
# แผนรับมือภัยคุกคามทางไซเบอร์
# สำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ

กลุ่มงานสารสนเทศ สำนักดิจิทัลสิทธิมนุษยชน

# สารบัญ

หน้า

## รายละเอียดการบังคับใช้เอกสาร

| รายละเอียดของเอกสาร (Document control and review) | |
|---|---|
| ผู้จัดทำเอกสาร (Author) | สำนักดิจิทัลสิทธิมนุษยชน |
| ผู้ดำเนินการตามเอกสาร (Owner) | บุคลากรของสำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ |
| วันที่จัดทำเอกสาร (Date created) | กันยายน ๒๕๖๗ |
| ผู้ตรวจสอบความถูกต้องของเอกสาร (Last reviewed by) | หัวหน้ากลุ่มงานสารสนเทศ สำนักดิจิทัลสิทธิมนุษยชน |
| วันที่ตรวจสอบความถูกต้องของเอกสาร (Last date reviewed) | ๒๐ กันยายน ๒๕๖๗ |
| ผู้อนุมัติเอกสาร และวันที่อนุมัติเอกสาร (Endorsed by and date) | |
| วันที่จะต้องมีการตรวจสอบเอกสารครั้งถัดไป (Next review due date) | ๑ ตุลาคม ๒๕๖๘ |

| ประวัติการแก้ไขเอกสาร (Version control) | | | |
|---|---|---|---|
| **รุ่น (Version)** | **วันที่อนุมัติ (Date of Approval)** | **ผู้อนุมัติ (Approved by)** | **สถานะ (Description of change)** |
| ๑.๐ | | นายภาณุวัฒน์ ทองสุข ที่ปรึกษาสำนักงานปฏิบัติราชการแทนเลขาธิการคณะกรรมการสิทธิมนุษยชนแห่งชาติ | ฉบับประกาศใช้ |
| | | | |

**๑. หลักการและเหตุผล**

แผนรับมือกับภัยคุกคามทางไซเบอร์ สำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ (สำนักงาน กสม.) ฉบับนี้ จัดทำขึ้นเพื่อให้เป็นไปตามมาตรา ๔๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ที่กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งอย่างน้อยต้องประกอบด้วย

(๑) แผนรับมือภัยคุกคามทางไซเบอร์

(๒) แผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยผู้ตรวจประเมิน ผู้ตรวจสอบภายใน หรือผู้ตรวจสอบอิสระจากภายนอก อย่างน้อยปีละ ๑ ครั้ง

**๒. วัตถุประสงค์**

(๑) เพื่อใช้เป็นแผนในการรับมือเหตุภัยคุกคามทางไซเบอร์ที่เกิดขึ้นของสำนักงาน กสม.

(๒) เพื่อกำหนดขั้นตอนการรับมือเหตุภัยคุกคามทางไซเบอร์ และการรายงานเหตุภัยคุกคามทางไซเบอร์ เพื่อกำหนดกระบวนการในการเฝ้าระวัง ตรวจสอบ ติดตาม และแก้ไขปัญหาที่เกิดจากภัยคุกคามทางไซเบอร์

(๓) เพื่อกำหนดขั้นตอนการรับมือเหตุภัยคุกคามทางไซเบอร์ การตรวจสอบและแก้ไขเหตุจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้น

**๓. ขอบเขต**

แผนรับมือกับภัยคุกคามทางไซเบอร์ สำนักงาน กสม. ฉบับนี้ ใช้รับมือเหตุภัยคุกคามทางไซเบอร์ที่เกิดขึ้นต่อระบบสารสนเทศ และข้อมูลดิจิทัลของสำนักงาน กสม. รวมถึงบุคคล หรืออุปกรณ์ใด ๆ ซึ่งเข้าถึงระบบารสนเทศและข้อมูลดิจิทัลดังกล่าว

**๔. หน้าที่การทบทวนแผน**

สำนักดิจิทัลสิทธิมนุษยชน มีหน้าที่ทบทวนและขออนุมัติแผนรับมือกับภัยคุกคามทางไซเบอร์ สำนักงาน กสม. ต่อเลขาธิการ กสม. หรือผู้ที่เลขาธิการ กสม. มอบหมาย

**๕. หน้าที่ในการดำเนินการตามแผน**

สำนักดิจิทัลสิทธิมนุษยชน มีหน้าที่เป็นผู้รับผิดชอบหลักในการดำเนินการตามแผนรับมือกับภัยคุกคามทางไซเบอร์ สำนักงาน กสม. ประกอบด้วย กลุ่มงานพัฒนาระบบสารสนเทศและฐานข้อมูล กลุ่มงานคอมพิวเตอร์และระบบเครือข่าย และกลุ่มงานสารสนเทศ โดยมีหน่วยงานสนับสนุน คือ สำนักกฎหมาย มีหน้าที่เป็นผู้รับผิดชอบในการตรวจสอบความถูกต้องครอบคลุมตามที่กฎหมายกำหนดไว้

**๖. เอกสารและกรอบมาตรฐานที่เกี่ยวข้อง**

**๖.๑ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒**

- ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔

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

- ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ. ๒๕๖๖

- ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. ๒๕๖๖

- ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานขั้นต่ำของข้อมูลหรือระบบสารสนเทศ พ.ศ. ๒๕๖๖

- ประกาศสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง แนวทางการจัดทำแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๗

**๖.๒ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒**

- ประกาศสำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ เรื่อง นโยบายการคุ้มครองข้อมูลส่วนบุคคลของสำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ พ.ศ. ๒๕๖๔

- ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕

- ประกาศสำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของข้อมูลส่วนบุคคลของสำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ พ.ศ. ๒๕๖๗

**๖.๓ แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ**

- ประกาศสำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ พ.ศ. ๒๕๖๖

**๖.๔ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม**

- ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. ๒๕๖๔

**๗. คำนิยาม**

**แนวปฏิบัติพื้นฐาน (Security Control Baselines)** หมายถึง แนวปฏิบัติพื้นฐานที่กำหนดไว้สำหรับการดำเนินมาตรการป้องกันรับมือ ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ

**Recovery Time Objective (RTO)** หมายถึง ระยะเวลาในการกู้คืนระบบ

**Recovery Point Objective (RPO)** หมายถึง ระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย

**Maximum Tolerance Period of Disruption (MTPD)** หมายถึง ระยะเวลาสูงสุดที่ยอมให้ธุรกิจหยุดชะงัก เพื่อรองรับการดำเนินธุรกิจอย่างต่อเนื่อง และรองรับการเกิดเหตุการณ์ผิดปกติต่าง ๆ ที่อาจส่งผลให้เกิดการหยุดชะงัก หรือเกิดความเสียหายต่อระบบ เช่น ภัยคุกคาม เป็นต้น การทำงานได้ตามปกติให้เร็วที่สุด

**เหตุการณ์ (Event)** หมายถึง การเกิดขึ้นที่สังเกตได้ใด ๆ (observable occurrence) ในระบบเครือข่าย สภาพแวดล้อม กระบวนการ ลำดับการดำเนินการ หรือบุคลากร เหตุการณ์อาจมี หรือไม่มีลักษณะที่ส่งผลเชิงลบก็ได้

**เหตุภัยคุกคามทางไซเบอร์ (Cyber incident)** หมายถึง เหตุการณ์ที่มีผลเชิงลบที่เกิดจากการกระทำหรือการดำเนินการใด ๆ โดยมิชอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์ โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

**เหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญ** หมายถึง เหตุภัยคุกคามทางไซเบอร์ที่ปรากฏต่อระบบสารสนเทศ และเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามมาตรา ๔๙ ซึ่งคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติได้กำหนดลักษณะของภัยคุกคามทางไซเบอร์ไว้ตามมาตรา ๖๐ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

**ภัยคุกคามทางไซเบอร์ (Cyber threat)** หมายถึง การกระทำหรือการดำเนินการใด ๆ โดยมิชอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์ โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง รูปแบบภัยคุกคาม เช่น

**๑) มัลแวร์ (Malware)** คือ ซอฟต์แวร์ที่ออกแบบมาเพื่อทำลายหรือรบกวนระบบคอมพิวเตอร์ มัลแวร์สามารถเป็นได้ทั้งไวรัสคอมพิวเตอร์, โทรจัน, สปายแวร์, รวมถึง Ransomware เป็นต้น

**๒) ไวรัสคอมพิวเตอร์ (Computer Viruses)** คือ โปรแกรมที่สามารถเข้าไปยังระบบคอมพิวเตอร์และทำลายข้อมูล หรือทำงานไม่ถูกต้องโดยไม่ได้รับอนุญาตจากผู้ใช้งาน

**๓) โทรจัน (Trojan)** คือ ซอฟต์แวร์ที่มีเป้าหมายการดักจับเปลี่ยนแปลงแก้ไขข้อมูลซึ่งอาจส่งผลต่อความถูกต้องของข้อมูลภายในระบบสารสนเทศหรืออาจเกิดความเสียหายภายในระบบสารสนเทศได้

**๔) เวิร์ม (Worms)** คือ ซอฟต์แวร์ที่เป็นอันตรายต่อระบบสารสนเทศที่มีการเชื่อมต่อผ่านระบบเครือข่ายทั้งภายในและภายนอกโดยซอฟต์แวร์ชนิดนี้มุ่งเน้นเพื่อการโจมตี ขัดขวางการทำงานและขยายตัวส่งต่อภายในระบบเครือข่ายจนทำให้ไม่สามารถใช้งานระบบสารสนเทศได้

**๕) สปายแวร์ (Spyware)** คือ ซอฟต์แวร์ประสงค์ร้ายที่ทำงานอย่างลับ ๆ บนคอมพิวเตอร์และรายงานกลับไปยังผู้ใช้ระยะไกล โดยสปายแวร์มุ่งเน้นเพื่อขโมยข้อมูลทางการเงินหรือข้อมูลส่วนบุคคล

**๖) แอดแวร์ (Adware)** คือ ซอฟต์แวร์ที่รวบรวมข้อมูลการใช้งานระบบคอมพิวเตอร์และจัดเตรียมโฆษณาให้กับเป้าหมาย ถึงแม้ว่าแอดแวร์อาจไม่เป็นอันตราย แต่ในบางกรณีแอดแวร์อาจทำให้เกิดปัญหากับระบบสารสนเทศได้ ซึ่งแอดแวร์สามารถเปลี่ยนแปลงเส้นทางการเข้าถึงเว็บไซต์ไปสู่เว็บไซต์ที่ไม่ปลอดภัยได้

**๗) ซอฟต์แวร์เรียกค่าไถ่ (ransomware)** คือ มัลแวร์ชนิดหนึ่ง ที่มีพฤติกรรมเข้ารหัสไฟล์ต่าง ๆ ที่อยู่บนเครื่องคอมพิวเตอร์ไม่ว่าจะเป็นไฟล์เอกสาร รูปภาพ วิดีโอ ผู้ใช้งานจะไม่สามารถเปิดไฟล์ใด ๆ ได้เลย หากไฟล์เหล่านั้นถูกเข้ารหัส ซึ่งการถูกเข้ารหัสก็หมายความว่าจะต้องใช้คีย์ในการปลดล็อคเพื่อกู้ข้อมูลคืนมา ผู้ใช้งานจะต้องทำการจ่ายเงินตามข้อความ "เรียกค่าไถ่" ที่ปรากฏ

**๘) ประตูหลัง (Backdoor)** คือ ช่องทางพิเศษที่ใช้เข้าถึงระบบงานคอมพิวเตอร์โดยที่ไม่ต้องผ่านการพิสูจน์ทราบตัวตน ซึ่งส่วนใหญ่เมื่อผู้บุกรุกสามารถเจาะเข้าระบบได้แล้ว ก็จะสร้างประตูหลังเอาไว้เพื่อใช้ในการบุกรุกเข้าสู่ระบบงานคอมพิวเตอร์ในภายหลัง

**๙) รูตคิต (Rootkit)** คือ โปรแกรมที่ถูกพัฒนาขึ้นมาเพื่อควบคุมระบบหรือขโมยข้อมูลที่อยู่ในระบบคอมพิวเตอร์ ทั้งนี้ นอกจากใช้สำหรับบุกรุกเข้าสู่ระบบงานแล้ว Rootkit ยังอาจใช้เพื่อดูแลหรือตรวจสอบระบบคอมพิวเตอร์ได้ด้วย

**๑๐) การเจาะระบบ (Hacking)** คือ การเข้าถึงระบบคอมพิวเตอร์หรือเครือข่ายโดยไม่ได้รับอนุญาต ซึ่งอาจทำโดยการใช้ช่องโหว่ในระบบหรือเทคนิคการบริหารจัดการผิดกฎหมาย

**๑๑) การโจมตีรหัสผ่าน (Brute Force Attacks)** คือ การโจมตีที่พยายามลองเข้าถึงระบบหรือบัญชีโดยใช้คำสั่งที่เป็นไปได้ทั้งหมด

**๑๒) การปิดกั้นบริการ (Denial of Service - DoS)** คือ การโจมตีที่เป็นการส่งข้อมูลมาที่เครือข่ายหรือระบบคอมพิวเตอร์เพื่อทำให้ระบบนั้นไม่สามารถให้บริการได้

**๑๓) การปลอมแปลงตัวตน (Identity Theft)** คือ การใช้ข้อมูลส่วนตัวของบุคคลอื่น ๆ โดยไม่ได้รับอนุญาตเพื่อข้อประโยชน์ต่าง ๆ อาจทำให้เกิดความเสียหายต่อบุคคลนั้น

**๑๔) การปลอมแปลงข้อมูล (Data Manipulation)** คือ การเข้าถึงข้อมูลและปรับเปลี่ยนข้อมูลให้เป็นไปตามที่ผู้โจมตีต้องการ โดยที่ผู้ใช้ไม่ทราบ

**๑๕) การปฏิบัติที่ไม่เหมาะสม (Cyberbullying)** คือ การใช้เทคโนโลยีสารสนเทศและการสื่อสารในการก่อกวนหรือก่อกวนผู้อื่นออนไลน์

**๑๖) การล่อลวง (Phishing)** คือ การปลอมแทรกช่องทางสื่อสารอย่างอีเมลหรือเว็บไซต์เพื่อล่อให้ผู้ใช้เผยข้อมูลส่วนตัวหรือข้อมูลบัญชี

**๑๗) การละเมิดความเป็นส่วนตัว (Privacy Breaches)** คือ การเข้าถึงหรือใช้ข้อมูลส่วนตัวของบุคคลโดยไม่ได้รับอนุญาตหรือไม่ถูกต้อง

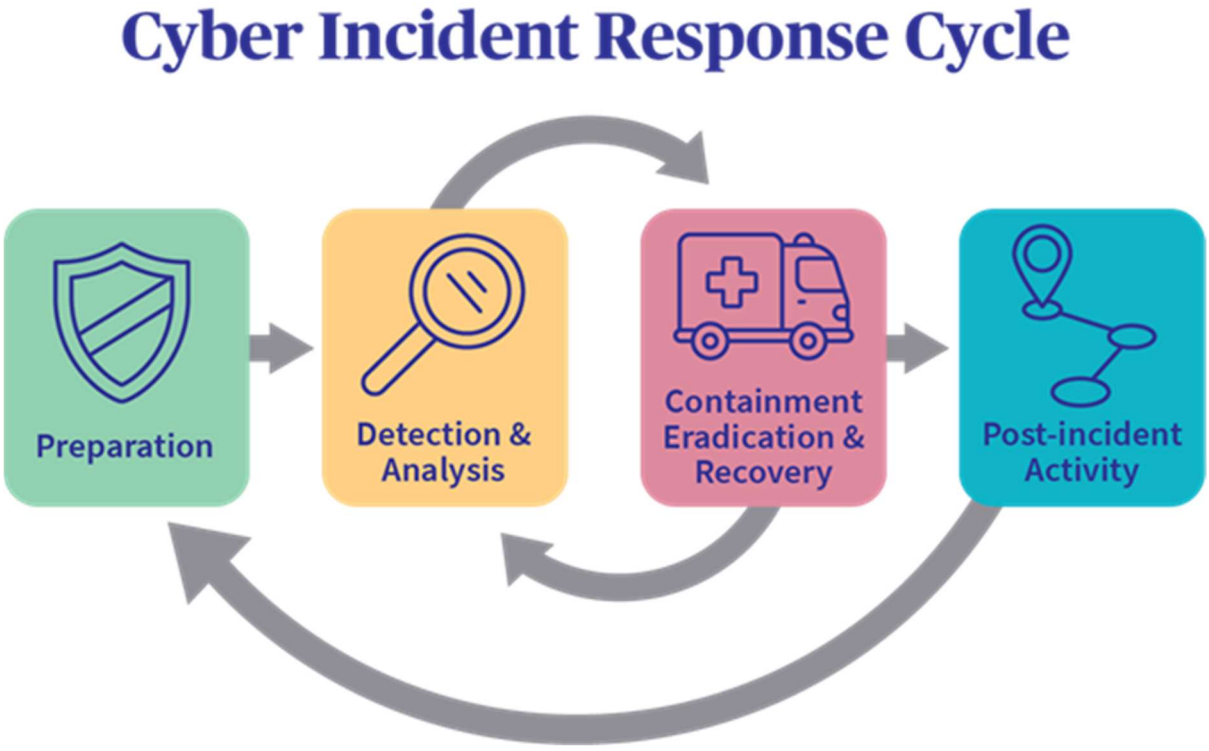
**๑๘) ข้อมูลรั่วไหล (Data leaks)** การที่ข้อมูลที่ละเอียดอ่อนหรือข้อมูลที่เป็นความลับถูกเปิดเผยโดยไม่ได้ตั้งใจบนอินเทอร์เน็ตหรือรูปแบบอื่นใด การนำข้อมูลออกอาจบันทึกผ่าน Flash drive External Hard disk หรือผ่านเครื่องคอมพิวเตอร์พกพาและเกิดการสูญหายซึ่งอาจเกิดความเสี่ยงที่ผู้ไม่หวังดีสามารถเข้าถึงข้อมูลที่ละเอียดอ่อนได้

**๑๙) บอทเน็ต (Botnet)** คือ กลุ่มของอุปกรณ์ที่ติดมัลแวร์และถูกเปลี่ยนเป็น Bot (ย่อมาจาก Robot) ไม่ว่าจะเป็นอุปกรณ์คอมพิวเตอร์ เว็บแคม เราท์เตอร์ หรืออุปกรณ์ IoT อื่น ๆ เพื่อรอรับคำสั่งจากผู้บุกรุก (Hacker) โดยผู้บุกรุก (Hacker) จะนำ Botnet ที่มีไปใช้ในการโจมตีขนาดใหญ่ เช่น การทำ DDoS เป็นต้น

**๒๐) การดักจับข้อมูลในเครือข่าย (Sniffing)** คือ การดักข้อมูลที่ส่งจากคอมพิวเตอร์เครื่องหนึ่งไปยังอีกเครื่องหนึ่ง หรือจากเครือข่ายหนึ่งไปยังอีกเครือข่ายหนึ่ง ซึ่งถือว่าเป็นการโจมตีรูปแบบหนึ่งผู้บุกรุกระบบนิยมใช้

## ๘. ขั้นตอนการรับมือกับภัยคุกคามทางไซเบอร์ (Cyber Incident Response Cycle)

แผนรับมือฯ ฉบับนี้ ประกอบด้วยขั้นตอนการรับมือเหตุภัยคุกคามทางไซเบอร์ในประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔, ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ และประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ. ๒๕๖๖ รวมถึงนโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของสำนักงาน กสม. ดังนี้




**๘.๑ ขั้นเตรียมความพร้อม (Preparation)**

สำนักงาน กสม. จะดำเนินการจัดทำมาตรการเพื่อเตรียมการและป้องกันการเกิดภัยคุกคามทางไซเบอร์ (preparation) เพื่อเตรียมความพร้อมเมื่อต้องเผชิญเหตุ ได้แก่ การจัดเตรียมข้อมูลให้พร้อม การจัดตั้งและฝึกอบรมบุคลากรหรือทีมงาน การจัดหาเครื่องมือและทรัพยากรต่าง ๆ ที่จำเป็น การตั้งค่าระบบต่าง ๆ ให้ปลอดภัย การจัดทำนโยบาย แผนงาน และกระบวนการที่เกี่ยวข้อง รวมถึงการสร้างเครือข่ายความร่วมมือ โดยดำเนินการดังต่อไปนี้

๑) กำหนดโครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT) (รายละเอียดตามภาคผนวก ข)

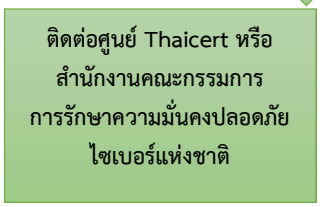
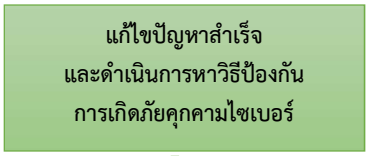
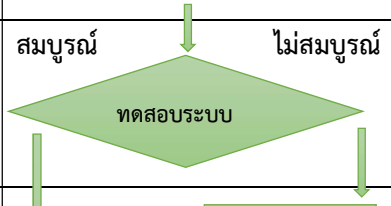
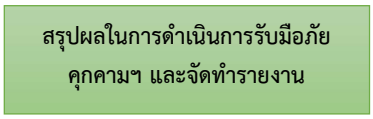
๒) กำหนดโครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure)

| ลำดับ | ผู้เกี่ยวข้อง | หน้าที่ |
|---|---|---|
| ๑ | ผู้ที่ได้รับผลกระทบจาก Incident (Incident Reporter) | แจ้งเหตุ หรือรายงานด้านความมั่นคงปลอดภัยไซเบอร์ที่พบหรือสงสัยว่ามีภัยคุกคามเกิดขึ้น |
| ๒ | ผู้รับแจ้งเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ภายในสำนักงาน กสม. | รับแจ้งเหตุหรือรับรายงานด้านความมั่นคงปลอดภัยไซเบอร์ |

| ลำดับ | ผู้เกี่ยวข้อง | หน้าที่ |
|---|---|---|
| ๓ | ทีมรับมือและตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ | ๑. รับมือและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์<br>๒. ให้คำแนะนำปรึกษาบุคลากรที่เกี่ยวกับจุดอ่อน การป้องกัน ข้อควรระมัดระวังและแจ้งเตือนภัยคุกคามที่เกิดใหม่ให้เจ้าหน้าที่ในหน่วยงาน<br>๓. มีส่วนร่วมกับหน่วยงานภายนอกองค์กร เช่น ThaiCERT เพื่อแบ่งปันข้อมูลข่าวสารด้านภัยคุกคามทางไซเบอร์ เพื่อป้องกัน และตอบสนองภัยคุกคามได้เร็วขึ้น |
| ๔ | ทีมเฝ้าระวังและวิเคราะห์การแจ้งเตือน Incident | ๑. เฝ้าระวังและวิเคราะห์การแจ้งเตือนภัยคุกคามจากอุปกรณ์ตรวจจับ<br>๒. ให้คำแนะนำปรึกษาบุคลากรที่เกี่ยวกับจุดอ่อน การป้องกัน ข้อควรระมัดระวัง และแจ้งเตือนภัยคุกคามที่เกิดใหม่ให้เจ้าหน้าที่ในหน่วยงาน<br>๓. มีส่วนร่วมกับหน่วยงานภายนอกองค์กร เช่น ThaiCERT เพื่อแบ่งปันข้อมูลข่าวสารด้านภัยคุกคามทางไซเบอร์ เพื่อป้องกัน และตอบสนองภัยคุกคามได้เร็วขึ้น |
| ๕ | ผู้บริหาร | รับผิดชอบการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา จัดหา และสนับสนุนงบประมาณสำหรับค่าใช้จ่าย ตลอดจนติดตาม กำกับ ดูแล ควบคุมเจ้าหน้าที่เกี่ยวกับการป้องกันความมั่นคงปลอดภัยไซเบอร์ |

๓) กำหนดเกณฑ์และขั้นตอนในการเรียกใช้งาน (Activate) การตอบสนองต่อเหตุการณ์และ CIRT

| ลำดับ | ขั้นตอน | รายละเอียด |
|---|---|---|
| ๑ | **ตรวจพบภัยคุกคามทางไซเบอร์** | - ผู้ใช้งานแจ้งเหตุภัยคุกคามทางไซเบอร์ หรือตรวจพบพฤติกรรมที่เป็นภัยคุกคามทางไซเบอร์จากอุปกรณ์ป้องกันระบบเครือข่ายหรือเครื่องมือด้านความปลอดภัยต่าง ๆ<br>- เจ้าหน้าที่ไอทีเฝ้าระวังและตรวจสอบเหตุการณ์ด้านความมั่นคงปลอดภัย (Detection) |
| ๒ | **ตรวจสอบภัยคุกคามทางไซเบอร์** | ตรวจสอบข้อมูลของภัยคุกคามทางไซเบอร์ (analysis) และประเมินระดับภัยคุกคามตามที่กำหนดในพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๖๐ |
| ๓ | **ควบคุมภัยคุกคามทางไซเบอร์** | ดำเนินการควบคุมภัยคุกคามทางไซเบอร์ (containment) ให้ส่งผลกระทบน้อยที่สุด และป้องกันไม่ให้เกิดการแพร่กระจายไปยังส่วนอื่น ๆ ซึ่งในกรณีที่เร่งด่วน สำนักงาน กสม. จะทำการปิดระบบหรือตัดการเชื่อมต่อของระบบคอมพิวเตอร์ชั่วคราว |

| ลำดับ | ขั้นตอน | รายละเอียด |
|---|---|---|
| ๔ |  | ดำเนินการแก้ไข (eradication) หรือกำจัดภัยคุกคามทางไซเบอร์ในเบื้องต้นในทันที |
| ๕ |  | ในกรณีที่ไม่สามารถแก้ไขปัญหาได้จะดำเนินการติดต่อศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (Thaicert) หรือสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เพื่อขอคำแนะนำหรือขอความช่วยเหลือ |
| ๖ |  | หลังจากแก้ไขปัญหาภัยคุกคามไซเบอร์สำเร็จแล้ว สำนักงาน กสม. จะบันทึกเหตุภัยคุกคามและดำเนินการประชุมเพื่อสรุปผลและหาวิธีป้องกัน/ตรวจหาช่องโหว่และหาวิธีการป้องกันการเกิดภัยคุกคามไซเบอร์ในลักษณะเดิม |
| ๗ |  | ตรวจสอบการทำงานของโครงสร้างพื้นฐานสำคัญทางสารสนเทศว่าสามารถทำงานได้สมบูรณ์หรือไม่ ในกรณีที่พบว่าการทำงานไม่สมบูรณ์หรือข้อมูลสำคัญสูญหายไปจะดำเนินการกู้คืนระบบงาน |
| ๘ |  | ดำเนินการตามขั้นตอนการกู้คืนข้อมูลตามที่ระบุในแผนการสำรองและกู้คืนระบบ ในกรณีที่กู้คืนระบบไม่ได้ สำนักงาน กสม. จะพิจารณาเปิดใช้ระบบงานคอมพิวเตอร์สำรองและเร่งกู้ระบบงานคอมพิวเตอร์หลัก |
| ๙ |  | เมื่อโครงสร้างพื้นฐานสำคัญและระบบเทคโนโลยีสารสนเทศของสำนักงาน กสม. สามารถทำงานได้เป็นปกติแล้ว หน่วยงานที่ดูแลรับผิดชอบด้านโครงข่ายระบบสารสนเทศของ สำนักงาน กสม. จะดำเนินการสรุปผลในการดำเนินการรับมือภัยคุกคามไซเบอร์ |
| ๑๐ |  | สรุปผลในการรับมือภัยคุกคามทางไซเบอร์ และแจ้งผลการดำเนินงานให้แก่ผู้เกี่ยวข้อง เช่น ผู้บริหารระดับสูงด้านสารสนเทศ เลขาธิการ กสม. เป็นต้น |

๔) จัดเตรียมข้อมูลและอุปกรณ์ (ข้อมูลการติดต่อและอุปกรณ์ติดต่อสื่อสารของบุคลากร) รวมถึงช่องทางในการติดต่อสื่อสารที่จำเป็น ได้แก่

๔.๑) รายชื่อและช่องทางการติดต่อของผู้ที่เกี่ยวข้องและประสานงานในการรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์

๔.๒) ช่องทางการรายงานเหตุการณ์ ให้ผู้ได้รับผลกระทบ หรือพบเห็นเหตุการณ์

๔.๓) ช่องทางการรายงานและติดตามข้อมูลสถานการณ์ดำเนินการของเหตุการณ์ที่ได้รับแจ้ง

๕) จัดเตรียมอุปกรณ์, ซอฟต์แวร์ และแหล่งข้อมูลสำหรับวิเคราะห์เหตุภัยคุกคามทางไซเบอร์ เช่น ระบบจัดเก็บและวิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์ การรวบรวมข่าวกรองเกี่ยวกับภัยคุกคามทางไซเบอร์ (Threat Intelligence) เป็นต้น

๖) จัดให้มีการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของสำนักงาน กสม. (Risk Assessment)

๗) จัดทำแผนผังโครงสร้างขั้นตอนการรับมือฯ ของสำนักงาน กสม. (รายละเอียดตามภาคผนวก ข)

๘) ดำเนินการตามแนวปฏิบัติพื้นฐาน (Security Control Baselines) เพื่อเตรียมการและป้องกันการเกิดภัยคุกคามทางไซเบอร์ (Preparation) ดังนี้

| แนวปฏิบัติ | รายละเอียด |
|---|---|
| ๑) การเตรียมพร้อมด้านบุคลากร | (๑) จัดฝึกอบรมสร้างความรู้ความเข้าใจเกี่ยวกับภัยคุกคามทางไซเบอร์และวิธีการตอบสนองและแจ้งเหตุเบื้องต้นเมื่อมีเหตุการณ์ผิดปกติ รวมถึงสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยให้กับเจ้าหน้าที่ (Awareness Training) เช่น การใช้รหัสผ่านที่มีความปลอดภัย เป็นต้น<br>(๒) การใช้เหตุการณ์และการจำลองเหตุการณ์ เพื่อสร้างสถานการณ์ที่เป็นไปได้ของการโจมตีและการรับมือกับภัยคุกคาม เพื่อสร้างความเข้าใจและทักษะในการตอบสนองต่อภัยคุกคามทางไซเบอร์<br>(๓) ดำเนินการแจ้งรายชื่อเจ้าหน้าที่สำหรับประสานงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตราที่ ๔๖ กำหนดให้หน่วยงานภาครัฐแจ้งรายชื่อเจ้าหน้าที่ระดับบริหารและระดับปฏิบัติการเพื่อประสานงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ไปยังสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ |
| ๒) การป้องกันมัลแวร์ / ป้องกันไวรัส /สปายแวร์ | การป้องกันมัลแวร์ (malware) / ไวรัส (viruses) / สปายแวร์ (spyware) เป็นส่วนสำคัญของแนวปฏิบัติพื้นฐานด้านความปลอดภัย โดยมีแนวทางในการป้องกัน ดังนี้<br>(๑) ใช้โปรแกรมแอนตี้ไวรัสและโปรแกรมป้องกันมัลแวร์ที่เชื่อถือได้เพื่อสแกนและตรวจจับภัยคุกคามทางไซเบอร์<br>(๒) อัปเดตซอฟต์แวร์และระบบปฏิบัติการอย่างสม่ำเสมอ จากผู้ผลิตซอฟต์แวร์เพื่อแก้ไขช่องโหว่ด้านความปลอดภัย<br>(๓) ประเมินและควบคุมสิทธิ์การเข้าถึงเครื่องคอมพิวเตอร์และข้อมูลที่สำคัญ เพื่อป้องกันการเข้าถึงที่ไม่ได้รับอนุญาต<br>(๔) ใช้การเข้ารหัสข้อมูลเมื่อส่งข้อมูลผ่านเครือข่าย เพื่อป้องกันการรั่วไหลข้อมูลจากการถูกโจมตี<br>(๕) ติดตั้งซอฟต์แวร์เพื่อตรวจสอบและคัดกรองอีเมล เพื่อป้องกันการติดเชื้อไวรัสผ่านทางอีเมล<br>(๖) การสร้างการสำรองข้อมูลและการคืนค่าข้อมูล เพื่อให้สามารถกู้คืนข้อมูลได้ในกรณีที่ข้อมูลถูกทำลายจากมัลแวร์หรือการโจมตีอื่น ๆ |

| แนวปฏิบัติ | รายละเอียด |
| --- | --- |
| ๓) ไฟร์วอลล์และอุปกรณ์ป้องกันการบุกรุก (IPD) | แนวปฏิบัติพื้นฐาน (Security Control Baselines) สำหรับไฟร์วอลล์และอุปกรณ์ป้องกันการบุกรุก (Intrusion Prevention Devices - IPDs) เป็นส่วนสำคัญในการปกป้องระบบและข้อมูลจากการโจมตีและการบุกรุก โดยมีแนวทางในการปฏิบัติ ดังนี้<br>(๑) ติดตั้งและกำหนดค่าไฟร์วอลล์และอุปกรณ์ป้องกันการบุกรุกให้เหมาะสมกับโครงสร้างและความต้องการของระบบเครือข่าย<br>(๒) ตั้งค่าไฟร์วอลล์และอุปกรณ์ IPD เพื่อตรวจจับและป้องกันการบุกรุกที่เข้ามาในระบบ เช่น การบล็อกการเชื่อมต่อที่ไม่ได้รับอนุญาต<br>(๓) อัปเดตและดูแลซอฟต์แวร์ โดยติดตั้งแพทช์เป็นประจำ เพื่อป้องกันการใช้ช่องโหว่เพื่อเข้าถึงระบบ<br>(๔) ตั้งค่าไฟร์วอลล์และอุปกรณ์ IPD ให้มีการจัดเก็บ Log ที่เกี่ยวข้อง เช่น การบุกรุก, การสแกนพอร์ต, และการเข้าถึงที่ไม่ได้รับอนุญาต<br>(๕) ปรับแต่งการตั้งค่าและเพิ่มความสามารถใหม่ ๆ ของอุปกรณ์เพื่อเสริมความปลอดภัยและป้องกันการโจมตีที่เพิ่มขึ้น<br>(๖) ทดสอบความเข้มแข็งและประสิทธิภาพของไฟร์วอลล์ และอุปกรณ์ IPD โดยประมาณการโจมตีและการทดสอบการป้องกัน<br>(๗) ฝึกอบรมบุคลากรเกี่ยวกับการใช้งานและการดูแลรักษาอุปกรณ์ไฟร์วอลล์และอุปกรณ์ IPD<br>(๘) วิเคราะห์ข้อมูลที่ได้รับจากไฟร์วอลล์และอุปกรณ์ IPS เพื่อตรวจสอบและปรับปรุงมาตรการต่างๆ ตามความเหมาะสม |
| ๔) มาตรการรักษาความปลอดภัยบุคลากร | การรักษาความปลอดภัยบุคลากร เพื่อป้องกันการเข้าถึงไม่พึงประสงค์และการละเมิดความเป็นส่วนตัวของข้อมูล โดยมีแนวทางในการปฏิบัติ ดังนี้<br>(๑) ตรวจสอบประวัติของบุคลากรที่มีการเข้าร่วมในองค์กร เช่น ประวัติการทำงาน ประวัติส่วนตัว ประวัติการศึกษา และประสบการณ์ทำงาน<br>(๒) จัดการสิทธิ์การเข้าถึงข้อมูลและระบบของบุคลากร โดยให้เข้าถึงข้อมูลและระบบที่เกี่ยวข้องเพียงเท่าที่จำเป็นตามหน้าที่ความรับผิดชอบ<br>(๓) จัดการฝึกอบรมและการประเมินความเข้าใจเกี่ยวกับนโยบายและมาตรการความปลอดภัย โดยให้บุคลากรรับทราบและปฏิบัติตามนโยบายของหน่วยงาน<br>(๔) ใช้เทคโนโลยีที่มีการรักษาความปลอดภัยอย่างเหมาะสม เช่น การใช้ระบบควบคุมการเข้าถึงและการตรวจสอบตัวตนที่เข้มงวด |

| แนวปฏิบัติ | รายละเอียด |
| --- | --- |
| | (๕) สร้างวัฒนธรรมความปลอดภัยในองค์กรโดยให้ความสำคัญกับความตระหนักและความรับผิดชอบในการรักษาความปลอดภัยไซเบอร์<br>(๖) ตรวจสอบการดำเนินการของบุคลากรในการใช้งานระบบเครือข่ายเพื่อตรวจจับและป้องกันกิจกรรมที่ไม่พึงประสงค์หรือเป็นอันตราย<br>(๗) รักษาความลับและข้อมูลที่มีค่าขององค์กรโดยให้สิทธิ์การเข้าถึงเฉพาะบุคคลที่มีความจำเป็นเท่านั้น |
| ๕) มาตรการรักษาความปลอดภัยทางกายภาพ | ความปลอดภัยทางกายภาพมีความสำคัญอย่างมากในการป้องกันการเข้าถึงที่ไม่เหมาะสมหรือที่ไม่ถูกต้อง และการละเมิดความเป็นส่วนตัวของข้อมูล โดยมีแนวทางในการปฏิบัติ ดังนี้<br>(๑) การเข้าถึงและควบคุมการเข้าออก ต้องมีการจัดระบบการเข้าถึงและควบคุมการเข้าออกของบุคคลและพาหนะที่เข้าสู่พื้นที่ที่มีข้อมูลสำคัญหรืออุปกรณ์ที่มีความสำคัญ<br>(๒) ใช้ระบบการรักษาความปลอดภัย เช่น การติดตั้งกล้องวงจรปิด (CCTV) เพื่อเฝ้าสังเกตและบันทึกการเข้าถึง<br>(๓) มีการรักษาความลับของข้อมูลและอุปกรณ์ที่มีความลับอย่างเข้มงวด เช่น การใช้ตู้เซฟหรือการรักษาคีย์การ์ด<br>(๔) ตรวจสอบและควบคุมสิทธิ์การเข้าถึงพื้นที่ที่มีความสำคัญ และมีการตรวจสอบเพื่อป้องกันการเข้าถึงที่ไม่ได้รับอนุญาต<br>(๕) มีการแนะนำบุคลากรของหน่วยงานให้มีความเข้าใจและปฏิบัติตามมาตรฐานของหน่วยงานเกี่ยวกับมาตรการความปลอดภัยทางกายภาพและระบบรักษาความปลอดภัย |
| ๖) การบันทึกเหตุการณ์ | การบันทึกเหตุการณ์ (Event Logs) เพื่อการตรวจสอบและการตรวจสอบกิจกรรมที่เกิดขึ้นในระบบขององค์กร โดยมีแนวทางในการปฏิบัติ ดังนี้<br>(๑) กำหนดขอบเขตและประเภทของเหตุการณ์ที่ควรถูกบันทึก เช่น เหตุการณ์เครือข่าย, เหตุการณ์ระบบ, เหตุการณ์การเข้าถึง ฯลฯ<br>(๒) ตรวจสอบและควบคุมความสมบูรณ์และความถูกต้องของบันทึกเหตุการณ์ เพื่อให้แน่ใจว่ามีข้อมูลที่เพียงพอและถูกต้องสำหรับการวิเคราะห์<br>(๓) จัดเก็บข้อมูลบันทึกเหตุการณ์ในที่ปลอดภัยและมีระบบ เพื่อป้องกันการสูญหายหรือการแก้ไขข้อมูล<br>(๔) ตรวจสอบและวิเคราะห์ข้อมูลบันทึกเหตุการณ์อย่างสม่ำเสมอเพื่อตรวจจับกิจกรรมที่ไม่เหมาะสมหรือไม่ปกติ |

| แนวปฏิบัติ | รายละเอียด |
|---|---|
| | (๕) จัดทำรายงานและแจ้งเตือนสำหรับเหตุการณ์ที่มีความสำคัญหรือเหตุการณ์ที่ต้องการดำเนินการต่อเนื่อง<br>(๖) ควบคุมการเข้าถึงข้อมูลบันทึกเหตุการณ์โดยให้สิทธิ์เฉพาะบุคคลที่มีความจำเป็น และมีหน้าที่เกี่ยวข้องเท่านั้น<br>(๗) วิเคราะห์และทำนายแนวโน้มจากข้อมูลบันทึกเหตุการณ์เพื่อการระบุและการป้องกันก่อนที่จะเกิดเหตุการณ์เชิงรุก |
| ๗) การแพตช์/อัปเดต | การแพตช์และอัปเดตเป็นส่วนสำคัญของแนวปฏิบัติพื้นฐานด้านความปลอดภัย (Security Control Baselines) เพื่อให้ระบบและโปรแกรมในองค์กรมีความปลอดภัยอยู่เสมอ โดยมีแนวทางในการปฏิบัติ ดังนี้<br>(๑) ติดตามและสแกนช่องโหว่ที่เกิดขึ้นในระบบและซอฟต์แวร์เพื่อตรวจจับและแก้ไขปัญหาที่เกิดขึ้นอย่างสม่ำเสมอ<br>(๒) ประเมินความเสี่ยงของช่องโหว่ที่พบ และดำเนินการอัปเดตเพื่อควบคุมความเสี่ยงอย่างเหมาะสม<br>(๓) ตั้งค่าระบบให้มีการอัปเดตอัตโนมัติเพื่อให้มั่นใจว่าระบบมีแพตช์ล่าสุดสามารถป้องกันช่องโหว่ที่เป็นภัยคุกคามได้<br>(๔) ทดสอบแพตช์ใหม่ในระบบทดสอบก่อนการใช้งานจริงเพื่อป้องกันปัญหาที่อาจเกิดขึ้น และพิจารณาการติดตั้งแพตช์ใหม่ให้กับระบบที่ใช้งานจริง<br>(๕) สร้างกระบวนการสำหรับการแพตช์และการอัปเดตเพื่อให้เป็นไปตามมาตรฐานและนโยบายขององค์กร |

**๘.๒ ขั้นตอนการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (Detection & Analysis)**

**๘.๒.๑ สำนักงาน กสม. จะดำเนินการในการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์** ซึ่งเป็นสิ่งจำเป็นที่จะช่วยให้หน่วยงานสามารถบรรเทาความเสี่ยงที่ยังคงเหลืออยู่ และสามารถแจ้งเตือนได้อย่างทันท่วงทีเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น โดยดำเนินการดังต่อไปนี้

๑) จัดทำแนวทางรับมือเมื่อเกิดการโจมตีรูปแบบทั่วไปที่เคยเกิดขึ้นหรืออาจเกิดขึ้นกับหน่วยงาน (Common Attack Vectors/ Common Threat Vectors) ดังนี้

| ประเภทการโจมตี | อธิบายลักษณะการโจมตี | วิธีการรับมือ |
|---|---|---|
| การโจมตีอุปกรณ์แบบถอดได้ | การโจมตีอุปกรณ์แบบถอดได้หรืออุปกรณ์ต่อพ่วง ตัวอย่างเช่น โค้ดที่ | - ให้สแกนเพื่อหาไวรัสจากสื่อบันทึกข้อมูลต่าง ๆ เช่น สื่อบันทึกพกพา |

| ประเภทการโจมตี | อธิบายลักษณะการโจมตี | วิธีการรับมือ |
|---|---|---|
| (External/Removable Media) | เป็นอันตรายแพร่กระจายไปยังระบบจากแฟลชไดรฟ์ที่ติดไวรัส | (Flash Drive) และ External Hard Disk เป็นต้น ก่อนใช้งานทุกครั้ง<br>- กรณีพบไฟล์แปลกปลอมหรือพบความผิดปกติของไฟล์ให้แจ้งเจ้าหน้าที่ไอทีทราบโดยเร็ว |
| การพยายามเข้าถึงระบบที่ไม่สำเร็จ (Unsuccessful Activity Attempt) | การพยายามเข้าถึงระบบที่ไม่สำเร็จหลายครั้ง (ผู้ใช้จำรหัสผ่านไม่ได้)<br>การพยายามโดยเจตนาเพื่อเข้าถึง Information System (IS) โดยไม่ได้รับอนุญาต (ผู้โจมตีพยายามสุ่มชื่อผู้ใช้และรหัสผ่านเพื่อเข้าระบบ) | ดำเนินการตรวจสอบ Log จากระบบ Firewall เพื่อตรวจสอบและวิเคราะห์ภัยเหตุการณ์ความผิดปกติซึ่งอาจเป็นภัยคุกคาม เพื่อป้องกันความเสี่ยงที่อาจเกิดขึ้นได้ |
| การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance) | กิจกรรมที่พยายามรวบรวมข้อมูลที่ใช้เพื่อระบุลักษณะของ IS, แอปพลิเคชัน, เครือข่ายข้อมูลของหน่วยงาน และผู้ใช้ที่อาจมีประโยชน์ในการกำหนดการโจมตี ซึ่งรวมถึงกิจกรรมต่าง ๆ เช่น การทำแผนที่เครือข่ายข้อมูลของหน่วยงาน อุปกรณ์และแอปพลิเคชัน IS การเชื่อมต่อระหว่างกัน และผู้ใช้หรือโครงสร้างการรายงาน กิจกรรมนี้ไม่ส่งผลให้เกิดการประนีประนอมโดยตรง | ดำเนินการบล็อก IP ต้นทาง หลังจากนั้นทำการสร้าง Rule เพื่อบล็อกการ Scan ระบบเครือข่าย หลังจากนั้นจะทำการรวบรวมหลักฐานของเหตุการณ์ Scan ระบบเครือข่ายเพื่อนำไปสร้างรายงานและองค์ความรู้ |
| การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยที่หน่วยงานกำหนด (Non-Compliance Activity) | ความเสี่ยงที่เกิดขึ้นกับระบบสารสนเทศ (IS) อาจมาจากการกระทำหรือการละเลยของผู้ใช้งานที่ได้รับอนุญาต ตัวอย่างของพฤติกรรมที่เป็นต้นเหตุของความเสี่ยงนี้ ได้แก่ การละเลยไม่อัปเดตแพทช์ความปลอดภัย, การไม่ติดตั้งซอฟต์แวร์ป้องกันไวรัส, การติดตั้งแอปพลิเคชันที่มีช่องโหว่ความปลอดภัย, หรือการไม่ปฏิบัติตามนโยบายของสำนักงาน กสม. | - หมั่นตรวจสอบและอัปเดตแพทช์ความปลอดภัยความปลอดภัยอย่างสม่ำเสมอ |

| ประเภทการโจมตี | อธิบายลักษณะการโจมตี | วิธีการรับมือ |
|---|---|---|
| | พฤติกรรมดังกล่าวส่งผลให้เกิดช่องโหว่ที่อาจนำไปสู่การโจมตีทางไซเบอร์ และเป็นต้นเหตุของความเสียหายต่อระบบสารสนเทศและข้อมูลสำคัญ | |
| การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic) | เป็นเหตุการณ์ที่เครื่องคอมพิวเตอร์ลูกข่าย หรือเครื่องคอมพิวเตอร์แม่ข่ายของสำนักงาน กสม. ถูกบุกรุกโดยการใช้มัลแวร์ (Malicious Logic) หรือชุดคำสั่งไม่พึงประสงค์ตามวรรคหนึ่ง หมายถึงชุดคำสั่งที่มีผลทำให้ข้อมูลคอมพิวเตอร์ หรือ ระบบคอมพิวเตอร์ หรือ ชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่ง อาทิ เช่น Virus, Worm, Trojan, Spyware, Ransomware, Backdoor หรือ Rootkit เป็นต้น โดยเหตุการณ์นั้นส่งผลกระทบการใช้งานที่เป็นปกติ หรือกระทบกับเครื่องคอมพิวเตอร์ไม่สามารถใช้งานได้เป็นวงกว้าง หรือกระทบกับข้อมูลชั้นความลับ ระดับลับขึ้นไป | อัพเดทระบบซอฟต์แวร์ให้เป็นปัจจุบันเพื่ออุดช่องโหว่ต่าง ๆ ของโปรแกรมระบบ (System Software) |
| การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion) | การเข้าถึงระบบสารสนเทศอย่างไม่ได้รับอนุญาตและไม่มีสิทธิพิเศษ การเข้าถึงแบบไม่มีสิทธิพิเศษ ซึ่งเรียกว่าการเข้าถึงระดับผู้ใช้ให้สิทธิ์การเข้าถึงระบบงาน ที่จำกัดตามสิทธิ์ที่ได้รับจากผู้ใช้ รวมถึงการเข้าถึงข้อมูลหรือเครดิตบัญชีที่ไม่ได้รับอนุญาตซึ่งอาจใช้ในการทำหน้าที่ | ดำเนินการตรวจสอบ log ที่มาจาก Firewall, IPS, WAF เพื่อตรวจสอบว่าตรงกับเกณฑ์ ดังนี้<br>๑) พยายาม log-in นอกเวลาทำงาน<br>๒) Log-in ภายใต้ IP ที่องค์กรกำหนด หากพยายาม Log-in นอกเวลา หรือ Log-in จาก IP ที่หน่วยงานได้กำหนดไว้ |

| ประเภทการโจมตี | อธิบายลักษณะการโจมตี | วิธีการรับมือ |
|---|---|---|
| | ของผู้ใช้ เช่น การเข้าถึงแอปพลิเคชันเว็บ พอร์ทัลเว็บ หรือทรัพยากรข้อมูลอื่นที่คล้ายคลึงกัน หากระบบงานถูกบุกรุกด้วยโค้ดที่มีเจตนาไม่ดี ซึ่งสามารถควบคุมโต้ตอบจากระยะไกล | |
| การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion) | การเข้าถึงระบบงานด้วยสิทธิพิเศษโดยไม่ได้รับอนุญาต การเข้าถึงแบบมีสิทธิพิเศษ ซึ่งมักเรียกว่าการเข้าถึงระดับผู้ดูแลระบบ หรือระดับรูท ช่วยให้เข้าถึงระบบงานได้ไม่จำกัด หมวดหมู่นี้รวมถึงการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาตหรือการเข้าถึงข้อมูลประจำตัวบัญชีโดยไม่ได้รับอนุญาต ซึ่งสามารถใช้เพื่อทำหน้าที่ด้านการดูแลระบบ (เช่น ผู้ดูแลระบบโดเมน) หากระบบงานถูกบุกรุกด้วยโค้ดที่เป็นอันตรายซึ่งมีการควบคุมแบบโต้ตอบระยะไกล ระบบจะรายงานข้อมูลดังกล่าว | ดำเนินการตรวจสอบ log ที่มาจาก Firewall, IPS, WAF เพื่อตรวจสอบเช็คว่าตรงกับเกณฑ์ ดังนี้<br>๑) พยายาม log-in นอกเวลาทำงาน<br>๒) Log-in ภายใต้ IP ที่องค์กรกำหนด<br>หากพยายาม Log-in นอกเวลา หรือ Log-in จาก IP ที่หน่วยงานได้กำหนดไว้ |
| การถูกโจมตีในรูปแบบ Network Scanning | กระบวนการที่ผู้ไม่ประสงค์ดีพยายามทำลายหรือเข้าถึงข้อมูลในระบบเครือข่ายของบุคคล หรือองค์กรอย่างไม่ถูกต้องหรือไม่ได้รับอนุญาต โดยเครื่องมือพิเศษที่ออกแบบมาเพื่อสแกนหรือสำรวจเครือข่าย | ตรวจสอบ log ที่มาจาก Firewall, IPS, WAF หากพบความเสี่ยงจะแจ้งทีมงาน |
| การถูกโจมตีในรูปแบบ Ransomware | การโจมตีจากมัลแวร์ชนิดหนึ่งที่เข้ารหัสไฟล์ของเหยื่อแล้วขโมยข้อมูลของเหยื่อไป จากนั้นผู้โจมตีก็จะเรียกค่าไถ่จากเหยื่อ เพื่อให้เหยื่อจ่ายเงินแลกกับการได้ข้อมูลคืน โดยส่วนใหญ่แล้วเหยื่อจะยอมจ่ายเงินเพื่อขอข้อมูลคืน | ให้ปิดการเชื่อมต่ออินเตอร์เน็ตโดยทันที และหาสาเหตุที่โดนโจมตีว่ามาจากช่องทางไหน และทำการสแกนไวรัสเครื่องคอมพิวเตอร์ที่ใช้งาน |

| ประเภทการโจมตี | อธิบายลักษณะการโจมตี | วิธีการรับมือ |
|---|---|---|
| การโจมตีการเข้ารหัส (Encryption Attacks): | การโจมตีการเข้ารหัสเกี่ยวข้องกับการบุกรุกหรือแทรกแซงกระบวนการเข้ารหัสข้อมูล เช่น การโจมตีช่องโหว่ในการใช้วิธีการเข้ารหัสที่ไม่ปลอดภัย เพื่อถอดรหัสข้อมูลที่ถูกเข้ารหัสไว้ หรือการโจมตีต่อการเข้ารหัสข้อมูลที่ส่งผ่านเครือข่าย รวมถึงการถอดรหัสข้อมูลที่ถูกเข้ารหัสไว้ | ๑) หยุดการโจมตี<br>- หากเป็นไปได้ หยุดการใช้งานระบบหรือข้อมูลที่ถูกโจมตีในขณะนั้นทันที เพื่อป้องกันความเสียหายที่เพิ่มเติมจากการโจมตีต่อไป<br>๒) ตรวจสอบและติดตามการเข้าถึง<br>- ทำการตรวจสอบประวัติการเข้าถึงระบบหรือข้อมูลที่ถูกโจมตี เพื่อดูว่าใครมีการเข้าถึงข้อมูลและทำอะไรในระบบบ้าง<br>๓) ประเมินความเสียหาย<br>- ประเมินความเสียหายที่เกิดขึ้นจากการโจมตี เช่น ข้อมูลที่สูญหาย ข้อมูลที่ถูกเปิดเผย หรือความเสียหายทางเศรษฐกิจ<br>๔) กู้คืนข้อมูล<br>- พยายามกู้คืนข้อมูลที่สูญหายหรือถูกเข้ารหัสโดยไม่ได้รับอนุญาต โดยการใช้วิธีการสำรองข้อมูล (backups) หรือซอฟต์แวร์กู้คืนข้อมูล<br>๕) ปรับปรุงความปลอดภัย<br>- ทำการปรับปรุงระบบการเข้ารหัสโดยเปลี่ยนวิธีการเข้ารหัสที่ใช้งานอยู่ในปัจจุบันเป็นวิธีที่มีความปลอดภัยมากยิ่งขึ้น<br>๖) เพิ่มความมั่นคงปลอดภัย<br>- ทำการเพิ่มระดับความปลอดภัยของระบบโดยการเพิ่มการตรวจสอบและการตรวจจับการเข้าถึงของผู้ใช้งานที่มีความเสี่ยง<br>๗) รายงานและวิเคราะห์เหตุการณ์ |

| ประเภทการโจมตี | อธิบายลักษณะการโจมตี | วิธีการรับมือ |
|---|---|---|
| | | - ทำการรายงานการเกิดการโจมตีแก่ผู้ที่เกี่ยวข้องและการประมวลผลข้อมูลเพื่อเรียนรู้จากประสบการณ์และป้องกันการเกิดซ้ำในอนาคต |
| การโจมตีเว็บ (Web Attacks): เช่น SQL Injection, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF) | ซึ่งทำให้ผู้ไม่ประสงค์ดีสามารถเข้าถึงข้อมูลหรือควบคุมเว็บไซต์ได้<br>- SQL Injection: การป้องกันไม่ให้ผู้ไม่ประสงค์ดีฝังโค้ด SQL ลงในคำสั่ง SQL ที่ส่งไปยังเว็บเซิร์ฟเวอร์<br>- Cross-Site Scripting (XSS): การแทรกสคริปต์ที่ไม่ปลอดภัยในหน้าเว็บที่ผู้ใช้สามารถเข้าถึงได้ เพื่อทำให้เกิดการกระทำที่ไม่ควรเกิดขึ้น<br>- Cross-Site Request Forgery (CSRF): การโจมตีที่นำการดำเนินการที่ผู้ใช้งานยอมรับและมักจะทำอย่างไม่ระมัดระวัง ให้ทำการกระทำกับเว็บไซต์อื่น ๆ ที่ผู้ไม่ประสงค์ดีควบคุมได้ | ๑) ปิดช่องโหว่ทันที<br>- แก้ไขช่องโหว่ที่เปิดเผยทันทีเพื่อป้องกันการโจมตีต่อไป ตัวอย่างเช่น ปรับแก้โค้ดหรือคำสั่งที่ทำให้เกิดช่องโหว่ SQL Injection หรือ XSS<br>๒) การตรวจสอบและทดสอบ<br>- ทำการตรวจสอบโครงสร้างของระบบเพื่อค้นหาช่องโหว่ที่เปิดเผยและทดสอบระบบเพื่อตรวจจับช่องโหว่ที่มีในระบบ<br>๓) การใช้งานอินพุตอย่างปลอดภัย<br>- ใช้เทคนิคการกรองอินพุต (Input Validation) และการตรวจสอบอินพุต (Input Sanitization) เพื่อป้องกันการเข้าถึงไม่ถูกต้องและการโจมตี<br>๔) การป้องกัน CSRF<br>- ใช้ CSRF Token เพื่อระบุและตรวจสอบคำขอที่ส่งมาจากผู้ใช้งานเพื่อป้องกันการโจมตี CSRF<br>๕) การป้องกัน XSS<br>- ใช้งาน Content Security Policy (CSP) เพื่อลดโอกาสของการโจมตี XSS โดยจำกัดการทำงานของสคริปต์ที่สามารถรันในหน้าเว็บได้<br>๖) การปรับแต่งความปลอดภัยของเซิร์ฟเวอร์<br>- ปรับแต่งการตั้งค่าของเซิร์ฟเวอร์เพื่อป้องกันการโจมตีต่าง ๆ รวมถึง |

| ประเภทการโจมตี | อธิบายลักษณะการโจมตี | วิธีการรับมือ |
|---|---|---|
| | | การใช้งาน HTTPS และ SSL/TLS เพื่อเข้ารหัสการสื่อสารระหว่างเซิร์ฟเวอร์และผู้ใช้<br>๗) การอัปเดตและการปรับปรุง<br>- อัปเดตและปรับปรุงระบบและไลบรารีที่ใช้งานเพื่อแก้ไขช่องโหว่ที่เกิดขึ้นและป้องกันการโจมตีใหม่ |
| การโจมตีเครือข่าย (Network Attacks): รวมถึงการช่วยให้ผู้ไม่ประสงค์ดีเข้าถึงเครือข่ายของระบบโดยไม่ได้รับอนุญาต | เมื่อระบบหรือองค์กรถูกโจมตีด้วยการโจมตีเครือข่าย (Network Attacks) เช่น<br>- การสแกนพอร์ต (Port Scanning)<br>- การสร้างการร้ายแรงในระบบ (Denial of Service)<br>-การบุกรุกความปลอดภัยของเครือข่าย (Network Security Breach)<br>- การโจมตีแบบ Man-in-the-Middle (MITM): ผู้ไม่ประสงค์ดีตัดสินใจที่จะเป็นตัวกลางระหว่างผู้ส่งและผู้รับข้อมูล และสามารถดักจับและแก้ไขข้อมูลได้ในระหว่างการสื่อสาร<br>- ARP Spoofing: การโจมตีซึ่งผู้ไม่ประสงค์ดีสร้างแพ็คเกจ ARP (Address Resolution Protocol) เพื่อเปลี่ยนการจับคู่ระหว่างที่อยู่ IP และ MAC ในเครือข่าย ทำให้สามารถมองเห็นการส่งข้อมูลที่ผ่านเครือข่ายได้ | ๑) หยุดการโจมตีทันที<br>- การรีบหยุดหรือแยกออกจากเครือข่ายที่ถูกโจมตีเพื่อลดความเสี่ยงและความเสียหายจากการโจมตีต่อไป<br>๒) ตรวจสอบและระบุแหล่งที่มาของการโจมตี<br>- ใช้เครื่องมือตรวจสอบเครือข่ายเพื่อระบุแหล่งที่มาของการโจมตี เช่น Intrusion Detection Systems (IDS) หรือ Security Information and Event Management (SIEM) เพื่อตรวจจับและระบุการโจมตี<br>๓) ป้องกันและลดความเสี่ยง<br>- ปรับแต่งการตั้งค่าของ Firewalls, Intrusion Prevention Systems (IPS), และอุปกรณ์รักษาความปลอดภัยอื่น ๆ เพื่อป้องกันการโจมตีให้มากที่สุด<br>๔) การสร้างการกระทำตามนโยบายความปลอดภัย<br>- อัพเดตนโยบายความปลอดภัยและเพิ่มเติมมาตรการป้องกันการโจมตีเครือข่ายในกรณีที่มีการโจมตีแบบเดียวกันเกิดขึ้นอีกครั้งในอนาคต<br>๕) การบริหารจัดการเหตุการณ์ (Incident Management) |

| ประเภทการโจมตี | อธิบายลักษณะการโจมตี | วิธีการรับมือ |
|---|---|---|
| | | - บันทึกข้อมูลและการวิเคราะห์เหตุการณ์เพื่อการปรับปรุงในอนาคต<br>๖) การปรับปรุงระบบเครือข่าย<br>- อัปเดตและปรับปรุงอุปกรณ์เครือข่าย เช่น เซิร์ฟเวอร์, เราเตอร์, และสวิตช์ ให้มีการแก้ไขช่องโหว่ล่าสุดและมีการควบคุมความปลอดภัยที่เพิ่มมากขึ้น<br>๗) การรายงานและการพัฒนา<br>- รายงานและวิเคราะห์ข้อมูลการโจมตีเพื่อเข้าใจและป้องกันการเกิดซ้ำในอนาคต พร้อมทั้งพัฒนามาตรการแก้ไขเพื่อป้องกันการโจมตีที่อาจจะเกิดขึ้นในอนาคต |
| การโจมตีที่เกี่ยวกับแอปพลิเคชัน (Application Attacks): | - Buffer Overflow Attacks: การโจมตีที่ใช้การเกินขนาดของพื้นที่หน่วยความจำเพื่อให้โปรแกรมทำงานผิดปกติ โดยบ่งชี้ไปยังโค้ดที่ไม่ปลอดภัยที่ถูกโหลดลงในหน่วยความจำ<br>- Code Injection Attacks: การฝังโค้ดที่ไม่ปลอดภัยลงในแอปพลิเคชัน เช่น SQL Injection, Command Injection | ๑) ปิดช่องโหว่ทันที<br>- แก้ไขโค้ดหรือคำสั่งที่ทำให้เกิดช่องโหว่ เช่น การทำคำสั่ง SQL Injection, XSS หรือ RCE เพื่อป้องกันการโจมตีต่อไป<br>๒) การตรวจสอบและทดสอบ<br>- ทำการตรวจสอบโครงสร้างของระบบเพื่อค้นหาช่องโหว่ที่เปิดเผยและทดสอบระบบเพื่อตรวจจับช่องโหว่ที่อาจไม่เปิดเผย<br>๓) การใช้งานอินพุตอย่างปลอดภัย<br>- ใช้เทคนิคการกรองอินพุต (Input Validation) และการตรวจสอบอินพุต (Input Sanitization) เพื่อป้องกันการเข้าถึงไม่ถูกต้องและการโจมตี<br>๔) การป้องกัน SQL Injection |

| ประเภทการโจมตี | อธิบายลักษณะการโจมตี | วิธีการรับมือ |
|---|---|---|
| | | - ใช้ Prepared Statements หรือ Parameterized Queries เพื่อป้องกันการฝังโค้ด SQL จากอินพุตผู้ใช้<br>๕) การป้องกัน Cross-Site Scripting (XSS)<br>- สร้าง Content Security Policy (CSP) เพื่อลดโอกาสของการโจมตี XSS โดยจำกัดการทำงานของสคริปต์ที่สามารถรันในหน้าเว็บ<br>๖) การป้องกัน Remote Code Execution (RCE)<br>- จำกัดสิทธิ์การเข้าถึงไฟล์และระบบ เช่น ใช้ Principle of Least Privilege เพื่อลดความเสี่ยงที่จะถูกโจมตีด้วย Remote Code Execution<br>๗) การอัปเดตและการปรับปรุง<br>- อัปเดตและปรับปรุงแอปพลิเคชันและไลบรารีที่ใช้งานเพื่อแก้ไขช่องโหว่ที่เปิดเผยและป้องกันการโจมตีใหม่ |
| การโจมตีช่องโหว่ในระบบปฏิบัติการ (Operating System Vulnerabilities): | ช่องโหว่ในระบบปฏิบัติการเป็นประตูเปิดให้ผู้ไม่ประสงค์ดีเข้าถึงระบบ อาจเป็นการไม่รักษาการปรับปรุงหรือการใช้งานที่ไม่ปลอดภัยของระบบปฏิบัติการ<br>เช่น การโจมตีและการระบาดของไวรัส ซึ่งอาจเกิดขึ้นจากช่องโหว่ในระบบปฏิบัติการ | ๑) การอัปเดตและปรับปรุง<br>- อัปเดตระบบปฏิบัติการและซอฟต์แวร์ทั้งหมดให้เป็นเวอร์ชันล่าสุด เพื่อปิดช่องโหว่ที่มีความเสี่ยงที่ถูกค้นพบและแก้ไข<br>๒) การใช้งานโปรแกรมป้องกัน<br>- ติดตั้งและใช้โปรแกรมป้องกันมัลแวร์ (Antivirus) และโปรแกรมป้องกันมัลแวร์อื่น ๆ เพื่อตรวจจับ และลบไวรัสหรือมัลแวร์ที่อาจจะเข้ามาผ่านช่องโหว่<br>๓) การปรับแต่งคอนฟิก<br>- ปรับแต่งคอนฟิกของระบบปฏิบัติการให้เหมาะสม และปิดการให้บริการที่ไม่จำเป็นที่อาจเป็นที่รู้จักของผู้โจมตี |

| ประเภทการโจมตี | อธิบายลักษณะการโจมตี | วิธีการรับมือ |
|---|---|---|
| | | ๔) การทำ Backups<br>- สร้างการสำรองข้อมูล (backups) ของข้อมูลที่สำคัญอย่างสม่ำเสมอ เพื่อให้สามารถกู้คืนข้อมูลหากเกิดความเสียหายจากการโจมตี<br>๕) การติดตั้ง Firewalls<br>- ติดตั้ง Firewalls เพื่อควบคุมการเข้าถึงเครือข่ายและป้องกันการโจมตีจากภายนอก<br>๖) การตรวจสอบการเข้าถึง<br>- ตรวจสอบการเข้าถึงของผู้ใช้ รวมทั้งการตรวจสอบล็อกอินและการใช้งานทั้งหมดของระบบ<br>๗) การปรับปรุงการตั้งค่าความปลอดภัย<br>- ปรับปรุงการตั้งค่าความปลอดภัยของระบบปฏิบัติการ เช่น การปิดฟีเจอร์ที่ไม่จำเป็นและการใช้งานการตั้งค่าความปลอดภัยที่เหมาะสม<br>๘) การจัดการการเข้าถึงและสิทธิ์<br>- จัดการสิทธิ์การเข้าถึงให้แม่นยำ ใช้หลักการของ "Least Privilege" เพื่อให้ผู้ใช้มีสิทธิ์เพียงพอที่จะทำงานเท่าที่จำเป็น<br>๙) การตรวจสอบล็อก (Logging)<br>- เปิดใช้งานการล็อกเพื่อรวบรวมข้อมูลการดำเนินการของระบบ และตรวจสอบล็อกเพื่อตรวจสอบความปลอดภัย<br>๑๐) การประเมินความเสี่ยง |

| ประเภทการโจมตี | อธิบายลักษณะการโจมตี | วิธีการรับมือ |
|---|---|---|
| | | - ทำการประเมินความเสี่ยงเพื่อตรวจจับและป้องกันการโจมตีที่อาจเกิดขึ้นในอนาคต |
| การโจมตี Firewall หรือ IPS (Intrusion Prevention System): | | การแก้ไขจะต้องให้ความสำคัญกับการกู้คืนระบบเพื่อให้ระบบกลับมาทำงานได้โดยมีความปลอดภัย<br>๑) ระงับการโจมตี<br>- หากเป็นเครื่องบริการหรือแอปพลิเคชันที่ถูกโจมตีด้วยการเจาะระบบ ต้องพยายามระงับการโจมตีโดยการตัดการเชื่อมต่อหรือบล็อกทรัพยากรที่ถูกโจมตี<br>๒) แยกแยะและวิเคราะห์การโจมตี<br>- ทำการวิเคราะห์และระบุว่าการโจมตีเกิดขึ้นอย่างไร และสามารถระบุรูปแบบและลักษณะของการโจมตีได้เหมือนกันหรือไม่<br>๓) อัปเดตและปรับปรุงกฎการตั้งค่า<br>- อัปเดตและปรับปรุงกฎการตั้งค่าของ Firewall หรือ IPS เพื่อให้มีประสิทธิภาพในการป้องกันการโจมตีในอนาคต<br>๔) การตรวจสอบและการตรวจจับอัตโนมัติ (Automatic Detection)<br>- ใช้ระบบตรวจสอบและการตรวจจับอัตโนมัติเพื่อตรวจจับการโจมตีและความผิดปกติที่เกิดขึ้นในเครือข่าย และปรับปรุงการตรวจจับเพื่อทำให้เป็นไปได้ที่สูงสุด<br>๕) การแก้ไขข้อบกพร่อง (Patch Management): |

| ประเภทการโจมตี | อธิบายลักษณะการโจมตี | วิธีการรับมือ |
|---|---|---|
| | | - ตรวจสอบและติดตั้งการแก้ไขข้อบกพร่อง (patch) ที่มีอยู่สำหรับ Firewall หรือ IPS เพื่อแก้ไขช่องโหว่ที่อาจถูกโจมตี<br>๖) การเรียนรู้และการป้องกัน<br>- ใช้ประสบการณ์จากการโจมตีนี้เพื่อปรับปรุงนโยบายและกระบวนการเพื่อป้องกันการโจมตีที่เป็นไปได้ในอนาคต<br>๗) การสร้างการสำรอง (Backups)<br>- สร้างการสำรองข้อมูลเพื่อป้องกันข้อมูลที่สำคัญจากการสูญเสียหรือทำลายในกรณีที่เกิดการโจมตี |
| การโจมตีอุปกรณ์เครือข่าย | | เมื่ออุปกรณ์เครือข่ายถูกโจมตี การดำเนินการทันทีเพื่อรักษาความปลอดภัยและความเสถียรของระบบเครือข่ายเป็นสิ่งสำคัญมาก ขั้นตอนเมื่อเผชิญกับการโจมตีที่เกิดขึ้นในอุปกรณ์เครือข่าย ดังนี้<br>๑) ตัดการเชื่อมต่อ<br>- ระงับการเชื่อมต่อของอุปกรณ์เครือข่ายที่ถูกโจมตีเพื่อหยุดการระบาดของการโจมตีและป้องกันความเสียหายเพิ่มเติม<br>๒) แจ้งเตือนทีมความปลอดภัย<br>- แจ้งทีมความปลอดภัยหรือผู้ที่เกี่ยวข้องให้ทราบเกี่ยวกับการโจมตีทันที เพื่อให้มีการตอบสนองและดำเนินการแก้ไขที่รวดเร็ว<br>๓) ทำการตรวจสอบและวิเคราะห์การโจมตีเพื่อระบุลักษณะและวิธีการโจมตี |

| ประเภทการโจมตี | อธิบายลักษณะการโจมตี | วิธีการรับมือ |
|---|---|---|
| | | รวมทั้งระบุบทบาทของอุปกรณ์เครือข่ายที่ถูกโจมตี<br>๔) ฟื้นคืนระบบ<br>- ดำเนินการฟื้นคืนอุปกรณ์เครือข่ายโดยการเคลียร์ค่าตั้งต่าง ๆ หรือทำการกู้คืนระบบให้กลับมาที่สถานะปกติ<br>๕) ปรับเปลี่ยนรหัสผ่าน<br>- เปลี่ยนรหัสผ่านทั้งในอุปกรณ์เครือข่ายและบัญชีผู้ใช้ที่เกี่ยวข้องเพื่อป้องกันการเข้าถึงที่ไม่พึงประสงค์<br>๖) อัปเดตและป้องกันโปรแกรมที่มีช่องโหว่<br>- ทำการอัปเดตซอฟต์แวร์และแพทช์ช่วยป้องกันการโจมตีที่ใช้ช่องโหว่ในโปรแกรมหรือระบบปฏิบัติการ<br>๗) การสร้างและปรับปรุงนโยบายความมั่นคงปลอดภัย<br>- สร้างและปรับปรุงนโยบายความมั่นคงปลอดภัยเพื่อเสริมสร้างระบบป้องกันการโจมตีขององค์กร<br>๘) การทดสอบและปรับปรุงระบบ<br>- ทดสอบระบบความปลอดภัยเพื่อตรวจสอบความเสี่ยงและปรับปรุงระบบเพื่อป้องกันการโจมตีในอนาคต |
| การโจมตีเครื่อง Server | | เมื่อเครื่องเซิร์ฟเวอร์ถูกโจมตี จะต้องดำเนินการทันทีเพื่อรักษาความปลอดภัยของระบบและป้องกันความเสียหายจากการโจมตีของผู้ไม่ประสงค์ดี<br>๑) ตัดการเชื่อมต่อ<br>- ตัดการเชื่อมต่อของเครื่องเซิร์ฟเวอร์ที่ถูกโจมตี เพื่อหยุดการเข้าถึงของ |

| ประเภทการโจมตี | อธิบายลักษณะการโจมตี | วิธีการรับมือ |
|---|---|---|
| | | ผู้ไม่ประสงค์ดีและลดความเสี่ยงที่อาจเกิดความเสียหายเพิ่มมากขึ้น<br>๒) แจ้งเตือนผู้ที่เกี่ยวข้อง<br>- แจ้งเตือนทีมด้านความปลอดภัยและผู้ที่เกี่ยวข้องให้ทราบเกี่ยวกับการโจมตีและเริ่มต้นกระบวนการตอบสนอง<br>๓) สำรวจและวิเคราะห์การโจมตี<br>- ทำการสำรวจและวิเคราะห์การโจมตีเพื่อระบุรูปแบบการโจมตี ลักษณะของการโจมตี และบทบาทของเครื่องเซิร์ฟเวอร์ที่ถูกโจมตี<br>๔) รักษาการเข้าถึงและความปลอดภัย<br>- ปรับปรุงการรักษาการเข้าถึงและความปลอดภัยของระบบโดยการเปลี่ยนรหัสผ่าน บล็อกการเข้าถึงที่ไม่พึงประสงค์ และอัปเดตระบบที่มีช่องโหว่<br>๕) ฟื้นคืนจากการโจมตี<br>- ทำการฟื้นคืนข้อมูลหรือไฟล์ที่ถูกทำลายหรือสูญเสียจากการโจมตีโดยใช้การสำรองข้อมูลที่มีอยู่<br>๖) ปรับปรุงการรักษาความปลอดภัย<br>- ปรับปรุงนโยบายและมาตรการเพื่อเสริมสร้างความปลอดภัยของระบบ เช่น การเพิ่มชั้นความปลอดภัย การปรับปรุงการตรวจจับอัตโนมัติ เป็นต้น<br>๗) การฟื้นคืนระบบ (System Recovery)<br>- ฟื้นคืนเครื่องเซิร์ฟเวอร์จากการโจมตีโดยการการลบหรือกำจัดไฟล์ที่ตรวจพบว่ามีความเสี่ยงหรืออันตรายออกจากระบบ และกู้คืนระบบให้อยู่ในสภาพปกติ |

| ประเภทการโจมตี | อธิบายลักษณะการโจมตี | วิธีการรับมือ |
|---|---|---|
| | | ๘) การทบทวนและการป้องกันอนาคต<br>- ทบทวนเหตุการณ์ที่เกิดขึ้นและการรับมือเพื่อป้องกันการโจมตีในอนาคต รวมถึงการปรับปรุงนโยบายและกระบวนการต่าง ๆ เพื่อเพิ่มความปลอดภัยของระบบ<br>๙) การเรียนรู้และพัฒนา<br>- ศึกษาการโจมตีเพื่อเรียนรู้และพัฒนากระบวนการป้องกันภัยคุกคามให้ดียิ่งขึ้นในอนาคต |
| การโจมตีเครื่อง Client: | | เมื่อเครื่อง Client ถูกโจมตี ควรดำเนินการอย่างรวดเร็วเพื่อป้องกันความเสียหายและรักษาความปลอดภัยของระบบ ดังนี้<br>๑) ตัดการเชื่อมต่อ<br>- หากเครื่อง Client ถูกโจมตีจากการเชื่อมต่อเครือข่ายที่ไม่ปลอดภัย ให้ระงับการเชื่อมต่อทันทีเพื่อลดความเสี่ยงที่อาจเกิดขึ้น<br>๒) เชื่อมต่อกับเครือข่ายปลอดภัย<br>- ให้เชื่อมต่อเครื่อง Client กับเครือข่ายที่มีความปลอดภัยเพื่อป้องกันการโจมตีจากเครือข่ายภายนอกที่ไม่พึงประสงค์<br>๓) สแกนและลบโปรแกรมเสี่ยง<br>- ใช้โปรแกรมตรวจสอบไวรัสและมัลแวร์เพื่อสแกนและลบโปรแกรมที่เป็นเสี่ยงออกจากระบบ<br>๔) อัปเดตและป้องกันอย่างมีระเบียบ<br>- อัปเดตระบบปฏิบัติการและโปรแกรมทั้งหมดในเครื่อง Client เพื่อ |

| ประเภทการโจมตี | อธิบายลักษณะการโจมตี | วิธีการรับมือ |
|---|---|---|
| | | ป้องกันการโจมตีผ่านช่องโหว่ที่มีอยู่ในระบบ<br>๕) เปลี่ยนรหัสผ่าน<br>- เปลี่ยนรหัสผ่านของผู้ใช้ทั้งในระบบเครือข่ายและบัญชีอินเทอร์เน็ตเพื่อป้องกันการเข้าถึงโดยไม่พึงประสงค์<br>๖) สำรวจและกำจัดไวรัสและมัลแวร์<br>- ใช้โปรแกรมแอนตี้ไวรัสและแอนตี้มัลแวร์เพื่อสำรวจและกำจัดไวรัสและมัลแวร์ที่อาจมีอยู่ในเครื่อง Client<br>๗) ทบทวนเพื่อเรียนรู้<br>- ทบทวนและเรียนรู้จากการโจมตีนี้เพื่อป้องกันการเกิดเหตุการณ์ที่คล้ายคลึงในอนาคต รวมถึงการปรับปรุงนโยบายและกระบวนการเพื่อป้องกันการโจมตีในอนาคต<br>๘) ฟื้นคืนจากการโจมตี<br>- สำรวจและฟื้นคืนข้อมูลหรือไฟล์ที่อาจถูกทำลายหรือเปลี่ยนแปลงจากการโจมตี |

**๘.๒.๒ สำนักงาน กสม. จัดให้มีกลไกที่สามารถตรวจจับสิ่งบ่งชี้หรือลักษณะเบื้องต้นของการเกิดภัยคุกคามทางไซเบอร์ได้ในเวลาอันเหมาะสม** โดยอาจอาศัยข้อมูลจากแหล่งข้อมูลต่าง ๆ เช่น ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ, ระบบไฟร์วอลล์, ระบบเว็บแอปพลิเคชันไฟร์วอลล์ เป็นต้น โดยกลไกที่สามารถใช้เพื่อตรวจจับสิ่งบ่งชี้หรือลักษณะเบื้องต้นของการเกิดภัยคุกคามทางไซเบอร์ คือ ระบบตรวจจับภัยคุกคามทางไซเบอร์ (Intrusion Detection Systems - IDS) และระบบตรวจจับภัยคุกคามทางไซเบอร์แบบล่วงหน้า (Intrusion Prevention Systems - IPS) เป็นเครื่องมือที่ใช้ในการตรวจจับและป้องกันการโจมตีทางไซเบอร์ได้ตลอดเวลา นอกจากนี้ยังมีเทคโนโลยีอื่น ๆ ที่ใช้ในการตรวจจับการเข้าถึงที่ไม่พึงประสงค์และภัยคุกคามทางไซเบอร์ได้ในเวลาที่เหมาะสมด้วย เช่น

๑) ระบบตรวจจับการเข้าถึงที่ไม่ปกติ (Anomaly Detection Systems) ระบบสามารถตรวจจับการเข้าถึงที่ไม่ปกติหรือพฤติกรรมที่ไม่เหมือนปกติของระบบ เช่น การเข้าสู่ระบบจากสถานที่ที่ไม่เคยเข้าใช้งานมาก่อน

๒) การตรวจสอบล็อก (Log Inspection) การตรวจสอบและวิเคราะห์บันทึกการเข้าถึงและกิจกรรมของระบบเครือข่ายและระบบของเซิร์ฟเวอร์ เพื่อตรวจจับและระบุกิจกรรมที่เป็นภัยคุกคาม

๓) การวิเคราะห์ลักษณะพฤติกรรม (Behavioral Analysis) ระบบสามารถวิเคราะห์พฤติกรรมของผู้ใช้หรือของระบบเครือข่าย เช่น พฤติกรรมการเข้าถึงข้อมูล, รูปแบบการส่งข้อมูล, และกิจกรรมที่ไม่ปกติ เพื่อตรวจจับภัยคุกคามที่เกิดขึ้นอย่างระบุเฉพาะ

๔) การใช้ลูกเล่นอัลกอริทึม (Honeypots) ระบบปลอดภัยที่ถูกสร้างขึ้นเพื่อดึงดูดผู้ไม่ประสงค์ดีเข้ามาโจมตี โดยทำให้ง่ายต่อการตรวจจับและวิเคราะห์ภัยคุกคามที่เกิดขึ้น

๕) การใช้เทคโนโลยีเสมือน (Virtualization) การใช้ระบบเสมือนหรือสภาพแวดล้อมเสมือนเพื่อทดสอบและตรวจจับภัยคุกคามทางไซเบอร์โดยไม่เสียความเสี่ยงต่อระบบที่มีข้อมูลจริง

๖) การใช้ซอฟต์แวร์ตรวจสอบภัยคุกคาม (Security Information and Event Management - SIEM) ระบบซึ่งรวมการรวบรวม, การจัดการ, และการวิเคราะห์ข้อมูลจากแหล่งต่าง ๆ เพื่อตรวจจับภัยคุกคามที่เกิดขึ้นในเครือข่าย

๗) แหล่งข่าวสารประกาศช่องโหว่ใหม่ของระบบปฏิบัติการวินโดร์และแอปพลิเคชันต่าง ๆ

๘) แหล่งข่าวสารภัยคุกคามจากภายนอก (Threat Intelligence)

- https://www.thaicert.or.th/
- https://ncsec.ncsa.or.th/
- https://www.facebook.com/NCSA.Thailand?locale=vi_VN

**๘.๒.๓ การแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์**

อุปกรณ์ที่ใช้เพื่อการป้องกันและตรวจจับต้องพิจารณาตามความเหมาะสมกับระบบที่ต้องการป้องกัน และต้องทำการปรับแต่ง (Fine-Tune) เพื่อให้มีความเหมาะสมกับสภาพการใช้งานของระบบนั้น ๆ ซึ่งข้อมูลการแจ้งเตือนเพื่อตรวจจับการบุกรุกระบบคอมพิวเตอร์และเครือข่ายมีดังนี้

๑) ประเภทของการแจ้งเตือน (Alert) ได้แก่

๑.๑) ระบบป้องกันการบุกรุก (Intrusion Protection System: IPS) ระบบที่ทำหน้าที่ตรวจจับและป้องกันการโจมตีในระบบเครือข่าย โดยมีการแจ้งเตือน เมื่อพบสิ่งที่ตรงกับวิธีการโจมตีที่ระบบรู้จัก

๑.๒) ระบบจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log Collection System) เป็นระบบตรวจจับความผิดปกติโดยใช้ข้อมูลจราจรทางคอมพิวเตอร์ (Log) ที่จัดเก็บจากระบบต่าง ๆ เพื่อนำมาใช้วิเคราะห์ โดยต้องตั้งค่า Rule set โดยผู้เชี่ยวชาญให้มีความเหมาะสมกับสภาพแวดล้อมที่เชื่อมต่ออยู่กับระบบจัดเก็บข้อมูลจราจรคอมพิวเตอร์

๑.๓) โปรแกรมป้องกันและกำจัดไวรัสคอมพิวเตอร์ (Antivirus) ทำหน้าที่ตรวจจับโปรแกรมประสงค์ร้าย (Malware) โดยมีลักษณะการตรวจจับทั้งในระดับเครือข่าย และในระดับ Host ซึ่งหาก

มีการตรวจพบ Malware ในระบบ สามารถเป็นข้อบ่งชี้ได้ว่าเกิดเหตุภัยคุกคามที่อาจกำลังพยายามโจมตี หรือได้มีการโจมตีสำเร็จแล้ว

๑.๔) ผู้ให้บริการภายนอก ทำหน้าที่ให้บริการการเฝ้าระวังและตรวจสอบความผิดปกติที่เกิดขึ้นกับระบบสารสนเทศ หรือระบบของหน่วยงาน หากตรวจพบว่าถูกนำไปโจมตีระบบอื่น ๆ ภายนอกองค์กร อาจเป็นข้อมูลบ่งชี้ได้ว่าระบบภายในหน่วยงานได้ถูกยึดครองโดยผู้ไม่ประสงค์ดี และนำไปใช้สร้างความเสียหาย

๒) ประเภทของข้อมูลจราจรทางคอมพิวเตอร์ (Log) ได้แก่

๒.๑) Operating System and Application Log เป็นข้อมูลจาก Log ของระบบปฏิบัติการและแอพพลิเคชัน ประกอบไปด้วยการบันทึกเหตุการณ์หลายประเภท สามารถนำมาใช้ในการตรวจจับภัยคุกคามบางอย่างได้ขึ้นอยู่กับประเภทของ Log และ Rule set ที่ใช้ในการวิเคราะห์

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

๓) ข้อมูลจากแหล่งสาธารณะ ข้อมูลช่องโหว่ และวิธีการโจมตีในรูปแบบใหม่ ๆ สามารถนำมาใช้เป็นข้อมูลบ่งชี้ภัยคุกคามได้

๔) บุคคลที่ทำหน้าที่แจ้งเตือนบุคคลภายในองค์กร หรือบุคลากรทุกตำแหน่งสามารถเข้ารับการฝึกฝน เพื่อทำหน้าที่สอดส่องดูแล

**๘.๒.๔ สำนักงาน กสม. ต้องดำเนินการวิเคราะห์เหตุภัยคุกคามหรือความผิดปกติเมื่อได้รับแจ้ง** เพื่อให้การดำเนินการในขั้นต่อไปสามารถดำเนินการได้อย่างรวดเร็วและมีความถูกต้อง โดยวิเคราะห์ความผิดปกติเมื่อได้รับแจ้งเหตุการณ์ ดังต่อไปนี้

๑) การบันทึกและจัดเก็บข้อมูล Log จากหลาย ๆ อุปกรณ์ เช่น Firewall, IDS/IPS, Network Devices และ Log ของระบบงานต่าง ๆ เป็นต้น จะมีความสำคัญเป็นอย่างมากในการวิเคราะห์หาสาเหตุการโจมตีและบันทึกเหตุการณ์เก็บไว้เพื่อเป็นหลักฐานทางกฎหมาย หรือเรียกดูในอนาคต จึงต้องมีการเก็บรักษาไว้เป็นอย่างดี และเป็นไปตามระยะเวลาที่กฎหมายกำหนดไว้ (log Retention Policy)

๒) อุปกรณ์ทุกเครื่องบนระบบเครือข่ายต้องได้รับการ Synchronize เวลาให้ตรงกันอยู่เสมอ เพื่อทำให้การ Correlate Event ทำได้โดยง่าย (Clock Synchronization)

๓) การดักจับข้อมูลทางเครือข่ายเพื่อนำมาวิเคราะห์ข้อมูล (Sniff and Analyze Network Data)

๔) ในกรณีที่ทีมรับมือและตอบสนองฯ ไม่สามารถดำเนินการวิเคราะห์ Incident เพื่อหาสาเหตุที่แท้จริงได้เพื่อกำจัดผู้บุกรุกออกจากระบบได้นั้น สามารถขอคำแนะนำจากที่ปรึกษาทั้งภายในและภายนอกหน่วยงานได้ เช่น CERT ต่าง ๆ หรือ สกมช. เป็นต้น (Seek Assistance)

**๘.๒.๕ สำนักงาน กสม. ต้องทำการบันทึกข้อมูลกิจกรรมเหตุการณ์ความปลอดภัยทางไซเบอร์ (Incident Documentation)** โดยควรบันทึกข้อมูลเกี่ยวกับเหตุการณ์ความปลอดภัยทางไซเบอร์ ทุกขั้นตอนตั้งแต่ตรวจพบเหตุการณ์จนถึงกระบวนการสุดท้ายและข้อมูลดังกล่าวควรระบุรายละเอียดพร้อมเวลาที่เกิดเหตุ

และระยะเวลาที่ใช้ด้วย บันทึกข้อมูลดังกล่าวที่เกี่ยวข้องกับเหตุการณ์ควรลงวันที่และลงนามโดยผู้มีหน้าที่จัดการรับมือเหตุการณ์นั้น ๆ เพื่อให้มั่นใจได้ว่าเหตุการณ์ความปลอดภัยทางไซเบอร์ที่เกิดขึ้นจะได้รับการจัดการแก้ไขภายในระยะเวลาที่เหมาะสมในแบบฟอร์ม (รายละเอียดแบบฟอร์มตามภาคผนวก ช ) โดยมีขั้นตอนในการจัดทำบันทึกข้อมูลกิจกรรมเหตุการณ์ความปลอดภัยทางไซเบอร์ ดังนี้

๑) บันทึกข้อมูลพื้นฐาน

- รวบรวมข้อมูลพื้นฐานเกี่ยวกับเหตุการณ์ที่เกิดขึ้น เช่น วันที่, เวลา, ประเภทของเหตุการณ์, ความรุนแรง, และรายละเอียดเกี่ยวกับทรัพยากรหรือระบบที่เกี่ยวข้อง เป็นต้น

๒) บันทึกข้อมูลผู้เกี่ยวข้อง

- ระบุและบันทึกข้อมูลเกี่ยวกับผู้ที่เกี่ยวข้องกับเหตุการณ์ เช่น ผู้รายงาน, ผู้รับผิดชอบการจัดการเหตุการณ์, และบุคคลที่มีส่วนเกี่ยวข้องในการสืบค้นหรือการแก้ไขปัญหา

๓) บันทึกการกระทำ

- บันทึกรายละเอียดเกี่ยวกับการกระทำที่ดำเนินการตามข้อเสนอแนะหรือแผนการแก้ไขปัญหา รวมถึงการตรวจสอบและการแก้ไขปัญหาที่เกี่ยวข้อง

๔) บันทึกข้อมูลการวิเคราะห์

- ระบุการวิเคราะห์เกี่ยวกับสาเหตุของเหตุการณ์, ผลกระทบที่เกิดขึ้น, และมาตรการที่ได้รับการนำเสนอเพื่อป้องกันหรือแก้ไขปัญหา

๕) บันทึกข้อมูลเพิ่มเติม

- รวบรวมข้อมูลเพิ่มเติมที่สำคัญเกี่ยวกับเหตุการณ์ เช่น การเก็บรวบรวมหลักฐานด้านเทคนิค, ภาพถ่ายหน้าจอ, หรือบันทึกประทับเวลา

๖) การตรวจสอบและการอัพเดต

- ตรวจสอบและอัพเดตบันทึกข้อมูลเหตุการณ์เพื่อให้มั่นใจว่าข้อมูลเป็นปัจจุบันและถูกต้อง

๗) การเก็บรักษา

- รักษาบันทึกข้อมูลเหตุการณ์ความปลอดภัยทางไซเบอร์อย่างมีปลอดภัยตามนโยบายและข้อกำหนดทางกฎหมายที่เกี่ยวข้อง

**๘.๒.๖ การวิเคราะห์ผลกระทบและระดับของภัยคุกคาม (Incident Prioritization)** เพื่อรับมือกับภัยคุกคามทางไซเบอร์ให้ทันท่วงที โดยพิจารณาปัจจัยต่าง ๆ ที่เกี่ยวข้องโดยอย่างน้อยควรครอบคลุมในด้านผลกระทบต่อการให้บริการ (Functional Impact) ผลกระทบต่อข้อมูล (Information Impact) และความสามารถในการฟื้นฟูระบบ (Recoverability) ดังนี้

**๑) ผลกระทบต่อการให้บริการ (Functional Impact)**

ผลกระทบต่อการให้บริการและการดำเนินงานของหน่วยงานที่เกิดเหตุการณ์ภัยคุกคามให้พิจารณาผลกระทบที่เกิดขึ้นทั้งในปัจจุบัน และผลกระทบที่มีโอกาสเกิดขึ้น หากเหตุการณ์ภัยคุกคามยังไม่ถูกควบคุมโดยทันที ซึ่งรวมถึงผลกระทบทางด้านการปฏิบัติงานของระบบงาน การให้บริการต่าง ๆ

ที่ส่งผลกระทบโดยตรงต่อการดำเนินธุรกิจ (Impact to Business) ที่ทำให้เกิดความขัดข้องหรือเสียหายต่อธุรกิจ ซึ่งหากไม่ได้รับการแก้ไขโดยเร็วอาจจะส่งผลเสียมากยิ่งขึ้น โดยระดับของ Functional Impact มีดังนี้

| ระดับผลกระทบ | ผลกระทบต่อการให้บริการ | ระยะเวลาการกู้คืนระบบ (SLA) |
|---|---|---|
| High (สูง) | ระบบไม่สามารถให้บริการได้เลย เกิดการหยุดชะงัก | ภายใน ๔๘ ชั่งโมง |
| Medium (ปานกลาง) | ระบบไม่สามารถให้บริการได้บางส่วน | ภายใน ๘ ชั่งโมง |
| Low (ต่ำ) | มีผลกระทบในการให้บริการน้อยมาก หน่วยงานยังคงสามารถให้บริการระบบงานหลักแก่ผู้ใช้ได้ แต่ประสิทธิภาพในการให้บริการอาจลดลง หรือระบบอาจทำงานช้าลงบ้าง | ภายใน ๔ ชั่งโมง |
| None | ไม่มีผลกระทบในการให้บริการ หรือระบบสามารถดำเนินงานได้ตามปกติ | - |

**๒) ผลกระทบต่อข้อมูล (Information Impact)**

ผลกระทบต่อข้อมูล ควรพิจารณา ๓ ด้าน ได้แก่ ด้านการรักษาความลับ (Confidentiality) ด้านการรักษาความครบถ้วน (Integrity) และด้านการรักษาสภาพพร้อมใช้ (Availability) รวมทั้งควรพิจารณาว่าเหตุการณ์ภัยคุกคามส่งผลต่อการดำเนินงานโดยรวมที่จะส่งผลต่อข้อมูลสำคัญ (Sensitive Information) อย่างไร เช่น ข้อมูลถูกทำลาย หรือสูญหาย หรือรั่วไหล หรือการแก้ไขโดยไม่ได้รับอนุญาต เป็นต้น โดยระดับของ Information Impact มีดังนี้

| ระดับผลกระทบ | ผลกระทบต่อข้อมูล | ระยะเวลาการกู้คืนระบบ (SLA) |
|---|---|---|
| Integrity Loss | ข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Information) หรือข้อมูลที่เป็นความลับของหน่วยงานรั่วไหล หรือข้อมูลสูญหายถูกทำลายทำให้ไม่สามารถใช้งานได้ | ภายใน ๒๔ ชั่งโมง |
| Medium | ข้อมูลที่เป็นของหน่วยงานรั่วไหล หรือถูกแก้ไขเปลี่ยนแปลง | ภายใน ๘ ชั่งโมง |
| Privacy Breach | ข้อมูลส่วนบุคคลรั่วไหลบางส่วน หรือถูกเข้าถึงโดยไม่ได้รับอนุญาต | ภายใน ๔ ชั่งโมง |
| None | ไม่มีข้อมูลรั่วไหล ถูกเปลี่ยนแปลง ทำลาย หรือเข้าถึงโดยที่ไม่ได้รับอนุญาต | - |

**๓) ความสามารถในการฟื้นฟูระบบ (Recoverability)**

ความสามารถในการฟื้นฟูระบบ ควรพิจารณาจากระยะเวลาและทรัพยากรที่ต้องใช้ในการฟื้นฟูระบบจากเหตุการณ์ภัยคุกคาม ซึ่งความรุนแรงของเหตุการณ์ภัยคุกคามและประเภทของทรัพย์สินสารสนเทศ เช่น ระบบงานสำคัญและข้อมูล เป็นต้น ที่ได้รับผลกระทบจะเป็นส่วนสำคัญในการพิจารณาถึงความสามารถ หรือความยากง่ายในการฟื้นฟูระบบ รวมทั้งทรัพยากรที่จำเป็นต้องใช้ โดยระดับของ Recoverability Effort มีดังนี้

| ระดับผลกระทบ | ความสามารถในการฟื้นฟูระบบ | ระยะเวลาการกู้คืนระบบ (SLA) |
|---|---|---|
| Not Recoverable | การกู้คืนไม่สามารถทำได้ โดยใช้กับเหตุการณ์ที่ข้อมูลได้รั่วไหลสู่สาธารณะแล้ว ทั้งนี้ ให้ใช้วิธีการติดตามและจำกัดการแพร่กระจาย รวมถึงการเยียวยาผลกระทบ | ภายใน ๒๔ ชั่งโมง |
| Extended | เวลาในการกู้คืนไม่สามารถคาดการณ์ได้ ต้องใช้ทรัพยากรและความช่วยเหลือจากภายนอก | ภายใน ๘ ชั่งโมง |
| Supplemented | เวลาในการกู้คืนสามารถคาดการณ์ได้ แต่ต้องมีการจัดหาทรัพยากรเพิ่ม | ภายใน ๔ ชั่งโมง |
| Regular | เวลาในการกู้คืนสามารถคาดการณ์ได้ โดยใช้ทรัพยากรที่มีอยู่ | ภายใน ๑ ชั่งโมง |

**๘.๒.๗ การติดต่อประสานงานและแจ้งข้อมูล**

๑) ทีมรับมือและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ แจ้งข้อมูลเกี่ยวกับเหตุการณ์ภัยคุกคามทางไซเบอร์ให้กับทีมงานทราบ เพื่อให้ทุกคนทราบและดำเนินการตามหน้าที่ความรับผิดชอบที่ได้มอบหมายไว้

๒) จัดให้มีการรายงานภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับบริการของโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้ผู้ที่เกี่ยวข้องทราบตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ. ๒๕๖๖ ดังนี้

(ก) กรณีมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นกับหน่วยงานรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศตาม ข้อ ๔ แห่งประกาศฯ ฉบับดังกล่าว ให้ใช้แบบฟอร์ม ก๑ โดยใช้แบบฟอร์มการรายงานตามกฎหมาย (รายละเอียดปรากฏตามภาคผนวก ช)

(ข) กรณีมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญต่อระบบของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศกับหน่วยงานรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามข้อ ๕ แห่งประกาศฯ ฉบับดังกล่าว ให้ใช้แบบฟอร์ม ก๒ รายงานไปยังสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ภายในระยะเวลา ๒๔ ชั่วโมง โดยใช้แบบฟอร์มการรายงานตามกฎหมาย (รายละเอียดปรากฏตามภาคผนวก ช)

(ค) หน่วยงานของรัฐหรือหน่วยงานควบคุมหรือกำกับดูแล จะต้องจัดทำและส่งรายงานสรุปจำนวนเหตุภัยคุกคามทางไซเบอร์ทั้งหมดที่ได้เกิดขึ้นกับข้อมูลหรือระบบสารสนเทศของหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ภายใต้การควบคุมหรือกำกับดูแลของตนในแต่ละปีภายในวันที่ ๓๑ มกราคม ของปีถัดไป ให้แก่สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ โดยให้แยกสถิติหมวดหมู่ตามแบบที่กำหนดในเอกสาร ก๓ โดยใช้แบบฟอร์มการรายงานตามกฎหมาย (รายละเอียดปรากฏตามภาคผนวก ช)

**๘.๓ ขั้นตอนการระงับภัยคุกคามทางไซเบอร์ การกำจัดเหตุภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ (Containment, Eradication & Recovery)**

เมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้นหรือเมื่อได้รับแจ้งเตือนการเกิดภัยคุกคามทางไซเบอร์ สำนักงาน กสม. จะต้องดำเนินการเพื่อระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ โดยควรกำหนดให้สอดคล้องกับความรุนแรงและระดับของภัยคุกคามทางไซเบอร์แต่ละระดับจนกระทั่งสามารถกู้คืนทรัพย์สินสำคัญทางสารสนเทศให้กลับมาดำเนินงานหรือให้บริการได้ตามปกติ ซึ่งการดำเนินการในขั้นตอนนี้อาจจะต้องกระทำควบคู่ไปกับการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ที่อาจมีการลุกลามหรือทวีความรุนแรงมากขึ้นเพื่อให้การระงับและการปราบปรามภัยคุกคามทางไซเบอร์ ตลอดจนฟื้นฟูระบบงานที่ได้รับผลกระทบจากภัยคุกคามทางไซเบอร์ให้สอดคล้องกับสถานการณ์ที่เปลี่ยนแปลงไป โดยดำเนินการดังต่อไปนี้

**๘.๓.๑ จำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์**

การดำเนินการเพื่อควบคุมความเสียหายจากภัยคุกคามทางไซเบอร์ และพยายามหยุด หรือลดผลกระทบให้ได้มากที่สุด เพื่อป้องกันไม่ให้เกิดความเสียหายเพิ่มมากขึ้น โดยการตัดสินใจเลือกใช้วิธีการที่เหมาะสม ดังนี้

- การปิดระบบ (Shut Down)
- การตัดการเชื่อมต่อทางเครือข่ายทั้งหมด (Network disconnection) ทั้งนี้อาจมียกเว้นการเชื่อมต่อสำหรับ Firewall และ WAF (กระบวนการตรวจสอบและตรวจจับกิจกรรมหรือเหตุการณ์ที่น่าสงสัยใด ๆ ที่เกิดขึ้นที่ปลายทางแบบเรียลไทม์)
- การหยุดการทำงานของฟังก์ชันที่เกี่ยวข้อง (Disabling Certain Functions)
- Redirect Network Traffic และ/หรือความสนใจของผู้บุกรุกไปยัง Blackhole/ Sandbox/ Honeypot
- การควบคุมกรณีการแพร่ระบาดของไวรัส อาจมีความจำเป็นต้องตัดการเชื่อมต่อส่วนที่ได้รับผลกระทบของเครือข่าย
- กรณีการโจมตีด้วยการ Hack อาจเกี่ยวข้องกับการปิดการใช้งานโปรไฟล์ หรือ Port บางอย่างบน Firewall

ทั้งนี้ การตัดสินใจเลือกใช้วิธีการควบคุมความเสียหายจะขึ้นอยู่กับลักษณะของสถานการณ์ที่กำลังเผชิญ ประเภทของภัยคุกคาม ระบบงานหรือบริการที่ได้รับผลกระทบ ระยะเวลาและทรัพยากรที่จำเป็นต่อการควบคุมความเสียหาย

**๘.๓.๒ เก็บรักษาหลักฐาน (Preservation of Evidence)** ก่อนเริ่มกระบวนการกู้คืน ต้องทำการเก็บรวบรวมและบันทึกหลักฐานทางคอมพิวเตอร์ หรืออุปกรณ์อื่น ๆ เพื่อสนับสนุนการสอบสวน หลักการบันทึกหลักฐานสำคัญที่รวบรวม มีดังนี้

๑) เป็นไปตามขั้นตอนที่กำหนดไว้ในกฎหมายข้อบังคับที่เกี่ยวกับหลักฐานดิจิทัล เพื่อให้สามารถนำไปใช้ได้ในชั้นศาล

๒) หลักฐานมีบันทึกการเข้าถึงและการกระทำการใด ๆ ต่อหลักฐานตลอดเวลาอย่างรัดกุม

๓) การเปลี่ยนตัวผู้ดูแล จำเป็นต้องมีการจัดทำบันทึกห่วงโซ่หลักฐาน (Chain of Custody) รายละเอียดเกี่ยวกับหลักฐาน ควรประกอบด้วยข้อมูลอย่างน้อยดังต่อไปนี้

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

๕) ชื่อ นามสกุล ตำแหน่ง และช่องทางการติดต่อผู้จัดเก็บและรักษาหลักฐานระหว่างการรับมือ Incident

๖) สถานที่จัดเก็บหลักฐาน

๗) ห้ามเปลี่ยนแปลงแก้ไขข้อมูลใด ๆ ก็ตามที่อยู่บนระบบหรืออุปกรณ์ที่ได้รับความเสียหายจากเหตุการณ์ที่เกิดขึ้น

๘) การเข้าถึงข้อมูลจะต้องถูกเข้าถึงได้เฉพาะที่จำเป็น และเข้าถึงโดยผู้เชี่ยวชาญเท่านั้น

การรวบรวมหลักฐานเพื่อจัดทำเป็นรายงานเพื่อนำเสนอให้กับผู้เกี่ยวข้องตามที่ได้รับมอบหมายรับทราบ และเฝ้าระวังเหตุการณ์ต่อไปเมื่อเกิดเหตุการณ์นี้เกิดขึ้น การติดตามผล ประกอบด้วยการทบทวนเหตุที่เกิดขึ้นการทำงานของเจ้าหน้าที่ หรือกระบวนการทำงาน หรือเครื่องมือที่ใช้ แล้วนำข้อมูลที่ได้ไปรายงานต่อผู้บริหาร เพื่อนำไปปรับปรุงแก้ไขกระบวนการหรือระบบรักษาความมั่นคงปลอดภัยด้านเทคนิคของสำนักงาน กสม. รวมถึงปรับปรุงจุดอื่น ๆ ที่อาจมีความเสี่ยงจากเหตุละเมิดความมั่นคงปลอดภัยในลักษณะเดียวกัน นอกจากนั้น หากต้องการค้นหาผู้กระทำความผิดและดำเนินคดีตามกฎหมาย ให้พิจารณาติดต่อขอความช่วยเหลือไปยังผู้เชี่ยวชาญจากภายนอก หรือเจ้าหน้าที่ของรัฐ เพื่อดำเนินการเก็บหลักฐานอิเล็กทรอนิกส์ตามกฎหมาย ทั้งนี้ การติดต่อไปยังหน่วยงานภายนอก ต้องได้รับการอนุมัติจากผู้บริหารระดับสูงก่อนดำเนินการ นอกจากนี้หน่วยงานต้องเก็บรักษาข้อมูลและพยานหลักฐานที่จำเป็น เพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์ หรือใช้ในกรณีที่ต้องการร้องทุกข์หรือดำเนินคดี เนื่องจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้นนั้น อาจเข้าลักษณะเป็นความผิดตามประมวลกฎหมายอาญา หรือพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม หรือกฎหมายอื่น ๆ ที่เกี่ยวข้อง

โดยการเก็บข้อมูลบางประเภทนั้นต้องดำเนินการตั้งแต่เริ่มตรวจพบว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้น เนื่องจากข้อมูลดังกล่าวอาจสูญหายไปในระหว่างที่ต้องระงับเหตุภัยคุกคามทางไซเบอร์นั้น หรืออาจถูกลบหรือทำลายโดยผู้โจมตี เมื่อมีการเก็บรวบรวมข้อมูลและหลักฐานที่จำเป็นแล้วให้นำข้อมูลและหลักฐานที่รวบรวมได้มาใช้ในการจัดทำบันทึกข้อมูลสถิติภัยคุกคามทางไซเบอร์ โดยอาจจัดทำเป็นรายเดือน/รายปี เพื่อเสนอต่อผู้ที่มีหน้าที่ดูแลและรับผิดชอบภายในหน่วยงาน และกำหนดขั้นตอนที่หน่วยงานควรดำเนินการ เพื่อป้องกันไม่ให้เกิดภัยคุกคามทางไซเบอร์ในลักษณะดังกล่าวขึ้นอีกในอนาคต

**หลักการดูแลรักษาหลักฐานทางดิจิทัลที่สำคัญมีดังนี้**

| หัวข้อ | การดำเนินการ |
|---|---|
| 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<br>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 MD๕, SHA๑, SHA๒๕๖ |
| 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 เนื่องจากหลักฐานที่พบสามารถนำไปใช้ในการยืนยัน

ได้ในชั้นศาล หลักฐานเหล่านี้จึงจะต้องได้รับการจัดการอย่างระมัดระวัง และรอบคอบเพื่อหลีกเลี่ยงข้อกล่าวหาว่าเป็นหลักฐานที่ปลอมหรือทำขึ้นมา

**๘.๓.๓ การกำจัดเหตุภัยคุกคามทางไซเบอร์ (Eradication)**

การดำเนินการกำจัดภัยคุกคาม ผู้เผชิญเหตุภัยคุกคามทางไซเบอร์จะต้องลบโปรแกรมหรือสิ่งที่ไม่พึงประสงค์ (malicious object) ออกให้หมด และตรวจสอบระบบที่ได้รับผลกระทบทั้งระบบเพื่อให้มั่นใจถึงความปลอดภัยด้านไซเบอร์ โดยพยายามให้เกิดความเสียหายต่อข้อมูลน้อยที่สุด ทั้งนี้ การค้นหาสาเหตุของเหตุละเมิดความมั่นคงปลอดภัย และดำเนินการแก้ไขเพื่อกำจัดเหตุการณ์ดำเนินงานทั้งหมดในขั้นตอนนี้ ซึ่งวิธีการการกำจัดสาเหตุที่ทำให้เกิด Incident และผลกระทบ ได้แก่

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

**๘.๓.๔ เรียกใช้งานกระบวนการกู้คืน (Recovery Process)**

การดำเนินการเพื่อนำระบบให้กลับมาอยู่ในสถานะปกติ ต้องมีการตรวจสอบอย่างถี่ถ้วน เพื่อให้มั่นใจว่าระบบสารสนเทศที่เกี่ยวข้องจะได้รับการปกป้องอย่างเหมาะสม โดยรวมถึงการเฝ้าระวังเหตุอย่างใกล้ชิด และตรวจสอบระบบที่ถูกกู้คืนในระยะแรกของการนำกลับมาใช้งาน เพื่อป้องกันการเกิดเหตุซ้ำ ทั้งนี้ สิ่งที่ต้องดำเนินการ ได้แก่

- การทำกู้คืนระบบ (Operating System หรือ Application Software) จากไฟล์ Master Image ที่มีความปลอดภัย
- การกู้คืนข้อมูลจาก Backup Storage

**๘.๓.๕ ดำเนินการสอบสวน (Investigate) สาเหตุและผลกระทบของเหตุการณ์**

เพื่อทราบสาเหตุและผลกระทบของเหตุการณ์ที่เกิดขึ้น ซึ่งเป็นขั้นตอนสำคัญในการจัดการกับเหตุการณ์ทางความมั่นคงปลอดภัยไซเบอร์ ดังนี้

๑) ระบุและบันทึกข้อมูล

- รวบรวมข้อมูลที่เกี่ยวข้องกับเหตุการณ์ที่เกิดขึ้น เช่น บันทึกเหตุการณ์ รายงานการแจ้งเตือน และข้อมูลเชิงลึกอื่น ๆ ที่สามารถช่วยในการสอบสวน

๒) การวิเคราะห์ข้อมูล

- วิเคราะห์ข้อมูลเพื่อให้เข้าใจถึงลักษณะและลักษณะของเหตุการณ์ที่เกิดขึ้น
- วิเคราะห์และสรุปความสัมพันธ์ระหว่างข้อมูลที่แตกต่างกันเพื่อหาแนวทางในการสอบสวน

๓) การสอบสวนเทคนิค

- ใช้เทคนิคทางเทคโนโลยีและเครื่องมือสำหรับการสอบสวน เช่น การวิเคราะห์บล็อกกิจกรรม (Activity Logs) การตรวจสอบบัญชีผู้ใช้ การวิเคราะห์แพทเทิร์นของการโจมตี เป็นต้น

๔) การสัมภาษณ์

- สัมภาษณ์บุคคลที่เกี่ยวข้อง เพื่อให้ได้ข้อมูลเพิ่มเติมเกี่ยวกับเหตุการณ์ที่เกิดขึ้น รวมถึงการสัมภาษณ์ผู้รับผิดชอบระบบและพยานพิสูจน์อื่น ๆ

๕) การศึกษาข้อความและโค้ด

- การศึกษาข้อความและโค้ดที่เกี่ยวข้อง เพื่อหาหลักฐานและความรู้เกี่ยวกับวิธีการโจมตี และช่องโหว่ที่เป็นไปได้

๖) การสรุปสมมติฐาน

- สรุปสมมติฐานเกี่ยวกับสาเหตุของเหตุการณ์ และแนวทางที่เป็นไปได้ที่สามารถอธิบายได้

๗) การเขียนรายงาน

- เขียนรายงานสำหรับการสอบสวนเพื่อระบุสาเหตุและผลกระทบของเหตุการณ์ รวมถึงแนวทางแก้ไขและป้องกันในอนาคต

๘) การบูรณาการและการวางแผนการป้องกันในอนาคต

- บูรณาการข้อมูลและความรู้ที่ได้จากการสอบสวนเพื่อวางแผนการป้องกันในอนาคตและเพิ่มความเข้มแข็งของระบบความมั่นคงปลอดภัย

**๘.๓.๖ ดำเนินการตามระเบียบวิธีการมีส่วนร่วม (Engagement Protocols) กับบุคคลภายนอก หรือแนวปฏิบัติการบริหารจัดการบุคคลภายนอก ซึ่งรวมถึงรายละเอียดการติดต่อ** ตัวอย่างเช่น ผู้ให้บริการด้านนิติวิทยาศาสตร์/การกู้คืนและการบังคับใช้กฎหมายเพื่อดำเนินคดี

**๘.๔ ขั้นการดำเนินการภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ (Post-Incident Activity)**

หลังจากที่เกิดเหตุการณ์ภัยคุกคามทางไซเบอร์เกิดขึ้นแล้ว การเก็บรักษาข้อมูลและพยานหลักฐานที่จำเป็น เพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์ หรือใช้ในกรณีที่ต้องการร้องทุกข์หรือดำเนินคดี เนื่องจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้น อาจเข้าลักษณะเป็นความผิดตามประมวล กฎหมายอาญา หรือพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม หรือกฎหมายอื่น ๆ ที่เกี่ยวข้อง โดยมีขั้นตอนที่ควรดำเนินการเพื่อช่วยในการรับมือและป้องกันเหตุการณ์ที่เป็นไปได้อีกในอนาคต ดังนี้

**๘.๔.๑ ขั้นตอนของการดำเนินการภายหลังการแก้ปัญหา**

๑) การวินิจฉัย (Diagnosis) การทำการวินิจฉัยเหตุการณ์เพื่อให้เข้าใจถึงลักษณะของการโจมตีหรือปัญหาที่เกิดขึ้น รวมถึงการหาสาเหตุของเหตุการณ์ให้เจ้าหน้าที่สามารถดำเนินการแก้ไขได้อย่างมีประสิทธิภาพ

๒) การแก้ไข (Remediation) การดำเนินการแก้ไขปัญหาที่เกิดขึ้น รวมถึงการปรับปรุงระบบเพื่อป้องกันไม่ให้เหตุการณ์นั้นเกิดขึ้นอีกต่อไป การแก้ไขอาจมีการปรับแก้ระบบเทคโนโลยี การเปลี่ยนแปลงกระบวนการ หรือการปรับเปลี่ยนนโยบายในองค์กร

๓) การทบทวนเหตุการณ์ (Incident Review) การทบทวนเหตุการณ์เพื่อทราบถึงสาเหตุและผลกระทบที่เกิดขึ้น รวมถึงการตรวจสอบกระบวนการและมาตรการที่ดำเนินการและการตอบสนองต่อเหตุการณ์

๔) การประเมินความเสี่ยง (Risk Assessment) การประเมินความเสี่ยงที่อาจเกิดจากเหตุการณ์นั้น ๆ และการดำเนินการในอนาคต ซึ่งอาจจะมีการปรับปรุงและปรับเปลี่ยนเทคโนโลยีและนโยบายตามความเสี่ยงที่พบ

๕) การปรับปรุงและการเรียนรู้ (Improvement and Learning) การใช้ข้อมูลและประสบการณ์จากเหตุการณ์เพื่อปรับปรุงกระบวนการ นโยบาย และเทคโนโลยี อาจรวมถึงการอบรมพนักงานใหม่และการปรับปรุงระบบการเฝ้าระวังและการตอบสนอง

๖) การรายงาน (Reporting) การรายงานเหตุการณ์และผลกระทบที่เกิดขึ้นให้กับผู้บริหาร และหน่วยงานที่เกี่ยวข้อง เพื่อให้ทราบถึงสถานะและข้อกำหนดในการปรับปรุงและการเรียนรู้

๗) การเขียนรายงานการสำรวจ (Forensic Report Writing) การสร้างรายงานทาง forensic เพื่อระบุประเภทของการโจมตีและเทคนิคที่ใช้ รวมถึงการเก็บหลักฐานและข้อมูลที่สามารถใช้ในการจัดการคดีหรือการแก้ไขปัญหาในอนาคต

๘) การปรับปรุงนโยบายและขั้นตอนการดำเนินการ (Policy and Procedure Enhancement) การปรับปรุงนโยบายและขั้นตอนการดำเนินการที่เกี่ยวข้องกับการรับมือกับภัยคุกคามเพื่อป้องกันเหตุการณ์ที่เป็นไปได้อีกในอนาคต

๙) การสร้างแผนการป้องกันและการตอบสนอง (Prevention and Response Planning) การพัฒนาแผนการป้องกันและการตอบสนองเพื่อเตรียมความพร้อมในการรับมือกับภัยคุกคามในอนาคต

๑๐) การควบคุมความเสี่ยง (Risk Control) การนำเสนอและดำเนินการเพื่อควบคุมความเสี่ยงตามผลจากการประเมินความเสี่ยงที่เกิดขึ้น

๑๐.๑) ขั้นตอนการจัดเก็บและรักษาข้อมูลและพยานหลักฐานทางไซเบอร์ เป็นขั้นตอนสำคัญที่ต้องปฏิบัติตามอย่างเคร่งครัดเพื่อให้ข้อมูลเหล่านั้นมีความปลอดภัยและสามารถใช้งานได้อย่างเหมาะสม

๑๐.๑.๑) การระบุข้อมูลที่จะเก็บรักษา

- ระบุประเภทของข้อมูลที่จะเก็บรักษาอย่างชัดเจน เช่น ข้อมูลส่วนบุคคล เอกสารสำคัญ ข้อมูลการเงิน เป็นต้น

๑๐.๑.๒) การใช้มาตรการความปลอดภัย

- ใช้มาตรการความปลอดภัยที่เหมาะสมเพื่อป้องกันข้อมูลจากการเข้าถึงโดยมิชอบ รวมถึงการใช้ระบบการเข้ารหัสข้อมูล การตรวจจับและป้องกันการบุกรุก เป็นต้น

๑๐.๑.๓) การใช้เทคโนโลยีการจัดเก็บข้อมูลที่เหมาะสม

- เลือกใช้เทคโนโลยีการจัดเก็บข้อมูลที่เหมาะสมกับประเภทข้อมูล เช่น ฐานข้อมูลที่ปลอดภัย บริการคลาวด์ เป็นต้น

๑๐.๑.๔) การสร้างการสำรองข้อมูล (Backup)

- สร้างการสำรองข้อมูลอย่างเป็นระบบเพื่อป้องกันข้อมูลจากการสูญหายหรือเสียหาย โดยการใช้วิธีการสำรองข้อมูลแบบที่เหมาะสม เช่น การสำรองบนคลาวด์ หรือการใช้เทคโนโลยี RAID

๑๐.๑.๕) การตรวจสอบความปลอดภัยเป็นระยะ ๆ

- ตรวจสอบและปรับปรุงมาตรการความปลอดภัยของระบบเก็บข้อมูลอย่างสม่ำเสมอเพื่อให้มั่นใจว่าข้อมูลยังคงปลอดภัย

๑๐.๑.๖) การกำหนดสิทธิ์การเข้าถึงข้อมูล:

- กำหนดสิทธิ์และการเข้าถึงข้อมูลให้เหมาะสมแก่ผู้ใช้งานเพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๑๐.๑.๗) การปฏิบัติตามกฎหมายและข้อบังคับ

- ปฏิบัติตามกฎหมายและข้อบังคับที่เกี่ยวข้องกับการจัดเก็บและรักษาข้อมูลทางไซเบอร์ อย่างเคร่งครัด

๑๐.๑.๘) การบันทึกกิจกรรมการเข้าถึงข้อมูล

- บันทึกกิจกรรมการเข้าถึงข้อมูลเพื่อติดตามและตรวจสอบการใช้ข้อมูลอย่างมีประสิทธิภาพ

๑๐.๑.๙) การทำคู่มือและขั้นตอนการจัดเก็บข้อมูล

- สร้างคู่มือและขั้นตอนการจัดเก็บข้อมูลที่ชัดเจนและเป็นมาตรฐาน เพื่อให้ทุกคนในองค์กรสามารถปฏิบัติตามได้อย่างเป็นระบบ

๑๐.๑.๑๐) การรักษาความลับและการปกป้องข้อมูล

- รักษาความลับของข้อมูลและพยานหลักฐานที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์อย่างเคร่งครัด เพื่อป้องกันการรั่วไหลของข้อมูลที่มีความสำคัญ

๑๐.๒) การทบทวนหลังการดำเนินการ (After-Action Review Process) เพื่อการเรียนรู้จากประสบการณ์ ปรับปรุงกระบวนการ ป้องกันการเกิดซ้ำ และเตรียมความพร้อมในการเผชิญหน้ากับอุบัติเหตุทางไซเบอร์ในอนาคต

๑๐.๒.๑) รวบรวมข้อมูลเกี่ยวกับเหตุการณ์:

- รวบรวมข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้น รวมถึงลักษณะของการโจมตี เทคนิคที่ใช้ และผลกระทบที่เกิดขึ้นกับระบบและข้อมูล

๑๐.๒.๒) ทบทวนกระบวนการและมาตรการป้องกัน:

- ตรวจสอบกระบวนการที่ใช้ในการตอบสนองต่อการโจมตีและมาตรการความปลอดภัยที่เคยวางไว้ การทบทวนนี้ช่วยให้องค์กรเข้าใจถึงความสามารถและข้อบกพร่องของระบบปัจจุบัน

๑๐.๒.๓) วิเคราะห์ความสำเร็จและข้อผิดพลาด

- พิจารณาสิ่งที่ดำเนินไปได้ดีและสิ่งที่ต้องปรับปรุง ระบุข้อผิดพลาดที่เกิดขึ้นและปัจจัยที่เกี่ยวข้อง

๑๐.๒.๔) สรุปข้อเสนอแนะ

- สรุปสิ่งที่เรียนรู้และข้อเสนอแนะที่สามารถเพิ่มประสิทธิภาพในการจัดการภัยคุกคามทางไซเบอร์ในอนาคต

๑๐.๒.๕) การแก้ไขและการปรับปรุง

- จัดทำแผนการแก้ไขข้อผิดพลาดและปรับปรุงกระบวนการต่าง ๆ เพื่อเตรียมความพร้อมในการรับมือกับภัยคุกคามทางไซเบอร์ในอนาคต

๑๐.๒.๖) การสร้างรายงาน

- จัดทำรายงานการทบทวนภัยคุกคามทางไซเบอร์ที่เกิดขึ้น รวมถึงการแสดงผลของการทบทวนและแนวทางการปรับปรุงต่อไป

๑๐.๒.๗) การส่งเสริมวัฒนธรรมการเรียนรู้

- สร้างวัฒนธรรมในองค์กรที่เน้นการเรียนรู้จากประสบการณ์ โดยส่งเสริมให้ทุกคนมีส่วนร่วมในกระบวนการทบทวน

**๘.๕ การจัดทำรายการตรวจสอบการจัดการเหตุการณ์ (Incident Handling Checklist)**

สำนักงาน กสม. จะต้องจัดทำรายการตรวจสอบการจัดการเหตุการณ์ (Incident Handling Checklist) ที่เกิดขึ้น โดยมีขั้นตอนในการจัดทำรายการตรวจสอบการจัดการเหตุการณ์ที่ควรพิจารณาเพื่อให้การตอบสนองต่อภัยคุกคามมีประสิทธิภาพ ดังนี้

๘.๕.๑ การวิเคราะห์ความเสี่ยงและการตอบสนองทันใจ (Immediate Risk Analysis and Response)

- ประเมินระดับความรุนแรงของเหตุการณ์ รายละเอียดตามตารางแสดงระดับความรุนแรงของเหตุการณ์ (Severity Procedure) ดังนี้

| ระดับขั้นความรุนแรง (Severity Level) | คุณลักษณะ (Characteristics) |
|---|---|
| วิกฤติ | ๑. บริการที่สำคัญที่ให้บริการบนเครือข่ายของสำนักงาน กสม. ถูกโจมตีในระดับร้ายแรง ส่งผลกระทบรุนแรงต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศของสำนักงาน กสม. มีการลุกลามกระจายเป็นวงกว้าง ระบบถูกโจมตีทำลายจนไม่สามารถทำงานให้บริการได้ หรือ<br>๒. ข้อมูลที่มีความสำคัญหรือข้อมูลที่เป็นความลับถูกบุกรุกและขโมยข้อมูลของหน่วยงานไปเผยแพร่ต่อสาธารณชนจนทำให้เกิดความเสียหายอย่างร้ายแรง หรือ<br>๓. สื่อสังคมออนไลน์ที่ใช้ประชาสัมพันธ์ข่าวสารของหน่วยงาน/เว็บไซต์ของสำนักงาน กสม. ถูกขโมยบัญชีผู้ใช้งาน หรือมีทำลายข้อมูลหรือการแก้ไขเปลี่ยนแปลงเนื้อหาโดยส่งผลกระทบต่อภาพลักษณ์ของสำนักงาน กสม. อย่างร้ายแรง |
| ร้ายแรง | ๑. บริการที่สำคัญที่ให้บริการบนเครือข่ายของสำนักงาน กสม. ถูกโจมตีส่งผลกระทบต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศของสำนักงาน กสม. จนทำให้ระบบหยุดชะงัก/เสียหายจนไม่สามารถทำงานให้บริการได้ หรือ<br>๒. ข้อมูลที่มีความสำคัญหรือข้อมูลที่เป็นความลับถูกเข้าถึงโดยผู้ที่ไม่มีสิทธิ์ในการเข้าถึงข้อมูล เช่น เกิดจากการที่มีผู้บุกรุกทำการเจาะระบบเพื่อเข้าถึงข้อมูลสำคัญในระบบได้สำเร็จ หรือมีการบุกรุกเพื่อขโมยข้อมูลรายชื่อผู้ใช้งานหรือรหัสผ่านได้สำเร็จ เป็นต้น<br>๓. ข้อมูลในระบบของหน่วยงานถูกเข้าถึงหรือถูกแก้ไขเปลี่ยนแปลงข้อมูลโดยผู้ที่ไม่มีสิทธิ์ในการเข้าถึงข้อมูล หรือทำให้ข้อมูลได้รับความเสียหายโดยไม่ได้รับอนุญาต เช่น ระบบมีการติดไวรัสหรือเวิร์ม เป็นต้น |
| ไม่ร้ายแรง | ๑. บริการที่สำคัญที่ให้บริการบนเครือข่ายของสำนักงาน กสม. ถูกผู้ไม่ประสงค์ดีพยายามโจมตี/เจาะระบบ ระบบยังสามารถทำงานให้บริการได้ตามปกติ แต่ส่งผลทำให้ระบบช้าลง ไปหรือบางฟังก์ชั่นไม่สามารถใช้งานได้ แต่ไม่ถึงขนาดที่จะทำให้ระบบหรือบริการต้องหยุดชะงักหรือไม่สามารถใช้งานได้ทั้งหมด<br>๒. มีความพยายามเข้าถึงข้อมูลในระบบของหน่วยงาน โดยผู้ที่ไม่มีสิทธิ์ในการเข้าถึงข้อมูล |

- ระบุเหตุการณ์และระดับความรุนแรง ตามตารางดังนี้

| ชื่อเหตุการณ์ | ระดับขั้นความรุนแรง (Severity Level) | | |
|---|---|---|---|
| | ไม่ร้ายแรง | ร้ายแรง | วิกฤติ |
| ข้อมูลส่วนบุคคลหรือข้อมูลที่เป็นความลับของหน่วยงานรั่วไหล | | | × |
| ตรวจพบภัยคุกคามบนระบบเครือข่ายของหน่วยงาน ประเภทข่มขู่เรียกค่าไถ่ | | | × |
| บัญชีสื่อสังคมออนไลน์ของสำนักงาน กสม. /เว็บไซต์สำนักงาน กสม. ถูกขโมยบัญชีผู้ใช้งาน หรือมีทำลายข้อมูลหรือการแก้ไขเปลี่ยนแปลงเนื้อหา | | | × |
| ตรวจพบการโจมตีด้วยวิธีการ SQL Injection | | × | |
| ตรวจพบการโจมตีด้วยวิธีการ Directory Traversal (การเข้าถึงไฟล์ผ่านช่องโหว่ด้านความปลอดภัยของระบบ) | | × | |
| ระบบสารสนเทศถูกโจมตีจากภัยคุกคามทางไซเบอร์ เช่น การติดไวรัสหรือเวิร์ม | | × | |
| ตรวจพบการโจมตีด้วยวิธีการสแกนช่องโหว่ | × | | |
| มีการพยายามคาดเดารหัสผ่านผู้ใช้งานเป็นจำนวนมาก | × | | |
| อีเมลโดเมน @nhrc.or.th ได้รับอีเมลหลอกลวง | × | | |

- ดำเนินการทันทีในการล็อกเครื่องหรือระบบที่เสี่ยงหรือที่โจมตีอยู่
- แจ้งผู้เกี่ยวข้องที่เกี่ยวข้องเพื่อให้ความช่วยเหลือและการสนับสนุน

๘.๕.๒ การรายงานเหตุการณ์ (Incident Reporting)

- รายงานเหตุการณ์ให้แก่ทีมงานที่เกี่ยวข้อง โดยระบุรายละเอียดที่เป็นประโยชน์ เช่น วัน เวลา ที่เกิดเหตุ รายละเอียดของเหตุการณ์ และผู้ที่มีส่วนเกี่ยวข้อง

๘.๕.๓ การประเมินและการจัดลำดับความสำคัญ (Assessment and Prioritization)

- ประเมินผลกระทบที่เกิดขึ้นและการเสี่ยงที่เป็นไปได้
- จัดลำดับความสำคัญของเหตุการณ์ตามระดับความรุนแรง

๘.๕.๔ การแก้ไขและการควบคุม (Mitigation and Control)

- ดำเนินการในการแก้ไขเหตุการณ์เพื่อลดความเสี่ยงและควบคุมสถานการณ์
- ใช้เครื่องมือและเทคโนโลยีที่เหมาะสมเพื่อตรวจสอบและระงับการโจมตี
- รักษาข้อมูลและบันทึกข้อมูลเพื่อการวิเคราะห์ในอนาคต

๘.๕.๕ การสืบค้นและการวิเคราะห์ (Investigation and Analysis)

- สืบค้นและวิเคราะห์เหตุการณ์เพื่อหาสาเหตุและลักษณะของการโจมตี
- ระบุบทบาทและผู้ที่มีส่วนเกี่ยวข้องในการเกิดเหตุการณ์

๘.๕.๖ การจัดการการสื่อสาร (Communication Management)

- จัดการการสื่อสารกับผู้ที่เกี่ยวข้องภายในองค์กร เช่น บุคลากรทางบริหาร และทีมงานที่เกี่ยวข้อง

- จัดการการสื่อสารกับผู้ใช้และสื่อมวลชน (สำหรับเหตุการณ์ที่มีผลกระทบต่อสาธารณชน)

๘.๕.๗ การทบทวนและการเรียนรู้ (Review and Learn)

- ทบทวนกระบวนการการจัดการเหตุการณ์ทุกครั้งหลังจากเกิดเหตุการณ์

- วิเคราะห์เหตุการณ์เพื่อเรียนรู้จากประสบการณ์และปรับปรุงกระบวนการในอนาคต

๘.๕.๘ การเก็บรักษาบันทึกและการรายงาน (Documentation and Reporting)

- เก็บบันทึกของเหตุการณ์ทั้งหมด รวมถึงขั้นตอนการตอบสนองและการแก้ไข

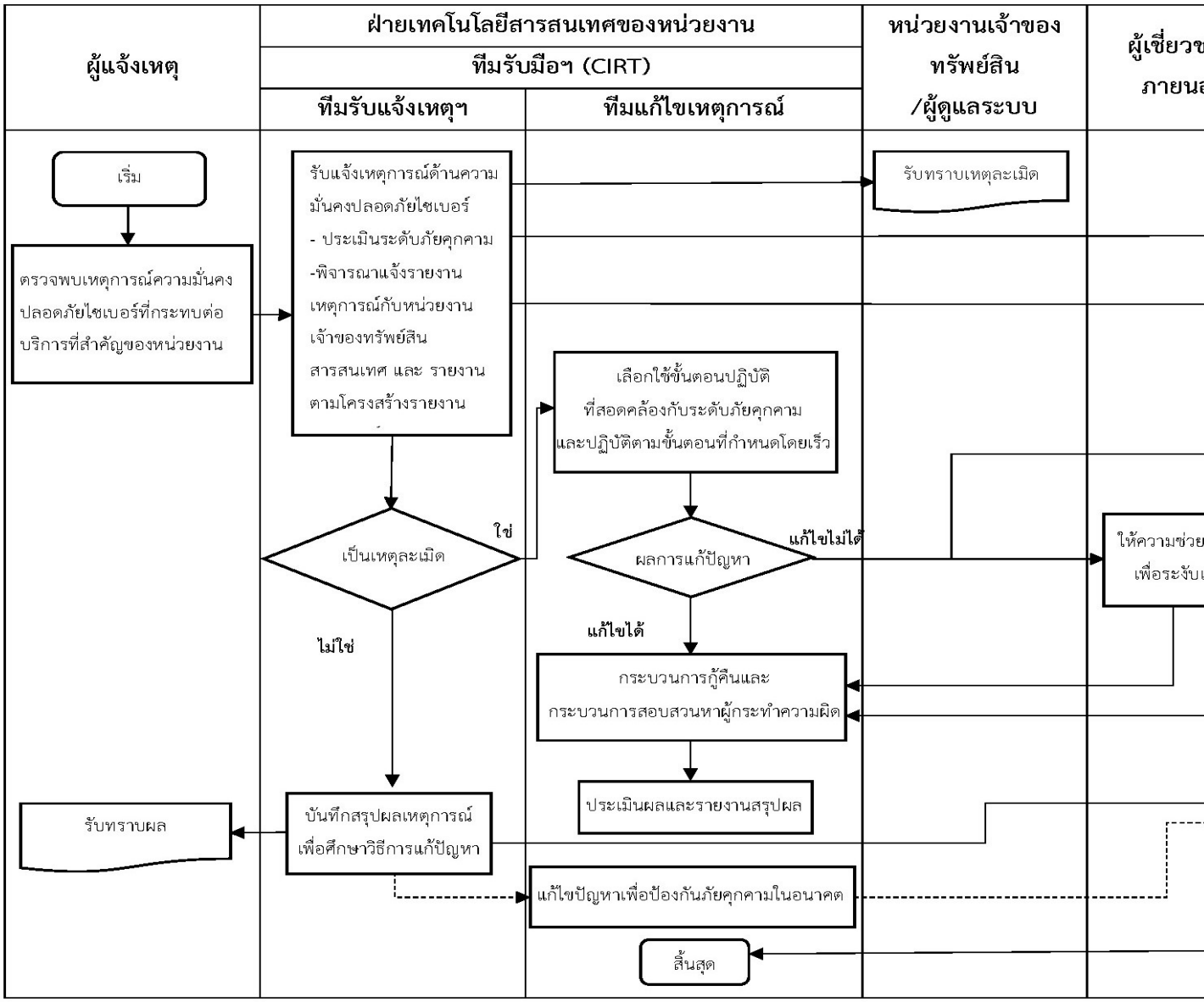
- รายงานการเกิดเหตุการณ์ตามความเหมาะสม และตามนโยบายขององค์กร

## ๙. เอกสารที่เกี่ยวข้อง (Related Document)

| รหัสเอกสาร | ชื่อเอกสาร |
|---|---|
| - | ใบรายงานผลภัยคุกคามทางคอมพิวเตอร์ |
| - | |
| - | |
| | |
| | |

# ภาคผนวก ก

## แผนผังโครงสร้างขั้นตอนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response)


ผู้แจ้งเหตุ
ฝ่ายเทคโนโลยีสารสนเทศของหน่วยงาน
ทีมรับมือฯ (CIRT)
ทีมรับแจ้งเหตุฯ
ทีมแก้ไขเหตุการณ์
หน่วยงานเจ้าของทรัพย์สิน /ผู้ดูแลระบบ
ผู้เชี่ยวช
ภายนอ
เริ่ม
ตรวจพบเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ที่กระทบต่อบริการที่สำคัญของหน่วยงาน
รับแจ้งเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์
- ประเมินระดับภัยคุกคาม
-พิจารณาแจ้งรายงานเหตุการณ์กับหน่วยงานเจ้าของทรัพย์สิน สารสนเทศ และ รายงานตามโครงสร้างรายงาน
รับทราบเหตุละเมิด
เลือกใช้ขั้นตอนปฏิบัติที่สอดคล้องกับระดับภัยคุกคามและปฏิบัติตามขั้นตอนที่กำหนดโดยเร็ว
เป็นเหตุละเมิด
ใช่
ไม่ใช่
ผลการแก้ปัญหา
แก้ไขไม่ได้
แก้ไขได้
ให้ความช่วย
เพื่อระงับเ
กระบวนการกู้คืนและกระบวนการสอบสวนหาผู้กระทำความผิด
ประเมินผลและรายงานสรุปผล
รับทราบผล
บันทึกสรุปผลเหตุการณ์เพื่อศึกษาวิธีการแก้ปัญหา
แก้ไขปัญหาเพื่อป้องกันภัยคุกคามในอนาคต
สิ้นสุด

**ภาคผนวก ข**

**โครงสร้างทีมงานรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์**

**(Cyber Incident Response Team: CIRT)**

**ผู้รับแจ้งเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ภายในสำนักงาน กสม.**

| ลำดับ | ชื่อ – นามสกุล | ระยะเวลาในการปฏิบัติงาน | ช่องทางการติดต่อสื่อสาร | หน้าที่ | ความรับผิดชอบ |
|---|---|---|---|---|---|
| ๑ | นายวณัท รุจนันตกุล<br>เจ้าหน้าที่สำนักดิจิทัลสิทธิมนุษยชน | ๒๔ ชั่วโมง/ ๗ วัน | ๐๘๑-๓๗๖-๘๘๖๓ | ผู้รับแจ้งเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ภายในหน่วยงาน | เจ้าหน้าที่รับแจ้งเหตุฯ |
| ๒ | นายนพดล คงสมฤทธิ์<br>เจ้าหน้าที่สำนักดิจิทัลสิทธิมนุษยชน | ๒๔ ชั่วโมง/ ๗ วัน | ๐๙๒-๙๕๙-๑๙๒๕ | ผู้รับแจ้งเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ภายในหน่วยงาน | เจ้าหน้าที่รับแจ้งเหตุฯ |

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

สำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ ใช้โมเดลโครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ในลักษณะแบบรวมศูนย์ ประกอบด้วย ทีมงานรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (ลำดับที่ ๑ - ๑๒) และทีมงานสนับสนุนการดำเนินการของแผนรับมือฉบับนี้ (ลำดับที่ ๑๒ - ๑๙)

| ลำดับ | ชื่อ นามสกุล | ช่องทางการติดต่อสื่อสาร | หน้าที่ | ความรับผิดชอบ |
|---|---|---|---|---|
| ๑ | นายภาณุวัฒน์ ทองสุข<br>ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง | ๐๒ ๑๔๑ ๓๘๒๘<br>panuwat_t@nhrc.or.th | ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง | รับผิดชอบการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา จัดหา สนับสนุนด้านงบประมาณและสื่อสารกับผู้บริหารของหน่วยงาน |
| ๒ | นางสาวจิราภรณ์ ทองคำวัฒนะ<br>ผู้อำนวยการสำนักดิจิทัลสิทธิมนุษยชน | ๐๒ ๑๔๑ ๓๙๐๙<br>jiraporn.thong@nhrc.or.th | หัวหน้าทีมรับมือฯ<br>(Team manager) | ติดตาม กำกับ ดูแล ควบคุมเจ้าหน้าที่เกี่ยวกับการป้องกันความมั่นคงปลอดภัยไซเบอร์ |

| ลำดับ | ชื่อ นามสกุล | ช่องทางการติดต่อสื่อสาร | หน้าที่ | ความรับผิดชอบ |
|---|---|---|---|---|
| ๓ | นายคเณศศักดิ์ ชัยอินทร์<br>หัวหน้ากลุ่มงานพัฒนาระบบสารสนเทศและฐานข้อมูล<br>สำนักดิจิทัลสิทธิมนุษยชน | ๐๒ ๑๔๑ ๓๙๐๙<br>khanatsak_c@nhrc.or.th | รองหัวหน้าทีมรับมือฯ<br>(Deputy team manager) | ทำหน้าที่แทนกรณีหัวหน้าทีมรับมือฯ ไม่อยู่หรือไม่สามารถปฏิบัติงานได้ |
| ๔ | นางสุพรรณี ชาติสุข<br>หัวหน้ากลุ่มงานคอมพิวเตอร์และระบบเครือข่าย | ๐๒ ๑๔๑ ๓๘๙๗<br>๐๘๕-๖๖๑-๗๑๗๘<br>supunnee_c@nhrc.or.th | เจ้าหน้าที่รับมือฯ ด้านความปลอดภัย (Incident lead) (หลัก) | ทำหน้าที่กำกับดูแลการปฏิบัติงานของศูนย์ปฏิบัติการความมั่นคงปลอดภัยและเฝ้าระวังความมั่นคงปลอดภัยสารสนเทศ ให้สามารถควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์ได้ |
| ๕ | นางสาวจิราพร อาจเจริญ<br>หัวหน้ากลุ่มงานสารสนเทศ | ๐๘๐-๐๗๙-๑๕๗๕<br>jirapon_a@nhrc.or.th | เจ้าหน้าที่เฝ้าระวังความมั่นคงปลอดภัยระบบสารสนเทศ | ทำหน้าที่ควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์ |
| ๖ | นายวณัท รุจนันตกุล<br>เจ้าหน้าที่สำนักดิจิทัลสิทธิมนุษยชน | ๐๒ ๑๔๑ ๓๘๘๔<br>๐๘๑-๓๗๖-๘๘๖๓<br>wanut_r@nhrc.or.th | เจ้าหน้าที่รับมือฯ ด้านความปลอดภัย (สำรอง) | ทำหน้าที่แทนกรณีเจ้าหน้าที่รับมือฯ ด้านความปลอดภัยฯ (หลัก) ไม่อยู่ หรือ ไม่สามารถปฏิบัติงานได้ |
| ๗ | นายนพดล คงสมฤทธิ์<br>เจ้าหน้าที่สำนักดิจิทัลสิทธิมนุษยชน | ๐๙๒-๙๕๙-๑๙๒๕<br>kong_somrit@nhrc.or.th | เจ้าหน้าที่เทคนิค (Technical lead) (หลัก) | ทำหน้าที่ให้ความเห็นเกี่ยวกับแนวทางที่เหมาะสมในการควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์ |
| ๘ | นายสุทธิจิตต์ เวชโสภณ<br>เจ้าหน้าที่สำนักดิจิทัลสิทธิมนุษยชน | ๐๒ ๑๔๑ ๑๙๘๖<br>๐๘๔-๖๓๔-๕๙๑๙<br>suttijit_w@nhrc.or.th | เจ้าหน้าที่เทคนิค (สำรอง) | ทำหน้าที่แทนกรณีเจ้าหน้าที่เทคนิค (หลัก) ไม่อยู่หรือ ไม่สามารถปฏิบัติงานได้ |

| ลำดับ | ชื่อ นามสกุล | ช่องทางการติดต่อสื่อสาร | หน้าที่ | ความรับผิดชอบ |
|---|---|---|---|---|
| ๙ | นายนที เกตุรัตน์<br>เจ้าหน้าที่สำนักดิจิทัลสิทธิมนุษยชน | ๐๘๔-๗๐๐-๖๙๕๗<br>natee_g@nhrc.or.th | เจ้าหน้าที่รับมือฯ<br>ด้านเครือข่าย<br>(Incident lead) (หลัก) | ทำหน้าที่กำกับดูแลการปฏิบัติงานของศูนย์ปฏิบัติการระบบเครือข่าย และประสานงานระหว่างศูนย์ฯ เมื่อต้องการความช่วยเหลือ |
| ๑๐ | นางสาวกฤติกา ปัญญาโรจน์สุข<br>เจ้าหน้าที่สำนักดิจิทัลสิทธิมนุษยชน | ๐๒ ๑๔๑ ๓๘๘๔<br>kittika_p@nhrc.or.th | เจ้าหน้าที่รับมือฯ<br>ด้านเครือข่าย (สำรอง) | ทำหน้าที่แทนกรณีเจ้าหน้าที่รับมือฯ ด้านเครือข่าย (หลัก) ไม่อยู่ หรือ ไม่สามารถปฏิบัติงานได้ |
| ๑๑ | นายกุลกฤษ งามเกิดเกียรติ<br>เจ้าหน้าที่สำนักดิจิทัลสิทธิมนุษยชน | ๐๒ ๑๔๑ ๓๘๙๖<br>๐๖๕-๙๕๑-๕๒๔๕<br>kunlakit@nhrc.or.th | เจ้าหน้าที่รับมือฯ<br>ด้านเว็บไซต์ฯ<br>(Incident lead) (หลัก) | ทำหน้าที่ช่วยเหลือ กลุ่มเว็บไซต์ฯ และประสานงานระหว่างศูนย์ฯ เมื่อต้องการความช่วยเหลือ |
| ๑๒ | นางสาวนพรัตน์ พนอพัฒนาชัย<br>เจ้าหน้าที่สำนักดิจิทัลสิทธิมนุษยชน | ๐๒ ๑๔๑ ๓๘๘๑<br>nopparat@nhrc.or.th | เจ้าหน้าที่รับมือฯ<br>ด้านเว็บไซต์ฯ (สำรอง) | ทำหน้าที่แทนกรณีเจ้าหน้าที่รับมือฯ ด้านเว็บไซต์ (หลัก) ไม่อยู่ หรือ ไม่สามารถปฏิบัติงานได้ |
| ๑๓ | นางจิราพร ขาวจันทร์<br>เจ้าหน้าที่สำนักดิจิทัลสิทธิมนุษยชน | ๐๘๙-๒๐๙-๖๖๖๔<br>jirapon_k@nhrc.or.th | ผู้บริหารจัดการความเสี่ยง | ทำหน้าที่ประเมินผลกระทบ-ความเสี่ยงเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ |
| ๑๔ | ผู้ตรวจสอบและทดสอบจากภายนอก | | ผู้ทดสอบเจาะระบบ | ทำหน้าที่ทดสอบเจาะระบบและตรวจสอบความปลอดภัย |
| ๑๕ | นายเกรียงไกร แก้วกัน<br>เจ้าหน้าที่สำนักดิจิทัลสิทธิมนุษยชน | ๐๒ ๑๔๑ ๑๙๒๖<br>kriangkrai_k@nhrc.or.th | ผู้ประสานงานด้านสื่อสารองค์กร (หลัก) | ทำหน้าที่ประสานงานกับโฆษกของหน่วยงาน |
| ๑๖ | นางสาวภารดี บุตรพันธ์<br>เจ้าหน้าที่สำนักดิจิทัลสิทธิมนุษยชน | ๐๒ ๑๔๑ ๓๘๘๕<br>paradee_b@nhrc.or.th | ผู้ประสานงานด้านสื่อสารองค์กร (สำรอง) | ทำหน้าที่แทนกรณีผู้ประสานสานด้านสื่อสารองค์กร (หลัก) ไม่อยู่ หรือ ไม่สามารถปฏิบัติงานได้ |
| ๑๗ | นายโกเมศ สุบงกช<br>ผู้แทนจากสำนักกฎหมาย | ๐๘๔-๐๖๒-๔๑๙๙<br>komate_law@hotmail.com | ผู้เชี่ยวชาญด้านกฎหมาย | ให้คำปรึกษาด้านกฎหมายของหน่วยงาน |

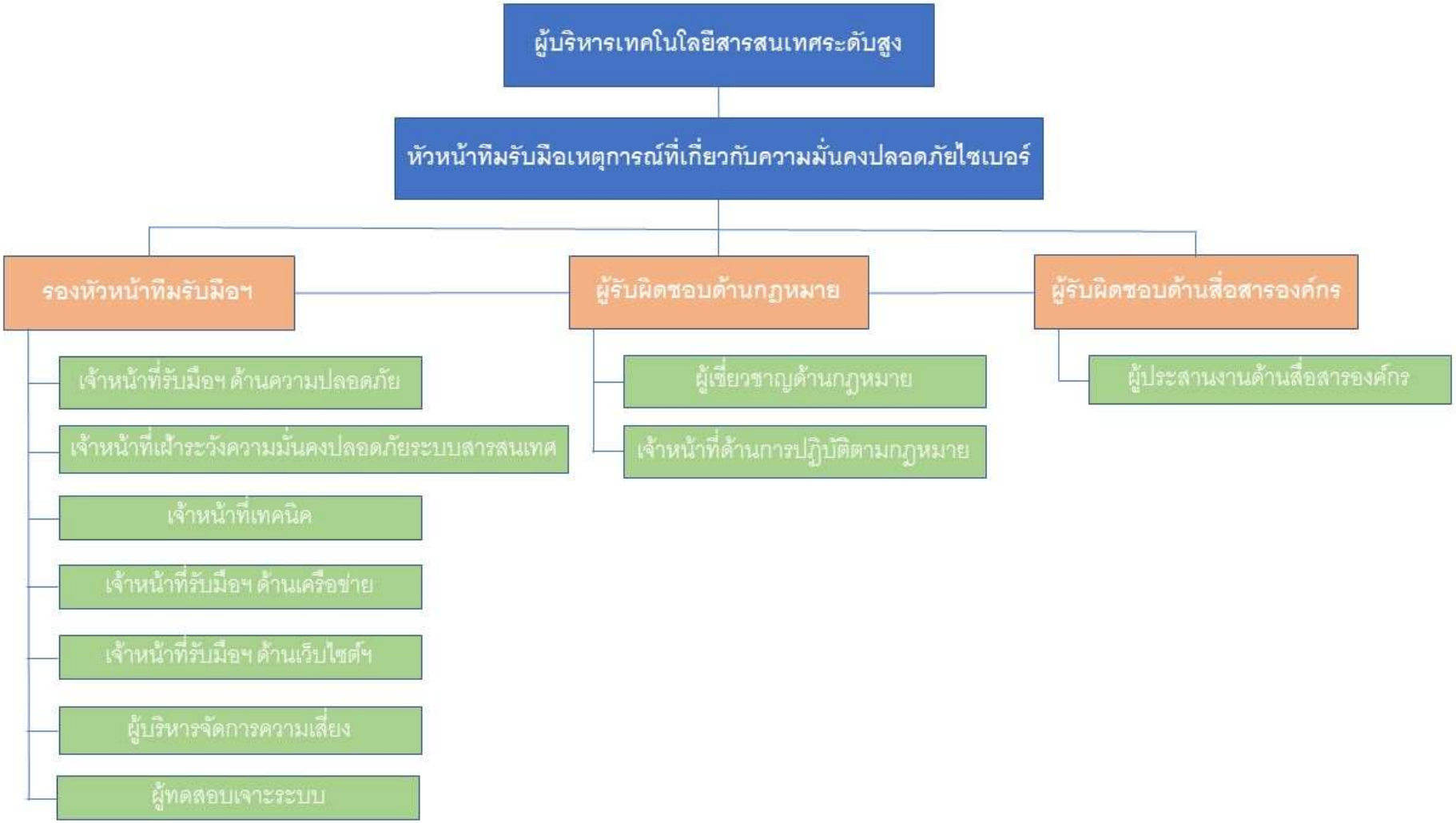
| ลำดับ | ชื่อ นามสกุล | ช่องทางการติดต่อสื่อสาร | หน้าที่ | ความรับผิดชอบ |
|---|---|---|---|---|
| ๑๘ | นายเอกลักษณ์ ภูมิศาสตรา<br>ผู้แทนจากสำนักกฎหมาย | ๐ ๒๑๔๑ ๑๙๒๐<br>๐๙๗-๙๗๑-๙๑๙๐<br>nitikan@nhrc.or.th | เจ้าหน้าที่ด้านการปฏิบัติตามกฎหมาย (Compliance) | ให้คำปรึกษาด้านกฎหมายของหน่วยงาน |
| ๑๙ | เจ้าหน้าที่จาก สกมช. | ๐๒ ๑๔๒ ๖๘๘๘<br>thaicert@ncsa.or.th | ผู้เชี่ยวชาญด้านความปลอดภัย | ทำหน้าที่ให้คำปรึกษาและแนะนำแนวทางในการรับมือปัญหาด้านภัยคุกคามทางไซเบอร์ที่เกิดขึ้น |

**หมายเหตุ** : ข้อมูลส่วนบุคคลของผู้ติดต่อที่นำมาเปิดเผย ได้รับความยกเว้นจากพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ ตามมาตรา ๒๔ ข้อ (๕) และมาตรา ๒๖ ข้อ (๑)

**หน่วยงานภายนอกที่เกี่ยวข้อง**

| ลำดับ | ชื่อ - นามสกุล | ช่องทางการติดต่อสื่อสาร | หน่วยงาน | ความเกี่ยวข้อง |
|---|---|---|---|---|
| ๑ | ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ | ๐๒-๑๔๒-๖๘๘๕ (ติดต่อเวลาทำการ),<br>๐๒-๑๑๔-๓๕๓๑ (๒๔ ชั่วโมง)<br>thaicert@ncsa.or.th | ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) | หน่วยงานสนับสนุนและให้คำปรึกษาด้านความมั่นคงปลอดภัยไซเบอร์ |
| ๒ | นางสาววรรณา ใจเย็น (eng)<br><br>นางสาวอัญชลีย์ ชั่งชู | ๐ ๒๑๔๑ ๑๔๙๒<br>karokejung@gmail.com<br>๐๘๙-๓๐๑-๑๕๒๙<br>anchalec@ntplc.co.th<br>๐๒ ๕๗๔ ๘๕๐๔ – ๕<br>corporate-net@totisp.net | บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) | ฝ่ายโครงข่าย<br><br>ฝ่ายขาย<br><br>ฝ่ายให้บริการอินเทอร์เน็ต (ISP) |
| ๓ | นายวรสิทธิ์ พันธ์เลิศ | ๐๙๘-๘๘๕-๙๒๓๘<br>๐๘๑-๔๘๕-๒๓๗๓<br>worasit.p@woratechnology.com | บริษัท วรเทคโนโลยี จำกัด | บริษัทคู่สัญญารับจ้างดูแลบำรุงรักษาครุภัณฑ์และระบบต่าง ๆ ในห้องควบคุมระบบเทคโนโลยีสารสนเทศ |
| ๔ | นายปณิธาน คันธมาศ | ๐ ๒๑๔๒ ๒๒๓๓<br>๐ ๒๑๔๒ ๒๒๐๓ | บริษัท ธนารักษ์พัฒนาสินทรัพย์ จำกัด | ส่วนวิศวกรรม ฝ่ายวิศวกรรมและบริหารโครงการ |
| ๕ | นายปุณวิพัชร์ นนทะไชย | ๐๘๗-๖๑๗-๑๑๑๗ | บริษัท แอ็ดวานซ์ อินโนเวชั่น เทคโนโลยี จำกัด | บริษัทคู่สัญญาดูแลบำรุงรักษาระบบสารสนเทศและฐานข้อมูลด้านสิทธิมนุษยชน |
| ๖ | น.ส. ภัทริยา วงศ์สายสถิตย์ | ๐๖๔-๕๑๖-๔๖๖๖ | บริษัท บิซโพเทนเชียล จำกัด | บริษัทคู่สัญญาดูแลบำรุงรักษาระบบแผนงานและการบริหารงบประมาณ |
| ๗. | นางสาวปิยะดา จูมปา | ๐๖๒-๔๖๓-๖๖๑๖ | บริษัท ไอคอน คอนเนคท์ จำกัด | บริษัทคู่สัญญาดูแลบำรุงรักษาระบบเว็บไซต์ของสำนักงาน กสม. |

**แผนผัง โครงสร้างทีมงานรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT)**



**ภาคผนวก ค**

รายละเอียดของขั้นตอนการปฏิบัติเพื่อรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์

(Incident Response Plan)

**<u>รายละเอียดขั้นตอนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response)</u> ดังนี้**

| 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 เตรียมรายละเอียดช่องทางการติดต่อสื่อสาร<br>๒.๕ การให้ความรู้ และวิธีปฏิบัติ<br>๒.๖ ทดสอบการตอบสนองต่อภัยคุกคามทางไซเบอร์ | ทีมรับมือและตอบสนองต่อ Incident และเจ้าของระบบฯ /ผู้ดูแลระบบ |
| ๓. ขั้นการตรวจจับและวิเคราะห์ภัยคุกคาม (Detection & Analysis)<br>๓.๑ รับแจ้งเหตุ<br>๓.๒ วิเคราะห์ความผิดปกติเมื่อได้รับแจ้ง<br>๓.๓ บันทึกข้อมูลเหตุการณ์ภัยคุกคาม<br>๓.๔ จัดลำดับความสำคัญของ incident<br>๓.๕ ติดต่อประสานงานกับหน่วยงานภายในและภายนอก | ผู้รับแจ้งเหตุ<br>ทีมเฝ้าระวังและวิเคราะห์การแจ้งเตือนภัยคุกคามจากอุปกรณ์ตรวจจับ<br>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 |

**ภาคผนวก ง**

ตัวอย่าง : รายการตรวจสอบการจัดการเหตุการณ์

(Incident Handling Checklist)

**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, จัดเก็บและดูแลรักษาหลักฐานเกี่ยวกับเหตุการณ์ทั้งหมดก่อนเริ่มกระบวนการกู้คืนซึ่งรวมถึงการได้มาของบันทึกการยึดหลักฐานคอมพิวเตอร์ที่ได้มาหรืออุปกรณ์อื่น ๆ เพื่อสนับสนุนการสอบสวน | |
| ๕ | จำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ | |
| ๖ | ดำเนินการสอบสวน (Investigate) สาเหตุและผลกระทบของเหตุการณ์ | |
| ๗ | ทำการกำจัดสาเหตุ (Eradicate the incident) | |
| ๗.๑ | ระบุช่องโหว่ของระบบที่โดนโจมตีและบรรเทาผลกระทบที่เกิดขึ้น | |
| ๗.๒ | กำจัด หรือลบมัลแวร์ และสาเหตุภัยคุกคามอื่น ๆ | |
| 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 | |

## ภาคผนวก จ

การวิเคราะห์ระบบที่ให้บริการอิเล็กทรอนิกส์ของสำนักงาน กสม. ที่มีความสำคัญ

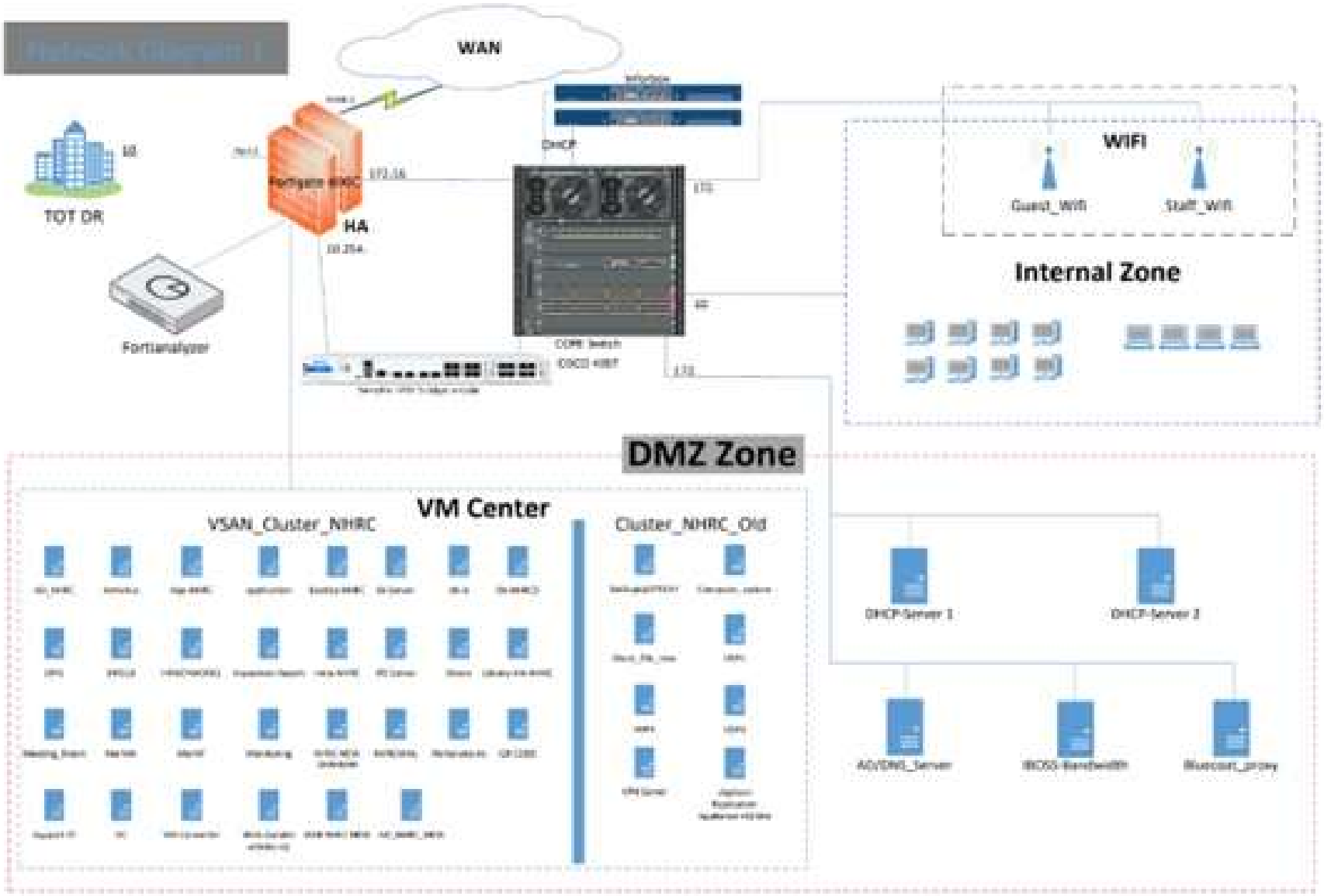
(Business Impact Analysis)

**ระบบงานที่ให้บริการอิเล็กทรอนิกส์ของสำนักงาน กสม.**

| ลำดับ | ระบบงาน | RTO ภายใน | RPO ภายใน | MTPD ภายใน |
|---|---|---|---|---|
| ๑ | ระบบสารสนเทศและฐานข้อมูลด้านสิทธิมนุษยชน | ๑๒ ชม. | ๒๔ ชม. | ๒๔ ชม. |
| ๒ | ระบบแผนงานและการบริหารงบประมาณ | ๑๒ ชม. | ๒๔ ชม. | ๒๔ ชม. |
| ๓ | ระบบสารบรรณอิเล็กทรอนิกส์ | ๑๒ ชม. | ๒๔ ชม. | ๒๔ ชม. |
| ๔ | ระบบการเงินการคลัง | ๑๒ ชม. | ๒๔ ชม. | ๒๔ ชม. |
| ๕ | ระบบฐานข้อมูลบัญชีรายชื่อและระบบยืนยันตัวตนผู้ใช้งาน (Active Directory & Authentication Systems & DNS Server) | ๑๒ ชม. | ๒๔ ชม. | ๒๔ ชม. |
| ๖ | ระบบให้บริการข้อมูลผ่านเครือข่าย (File Sharing Server) | ๑๒ ชม. | ๒๔ ชม. | ๒๔ ชม. |
| ๗ | ระบบเว็บไซต์สำนักงาน กสม. | ๑๒ ชม. | ๒๔ ชม. | ๒๔ ชม. |
| ๘ | ระบบบริการเครือข่ายภายใน (Web Portal) | ๑๒ ชม. | ๒๔ ชม. | ๒๔ ชม. |
| ๙ | ระบบเว็บไซต์ศูนย์สารสนเทศสิทธิมนุษยชน | ๑๒ ชม. | ๒๔ ชม. | ๒๔ ชม. |
| ๑๐ | ระบบอีเมล์สำนักงาน (Mail Server) | ๑๒ ชม. | ๒๔ ชม. | ๒๔ ชม. |
| ๑๑ | ระบบแอปพลิเคชันสำนักงานคณะกรรมการสิทธิมนุษยชนแห่งชาติ | ๑๒ ชม. | ๒๔ ชม. | ๒๔ ชม. |
| ๑๒ | ระบบสารสนเทศทรัพยากรบุคคล (D-Pis) | ๒๔ ชม. | ๒๔ ชม. | ๒๔ ชม. |
| ๑๓ | ระบบสมุดโทรศัพท์ | ๒๔ ชม. | ๒๔ ชม. | ๒๔ ชม. |
| ๑๔ | ระบบแจ้งซ่อมคอมพิวเตอร์ออนไลน์ | ๒๔ ชม. | ๒๔ ชม. | ๒๔ ชม. |
| ๑๕ | ระบบจองห้องประชุม | ๒๔ ชม. | ๒๔ ชม. | ๒๔ ชม. |

หมายเหตุ ความสำคัญของระบบงาน

| ระดับความสำคัญ | ผลกระทบต่อผู้ใช้งาน |
|---|---|
| สูง (๑) | กระทบผู้ใช้งานเป็นส่วนใหญ่ ทำให้เกิดการหยุดชะงักงานโดยรวม |
| ปานกลาง (๒) | กระทบผู้ใช้งาน ทำให้เกิดการหยุดชะงักงานเล็กน้อย |
| น้อย (๓) | กระทบผู้ใช้งานเล็กน้อย ทำให้เกิดไม่สะดวกในการใช้งาน |


WAN
TOT DR
HA
Fortianalyzer
DHCP
WIFI
Guest_Wifi
Staff_Wifi
Internal Zone
DMZ Zone
VM Center
VSAN_Cluster_NHRC
Cluster_NHRC_Old
DHCP-Server 1
DHCP-Server 2
AD/DNS_Server

**ทะเบียนทรัพย์สินด้านเทคโนโลยีสารสนเทศที่สำคัญของสำนักงาน กสม.**

| รายการ | ยี่ห้อ/รุ่น |
|---|---|
| ๑. ระบบเครื่องปรับอากาศแบบควบคุมความชื้น (Precision Air Conditioning) | ยี่ห้อ Liebert รุ่น PEX ๑๐๓๐ ขนาด ๓๕,๐๐๐ BTU |
| ๒. ระบบสำรองไฟฟ้าอัตโนมัติ (Uninterruptible Power Supply) | ยี่ห้อ Emerson ITA ๒๐kVA |
| ๓. ระบบดับเพลิงอัตโนมัติด้วยก๊าซ HFC ๒๒๗ ea (Fire Suppression System) | ยี่ห้อ Kiddle Fire Protection |
| ๔. ระบบการควบคุมการเข้าออกประตูอัตโนมัติ (Access Control System) | ยี่ห้อ TAFF รุ่น MU-๖๓ |
| ๕. ระบบตรวจจับการรั่วซึมของน้ำ (Water Leak Detector System) | ยี่ห้อ Liebert รุ่น LPL ๒๓๐๐ |
| ๖. ระบบเฝ้าดูและแจ้งเตือนอัตโนมัติ (Environment Monitoring System) | ยี่ห้อ TCE รุ่น x๒๐๐ |
| ๗. อุปกรณ์จัดเก็บข้อมูลแบบภายนอก (External Storage) | ยี่ห้อ EMC รุ่น VNX ๕๓๐๐ |
| ๘. หน่วยเก็บข้อมูลสำรอง (Hard Disk) | ยี่ห้อ EMC ๖๐๐ GB/๑๕,๐๐๐ RPM |
| ๙. เครื่องคอมพิวเตอร์แม่ข่าย | HP DL ๓๘๐ G๗ |
| ๑๐. เครื่องคอมพิวเตอร์แม่ข่าย | Dell R๗๔๐xd |
| ๑๑. เครื่องคอมพิวเตอร์แม่ข่าย | HP DL ๓๖๐ G๗ |
| ๑๒. อุปกรณ์กระจายสัญญาณหลัก | CISCO Catalyst๔๕๐๐E ๗ Slot Chassis for ๔๘ Gbps/slot |
| ๑๓. อุปกรณ์บริหารจัดการการให้บริการบนระบบเครือข่ายคอมพิวเตอร์ (DNS/DHCP Server Appliance) | Infoblox model ๘๒๕ |
| ๑๔. อุปกรณ์ป้องกันและตรวจจับการบุกรุก (Intrusion Prevention System) | McAfee Network Security IPS NS๕๒๐๐ |
| ๑๕. อุปกรณ์ป้องกันการบุกรุกระบบคอมพิวเตอร์ | ยี่ห้อ Fortigate รุ่น ๖๐๐ C |
| ๑๖. อุปกรณ์ควบคุมและบริหารจัดการเว็บแอพพลิเคชั่น (Bandwidth Management) | IBOSS: Web/Application/Bandwidth Management ๒๑๖๐ |

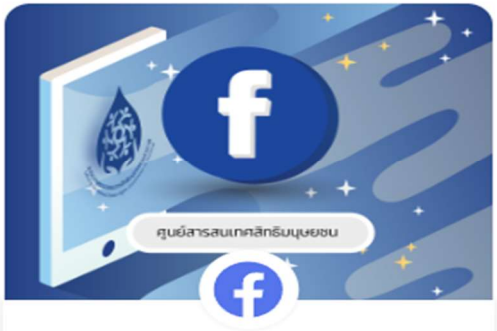
**สื่อสังคมออนไลน์ของสำนักงาน กสม.**


**สำนักงานคณะกรรมการสิทธิมนุษยชน**

เข้าสู่ Facebook


**สำนักงานคณะกรรมการสิทธิมนุษยชน**

เข้าสู่ Youtube




**ศูนย์สารสนเทศสิทธิมนุษยนชน**

เข้าสู่ Facebook


**สำนักงาน กสม.**

เข้าสู่ Tiktok

## ภาคผนวก ฉ

ลักษณะภัยคุกคามทางไซเบอร์ และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ

**ข้อ ๑ การจำแนกหมวดหมู่ของภัยคุกคามทางไซเบอร์**

| หมวดหมู่ | คำอธิบาย |
|---|---|
| ๐ | เหตุการณ์จำลอง และการฝึกจู่โจมของหน่วยงานเอง (Training and Exercises) |
| ๑ | การพยายามเข้าถึงระบบที่ไม่สำเร็จ (Unsuccessful Activity Attempt) |
| ๒ | การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance) |
| ๓ | การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยที่หน่วยงานงานกำหนด (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 ลักษณะภัยคุกคามทางไซเบอร์แยกตามระดับต่าง ๆ**

| ประเภทอุปกรณ์เครือข่าย | หมวดหมู่ภัยคุกคาม | | | | | | |
|---|---|---|---|---|---|---|---|
| | ๑ | ๒ | ๓ | ๔ | ๕ | ๖ | ๗ |
| Backbone | ไม่ร้ายแรง | ไม่ร้ายแรง | ไม่ร้ายแรง | ไม่ร้ายแรง | วิกฤต | วิกฤต | วิกฤต |
| เราท์เตอร์ | ไม่ร้ายแรง | ไม่ร้ายแรง | ร้ายแรง | ไม่ร้ายแรง | วิกฤต | วิกฤต | วิกฤต |
| เครื่องแม่ข่ายสำหรับการจัดการเครือข่าย หรือดูแลความปลอดภัย | ไม่ร้ายแรง | ไม่ร้ายแรง | ร้ายแรง | ร้ายแรง | วิกฤต | วิกฤต | วิกฤต |
| เครื่องแม่ข่ายที่ไม่ได้ให้บริการกับสาธารณะ | ไม่ร้ายแรง | ไม่ร้ายแรง | ร้ายแรง | ร้ายแรง | ร้ายแรง | ร้ายแรง | ร้ายแรง |
| เครื่องแม่ข่ายที่เปิดให้บริการกับสาธารณะ | ไม่ร้ายแรง | ไม่ร้ายแรง | ไม่ร้ายแรง | ร้ายแรง | ไม่ร้ายแรง | ไม่ร้ายแรง | ร้ายแรง |

**ข้อ ๓ การกำหนดระยะเวลาในการแจ้งและการแก้ไขปัญหาภัยคุกคามทางไซเบอร์**

| ระดับภัยคุกคามทางไซเบอร์ | การแจ้งเบื้องต้นตามช่องทางที่กำหนด (ภายในเวลา หลังจากการตรวจพบ หรือเกิดเหตุภัยคุกคามทางไซเบอร์) | การแก้ไขปัญหาภัยคุกคาม (ภายในเวลาหลังจากการตรวจพบ หรือเหตุภัยคุกคามทางไซเบอร์) | การแจ้งเหตุภัยคุกคามให้ สกมช. ทราบ (ภายในเวลาหลังจากการตรวจพบหรือเหตุภัยคุกคามทางไซเบอร์) |
|---|---|---|---|
| ระดับไม่ร้ายแรง | ภายใน ๒๔ ชั่วโมง | ภายใน ๓๐ วัน | ภายใน ๓๐ วัน |
| ระดับร้ายแรง | ภายใน ๑ ชั่วโมง | ภายใน ๔๘ ชั่วโมง | ภายใน ๔๘ ชั่วโมง |
| ระดับวิกฤต | ภายใน ๓๐ นาที | ภายใน ๖ ชั่วโมง | ภายใน ๒๔ ชั่วโมง |
| ช่องทางการติดต่อ | ๐ ๒๑๔๑ ๑๙๒๖<br>๐๒ ๑๔๑ ๓๘๘๕<br>digital@nhrc.or.th | ๐๒ ๑๔๑ ๓๙๐๙<br>jiraporn.thong@nhrc.or.th<br>Cc: digital@nhrc.or.th | ๐๒ ๑๔๒ ๖๘๘๘<br>thaicert@ncsa.or.th |

<u>หมายเหตุ</u> กรณีเกิดเหตุการณ์สุดวิสัย หรือเหตุการณ์ไม่คาดคิด หรือมีปัจจัยอื่นที่ส่งผลกระทบต่อระบบสารสนเทศ อาจส่งผลต่อระยะเวลาในการแก้ไขปัญหาภัยคุกคามทางไซเบอร์ที่เพิ่มขึ้น

**ภาคผนวก ช**

แบบฟอร์มต่าง ๆ

**บันทึกรายงานสถานการณ์เหตุการณ์ความมั่นคงปลอดภัยไซเบอร์**

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

**บันทึกข้อมูลกิจกรรมเหตุการณ์ความปลอดภัยทางไซเบอร์ (Incident Documentation)**

| วันที่และเวลา | บันทึกกิจกรรมที่เกิดขึ้น<br>(ข้อเท็จจริง, สถานการณ์ที่เกิดขึ้น, การตัดสินใจ, ผลกระทบ) |
|---|---|
| *๑๒/๑/๖๖ – ๐๙.๐๐ น.* | *ทีมรับมือฯ ตรวจสอบพบภัยคุกคามลักษณะ Phishing ทำให้เกิด Ransomware เข้าสู่ระบบเครือข่ายภายในหน่วยงาน* |
| | |
| | |
| | |
| | |
| | |
| | |

**เอกสาร ก๑ ข้อมูลที่ต้องแจ้ง**

**ข้อมูลการประสานงานและผลการตรวจสอบภัยคุกคามเบื้องต้น**

**๑. ข้อมูลการประสานงาน**

ชื่อหน่วยงานที่รับผิดชอบติดตามเหตุภัยคุกคาม

วันที่และเวลาที่แจ้ง

**๒. ด้านภารกิจหรือบริการของหน่วยงาน และชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม**

ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม

ที่อยู่ของหน่วยงานหรือหน่วยงานย่อยที่เกิดเหตุภัยคุกคาม

**๓. ข้อมูลการติดต่อสำหรับการประสานงานเหตุภัยคุกคาม**

ชื่อ-นามสกุล ตำแหน่งงาน

ชื่อหน่วยงาน อีเมล

โทรศัพท์ (ที่ทำงาน / มือถือ)

**๔. ความต่อเนื่องของเหตุภัยคุกคาม**

☐ เหตุภัยคุกคามใหม่ ☐ การรายงานข้อมูลต่อเนื่องจากเหตุภัยคุกคามเดิม

**๕. ลักษณะภัยคุกคามทางไซเบอร์**

ระบบที่ได้รับผลกระทบมีความสำคัญต่อพันธกิจหลักของหน่วยงานหรือไม่

เหตุการณ์ที่เกิดขึ้นเกิดจากภัยคุกคามทางไซเบอร์[๑] 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)

[๑] พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดความหมายของ “ภัยคุกคามทางไซเบอร์” ดังนี้ การกระทำหรือการดำเนินการใด ๆ โดยมิชอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

**เอกสาร ก๒ แบบรายงานภัยคุกคามทางไซเบอร์**

| **ส่วนที่ ๑** |
| --- |
| **หมวด ก. ข้อมูลการประสานงานและผลการตรวจสอบภัยคุกคามเบื้องต้น** |
| **หมายเลขอ้างอิง (สำหรับเจ้าหน้าที่ สกมช.):** โปรดระบุ<br>**หน่วยงานที่รับผิดชอบติดตามเหตุภัยคุกคาม (ถ้ามี):** โปรดระบุ<br>**วันที่:** เลือกวันที่ **เวลา:** โปรดระบุ |
| **ก๑. ด้านภารกิจหรือบริการของหน่วยงาน และ ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม**<br>ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม: โปรดระบุ<br>ที่อยู่ของหน่วยงานหรือหน่วยงานย่อยที่เกิดเหตุภัยคุกคาม: โปรดระบุ |
| **ก๒. ข้อมูลการติดต่อสำหรับการประสานงานเหตุภัยคุกคาม**<br>ชื่อ-นามสกุล: โปรดระบุ ตำแหน่งงาน: โปรดระบุ<br>ชื่อหน่วยงาน: โปรดระบุ อีเมล: โปรดระบุ<br>โทรศัพท์ (ที่ทำงาน / มือถือ) : โปรดระบุ |
| **ก๓. ความต่อเนื่องของเหตุภัยคุกคาม**<br>☐ เหตุภัยคุกคามใหม่ ☐ การรายงานข้อมูลต่อเนื่องจากเหตุภัยคุกคามเดิม |
| **ก๔. ลักษณะภัยคุกคามทางไซเบอร์**<br>ระบบที่ได้รับผลกระทบมีความสำคัญต่อพันธกิจหลักของหน่วยงาน<br>☐ ใช่ ☐ ไม่ใช่<br>เหตุการณ์ที่เกิดขึ้นเกิดจากภัยคุกคามทางไซเบอร์[๒] ในระดับใด (มาตรา ๖๐)<br>☐ ไม่ร้ายแรง ☐ ร้ายแรง ☐ วิกฤต (ก) ☐ วิกฤต (ข)<br>☐ ยังไม่สามารถระบุได้ |

[๒] 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)**<br>☐ เพิ่งพบเหตุการณ์ ☐ อยู่ในขั้นตอนการขอความช่วยเหลือ<br>☐ อยู่ในขั้นตอนการสอบสวน ☐ กำลังลุกลาม<br>☐ อยู่ในขั้นตอนการระงับภัย ☐ สามารถระงับภัยได้แล้ว<br>☐ รายงานปิดเหตุการณ์ภัยคุกคามแล้ว ☐ อื่น ๆ: โปรดระบุ |
| **ค๒. สิ่งที่ได้ดำเนินการหรือได้แก้ไขไปแล้ว**<br>☐ ยังไม่ได้ดำเนินการแก้ไขใด ๆ ☐ ยกเลิกการเชื่อมต่อระบบออกจากเครือข่ายแล้ว<br>☐ ตรวจสอบข้อมูลจราจร (Log) แล้ว ☐ ตรวจสอบโปรแกรม (แฟ้ม binaries/.exe) แล้ว<br>☐ กู้คืนกลับมาด้วยระบบหรือข้อมูลสำรองที่ตรวจสอบความถูกต้องแล้ว<br>☐ รายละเอียดการแก้ไขภัยคุกคามที่เกิดขึ้นเพิ่มเติม: โปรดระบุ |
| **ค๓. รายละเอียดการรับมือภัยคุกคามอื่น ๆ (ถ้ามี)**<br>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[๓]**

| 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) | |
| สวิตซ์ (Switch) /เราเตอร์ (Router) | |
| เว็บไซต์ (Website) | |
| อื่น ๆ | |

**ข้อ ๓ สถิติรายปีจำแนกตามระดับภัยคุกคามทางไซเบอร์[๔]**

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

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

[๔] ระดับภัยคุกคามทางไซเบอร์ตามมาตรา ๖๐ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

## ภาคผนวก ซ

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, จัดเก็บและดูแลรักษาหลักฐานเกี่ยวกับเหตุการณ์ทั้งหมดก่อนเริ่มกระบวนการกู้คืนซึ่งรวมถึงการได้มาของบันทึกการยึดหลักฐานคอมพิวเตอร์ที่ได้มาหรืออุปกรณ์อื่น 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 | |