโจมตี นอกจากนั้น การติดตามหรือสืบหาร่องรอยยังอาจรวมถึงการพยายามระบุตัวตนของผู้ประสงค์ร้าย แม้ว่าการให้บริการนี้อาจสามารถดำเนินการได้โดย CSIRT เพียงลำพัง แต่โดยทั่วไปแล้วจะทำงานร่วมกับองค์กรบังคับใช้กฎหมาย ผู้ให้บริการอินเทอร์เน็ต หรือองค์กรอื่น ๆ ที่เกี่ยวข้อง

o <u>การรับมือและแก้ไขเหตุภัยคุกคาม ณ สถานที่เกิดเหตุ (on site)</u>

ให้บริการนอกสถานที่เกิดเหตุเพื่อวิเคราะห์และช่วยฟื้นฟูระบบกลับมาให้บริการหรือใช้งานได้ตามปกติโดยเร็วที่สุด แทนที่จะให้เพียงการสนับสนุนทางโทรศัพท์หรืออีเมล บุคลากรของ CSIRT อาจจำเป็นต้องก็จะเดินทางลงพื้นที่เพื่อดำเนินการแก้ไขปัญหา แต่ในบางกรณีพบว่ามี CSIRT ประจำสถานที่หรือผู้ดูแลระบบซึ่งได้รับหน้าที่ให้รับมือและแก้ไขเหตุภัยคุกคามเป็นประจำอยู่แล้ว

o <u>การสนับสนุนการรับมือและแก้ไขเหตุภัยคุกคาม</u>

ให้ความช่วยเหลือและเสนอแนะแนวทางแก้ไขแก่ผู้เสียหายที่ถูกโจมตีเพื่อให้ฟื้นตัวจากเหตุภัยคุกคามผ่านทางโทรศัพท์ อีเมล โทรสาร

หรือเอกสาร โดยอาจรวมถึงการให้ความช่วยเหลือทางเทคนิคในการวิเคราะห์ข้อมูลที่รวบรวม การจัดหาข้อมูลติดต่อ หรือการเผยแพร่แนวทางการจำกัดความเสียหายและการฟื้นฟูระบบ การให้บริการในลักษณะนี้ไม่ใช่การรับมือและแก้ไขเหตุภัยคุกคาม ณ สถานที่เกิดเหตุ แต่จะเป็นผู้ให้ความช่วยเหลือจากระยะไกลเพื่อให้บุคลากรในสถานที่นั้นสามารถดำเนินการรับมือเหตุภัยคุกคามและฟื้นฟูระบบได้ด้วยตนเอง

o การประสานงานเพื่อรับมือและแก้ไขเหตุภัยคุกคาม

ประสานงานกับองค์กรหรือบุคคลที่เกี่ยวข้องกับเหตุภัยคุกคาม เช่น ผู้เสียหายที่ถูกโจมตี องค์กรที่อาจต้องการความช่วยเหลือในการวิเคราะห์การโจมตี รวมถึงองค์กรอื่น ๆ ที่เกี่ยวข้องกับผู้เสียหาย อย่าง ผู้ดูแลระบบ ผู้ให้บริการอินเทอร์เน็ต CSIRT อื่น ๆ หน้าที่ของ CSIRT ในที่นี้อาจรวมถึงการจัดเก็บข้อมูลติดต่อ การแจ้งเตือนองค์กรอื่นที่มีแนวโน้มเกี่ยวข้องในฐานะผู้เสียหายหรือแหล่งที่มาของการโจมตี การจัดเก็บสถิติการดำเนินการกับองค์กรที่เกี่ยวข้อง การอำนวยความสะดวกในการแลกเปลี่ยนข้อมูลและการวิเคราะห์ข้อมูล การร่วมมือกับผู้เชี่ยวชาญทางกฎหมายขององค์กร ส่วนงานทรัพยากรบุคคลหรือส่วนงานประชาสัมพันธ์ ตลอดจนผู้บังคับใช้กฎหมาย ทั้งนี้ การประสานงานดังกล่าวไม่ถือเป็นการรับมือและแก้ไขเหตุภัยคุกคาม ณ สถานที่

6.1.1.3 การจัดการกับช่องโหว่ด้านความมั่นคงปลอดภัย

ประกอบด้วยการรับแจ้งและรวบรวมข้อมูลและรายงานที่เกี่ยวข้องกับช่องโหว่ของฮาร์ดแวร์และซอฟต์แวร์ต่าง ๆ การวิเคราะห์ลักษณะและผลกระทบของช่องโหว่ที่มีต่อระบบ การพัฒนาวิธีการตรวจสอบและแก้ไขช่องโหว่ ทั้งนี้ มีบริการย่อยสองประเภทที่ CSIRT อาจดำเนินการโดยถือเป็นส่วนหนึ่งของการจัดการกับช่องโหว่ด้านความมั่นคงปลอดภัย ได้แก่

- การวิเคราะห์ช่องโหว่

ตรวจสอบยืนยันข้อมูลช่องโหว่ว่าเป็นจริงหรือไม่ ด้วยการทดสอบหาวิธีโจมตีผ่านช่องโหว่ในฮาร์ดแวร์หรือซอฟต์แวร์ที่ได้รับผลกระทบ ในบริการนี้ยังรวมถึงการวิเคราะห์ซอร์สโค้ดและการใช้ debugger เพื่อหาช่องโหว่

- การตอบสนองต่อช่องโหว่

เป็นการหาแนวทางที่เหมาะสมในการจัดการช่องโหว่ที่พบ เช่น การพัฒนาและติดตั้งแพตช์หรือ workaround เพื่อแก้ไขช่องโหว่ดังกล่าว รวมถึงการแจ้งส่วนงานและองค์กรที่ได้รับผลกระทบทราบแนวทางแก้ไข

- การประสานงานเพื่อแก้ไขช่องโหว่

เป็นการแจ้งทุกหน่วยงาน ทุกฝ่ายที่เกี่ยวข้องเกี่ยวกับช่องโหว่และวิธีแก้ไข โดยการสื่อสารกับ vendors CSIRT อื่น ๆ ผู้เชี่ยวชาญทางเทคนิค ผู้มีส่วนเกี่ยวข้อง ตลอดจนบุคคลหรือกลุ่มต่าง ๆที่เป็นผู้ค้นพบหรือรายงานเกี่ยวกับช่องโหว่นั้นตั้งแต่แรก

บริการนี้ยังรวมถึง การประสานงานเพื่อให้การวิเคราะห์และออกรายงานช่องโหว่เป็นไปอย่างราบรื่น การประสานงานเพื่อกำหนดวันเผยแพร่แพตช์ workaround และเอกสารที่เกี่ยวข้อง รวมถึงการสร้างฐานข้อมูลจัดเก็บข้อมูลช่องโหว่และแนวทางการแก้ไขด้วย

6.1.1.4 การจัดการกับ artifact

artifact คือไฟล์หรือร่องรอยใด ๆ ก็ตามที่พบในระบบที่เกี่ยวข้องกับการโจมตีระบบและเครือข่าย อาจรวมถึงไวรัสคอมพิวเตอร์ โทรจัน เวิร์ม สคริปต์หรือเครื่องมือต่าง ๆ ที่ใช้โจมตี ในบริการนี้ CSIRT

มีหน้าที่รวบรวม artifact หรือข้อมูลที่เกี่ยวกับ artifact ที่ถูกใช้ในการเจาะระบบ การสอดแนม การขัดขวางการทำงานของระบบ

เมื่อได้รับ artifact มาแล้ว บุคลากรใน CSIRT จะนำมาตรวจสอบในด้านต่าง ๆ เช่น วิเคราะห์ลักษณะ ฟังก์ชันการทำงาน เวอร์ชัน จุดประสงค์ของ artifact นั้น ก่อนจะหาแนวทางที่เหมาะสมในการตรวจจับ กำจัด และป้องกัน artifact เหล่านี้

ในบริการนี้สามารถจำแนกเป็นบริการย่อยได้แก่

- การวิเคราะห์ artifact

ตรวจสอบและวิเคราะห์ artifact ที่พบในระบบ อาจประกอบด้วยการระบุประเภทของไฟล์ โครงสร้างของ artifact การเปรียบเทียบ artifact ใหม่กับ artifact ที่มีอยู่แล้วเพื่อหาความเหมือนและความแตกต่าง การทำวิศวกรรมย้อนกลับ (reverse engineering) การวิเคราะห์โค้ดเพื่อหาวัตถุประสงค์และฟังก์ชันการทำงานของ artifact นั้น

- การดำเนินการต่อ artifact

ประกอบด้วยการหาวิธีการตรวจจับ กำจัด และป้องกัน artifact โดยอาจสร้าง signature ให้กับแอนติไวรัสหรือ IDS ใช้ในการตรวจจับ artifact

- การประสานงานเพื่อจัดการกับ artifact

ประกอบด้วยการประสานงานแบ่งปันข้อมูลจากการวิเคราะห์ artifact ให้กับ CSIRT vendors ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยและผู้ที่เกี่ยวข้องอื่น ๆ และยังอาจรวมถึงการดูแลฐานข้อมูลที่รวบรวม artifact รวมถึงข้อมูลผลกระทบและวิธีการรับมือ

6.1.2 บริการเชิงรุกเพื่อป้องกันภัยคุกคาม

บริการเชิงรุกมีวัตถุประสงค์เพื่อพัฒนาระบบและกระบวนการด้านความมั่นคงปลอดภัยให้พร้อม เพื่อป้องกันตั้งแต่ก่อนเกิดเหตุภัยคุกคาม หรือลดผลกระทบเมื่อเกิดเหตุภัยคุกคาม

6.1.2.1 การแจ้งเตือนและเผยแพร่ข้อมูลข่าวสาร

อาจประกอบด้วยการแจ้งเตือนการโจมตี การแจ้งเตือนช่องโหว่และการออกคำแนะนำ เกี่ยวกับความมั่นคงปลอดภัย ซึ่งจะช่วยให้ผู้รับบริการสามารถปกป้องระบบและเครือข่ายก่อนที่จะถูกโจมตี

6.1.2.2 การเฝ้าติดตามพัฒนาการทางเทคโนโลยี

ติดตามพัฒนาการทางเทคโนโลยีใหม่ ๆ ซึ่งอาจประกอบด้วยการศึกษาวิธีการของผู้ประสงค์ร้าย แนวโน้มของภัยคุกคามในอนาคต และอาจขยายขอบเขตการติดตาม รวมไปถึงคำตัดสินคดีและการออกกฎหมายที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ ภัยคุกคามทางสังคมหรือทางการเมือง รูปแบบของการติดตาม เช่น การสมัครอีเมลรับข่าวสาร ศึกษาข้อมูลบนเว็บไซต์อ่านข่าวและบทความในวารสารด้านความมั่นปลอดภัย รวมทั้งการติดตามข้อมูลในสาขาอื่นอย่าง วิทยาศาสตร์ เทคโนโลยี การเมืองและการปกครอง แล้วนำมาวิเคราะห์หาข้อมูลที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบและเครือข่ายขององค์กร โดย CSIRT อาจขอความช่วยเหลือจากส่วนงานอื่น ๆ ที่มีความเชี่ยวชาญในแขนงเหล่านี้เพื่อให้มั่นใจว่าข้อมูลหรือการตีความที่ได้มานั้นมีความถูกต้อง

6.1.2.3 การตรวจสอบและประเมินด้านความมั่นคงปลอดภัย

ประกอบด้วยการตรวจสอบและวิเคราะห์ความมั่นคงปลอดภัยของ

ระบบและเครือข่ายขององค์กรว่าเป็นไปตามข้อกำหนดขององค์กร หรือมาตรฐานที่เกี่ยวข้องหรือไม่ นอกจากนั้นยังอาจรวมถึงการทบทวนแนวปฏิบัติด้านความมั่นคงปลอดภัยที่ใช้ในองค์กร

การตรวจสอบและประเมินด้านความมั่นคงปลอดภัยสามารถแบ่งได้ดังนี้

- การตรวจสอบระบบและเครือข่าย: ตรวจสอบการตั้งค่าซอฟต์แวร์และฮาร์ดแวร์อย่าง เราเตอร์ไฟร์วอลล์ เซิร์ฟเวอร์ และอุปกรณ์ต่าง ๆ เพื่อให้เป็นไปตามนโยบายด้านความมั่นคงปลอดภัยขององค์กรหรือมาตรฐานที่สากลยอมรับ
- การตรวจสอบแนวปฏิบัติ: สัมภาษณ์พนักงานและผู้ดูแลระบบเพื่อสำรวจว่าสิ่งที่ปฏิบัติหรือดำเนินการอยู่นั้นสอดคล้องกับนโยบายหรือมาตรฐานด้านความมั่นคงปลอดภัยที่นำมาใช้หรือไม่
- การสแกน: ใช้เครื่องมือตรวจสอบหาช่องโหว่หรือมัลแวร์ในระบบหรือเครือข่าย
- การทดสอบเจาะระบบ: ทดสอบความมั่นคงปลอดภัยโดยการทดสอบเจาะระบบสารสนเทศจริง

CSIRT ควรจัดทำแนวปฏิบัติ รวมทั้งส่งเสริมให้บุคลากรสร้างทักษะที่จำเป็นและสอบประกาศนียบัตรรับรองความสามารถในการตรวจสอบข้างต้น หรืออาจ outsource ให้ผู้เชี่ยวชาญดำเนินการภารกิจเหล่านี้แทนภายใต้การกำกับดูแลของ CSIRT

อนึ่ง ก่อนที่จะดำเนินการตรวจสอบ CSIRT ต้องได้รับการอนุมัติจากผู้บริหาร เนื่องจากนโยบายขององค์กรอาจห้ามไม่ให้ดำเนินการตรวจสอบบางประเภท

6.1.2.4 การตั้งค่าและดูแลเครื่องมือด้านความมั่นคงปลอดภัย แอปพลิเคชัน โครงสร้างและบริการด้านสารสนเทศ

แนะนำแนวทางที่เหมาะสมในการตั้งค่าและดูแล เครื่องมือ applications และโครงสร้างและบริการด้านสารสนเทศ และอาจมีบทบาทเข้ามาปรับตั้งค่าและดูแลเครื่องมือด้านความมั่นคงปลอดภัยต่าง ๆ เช่น IDS, filter, wrapper, firewalls, VPN และระบบยืนยันตัวตนต่าง ๆ รวมถึงอุปกรณ์ทั่วไปอย่าง เซิร์ฟเวอร์ เดสก์ท็อป แล็ปท็อป แท็บเล็ต สมาร์ตโฟน และอุปกรณ์ไร้สายอื่น ๆ ให้เป็นไปตามแนวทางที่กำหนด

ทั้งนี้ CSIRT ควรแจ้งให้ผู้บริหารรับทราบหากพบปัญหาในการตั้งค่าหรือใช้งานเครื่องมือ/ แอปพลิเคชันที่ส่งผลให้ระบบมีช่องโหว่หรือถูกโจมตีได้

6.1.2.5 การพัฒนาเครื่องมือด้านความมั่นคงปลอดภัย

CSIRT พัฒนาเครื่องมือใหม่ ๆ อาจเป็นเครื่องมือเฉพาะสำหรับ CSIRT เครื่องมือสำหรับกลุ่มผู้รับบริการตามความจำเป็น บริการอาจประกอบด้วยการพัฒนาแพตช์สำหรับซอฟต์แวร์ที่ผู้รับบริการใช้งาน การจัดเตรียมชุดซอฟต์แวร์ที่มั่นคงปลอดภัยสำหรับติดตั้งเครื่องคอมพิวเตอร์ใหม่ การพัฒนาเครื่องมือหรือสคริปต์สำหรับเครื่องมือด้านความมั่นคงปลอดภัยที่มีอยู่ เช่น plug-in สำหรับเครื่องมือตรวจสอบช่องโหว่ กลไกการติดตั้งแพตช์อัตโนมัติ เป็นต้น

6.1.2.6 บริการตรวจจับการเจาะระบบ

ประกอบด้วยการตรวจสอบโดยการวิเคราะห์ล็อกจากซอฟต์แวร์หรืออุปกรณ์สำหรับเฝ้าเหตุภัยคุกคาม เช่น IDS, SIEM ซึ่งเป็นงานที่ท้าทายและต้องใช้ความพยายาม เนื่องจากไม่เพียงต้องกำหนดว่าจะวางเซ็นเซอร์สำหรับเฝ้าระวังเหตุภัยคุกคามไว้ที่ใด แต่ยังต้องเก็บและ

วิเคราะห์ข้อมูลปริมาณมหาศาล ในหลายกรณีจำเป็นต้องใช้เครื่องมือเฉพาะหรือความเชี่ยวชาญในวิเคราะห์ข้อมูลเพื่อระบุยืนยันความถูกต้องของการแจ้งเตือนพบเหตุภัยคุกคาม ซึ่งบ่อยครั้งที่อาจพบว่าไม่ใช่เหตุภัยคุกคามจริง จึงจำเป็นต้องมีมาตรการหรือตั้งค่าเครื่องมือของอุปกรณ์สำหรับเฝ้าระวังให้ลดการเกิดเหตุการณ์เหล่านั้นลงได้ให้มากที่สุด บางองค์กรเลือกที่จะ outsource ภารกิจนี้แก่องค์กรอื่นที่มีความเชี่ยวชาญมากกว่าโดยอยู่ภายใต้การกำกับดูแลของ CSIRT

6.1.2.7 <u>การเผยแพร่ข้อมูลที่เกี่ยวข้องกับความมั่นคงปลอดภัย</u>

CSIRT รวบรวมและเผยแพร่ชุดข้อมูลด้านความมั่นคงปลอดภัยที่เป็นประโยชน์และง่ายต่อการสืบค้นแก่ผู้รับบริการและผู้มีส่วนเกี่ยวข้อง อาทิ

- แนวทางการรายงานและข้อมูลติดต่อสำหรับ CSIRT
- ฐานข้อมูลที่มีข้อมูลการแจ้งเหตุ การเตือนและข่าวสารต่าง ๆ
- แนวปฏิบัติด้านความมั่นคงปลอดภัยที่ใช้ในปัจจุบัน
- แนวทางการใช้งานคอมพิวเตอร์อย่างมั่นคงปลอดภัย
- นโยบาย กระบวนการ และเช็กลิสต์
- การพัฒนาแพตช์และ distribution ของซอฟต์แวร์ต่าง ๆ
- ลิงก์เว็บไซต์ทางการของ vendors
- สถิติปัจจุบันและแนวโน้มในการรายงานเหตุภัยคุกคาม
- ข้อมูลอื่น ๆ ที่อาจช่วยปรับปรุงแนวปฏิบัติด้านความมั่นคงปลอดภัยโดยรวม

ข้อมูลเหล่านี้อาจจัดทำและจัดพิมพ์โดย CSIRT หรือส่วนงานอื่น ๆ ขององค์กร (ส่วนงาน IT ทรัพยากรบุคคลหรือสื่อมวลชนสัมพันธ์) และอาจผนวกข้อมูลจากแหล่งข้อมูลภายนอก อาทิ จาก vendors CSIRT อื่น ๆ หรือผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยด้วย

6.1.3 บริการบริหารคุณภาพทางด้านความมั่นคงปลอดภัย

เป็นบริการที่มีเป้าหมายเพื่อปรับปรุงและพัฒนาความมั่นคงปลอดภัยโดยรวมขององค์กร แม้บริการนี้จะไม่เกี่ยวข้องกับการรับมือและแก้ไขเหตุภัยคุกคามหรือภารกิจของ CSIRT โดยตรง แต่เป็นการนำบทเรียนและประสบการณ์ทั้งจากการให้บริการเชิงรับเพื่อรับมือเหตุภัยคุกคามและบริการเชิงรุกเพื่อป้องกันเหตุภัยคุกคามมาสนับสนุนการบริหารการรักษาความมั่นคงปลอดภัยขององค์กรในระยะยาว ทั้งนี้ CSIRT อาจเป็นหน่วยงานหลักหรือเป็นส่วนหนึ่งร่วมกับส่วนงานอื่นในการดำเนินภารกิจบริหารคุณภาพทางด้านความมั่นคงปลอดภัยในระดับองค์กร ขึ้นอยู่กับโครงสร้างและการแบ่งความรับผิดชอบภายในองค์กรนั้น ๆ

บริการย่อยที่ CSIRT ดำเนินการภายใต้บริการบริหารคุณภาพทางด้านความมั่นคงปลอดภัย มีดังนี้

6.1.3.1 <u>การวิเคราะห์ความเสี่ยง</u>

ประเมินหรือช่วยสนับสนุนหรือการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสำหรับระบบและธุรกิจใหม่ ประเมินภัยคุกคามและความเป็นไปได้ที่จะเกิดการโจมตีที่ส่งผลกระทบต่อสินทรัพย์ของผู้รับบริการ ผู้มีส่วนเกี่ยวข้อง ตลอดจนระบบต่าง ๆ ทั้งในแง่ของคุณภาพและปริมาณ และช่วยในการประเมินแนวทางการป้องกันรับมือและแก้ไขเหตุภัยคุกคามได้อย่างมีประสิทธิภาพ

6.1.3.2 การวางแผนความต่อเนื่องทางธุรกิจและการฟื้นตัวจากเหตุภัยพิบัติ

จากข้อมูลในอดีตและการคาดการณ์เกี่ยวกับแนวโน้มด้านความมั่นคงปลอดภัยพบว่า เหตุภัยคุกคามสามารถสร้างความเสียหายอย่างร้ายแรงต่อธุรกิจ ดังนั้น CSIRT จึงมีบทบาทในการนำประสบการณ์และข้อเสนอแนะมาร่วมวางแผนความต่อเนื่องทางธุรกิจและการฟื้นตัวจากเหตุภัยพิบัติ (business continuity and disaster recovery planning) รวมถึงการฟื้นตัวจากเหตุภัยคุกคามเพื่อให้ธุรกิจขององค์กรเป็นไปอย่างต่อเนื่อง

6.1.3.3 การให้คำปรึกษาด้านความมั่นคงปลอดภัย

ให้คำแนะนำและแนวทางปฏิบัติด้านความมั่นคงปลอดภัยในการจัดซื้อ ติดตั้ง ตั้งค่า ระบบ อุปกรณ์เครือข่าย แอปพลิเคชัน รวมถึงให้คำแนะนำในการร่างนโยบายด้านความมั่นคงปลอดภัยสำหรับองค์กร ตลอดจนการให้การชั้นศาล หรือให้คำแนะนำแก่องค์กรด้านนิติบัญญัติ

6.1.3.4 การสร้างความตระหนักเรื่องความมั่นคงปลอดภัย

สร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยผ่านการเขียนบทความ จัดทำโปสเตอร์ บริการเผยแพร่ข่าวสารทางอีเมล เว็บไซต์ ให้ข้อมูลแนวปฏิบัติรวมถึงคำแนะนำและข้อควรระวังต่าง ๆ CSIRT ควรทราบว่าผู้รับบริการยังขาดข้อมูลส่วนใดและพัฒนาความรู้ความเข้าใจในส่วนดังกล่าว เมื่อพนักงานที่ทักษะและความรู้จะทำให้ลดโอกาสการตกเป็นเหยื่อของเหตุภัยคุกคาม และเพิ่มโอกาสที่พนักงานจะตรวจพบและรายงานการถูกโจมตี ทำให้สามารถจำกัดความเสียหายได้อย่างมีประสิทธิภาพ[34]

[34] ไทยเซิร์ตได้จัดทำเอกสารให้ความรู้และสร้างความตระหนักด้านความมั่นคงปลอดภัยสำหรับเผยแพร่ให้ประชาชนและองค์กรที่สนใจ โดยสามารถดาวน์โหลดได้ที่ https://www.thaicert.or.th/downloads/downloads.html

6.1.3.5 บริการวิชาการด้านความมั่นคงปลอดภัย

ให้ความรู้ผ่านการจัดหลักสูตรอบรม สัมมนา ประชุมเชิงปฏิบัติการ เพื่อให้ความรู้และสร้างความตระหนักเรื่องความมั่นคงปลอดภัย โดยองค์ความรู้ต่าง ๆ อาจประกอบด้วย การรายงานเหตุภัยคุกคาม วิธีการรับมือและแก้ไขที่เหมาะสม เครื่องมือที่ใช้ในการรับมือและแก้ไขเหตุภัยคุกคาม วิธีการป้องกันเหตุภัยคุกคามและข้อมูลอื่น ๆ ที่จำเป็น

6.1.3.6 การประเมินหรือการออกประกาศนียบัตรรับรองผลิตภัณฑ์

CSIRT ประเมินเครื่องมือ อุปกรณ์ แอปพลิเคชันหรือบริการต่าง ๆ เพื่อตรวจสอบว่าผลิตภัณฑ์เหล่านั้นมีความมั่นคงปลอดภัยและสอดคล้องกับแนวปฏิบัติด้านความมั่นคงปลอดภัยในระดับองค์กรหรือตามที่ CSIRT กำหนดหรือไม่ โดยอาจออกประกาศนียบัตรเพื่อรับรองผลิตภัณฑ์


TEAMWORK

ภาคผนวก ก: แม่แบบกรอบงาน CSIRT

กรอบงาน CSIRT

ชื่อของ CSIRT: .....

พันธกิจ: .....

.....

.....

.....

ผู้รับบริการ: .....

อำนาจหน้าที่: .....

ความรับผิดชอบ:.....

โครงสร้างของ CSIRT:.....

ความพร้อมในการให้บริการ:.....

.....

บริการต่าง ๆ ของ CSIRT:.....

.....

.....

บุคลากร: .....

.....

โครงสร้างพื้นฐานสารสนเทศและเครื่องมือ: .....

.....

.....

ความสัมพันธ์ภายในและภายนอกองค์กร: .....

.....

.....

.....

รูปแบบการรับเงินทุนสนับสนุนค่าใช้จ่าย: .....

.....

.....

.....

.....

ภาคผนวก ข: ตัวอย่างแบบฟอร์มการรายงานเหตุภัยคุกคาม

แบบฟอร์มการรายงานเหตุภัยคุกคาม

กรุณากรอกแบบฟอร์มนี้และส่งทางโทรสารหรืออีเมล์ไปที่ .....
กรุณากรอกข้อมูลในส่วนที่มีเครื่องหมาย * ให้ครบ

ผู้แจ้งและองค์กร

1. ชื่อ*:
2. ชื่อองค์กร*:
3. ภาคส่วนหรือประเภทขององค์กร:
4. ประเทศ*:
5. เมือง:
6. ที่อยู่อีเมล*:
7. หมายเลขโทรศัพท์*:
8. ข้อมูลอื่น ๆ:

ระบบที่ได้รับผลกระทบ

9. จำนวนของระบบ:
10. Host name และ IP*:
11. หน้าที่ของระบบ*:

12. Time-zone:
13. ฮาร์ดแวร์:
14. ระบบปฏิบัติการ:
15. ซอฟต์แวร์ที่ได้รับผลกระทบ:
16. ไฟล์ที่ได้รับผลกระทบ:
17. โปรโตคอล/ พอร์ต:

<u>เหตุภัยคุกคาม</u>

18. หมายเลขอ้างอิง ref#:
19. ประเภทของเหตุภัยคุกคาม:
20. เหตุภัยคุกคามเกิดขึ้นเมื่อ:
21. เหตุภัยคุกคามต่อเนื่องมาจากเหตุภัยคุกคามก่อนหน้าหรือไม่:
    ใช่ ไม่ใช่
22. เวลาและวิธีการค้นพบเหตุภัยคุกคาม:
23. ช่องโหว่ที่เกี่ยวข้อง:
24. ไฟล์ที่น่าสงสัย:
25. มาตรการรับมือ:
26. รายละเอียด:

ภาคผนวก ค: เครื่องมือด้านความมั่นคงปลอดภัย

ตารางด้านล่างแสดงเครื่องมือที่ CSIRT และผู้ที่เกี่ยวข้องใช้อยู่เป็นประจำ ซึ่งเครื่องมือส่วนใหญ่ที่ระบุในตารางถูกเผยแพร่ให้ใช้งานโดยไม่เสียค่าใช้จ่าย

Domain and IP address query tools	
DomainTools	<https://www.domaintools.com/>
Domain Dossier	<http://centralops.net/co/DomainDossier.aspx>
IP to ASN Mapping	<http://www.team-cymru.org/IP-ASN-mapping.html>
GeoLite2	<http://dev.maxmind.com/geoip/geoip2/geolite2/>
RIPEstat	<https://stat.ripe.net/>
E-mail header analysis tools	
Google Apps Messageheader	<https://toolbox.googleapps.com/apps/messageheader/>
MXToolbox	<http://mxtoolbox.com/EmailHeaders.aspx>
Network monitoring tools	
nfdump	<http://nfdump.sourceforge.net/>
nfsen	<http://nfsen.sourceforge.net/>
Network auditing tools	

nmap	<https://nmap.org/>
AutoScan-Network	<http://autoscan-network.com/>
Wireshark	<https://www.wireshark.org/>
AbuseHelper	<https://github.com/abusesa/abusehelper>
Vulnerability assessment tools	
Nessus	<http://www.tenable.com/products/nessus-vulnerability-scanner>
Metasploit	<https://www.metasploit.com/>
Vega	<https://subgraph.com/vega/index.en.html>
OWASP ZAP	<https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project>
SQLcheck	<http://www.softpedia.com/get/Internet/Servers/Database-Utils/SQL-Check.shtml>
Burp Suite	<https://portswigger.net/burp/>
Kali	<https://www.kali.org/>
Intrusion detection tools	
Snort	<https://www.snort.org/>
Tripwire	<https://sourceforge.net/projects/tripwire/>
Forensic tools	
Sleuth Kit	<http://www.sleuthkit.org/>
Autopsy	<http://www.sleuthkit.org/autopsy/>

Tcpxtract	<http://tcpxtract.sourceforge.net/>
EnCase	<https://www.guidancesoftware.com/encase-forensic>
FTK, Forensic Toolkit	<http://accessdata.com/solutions/digital-forensics/forensic-toolkit-ftk>
Malware analysis tools	
VirusTotal	<https://www.virustotal.com/>
Malware Domain List	<http://www.malwaredomainlist.com/>
Malware Hash Registry	<http://www.team-cymru.org/MHR.html>
MISP, Malware Information Sharing Platform	<https://mispprivcircl.lu/>
AlienVault Open Threat Exchange	<https://otx.alienvault.com/>
Malwr	<https://malwr.com/>
Honeypots	
honeyd	<http://www.honeyd.org/index.php>
WiFi tools	
inSSIDer	<http://www.metageek.com/products/inssider/>

Acrylic WiFi Scanner	<https://www.acrylicwifi.com/en/wlan-software/wlan-scanner-acrylic-wifi-free/>
SIEM tools	
Splunk	<http://www.splunk.com/>
Encryption tools	
GnuPG	<https://www.gnupg.org/>
VeraCrypt	<https://veracrypt.codeplex.com/>
Incident-tracking tools	
RTIR	<https://bestpractical.com/>
OTRS	<https://www.otrs.com/>
Databases	
SQLite	<https://www.sqlite.org/>
MySQL	<https://www.mysql.com/>
PostgreSQL	<https://www.postgresql.org/>

นอกเหนือเครื่องมือข้างต้น ในการนำไฟล์ล็อกมาวิเคราะห์ CSIRT สามารถใช้เครื่องมือคำสั่งต่าง ๆ เช่น sed/ awk และ grep เพื่อค้นหาไฟล์ล็อกในเครื่อง ซึ่งส่วนใหญ่เก็บอยู่ในรูปแบบ plain text และสามารถใช้คำสั่งดังกล่าวในการแปลงไฟล์ล็อกจากแหล่งที่มาที่แตกต่างกันให้อยู่รูปแบบเดียวกัน ทำให้สามารถใช้เครื่องมือวิเคราะห์ได้

ภาคผนวก ง: แหล่งที่มาของข้อมูล

CSIRT อาจพิจารณาสมัครรับข้อมูลจากจากแหล่งข้อมูลต่อไปนี้เพื่อประโยชน์ในการแจ้งเตือนเหตุภัยคุกคาม โดยส่วนใหญ่ไม่มีค่าใช้จ่าย

การแจ้งเตือนเหตุภัยคุกคาม		
APWG, Anti-Phishing Working Group	http://apwg.org/	Phishing
Phish Tank	http://www.phishtank.com/	Phishing
Dark-H	http://dark-h.org/	Web defacements
Mirror-Zone	http://mirror-zone.org	Web defacements
Zone-H	http://zone-h.org/	Web defacements
Zone-HC	http://zone-hc.com	Web defacements
Shadowserver	https://www.shadowserver.org	Botnet Open DNS resolver Open proxy server etc.

Team Cymru	http://www.team-cymru.org/services.html	Botnet Brute force DDoS Malware URL Open DNS resolver Open proxy server Phishing Scanning

นอกจากนี้ในกรณีที่เกิดเหตุภัยคุกคาม CSIRT อาจติดต่อเครือข่ายความร่วมมือที่เกี่ยวข้อง เพื่อขอความช่วยเหลือ

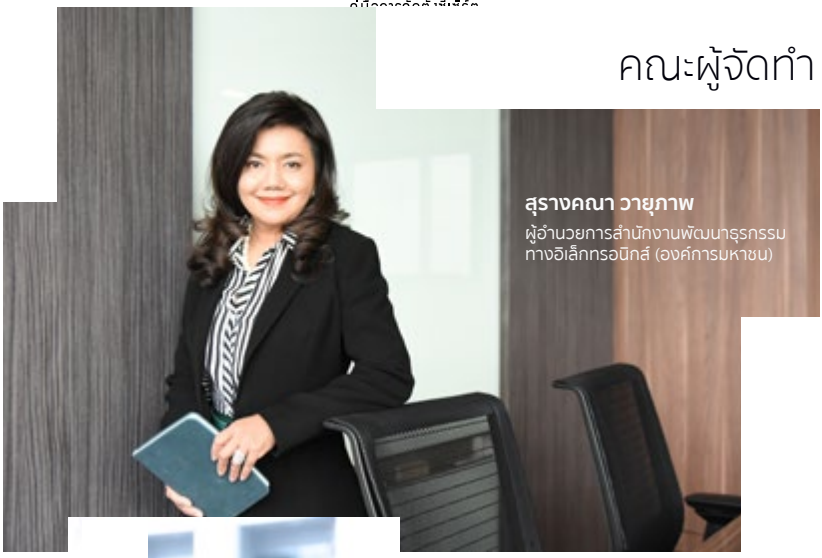
ข้อมูลติดต่อ (CSIRT สมาชิก)	
FIRST, Forum of Incident Response and Security Teams	https://www.first.org/
APCERT, Asia Pacific CERT	http://www.apcert.org/
Trusted Introducer	https://www.trusted-introducer.org/
AfricaCERT	http://www.africacert.org/
Latin American CSIRTs	http://www.lacnic.net/en/web/lacnic/csirts
OIC-CERT, Organisation of the Islamic Cooperation CERT	http://www.oic-cert.org/
NatCSIRT, National CSIRTs	http://www.cert.org/incident-management/national-csierts/national-csirts.cfm

ภาคผนวก จ: เช็กลิสต์การจัดตั้ง CSIRT

	ขั้นตอน	อ้างอิง
Plan		
☐	1. ร่าง CSIRT framework และแผนธุรกิจ รวมถึงกำหนดงบประมาณ	บทที่ 1 หน้าที่ 18 และบทที่ 2
☐	2. ขอผู้ที่มีอำนาจอนุมัติแผนงานและงบประมาณในข้อที่ 1	บทที่ 1 หน้าที่ 19 และบทที่ 3
Do		
☐	3. รวบรวมและจัดทำรายการแหล่งข้อมูลด้านต่าง ๆ	บทที่ 1 หน้าที่ 20 และบทที่ 4 หัวข้อ 4.1
☐	4. ร่างนโยบายการรับมือและแก้ไขเหตุภัยคุกคาม	บทที่ 1 หน้าที่ 20 และบทที่ 4 หัวข้อ 4.2
☐	5. ร่างนโยบายการจัดการและแลกเปลี่ยนข้อมูล	บทที่ 1 หน้าที่ 20 และบทที่ 4 หัวข้อ 4.3
☐	6. สำรวจและจัดทำรายการซอฟต์แวร์และฮาร์ดแวร์ที่ใช้ในองค์กร	บทที่ 1 หน้าที่ 20 และบทที่ 4 หัวข้อ 4.4
☐	7. ประชาสัมพันธ์การจัดตั้ง CSIRT	บทที่ 1 หน้าที่ 20 และบทที่ 4 หัวข้อ 4.5

☐	8. สร้างเครือข่ายความร่วมมือจากการเข้าร่วมการประชุมและการเสวนาต่าง ๆ	บทที่ 1 หน้าที่ 20 และบทที่ 4 หัวข้อ 4.6
☐	9. ซ้อมรับมือเหตุภัยคุกคาม	บทที่ 1 หน้าที่ 20 และบทที่ 4 หัวข้อ 4.7
☐	10. ดำเนินการรับมือและแก้ไขเหตุภัยคุกคาม และให้บริการตามภารกิจหลักอื่น ๆ	บทที่ 1 หน้าที่ 20 บทที่ 5 และบทที่ 6
Check		
☐	11. ประเมินคุณภาพและประสิทธิภาพของการให้บริการ	บทที่ 1 หน้าที่ 20
Act		
☐	12. นำผลการประเมินไปปรับปรุงแผนงานและการดำเนินการ.	บทที่ 1 หน้าที่ 22
☐	13. ขยายขีดความสามารถในการให้บริการ	บทที่ 1 หน้าที่ 22 และบทที่ 6

คณะผู้จัดทำ



สุรางคณา วายุภาพ
ผู้อำนวยการสำนักงานพัฒนาธุรกรรม
ทางอิเล็กทรอนิกส์ (องค์การมหาชน)

ชัยชนะ มิตรพันธ์
รองผู้อำนวยการสำนักงานพัฒนาธุรกรรม
ทางอิเล็กทรอนิกส์ (องค์การมหาชน)

พรพรหม ประภากิตติกุล
ผู้อำนวยการสำนักความมั่นคงปลอดภัย

Martijn Van Der Heide
ThaiCERT Specialist

ณัฐโชติ ดุสิตานนท์
วิศวกรความมั่นคงปลอดภัย

พิสูจน์อักษร
ทศพร โขมพัตร

ฝ่ายศิลป์
นภดล อุษณบุญศิริ

ESTABLISHING A

COMPUTER SECURITY INCIDENT RESPONSE TEAM

ISBN : 978-616-7956-28-2

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)
อาคารเดอะ ไนน์ ทาวเวอร์ แกรนด์
พระรามเก้า (อาคารบี) ชั้น 21 เลขที่ 33/4 ถนนพระราม 9
แขวงห้วยขวาง เขตห้วยขวาง กรุงเทพมหานคร 10310
โทรศัพท์ 0 2123 1212 | โทรสาร 0 2123 1200