องค์การตลาดเพื่อเกษตรกร
WWW.ORTORKOR.COM

# แผนรับมือเหตุภัยคุกคามทางไซเบอร์ องค์การตลาดเพื่อเกษตรกร พ.ศ. 2569 - 2570



**สารบัญ**


๑. หลักการและเหตุผล ๑

๒. วัตถุประสงค์ ๑

๓. ขอบเขต ๑

๔. หน้าที่การทบทวน ๑

๕. หน้าที่ในการดำเนินการตามแผน ๑

๖. รายละเอียดการบังคับใช้เอกสาร ๒

๖.๑ รายละเอียดของเอกสาร ๒

๖.๒ การเปลี่ยนแปลงเอกสาร ๒

๗. เอกสารและกรอบมาตรฐานที่เกี่ยวข้อง ๒

๘. นิยาม ๓

๙. บทบาทหน้าที่และโครงสร้างทีมรับมือเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ ๕

๙.๑ ผู้รับแจ้งเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ภายในหน่วยงาน ๕

๙.๒ โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ ๖

๙.๓ หน่วยงานภายนอกที่เกี่ยวข้อง ๘

๙.๔ โครงสร้างการรายงานเหตุการณ์ ๙

๑๐. ขั้นตอนการรับมือ ๑๐

๑๐.๑ ขั้นตอนการเตรียมการ ๑๑

๑๐.๒ ขั้นตอนการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ ๑๒

๑๐.๓ ขั้นตอนการระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ ๑๙

๑๐.๔ ขั้นตอนการดำเนินการภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ ๒๐

๑๐.๕ การจัดทำรายการตรวจสอบการจัดการเหตุการณ์ ๒๑

๑๑. การเตรียมความพร้อม ๒๑

๑๑.๑ การเตรียมพร้อมด้านฮาร์ดแวร์และซอฟต์แวร์ ๒๑

๑๑.๒ การเตรียมพร้อมแผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ๒๒

๑๑.๓ การเตรียมพร้อมด้านบุคลากร ๒๒
๑๑.๔ การเตรียมความพร้อมด้านการสำรองข้อมูลและระบบคอมพิวเตอร์สำรอง ๒๓

**ภาคผนวก**

ภาคผนวก ๑ ๒๕
ภาคผนวก ๒ ๒๗
ภาคผนวก ๓ ๒๘
ภาคผนวก ๔ ๒๙
ภาคผนวก ๕ ๓๐
ภาคผนวก ๖ ๓๗
แหล่งที่มา ๓๘

# แผนรับมือเหตุภัยคุกคามทางไซเบอร์องค์การตลาดเพื่อเกษตรกร

## ๑. หลักการและเหตุผล

แผนรับมือเหตุภัยคุกคามทางไซเบอร์ขององค์การตลาดเพื่อเกษตรกร ฉบับนี้จัดทำขึ้นเพื่อให้เป็นไปตามมาตรา ๔๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ ที่กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร็ว ซึ่งอย่างน้อยต้องประกอบด้วยเรื่องแผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยผู้ตรวจประเมิน ผู้ตรวจสอบภายใน หรือผู้ตรวจสอบอิสระจากภายนอกอย่างน้อยปีละหนึ่งครั้งและแผนการรับมือภัยคุกคามทางไซเบอร์ รวมทั้งเพื่อให้เป็นไปตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศองค์การตลาดเพื่อเกษตรกร ด้วย

## ๒. วัตถุประสงค์

เพื่อใช้เป็นแผนในการรับมือเหตุภัยคุกคามทางไซเบอร์ที่เกิดขึ้นในองค์การตลาดเพื่อเกษตรกร โดยจะเป็นการกำหนดหน้าที่และความรับผิดชอบให้กับหน่วยงานต่างๆ ภายใต้องค์การตลาดเพื่อเกษตรกร การกำหนดประเภทของเหตุภัยคุกคามทางไซเบอร์ การกำหนดความสัมพันธ์กับนโยบายและแนวปฏิบัติที่เกี่ยวข้องการรายงานเหตุภัยคุกคามทางไซเบอร์ และขั้นตอนการรับมือเหตุภัยคุกคามทางไซเบอร์ ตามขอบเขตของระบบสารสนเทศที่กำหนดไว้ รวมไปถึงการสื่อสารไปยังผู้มีส่วนได้ส่วนเสีย เพื่อลดผลกระทบที่อาจเกิดขึ้นต่อการดำเนินงานขององค์การตลาดเพื่อเกษตรกร

## ๓. ขอบเขต

แผนรับมือฯ ฉบับนี้ ใช้รับมือเหตุภัยคุกคามทางไซเบอร์ที่เกิดขึ้นต่อระบบสารสนเทศ และข้อมูลดิจิทัลขององค์การตลาดเพื่อเกษตรกร รวมถึงบุคคลหรืออุปกรณ์ใดๆ ซึ่งเข้าถึงระบบสารสนเทศ และข้อมูลดิจิทัลดังกล่าว

## ๔. หน้าที่การทบทวนแผน

กองเทคโนโลยีและสารสนเทศ มีหน้าที่ทบทวนและขออนุมัติแผนรับมือฯ ฉบับนี้ถึงผู้อำนวยการขององค์การตลาดเพื่อเกษตรกร หรือผู้ที่รับมอบอำนาจหน่วยงาน ได้แก่ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ระดับกรม (Department Chief Information Officer : DCIO)

## ๕. หน้าที่ในการดำเนินการตามแผน

กองเทคโนโลยีและสารสนเทศ (กส.) มีหน้าที่เป็นผู้รับผิดชอบหลักในการดำเนินการตามแผนรับมือฯ ฉบับนี้โดยมีหน่วยงานสนับสนุนประกอบด้วยหน่วยงานภายในองค์การตลาดเพื่อเกษตรกรทุกส่วนงาน รวมถึงหน่วยงานที่เป็นคู่สัญญา

**๖. รายละเอียดการบังคับใช้เอกสาร**

หน่วยงานจะต้องระบุรายละเอียดที่เกี่ยวข้องกับเอกสาร ดังต่อไปนี้

**๖.๑ รายละเอียดของเอกสาร (Document control and review)**

| **รายละเอียดของเอกสาร (Document control)** | |
|---|---|
| ผู้จัดทำเอกสาร (Author) | กองเทคโนโลยีและสารสนเทศ |
| ผู้ดำเนินการตามเอกสาร (Owner) | กองเทคโนโลยีและสารสนเทศ และส่วนงานอื่นๆที่เกี่ยวข้อง |
| วันที่จัดทำเอกสาร (Date created) | ๓๑ มกราคม ๒๕๖๘ |
| ผู้ตรวจสอบความถูกต้องของเอกสาร (Last reviewed by) | หัวหน้ากองเทคโนโลยีและสารสนเทศ |
| วันที่ตรวจสอบความถูกต้องของเอกสาร (Last date reviewed) | ๗ กุมภาพันธ์ ๒๕๖๙ |
| ผู้อนุมัติเอกสาร และวันที่อนุมัติเอกสาร (Endorsed by and date) | ผู้อำนวยการ อ.ต.ก. |
| วันที่จะต้องมีการตรวจสอบเอกสารครั้งถัดไป (Next review due date) | ปีงบประมาณ ๒๕๗๐ |

**๖.๒ การเปลี่ยนแปลงเอกสาร (Version control)**

| รุ่น (Version) | วันที่อนุมัติ (Date of Approval) | ผู้อนุมัติ (Approved by) | สถานะ (Description of change) |
|---|---|---|---|
| ๑.๐ | ปี ๒๕๖๘ | ผู้อำนวยการ อ.ต.ก. | ยกเลิก |
| ๒.๐ | ปี ๒๕๖๙ | ผู้อำนวยการ อ.ต.ก. | ใช้งานอยู่ |

**๗. เอกสารและกรอบมาตรฐานที่เกี่ยวข้อง**

๑) นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ องค์การตลาดเพื่อเกษตรกร
๒) นโยบายคุ้มครองข้อมูลส่วนบุคคล (Personal Data Privacy Policy) องค์การตลาดเพื่อเกษตรกร
๓) แผนบริหารความต่อเนื่องทางธุรกิจด้านเทคโนโลยีสารสนเทศ องค์การตลาดเพื่อเกษตรกร
๔) แผนบริหารความต่อเนื่องทางธุรกิจ องค์การตลาดเพื่อเกษตรกร

**๘. นิยาม**

**เหตุการณ์ (Event)** หมายความว่า เหตุการณ์ที่เกิดขึ้นจากการเฝ้าระวังสังเกตการณ์ (observable occurrence) ในระบบเครือข่าย สภาพแวดล้อม กระบวนการ ลำดับการดำเนินการ หรือบุคลากร เหตุการณ์อาจมีหรือไม่มีลักษณะที่ส่งผลเชิงลบก็ได้

**เหตุภัยคุกคามทางไซเบอร์ (Cyber incident)** หมายความว่า เหตุการณ์ที่มีผลเชิงลบที่เกิดจากการกระทำหรือการดำเนินการใด ๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์ โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

**ภัยคุกคามทางไซเบอร์ (Cyber threat)** หมายความว่า การกระทำหรือการดำเนินการใด ๆ โดยมิชอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์ โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

**เหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญ**[1] หมายความว่า เหตุภัยคุกคามทางไซเบอร์ที่ปรากฏต่อระบบสารสนเทศ และเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามมาตรา ๔๙ ซึ่งคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติได้กำหนดลักษณะของภัยคุกคามทางไซเบอร์ไว้ตามมาตรา ๖๐ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒

**แพตช์** หมายถึง โปรแกรมที่ใช้ในการปรับปรุงแก้ไขซอฟต์แวร์ โดยส่วนใหญ่จะอยู่ในลักษณะของไฟล์และใช้เพื่อแก้ไขช่องโหว่เรื่องความมั่นคงปลอดภัย หรือเพื่อเพิ่มความสามารถของซอฟต์แวร์ ผู้พัฒนาซอฟต์แวร์หลายรายได้เผยแพร่แพตช์ออกมาเป็นระยะ เช่น บริษัท Microsoft จะเผยแพร่แพตช์ที่แก้ไขช่องโหว่ของซอฟต์แวร์ผ่านระบบ Windows Update

**รูปแบบภัยคุกคามไซเบอร์** หมายถึง รูปแบบของการกระทำหรือการดำเนินการใด ๆ โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลของบุคคลหรือหน่วยงาน แบ่งเป็น

- ซอฟต์แวร์ประสงค์ร้าย (Malicious Software) หรือที่เรียกโดยทั่วไปว่ามัลแวร์ (Malware) เป็นโปรแกรมที่มีการทำงานที่มุ่งประสงค์ร้ายต่อคอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์

- ไวรัสคอมพิวเตอร์ (Computer Virus) เป็นมัลแวร์ชนิดหนึ่งที่สามารถคัดลอกตัวเอง ติดตั้งตัวเองในเครื่องคอมพิวเตอร์อื่น ๆ โดยที่เจ้าของเครื่องคอมพิวเตอร์ไม่อนุญาต ไวรัสคอมพิวเตอร์สามารถแพร่กระจายตัวเองไปสู่เครื่องคอมพิวเตอร์เครื่องอื่น ๆ โดยใช้พาหะ เช่น แฟลชไดรว์ติดไวรัส หรือไฟล์คอมพิวเตอร์ติดไวรัส เป็นต้น

- หนอนคอมพิวเตอร์ (Computer worm) เป็นมัลแวร์ชนิดหนึ่งที่สามารถคัดลอกตัวเอง ติดตั้งตัวเองในเครื่องคอมพิวเตอร์อื่น ๆ โดยที่เจ้าของเครื่องคอมพิวเตอร์ไม่อนุญาต หนอนคอมพิวเตอร์จะต่างกับไวรัสตรงที่ไวรัสจะ

[1] เหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญ มีนิยามตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ.๒๕๖๖

แพร่กระจายตัวเองไปสู่คอมพิวเตอร์เครื่องอื่น ๆ โดยอาศัยพาหะ แต่หนอนคอมพิวเตอร์จะใช้วิธีสแกนเครื่องคอมพิวเตอร์ที่อยู่ในระบบเครือข่ายและตรวจหาช่องโหว่ของระบบปฏิบัติการหรือช่องโหว่ของแอปพลิเคชัน จากนั้นจึงทำการคัดลอกตัวเองเข้าไปฝังโดยใช้ช่องโหว่ดังกล่าว

- ม้าโทรจัน (Trojan horse) เป็นมัลแวร์ชนิดหนึ่งที่มีจุดประสงค์เพื่อบุกรุก เข้าถึงและควบคุมเครื่องคอมพิวเตอร์จากระยะไกล ดำเนินการเปลี่ยนแปลง ทำลายไฟล์ข้อมูลสำคัญ หรือทำการคัดลอกข้อมูลดังกล่าวส่งให้แก่ผู้คุกคามผ่านระบบเครือข่ายอินเทอร์เน็ต ซึ่งข้อมูลสำคัญที่ผู้คุกคามต้องการอาจเป็น ชื่อผู้ใช้ รหัสผ่าน เลขที่บัญชีธนาคาร และข้อมูลส่วนบุคคลอื่น ๆ ลักษณะของการติดตั้งม้าโทรจันจะเหมือนกับไวรัสคอมพิวเตอร์คืออาศัยพาหะซึ่งอาจมาจากแฟลชไดรว์หรือทางอีเมล์

- สปายแวร์ (Spyware) เป็นมัลแวร์ชนิดหนึ่ง ที่มีวัตถุประสงค์เพื่อบันทึกการกระทำของผู้ใช้บนเครื่องคอมพิวเตอร์และส่งผ่านอินเทอร์เน็ตโดยที่ผู้ใช้ไม่ได้รับทราบ โปรแกรมแอบดัก ข้อมูลนั้นสามารถรวบรวมข้อมูล สถิติการใช้งานจากผู้ใช้ได้หลายอย่างขึ้นอยู่กับการออกแบบของโปรแกรม

- ซอฟต์แวร์เรียกค่าไถ่ (Ransomware) เป็นมัลแวร์ชนิดหนึ่งที่มีพฤติกรรมเข้ารหัสไฟล์ต่าง ๆ ที่อยู่บนเครื่องคอมพิวเตอร์ไม่ว่าจะเป็นไฟล์เอกสาร รูปภาพ วิดีโอ ผู้ใช้งานจะไม่สามารถเปิดไฟล์ใด ๆ ได้เลยหากไฟล์เหล่านั้นถูกเข้ารหัส ซึ่งการถูกเข้ารหัสก็หมายความว่าจะต้องใช้คีย์ในการปลอดล็อคเพื่อกู้ข้อมูลคืนมาโดยผู้ใช้งานจะต้องทำการจ่ายเงินตามข้อความ “เรียกค่าไถ่” ที่ปรากฏ

- Backdoor เป็นช่องทางพิเศษที่ใช้เข้าถึงระบบหรือเครื่องคอมพิวเตอร์โดยที่ไม่ต้องผ่านการพิสูจน์ตัวตน ซึ่งส่วนใหญ่เมื่อผู้บุกรุกสามารถเจาะเข้าระบบได้แล้ว ก็จะสร้างประตูหลังเอาไว้เพื่อใช้ในการบุกรุกเข้าสู่ระบบหรือเครื่องคอมพิวเตอร์ในภายหลัง

- Rootkit เป็นโปรแกรมที่ถูกพัฒนาขึ้นมาเพื่อควบคุมระบบหรือขโมยข้อมูลที่อยู่ในระบบคอมพิวเตอร์ ทั้งนี้นอกจากใช้สำหรับบุกรุกเข้าสู่ระบบงานแล้ว Rootkit ยังอาจใช้เพื่อดูแลหรือตรวจสอบระบบคอมพิวเตอร์ได้ด้วย

- การโจมตีแบบ DoS/DDoS มีจุดประสงค์เพื่อทำให้เครื่องคอมพิวเตอร์แม่ข่าย (Server) หยุดทำงาน หากเครื่องคอมพิวเตอร์ที่โจมตีมีเครื่องเดียว เรียกว่าการโจมตีแบบ Denial of Service (DoS) แต่หากมีเครื่องคอมพิวเตอร์ที่โจมตีมากกว่า ๑ เครื่องและทำการโจมตีพร้อม ๆ กัน ไม่ว่าจะโดยตั้งใจหรือไม่ตั้งใจก็ตาม จะเรียกว่าการโจมตีแบบ Distributed Denial of Service (DDoS)

- Botnet เป็นกลุ่มของอุปกรณ์ที่ติดมัลแวร์และถูกเปลี่ยนเป็น Bot (ย่อมาจาก Robot) ไม่ว่าจะเป็นอุปกรณ์คอมพิวเตอร์ เว็บแคม เราท์เตอร์ หรืออุปกรณ์อื่นๆ เพื่อรอรับสั่งจากผู้บุกรุกโดยผู้บุกรุกจะนำ Botnet ที่มีไปใช้ในการโจมตีขนาดใหญ่ เช่นการทำ DDoS เป็นต้น

- Spam Mail หรืออีเมล์ขยะ เป็นขยะออนไลน์ที่ส่งตรงถึงผู้รับ โดยที่ผู้รับนั้นไม่ต้องการและสร้างความเดือดร้อนรำคาญให้กับผู้รับได้ในลักษณะของการโฆษณาสินค้าหรือบริการ การชักชวนเข้าไปยังเว็บไซต์ต่าง ๆ ซึ่งอาจมีภัยคุกคามชนิด Phishing แฝงเข้ามาด้วย ด้วยเหตุนี้จึงควรติดตั้งระบบ Anti Spam หรือหากใช้ฟรีอีเมล์ก็ควรมีโปรแกรมคัดกรองอีเมล์ขยะในชั้นหนึ่งแล้ว

- Phishing คือการหลอกลวงทางอินเทอร์เน็ตเพื่อขอข้อมูลที่สำคัญ เช่น รหัสผ่าน หรือหมายเลขบัตรเครดิต โดยการส่งข้อความผ่านทางอีเมล์หรือเมสเซนเจอร์ ตัวอย่างของการ Phishing เช่น การบอกแก่ผู้รับปลายทางว่าเป็นธนาคารหรือบริษัทที่น่าเชื่อถือ และแจ้งว่ามีสาเหตุทำให้คุณต้องเข้าสู่ระบบและใส่ข้อมูลที่สำคัญใหม่ โดยเว็บไซต์ที่ลิงก์ไปนั้นจะมีหน้าตาคล้ายคลึงกับเว็บที่กล่าวถึง Phishing

- Sniffing เป็นการดักข้อมูลที่ส่งจากคอมพิวเตอร์เครื่องหนึ่งไปยังอีกเครื่องหนึ่ง หรือจากเครือข่ายหนึ่งไปยังอีกเครือข่ายหนึ่ง เป็นวิธีการหนึ่งที่ผู้บุกรุกนิยมใช้

- Hacking เป็นการเจาะระบบเครือข่ายคอมพิวเตอร์ไม่ว่าจะกระทำด้วยมนุษย์หรืออาศัยโปรแกรมด้วยวัตถุประสงค์ต่าง ๆ กัน โดยทั่วไปแล้วการ Hacking เป็นสิ่งผิดกฎหมาย เว้นแต่หากได้รับอนุญาตจากเจ้าของเครื่องคอมพิวเตอร์หรือระบบ โดยตัวอย่างของการ Hacking อย่างถูกกฎหมาย เช่น การเจาะระบบ เพื่อประเมินความเสี่ยงของระบบคอมพิวเตอร์ และทดสอบระบบการรักษาความปลอดภัยเครือข่ายขององค์กร

- ผู้บุกรุก (Hacker) หมายถึง ผู้ที่ไม่ได้รับอนุญาตในการใช้งานระบบหรือเครื่องคอมพิวเตอร์แต่พยายามลักลอบเข้ามาใช้งานด้วยวัตถุประสงค์ต่าง ๆ เช่น การโจรกรรมข้อมูล แสวงหาผลกำไร หรือเพื่อความสนุกส่วนตัว

- Social Engineering หมายถึง การหลอกลวง ล่อหลอกผู้อื่น ใช้หลักการพื้นฐานทางจิตวิทยาให้เหยื่อเปิดเผยข้อมูล เพื่อให้ได้ผลประโยชน์ตามที่แฮกเกอร์ต้องการ โดยอาศัยจุดอ่อน ความรู้เท่าไม่ถึงการณ์ ความไม่รู้ ความประมาทของผู้ใช้งานระบบคอมพิวเตอร์

- Password Attack หมายถึง การโจมตีที่ผู้บุกรุกพยายามคาดเดา หรือทำให้ได้มาซึ่งรหัสผ่านของผู้ใช้คนใดคนหนึ่ง สำหรับนำไปโจมตีระบบคอมพิวเตอร์

- Insider Treats หมายถึง ภัยคุกคามทางไซเบอร์ที่เกิดจากบุคคลภายในองค์กร แบ่งออกเป็น ๓ ประเภท คือ ภัยที่เกิดจากการประมาทโดยไม่ได้ตั้งใจของบุคลากร ภัยที่เกิดจากการขโมยตัวตนหรือข้อมูลบุคลากรที่ทำให้แฮกเกอร์สามารถเจาะเข้าระบบได้และภัยจากตัวบุคลากรเองที่ต้องการจะบ่อนทำลายองค์กรจากภายใน

- SQL Injection หมายถึง การโจมตีที่ระบบฐานข้อมูลของระบบผ่านช่องโหว่ของ SQL ส่งผลให้ระบบฐานข้อมูลถูกขโมย หรือถูกทำลาย หรือแก้ไขให้เกิดความเสียหายได้

- Form Jacking หมายถึง ภัยคุกคามทางไซเบอร์ที่เกิดจากผู้ไม่ประสงค์ดีสร้างโค้ดแปลกปลอมไว้บนเว็บไซต์ต่างๆ เพื่อหลอกลวงเป้าหมาย โดยมจุดประสงค์ในการเข้าถึงระบบสารสนเทศและข้อมูลเพื่อก่ออาชญากรรม

**๙. บทบาทหน้าที่และโครงสร้างทีมรับมือเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์**

**<u>๙.๑ ผู้รับแจ้งเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ภายในหน่วยงาน</u>**

| ลำดับ | ชื่อ – นามสกุล | ระยะเวลาในการปฏิบัติงาน | ช่องทางการติดต่อสื่อสาร | หน้าที่ | ความรับผิดชอบ |
|---|---|---|---|---|---|
| ๑ | นายวีรวัฒน์ สุวพจน์ | ๕x๘ | ๐๙๘-๐๙๐-๗๘๙๔ | ผู้ประสานงาน | รับแจ้งเหตุ |
| ๒ | นายภานุรุจ จามะรีย์ | ๕x๘ | ๐๘๐-๐๖๔-๐๕๙๓ | ผู้ประสานงาน | รับแจ้งเหตุ |

**๙.๒ โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber incident Response Team : CIRT)**

องค์การตลาดเพื่อเกษตรกรใช้โมเดลโครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ในลักษณะแบบรวมศูนย์ (รายละเอียดโครงสร้างทีมดังภาคผนวก ๑) ประกอบด้วย

| ลำดับ | ชื่อ - นามสกุล | ช่องทางการติดต่อสื่อสาร | หน้าที่ | ความรับผิดชอบ |
|---|---|---|---|---|
| ๑ | นายโชติเชาว์ ปาลคำ | เบอร์โทรศัพท์ภายใน : ๐๒-๒๗๙-๒๐๘๐-๙ ต่อ ๒๐๕<br>เบอร์โทรศัพท์มือถือ : ๐๙๒-๙๘๖-๘๔๔๕<br>Email : choatchaw.p@mof.or.th | หัวหน้าทีมรับมือฯ (Team manager) | ทำหน้าที่สื่อสารกับผู้บริหารของหน่วยงาน |
| ๒ | นายปรเมษฐ์ เจริญสุข | เบอร์โทรศัพท์ภายใน : ๐๒-๒๗๙-๒๐๘๐-๙ ต่อ ๒๐๗<br>เบอร์โทรศัพท์มือถือ : ๐๘๔-๑๐๙-๑๙๑๒<br>Email : proramez.c@mof.or.th | รองหัวหน้าทีมรับมือฯ (Deputy team manager) | ทำหน้าที่แทนกรณีหัวหน้าทีมรับมือฯ ไม่อยู่/ไม่สามารถปฏิบัติงานได้ |
| ๓ | นายเพชราวุธ ละเอียดอ่อน | เบอร์โทรศัพท์ภายใน : ๐๒-๒๗๙-๒๐๘๐-๙ ต่อ ๒๐๖<br>เบอร์โทรศัพท์มือถือ : ๐๙๒-๕๒๐-๙๐๐๙<br>Email : petcharawut.l@mof.or.th | เจ้าหน้าที่รับมือฯ (Incident leader) | ทำหน้าที่ช่วยเหลือให้สามารถควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์ได้ |
| ๔ | นายวีรวัฒน์ สุวพจน์ | เบอร์โทรศัพท์ภายใน : ๐๒-๒๗๙-๒๐๘๐-๙ ต่อ ๒๐๖<br>เบอร์โทรศัพท์มือถือ : ๐๘๐-๓๐๓-๙๔๔๙<br>Email : weerawat.s@mof.or.th | เจ้าหน้าที่เทคนิคฯ (Technical lead) | ทำหน้าที่ให้ความเห็นเกี่ยวกับแนวทางที่เหมาะสมในการควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์ |
| ๕ | นายภาณุรุจ จามะรีย์ | เบอร์โทรศัพท์ภายใน : ๐๒-๒๗๙-๒๐๘๐-๙ ต่อ ๒๐๗<br>เบอร์โทรศัพท์มือถือ : ๐๘๐-๐๖๔-๐๕๙๓<br>Email : phanurut.c @mof.or.th | เจ้าหน้าที่เทคนิคฯ (Technical lead) | ทำหน้าที่ให้ความเห็นเกี่ยวกับแนวทางที่เหมาะสมในการควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์ |

ทั้งนี้ นอกจากทีมรับมือฯ ดังกล่าวข้างต้น ให้มีบุคคลดังต่อไปนี้ทำหน้าที่สนับสนุนการดำเนินการของแผนรับมือฯ ฉบับนี้ ดังนี้

| ลำดับ | ชื่อ - นามสกุล | ช่องทางการติดต่อสื่อสาร | หน้าที่ | ความรับผิดชอบ |
|---|---|---|---|---|
| ๑ | นายโชติเชาว์<br>ปาลคำ | เบอร์โทรศัพท์ภายใน : ๐๒-๒๗๙-๒๐๘๐-๙ ต่อ ๒๐๕<br>เบอร์โทรศัพท์มือถือ : ๐๙๒-๙๘๖-๘๔๔๕<br>Email : choatchaw.p@mof.or.th | หัวหน้ากองเทคโนโลยีและสารสนเทศ | ทำหน้าที่ควบคุมผลกระทบจากภัยคุกคาม |
| ๒ | นางดวงรัตน์<br>รูปสม | เบอร์โทรศัพท์ภายใน : ๐๒-๒๗๙-๒๐๘๐-๙ ต่อ ๔๐๐<br>เบอร์โทรศัพท์มือถือ : -<br>Email : duangrata.r@mof.or.th | ผู้ตรวจสอบภายใน | ทำหน้าที่ตรวจสอบความมั่นคงปลอดภัยไซเบอร์ |
| ๓ | นางวริศรา<br>อจลานนท์ | เบอร์โทรศัพท์ภายใน : ๐๒-๒๗๙-๒๐๘๐-๙ ต่อ ๕๑๐<br>เบอร์โทรศัพท์มือถือ : -<br>Email : - | ผู้เชี่ยวชาญด้านกฎหมาย | ทำหน้าที่เป็นที่ปรึกษาด้านกฎหมายที่เกี่ยวข้อง |
| ๔ | นางศิริลักษณ์<br>นุ่นแป้น | เบอร์โทรศัพท์ภายใน : ๐๒-๒๗๙-๒๐๘๐-๙ ต่อ ๒๐๘<br>เบอร์โทรศัพท์มือถือ : -<br>Email : - | ผู้บริหารจัดการความเสี่ยง | ทำหน้าที่ประเมินผลกระทบ-ความเสี่ยงเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ |
| ๕ | นางสาวศิรดา<br>กานตรัตน์ | เบอร์โทรศัพท์ภายใน : ๐๒-๒๗๙-๒๐๘๐-๙ ต่อ ๑๒๑<br>เบอร์โทรศัพท์มือถือ : ๐๙๒-๔๖๕-๑๔๐๙<br>Email : - | ผู้รับผิดชอบด้านสื่อสารองค์กร | ประชาสัมพันธ์ไปยังผู้มีส่วนได้ส่วนเสียเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ |

**๙.๓ หน่วยงานภายนอกที่เกี่ยวข้อง**

| ลำดับ | ชื่อ - นามสกุล | ช่องทางการติดต่อสื่อสาร | หน่วยงาน | ความเกี่ยวข้อง |
|---|---|---|---|---|
| ๑ | เจ้าหน้าที่ สกมช. | เบอร์โทรศัพท์ :๐๒-๑๑๔-๓๕๓๑ Email : thaicert@ncsa.or.th ที่อยู่สำนักงาน : ๑๒๐ หมู่ ๓ อาคารรัฐประศาสนภักดี (อาคารบี) ชั้น ๗ ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา ๕ ธันวาคม ๒๕๕๐ ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ ๑๐๒๑๐ | สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) | หน่วยงานรับแจ้งเหตุภัยคุกคามไซเบอร์ |
| ๒ | เจ้าหน้าที่ สดช. | เบอร์โทรศัพท์ :๐๒-๐๒๔-๑๙๙๙ Email : - helpdesk@gdcc.onde.go.th ที่อยู่สำนักงาน : ๑๒๐ หมู่ ๓ ชั้น ๖-๙ อาคารรัฐประศาสนภักดี ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา ๕ ธันวาคม ๒๕๕๐ ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพ ๑๐๒๑๐ | สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ (สดช.) | หน่วยงานให้บริการคลาวด์ภาครัฐ (GDCC) |
| ๓ | เจ้าหน้าที่ สพร. | เบอร์โทรศัพท์ :๐๒-๖๑๒-๖๐๖๐ Email : - ที่อยู่สำนักงาน : ชั้น ๑๗ อาคารบางกอกไทย ทาวเวอร์ ๑๐๘ ถนน รางน้ำ แขวงถนนพญาไท เขตราชเทวี กทม. ๑๐๔๐๐ | สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.) | ให้บริการคลาวด์กลางภาครัฐ (GDCC) |
| ๔ | ตัวแทน หน่วยงาน | เบอร์โทรศัพท์ : ๐๘๕-๙๓๓-๖๖๖๙ Email : - ที่อยู่สำนักงาน : ซอยประชาอุทิศ ๔ แขวงดอนเมือง เขตดอนเมือง กทม. ๑๐๒๑๐ | บริษัท เน็ตเวิร์ค ซีสเต็ม อินเตอร์กรุ๊ป จำกัด | เป็นผู้ดูแลอุปกรณ์ป้องกันเครือข่าย (Firewall) |

| | | | | |
|---|---|---|---|---|
| ๕ | ตัวแทน<br>หน่วยงาน | เบอร์โทรศัพท์ :๐๒-๑๗๕-๕๕๕๕<br>Email : -<br>ที่อยู่สำนักงาน : ๖๒ ซอยอุดมสุข ๖๐ (แยก ๑) แขวงหนองบอน เขตประเวศ กทม. ๑๐๒๕๐ | บริษัท เจนเนซิส ไฮเทค จำกัด | เป็นผู้ให้บริการลิขสิทธิ์ Anti-virus |
| ๖ | ตัวแทน<br>หน่วยงาน | เบอร์โทรศัพท์ : ๐๙๔-๖๖๙-๔๙๓๙<br>Email : -<br>ที่อยู่สำนักงาน : ๖๖๗/๑๕ อาคารอรรถบูรณ์ ชั้นที่ ๕ ห้องเลขที่ ๕๐๒/๓ ถนนจรัญสนิทวงศ์ แขวงอรุณอมรินท์ เขตบางกอกน้อย กทม. ๑๐๗๐๐ | บริษัท วีทูเอ็น ดีเวลลอปเปอร์ จำกัด | เป็นผู้พัฒนาและดูแลระบบชำระเงินทางอิเล็กทรอนิกส์ (e-Payment) และระบบบริหารจัดการแผนงานงบประมาณ |
| ๗ | ตัวแทน<br>หน่วยงาน | เบอร์โทรศัพท์ : ๐๙๓-๘๘๑-๐๘๘๗<br>Email : -<br>ที่อยู่สำนักงาน : ๑๔๒/๑๔๕ ซอยลาดพร้าว ๑๐๒ (เปี่ยมจันทร์) แขวงพลับพลา เขตวังทองหลาง กทม. ๑๐๓๐๐ | บริษัท นิวไดซ์ จำกัด (สำนักงานใหญ่) | เป็นผู้พัฒนาและดูแลระบบโครงสร้างองค์กรและการบริหารจัดการบุคลากร |
| ๘ | ตัวแทน<br>หน่วยงาน | เบอร์โทรศัพท์ : ๐๘๑-๖๑๕-๖๕๓๕<br>Email : -<br>ที่อยู่สำนักงาน : ๒๙ ซอยราม อินทรา ๑๐๑ แขวง/เขตคันนายาว กทม. ๑๐๒๓๐ | บริษัท สุดสุดดีไซน์ จำกัด (สำนักงานใหญ่) | เป็นผู้ดูแลระบบบริหารจัดการศูนย์แสดงสินค้าผลิตภัณฑ์เกษตรคุณภาพสูง |

**<u>๙.๔ โครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure)</u>**

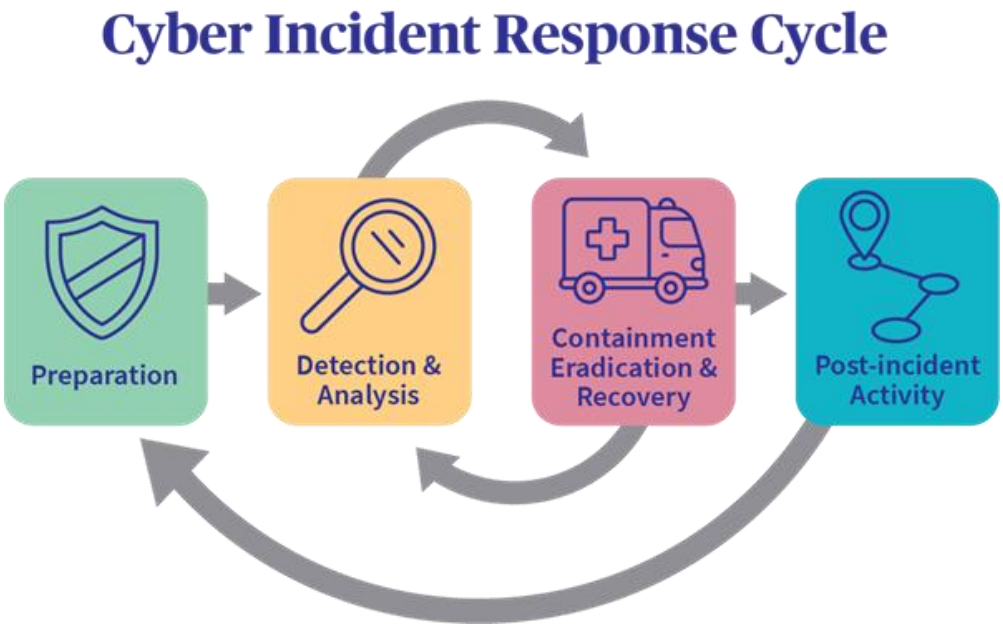
รายละเอียดของขั้นตอนการปฏิบัติเพื่อรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์มีดังนี้

| ขั้นตอน | ผู้รับผิดชอบ |
|---|---|
| ๑. การแจ้งเหตุ | ผู้พบเห็น/ผู้ที่ได้รับผลกระทบจาก incident |
| ๒. ขั้นการเตรียมการ (Preparation)<br>๒.๑ นโยบายหรือแนวปฏิบัติที่เกี่ยวข้อง<br>๒.๒ จัดเตรียมทรัพยากรที่ใช้ในการดำเนินงาน<br>๒.๓ เตรียมการป้องกันและแจ้งเตือน<br>๒.๔ เตรียมรายละเอียดช่องทางการ ติดต่อสื่อสาร<br>๒.๕ การให้ความรู้ และวิธีปฏิบัติ<br>๒.๖ ทดสอบการตอบสนองต่อภัยคุกคามทางไซเบอร์ | ทีมรับมือและตอบสนองต่อ incident และเจ้าของระบบฯ |

| | |
|---|---|
| ๓. ขั้นการตรวจจับและวิเคราะห์ภัยคุกคาม (Detection & Analysis)<br>๓.๑ รับแจ้งเหตุ<br>๓.๒ วิเคราะห์ความผิดปกติเมื่อได้รับแจ้ง<br>๓.๓ บันทึกข้อมูลเหตุการณ์ภัยคุกคาม<br>๓.๔ จัดลำดับความสำคัญของ incident<br>๓.๕ ติดต่อประสานงานกับหน่วยงานภายใน และภายนอก | ผู้รับแจ้งเหตุ ทีมเฝ้าระวังและวิเคราะห์การแจ้งเตือนภัยคุกคามจากอุปกรณ์ตรวจจับ ผู้รับแจ้งเหตุ ทีมรับมือและตอบสนองต่อ incident ทีมรับมือและตอบสนองต่อ incident |
| ๔. การระงับภัยคุกคามทางไซเบอร์ (Containment)<br>๔.๑ ควบคุมความเสียหาย<br>๔.๒ จัดเก็บและดูแลหลักฐานทางดิจิทัล | ทีมรับมือและตอบสนองต่อ incident |
| ๕. การปราบปรามภัยคุกคามทางไซเบอร์และการฟื้นฟู (Eradication & Recovery)<br>๕.๑ แก้ไขสาเหตุ และผลกระทบจากการโจมตี<br>๕.๒ กู้คืนระบบ ข้อมูล และภาพลักษณ์จากความเสียหาย | ทีมรับมือและตอบสนองต่อ incident |
| ๖. การดำเนินการภายหลังการแก้ปัญหาภัยคุกคาม (Post-incident)<br>๖.๑ เก็บรักษาหลักฐานและบันทึกการดำเนินงาน<br>๖.๒ ปรับปรุงและพัฒนากระบวนการ กลไก แนวปฏิบัติในการรับมือ | ทีมรับมือและตอบสนองต่อ incident |

**๑๐. ขั้นตอนการรับมือ**

แผนรับมือฯ ฉบับนี้ ประกอบด้วยขั้นตอนการรับมือเหตุภัยคุกคามทางไซเบอร์ตามข้อ ๑๙.๑ ในประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔, ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ.๒๕๖๔ และประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ. ๒๕๖๖ รวมถึงนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ องค์การตลาดเพื่อเกษตรกร ดังนี้




**๑๐.๑ ขั้นตอนการเตรียมการ (preparation)**

อ.ต.ก. มีมาตรการเพื่อเตรียมการและป้องกันการเกิดภัยคุกคามทางไซเบอร์ (preparation) เป็นสิ่งที่จะต้องทำในระยะเริ่มต้น เพื่อเตรียมความพร้อมเมื่อต้องเผชิญเหตุ ได้แก่ การจัดเตรียมข้อมูลให้พร้อม การจัดตั้งและฝึกอบรมบุคลากรหรือทีมงาน การจัดหาเครื่องมือและทรัพยากรต่าง ๆ ที่จำเป็น การตั้งค่าระบบต่าง ๆ ให้ปลอดภัย การจัดทำนโยบาย แผนงาน และกระบวนการที่เกี่ยวข้อง รวมถึงการสร้างเครือข่ายความร่วมมือ โดยดำเนินการดังต่อไปนี้

๑) กำหนดโครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT) รายละเอียดปรากฏตามข้อ ๙.๒

๒) กำหนดโครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure) รายละเอียดปรากฏตามข้อ ๙.๔

๓) กำหนดเกณฑ์และขั้นตอนในการเรียกใช้งาน (Activate) การตอบสนองต่อเหตุการณ์ และ CIRT

๔) จัดเตรียมข้อมูลและอุปกรณ์ รวมถึงช่องทางในการติดต่อสื่อสารที่จำเป็น เช่น ข้อมูลการติดต่อและอุปรกรณ์ติดต่อสื่อสารของบุคลากร, กลไกรายงานเหตุการณ์, ห้องประชุม War room เป็นต้น

๕) จัดเตรียมอุปกรณ์, ซอฟต์แวร์ และแหล่งข้อมูลสำหรับวิเคราะห์เหตุภัยคุกคามทางไซเบอร์

๖) จัดให้มีการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน (Risk Assessment)

๗) จัดทำแผนผังโครงสร้างขั้นตอนการรับมือฯ ของหน่วยงาน โดยหน่วยงานอาจดูตัวอย่างการจัดทำแผนผังโครงสร้างขั้นตอนการรับมือฯ ได้ (รายละเอียดปรากฏตามภาคผนวก ๒)

## ๑๐.๒ ขั้นตอนการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (Detection and Analysis)

เป็นการดำเนินการในการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (detection and analysis) ซึ่งเป็นสิ่งจำเป็นที่จะช่วยให้ อ.ต.ก. สามารถบรรเทาความเสี่ยงที่ยังคงเหลืออยู่ และสามารถแจ้งเตือนได้อย่างทันท่วงทีเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น ประกอบด้วยการดำเนินการตามเอกสารแนบท้าย ๒ ตารางที่ ๒.๒ ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔

แม้ว่า อ.ต.ก. จะจัดให้มีมาตรการต่าง ๆ เพื่อป้องกันหรือควบคุมมิให้เกิดภัยคุกคามทางไซเบอร์ขึ้นแล้วก็ตาม แต่ อ.ต.ก. ก็ยังคงต้องเตรียมความพร้อมอยู่เสมอเพื่อรับมือกับสถานการณ์ภัยคุกคามทางไซเบอร์ที่ไม่อาจหลีกเลี่ยงได้ การดำเนินมาตรการในการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (Detection and Analysis) จึงเป็นสิ่งจำเป็นที่จะช่วยให้ อ.ต.ก. สามารถบรรเทาความเสี่ยงที่ยังคงเหลืออยู่ และสามารถแจ้งเตือนได้อย่างทันทวงทีเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น

### ๑๐.๒.๑ การกำหนดวิธีการที่จะใช้ในการตรวจจับ incident

การตรวจจับ incident จะขึ้นอยู่กับระบบงานที่ใช้อยู่ รูปแบบของความพยายามโจมตี และกลไกในการปกป้องระบบ เพราะระบบการป้องกันจะแจ้งเตือน (Alert) หรือเก็บบันทึกข้อมูล (Log) เพื่อใช้ในการวิเคราะห์หาความผิดปกติ และมีการปรับ Fine Tune เพื่อให้มีความเหมาะสมกับสภาพการใช้งานของระบบ ลักษณะของข้อมูลแจ้งเตือนที่ใช้ในการตรวจจับแบ่งได้เป็น ๒ ประเภท

- Precursor เป็นข้อมูลบ่งบอกว่า incident จะเกิดขึ้นในอนาคต
- Indicator เป็นข้อมูลบ่งบอกว่า incident ได้เคยเกิดขึ้นหรือกำลังเกิดขึ้นอยู่

อุปกรณ์ที่ใช้เพื่อการป้องกันและตรวจจับต้องพิจารณาตามความเหมาะสมกับระบบที่ต้องการป้องกัน และต้องทำการปรับ Fine Tune เพื่อให้มีความเหมาะสมกับสภาพการใช้งานของระบบนั้น ๆ ซึ่งข้อมูลการแจ้งเตือนเพื่อตรวจจับการบุกรุกระบบคอมพิวเตอร์และเครือข่ายมีดังนี้

๑๐.๒.๑.๑ ประเภท Alert

๑) IPS ระบบที่ทำหน้าที่ตรวจจับและป้องกันการโจมตีในระบบเครือข่าย มีการแจ้งเตือนเมื่อพบสิ่งที่ตรงกับวิธีการโจมตีที่ระบบรู้จัก

๒) SIEM ระบบตรวจจับความผิดปกติโดยใช้ข้อมูล Log จากระบบอื่น ๆ เพื่อนำมาวิเคราะห์ โดยต้องตั้งค่า Rule set โดยผู้เชี่ยวชาญ และเหมาะสมกับสภาพแวดล้อมที่เชื่อมต่ออยู่กับ SIEM

๓) Anti-Malware ทำหน้าที่ตรวจจับโปรแกรมประสงค์ร้าย ทำงานทั้งในระดับเครือข่าย และ Host การตรวจเจอ Malware ในระบบเป็นข้อบ่งชี้ได้ทั้งที่กำลังพยายามโจมตีและการโจมตีได้สำเร็จแล้ว

๔) Third-Party บริการสอดส่องดูแลความผิดปกติที่เกิดขึ้นกับระบบ หรือระบบของหน่วยงาน ถูกนำไปโจมตีระบบอื่น ๆ ภายนอกองค์กรซึ่งบ่งบอกได้ว่าระบบภายในหน่วยงานได้ถูกยึดครองโดยผู้ไม่ประสงค์ดี และนำไปใช้สร้างความเสียหาย

๑๐.๒.๑.๒ ประเภท Log

๑) Operating System and Application Log ข้อมูลจาก Log ของ OS และ Application ที่ประกอบไปด้วยการบันทึกเหตุการณ์หลายประเภท สามารถถูกใช้ในการตรวจจับภัยคุกคามบางอย่างได้ขึ้นอยู่กับประเภทของ Log และ Rule set ที่ใช้ในการวิเคราะห์

๒) Network Device Log อุปกรณ์เครือข่ายที่มีการบันทึกข้อมูลที่ผ่านเข้าออกเครือข่าย สามารถถูกใช้ในการตรวจจับเหตุการณ์ภัยคุกคามบางอย่างได้ขึ้นอยู่กับประเภทของ Log และ Rule set ที่ใช้ในการวิเคราะห์

๑๐.๒.๑.๓ ข้อมูลจากแหล่งสาธารณะข้อมูลช่องโหว่และวิธีการโจมตีระบบรูปแบบใหม่สามารถถูกใช้เป็นข้อบ่งชี้ภัยคุกคามได้

๑๐.๒.๑.๔ บุคคลที่ทำหน้าที่แจ้งเตือนบุคคลภายในองค์กร บุคลากรทุกตำแหน่งสามารถเข้ารับการฝึกฝนเพื่อช่วยสอดส่องดูแล

**๑๐.๒.๒ การวิเคราะห์เหตุภัยคุกคามหรือความผิดปกติเมื่อได้รับแจ้ง**

การวิเคราะห์ภัยคุกคามเพื่อให้การดำเนินการต่อไปสามารถทำได้เร็วและถูกต้อง ใช้การวิเคราะห์ความผิดปกติเมื่อได้รับแจ้งดังนี้

๑๐.๒.๒.๑ Log Retention Policy คือ การใช้ Log จากอุปกรณ์ต่าง ๆ เช่น IPS, Network Devices เป็นต้น จะมีความสำคัญเป็นอย่างมากในการวิเคราะห์หาสาเหตุการโจมตี และบันทึกเหตุการณ์เก็บไว้เพื่อหลักฐานทางกฎหมายหรือเรียกดูในอนาคต จึงต้องมีการเก็บรักษาไว้เป็นอย่างดี และตามระยะเวลาตามกฎหมายกำหนด

๑๐.๒.๒.๒ Clock Synchronization อุปกรณ์ทุกชิ้นบนเครือข่ายต้องได้รับการ Synchronize เวลาให้ตรงกันอยู่เสมอเพื่อทำให้การ Correlate Event ทำได้ง่าย

๑๐.๒.๒.๓ Sniff and Analyze Network Data ทำการดักจับข้อมูลทางเครือข่ายเพื่อนำมาวิเคราะห์ข้อมูล

๑๐.๒.๒.๔ Seek Assistance เมื่อทีมตอบสนองไม่สามารถดำเนินการวิเคราะห์ incident เพื่อหาสาเหตุที่แท้จริงได้เพื่อกำจัดผู้บุกรุกออกจากระบบ จะใช้บริการให้คำแนะนำปรึกษาจากภายนอก เช่น CERT ต่าง ๆ

**๑๐.๒.๓ การบันทึกภัยคุกคาม**

ต้องทำการบันทึกข้อมูลเหตุการณ์ภัยคุกคามเพื่อช่วยในการรับมือและตอบสนองภัยคุกคามอย่างมีประสิทธิภาพและเป็นระบบ โดยทำการบันทึกตั้งแต่การตรวจพบจนถึงสิ้นสุดของเหตุการณ์ภัยคุกคาม แบบฟอร์มการบันทึกข้อมูลเหตุการณ์ภัยคุกคาม (รายละเอียดดังภาคผนวก ๓)

**๑๐.๒.๔ การบันทึกข้อมูลกิจกรรมเหตุการณ์ความปลอดภัยทางไซเบอร์ (Incident Documentation)**

ต้องจัดให้มีการจัดทำบันทึกข้อมูลกิจกรรมเหตุการณ์ความปลอดภัยทางไซเบอร์ (Incident Documentation) โดย อ.ต.ก. ควรบันทึกข้อมูลเกี่ยวกับเหตุการณ์ความปลอดภัยทางไซเบอร์ ทุกขั้นตอนตั้งแต่ตรวจพบเหตุการณ์จนถึงกระบวนการสุดท้าย และข้อมูลดังกล่าวควรระบุรายละเอียดพร้อมเวลาที่เกิดเหตุและระยะเวลาที่ใช้ด้วยบันทึกข้อมูลดังกล่าวที่เกี่ยวข้องกับเหตุการณ์ควรลงวันที่และลงนามโดยผู้มีหน้าที่จัดการรับมือเหตุการณ์นั้นๆ เพื่อให้มั่นใจได้ว่าเหตุการณ์ความปลอดภัยทางไซเบอร์ที่เกิดขึ้นจะได้รับการจัดการแก้ไขภายในระยะเวลาที่เหมาะสมโดยอาจกำหนดให้มีรายละเอียดตามแบบฟอร์มตัวอย่าง (รายละเอียดปรากฏตามภาคผนวก ๔)

**๑๐.๒.๕ การรายงานภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับบริการของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ**

ต้องจัดให้มีการรายงานภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับบริการของโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้ผู้ที่เกี่ยวข้องทราบตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ.๒๕๖๖ ดังนี้

๑) กรณีมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นกับหน่วยงานรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศตาม ข้อ ๔ แห่งประกาศฯ ฉบับดังกล่าว ให้ใช้แบบฟอร์ม ก๑ โดยใช้แบบฟอร์มการรายงานตามกฎหมาย (รายละเอียดปรากฏตามภาคผนวก ๕)

๒) กรณีมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญต่อระบบของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศกับหน่วยงานรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศตาม ข้อ ๕ แห่งประกาศฯ ฉบับดังกล่าว ให้ใช้แบบฟอร์ม ก๒ รายงานไปยัง สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ภายในระยะเวลา ๒๔ ชั่วโมง โดยใช้แบบฟอร์มการรายงานตามกฎหมาย (รายละเอียดปรากฏตามภาคผนวก ๕)

๓) หน่วยงานของรัฐหรือหน่วยงานควบคุมหรือกำกับดูแล จะต้องจัดทำและส่งรายงานสรุปจำนวนเหตุภัยคุกคามทางไซเบอร์ทั้งหมดที่ได้เกิดขึ้นกับข้อมูลหรือระบบสารสนเทศของหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ภายใต้การควบคุมหรือกำกับดูแลของตนในแต่ละปี ภายในวันที่ ๓๑ มกราคม ของปีถัดไป ให้แก่สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ โดยให้แยกสถิติหมวดหมู่ตามแบบที่กำหนดในเอกสาร ก๓ โดยใช้แบบฟอร์มการรายงานตามกฎหมาย (รายละเอียดปรากฏตามภาคผนวก ๕)

**๑๐.๒.๖ การวิเคราะห์ผลกระทบและการจัดลำดับความสำคัญของ Incident**

การวิเคราะห์ผลกระทบและความรุนแรง เพื่อจัดลำดับความสำคัญของ Incident และช่วยในการตัดสินใจเชิงกลยุทธ์เพื่อดำเนินการรับมือและตอบสนองต่อภัยคุกคามที่เกิดขึ้นได้อย่างเหมาะสมภายใต้ทรัพยากรที่มีอยู่อย่างจำกัด และลดผลกระทบทางธุรกิจให้น้อยลงที่สุด การกำหนดแนวทางในการวิเคราะห์ผลกระทบและการจัดลำดับความสำคัญของ Incident โดยอย่างน้อยควรครอบคลุมในด้านผลกระทบต่อการให้บริการ (Functional Impact) ผลกระทบต่อข้อมูล (Information Impact) และความสามารถในการฟื้นฟูระบบ (Recoverability)

๑๐.๒.๖.๑ ผลกระทบต่อการให้บริการ (Functional Impact) ผลกระทบต่อการให้บริการ และการดำเนินงานของ อ.ต.ก. ที่เกิดภัยคุกคาม พิจารณาผลกระทบที่เกิดขึ้นทั้งในปัจจุบัน และผลกระทบที่มีโอกาสเกิดขึ้นหากเหตุการณ์ภัยคุกคามยังไม่ถูกควบคุมโดยทันทีซึ่งรวมถึงผลกระทบทางด้านการปฏิบัติงานของระบบ การให้บริการต่าง ๆ ซึ่งส่งผลโดยตรงต่อการดำเนินธุรกิจ (Impact to Business) ที่ทำให้เกิดความขัดข้องหรือเสียหายต่อธุรกิจ ซึ่งหากไม่ได้รับการแก้ไขโดยเร็วอาจจะมีผลเสียมากยิ่งขึ้น โดยระดับของ Functional Impact มีดังนี้

| Security Level | คำอธิบาย | ประเภท/รูปแบบของภัยคุกคาม |
|---|---|---|
| Low | ภัยคุกคามทางไซเบอร์ที่ส่งผลต่อระบบคอมพิวเตอร์อุปกรณ์โครงสร้างเครือข่าย หรือระบบงานขององค์กร เพียงเล็กน้อย หรืออาจทำให้ด้อยประสิทธิภาพ ลงไปบ้าง แต่ไม่กระทบกับระบบโดยรวม | - ไวรัสคอมพิวเตอร์ (Computer Virus)<br>- หนอนคอมพิวเตอร์ (Computer worm)<br>- Spam Mail หรืออีเมล์ขยะ<br>- Botnet<br>- สปายแวร์ (Spyware) |
| Medium | ภัยคุกคามทางไซเบอร์ที่ส่งผลต่อระบบคอมพิวเตอร์อุปกรณ์โครงสร้าง เครือข่าย หรือระบบงานขององค์กร เพียงเล็กน้อย หรืออาจทำให้ด้อย ประสิทธิภาพลงไปบ้าง แต่ไม่ถึงกับทำให้ระบบหรือบริการต้องหยุดชะงัก หรือไม่สามารถใช้งานได้ | - ม้าโทรจัน (Trojan horse)<br>- Backdoor - Rootkit<br>- การโจมตีแบบ DoS/DDoS<br>- Phishing |
| High | ภัยคุกคามทางไซเบอร์ที่ส่งผลหรือ อาจต่อระบบคอมพิวเตอร์อุปกรณ์ โครงสร้างเครือข่าย หรือระบบงานขององค์กรโดยรวมอย่างรุนแรง หรือมีเหตุอันควรเชื่อได้ว่า ผู้โจมตี มีความมุ่งหมายที่จะทำให้ระบบ และข้อมูลของหน่วยงานเสียหาย จนไม่สามารถทำงานหรือให้บริการได้ | - ซอฟต์แวร์เรียกค่าไถ่ (Ransomware)<br>- Sniffing - Social Engineering<br>- Password Attack<br>- Insider Treats<br>- SQL Injection<br>- Form Jacking |
| Extreme | ภัยคุกคามทางไซเบอร์ที่ส่งผลต่อระบบคอมพิวเตอร์อุปกรณ์โครงสร้าง เครือข่าย หรือระบบงานขององค์กร อย่างรุนแรง หรือมีเหตุอันควรเชื่อได้ว่า ผู้โจมตีจะทำให้ระบบและข้อมูลของหน่วยงานเสียหาย จนไม่สามารถทำงานหรือให้บริการได้ส่งผลเสียหาย เป็นวงกว้างซึ่งอาจทำให้หน่วยงาน อยู่ในภาวะคับขัน หรือมีการกระทำความผิดเกี่ยวกับการก่ออาชญากรรม ตามประมวลกฎหมายอาญา | - ผู้บุกรุก (Hacker) |

๑๐.๒.๖.๒ ผลกระทบต่อข้อมูล (Information Impact) ควรพิจารณา ๓ ด้าน ได้แก่ ด้านการรักษาความลับ (Confidentiality) ด้านการรักษาความครบถ้วน (Integrity) และด้านการรักษาสภาพพร้อม ใช้ (Availability) รวมทั้งควรพิจารณาว่าเหตุการณ์ภัยคุกคามส่งผลต่อการดำเนินงานโดยรวมที่จะส่งผลต่อข้อมูลสำคัญ (Sensitive Information) อย่างไร เช่น ข้อมูลถูกทำลาย หรือสูญหาย หรือรั่วไหล หรือการแก้ไขโดยไม่ได้รับอนุญาตเป็นต้น โดยระดับของ Functional Impact มีดังนี้

- None ไม่มีข้อมูลรั่วไหล ถูกเปลี่ยนแปลง ทำลาย หรือเข้าถึง โดยที่ไม่ได้รับอนุญาต
- Privacy Breach ข้อมูลที่ใช้ระบุตัวบุคคล (Personal Identifiable Information; PII) รั่วไหลหรือถูกเข้าถึงโดยไม่ได้รับอนุญาต
- Proprietary Breach ข้อมูลความลับที่ใช้ในการดำเนินธุรกิจ รั่วไหล หรือถูกเข้าถึงโดยไม่ได้ รับอนุญาต
- Integrity Loss ข้อมูลที่เป็น Privacy และ Propriety ถูกเปลี่ยนแปลง หรือทำลาย โดยไม่ได้ รับอนุญาต

๑๐.๒.๖.๓ ความสามารถในการฟื้นฟูระบบ (Recoverability) ความสามารถในการฟื้นฟูระบบ ควรพิจารณาจากระยะเวลาและทรัพยากรที่ต้องใช้ในการฟื้นฟูระบบจากเหตุภัยคุกคาม ซึ่งความรุนแรงของเหตุ ภัยคุกคามและประเภทของทรัพย์สินสารสนเทศเช่น ระบบ และข้อมูล เป็นต้น ที่ได้รับผลกระทบจะเป็นส่วนสำคัญในการพิจารณาความสามารถ หรือความยากง่ายในการฟื้นฟูระบบ รวมทั้งทรัพยากรที่จำเป็นต้องใช้โดยระดับของ Recoverability Effort มีดังนี้

- Regular เวลาในการกู้คืนสามารถคาดการณ์ได้ โดยใช้ทรัพยากรที่มี
- Supplemented เวลาในการกู้คืนสามารถคาดการณ์ได้ แต่ต้องมีการจัดหาทรัพยากรเพิ่ม
- Extended เวลาในการกู้คืนไม่สามารถคาดการณ์ได้ ต้องใช้ทรัพยากรและความช่วยเหลือจากภายนอก
- Not Recoverable การกู้คืนไม่สามารถทำได้ ใช้กับสถานการณ์ที่ข้อมูลได้รั่วไหลสู่สาธารณะแล้ว เป็นต้น ให้ใช้วิธีการติดตามและจำกัดการแพร่กระจายรวมถึงการเยียวยาผลกระทบ

**๑๐.๒.๗ การติดต่อประสานงานและแจ้งข้อมูล**

ทีมรับมือและตอบสนองภัยคุกคามต้องแจ้งข้อมูลเกี่ยวกับเหตุภัยคุกคามกับผู้ที่เกี่ยวข้องเพื่อให้ ทุกคนสามารถดำเนินการตามหน้าที่ความรับผิดชอบที่ได้กำหนดไว้ โดยมีบุคลากรที่เกี่ยวข้อง โครงสร้างการรับมือ ภัยคุกคามทางไซเบอร์ รายละเอียดมีดังนี้

| ลำดับ | ผู้เกี่ยวข้อง | หน้าที่ |
|---|---|---|
| ๑ | ผู้ที่ได้รับผลกระทบจาก incident | แจ้งเหตุหรือรายงานด้านความมั่นคงปลอดภัยไซเบอร์ที่พบหรือสงสัยว่ามีภัยคุกคามเกิดขึ้น |
| ๒ | ผู้รับแจ้งเหตุ | รับแจ้งเหตุหรือรับรายงานด้านความมั่นคงปลอดภัยไซเบอร์ |
| ๓ | ทีมรับมือและตอบสนองต่อ incident | ๑.รับมือและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์<br>๒.ให้คำแนะนำปรึกษาบุคลากรที่เกี่ยวกับจุดอ่อน การป้องกัน ข้อควรระมัดระวัง และแจ้งเตือนภัยคุกคามที่เกิดใหม่ให้เจ้าหน้าที่ ในหน่วยงาน<br>๓.มีส่วนร่วมกับหน่วยงานภายนอกองค์กร เช่น Thai CERT เพื่อแบ่งปันข้อมูลข่าวสารด้านภัยคุกคามทางไซเบอร์เพื่อป้องกันและตอบสนองภัยคุกคามได้เร็วขึ้น |

| | | |
|---|---|---|
| ๔ | ทีมเฝ้าระวังและวิเคราะห์การแจ้งเตือน incident | ๑.เฝ้าระวังและวิเคราะห์การแจ้งเตือนภัยคุกคามจากอุปกรณ์ตรวจจับ<br>๒.ให้คำแนะนำปรึกษาบุคลากรที่เกี่ยวกับจุดอ่อน การป้องกัน ข้อควรระมัดระวัง และแจ้งเตือนภัยคุกคามที่เกิดใหม่ให้เจ้าหน้าที่ ในหน่วยงาน<br>๓.มีส่วนร่วมกับหน่วยงานภายนอกองค์กร เช่น Thai CERT เพื่อแบ่งปันข้อมูลข่าวสารด้านภัยคุกคามทางไซเบอร์เพื่อป้องกัน และตอบสนองภัยคุกคามได้เร็วขึ้น |
| ๕ | ผู้บริหาร | รับผิดชอบกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา จัดหา และสนับสนุนงบประมาณสำหรับค่าใช้จ่าย ตลอดจนติดตาม กำกับ ดูแล ควบคุมเจ้าหน้าที่ เกี่ยวกับการป้องกันความมั่นคงปลอดภัยไซเบอร์ |

**หมายเหตุ** ทีมรับมือและตอบสนองต่อ incident และทีมเฝ้าระวังและวิเคราะห์การแจ้งเตือน incident ควรเป็นบุคลากรที่มีความรู้ ความสามารถ มีประสบการณ์ ผ่านการอบรมด้าน Cybersecurity ที่มีการรับรอง Certification และความเชี่ยวชาญเฉพาะด้านเกี่ยวกับการรักษาความปลอดภัยทางไซเบอร์

**๑๐.๒.๘ การฝึกฝนและการทดสอบ**

ผู้ทำหน้าที่รับมือและตอบสนองต่อ incident ควรได้รับการอบรมฝึกฝนและทดสอบการรับมือ และตอบสนองต่อ incident เพื่อให้ทุกคนตระหนักและเข้าใจถึงหน้าที่ความรับผิดชอบ และเป้าหมายตามแผนที่กำหนด รวมทั้งเพื่อเป็นการพัฒนาทักษะเพื่อให้สามารถดำเนินงานตามแผนได้อย่างมีประสิทธิภาพ และควรจัดให้มีการทดสอบแผนเป็นประจำเพื่อประเมินและทราบถึงประเด็นหรือช่องโหว่ (Gap) ที่ควรพัฒนา และเพิ่มความชำนาญให้กับบุคลากรของทีมรับมือและตอบสนองฯ โดยการทดสอบแผนควรดำเนินการทดสอบอย่างสม่ำเสมอ

(๑) ประเภทของการฝึกซ้อม

การฝึกซ้อมแบ่งออกเป็น ๓ ระดับ ตามความซับซ้อนของสถานการณ์ภัยคุกคาม

| ประเภทการฝึกซ้อม | รายละเอียด | ความถี่ |
|---|---|---|
| Tabletop Exercise (TTX) | ฝึกซ้อมในรูปแบบการประชุมเชิงปฏิบัติการ โดยทีมงานจะจำลองสถานการณ์ภัยคุกคาม และให้ทีม CIRT วิเคราะห์แนวทางตอบโต้ | ทุกๆ ๖ เดือน |
| Simulation Exercise (SIMEX) | จำลองสถานการณ์ภัยคุกคามไซเบอร์แบบสมจริง เช่น การโจมตี Ransomware หรือ Phishing Attack ให้ทีมปฏิบัติจริง | ปีละ ๑ ครั้ง |
| Red Team vs. Blue Team Drill | ทดสอบทีมรักษาความปลอดภัย (Blue Team) โดยให้ทีมโจมตี (Red Team) พยายามเจาะระบบและตรวจสอบช่องโหว่ | ปีละ ๑ ครั้ง |

(๒) กระบวนการฝึกซ้อม

ขั้นตอนที่ ๑ การวางแผนการฝึกซ้อม (Preparation)

ผู้รับผิดชอบ : กองเทคโนโลยีและสารสนเทศ (กส.) ร่วมกับทีม CIRT

แนวทางดำเนินการ :

- กำหนดวัตถุประสงค์ ของการฝึกซ้อม เช่น ทดสอบการตอบสนองต่อ Ransomware
- เลือกประเภทของการฝึกซ้อม (Tabletop, Simulation หรือ Red/Blue Team)
- กำหนดขอบเขตของการฝึกซ้อม (เช่น ระบบ ERP, ระบบ e-Payment)
- จัดทำ Scenario จำลองภัยคุกคามทางไซเบอร์ เช่น Phishing Attack, DDoS

ขั้นตอนที่ ๒ การดำเนินการฝึกซ้อม (Execution)

ผู้รับผิดชอบ : ทีมรับมือภัยคุกคามไซเบอร์ (CIRT) และบุคลากรที่เกี่ยวข้อง

แนวทางดำเนินการ :

- แจ้งเตือนสถานการณ์จำลองให้ทีมงานทราบล่วงหน้า (สำหรับ Tabletop Exercise เท่านั้น)
- เริ่มต้นการจำลองเหตุการณ์ โดยทีมผู้ฝึกซ้อม (Exercise Controller)
- ทีม CIRT วิเคราะห์และตอบโต้ ตามแผนรับมือที่กำหนด
- บันทึกการดำเนินการ และระยะเวลาการตอบสนอง (Response Time)

ขั้นตอนที่ ๓ การประเมินผลและสรุปบทเรียน (Post-Exercise Review)

ผู้รับผิดชอบ : กองเทคโนโลยีและสารสนเทศ (กส.), ผู้บริหาร และทีม CIRT

แนวทางดำเนินการ :

- ประเมินประสิทธิภาพของทีม CIRT โดยเปรียบเทียบกับ RTO (Recovery Time Objective) และ RPO (Recovery Point Objective)
- วิเคราะห์จุดอ่อนและข้อผิดพลาด เช่น ช่องโหว่ที่ถูกโจมตีสำเร็จ
- จัดทำรายงานสรุป (After-Action Report : AAR) พร้อมข้อเสนอแนะในการปรับปรุง

(๓) ตัวอย่างสถานการณ์จำลอง (Cyber Attack Scenarios)

| สถานการณ์ | รายละเอียด | เป้าหมายของการฝึกซ้อม |
|---|---|---|
| Phishing Attack | พนักงานได้รับอีเมลปลอมที่มีลิงก์อันตราย | ตรวจสอบว่าพนักงานรู้เท่าทันภัยคุกคามและมีการแจ้งเตือนที่เหมาะสม |
| Ransomware Attack | ระบบ ERP ถูกเข้ารหัสเรียกค่าไถ่ | ทดสอบการกู้คืนข้อมูลจาก Immutable Backup |
| Insider Threat | พนักงานพยายามดาวน์โหลดข้อมูลสำคัญออกจากระบบ | ทดสอบการตรวจจับของ SIEM และมาตรการ Zero Trust |
| DDoS Attack | เว็บไซต์หลักของ อ.ต.ก. ถูกโจมตีทำให้ใช้งานไม่ได้ | ทดสอบการป้องกันด้วย Firewall และ CDN |
| Zero-Day Exploit | ระบบถูกโจมตีด้วยช่องโหว่ที่ยังไม่มีแพตช์แก้ไข | ทดสอบการตอบสนองของทีม CIRT |

**<u>๑๐.๓ ขั้นตอนการระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ (containment, eradication, and recovery)</u>**

เมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้นหรือเมื่อหน่วยงานได้รับแจ้งเตือนการเกิดภัยคุกคามทางไซเบอร์ หน่วยงานต้องมีการกำหนดแนวทางการดำเนินมาตรการเพื่อระงับภัยคุกคามทางไซเบอร์และการฟื้นฟูระบบที่ได้รับผลกระทบ (Containment, Eradication, and Recovery) โดยกำหนดให้สอดคล้องกับความรุนแรง และระดับของภัยคุกคามทางไซเบอร์แต่ละระดับ จนกระทั่งสามารถกู้คืนทรัพยสินสำคัญทางสารสนเทศให้กลับมาดำเนินงานหรือให้บริการได้ตามปกติ

**๑๐.๓.๑ วิธีการควบคุมความเสียหาย คือการตัดสินใจเลือกใช้วิธีการที่เหมาะสม ดังนี้**

- ปิดระบบ (Shut Down)
- ตัดการเชื่อมต่อทางเครือข่ายทั้งหมด (Network disconnection) ทั้งนี้ อาจมียกเว้นการเชื่อมต่อสำหรับ Endpoint Detection & Response Agent (กระบวนการตรวจสอบและตรวจจับกิจกรรมหรือเหตุการณ์ ที่น่าสงสัยใด ๆ ที่เกิดขึ้นที่ปลายทางแบบเรียลไทม์)
- หยุดการทำงานของฟังก์ชันที่เกี่ยวข้อง (Disabling Certain Functions)
- Redirect Network Traffic และ/หรือความสนใจของผู้บุกรุกไปยัง Blackhole/ Sandbox/ Honeypot

ทั้งนี้ การตัดสินใจเลือกใช้วิธีการควบคุมความเสียหายจะขึ้นอยู่กับลักษณะสถานการณ์ที่กำลังเผชิญ ประเภทของภัยคุกคาม ระบบงานหรือบริการที่ได้รับผลกระทบ ระยะเวลาและทรัพยากรที่จำเป็นต่อการควบคุมความเสียหาย

**๑๐.๓.๒ การจัดเก็บและดูแลรักษาหลักฐานทางดิจิทัล**

วัตถุประสงค์หลักของการจัดเก็บหลักฐาน คือเพื่อให้การแก้ไข Incident ส่งผลกระทบต่อธุรกิจให้น้อยที่สุด (Minimizing impact to the business) นอกจากนี้ หลักฐานอาจมีความจำเป็นที่จะต้องใช้ในการดำเนินการตามขั้นตอนทางกฎหมาย ดังนี้ การดำเนินการจัดเก็บหลักฐานทางดิจิทัลสามารถดำเนินการโดยพิจารณาตามหลักการดังต่อไปนี้

- เป็นไปตามขั้นตอนที่กำหนดไว้ในกฎหมายข้อบังคับที่เกี่ยวกับหลักฐานดิจิทัล เพื่อให้สามารถนำไปใช้ ได้ในชั้นศาล
- หลักฐานมีบันทึกการเข้าถึงและการกระทำการใด ๆ ต่อหลักฐานตลอดเวลาอย่างรัดกุม
- การเปลี่ยนตัวผู้ดูแลจำเป็นต้องมีการจัดทำบันทึกห่วงโซ่หลักฐาน (Chain of Custody) รายละเอียดเกี่ยวกับหลักฐาน ควรประกอบด้วยข้อมูลอย่างน้อยดังต่อไปนี้

๑) ข้อมูลเฉพาะ เช่น Location, Serial Number, Model Number, Hostname, Media Access Control (MAC) และ Address เป็นต้น

๒) ชื่อ ตำแหน่ง และช่องทางการติดต่อผู้จัดเก็บและรักษาหลักฐานระหว่างการรับมือ Incident

๓) สถานที่จัดเก็บหลักฐาน

**๑๐.๓.๓ การกำจัดสาเหตุและการกู้คืนระบบให้กลับมาทำงานปกติ**

เมื่อมีการควบคุมความเสียหาย และมีการเก็บหลักฐานข้อมูลเพิ่มเติมเรียบร้อยแล้วข้อมูลทั้งหมด จะต้องนำกลับมาวิเคราะห์ตามหลักการที่ได้กล่าวไว้ใน “ขั้นตอนที่ ๒ เรื่องการตรวจจับและวิเคราะห์ (Detection & Analysis)” จนกว่าจะสามารถกำจัดสาเหตุที่ทำให้เกิด Incident และช่องทางที่ผู้บุกรุกได้สร้างไว้เพื่อเข้ามาในระบบทั้งหมดได้เรียบร้อย ซึ่งการกำจัดสาเหตุที่ทำให้เกิด Incident และผลกระทบ ได้แก่

- การปิดช่องโหว่ของระบบ
- การยกเลิก User Account ที่ผู้บุกรุกใช้เข้าสู่ระบบ
- การแจ้งให้ผู้ใช้งานเปลี่ยนรหัสผ่าน
- การลบโปรแกรมประเภท Backdoor ออกจากระบบ
- การใช้ข้อมูล Indicator of Compromise (Ioc) ในการสแกนหา Malware หรือร่องรอยอื่น ๆ ในระบบที่ยังหลงเหลือของผู้บุกรุกเพื่อดำเนินการกำจัดให้ออกจากระบบทั้งหมด

หลังจากดำเนินการควบคุมความเสียหาย กำจัดสาเหตุของภัยคุกคามเสร็จเรียบร้อยแล้ว จะเข้าสู่กระบวนการฟื้นฟูระบบให้เข้าสู่สภาวะการทำงานปกติโดยในขั้นตอนนี้สิ่งที่มีความสำคัญเป็นอย่างยิ่ง และควรเตรียมการล่วงหน้าในเรื่องดังต่อไปนี้

- การ Restore Operating System หรือ Application Software ต่าง ๆ จาก Master Image ที่ปลอดภัย
- การ Restore ข้อมูลกลับเข้าระบบจาก Back Up Storage

**<u>๑๐.๔ ขั้นตอนการดำเนินการภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ (Post-Incident activity)</u>**

การดำเนินกิจกรรมที่เกี่ยวของภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ (Post-incident Activity) นั้น ให้จัดทำข้อกำหนดขั้นตอน วิธีปฏิบัติ ที่เกี่ยวของเพื่อให้มีแนวทางที่ชัดเจน ซึ่งการปฏิบัติตามมาตรการดังกล่าว เพื่อให้สามารถเรียนรู้จากเหตุภัยคุกคามทางไซเบอร์ที่ผ่านมา และสามารถหาแนวทางเพื่อแก้ไขจุดบกพร่อง และพัฒนาแนวทางรับมือกับภัยคุกคามทางไซเบอร์ตอไปในอนาคต โดยให้มีการประชุมหารือเพื่อแลกเปลี่ยนข้อมูล ความคิดเห็นในการนำไปพัฒนาและปรับปรุงแนวทางในการรับมือและตอบสนองภัยคุกคามทางไซเบอร์ รวมทั้งการใช้ข้อมูลเพื่อประกอบการพิจารณาปรับปรุง

นอกจากนี้ต้องเก็บรักษาข้อมูลและพยานหลักฐานที่จำเป็น เพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์ หรือใช้ในกรณีที่ต้องการร้องทุกข์หรือดำเนินคดี เนื่องจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้นนั้น อาจเข้าลักษณะเป็น ๑๒ ความผิดตามประมวลกฎหมายอาญา หรือพระราชบัญญัติวาด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐ และที่แก้ไขเพิ่มเติม หรือกฎหมายอื่น ๆ ที่เกี่ยวข้อง โดยการเก็บข้อมูลบางประเภทนั้นอาจจำเป็นต้องดำเนินการตั้งแต่เมื่อมีการตรวจพบว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้น เนื่องจากข้อมูลดังกล่าวอาจสูญหายไปในระหว่างที่ต้องระงับเหตุภัยคุกคามทางไซเบอร์นั้น หรืออาจถูกลบหรือทำลายโดยผู้โจมตีเมื่อมีการเก็บรวบรวมข้อมูล และหลักฐานที่จำเป็นแล้วให้นำข้อมูลและหลักฐานที่รวบรวมได้มาใช้ในการจัดทำบันทึกข้อมูลสถิติภัยคุกคามทางไซเบอร์โดยอาจจัดทำเป็นรายสัปดาห์หรือรายเดือนเพื่อเสนอต่อผู้ที่มีหน้าที่ดูแลและรับผิดชอบภายในหน่วยงาน และกำหนดขั้นตอนที่หน่วยงานควรดำเนินการเพื่อป้องกันไม่ให้เกิดภัยคุกคามทางไซเบอร์ในลักษณะดังกล่าวขึ้นอีกในอนาคต

หลักการดูแลรักษาหลักฐานทางดิจิทัลที่สำคัญมีดังนี้

| | |
|---|---|
| ๑. Assessment | การประเมินเพื่อหาจุดที่ต้องดำเนินการจัดเก็บหลักฐานของ incident ที่กำลังรับมือและตอบสนอง เช่น Hard Disk, RAM, External Hard Disk, Mobile Device เป็นต้น |
| ๒. Acquisition | ดำเนินการจัดเก็บหลักฐานด้วยการทำสำเนา (Duplication/Bit-for-bit Acquisition) ด้วยเครื่องมือที่เหมาะสม โดยมีข้อควรระวังในเรื่องดังต่อไปนี้<br>๑. ต้องป้องกันการเปลี่ยนแปลงของหลักฐานด้วยการใช้งาน Hardware Write Blocker |

| | |
|---|---|
| | ๒. ต้องคำนึงถึง Volatility หรือความอ่อนไหวต่อการสูญเสียกระแสไฟฟ้าของหลักฐาน เช่น ข้อมูลที่เสี่ยงต่อการสูญหายหากไม่มีกระแสไฟคอยเลี้ยง เช่น RAM ต้องได้รับการเก็บรักษาเป็นอันดับแรก เป็นต้น<br>๓. ต้องบันทึกรายละเอียดการดำเนินงานทุกขั้นตอนที่ลงมือปฏิบัติอย่างละเอียด<br>๔. ต้องทำการบันทึกหลักฐาน (Chain of Custody) |
| ๓. Authentication | ทำการตรวจสอบความถูกต้องของหลักฐานที่ Duplicate และเปรียบเทียบกับต้นฉบับด้วยวิธี Cryptographic Hash เช่น MD5, SHA1, SHA256 |
| ๔. Analysis & Report | วิเคราะห์หาข้อมูลจากชุดหลักฐานที่ดำเนินการจัดเก็บเพื่อพิสูจน์ข้อเท็จจริง หรือเพื่อค้นหาสาเหตุของการเกิด Incident |
| ๕. Archive | จัดเก็บหลักฐานไว้ในที่เหมาะสม ปลอดภัย และบันทึก Chain of Custody Form ทุกครั้งที่มีการเคลื่อนย้ายหลักฐาน พร้อมทั้งระบุเหตุผลของการเคลื่อนย้าย |

Chain of custody หรือ “ห่วงโซ่การคุ้มครองพยานหลักฐาน” คือ เอกสารแสดงลำดับการเกิดเหตุการณ์ หรือเอกสารแสดงทุกขั้นตอน ตั้งแต่การยึดเครื่องคอมพิวเตอร์ การดูแลรักษา การควบคุม การวิเคราะห์ และการจัดเก็บหลักฐานทางอิเล็กทรอนิกส์ เนื่องจากหลักฐานที่พบสามารถนำไปใช้ในยืนยันได้ในชั้นศาล หลักฐานเหล่านี้จึงจะต้องได้รับการจัดการอย่างระมัดระวัง และรอบคอบเพื่อหลีกเลี่ยงข้อกล่าวหาว่าเป็นหลักฐานที่ปลอมหรือทำขึ้นมา

### ๑๐.๕ การจัดทำรายการตรวจสอบการจัดการเหตุการณ์ (Incident Handling Checklist)

การจัดทำรายการตรวจสอบการจัดการเหตุการณ์ (Incident Handling Checklist) ซึ่งจะช่วยให้แนวทางแก่หน่วยงานเกี่ยวกับขั้นตอนสำคัญที่ควรดำเนินการ โดยสามารถใช้ข้อมูลเพื่อประกอบการพิจารณาความเหมาะสมในการจัดทำรายการตรวจสอบได้ (รายละเอียดปรากฏตามภาคผนวก ๖)

## ๑๑. การเตรียมความพร้อม

### ๑๑.๑ การเตรียมพร้อมด้านฮาร์ดแวร์และซอฟต์แวร์

(๑) อุปกรณ์ป้องกันเครือข่าย (Next Generation Firewall) ใช้สำหรับป้องกันภัยคุกคามทางไซเบอร์ประเภท Dos/DDos, BOTNET, Phishing, Sniffing, Hacker ทั้งนี้อุปกรณ์ป้องกันระบบเครือข่ายต้องมีความสามารถอื่น ๆ เพิ่มเติม ได้แก่ ความสามารถในการด้านการตรวจจับการบุกรุก (IPS) ความสามารถในการคัดกรองเว็บไซต์อันตราย (Web Filtering) และการควบคุมการใช้งานซอฟต์แวร์ (Application Control) เป็นอย่างน้อย

(๒) ชุดโปรแกรมตรวจสอบประสิทธิภาพระบบเครือข่าย (Next Monitoring Software) ใช้สำหรับตรวจจับความผิดปกติที่เกิดขึ้นกับระบบเครือข่ายคอมพิวเตอร์กลางของ อ.ต.ก.

(๓) อุปกรณ์ป้องกันการบุกรุกเว็บไซต์ (Web Application Firewall: WAF) ใช้สำหรับป้องกันภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับระบบงานคอมพิวเตอร์ของ อ.ต.ก. ที่พัฒนาขึ้นมาและให้บริการผ่าน Web Browser ได้แก่ การคุกคามทางไซเบอร์ประเภท Hacker โดยสามารถป้องกันเทคนิคการบุกรุก เช่น Cross-site Scripting และ SQL Injection ได้เป็นอย่างน้อย

(๔) ชุดโปรแกรมสำรองข้อมูล ใช้สำหรับกระบวนการสำรองข้อมูล และการกู้ข้อมูล ของระบบเครือข่ายคอมพิวเตอร์ของ อ.ต.ก. รวมทั้งยังสามารถสำรองข้อมูลแบบเข้ารหัสได้

(๕) อุปกรณ์สำหรับจัดเก็บข้อมูลแบบ SAN (Storage Area Network) เป็นอุปกรณ์ที่ใช้สำหรับติดตั้งระบบงานคอมพิวเตอร์ของ อ.ต.ก. และสามารถลดผลกระทบที่เกิดจาก Ransomware ได้ โดย อ.ต.ก. จะใช้อุปกรณ์จัดเก็บข้อมูลภายนอกดังกล่าวจัดทำพื้นที่จัดเก็บข้อมูลส่วนกลาง โดยกำหนดให้แต่ละหน่วยงานภายใน อ.ต.ก. มีพื้นที่จัดเก็บข้อมูลอย่างน้อย ๕๐๐ GB และจะมีการสำรองข้อมูลจากพื้นที่จัดเก็บข้อมูลส่วนกลางอย่างสม่ำเสมอ ซึ่งหากหน่วยงานภายใน อ.ต.ก. นำไฟล์สำคัญมาจัดเก็บไว้บนพื้นที่จัดเก็บข้อมูลส่วนกลางแล้วแม้ว่าจะเกิดภัยคุกคามไซเบอร์ประเภท Ransomware ก็จะสามารสำเนาข้อมูลสำคัญที่เก็บข้อมูลบนพื้นที่จัดเก็บข้อมูลส่วนกลางกลับมาใช้งานได้

(๖) ระบบงานคอมพิวเตอร์สำรอง ใช้ในกรณีที่ไม่สามารถกู้ระบบงานคอมพิวเตอร์ขึ้นมาได้

(๗) อุปกรณ์จัดเก็บ Log File ใช้สำหรับจัดเก็บข้อมูลจราจรคอมพิวเตอร์ ที่เกิดขึ้นจากการใช้งานเครือข่ายคอมพิวเตอร์กลางของ อ.ต.ก.

(๘) อุปกรณ์วิเคราะห์ Log File ใช้สำหรับวิเคราะห์ข้อมูลจราจรคอมพิวเตอร์ที่เกิดขึ้นจากการใช้งานเครือข่ายคอมพิวเตอร์กลางของ อ.ต.ก. ซึ่งข้อมูลที่ถูกวิเคราะห์ดังกล่าวจะช่วยระบุถึงหมายเลข IP Address ของผู้คุกคาม/ผู้โจมตี และลักษณะภัยคุกคามไซเบอร์ที่โจมตีระบบเครือข่ายคอมพิวเตอร์กลางของ อ.ต.ก. และใช้ประกอบการทำรายงาน

(๙) ชุดโปรแกรมป้องกันไวรัสคอมพิวเตอร์แบบองค์กร (Corporate Antivirus Software) ใช้สำหรับติดตั้งบนเครื่องคอมพิวเตอร์ เครื่องคอมพิวเตอร์โน๊ตบุ๊ค และเครื่องคอมพิวเตอร์แม่ข่ายของ อ.ต.ก. ซึ่งสามารถป้องกันภัยคุกคามไซเบอร์ประเภท Malware, Computer Virus, Computer Worm, Trojan, Spyware, Ransomware, Botnet, Spam Mail ได้

**<u>๑๑.๒ การเตรียมพร้อมแผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์</u>**

เพื่อให้ระบบเครือข่ายคอมพิวเตอร์กลางของ อ.ต.ก. สามารถรับมือกับภัยคุกคามทางไซเบอร์ ที่มีการพัฒนาขึ้นตลอดเวลา อ.ต.ก. จะพิจารณาจัดหาหรือจ้างผู้เชี่ยวชาญในการประเมินความเสี่ยงการรักษาความมั่นคงปลอดภัยไซเบอร์มาตรวจสอบ โดยจะมีการตรวจสอบอย่างน้อยปีละ ๑ ครั้ง ซึ่งในการตรวจสอบ และประเมินความเสี่ยงนี้ สามารถค้นหาภัยคุกคามไซเบอร์ประเภท Backdoor ที่ถูกซ่อนอยู่ในระบบคอมพิวเตอร์ จากขั้นตอนการพัฒนาระบบงานได้

**<u>๑๑.๓ การเตรียมพร้อมด้านบุคลากร</u>**

(๑) การให้ความรู้ เพื่อให้บุคลากรของ อ.ต.ก. มีความรู้เกี่ยงกับภัยคุกคามทางไซเบอร์ อ.ต.ก.จะพิจารณาจัดหาหรือจ้างผู้เชี่ยวชาญในการประเมินความเสี่ยงการรักษาความมั่นคงปลอดภัยไซเบอร์ ดำเนินการจัดฝึกอบรมให้ความรู้แก่บุคลากรของ อ.ต.ก. อย่างน้อยปีละ ๑ ครั้ง

(๒) การแจ้งรายชื่อเจ้าหน้าที่ สำหรับประสานงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตราที่ ๔๖ กำหนดให้หน่วยงานภาครัฐแจ้งรายชื่อเจ้าหน้าที่ระดับบริหารและระดับปฏิบัติการ โดย อ.ต.ก. จะกำหนดระดับภัยคุกคามทางไซเบอร์ตาม พระราชบัญญัติการ

รักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตราที่ ๖๐ และจะแจ้งรายชื่อผู้เจ้าหน้าที่เพื่อประสานงานด้านการรักษาความปลอดภัยไซเบอร์ในระดับต่าง ๆ

(๓) มีผู้ดูแลด้านการรักษาความมั่นคงปลอดภัยเครือข่าย และผู้ดูแลระบบเครือข่ายคอมพิวเตอร์กลางของ อ.ต.ก.

**๑๑.๔ การเตรียมความพร้อมด้านการสำรองข้อมูลและระบบคอมพิวเตอร์สำรอง**

ในกรณีที่ภัยคุกคามทางไซเบอร์ ก่อเกิดความเสียหายแก่ระบบคอมพิวเตอร์กลางของ อ.ต.ก. อย่างมากจนไม่สามารถทำงานได้เป็นเวลานาน อ.ต.ก. จะพิจารณาทางเลือกในการแก้ไขปัญหาโดยวิธีการกู้คืนข้อมูลที่เสียหาย หรือเปิดใช้ระบบคอมพิวเตอร์สำรอง โดยมีเป้าหมายเพื่อให้ระบบเครือข่ายคอมพิวเตอร์กลางของ อ.ต.ก. สามารถใช้งานได้อย่างรวดเร็วที่สุด

การสำรองข้อมูลของ อ.ต.ก. จะใช้ ๓ ระดับหลัก ได้แก่

๑. Primary Backup (On-Premise Backup) – สำรองข้อมูลในศูนย์ข้อมูลหลักของ อ.ต.ก.

๒. Immutable Backup (WORM Storage) – สำรองข้อมูลที่ไม่สามารถเปลี่ยนแปลงหรือลบได้

๓. Offsite Backup (Government Cloud & Data Center) – สำรองข้อมูลไปยังระบบภายนอกเพื่อป้องกันภัยพิบัติ

**๑๑.๔.๑ วิธีการสำรองข้อมูล**

(๑) Immutable Backup (สำรองข้อมูลแบบเปลี่ยนแปลงไม่ได้)

วัตถุประสงค์ : ป้องกันการแก้ไข หรือลบข้อมูลสำรองโดยไม่ได้รับอนุญาต

แนวทางดำเนินการ :

- ใช้ระบบ WORM (Write Once, Read Many) Storage เช่น Dell EMC Data Domain หรือ NetApp SnapLock
- กำหนด Retention Policy ไม่ให้ข้อมูลถูกเปลี่ยนแปลงเป็นระยะเวลา ๙๐ - ๓๖๕ วัน
- แยก Credential สำหรับการเข้าถึงข้อมูลสำรอง ออกจากบัญชีที่ใช้ในระบบหลัก
- ใช้ Multi-Factor Authentication (MFA) ในการเข้าถึงระบบสำรองข้อมูล

(๒) Offsite Backup (สำรองข้อมูลนอกสถานที่)

วัตถุประสงค์ : ป้องกันความเสียหายของข้อมูลจากภัยพิบัติหรือการโจมตีระบบทั้งหมด

แนวทางดำเนินการ :

- สำรองข้อมูลไปยัง Government Cloud (GDCC – Government Data Center and Cloud)
- ใช้ Offsite Data Center ที่ได้รับมาตรฐาน ISO ๒๗๐๐๑ และ PDPA
- กำหนด Geo-Redundant Backup (สำรองข้อมูลในหลายสถานที่)
- ใช้ Hybrid Cloud Backup เช่น Veeam Cloud Connect หรือ AWS S๓ Glacier

**๑๑.๔.๒ ตารางกำหนดการสำรองข้อมูล**

| ประเภทข้อมูล | ความถี่ในการสำรอง | รูปแบบสำรอง | ระยะเวลาการเก็บรักษา | สถานที่เก็บ |
|---|---|---|---|---|
| ข้อมูลทั่วไป (Public) | รายวัน | Incremental Backup | ๓ เดือน | On-Premise Backup |
| ข้อมูลสำคัญ (Critical) | รายชั่วโมง | Immutable Backup | ๑ ปี | WORM Storage |
| ข้อมูลความลับ (Confidential) | รายชั่วโมง | Immutable + Offsite Backup | ๕ ปี | Government Cloud |
| ข้อมูลที่ต้องการความต่อเนื่องสูง (Business Continuity) | Real-time | Continuous Replication | ๗ ปี | Hybrid Cloud Backup |

**๑๑.๔.๓ การทดสอบและกู้คืนข้อมูล (Disaster Recovery Testing)**

การทดสอบการกู้คืนข้อมูล (Restore Testing)

(๑) ทดสอบการกู้คืนข้อมูลจาก Immutable Backup ทุก ๓ เดือน

(๒) ทดสอบ Failover ไปยัง Offsite Backup อย่างน้อย ปีละ ๑ ครั้ง

(๓) ทดสอบการสำรองและกู้คืน ฐานข้อมูลสำคัญ เช่น ระบบ ERP และ e-Payment

**๑๑.๔.๔ มาตรการควบคุมความปลอดภัยในการสำรองข้อมูล**

(๑) กำหนดให้เจ้าหน้าที่ IT ที่มีสิทธิ์เข้าถึงข้อมูลสำรองต้องผ่านการอบรม Cybersecurity Awareness

(๒) บังคับใช้ Zero Trust Policy โดยกำหนด Least Privilege Access

(๓) ใช้ Data Encryption (AES-๒๕๖) ในการป้องกันข้อมูลสำรอง

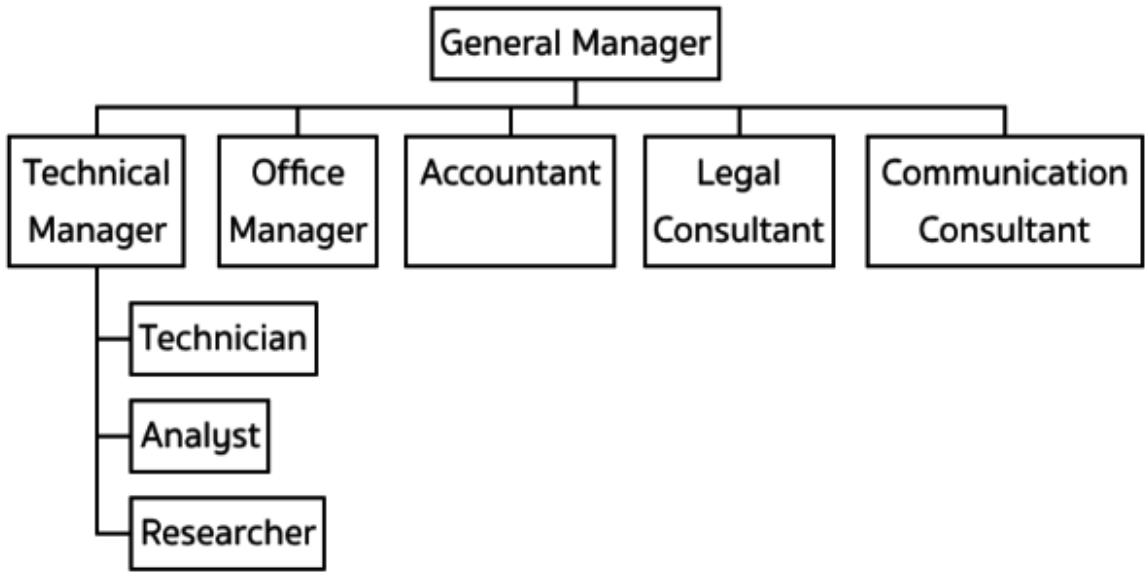
(๔) ติดตั้ง EDR (Endpoint Detection & Response) และ SIEM (Security Information & Event Management) เพื่อมอนิเตอร์กิจกรรมที่ผิดปกติ

**ภาคผนวก ๑**
**โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์**
**( Cyber Incident Response Team: CIRT)**

ทีมตอบสนองต่อเหตุการณ์ซึ่งเรียกอีกอย่างว่าทีมตอบสนองต่อเหตุการณ์ด้านความปลอดภัยของคอมพิวเตอร์ (CSIRT), ทีมตอบสนองต่อเหตุการณ์ไซเบอร์ (CIRT), หรือทีมตอบสนองต่อเหตุฉุกเฉินเกี่ยวกับคอมพิวเตอร์ (CERT) ประกอบด้วยกลุ่มบุคลากรข้ามสายงานในองค์กรที่มีหน้าที่รับผิดชอบในการดำเนินการตามแผนตอบสนองต่อเหตุการณ์ ซึ่งไม่เพียงรวมถึงบุคคลที่กำจัดภัยคุกคามเท่านั้น แต่ยังรวมถึงบุคคลที่ตัดสินใจทางธุรกิจหรือทางกฎหมายที่เกี่ยวข้องกับเหตุการณ์ด้วย ทีมโดยทั่วไปประกอบด้วยสมาชิกดังต่อไปนี้

- ผู้จัดการการตอบสนองต่อเหตุการณ์ ซึ่งจะเป็นหัวหน้ากองเทคโนโลยีและสารสนเทศ จะกำกับดูแลการตอบสนองทุกขั้นและแจ้งให้ผู้เกี่ยวข้องภายในรับทราบ
- นักวิเคราะห์ด้านการรักษาความปลอดภัยจะศึกษาเหตุการณ์ดังกล่าวเพื่อพยายามทำความเข้าใจถึงสิ่งที่เกิดขึ้น พร้อมทั้งบันทึกการค้นพบและรวบรวมหลักฐานการพิสูจน์อีกด้วย
- นักวิจัยด้านภัยคุกคามจะศึกษาข้อมูลภายนอกองค์กรเพื่อรวบรวมข่าวกรองที่ให้บริบทเพิ่มเติม
- บุคคลจากคณะผู้บริหาร เช่น ประธานเจ้าหน้าที่บริหารฝ่ายการรักษาความปลอดภัยของข้อมูลหรือประธานเจ้าหน้าที่บริหารฝ่ายสารสนเทศ ให้คำแนะนำและทำหน้าที่เป็นผู้ประสานงานกับผู้บริหารคนอื่นๆ
- ผู้เชี่ยวชาญด้านทรัพยากรบุคคลจะช่วยจัดการภัยคุกคามจากภายใน
- ที่ปรึกษาทั่วไปจะช่วยทีมสำรวจปัญหาด้านการรับผิดและตรวจสอบให้แน่ใจว่ามีการรวบรวมหลักฐานการพิสูจน์
- ผู้เชี่ยวชาญด้านการประชาสัมพันธ์จะประสานงานในการสื่อสารภายนอกที่ถูกต้องกับสื่อ ลูกค้า และผู้เกี่ยวข้องรายอื่นๆ

ทีมตอบสนองต่อเหตุการณ์อาจเป็นชุดย่อยของศูนย์การดำเนินการรักษาความปลอดภัย (SOC) ซึ่งจัดการการดำเนินการรักษาความปลอดภัยนอกเหนือจากการตอบสนองต่อเหตุการณ์

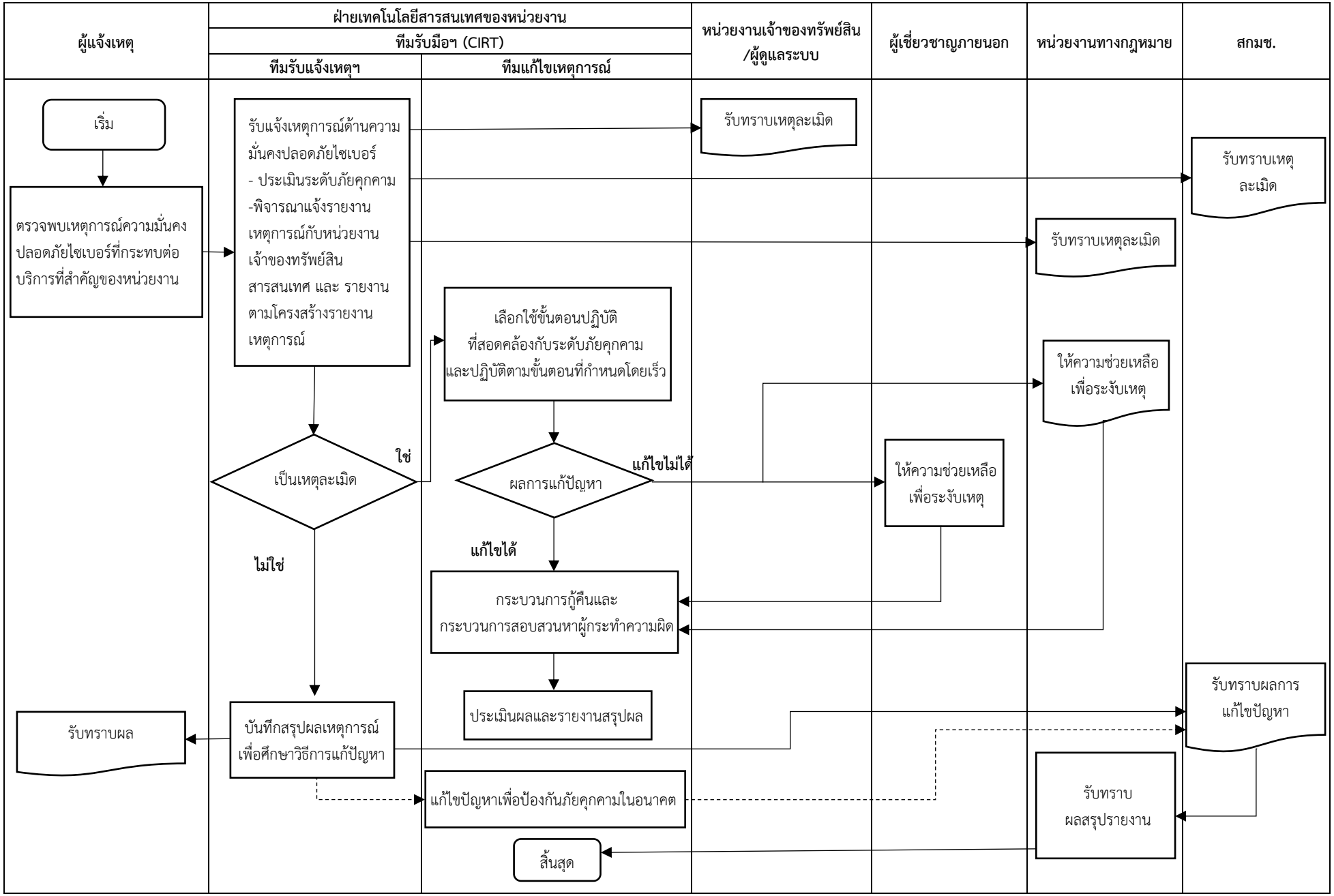


**คุณสมบัติและทักษะ Technician ที่พึงมี ประกอบด้วย**

- ศักยภาพด้านบุคคล
  - ยืดหยุ่น มีความคิดสร้างสรรค์ และทำงานเป็นทีม
  - มีทักษะการวิเคราะห์ที่ดีเยี่ยม
  - สามารถอธิบายข้อมูลเชิงเทคนิคให้ผู้อื่นเข้าใจได้ง่าย
  - มีความมั่นใจสูงและทำงานอย่างเป็นระบบ
  - อดทนต่อความกดดัน
  - มีทักษะด้านการติดต่อสื่อสารและการเขียนดีเยี่ยม
  - เปิดใจและพร้อมที่เรียนรู้สิ่งใหม่
- ศักยภาพด้านเทคนิค
  - มีความรู้ทางด้านเทคโนโลยีอินเทอร์เน็ตและโปรโตคอลอย่างกว้างขวาง
  - มีความรู้ทางด้านระบบ Linux, Unix และ Windows
  - มีความรู้ทางด้านอุปกรณ์โครงสร้างเครือข่าย
  - มีความรู้ทางด้านแอพพลิเคชันและบริการบนอินเทอร์เน็ต เช่น SMTP, HTTP(s), Social Media และอื่นๆ
  - มีความรู้ทางด้านภัยคุกคาม เช่น DDoS, Phishing, Defacing, Malware และอื่นๆ
  - มีความรู้ทางด้านการประเมินความเสี่ยงและการวางระบบ
  - มีความรู้ทางด้านการวิเคราะห์ข้อมูลแบบ Big Data และ Malware
- ศักยภาพด้านอื่นๆ
  - พร้อมทำงานแบบ ๕x๘ (จันทร์-ศุกร์ เวลา ๘.๓๐ - ๑๖.๓๐)
  - สามารถทำงานต่างจังหวัดหรือระยะไกลได้
  - มีประสบการณ์การทำงานในสาย IT Security

**ภาคผนวก ๒**

## แผนผังโครงสร้างขั้นตอนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response)



**ภาคผนวก ๓**

**ตัวอย่าง : บันทึกรายงานสถานการณ์เหตุการณ์ความมั่นคงปลอดภัยไซเบอร์**

| | | |
|---|---|---|
| วันที่ : | เวลา : | ผู้บันทึกรายงาน :<br>ติดต่อ : |
| วันและเวลาที่เกิดเหตุการณ์ : | | |
| สถานะเหตุการณ์ปัจจุบัน : | | |
| ประเภทเหตุการณ์ : | | |
| ระดับความรุนแรง : | | |
| รายละเอียดเหตุการณ์ : | | |
| ผลกระทบที่เกิดขึ้น : | | |
| ความเสียหายที่เกิดขึ้น : | | |
| การรายงานเหตุการณ์ : | | |
| หน่วยงานที่ขอความช่วยเหลือ : | | |
| การดำเนินการตอบสนองต่อเหตุการณ์ : | | |
| รายละเอียดเพิ่มเติม : | | |
| ผู้จัดการรับมือฯ เหตุการณ์ : | | |
| ข้อมูลติดต่อผู้จัดการรับมือฯ เหตุการณ์ : | | |
| วันและเวลาที่มีรายงานความคืบหน้าครั้งถัดไป : | | |

**ภาคผนวก ๔**

## บันทึกข้อมูลกิจกรรมเหตุการณ์ความปลอดภัยทางไซเบอร์ (Incident Documentation)

| วันที่และเวลา | บันทึกกิจกรรมที่เกิดขึ้น<br>(ข้อเท็จจริง, สถานการณ์ที่เกิดขึ้น, การตัดสินใจ, ผลกระทบ) |
|---|---|
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |

**เอกสาร ก๑ ข้อมูลที่ต้องแจ้ง**

**ข้อมูลการประสานงานและผลการตรวจสอบภัยคุกคามเบื้องต้น**

**๑. ข้อมูลการประสานงาน**

ชื่อหน่วยงานที่รับผิดชอบติดตามเหตุภัยคุกคาม

วันที่และเวลาที่แจ้ง

**๒. ด้านภารกิจหรือบริการของหน่วยงาน และ ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม**

ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม

ที่อยู่ของหน่วยงานหรือหน่วยงานย่อยที่เกิดเหตุภัยคุกคาม

**๓. ข้อมูลการติดต่อสำหรับการประสานงานเหตุภัยคุกคาม**

ชื่อ-นามสกุล ตำแหน่งงาน

ชื่อหน่วยงาน อีเมล

โทรศัพท์ (ที่ทำงาน / มือถือ)

**๔. ความต่อเนื่องของเหตุภัยคุกคาม**

☐ เหตุภัยคุกคามใหม่ ☐ การรายงานข้อมูลต่อเนื่องจากเหตุภัยคุกคามเดิม

**๕. ลักษณะภัยคุกคามทางไซเบอร์**

ระบบที่ได้รับผลกระทบมีความสำคัญต่อพันธกิจหลักของหน่วยงานหรือไม่

เหตุการณ์ที่เกิดขึ้นเกิดจากภัยคุกคามทางไซเบอร์[2] ในระดับใด (มาตรา ๖๐)

☐ ไม่ร้ายแรง ☐ ร้ายแรง ☐ วิกฤต (ก) ☐ วิกฤต (ข)

☐ ยังไม่สามารถระบุได้

**๖. หมวดหมู่ของภัยคุกคาม (แจ้งได้มากกว่า ๑ รายการ)**

| หมวดหมู่* | คำอธิบาย |
|---|---|
| หมวดหมู่ที่ ๒ | การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance) |
| หมวดหมู่ที่ ๓ | การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยของหน่วยงาน (Non-Compliance Activity) |
| หมวดหมู่ที่ ๔ | การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic) |
| หมวดหมู่ที่ ๕ | การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion) |
| หมวดหมู่ที่ ๖ | การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion) |
| หมวดหมู่ที่ ๗ | การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service) |
| หมวดหมู่ที่ ๘ | เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating) |

* อ้างอิงหมวดหมู่ตามภาคผนวกท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ (ทั้งนี้ ภัยคุกคามทางไซเบอร์หมวดหมู่ที่ ๐ หมวดหมู่ที่ ๑ และหมวดหมู่ที่ ๙ ไม่เข้าข่ายเป็นภัยคุกคามทางไซเบอร์ที่ต้องรายงาน)

[2] พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 กำหนดความหมายของ “ภัยคุกคามทางไซเบอร์” ดังนี้ การกระทำหรือการดำเนินการใด ๆ โดยมิชอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

**เอกสาร ก๒ แบบรายงานภัยคุกคามทางไซเบอร์**

**ส่วนที่ ๑**

**หมวด ก. ข้อมูลการประสานงานและผลการตรวจสอบภัยคุกคามเบื้องต้น**

**หมายเลขอ้างอิง (สำหรับเจ้าหน้าที่ สกมช.):** โปรดระบุ
**หน่วยงานที่รับผิดชอบติดตามเหตุภัยคุกคาม (ถ้ามี):** โปรดระบุ
**วันที่:** เลือกวันที่ **เวลา:** โปรดระบุ

**ก๑. ด้านภารกิจหรือบริการของหน่วยงาน และ ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม**
ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม: โปรดระบุ
ที่อยู่ของหน่วยงานหรือหน่วยงานย่อยที่เกิดเหตุภัยคุกคาม: โปรดระบุ

**ก๒. ข้อมูลการติดต่อสำหรับการประสานงานเหตุภัยคุกคาม**
ชื่อ-นามสกุล: โปรดระบุ ตำแหน่งงาน: โปรดระบุ
ชื่อหน่วยงาน: โปรดระบุ อีเมล: โปรดระบุ
โทรศัพท์ (ที่ทำงาน / มือถือ) : โปรดระบุ

**ก๓. ความต่อเนื่องของเหตุภัยคุกคาม**
☐ เหตุภัยคุกคามใหม่ ☐ การรายงานข้อมูลต่อเนื่องจากเหตุภัยคุกคามเดิม

**ก๔. ลักษณะภัยคุกคามทางไซเบอร์**
ระบบที่ได้รับผลกระทบมีความสำคัญต่อพันธกิจหลักของหน่วยงาน
☐ ใช่ ☐ ไม่ใช่
เหตุการณ์ที่เกิดขึ้นเกิดจากภัยคุกคามทางไซเบอร์[3] ในระดับใด (มาตรา ๖๐)
☐ ไม่ร้ายแรง ☐ ร้ายแรง ☐ วิกฤต (ก) ☐ วิกฤต (ข)
☐ ยังไม่สามารถระบุได้

[3] พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดความหมายของ “ภัยคุกคามทางไซเบอร์” ดังนี้ การกระทำ หรือการดำเนินการใด ๆ โดยมิชอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหาย หรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

**หมวด ข. ข้อมูลการตรวจพบภัยคุกคามไซเบอร์**

**ข๑. วัน เวลา ที่เกิดเหตุภัยคุกคาม**

วันที่ : เลือกวันที่ เวลา : โปรดระบุ

**วัน เวลา ที่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศทราบเหตุภัยคุกคาม**

วันที่ : เลือกวันที่ เวลา : โปรดระบุ

**ข๒. วัน เวลา ที่แจ้งเหตุภัยคุกคามให้หน่วยงานควบคุมหรือกำกับดูแลทราบ**

☐ ยังไม่ได้แจ้ง ☐ แจ้งแล้ว _____

**ข๓. หมวดหมู่ของภัยคุกคาม (เลือกได้มากกว่า ๑ รายการ)**

| หมวดหมู่* | คำอธิบาย |
|---|---|
| ☐ หมวดหมู่ที่ ๒ | การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance) |
| ☐ หมวดหมู่ที่ ๓ | การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยของหน่วยงาน (Non-Compliance Activity) |
| ☐ หมวดหมู่ที่ ๔ | การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic) |
| ☐ หมวดหมู่ที่ ๕ | การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion) |
| ☐ หมวดหมู่ที่ ๖ | การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion) |
| ☐ หมวดหมู่ที่ ๗ | การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service) |
| ☐ หมวดหมู่ที่ ๘ | เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating) |
| ☐ อื่น ๆ | โปรดระบุ |

* อ้างอิงหมวดหมู่ตามภาคผนวกท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ (ทั้งนี้ ภัยคุกคามหมวดหมู่ที่ ๐ ๑ และ ๙ ไม่เข้าข่ายเป็นภัยคุกคามทางไซเบอร์ที่ต้องรายงาน)

**ข๔. ข้อมูลเบื้องต้นเกี่ยวกับระบบคอมพิวเตอร์ คอมพิวเตอร์ บริการ หรือข้อมูลที่ได้รับผลกระทบ:**

สถานที่ตั้งของเครื่อง ข้อมูล หรือสินทรัพย์ที่ได้รับผลกระทบ (เช่น จังหวัด ตำบล ตึก ห้อง):

โปรดระบุ

ชื่อผู้ให้บริการเครือข่ายที่ให้บริการแก่ระบบ บริการ หรือข้อมูลที่ได้รับผลกระทบ :

โปรดระบุ

บริการของระบบ ข้อมูล หรือสินทรัพย์ที่ได้รับผลกระทบ (เช่น บริการการโอนเงิน):

โปรดระบุ

ฮาร์ดแวร์ ซอฟต์แวร์ที่ได้รับผลกระทบ (โปรดระบุรายละเอียด เช่น ผู้ผลิตหรือยี่ห้อ รุ่นของเครื่องคอมพิวเตอร์): โปรดระบุรายละเอียด

มีผลกระทบต่อการสื่อสาร (ทางโทรศัพท์ หรือ การใช้งานเครือข่าย): โปรดระบุ

รายละเอียดอื่น ๆ: โปรดระบุ

**หมวด ค: ข้อมูลการรับมือภัยคุกคาม**

**ค๑. สถานการณ์หรือการแก้ไขเหตุภัยคุกคาม (เลือกได้มากกว่า ๑ รายการ)**

☐ เพิ่งพบเหตุการณ์ ☐ อยู่ในขั้นตอนการขอความช่วยเหลือ

☐ อยู่ในขั้นตอนการสอบสวน ☐ กำลังลุกลาม

☐ อยู่ในขั้นตอนการระงับภัย ☐ สามารถระงับภัยได้แล้ว

☐ รายงานปิดเหตุการณ์ภัยคุกคามแล้ว ☐ อื่น ๆ: โปรดระบุ

**ค๒. สิ่งที่ได้ดำเนินการหรือได้แก้ไขไปแล้ว**

☐ ยังไม่ได้ดำเนินการแก้ไขใด ๆ ☐ ยกเลิกการเชื่อมต่อระบบออกจากเครือข่ายแล้ว

☐ ตรวจสอบข้อมูลจราจร (Log) แล้ว ☐ ตรวจสอบโปรแกรม (แฟ้ม binaries/.exe) แล้ว

☐ กู้คืนกลับมาด้วยระบบหรือข้อมูลสำรองที่ตรวจสอบความถูกต้องแล้ว

☐ รายละเอียดการแก้ไขภัยคุกคามที่เกิดขึ้นเพิ่มเติม: โปรดระบุ

**ค๓. รายละเอียดการรับมือภัยคุกคามอื่น ๆ (ถ้ามี)**

โปรดระบุ

**ส่วนที่ ๒**

**หมวด ง : รายละเอียดภัยคุกคาม**

**ง๑. ข้อมูลการตรวจจับและการวิเคราะห์**

**ง๑.๑ <u>วัน เวลา ที่ผู้โจมตีได้เริ่มต้นเข้าถึงระบบ</u> (System Access)**

**วันที่:** เลือกวันที่ **เวลา:** โปรดระบุ **ไม่ทราบ:** ☐

**ง๑.๒ ข้อมูลการพบเห็นเหตุภัยคุกคามทางไซเบอร์**

รายละเอียดแหล่งที่มา หรือต้นเหตุของเหตุภัยคุกคาม (เท่าที่ทราบ เช่น คน, ความผิดพลาดของระบบ, ภัยธรรมชาติ, การจู่โจม, ความผิดพลาดจากคนนอกองค์กร):

โปรดระบุ

บุคคล วิธี หรือเครื่องมือที่ตรวจพบภัยคุกคาม (เช่น ผู้ใช้, ผู้ดูแลระบบ, โปรแกรม Anti-virus, IDS, การวิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์, ไม่ทราบ):

โปรดระบุ

รายละเอียดของปัญหาลักษณะคล้ายกันที่หน่วยงานเคยพบมาก่อน (ถ้ามี โปรดระบุรายละเอียด):

โปรดระบุ

**ง๑.๓ รายละเอียดผลกระทบจากเหตุภัยคุกคาม (ระบุผลกระทบที่มีเกิดขึ้นต่อ ระบบ คน หรือข้อมูล)**

จำนวนระบบ บริการ หรือสินทรัพย์ที่เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่ได้รับผลกระทบ (โดยประมาณ): โปรดระบุ

ทรัพย์สินที่สำคัญอื่น ๆ ที่อาจได้รับผลกระทบ: โปรดระบุ

จำนวนผู้ได้รับผลกระทบ (โดยประมาณ): โปรดระบุ

มูลค่าความเสียหาย (โดยประมาณ): โปรดระบุ

ในกรณีที่ข้อมูลที่ระบุตัวบุคคลได้รั่วไหล (หรือถูกขโมย):

จำนวนบุคคลที่เป็นเจ้าของข้อมูล : โปรดระบุ

ชนิดของข้อมูล (เลือกทุกข้อที่ใช่):

☐ ข้อมูลไบโอเมตริกซ์ ☐ ข้อมูลการติดต่อ

☐ ข้อมูลการเงิน ☐ ข้อมูลบุคลากรของรัฐ

☐ หมายเลขบัตรประชาชน ☐ ข้อมูลการติดต่อกับหน่วยงานต่าง ๆ

☐ ข้อมูลทางการแพทย์

☐ อื่น ๆ : โปรดระบุ

จำนวนข้อมูล (Record) ที่ได้รับผลกระทบ: โปรดระบุ

ผลกระทบอื่น ๆ ที่เกิดขึ้น: โปรดระบุ

**๑.๔ <u>รายละเอียดของระบบ หรือข้อมูลที่ได้รับผลกระทบ (Information of Affected System)</u>**

หมายเลข CVE: โปรดระบุ

ช่องโหว่ที่ถูกใช้จู่โจม: โปรดระบุ

การใช้ระบบหรือเครื่องที่ได้รับผลกระทบเป็นฐานเพื่อจู่โจมขยายผลไปยังระบบหรือเครื่องอื่น:

โปรดระบุ

อาการหรือสิ่งผิดปกติ (เลือกได้มากกว่า ๑ รายการ)

☐ ระบบล่ม ☐ รายการข้อมูลจราจรทางคอมพิวเตอร์ที่ผิดปกติ

☐ บัญชีผู้ใช้ถูกสร้างขึ้นมาใหม่โดยไม่ทราบสาเหตุ หรือ บัญชีผู้ใช้มีความผิดปกติ

☐ การจู่โจมด้วยวิศวกรรมสังคม (Social Engineering) ทั้งที่สำเร็จและไม่สำเร็จ

☐ ประสิทธิภาพของระบบด้อยลง (ทั้งที่รู้ว่าเป็นเพราะเหตุภัยคุกคามและที่ไม่รู้สาเหตุ)

☐ การเปลี่ยนแปลงใน DNS หรือ กฎของ Router หรือกฎไฟร์วอลล์ โดยไม่ทราบสาเหตุ

☐ การยกระดับสิทธิ์การเข้าถึงระบบโดยไม่ทราบสาเหตุ

☐ การตรวจพบการทำงานของโปรแกรมหรืออุปกรณ์ Sniffer เพื่อจับการรับส่งข้อมูลภายในเครือข่าย

☐ การเข้าใช้งานครั้งสุดท้ายของผู้ใช้ที่ไม่สอดคล้องกับการใช้งานครั้งสุดท้ายที่เกิดขึ้นจริง

☐ การแจ้งเตือนจากเครื่องมือตรวจจับการบุกรุก

☐ การเข้ามาลาดตระเวน (Probing) หรือการเรียกดู (Browsing) ที่น่าสงสัย

☐ รูปแบบการใช้งานที่ผิดปกติ ☐ การเปลี่ยนแปลงขนาดไฟล์ไปจากเดิมแบบผิดปกติ

☐ ความพยายามที่จะเขียนไฟล์ของระบบ ☐ การเปลี่ยนแปลงวันที่ของไฟล์ไปจากเดิมแบบผิดปกติ

☐ การแก้ไขหรือลบข้อมูลที่ผิดปกติ ☐ การจู่โจมให้เกิดการปฏิเสธการให้บริการ (DOS, DDOS)

☐ ไฟล์ใหม่ถูกสร้างขึ้นโดยไม่ทราบสาเหตุ ☐ การใช้งานหรือมีกิจกรรมที่เกิดในเวลาที่ผิดปกติ

☐ การแก้ไขหน้าเว็บ ☐ การสร้างแฟ้มข้อมูล setuid หรือ setgid ใหม่ที่ผิดปกติเกิดขึ้น

☐ การเปลี่ยนแปลงในไดเรกทอรีและแฟ้มข้อมูลของระบบปฏิบัติการที่ผิดปกติ

☐ การตรวจพบโปรแกรมเจาะระบบ (Crack utility)

☐ สิ่งที่ผิดปกติไปจากเดิมอื่น ๆ: โปรดระบุ

**๑.๕ รายละเอียดของเหตุภัยคุกคามตามลำดับเวลา ตั้งแต่การจู่โจมครั้งแรก จนถึงปัจจุบัน (เช่น ลำดับของการจู่โจม, Attack vector, เทคนิคหรือเครื่องมือที่ผู้จู่โจมใช้ ฯลฯ)**

โปรดระบุ

**๑.๖ รายละเอียดอื่น ๆ ที่พบเกี่ยวข้องกับเหตุภัยคุกคาม:** โปรดระบุ

**๒. ข้อมูลการระงับ ปราบปราม และฟื้นฟู**

**๒.๑ รายละเอียดการดำเนินการเพื่อแก้ไขเหตุภัยคุกคาม:** โปรดระบุ

**๒.๒ การคาดการณ์ความสามารถฟื้นฟู**

โปรดระบุรายละเอียดการฟื้นฟู ทรัพยากรที่ต้องใช้และที่ต้องการเพิ่ม และประมาณระยะเวลาการฟื้นฟู

**๓. ข้อมูลกิจกรรมภายหลังการแก้ปัญหา (ถ้ามี)**

**๓.๑ วัน เวลา ที่เหตุภัยคุกคามสิ้นสุด วันที่:** เลือกวันที่ **เวลา:** โปรดระบุ

**๓.๒ การดำเนินการเพื่อป้องกันเหตุภัยคุกคามที่คล้ายคลึงกัน:** โปรดระบุ

**๓.๓ บทเรียนที่ได้จากเหตุภัยคุกคาม:** โปรดระบุ

**เอกสาร ก๓ แบบรายงานสรุปภัยคุกคามทางไซเบอร์ในหนึ่งรอบปี**

**ข้อ ๑ สถิติรายปีจำแนกตามหมวดหมู่ของภัยคุกคามทางไซเบอร์[4]**

| หมวดหมู่ | คำอธิบาย | จำนวน |
|---|---|---|
| ๐ | เหตุการณ์จำลองและการฝึกจู่โจมของหน่วยงาน (Training and Exercises) | |
| ๑ | การพยายามเข้าถึงระบบที่ไม่สำเร็จ (Unsuccessful Activity Attempt) | |
| ๒ | การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance) | |
| ๓ | การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยที่หน่วยงานกำหนด (Non-Compliance Activity) | |
| ๔ | การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic) | |
| ๕ | การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion) | |
| ๖ | การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion) | |
| ๗ | การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service) | |
| ๘ | เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating) | |
| ๙ | เหตุการณ์ผิดปกติที่ได้รับการวิเคราะห์แล้วว่าไม่ใช่เหตุการณ์ที่เป็นภัยคุกคาม (Explained Anomaly) | |

**ข้อ ๒ สถิติรายปีจำแนกตามทรัพย์สินที่ได้รับผลกระทบ**

| ทรัพย์สินที่ได้รับผลกระทบ | จำนวน |
|---|---|
| เครื่องแม่ข่าย / แอคทีฟ ไดเรกทอรี (Active Directory) | |
| เครื่องเวิร์กสเตชัน (Workstation) | |
| สวิตช์ (Switch) /เราเตอร์ (Router) | |
| เว็บไซต์ (Website) | |
| อื่น ๆ | |

**ข้อ ๓ สถิติรายปีจำแนกตามระดับภัยคุกคามทางไซเบอร์[5]**

| ระดับภัยคุกคาม | จำนวน |
|---|---|
| ไม่ร้ายแรง | |
| ร้ายแรง | |
| วิกฤต (ก) | |
| วิกฤต (ข) | |

[4] หมวดหมู่ตามข้อ ๑ ของภาคผนวกท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์ แต่ละระดับ พ.ศ.๒๕๖๔

[5] ระดับภัยคุกคามทางไซเบอร์ตามมาตรา ๖๐ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒

**ภาคผนวก ๖**

**ตัวอย่าง : รายการตรวจสอบการจัดการเหตุการณ์ (Incident Handling Checklist)**

| | **รายการตรวจสอบการจัดการเหตุการณ์** | **Complete** |
|---|---|---|
| | **ขั้นการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (detection and analysis)** | |
| ๑ | ตรวจสอบว่ามีเหตุการณ์เกิดขึ้นหรือไม่ | |
| ๑.๑ | วิเคราะห์ตรวจจับสัญญาณเหตุการณ์ความปลอดภัยทางไซเบอร์ | |
| ๑.๒ | ค้นหาข้อมูลเพิ่มเติมที่มีความสัมพันธ์กัน | |
| ๑.๓ | ดำเนินการสืบค้นข้อมูล (เช่น search engines, ฐานข้อมูลอื่น ๆ เป็นต้น) | |
| ๑.๔ | ทันทีที่ผู้จัดการรับมือฯ เหตุการณ์เชื่อว่ามีเหตุการณ์เกิดขึ้น ให้เริ่มบันทึกการสอบสวนและรวบรวมหลักฐาน | |
| ๒ | จัดลำดับความสำคัญในการจัดการเหตุการณ์ตามระดับความรุนแรงของภัยคุกคามที่เกิดขึ้น | |
| ๓ | รายงานเหตุการณ์ดังกล่าวต่อผู้บริหารและหน่วยงานภายนอกที่เกี่ยวข้อง | |
| | **ขั้นการระงับภัยคุกคาม ปราบปราม และฟื้นฟูระบบงานที่ได้รับผลกระทบ (containment, eradication, and recovery)** | |
| ๔ | บันทึกเหตุการณ์, จัดเก็บและดูแลรักษาหลักฐานเกี่ยวกับเหตุการณ์ทั้งหมดก่อนเริ่มกระบวนการกู้คืนซึ่งรวมถึงการได้มาของบันทึกการยึดหลักฐานคอมพิวเตอร์ที่ได้มา หรืออุปกรณ์อื่น ๆ เพื่อสนับสนุนการสอบสวน | |
| ๕ | จำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ | |
| ๖ | ดำเนินการสอบสวน (Investigate) สาเหตุและผลกระทบของเหตุการณ์ | |
| ๗ | ทำการกำจัดสาเหตุ (Eradicate the incident) | |
| ๗.๑ | ระบุช่องโหว่ของระบบที่โดนโจมตีและบรรเทาผลกระทบที่เกิดขึ้น | |
| ๗.๒ | กำจัด หรือลบมัลแวร์ และสาเหตุภัยคุกคามอื่นๆ | |
| ๗.๓ | หากมีการตรวจพบว่ามีระบบใหม่ได้รับผลกระทบ (เช่น การติดมัลแวร์ใหม่) ให้ทำซ้ำขั้นตอนการตรวจจับและการวิเคราะห์ภัยคุกคามทางไซเบอร์ (detection and analysis) | |
| ๘ | เรียกใช้งานกระบวนการกู้คืน (Recovery Process) | |
| ๘.๑ | ระบบที่ได้รับผลกระทบจากภัยคุกคามกลับสู่สถานะพร้อมใช้งาน | |
| ๘.๒ | ยืนยันว่าระบบที่ได้รับผลกระทบกลับมาทำงานได้ตามปกติ | |
| ๘.๓ | หากจำเป็น ให้ดำเนินการติดตามสถานการณ์ต่อไป เพื่อค้นหาเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ที่อาจเกี่ยวข้องในอนาคต | |
| | **การดำเนินการภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ (Post-Incident Activity)** | |
| ๙ | จัดทำรายงานการติดตามผล | |
| ๑๐ | จัดการประชุมทบทวนบทเรียนที่เกิดจากเหตุการณ์ดังกล่าว | |

**แหล่งที่มา**

- ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ.๒๕๖๔

- ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ.๒๕๖๔

- ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ.๒๕๖๖

- NIST SP ๘๐๐-๖๑r๒ Computer Security Incident Handling Guide

- ACSC Cyber Incident Response Plan Guidance