แผนตอบสนองภัยคุกคาม
(Incident Response Plan)

รหัสเอกสาร: SOC-IRP-001
เวอร์ชั่น: 1.0
วันที่มีผลบังคับใช้: 2564

ชั้นความลับของเอกสาร: ☐ลับมาก ☐ลับ ☑ปกปิด ☐ไม่ระบุ

จัดเตรียมเอกสารโดย : นายสุธี ยืนแน่นอน นักวิชาการคอมพิวเตอร์/สผ. ก.ค. 64

พิจารณาทบทวนโดย : คณะอนุกรรมการขับเคลื่อนแผนการรักษาความมั่นคงปลอดภัย ด้านเทคโนโลยีสารสนเทศและการสื่อสาร ของรัฐสภา ระยะ 4 ปี (พ.ศ. 2562 - 2565)

เห็นชอบโดย : คณะกรรมการขับเคลื่อนแผนพัฒนา Digital Parliament ของรัฐสภา ระยะ 5 ปี (พ.ศ. 2561-2565)

ประวัติการแก้ไขเอกสาร

เวอร์ชั่นแก้ไข	วันที่มีผลบังคับใช้	บทที่/หน้าที่แก้ไข	รายละเอียดการ
1.0	___ 2564	ทั้งหมด	เอกสารใหม่

สารบัญ

สารบัญแผนภาพ

สารบัญตาราง

ตาราง **หน้าที่**

แผนตอบสนองภัยคุกคาม
(Incident Response Plan)

1. บทนำ

สถานการณ์ที่ผิดปกติในระบบเทคโนโลยีสารสนเทศนั้นมีอยู่หลายสาเหตุ ทั้งสาเหตุที่เกิดขึ้นจากตัวอุปกรณ์เอง หรืออาจเกิดจากผู้ก่อการร้าย ซึ่งต้องยอมรับว่าในปัจจุบันการโจมตีไซเบอร์ทวีความรุนแรงและแยบยลขึ้นเรื่อยๆ การป้องกันเพียงอย่างเดียวไม่สามารถปกป้องสำนักงานจากภัยคุกคามระดับสูงได้ ถึงแม้ว่าเหตุการณ์ที่เกิดขึ้นอาจผ่านกระบวนการลดความเสี่ยงมาแล้ว แต่สถานการณ์บางอย่างอาจเหนือการควบคุมเมื่อภัยคุกคามเหล่านั้นหลุดเข้ามาได้ ย่อมเกิดความเสียหายต่อทรัพยากรข้อมูล ชื่อเสียงและสิ่งที่ตามมาคือความเชื่อมั่นจากผู้ใช้งาน สำนักงานจำเป็นต้องมีกระบวนการในการรับมือกับสถานการณ์ที่ผิดปกติเมื่อภัยคุกคามเหล่านั้นหลุดเข้ามาได้ ยิ่งสำนักงานสามารถตอบสนองต่อภัยคุกคามได้เร็ว ยิ่งช่วยให้สามารถกักกันหรือลดความเสียหายที่จะเกิดขึ้นและสามารถฟื้นฟูระบบให้กลับมาใช้งานตามปกติได้เร็วขึ้นเท่านั้น จะเห็นได้ว่าการตอบสนองต่อภัยคุกคามจึงเป็นเรื่องสำคัญมากสำหรับจัดการกับเหตุการณ์ผิดปกติในระบบเทคโนโลยีสารสนเทศดังนั้นสำนักงานจึงจำเป็นต้องมีการจัดทำ “แผนตอบสนองภัยคุกคาม”ขึ้นมาเพื่อช่วยลดความเสี่ยงต่อความเสียหายของระบบ โดยแผนฯ นี้จะนำเสนอแนวทางในการตอบสนองต่อเหตุการณ์ที่ผิดปกติ ซึ่งจะเน้นในส่วนของฮาร์ดแวร์ระบบปฏิบัติการและแอพพลิเคชั่นโดยเฉพาะในการกำหนดแนวทางแผนตอบสนองภัยคุกคามได้อย่างมีประสิทธิภาพ ในการตรวจสอบ (detecting) การวิเคราะห์ (analyzing) การจัดลำดับความสำคัญ (prioritizing) และ การจัดการ (handling) เหตุการณ์ที่ไม่คาดคิด

การจัดทำแผนตอบสนองภัยคุกคาม (Incident Response Plan)นั้นได้นำนโยบายความมั่นคงปลอดภัยสารสนเทศของรัฐสภา STD_PY_01 เวอร์ชั่น : 1.0 รวมทั้งแนวปฏิบัติความมั่นคงปลอดภัยสารสนเทศของรัฐสภา STD_PY_02 เวอร์ชั่น : 1.0 และข้อกำหนดComputer SecurityIncident Handling GuideตามมาตรฐานNIST Special Publication 800-61 Revision 2 มาเป็นกรอบแนวทางการเกี่ยวกับกระบวนการของแผนตอบสนองภัยคุกคาม(Incident Response Plan)

2. วัตถุประสงค์

2.1 เพื่อใช้เป็นแนวทางในการตอบสนองภัยคุกคาม ของรัฐสภา

2.2 เพื่อให้สำนักงาน/หน่วยงานมีการเตรียมความพร้อมล่วงหน้าในการรับมือกับสถานการณ์ที่ผิดปกติที่เกิดขึ้น

2.3 เพื่อลดระยะเวลาผลกระทบจากการหยุดชะงักในการให้บริการด้านเทคโนโลยีสารสนเทศและการสื่อสารให้น้อยที่สุดและสามารถกลับมาดำเนินงานหรือให้บริการได้ตามปกติในเวลาและเป้าหมายที่กำหนด

2.4 เพื่อให้ผู้มีส่วนได้ส่วนเสีย (Stakeholder) มีความเชื่อมั่นในศักยภาพของหน่วยงานแม้หน่วยงานต้องเผชิญกับสถานการณ์ที่ผิดปกติร้ายแรง

3. นิยามคำศัพท์

ภัยคุกคามทางไซเบอร์	หมายถึงการกระทำหรือการดำเนินการใดๆโดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ข้อมูลคอมพิวเตอร์หรือข้อมูลอื่นที่เกี่ยวข้องและเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ระบบคอมพิวเตอร์หรือข้อมูลอื่นที่เกี่ยวข้อง
ไซเบอร์	หมายถึงข้อมูลและการสื่อสารที่เกิดจากการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ระบบอินเทอร์เน็ตหรือโครงข่ายโทรคมนาคมรวมทั้งการให้บริการโดยปกติของดาวเทียมและระบบเครือข่ายที่คล้ายคลึงกันที่เชื่อมต่อกันเป็นการทั่วไป
สำนักงาน	หมายถึงสำนักงานเลขาธิการสภาผู้แทนราษฎร และ สำนักงานเลขาธิการวุฒิสภา
การตอบสนองต่อเหตุการณ์	หมายถึงการตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ที่อาจส่งผลกระทบให้เกิดการหยุดชะงักหรือเกิดความเสียหายต่อระบบ
Cyber Threat Intelligence	หมายถึงผู้เชี่ยวชาญจากระบบคลังข้อมูลภัยคุกคามทางไซเบอร์อัจฉริยะชั้นนำ
Security information and event management: SIEM	หมายถึงระบบบริหารจัดการข้อมูลและวิเคราะห์เหตุการณ์ด้านความมั่นคงปลอดภัย ช่วยในการตรวจจับและทำการแจ้งเตือนจากการวิเคราะห์ที่ได้จากข้อมูลบันทึกเหตุการณ์ (Log data)
Threat Intelligence	แบ่งออกเป็น 3 แบบ คือ **Strategic Intelligence:** ข้อมูลหลังผ่านการวิเคราะห์ เช่น กลุ่มผู้ไม่ประสงค์ดีที่กำลังพุ่งเป้ามาที่องค์กรและเป้าหมายของพวกเขา ความเสี่ยงที่อาจจะเกิดขึ้น และกฎหมายข้อบังคับต่างๆ ที่ต้องปฏิบัติตาม สำหรับนำไปปรับใช้กับนโยบายและการวางแผนกลยุทธ์ด้านความมั่นคงปลอดภัย **Tactical Intelligence:** ข้อมูลที่รวบรวมโดยระบบและเซ็นเซอร์ด้านความมั่นคงปลอดภัย ส่วนใหญ่มักเป็น Indicator of Compromise สำหรับใช้ตรวจสอบหลักฐานทางดิจิทัลและฟื้นฟูความเสียหายที่เกิดขึ้น **Operational Intelligence:** องค์ประกอบสำคัญที่สุดในการสร้างบริบทของภัยคุกคาม ไม่ว่าจะเป็นขอบเขตหรืออาณาบริเวณของการโจมตี รวมไปถึงวิธีที่

ดีที่สุดในการตอบสนองต่อการโจมตีเหล่านั้น Big Data Analytics, Machine Learning และเทคนิคการวิเคราะห์โดยอัตโนมัติต่างๆ จะถูกนำเข้ามาใช้เพื่อสนับสนุนการตัดสินใจของผู้รับผิดชอบ

4. เป้าหมาย

4.1 สำนักงานมีแผนการและวิธีปฏิบัติในการรับมือภัยคุกคามและการตอบสนองต่อเหตุการณ์ผิดปกติซึ่งรวมถึงการตรวจพิสูจน์พยานหลักฐานทางดิจิตอล (Digital Forensics)

4.2 สำนักงานตอบสนองต่อเหตุการณ์ผิดปกติ (Incident Response) สำหรับภัยไซเบอร์สำคัญที่ สำนักงานมีโอกาสเผชิญ โดยมีการตรวจสอบ วิเคราะห์หาสาเหตุ และประเมินผลกระทบเพื่อให้สามารถใช้อ้างอิงในการรับมือภัยคุกคาม ตอบสนองต่อเหตุการณ์ และกู้คืนระบบและข้อมูลได้อย่างรวดเร็วและทันการณ์

4.3 สำนักงานนำสิ่งที่ได้เรียนรู้ (Lessons learned) จากการถูกโจมตีหรือจากที่มีเหตุการณ์ผิดปกติที่เกิดขึ้นทั้งภายในและภายนอกสำนักงานมาปรับปรุงแผนรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติ

4.4 สำนักงานมีการทบทวนแผนฯ โดยจำลองถึงเหตุการณ์ต่างๆ จากภัยไซเบอร์ที่อาจส่งผลกระทบรุนแรง และความเสียหายที่อาจเกิดขึ้น เพื่อยกระดับขีดความสามารถต่อการตอบสนองต่อเหตุการณ์ผิดปกติ

5. บทบาทหน้าที่การรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติ (Incident Response Function)

5.1 สำนักงานมีการกำหนดบทบาทหน้าที่ความรับผิดชอบในการรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์

5.2 สำนักงานมีบุคลากรที่ทำหน้าที่รับมือและตอบสนองต่อภัยคุกคามที่มีความรู้ความเชี่ยวชาญอย่างเพียงพอ รวมทั้งประเมินบุคลากรทางด้านเทคนิค ที่ปรึกษาหรือผู้เชี่ยวชาญที่เกี่ยวข้องกับการรับมือเหตุการณ์ผิดปกติ เพื่อให้มีความพร้อมสำหรับการตอบสนองในระหว่างหรือหลังเกิดเหตุการณ์

5.3 สำนักงานมีบุคลากรที่ทำหน้าที่ในการรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติของสำนักงาน รวมถึงการประสานงานและติดต่อสื่อสารกับหน่วยงานและผู้มีส่วนได้เสียทั้งภายในและภายนอก ทั้งระหว่างและหลังการเกิดเหตุการณ์การโจมตีทางไซเบอร์

5.4 เมื่อมีเหตุการณ์ผิดปกติเกิดขึ้น ผู้ทำหน้าที่บริหารจัดการเหตุการณ์ผิดปกติและผู้ทำหน้าที่ติดตามและวิเคราะห์ Cyber Threat Intelligence ต้องมีการทำงานอย่างใกล้ชิด

5.5 สำนักงานเชื่อมโยงและวิเคราะห์ Threat Intelligence ข้อมูลการบริหารจัดการระบบเครือข่าย และข้อมูลการรับมือเหตุการณ์ผิดปกติเพื่อเตรียมรับมือภัยคุกคามและตอบสนองในเชิงรุกต่อเหตุการณ์ผิดปกติที่อาจเกิดขึ้น

6. ขั้นตอนการรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติ

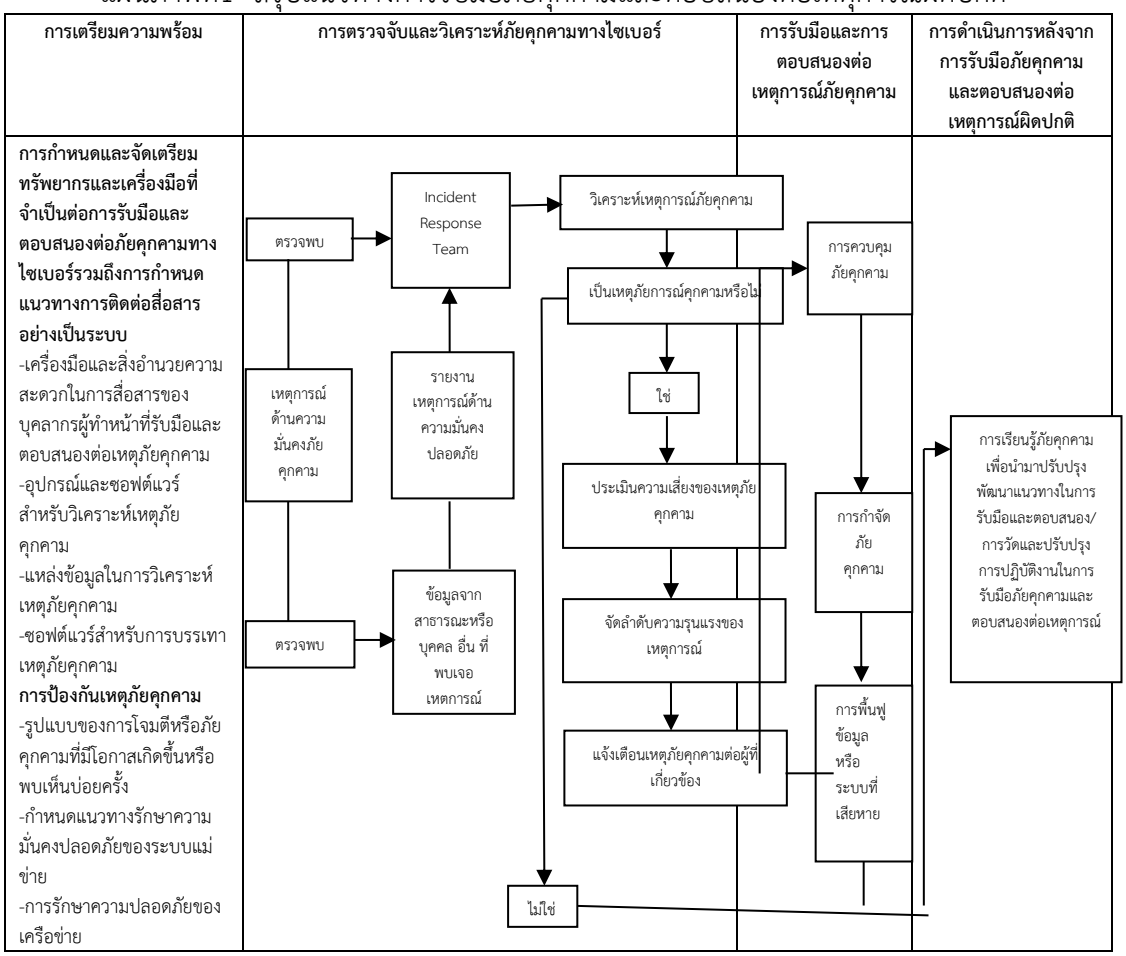
6.1. การเตรียมความพร้อม (Preparation)

6.2 การตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (Detection and Analysis)

6.3 การรับมือและการตอบสนองต่อเหตุการณ์ภัยคุกคาม

6.4 การดำเนินการหลังจากการรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติ (Post Incident Activity)

แผนภาพที่1 สรุปแนวทางการรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติ



6.1. การเตรียมความพร้อม (Preparation)

6.1.1 การกำหนดและจัดเตรียมทรัพยากรและเครื่องมือที่จำเป็นต่อการรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์รวมถึงการกำหนดแนวทางการติดต่อสื่อสารอย่างเป็นระบบ

สำนักงานควรมีเครื่องมือสำหรับทำการวิเคราะห์เหตุการณ์ภัยคุกคามทางไซเบอร์และมีการกำหนดแนวทางรักษาความปลอดภัยของระบบแม่ข่าย (Host Security) ควรติดตั้งโปรแกรม (Software) เพื่อตรวจจับและยับยั้งโปรแกรมไม่ประสงค์ดี (Malware) ภายในระบบเทคโนโลยีสารสนเทศของสำนักงานระบบปฏิบัติการระบบโปรแกรมที่ใช้งาน (Application) และระบบโปรแกรมงานสำหรับเครื่องลูกข่าย (Application Clients) โดยมีเครื่องมือและทรัพยากรที่จำเป็นต่อการรับมือและตอบสนองต่อภัยคุกคามควรครอบคลุมดังนี้

6.1.1.1 เครื่องมือและสิ่งอำนวยความสะดวกในการสื่อสารของบุคลากรผู้ทำหน้าที่รับมือและตอบสนองต่อเหตุภัยคุกคาม (Incident Handler and Facilities)

(1) รายชื่อและช่องทางการติดต่อสำหรับสมาชิกภายในทีมรับมือภัยคุกคามทางไซเบอร์รวมถึงหน่วยงานอื่นๆที่จำเป็นต่อการรับมือเหตุทั้งภายในและภายนอกสำนักงาน (รายชื่อผู้รับผิดชอบหลักและรายชื่อสำรอง)

(2) รายชื่อและช่องทางการติดต่อสำหรับทีมหรือหน่วยงานภายในสำนักงานในกรณีที่มีการยกระดับความรุนแรงของเหตุการณ์โดยสามารถให้ความช่วยเหลือหรือรับช่วงต่อในการรับมือได้ทันท่วงทีหลังได้รับการแจ้ง

(3) ช่องทางการรายงานเหตุการณ์เช่นหมายเลขโทรศัพท์อีเมลแบบรายงานออนไลน์และระบบการส่งข้อความทันทีที่มีเหตุการณ์กระทบต่อความมั่นคงปลอดภัยเพื่อให้ผู้ใช้งานทั่วไปสามารถใช้ในการรายงานเหตุการณ์ที่เข้าข่ายจะเป็นภัยคุกคามทางไซเบอร์

(4) ระบบในการรายงานและติดตามข้อมูลสถานะการดำเนินการของเหตุการณ์ที่ได้รับแจ้ง

(5) โปรแกรมเข้ารหัส (Encryption Software) เพื่อเพิ่มความปลอดภัยในการสื่อสารทั้งระหว่างภายในและภายนอกสำนักงาน

(6) ห้องประชุม (War Room) สำหรับการสื่อสารและประสานงานระหว่างส่วนกลางและหน่วยงานที่เกี่ยวข้องซึ่งอาจเป็นห้องประชุมที่ใช้งานชั่วคราวเพื่อการรับมือภัยคุกคามทางไซเบอร์ก็ได้

(7) สถานที่จัดเก็บที่มีความมั่นคงปลอดภัยเพื่อใช้ในการจัดเก็บหลักฐานข้อมูลและพยานวัตถุอื่นๆที่สำคัญ

6.1.1.2 อุปกรณ์และซอฟต์แวร์สำหรับวิเคราะห์เหตุภัยคุกคาม (Incident Hardware and Software)

(1) เครื่องคอมพิวเตอร์หรืออุปกรณ์สำรองข้อมูลที่ใช้งานเพื่อการจัดเก็บข้อมูลบันทึกเหตุการณ์ (Log Files) หรือสร้าง Disk Image หรือบันทึกข้อมูลเหตุการณ์ที่เกี่ยวข้องอื่นๆโดยเฉพาะ

(2) เครื่องมือสำหรับตรวจจับและวิเคราะห์ข้อมูลในเครือข่ายคอมพิวเตอร์ (Packet Sniffers and Protocol Analyzers) เพื่อเก็บข้อมูลและวิเคราะห์การดักจับข้อมูลที่ผ่านไปมาระหว่างเครือข่าย

(3) เครื่องคอมพิวเตอร์สำรองเซิร์ฟเวอร์และอุปกรณ์เครือข่ายที่สามารถใช้ทดแทนเครื่องคอมพิวเตอร์หรืออุปกรณ์หลักได้ซึ่งสามารถใช้เพื่อสำหรับสนับสนุนการวิเคราะห์เหตุภัยคุกคามทางไซเบอร์

(4) อุปกรณ์ที่ใช้ในการรวบรวมหลักฐานเช่นโน้ตบุ๊กกล้องดิจิตอลเครื่องบันทึกเสียงแบบบันทึกข้อมูลผู้ครอบครองพยานหลักฐานเป็นต้นเพื่อเก็บหลักฐานสำหรับการดำเนินการทางกฎหมาย

6.1.1.3 แหล่งข้อมูลในการวิเคราะห์เหตุภัยคุกคาม (Incident Analysis Resources)

(1) รายการพอร์ตช่องทางการแลกเปลี่ยนข้อมูลผ่านอินเตอร์เน็ตหรือระบบเครือข่ายคอมพิวเตอร์ (Port Lists) ตั้งแต่พอร์ตที่ใช้งานทั่วไปจนถึงพอร์ตที่เสี่ยงต่อการถูกโจมตี

(2) เอกสารหรือคู่มือการใช้งานของระบบปฏิบัติการแอพพลิเคชั่นโปรโตคอลที่ใช้ในการสื่อสารระหว่างเครื่องคอมพิวเตอร์ซอฟต์แวร์สำหรับตรวจจับการบุกรุกและซอฟต์แวร์ป้องกันไวรัส

(3) แผนผังเครือข่ายและรายการทรัพย์สินทางสารสนเทศที่สำคัญเช่นฐานข้อมูลเป็นต้น

(4) ค่าปกติ (Baseline) ของระบบเครือข่ายและแอพพลิเคชั่น

(5) ค่า hash ของไฟล์ที่มีความสำคัญเพื่อเพิ่มความเร็วในการวิเคราะห์การตรวจสอบและกำจัดภัยคุกคามที่เกิดขึ้น

6.1.1.4 ซอฟต์แวร์สำหรับการบรรเทาเหตุภัยคุกคาม (Incident Mitigation Software) ไฟล์ disk image ของระบบปฏิบัติการ (OS) และแอพพลิเคชั่น (Application) เพื่อใช้ในการกู้คืนและฟื้นฟูระบบ

6.1.2 การป้องกันเหตุภัยคุกคาม

สิ่งสำคัญที่สุดในการป้องกันเหตุภัยคุกคามทางไซเบอร์คือการลดจำนวนเหตุภัยคุกคามให้เหลือน้อยที่สุดเพื่อลดผลกระทบต่อภารกิจของสำนักงานการป้องกันเหตุภัยคุกคามทางไซเบอร์ควรครอบคลุมในเรื่องดังต่อไปนี้

6.1.2.1 การประเมินความเสี่ยงภัยคุกคามทางไซเบอร์ (Risk Assessments)

สำนักงานควรทำการประเมินความเสี่ยงเพื่อพิจารณาว่ามีความเสี่ยงใดบ้างที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์หรือช่องโหว่ด้านความมั่นคงปลอดภัยโดยควรระบุเหตุการณ์ภัยคุกคามที่อาจเกิดขึ้นและส่งผลกระทบหรือสร้างความเสียหายต่อระบบงานข้อมูลสำคัญและการดำเนินงานของสำนักงานทั้งนี้ควรประเมินความเสี่ยงรวมทั้งผลกระทบที่เกิดขึ้นจริงในระหว่างการเกิดเหตุอย่างน้อยปีละ 1 ครั้งเพื่อประเมินผลกระทบและมูลค่าความเสียหายที่แท้จริงและเป็นข้อมูลประกอบการพิจารณาทบทวนหรือปรับปรุงแนวทางในการรับมือและการตอบสนองต่อภัยคุกคามทางไซเบอร์ต่อไป

6.1.2.2 การกำหนดแนวทางรักษาความมั่นคงปลอดภัยของระบบแม่ข่าย (Host Security)

ระบบแม่ข่าย (Host) ควรกำหนดให้มีการรักษาความมั่นคงปลอดภัยที่เหมาะสมและมีมาตรฐานรวมทั้งการปิดช่องโหว่และทำการแพตช์ระบบอย่างเหมาะสมนอกจากนี้ควรมีการกำหนดสิทธิ์ของผู้ใช้งานโดยให้สิทธิเท่าที่จำเป็นต่อการปฏิบัติงานที่ได้รับอนุญาตเท่านั้นรวมทั้งระบบแม่ข่ายควรบันทึกเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยที่สำคัญของสำนักงานและได้รับการติดตามตรวจสอบอย่างสม่ำเสมอ

6.1.2.3 การรักษาความปลอดภัยของเครือข่าย (Network Security)

ระบบการรักษาความมั่นคงปลอดภัยของเครือข่ายควรตั้งค่าให้ปฏิเสธการเข้าถึงของกิจกรรมทั้งหมดที่ไม่ได้รับอนุญาตรวมทั้งอุปกรณ์เครือข่ายทั้งหมดของสำนักงานที่เชื่อมต่อกับเครือข่ายภายนอก

6.2 การตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (Detection and Analysis)

การรวบรวมข้อมูลและตรวจวิเคราะห์จากระบบงานที่มีช่องโหว่จากการโจมตีทางไซเบอร์ภายในสำนักงานควรมีเครื่องมือในการชี้วัดและเฝ้าระวังภัยคุกคามทางไซเบอร์จากหลายแหล่งที่มาโดยอย่างน้อยต้องมีการจัดเก็บและสอบทานบันทึกการเข้าถึงระบบ (Access Log) และบันทึกการดำเนินงาน (Activity Log) และทำการแจ้งเตือนแก่ผู้เกี่ยวข้องเมื่อพบเหตุการณ์ภัยคุกคามทางไซเบอร์

6.2.1 รูปแบบของการโจมตีหรือภัยคุกคามที่มีโอกาสเกิดขึ้นหรือพบเห็นบ่อยครั้ง

6.2.1.1 การโจมตีเพื่อทำให้ระบบลดประสิทธิภาพลงเช่นการโจมตีแบบ DDoS เพื่อทำให้ระบบไม่สามารถให้บริการได้

6.2.1.2 การโจมตีหรือภัยคุกคามที่เกิดจากสื่อบันทึกข้อมูลที่สามารถถอดหรือเคลื่อนย้ายได้หรืออุปกรณ์ต่อพ่วง เช่น มัลแวร์ที่แพร่กระจายเข้าระบบงานจากแฟลชไดรฟ์ USB ที่ติดมัลแวร์

6.2.1.3 การโจมตีผ่านเว็บไซต์หรือระบบงานบนเว็บไซต์เช่นการโจมตีด้วยวิธี Cross Site Scripting เพื่อขโมยข้อมูลหรือการเปลี่ยนเส้นทางไปยังเว็บไซต์ที่มีการโจมตีผ่านช่องโหว่ของ Web Browser และติดตั้งมัลแวร์ไว้และการโจมตีผ่านทางข้อความหรือเอกสารแนบในอีเมลเป็นต้น

6.2.1.4 การโจมตีที่เข้าข่ายการปลอมแปลงตัวตนเช่นการปลอมตัว (Spoofing) เพื่อหลอกลวงและควบคุมระบบการโจมตีโดยการปลอมตัวเป็นบุคคลอื่นเพื่อแทรกสัญญาณการรับส่งข้อมูลระหว่างผู้ใช้งานระบบ (Man in the Middle Attack) และการโจมตีโดยส่งคำสั่ง SQL ผ่านทางระบบงานบนเว็บไซต์เพื่อไปโจมตีระบบฐานข้อมูล (SQL Injection) เป็นต้น

6.2.1.5 ภัยคุกคามที่เกิดจากผู้ใช้งานละเมิดนโยบายการใช้งานระบบเทคโนโลยีสารสนเทศของสำนักงานเช่นการติดตั้งโปรแกรมที่นำไปสู่การรั่วไหลข้อมูลสำคัญหรือผู้ใช้งานทำกิจกรรมที่ผิดกฎหมายผ่านระบบงานเทคโนโลยีสารสนเทศเป็นต้น

6.2.1.6 อุปกรณ์คอมพิวเตอร์หรือสื่อต่างๆสูญหายเช่นเครื่องโน้ตบุคแทบเล็ตโทรศัพท์มือถือหรือสิ่งที่ใช้ยืนยันตัวตนซึ่งเป็นทรัพย์สินของสำนักงานที่สูญหายหรือถูกขโมย

6.2.2 สัญญาณการเกิดเหตุภัยคุกคาม

6.2.2.1 สัญญาณแจ้งเตือนเหตุภัยคุกคามทางไซเบอร์สามารถตรวจสอบได้จากระบบดังต่อไปนี้

(1) ระบบตรวจจับและป้องกันการบุกรุก (Intrusion Detection and Prevention Systems: IDPS) ใช้ในการระบุเหตุการณ์ที่น่าสงสัยว่าอาจเป็นภัยคุกคามและบันทึกข้อมูลที่เกี่ยวข้องรวมถึงวันที่และเวลาที่ตรวจพบการโจมตีประเภทของการโจมตีที่อยู่ IP ต้นทางและปลายทางและชื่อผู้ใช้งานโดยส่วนใหญ่ระบบ IDPS จะระบุกิจกรรมที่เป็นอันตรายโดยใช้ลักษณะเฉพาะของการโจมตี (attack signature) ดังนั้นข้อมูลลักษณะเฉพาะของการโจมตีจะต้องได้รับการอัพเดตอย่างสม่ำเสมอเพื่อให้สามารถตรวจพบการโจมตีรูปแบบใหม่ได้ทั้งนี้ระบบ IDPS สามารถเกิดการแจ้งเตือนที่ผิดพลาดได้ (false positive) โดยแจ้งว่ามีกิจกรรมที่เป็นอันตรายกำลังเกิดขึ้นแต่ในความจริงยังไม่เกิดดังนั้นผู้รับผิดชอบหรือนักวิเคราะห์ระบบจึงควรตรวจสอบข้อมูลแจ้งเตือนจาก IDPS และทบทวนรายละเอียดหรือรวมรวมข้อมูลที่เกี่ยวข้องจากแหล่งข้อมูลอื่นๆ ประกอบการวิเคราะห์

(2) ซอฟแวร์ป้องกันไวรัส (Antivirus Software) เพื่อป้องกันและตรวจจับไวรัสหรือมัลแวร์ในรูปแบบต่างๆแล้วแจ้งเตือนและป้องกันไม่ให้เกิดการแพร่กระจายที่ระบบแม่ข่ายรวมทั้งเพื่อให้ระบบทำงานได้อย่างมีประสิทธิภาพในการป้องกันควรมีการอัพเดตลักษณะเฉพาะของการโจมตีอยู่เสมอ

(3) ระบบบริหารจัดการข้อมูลและวิเคราะห์เหตุการณ์ด้านความมั่นคงปลอดภัย (SIEM) ช่วยในการตรวจจับและทำการแจ้งเตือนจากการวิเคราะห์ที่ได้จากข้อมูลบันทึกเหตุการณ์ (Log data)

(4) ซอฟแวร์ตรวจสอบความถูกต้องของไฟล์เพื่อตรวจสอบการเปลี่ยนแปลงหรือการแก้ไขที่เกิดขึ้นกับไฟล์ที่มีความสำคัญในระหว่างเกิดเหตุภัยคุกคาม (File Integrity Checking Software)

(5) การใช้บริการเฝ้าระวังภัยคุกคามจากผู้ให้บริการภายนอก (Third-Party Monitoring Services)

6.2.2.2 ข้อมูลบันทึกเหตุการณ์ควรจัดเก็บข้อมูลดังต่อไปนี้เป็นอย่างน้อย

(1) ข้อมูลบันทึกเหตุการณ์ของระบบปฏิบัติการการบริการและแอพพลิเคชั่น (Operating System, Service and Application Logs)

(2) ข้อมูลบันทึกเหตุการณ์ของอุปกรณ์เครือข่าย (Network Device Logs)

(3) ข้อมูลบันทึกการเคลื่อนไหวของข้อมูลในเครือข่าย (Network Flow Logs)

6.2.2.3 ข้อมูลสาธารณะ (Publicly Available Information)

ข้อมูลของช่องโหว่หรือจุดอ่อนใหม่จากหน่วยงานด้านการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ เช่น CSIRT หรือช่องทางอื่นๆ ที่มีการอัพเดตและเผยแพร่ข้อมูลภัยคุกคามสู่สาธารณะเป็นต้น

6.2.2.4 บุคคล (People)

(1) บุคลากรภายใน เช่น ผู้ใช้งานระบบผู้ดูแลระบบผู้ดูแลระบบเครือข่ายเจ้าหน้าที่ด้านความมั่นคงปลอดภัยเป็นต้นซึ่งเมื่อได้รับรายงานแล้วจะต้องมีการตรวจสอบข้อเท็จจริงหรือยืนยันข้อมูลทุกครั้ง

(2) บุคคลภายนอกเช่นรายงานจากผู้ใช้งานภายนอกถึงหน้าเว็บไซต์ที่ไม่สามารถใช้งานได้ เป็นต้น และควรมีขั้นตอนในการรับรายงานและตรวจสอบข้อมูลอย่างละเอียดถี่ถ้วน

6.2.3 การวิเคราะห์เหตุการณ์ภัยคุกคาม

6.2.3.1 การจัดทำข้อมูลเครือข่ายและระบบ (Profile Network and System) เพื่อให้สามารถระบุการเปลี่ยนแปลงที่เกิดขึ้นจากการเข้าถึงหรือใช้งานเครือข่ายและระบบงาน จากปกติได้เช่นการวัดปริมาณการใช้งาน bandwidth ของเครือข่ายและบันทึกข้อมูลระดับการใช้งานเฉลี่ยและระดับสูงสุดในแต่ละช่วงเวลาเพื่อตรวจสอบพฤติกรรมการใช้งานที่ผิดปกติของเครือข่าย

6.2.3.2 ศึกษาและเข้าใจพฤติกรรมตามปกติของระบบเครือข่ายและแอพพลิเคชั่นเพื่อช่วยในการสังเกตพฤติกรรมที่ผิดปกติโดยการตรวจสอบบันทึกเหตุการณ์และการแจ้งเตือนด้านความมั่นคงปลอดภัยเพื่อให้มีความคุ้นเคยและจะช่วยให้การสังเกตเหตุการณ์และการแจ้งเตือนที่ผิดปกติได้เร็วและแม่นยำมากยิ่งขึ้น

6.2.3.3 การจัดทำนโยบายการเก็บรักษาบันทึกเหตุการณ์ (Log Retention Policy)

6.2.3.4 การตรวจสอบความสัมพันธ์ของเหตุการณ์ภัยคุกคาม (Event Correlation) โดยการตรวจสอบข้อมูลบันทึกเหตุการณ์ของเครื่องแม่ข่ายเพื่อหาความเชื่อมโยงเพื่อนำประกอบการพิจารณาว่ามีเหตุภัยคุกคามเกิดขึ้นจริงหรือไม่

6.2.3.5 การตั้งเวลาเครื่องแม่ข่ายให้เป็นมาตรฐานเดียวกัน

6.2.3.6 การจัดทำเอกสารหรือฐานข้อมูลที่ใช้เพื่ออ้างอิงสำหรับการดำเนินการวิเคราะห์ข้อมูลภัยคุกคาม

6.2.3.7 การเปิดใช้งานโปรแกรมสำหรับดักจับภัยคุกคาม (Packet Sniffer) เพื่อบันทึกหรือเก็บข้อมูลการจราจรภายในเครือข่ายของสำนักงานเพิ่มเติม

6.2.4 การลงบันทึกข้อมูลเหตุการณ์ภัยคุกคาม

การบันทึกข้อมูลเหตุการณ์ภัยคุกคามจะช่วยให้การรับมือและตอบสนองภัยคุกคามมีประสิทธิภาพและเป็นระบบมากขึ้นสำนักงานควรบันทึกข้อมูลเกี่ยวกับเหตุการณ์ที่เกิดขึ้นตั้งแต่การตรวจพบจนถึงการสิ้นสุดของเหตุการณ์ภัยคุกคามโดยการบันทึกข้อมูลเกี่ยวกับสถานะของเหตุการณ์ภัยคุกคามและข้อมูลที่เกี่ยวข้องอาจจัดเก็บในโปรแกรมประยุกต์หรือฐานข้อมูลเช่นระบบติดตามปัญหา (Issues Tracking System) เพื่อประโยชน์ในการติดตามเหตุการณ์ขั้นตอนการจัดการและแก้ไขเหตุภัยคุกคามเพื่อให้มั่นใจได้ว่าเหตุการณ์ภัยคุกคามที่เกิดขึ้นได้รับการจัดการแก้ไขภายในระยะเวลาที่เหมาะสมในการบันทึกข้อมูลเหตุการณ์ภัยคุกคามควรประกอบด้วยข้อมูลอย่างน้อยดังนี้

- ชื่อเหตุการณ์ภัยคุกคาม
- วันที่บันทึกเหตุการณ์ภัยคุกคาม
- หมายเลขของเหตุการณ์ภัยคุกคาม
- หมายเลขของเหตุการณ์ภัยคุกคามอื่นๆที่เกี่ยวข้องกับเหตุการณ์นี้
- ข้อมูลของผู้แจ้งเหตุการณ์ภัยคุกคาม
- ข้อมูลของเจ้าหน้าที่ผู้รับมือเหตุการณ์ภัยคุกคาม
- ข้อมูลติดต่อสำหรับผู้ที่เกี่ยวข้องอื่นๆเช่นเจ้าของระบบงานผู้ดูแลระบบงานเป็นต้น
- ประเภทของเหตุการณ์ภัยคุกคาม

- วันที่และเวลาเกิดเหตุการณ์ภัยคุกคาม
- วันที่และเวลาพบเหตุภัยการณ์คุกคาม
- วันที่และเวลารายงานเหตุภัยคุกคาม
- รายละเอียดเหตุการณ์ภัยคุกคาม
    - สิ่งที่เกิดขึ้น
    - เกิดขึ้นอย่างไร
    - ทำไมจึงเกิดขึ้น
    - การประเมินทรัพย์สินสารสนเทศที่เสียหาย
    - ผลกระทบทางธุรกิจ
    - ช่องโหว่ที่พบ/ตัวบ่งชี้ของเหตุการณ์ภัยคุกคาม
- การดำเนินการทั้งหมดของทีมรับมือและตอบสนองภัยคุกคามในเหตุการณ์นี้
- การดำเนินการในขั้นถัดไปของทีมรับมือและตอบสนองภัยคุกคามในเหตุการณ์นี้
- ค่าใช้จ่ายในการฟื้นคืนสู่สภาพปกติ
- รายการหลักฐานที่รวบรวมระหว่างการสืบสวนเหตุการณ์ภัยคุกคาม
- สรุปสาระสำคัญของเหตุการณ์ภัยคุกคาม

โดยมีตัวอย่างของแบบฟอร์มบันทึกข้อมูลเหตุการณ์ภัยคุกคามดังภาคผนวก 1

6.2.5 การจัดลำดับความรุนแรงของเหตุการณ์ภัยคุกคามควรคำนึงปัจจัยดังต่อไปนี้

6.2.5.1 ผลกระทบต่อการให้บริการและการดำเนินงานของหน่วยงานที่เกิดภัยคุกคามโดยควรพิจารณาผลกระทบที่เกิดขึ้นทั้งในปัจจุบันและผลกระทบที่มีโอกาสเกิดขึ้นหากเหตุการณ์ภัยคุกคามยังไม่ถูกควบคุมโดยทันที

6.2.5.2 ผลกระทบต่อข้อมูลควรพิจารณา 3 ด้านได้แก่ด้านการรักษาความลับ (Confidentiality) ด้านการรักษาความครบถ้วน (Integrity) และด้านการรักษาสภาพพร้อมใช้ (Availability) รวมทั้งควรพิจารณาว่าเหตุการณ์ภัยคุกคามส่งผลต่อการดำเนินงานโดยรวมของสำนักงานอย่างไรและส่งผลต่อข้อมูลสำคัญของสำนักงาน (Sensitive Information) อย่างไร

6.2.5.3 ความสามารถในการฟื้นฟูระบบควรพิจารณาจากระยะเวลาและทรัพยากรที่ต้องใช้ในการฟื้นฟูระบบจากเหตุภัยคุกคามซึ่งความรุนแรงของเหตุภัยคุกคามและประเภทของทรัพย์สินสารสนเทศที่ได้รับผลกระทบจะเป็นส่วนสำคัญในการพิจารณาความสามารถในการฟื้นฟูระบบ

6.2.6 การแจ้งเตือนเหตุภัยคุกคามทางไซเบอร์แก่ผู้ที่เกี่ยวข้อง

ทีมรับมือและตอบสนองควรดำเนินการแจ้งข้อมูลเกี่ยวกับเหตุภัยคุกคามกับผู้ที่เกี่ยวข้องเพื่อให้ทุกคนสามารถดำเนินการตามหน้าที่ความรับผิดชอบที่ได้กำหนดไว้ทั้งนี้ควรมีข้อกำหนดเกี่ยวกับการแจ้งข้อมูลเหตุภัยคุกคามข้อมูลอะไรบ้างที่ต้องรายงานรายงานต่อใครและเมื่อใดโดยอย่างน้อยควรกำหนดบุคคลผู้รับรายงานข้อมูลที่ต้องรายงานและเวลาที่ต้องรายงานรวมถึงหน่วยงานต่างๆทั้งภายในและภายนอกที่ต้องได้รับแจ้งบุคลากรหรือหน่วยงานที่ควรได้รับการแจ้งเหตุภัยคุกคามมีดังต่อไปนี้

- ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรม (DCIO) หรือเทียบเท่า
- ผู้บริหารความมั่นคงปลอดภัยสารสนเทศ (CISO) หรือเทียบเท่า

- ทีมรับมือและตอบสนองต่อเหตุการณ์อื่นๆ ของสำนักงาน
- ทีมรับมือและตอบสนองต่อเหตุการณ์ภายนอกสำนักงาน (ตามความเหมาะสม)
- เจ้าของระบบงาน
- ฝ่ายกฎหมาย (สำหรับเหตุการณ์ที่อาจมีข้อเกี่ยวข้องทางกฎหมาย)
- ทีมรับมือและตอบสนองต่อเหตุการณ์ CSIRT ดำเนินการตรวจสอบ
  - ความเสียหายที่อาจเกิดขึ้นและการโจรกรรมข้อมูล
  - ความจำเป็นในการเก็บรักษาหลักฐาน
  - ความพร้อมให้บริการเช่นการเชื่อมต่อเครือข่ายการให้บริการระบบงานเป็นต้น
  - เวลาและทรัพยากรที่จำเป็นในการดำเนินการ

6.3 การรับมือและการตอบสนองต่อเหตุการณ์ภัยคุกคาม

การรับมือและการตอบสนองต่อเหตุการณ์ภัยคุกคามประกอบด้วย 3 ขั้นตอนได้แก่การควบคุมภัยคุกคามและจำกัดความเสียหาย (Containment) การกำจัดภัยคุกคาม (Eradication) และการฟื้นฟูระบบ (Recovery) โดยมีรายละเอียดดังนี้

6.3.1 การควบคุมภัยคุกคามและจำกัดความเสียหายที่เกิดขึ้นจากเหตุการณ์ภัยคุกคามทางไซเบอร์ซึ่งจะมีความแตกต่างกันไปขึ้นกับลักษณะประเภทของภัยคุกคามระบบงานหรือบริการที่ได้รับผลกระทบระยะเวลาและทรัพยากรที่จำเป็นต่อการควบคุมความเสียหาย โดยเกณฑ์ประกอบการพิจารณากำหนดแนวทางการควบคุมภัยคุกคามและจำกัดความเสียหายควรพิจารณาในเรื่องดังต่อไปนี้

6.3.1.1 ประสิทธิผลของแนวทางในการควบคุมและจำกัดความเสียหายเช่นการควบคุมบางส่วนหรือการควบคุมทั้งหมด

6.3.1.2 ระยะเวลาในการแก้ปัญหา เช่น การแก้ไขปัญหาแบบฉุกเฉินภายใน 4 ชั่วโมงการแก้ไขปัญหาแบบชั่วคราวภายใน 2 สัปดาห์และการแก้ไขปัญหาแบบถาวรเป็นต้น

นอกจากนี้ สำนักงานควรเก็บรวบรวมหลักฐานที่เกิดขึ้นระหว่างเกิดเหตุการณ์ภัยคุกคามเพื่อใช้ในการแก้ไขปัญหาและจัดการเหตุภัยคุกคาม เพื่อใช้ในกระบวนการทางกฎหมาย หากจำเป็นสำนักงานควรจัดทำเอกสารรวบรวมหลักฐานทั้งหมด ที่ได้ถูกบุกรุกโจมตีรวมถึงระบุขั้นตอนการเก็บรักษาหลักฐานตามกฎหมายและระเบียบข้อบังคับ เพื่อให้สามารถใช้เป็นพยานหลักฐานได้ในชั้นศาล นอกจากนี้ควรมีการบันทึกหลักฐานทุกครั้งหากมีการถ่ายโอนหลักฐานจากบุคคลหนึ่งสู่อีกคน และลงลายมือชื่อกำกับของแต่ละฝ่าย

การจัดทำเอกสารรายละเอียดหลักฐานควรครอบคลุมอย่างน้อย ดังนี้

- ข้อมูลระบุพยานหลักฐานเช่นสถานที่ตั้งหมายเลขซีเรียล (Serial Number) หมายเลขรุ่น (Model Number) ชื่อเครื่องแม่ข่ายที่อยู่สำหรับควบคุมการเข้าใช้งานสื่อกลาง (Media Access Control Addresses) และที่อยู่ IP ของคอมพิวเตอร์
- ชื่อ-สกุลและหมายเลขโทรศัพท์ของบุคคลที่เก็บรวบรวมหรือดูแลพยานหลักฐานในระหว่างการสอบสวน
- วันที่และเวลาที่มีการดำเนินการกับพยานหลักฐานในแต่ละครั้ง
- สถานที่เก็บหลักฐาน

6.3.2 การกำจัดภัยคุกคามทางไซเบอร์ (Eradication) สำนักงานควรกำจัดต้นเหตุของเหตุการณ์ที่เป็นอันตรายต่อเครือข่ายระบบหรือแอพพลิเคชั่น รวมถึงการกำจัดไฟล์ที่เกี่ยวข้องกับการโจมตีและการปิดช่องโหว่ที่ถูกใช้ในการโจมตี ทั้งนี้การกำจัดภัยคุกคามมีวิธีที่แตกต่างกันโดยขึ้นกับประเภทของเหตุภัยคุกคาม
ตัวอย่างของวิธีการกำจัดภัยคุกคามดังนี้

6.3.2.1 การลบมัลแวร์ (Malware) คือการกักกันลบแทนที่หรือกู้คืนไฟล์ที่ติดมัลแวร์ซึ่งโดยส่วนใหญ่หน่วยงานจะต้องกู้คืนระบบสารสนเทศใหม่ โดยการติดตั้งระบบปฏิบัติการระบบงานและข้อมูลจากสื่อบันทึกข้อมูลที่เชื่อถือได้และอาจรวมถึงการอัพเดตข้อมูลคุณลักษณะเฉพาะของโปรแกรมป้องกันไวรัส (antivirus signature) ให้เป็นปัจจุบัน

6.3.2.2 การแก้ไขหรือลดผลกระทบจากช่องโหว่การแก้ไขช่องโหว่สามารถทำได้ด้วยการติดตั้งแพตช์ (Patch) รุ่นล่าสุดของระบบปฏิบัติการและระบบงานเพื่อป้องกันการใช้งานช่องโหว่ที่เป็นช่องทางการโจมตีทั้งนี้หากระบบสารสนเทศไม่สามารถติดตั้งแพตช์ได้ด้วยเหตุผลทางเทคนิคหรือเหตุผลในการปฏิบัติงานให้ลดผลกระทบจากช่องโหว่โดยปรับปรุงการตั้งค่า (configuration) ของระบบสารสนเทศให้สามารถป้องกันหรือจำกัดความเสียหายจากเครื่องแม่ข่ายที่ติดมัลแวร์หากกรณียังไม่มีแพตช์ (patch)ให้ใช้วิธีแก้ไขปัญหาหรือลดผลกระทบชั่วคราว

6.3.2.3 การปรับปรุงการควบคุมการเข้าถึงผู้ใช้งานและเครือข่ายเช่นการลบบัญชีผู้ใช้งานหรือผู้ดูแลระบบที่ถูกบุกรุกการปรับปรุงการควบคุมการเข้าถึงเครือข่ายเช่นการตั้งค่าของระบบตรวจจับและป้องกันการบุกรุก (IDPS) ไฟร์วอลล์ (firewall) เป็นต้นการปรับปรุงการกำหนดค่าพื้นฐาน (baseline configuration) และการลบกลไกการเข้าถึงอื่นๆที่ถูกใช้โดยผู้โจมตี

6.3.3 การฟื้นฟูระบบ (Recovery) การฟื้นฟูระบบเป็นการกู้คืนข้อมูลหรือระบบเพื่อทำให้ระบบสารสนเทศข้อมูลความมั่นคงปลอดภัยของระบบและเครือข่ายกลับสู่สถานะปกติด้วยการติดตั้งระบบปฏิบัติการระบบงานและข้อมูลจากสื่อบันทึกข้อมูลที่เชื่อถือได้พร้อมทั้งมีกลไกติดตามการดำเนินการเพื่อป้องกันการเกิดเหตุภัยคุกคามที่มีความคล้ายคลึงกันขึ้นอีกในอนาคตการฟื้นฟูระบบมีวิธีการที่แตกต่างกันขึ้นอยู่กับประเภทของเหตุภัยคุกคามเช่นการติดตั้งระบบใหม่จากต้นฉบับหรือติดตั้งจากข้อมูลที่สำรองที่เชื่อถือได้การเปลี่ยนรหัสผ่านของระบบการติดตั้งแพตช์ (Patch) ให้เป็นเวอร์ชั่นปัจจุบันและการปรับปรุงความมั่นคงปลอดภัยของเครือข่ายเป็นต้นทั้งนี้ในกรณีที่การกู้คืนข้อมูลและระบบที่เสียหายเสร็จสิ้นผู้ดูแลระบบควรทำการยืนยันว่าระบบสามารถกลับมาทำงานได้ตามปกติให้ผู้ที่เกี่ยวข้องทราบ

6.4 การดำเนินการหลังจากการรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติ (Post Incident Activity)

6.4.1 การเรียนรู้จากภัยคุกคาม (Lessons Learned) สำนักงานควรมีการเรียนรู้จากเหตุภัยคุกคามที่เกิดขึ้น เพื่อนำมาปรับปรุงและพัฒนาแนวทางในการรับมือและตอบสนองต่อภัยคุกคาม รวมทั้งจัดสรรทรัพยากรและเทคโนโลยีให้มีความพร้อมต่อการรับมือเหตุภัยคุกคามต่อไปในอนาคต นอกจากนี้สำนักงาน ควรจัดให้มีการประชุมของหน่วยงานที่มีความเกี่ยวข้องกับเหตุการณ์ภัยคุกคามทางไซเบอร์ที่เกิดขึ้น โดยวัตถุประสงค์ของการประชุมเพื่อให้ทุกหน่วยงานที่เกี่ยวข้องได้มี

การแลกเปลี่ยนข้อมูล รวมทั้งทบทวนเหตุภัยคุกคามและวิธีการรับมือและตอบสนองต่อภัยคุกคามที่เกิดขึ้น

ตัวอย่างประเด็นคำถามที่สำนักงานสามารถพิจารณาปรับใช้ประกอบการประชุมแลกเปลี่ยนข้อมูลหลังจากการรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ เช่น

• เหตุภัยคุกคามที่เกิดขึ้นคืออะไรเกิดขึ้นเมื่อเวลาใดบ้าง

• เจ้าหน้าที่และฝ่ายบริหารสามารถรับมือภัยคุกคามได้ดีเพียงใดการดำเนินการเป็นไปตามขั้นตอนการปฏิบัติงานที่กำหนดไว้หรือไม่

• ข้อมูลอะไรบ้างที่จำเป็นต้องได้รับรายงานภายในระยะเวลาอันสั้นเพื่อเพิ่มประสิทธิภาพในการรับมือและตอบสนองต่อเหตุการณ์

• มีขั้นตอนหรือการดำเนินการใดๆที่อาจเป็นอุปสรรคหรือไม่สอดคล้องกับขั้นตอนของการฟื้นฟูระบบหรือไม่

• เจ้าหน้าที่และฝ่ายบริหารมีแนวทางดำเนินการเพิ่มเติมหรือแตกต่างไปจากเดิมหากเกิดภัยคุกคามที่มีรูปแบบคล้ายคลึงกันเกิดขึ้นในครั้งต่อไป

• การแลกเปลี่ยนข้อมูลกับหน่วยงานอื่นๆสามารถปรับปรุงให้ดีขึ้นได้อย่างไร

• แนวทางการดำเนินการแก้ไข (corrective action) ที่สามารถเพิ่มเติมเพื่อป้องกันภัยคุกคามที่คล้ายคลึงกันในอนาคตได้

• สัญญาณอะไรบ้างที่สามารถนำมาใช้เพื่อตรวจจับภัยคุกคามที่มีลักษณะคล้ายคลึงกันซึ่งอาจเกิดขึ้นในอนาคต

• เครื่องมือหรือทรัพยากรที่มีความจำเป็นต้องได้รับการจัดสรรเพิ่มเติมเพื่อใช้ดำเนินการในการตรวจจับวิเคราะห์และบรรเทาเหตุภัยคุกคามที่อาจเกิดขึ้นในอนาคต

6.4.2 การวัดผลและปรับปรุงการปฏิบัติงานในการรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติ

6.4.2.1 จำนวนเหตุการณ์ภัยคุกคามทางไซเบอร์ที่รับมือต่อเดือน/ไตรมาส/ปี

6.4.2.2 ระยะเวลาในการรับมือและตอบสนองต่อเหตุการณ์สามารถวัดได้หลายวิธี เช่น

• ระยะเวลาทั้งหมดที่ใช้ในการรับมือและตอบสนอง

• ระยะเวลาที่ใช้ในการดำเนินการในแต่ละช่วงของกระบวนการรับมือและตอบสนองในแต่ละขั้นตอน

• ระยะเวลาที่ทีมรับมือและตอบสนองต่อเหตุการณ์ใช้ในการตอบสนองหลังจากที่ได้รับรายงานภัยคุกคาม

• ระยะเวลาที่ทีมรับมือและตอบสนองต่อเหตุการณ์ใช้ในการรายงานภัยคุกคามต่อผู้บริหารหรือหน่วยงานภายนอกที่เกี่ยวข้อง เช่น CSIRT เป็นต้น

6.4.3 การประเมินกระบวนการรับมือในแต่ละเหตุการณ์ (Objective Assessment) ตัวอย่างของการประเมิน เช่น

•การตรวจทานบันทึกเหตุการณ์ (log) แบบฟอร์มรายงานและเอกสารอื่นๆที่เกี่ยวข้องกับภัยคุกคามเพื่อให้การปฏิบัติงานเป็นไปตามขั้นตอนการรับมือภัยคุกคามทางไซเบอร์ที่กำหนดไว้

•การระบุว่าสัญญาณการเกิดเหตุภัยคุกคามอะไรบ้างที่บันทึกไว้เพื่อพิจารณาว่าการบันทึกเหตุการณ์และระบุเหตุภัยคุกคามมีประสิทธิภาพเพียงใด

•พิจารณาว่าภัยคุกคามที่เกิดขึ้นก่อให้เกิดความเสียหายก่อนที่จะตรวจพบหรือไม่

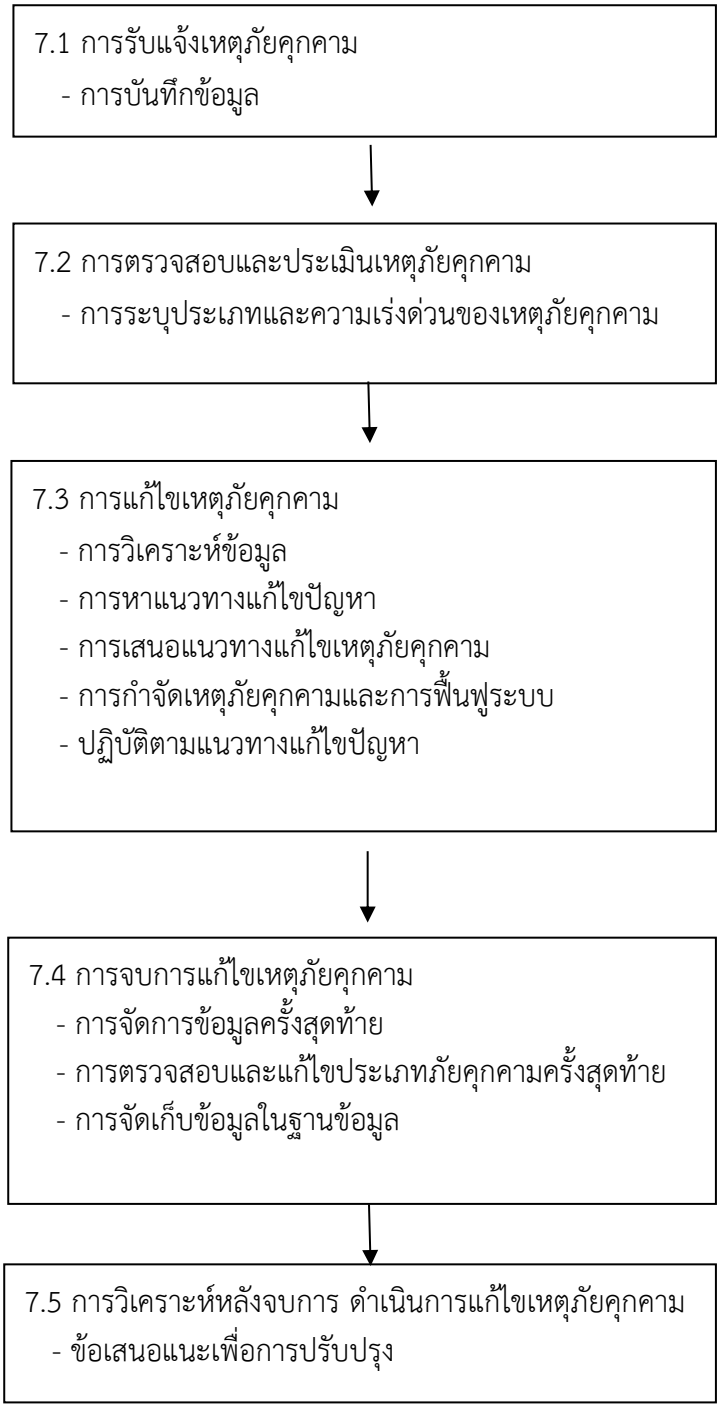
•พิจารณาว่ามีการระบุสาเหตุที่แท้จริงของภัยคุกคามไว้หรือไม่และการระบุช่องทางการโจมตีช่องโหว่ที่เปิดเผยและลักษณะของระบบเครือข่ายและแอพพลิเคชั่นที่เป็นถูกโจมตี

•พิจารณาว่าภัยคุกคามเป็นการเกิดขึ้นอีกครั้งของภัยคุกคามก่อนหน้าหรือไม่

•การประเมินความเสียหายทางการเงินจากภัยคุกคามที่เกิดขึ้นเช่นข้อมูลและกระบวนการทางธุรกิจที่สำคัญที่ได้รับผลกระทบจากภัยคุกคาม

6.4.4 การประเมินประสิทธิภาพของทีมรับมือและตอบสนอง (Subjective Assessment) สำนักงานอาจกำหนดให้มีการประเมินผลการปฏิบัติงานของทีมรับมือและตอบสนองทั้งในรูปแบบรายบุคคลหรือทั้งทีมรวมทั้งอาจให้เจ้าของระบบงานที่ระบบถูกโจมตีเป็นผู้ทำการประเมินการปฏิบัติหน้าที่ของทีมรับมือและตอบสนองก็ได้เพื่อประกอบการพิจารณาว่าประสิทธิภาพของการรับมือให้ผลลัพธ์เป็นที่น่าพอใจหรือไม่

7. กระบวนการรับมือและแก้ไขเหตุภัยคุกคาม



แผนภาพที่ 2 กระบวนการรับมือและแก้ไขเหตุภัยคุกคาม

7.1 การรับแจ้งเหตุภัยคุกคาม

7.1.1การแจ้งเตือนมีที่มาจากหลายแหล่งอาจมาจากการพบเองของ CSIRT หรือแหล่งอื่น ๆ แจ้งมา เช่น

- การแจ้งโดยระบบเฝ้าระวังเครือข่าย
- สมัครเพื่อรับข่าวสารทางอีเมลกลุ่มเครือข่ายด้านความมั่นคงปลอดภัยไซเบอร์
- การสมัครเพื่อรับข้อมูลในรูปแบบ automatic feed

และสร้างช่องทางติดต่อรับแจ้งเหตุภัยคุกคาม ได้แก่ อีเมล โทรศัพท์ แบบฟอร์มติดต่อทางเว็บไซต์ สื่อสังคมออนไลน์

7.1.2 การบันทึกข้อมูลเหตุภัยคุกคามทั้งหมดที่ได้รับแจ้งควรจะได้รับการบันทึกใน ticketing system ซึ่งเป็นระบบสำหรับรับแจ้งเหตุและติดตามการดำเนินการโดยจะมีการระบุหมายเลข ticket สำหรับแต่ละเหตุภัยคุกคามที่ได้รับแจ้งเพื่อใช้อ้างอิงเวลาติดต่อสื่อสารข้อมูลเหตุภัยคุกคามที่ได้รับแจ้งควรจัดการให้อยู่ในที่เดียวกันเนื่องจากข้อมูลอาจมีความสัมพันธ์กับข้อมูลที่ได้รับแจ้งก่อนหน้าข้อดีอีกอย่างของการมีศูนย์กลางในการจัดการข้อมูลคือในกรณีที่พบว่าเหตุภัยคุกคามที่ได้รับแจ้งมีความคล้ายคลึงกับที่ได้รับแจ้งก่อนหน้าก็อาจนำช่องทางการติดต่อหรือวิธีการจัดการเดิมมาใช้งานได้

7.2 การตรวจสอบและประเมินเหตุภัยคุกคาม

ขั้นตอนนี้ถือว่าเป็นหนึ่งในขั้นตอนที่สำคัญที่สุดในกระบวนการรับมือและแก้ไขเหตุภัยคุกคามเพราะเป็นขั้นตอนที่ต้องมีการตัดสินใจสำคัญอันดับแรก CSIRT ต้องตรวจสอบว่าเหตุภัยคุกคามที่ได้รับแจ้งเป็นเหตุภัยคุกคามจริงหรือไม่แหล่งที่มาของรายงานเชื่อถือได้มากน้อยเพียงใด จากนั้นควรพิจารณาดังนี้

- เหตุภัยคุกคามที่เกิดขึ้นอยู่ใต้ขอบเขตการทำงานและความรับผิดชอบของ CSIRT หรือไม่
- เกิดผลกระทบอะไรบ้าง
- เกิดความเสียหายร้ายแรงเพียงใด
- มีความเร่งด่วนมากน้อยแค่ไหนความเสียหายจะเพิ่มขึ้นตามเวลาที่ดำเนินไปหรือไม่จะลุกลามไปยังผู้รับบริการผู้มีส่วนเกี่ยวข้องอื่นๆหรือไม่

โดยหลังจากตรวจสอบเป็นการตอบสนองต่อผู้แจ้งโดยมีเนื้อหาดังนี้

- ตอบรับทราบการแจ้งเตือน
- อธิบายสิ่งที่จะดำเนินการ
- สิ่งที่ผู้แจ้งควรกระทำในระหว่างรอ CSIRT รับมือและแก้ปัญหาเหตุภัยคุกคามจนสำเร็จ

7.2.1 การระบุประเภทและความเร่งด่วนของเหตุภัยคุกคาม

เป็นการระบุเบื้องต้นว่าเหตุภัยคุกคามที่ได้รับแจ้งอยู่ในประเภทใดสามารถกลับมาแก้ไขเมื่อมีข้อมูลเพิ่มเติมและเมื่อพิจารณาประเภทของเหตุภัยคุกคามร่วมกับประเภทผู้แจ้งจะสามารถระบุความเร่งด่วนในการดำเนินการรวมถึงทรัพยากรที่จำเป็นในการรับมือเหตุภัยคุกคาม โดยการกำหนดความเร่งด่วนของเหตุภัยคุกคาม เพื่อการตอบสนองต่อเหตุการณ์ตามระดับความเร่งด่วน มาจากการกำหนดระดับความสำคัญและระดับความรุนแรง ดังตารางที่ 1-4

ตารางที่ 1 แสดงประเภทอุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายคอมพิวเตอร์ตามระดับความสำคัญ (Priority)

ระดับความสำคัญ	ประเภทอุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายคอมพิวเตอร์
1	เครื่องพิมพ์ทุกชนิด (ชนิดเลเซอร์ชนิดน้ำหมึกชนิดเข็มกระแทก)
2	ระบบคอมพิวเตอร์ลูกข่าย
3	- อุปกรณ์เครือข่ายที่เชื่อมต่อระบบคอมพิวเตอร์ลูกข่ายหรือเครื่องพิมพ์เข้าสู่ระบบ เครือข่ายคอมพิวเตอร์เช่น Switch Access Point (AP) Network Access Control (NAC) เป็นต้น - เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการปรับปรุงรุ่นหรือฐานข้อมูลของซอฟต์แวร์สำเร็จรูป
4	- เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบงานบนระบบเครือข่ายอินทราเน็ต - เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ e-Mail
5	- อุปกรณ์ป้องกันเครือข่ายคอมพิวเตอร์ (Firewall) - อุปกรณ์กระจายสัญญาณเครือข่ายคอมพิวเตอร์หลัก (Core Switch) - อุปกรณ์กระจายการทางานบนระบบเครือข่ายคอมพิวเตอร์ (Load Balance) - เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบงานบนระบบเครือข่ายอินเทอร์เน็ต

ตารางที่ 2 แสดงความหมายตามระดับความรุนแรง (Severity)

ระดับความรุนแรง	ลักษณะผลกระทบตามระดับความรุนแรง
5 (วิกฤต)	- ระบบสารสนเทศหลัก (Critical System) ที่ปฏิบัติงานหรือระบบโครงสร้างพื้นฐาน ทั้งระบบได้รับความเสียหายอย่างรุนแรงไม่สามารถปฏิบัติงานได้ - ส่งผลกระทบต่อระดับการปฏิบัติงานทั้งหมด - เจ้าหน้าที่ไม่สามารถปฏิบัติงานได้
4 (สูง)	- ระบบสารสนเทศหลัก (Critical System) หรือระบบโครงสร้างพื้นฐานเสียหาย อย่างรุนแรงบางส่วนและไม่สามารถปฏิบัติงานได้ - ส่งผลกระทบต่อระดับการปฏิบัติงานทั้งหมด - เจ้าหน้าที่ไม่สามารถปฏิบัติงานได้

ระดับความรุนแรง	ลักษณะผลกระทบตามระดับความรุนแรง
3 (ปานกลาง)	- ระบบสารสนเทศหลัก (Critical system) หรือระบบโครงสร้างพื้นฐานยังสามารถ ปฏิบัติงานได้แต่ประสิทธิภาพในการปฏิบัติงานลดลง - ส่งผลกระทบต่อระดับการปฏิบัติงาน - เจ้าหน้าที่ภายในสำนักงานยังสามารถปฏิบัติงานได้บางส่วน
2 (ต่ำ)	- ระบบสารสนเทศของสำนักงานบางส่วนได้รับความผลกระทบและยังสามารถปฏิบัติงานได้ - ไม่มีผลกระทบต่อระดับการให้บริการ (SLA) - มีผลกระทบต่อการปฏิบัติงานภายในสำนักงานเล็กน้อย
1 (ต่ำมาก)	- ระบบสารสนเทศได้รับผลกระทบเล็กน้อย - ไม่มีผลกระทบต่อระดับการปฏิบัติงาน

การกำหนดระดับความเร่งด่วนและข้อตกลงระดับการให้บริการแจ้งเตือน

ตารางที่ 3 แสดงการกำหนดระดับความเร่งด่วนตามระดับความสำคัญและระดับความรุนแรง

Priority / Severity	1	2	3	4	5
1	ต่ำมาก (Very Low)	ต่ำ (Low)	ต่ำ (Low)	ปานกลาง (Medium)	ปานกลาง (Medium)
2	ต่ำ (Low)	ต่ำ (Low)	ปานกลาง (Medium)	ปานกลาง (Medium)	สูง (High)
3	ต่ำ (Low)	ปานกลาง (Medium)	ปานกลาง (Medium)	สูง (High)	สูง (High)
4	ปานกลาง (Medium)	ปานกลาง (Medium)	สูง (High)	วิกฤต (Critical)	วิกฤต (Critical)
5	สูง (High)	วิกฤต (Critical)	วิกฤต (Critical)	วิกฤต (Critical)	วิกฤต (Critical)

ตารางที่ 4 แสดงการตอบสนองต่อเหตุการณ์ตามระดับความเร่งด่วน

ลำดับที่	การตอบสนอง	ระดับความเร่งด่วน				
		ต่ำมาก	ต่ำ	ปานกลาง	สูง	วิกฤต
1	ภายใน 20 นาที				☐	☐
2	ภายใน 40 นาที	☐	☐	☐		

7.3 การแก้ไขเหตุภัยคุกคาม

7.3.1 การวิเคราะห์ข้อมูล

ขั้นตอนนี้คือการรวบรวมข้อมูลให้มากที่สุดจากรายงานเพื่อให้ทีมได้ภาพรวมเกี่ยวกับเหตุภัยคุกคามและสาเหตุการเกิดเหตุภัยคุกคามที่สมบูรณ์ที่สุดตัวอย่างข้อมูลที่รวบรวมเช่น

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

นอกจากนี้อาจหาข้อมูลที่เกี่ยวข้องกับเหตุภัยคุกคามจากฐานข้อมูลของระบบหรืออุปกรณ์ต่างๆเช่น

- Netflow data
- ล็อกในเราเตอร์
- ล็อกใน proxy server
- ล็อกในเว็บแอปพลิเคชัน
- ล็อกในเมลเซิร์ฟเวอร์
- ล็อกใน DHCP เซิร์ฟเวอร์
- ล็อกในเซิร์ฟเวอร์ที่ให้บริการยืนยันตัวตน (authenticationserver)
- ฐานข้อมูลต่างๆที่เกี่ยวข้อง
- อุปกรณ์เกี่ยวกับความมั่นคงปลอดภัยเช่น Firewall หรือ IDS(Intrusion Detection System)

เมื่อแหล่งที่มาของการโจมตีทางไซเบอร์อยู่นอกขอบเขตนอกองค์กรหรือหน่วยงาน CSIRT อาจจำเป็นต้องใช้ข้อมูลจากแหล่งอื่นๆมาประกอบการวิเคราะห์ด้วยในการขอข้อมูลเพิ่มเติม CSIRT ต้องระบุแหล่งข้อมูล

เนื่องจากเหตุภัยคุกคามอาจดำเนินไปเรื่อยๆและความล่าช้าที่เกิดจากการรอข้อมูลจนครบถ้วนอาจกลายเป็นปัญหาหรือทำให้ผู้บุกรุกมีเวลาเพิ่มขึ้นในการปกปิดร่องรอย ซึ่งข้อมูลที่หาได้เพียงร้อยละ 20 ถือเป็นสี่ในห้าขององค์ความรู้ที่จำเป็นต้องใช้ในการแก้ไขเหตุภัยคุกคาม

7.3.2 การหาแนวทางแก้ไขปัญหา

การหาแนวทางแก้ไขปัญหาที่ดีที่สุดจากทางเลือกต่างๆโดยพิจารณาข้อสังเกตและข้อสรุปจากการวิเคราะห์ข้อมูลที่รวบรวมหรือจากการหารือระดมสมองผลลัพธ์อาจเป็นแนวทางการตั้งค่าอุปกรณ์หรือเครื่องมือเพื่อแก้ไขหรือลดผลกระทบของปัญหา

7.3.3 การเสนอแนวทางแก้ไขเหตุภัยคุกคาม

ในการแก้ไขเหตุภัยคุกคาม CSIRT อาจต้องเสนอแนวทางปฏิบัติหนึ่งหรือสองแนวทางทั้งนี้ขึ้นอยู่กับความซับซ้อนของเหตุภัยคุกคามนั้นๆหรือหากแนวทางแก้ไขเหตุภัยคุกคามมีค่าใช้จ่ายอาจต้องนำเสนอให้ฝ่ายบริหารเข้าใจ ตัวอย่างของแนวทางแก้ไขเหตุภัยคุกคามเช่น

- การยุติการให้บริการชั่วคราว
- การตรวจหามัลแวร์ในเครือข่าย
- การแก้ไขช่องโหว่ในระบบ
- การตั้งค่าระบบเพื่อเพิ่มความมั่นคงปลอดภัย
- การแยกระบบออกจากเครือข่าย
- การตรวจสอบระบบ
- การหาข้อมูลเพิ่มเติม (อาจว่าจ้างบุคคลภายนอก)
- การซื้อบริการเสริมเช่นบริการป้องกันจากการโจมตี DDoS
- การยกระดับการแก้ปัญหาให้ผู้บริหารหรือคณะกรรมการด้านกฎหมายร่วมตัดสินใจ
- การร่วมมือกับหน่วยงานบังคับใช้กฎหมายในกระบวนการสืบสวนอาชญากรรม
- หากระบบหรือแอปพลิเคชันที่องค์กรใช้งานมีการดูแลโดยองค์กรภายนอกเช่นระบบบนคลาวด์ CSIRT ก็อาจจำเป็นต้องส่งคำแจ้งเตือนหรือทำงานร่วมกับองค์กรเหล่านั้น

7.3.4 ปฏิบัติตามแนวทางแก้ไขเหตุภัยคุกคาม

เรื่องที่ควรพิจารณาหลังจากปฏิบัติตามแนวทางแก้ไขเหตุภัยคุกคามที่ดำเนินการเสร็จสิ้นแล้ว

- ระบบสามารถให้บริการตามปกติได้หรือไม่
- การปฏิบัตินั้นสามารถแก้ไขปัญหาได้เสร็จสิ้นหรือไม่
- ทราฟฟิกในเครือข่ายได้รับการเฝ้าระวังอย่างเหมาะสมหรือไม่

หากเป้าหมายของการโจมตียังมีช่องโหว่หรือแนวทางการแก้ไขปัญหาไม่สามารถแก้ไขเหตุภัยคุกคามอย่างสมบูรณ์ต้องทำตามขั้นตอนก่อนหน้าอีกครั้งเพื่อหาแนวทางการแก้ไขปัญหาที่เหมาะสมต่อไป

7.3.5 การกำจัดเหตุภัยคุกคามและการฟื้นฟูระบบ

หลังจากที่แก้ไขปัญหาที่สร้างความเสียหายให้กับระบบเรียบร้อยการฟื้นฟูระบบสามารถให้บริการตามปกติอย่างไรก็ตามในบางกรณีอาจต้องใช้เวลาเพิ่มเติมพอสมควรเช่นกรณีที่มีการดำเนินการทางกฎหมายเพื่อสืบสวนทางอาญา

7.4 การจบการแก้ไขเหตุภัยคุกคาม

CSIRT ควรมีนโยบายที่ชัดเจนว่าจะจบการดำเนินการรับมือและแก้ไขเหตุภัยคุกคามเมื่อใดและอย่างไรโดยสถานะ ticket ของเหตุภัยคุกคามที่ได้รับแจ้งใน ticket system คงสถานะเป็น open หรือ “ระหว่างการดำเนินการ” และมีการอัปเดตสถานะเพิ่มรายละเอียดการดำเนินการเรื่อยๆจนกว่าเหตุภัยคุกคามจะได้รับการแก้ไขโดยสมบูรณ์หรือจบการดำเนินการปิด ticket เปลี่ยน

สถานะป็นclosed เมื่อได้รับการแก้ไขในเชิงเทคนิคตามขั้นตอนที่กำหนดซึ่งอาจเลือกดำเนินการถึงการติดตามประเมินผล (follow-up) แล้วจึงจบการดำเนินการ

7.4.1 การจัดการข้อมูลครั้งสุดท้าย

แนบเอกสารที่เกี่ยวข้องทุกอย่างเข้าไปใน ticket จากนั้นจึงดำเนินการแจ้งฝ่ายต่างๆที่เกี่ยวข้องตามประเด็นดังนี้

- คำอธิบายสั้นๆเกี่ยวกับเหตุการณ์
- ผลลัพธ์จากการดำเนินการรับมือและแก้ไขเหตุภัยคุกคาม
- สิ่งที่พบและข้อเสนอแนะ

7.4.2 การตรวจสอบและแก้ไขประเภทภัยคุกคามครั้งสุดท้าย

เมื่อมีข้อมูลเกี่ยวกับเหตุภัยคุกคามที่ได้รับแจ้งครบถ้วนแล้วควรตรวจสอบความถูกต้องของประเภทภัยคุกคามที่ได้ระบุไว้หากไม่ถูกต้องให้แก้ไขและปรับปรุงการระบุประเภทภัยคุกคามให้แม่นยำยิ่งขึ้น

7.4.3 การจัดเก็บข้อมูลในฐานข้อมูล

ในการจัดเก็บข้อมูลที่อยู่ใน ticket ที่มีสถานะ “closed” หรือจบการดำเนินการหลังการดำเนินการรับมือเหตุภัยคุกคามเสร็จสิ้นควรเก็บในลักษณะที่สามารถสืบค้นได้ในภายหลังเพื่อใช้อ้างอิงวิธีการรับมือกรณีที่เกิดเหตุภัยคุกคามลักษณะใกล้เคียงกันในอนาคต

7.5 การวิเคราะห์หลังจบการดำเนินการแก้ไขเหตุภัยคุกคาม

ควรเรียนรู้จากบทเรียนที่ได้รับจากเหตุภัยคุกคามที่เกิดขึ้นเพื่อป้องกันไม่ให้เกิดเหตุเช่นนี้ขึ้นอีกในอนาคตหรือปรับปรุงกระบวนการให้รับมือและแก้ไขเหตุภัยคุกคามต่างๆได้รวดเร็วขึ้น ตัวอย่างของบทเรียนที่ได้และข้อเสนอแนะเพื่อนำไปปรับปรุงและพัฒนาได้แก่

- การเพิ่มเติมเนื้อหาหรือคำอธิบายในนโยบายความมั่นคงปลอดภัยขององค์กร
- การพัฒนาปรับปรุงโครงสร้างสถาปัตยกรรมของเครือข่าย
- การพัฒนาปรับปรุงกลไกการตรวจจับเหตุภัยคุกคาม
- การจัดหาเครื่องมือเพื่อเพิ่มความสามารถวิเคราะห์
- การได้เรียนรู้วิธีรับมือเหตุภัยคุกคามรูปแบบใหม่ๆ

8. ทีมรับมือและตอบสนองภัยคุกคาม(Computer Security Incident Response Team)

ทีมรับมือและตอบสนองภัยคุกคาม (Computer Security Incident Response Team : CSIRT) คือหน่วยงานประสานงานสนับสนุนต่อการตอบสนองและจัดการต่อเหตุการณ์ความมั่นคงปลอดภัยทางคอมพิวเตอร์สำหรับรับมือกับเหตุการณ์ด้านความมั่นคงปลอดภัยคอมพิวเตอร์ และให้บริการสิ่งจำเป็นสำหรับรับมือกับเหตุการณ์นั้นๆ เช่น การแจ้งเตือน การให้คำแนะนำ การอบรม และการบริหารจัดการทำหน้าที่ตรวจสอบเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์คอยส่งคำเตือนต่อการโจมตีไปยังผู้เกี่ยวข้องรวมทั้งตอบสนองต่อเหตุการณ์ต่างๆ

8.1 กรอบการทำงานสำหรับ CSIRT

8.1.1 Incident Monitoring เป็นงานเฝ้าระวังเหตุการณ์ภัยคุกคาม และตรวจสอบการแจ้งเตือนของระบบเฝ้าระวังต่างๆ เช่น SIEM IPS Firewall หากพบภัยคุกคามจะตรวจสอบเบื้องต้นเพื่อประเมินสถานการณ์ หากพบว่าเป็นภัยคุกคามจะสร้าง ticket และกำหนดระดับความรุนแรงเพื่อให้ส่วนงาน Incident Response ดำเนินการตอบสนองต่อเหตุการณ์ภัยคุกคาม

8.1.2 Incident Response เป็นงานที่ตอบสนองต่อเหตุการณ์ภัยคุกคาม มีหน้าที่เก็บข้อมูลจากเครื่องที่ได้รับผลกระทบวิเคราะห์เหตุการณ์ภัยคุกคามควบคุมสถานการณ์ไม่ให้ลุกลามแก้ไขสถานการณ์ให้คำแนะนำเจ้าของระบบเกี่ยวการวิธีการแก้ไขและสรุปผลการตอบสนองต่อเหตุการณ์ภัยคุกคาม ประสานกับหน่วยงานที่เกี่ยวข้อง รายงานความคืบหน้า

8.1.3 Digital Forensics เป็นงานที่รับข้อมูลจากIncident Response เพื่อวิเคราะห์ภัยคุกคาม ในเชิงลึก ผลการวิเคราะห์จะส่งให้ Incident Response เพื่อใช้ดำเนินงานต่อ และส่งต่อให้กับส่วนงาน Threat Analyst ต่อไป

8.1.4 Threat Analyst เป็นงานที่วิเคราะห์พฤติกรรมการใช้งานของระบบโดยรวม โดยวิเคราะห์ผ่านระบบ SIEM และสร้าง Dashboard ในระบบ SIEM สำหรับใช้เฝ้าระวังภัยคุกคาม นอกจากนี้ยังมีหน้าที่รวบรวมข้อมูลเกี่ยวกับภัยคุกคามใหม่ๆ เพื่อเตรียมเฝ้าระวังภัยคุกคาม

8.1.5 Command Center เป็นศูนย์กลางบริหารงาน CSOC มีหน้าที่บริหารและติดตามสถานะของเหตุการณ์ภัยคุกคามทั้งหมด

8.1.6 Lessons Learned เป็นงานการเรียนรู้จากเหตุภัยคุกคามที่เกิดขึ้นเพื่อนำมาปรับปรุงและพัฒนาแนวทางในการรับมือและตอบสนองต่อภัยคุกคามรวมทั้งจัดสรรทรัพยากรและเทคโนโลยีให้มีความพร้อมต่อการรับมือเหตุภัยคุกคามต่อไปในอนาคต

8.2 โครงสร้างทีม CSIRT

• หัวหน้าทีม CSIRT มีบทบาทสื่อสารและสรรหางบประมาณของทีม CSIRT

• ผู้จัดการเหตุการณ์ มีบทบาทประสานการประชุมทีม CSIRT เพื่อตอบสนองต่อเหตุภัยคุกคามรวมทั้งสื่อสารกับสมาชิก CSIRT ภายในองค์กรและผู้เชี่ยวชาญจากภายนอก

• สมาชิกทีมCSIRT มีบทบาททางเทคนิคเช่นรับผิดชอบในการตรวจจับเหตุการณ์การตอบสนองและการรายงานวิเคราะห์ และเฝ้าระวังการบุกรุกที่เกิดขึ้น กู้คืนและรักษาความสมบูรณ์ของหลักฐานเพื่อให้มีการสอบสวนที่ถูกต้องตามกฎหมาย

ภาคผนวก

1. แบบบันทึกเหตุการณ์ภัยคุกคาม
2. ตัวอย่างแสดงรายละเอียดคำอธิบายเหตุการณ์ต่อระดับความรุนแรง
3. ทีมรับมือและตอบสนองภัยคุกคาม CSIRTสำนักงานเลขาธิการสภาผู้แทนราษฎร
4. ทีมรับมือและตอบสนองภัยคุกคาม CSIRT สำนักงานเลขาธิการวุฒิสภา

1. แบบบันทึกเหตุการณ์ภัยคุกคาม

ตารางที่ 5 แบบบันทึกเหตุการณ์ภัยคุกคาม

<table>
<tr><td colspan="4">แบบบันทึกเหตุการณ์ภัยคุกคาม</td></tr>
<tr><td>วันที่ / เดือน / ปี

--</td><td>ชื่อเหตุการณ์ภัยคุกคาม
----------</td><td>หมายเลขของเหตุการณ์ภัยคุกคาม
----------</td><td>หมายเลขของเหตุการณ์ภัยคุกคามอื่นๆที่เกี่ยวข้อง
----------</td></tr>
<tr><td colspan="2">ข้อมูลของผู้แจ้งเหตุการณ์ภัยคุกคาม</td><td colspan="2">ข้อมูลของเจ้าหน้าที่ผู้รับมือเหตุการณ์ภัยคุกคาม</td></tr>
<tr><td>ชื่อ – นามสกุล</td><td>หน่วยงาน /โทรศัพท์/ อีเมล</td><td>ชื่อ – นามสกุล</td><td>โทรศัพท์/อีเมล</td></tr>
<tr><td colspan="2">วันที่และเวลาเกิดเหตุการณ์ภัยคุกคาม
----------</td><td>วันที่และเวลาพบเหตุภัยการณ์คุกคาม
----------</td><td>วันที่และเวลารายงานเหตุภัยคุกคาม
----------</td></tr>
<tr><td colspan="4">รายละเอียดเหตุการณ์ภัยคุกคาม</td></tr>
<tr><td colspan="4">- สิ่งที่เกิดขึ้น
- เกิดขึ้นอย่างไร
- เหตุใดจึงเกิดขึ้น
- การประเมินทรัพย์สินสารสนเทศที่เสียหาย
- ผลกระทบ
- ช่องโหว่ที่พบ/ตัวบ่งชี้ของเหตุการณ์ภัยคุกคาม</td></tr>
<tr><td colspan="2">การดำเนินการทั้งหมดของทีมตอบสนองภัยคุกคามต่อเหตุการณ์นี้</td><td colspan="2">รายการหลักฐานที่รวบรวมระหว่างการสืบสวนเหตุการณ์ภัยคุกคาม</td></tr>
<tr><td colspan="2"></td><td colspan="2"></td></tr>
<tr><td colspan="2">ค่าใช้จ่ายในการฟื้นคืนสู่สภาพปกติ</td><td colspan="2"></td></tr>
<tr><td colspan="4">สรุปสาระสำคัญของเหตุการณ์ภัยคุกคาม</td></tr>
<tr><td colspan="4"></td></tr>
</table>

2. ตัวอย่างแสดงรายละเอียดคำอธิบายเหตุการณ์ต่อระดับความรุนแรง

ตารางที่ 6 ตัวอย่างแสดงรายละเอียดคำอธิบายเหตุการณ์ต่อระดับความรุนแรง

ลำดับที่	แสดงรายละเอียดคำอธิบายเหตุการณ์ต่อระดับความรุนแรง
ความรุนแรงระดับวิกฤต (ระดับ 5)	
1	ตรวจพบ Website หรือ Server ไม่สามารถให้บริการได้
2	ตรวจพบเหตุการณ์พยายาม Login แต่ Failedระดับ Admin จำนวนหลายครั้ง
3	ตรวจพบพฤติกรรมการโจมตีจากข้อมูลที่มีการ Scan ระบบฯ
4	อุปกรณ์ Antivirus ตรวจพบ Malware ที่ไม่สามารถแก้ไขได้
5	ตรวจพบพฤติกรรมพยายามติดต่อไปยังIP/Domain ที่เกี่ยวข้อง Snatch Ransom ware
6	ตรวจพบพฤติกรรมพยายามติดต่อไปยังIP/Domain ที่เกี่ยวข้องSodinokibi Ransom ware
7	ตรวจพบพฤติกรรมพยายามติดต่อไปยังIP/Domain ที่เกี่ยวข้อง Maze Ransom ware
8	ตรวจพบพฤติกรรมพยายามติดต่อไปยังIP/Domain ที่เกี่ยวข้องWanacry
ความรุนแรงระดับสูง (ระดับ 4)	
9	ตรวจพบ IP ที่เป็นกลุ่มเสี่ยงจากภายนอกสามารถเข้าถึงระบบภายในได้
10	ตรวจพบ IP ที่เป็นกลุ่มเสี่ยงจากภายนอกสามารถเข้าถึงระบบภายในด้วย Remote Access Service ได้
11	ตรวจพบ IP จากภายในพยายามติดต่อไปยังIP กลุ่มเสี่ยงภายนอก
12	ตรวจพบพฤติกรรมพยายามติดต่อไปยังIP/Domain ที่เกี่ยวข้อง known Botnet Bot
13	ตรวจพบพฤติกรรม IP จากภายในพยายามติดต่อไปยัง IP กลุ่มเสี่ยงภายนอกด้วย DNS Communication with Malicious
14	ตรวจพบความผิดปกติที่คาดว่าเป็นพฤติกรรมของ Malware
15	ตรวจพบพฤติกรรมพยายามติดต่อไปยังIP/Domain ที่เกี่ยวข้องCobInt Backdoor
16	ตรวจพบพฤติกรรมพยายามติดต่อไปยังIP/Domain ที่เกี่ยวข้องEmotet Malware
17	ตรวจพบพฤติกรรมพยายามติดต่อไปยังIP/Domain ที่เกี่ยวข้องWanamineหรือ Crypto mining Activity
18	ตรวจพบพฤติกรรมพยายามการกระจาย Packet SMB ในปริมาณสูง
19	ตรวจพบพฤติกรรมจากหนึ่งแหล่งที่มาพยายามติดต่อในปริมาณสูงโดย Firewall อนุญาต
20	ตรวจพบพฤติกรรมจากหนึ่งแหล่งที่มาพยายามติดต่อในปริมาณสูงโดย Firewall ไม่อนุญาต
21	ตรวจพบพฤติกรรมพยายามติดต่อไปยัง IP/Domainที่เกี่ยวข้องSolarwind Supernova Backdoor

ลำดับที่	แสดงรายละเอียดคำอธิบายเหตุการณ์ต่อระดับความรุนแรง
22	ตรวจสอบพบการเผยแพร่ข้อมูลเกี่ยวข้องกับmail parliament ใน Web Site ที่ไม่ปลอดภัย (Dark Web) จากฐานข้อมูล Threat Intelligence
ความรุนแรงระดับปานกลาง (ระดับ 3)	
23	ตรวจพบพฤติกรรมพยายาม Scan หาข้อมูลระบบจาก IP ภายนอก
24	ตรวจพบพฤติกรรมพยายาม Scan หาข้อมูลระบบจาก IP ภายใน
25	ตรวจพบเหตุการณ์พยายาม Login Failed ระดับ User จำนวนหลายครั้ง
26	ตรวจพบพฤติกรรมที่คาดว่าไม่ใช่การทำงานที่ปกติ

3. ทีมรับมือและตอบสนองภัยคุกคาม CSIRT สำนักงานเลขาธิการสภาผู้แทนราษฎร

1. ผู้อำนวยการสำนักสารสนเทศ	ที่ปรึกษาทีม	
2. นายปกาสิต จำเรือง	หัวหน้าทีม	0926535556
3. นายสุธี ยืนแน่นอน	ผู้จัดการเหตุการณ์	0834470660
4. นางสมคิด แซ่ว่อง	สมาชิกทีม	0864716590
5. นายมุนินทร์ รัตนานุพงศ์	สมาชิกทีม	0891557893
6. นายธีรวุฒิ วงษ์วิจิตร	สมาชิกทีม	0867079077
7. นายวิษณุ แก้วประทุม	สมาชิกทีม	0813740501
8. นายจิรภัทร์ เต็มวุฒิโรจน์	สมาชิกทีม	0985845442
9. บริษัท โทรคมนาคมแห่งชาติ จำกัด	สมาชิกทีม	0838971720

4. ทีมรับมือและตอบสนองภัยคุกคาม CSIRT สำนักงานเลขาธิการวุฒิสภา

1. ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศและการสื่อสาร	ที่ปรึกษาทีม	
2. นายนรมิตร คุณโลยกะ	หัวหน้าทีม	0645364659
3. นายทวีศักดิ์ น้อยภาษี	ผู้จัดการเหตุการณ์	0853294040
4. นายประจักษ์ เพ็ญเลี้ยง	สมาชิกทีม	0896646272
5. นายสุวิทย์ น้อยอยู่	สมาชิกทีม	0894566661
6. นายรุ่งโรจน์ แสงธรรมชัย	สมาชิกทีม	0922460796
7. นายสมหวัง เรืองพรชัย	สมาชิกทีม	0971700112