แผนการรับมือภัยคุกคามทางไซเบอร์

พ.ศ. ๒๕๖๗

กรมอุตสาหกรรมพื้นฐานและการเหมืองแร่

แผนการรับมือภัยคุกคามทางไซเบอร์
กรมอุตสาหกรรมพื้นฐานและการเหมืองแร่

๑. หลักการและเหตุผล

แผนการรับมือภัยคุกคามทางไซเบอร์ของกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่ฉบับนี้ จัดทำขึ้นเพื่อให้เป็นไปตามมาตรา ๔๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ที่กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร็ว รวมทั้งเพื่อให้เป็นไปตามนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ของกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่ ซึ่งประมวลแนวทางปกิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างน้อยต้องประกอบด้วยเรื่อง ดังนี้

(๑) แผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจประเมิน ผู้ตรวจสอบภายใน หรือผู้ตรวจสอบอิสระจากภายนอก อย่างน้อยปีละหนึ่งครั้ง

(๒) แผนการรับมือภัยคุกคามทางไซเบอร์

๒. วัตถุประสงค์

(๑) เพื่อกำหนดวิธีการในการตรวจสอบ ควบคุม ป้องกัน แก้ไขปัญหาที่เกิดจากภัยคุกคามทางไซเบอร์เพื่อป้องกันและลดความเสียหายที่เกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ

(๒) เพื่อกำหนดวิธีการกู้คืนระบบเครือข่ายคอมพิวเตอร์กลางของกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่ให้สามารถใช้งานได้ตามปกติ

(๓) เพื่อเตรียมความพร้อมด้านบุคลากรของกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่ ในการรับมือกับปัญหาภัยคุกคามทางไซเบอร์

๓. ขอบเขต

แผนการรับมือภัยคุกคามทางไซเบอร์ฉบับนี้ ใช้รับมือเหตุภัยคุกคามทางไซเบอร์ที่เกิดขึ้นต่อระบบสารสนเทศ และข้อมูลดิจิทัลของกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่ รวมถึงบุคคลหรืออุปกรณ์ใด ๆ ซึ่งเข้าถึงระบบสารสนเทศ และข้อมูลดิจิทัลดังกล่าว

๔. หน้าที่ในการดำเนินการตามแผน

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร มีหน้าที่เป็นผู้รับผิดชอบหลักในการดำเนินการตามแผนการรับมือภัยคุกคามทางไซเบอร์ฉบับนี้ โดยมีหน่วยงานสนับสนุนประกอบด้วย กลุ่มพัฒนาระบบเครือข่ายและการสื่อสาร กลุ่มพัฒนาระบบสำนักงานอิเล็กทรอนิกส์ กลุ่มแผนงานและส่งเสริมเทคโนโลยีสารสนเทศ รวมถึงหน่วยงานเจ้าของกระบวนการและเจ้าของข้อมูลภายใต้หน่วยงานของกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่

๕. ความเกี่ยวข้องกับเอกสารอื่น

๕.๑ นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๐ กรมอุตสาหกรรมพื้นฐานและการเหมืองแร่

๕.๒ นโยบายและแนวปฏิบัติการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๔ กรมอุตสาหกรรมพื้นฐานและการเหมืองแร่

๖. นิยาม

เหตุการณ์ (Event) หมายความว่า การเกิดขึ้นที่สังเกตได้ใด ๆ (Observable Occurrence) ในระบบเครือข่าย สภาพแวดล้อม กระบวนการ ลำดับการดำเนินการ หรือบุคลากร เหตุการณ์อาจมีหรือไม่มีลักษณะที่ส่งผลเชิงลบก็ได้

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

ภัยคุกคามทางไซเบอร์ (Cyber Threat) หมายความว่า การกระทำหรือการดำเนินการใด ๆ โดยมิชอบโดยใช้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือโปรแกรมไม่พึงประสงค์ โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหาย หรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

เหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญ หมายความว่า เหตุภัยคุกคามทางไซเบอร์ที่ปรากฏต่อระบบสารสนเทศ และเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ซึ่งคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติได้กำหนดลักษณะของภัยคุกคามทางไซเบอร์ไว้ตามมาตรา ๖๐ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๗. รูปแบบภัยคุกคามทางไซเบอร์

๗.๑ ซอฟต์แวร์ประสงค์ร้าย (Malicious Software) หรือมัลแวร์ (Malware) ซึ่งเป็นโปรแกรมที่มีการทำงานที่มุ่งประสงค์ร้ายต่อคอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์

๗.๒ ไวรัสคอมพิวเตอร์ (Computer Virus) เป็นมัลแวร์ชนิดหนึ่งที่สามารถคัดลอกตัวเองติดตั้งตัวเองในเครื่องคอมพิวเตอร์อื่น ๆ โดยที่เจ้าของเครื่องคอมพิวเตอร์ไม่อนุญาต ซึ่งไวรัสคอมพิวเตอร์จะแพร่กระจายตัวเองสู่เครื่องคอมพิวเตอร์เครื่องอื่น ๆ โดยใช้พาหนะ เช่น แฟลชไดรว์ติดไวรัส หรือไฟล์คอมพิวเตอร์ติดไวรัส เป็นต้น

๗.๓ หนอนคอมพิวเตอร์ (Computer Worm) เป็นมัลแวร์ชนิดหนึ่ง สามารถคัดลอกตัวเองติดตั้งตัวเองในเครื่องคอมพิวเตอร์อื่น ๆ โดยที่เจ้าของเครื่องคอมพิวเตอร์ไม่อนุญาต โดยหนอนคอมพิวเตอร์จะต่างกับไวรัสตรงที่ไวรัสจะแพร่กระจายตัวเองไปสู่คอมพิวเตอร์เครื่องอื่น ๆ โดยอาศัยพาหนะ แต่หนอนคอมพิวเตอร์จะใช้วิธีสแกนเครื่องคอมพิวเตอร์ที่อยู่ในระบบเครือข่ายและตรวจหาช่องโหว่ของระบบปฏิบัติการ หรือช่องโหว่ของแอปพลิเคชัน จากนั้นจึงทำการคัดลอกตัวเองเข้าไปฝังตัวโดยใช้ช่องโหว่ดังกล่าว

๗.๔ ม้าโทรจัน (Trojan Horse) เป็นมัลแวร์ชนิดหนึ่งที่มีจุดประสงค์เพื่อบุกรุก เข้าถึง และควบคุมเครื่องคอมพิวเตอร์จากระยะไกล ดำเนินการเปลี่ยนแปลง ทำลายไฟล์ข้อมูลสำคัญ หรือทำการคัดลอกข้อมูลดังกล่าว ส่งให้แก่ผู้คุกคามผ่านระบบเครือข่ายอินเทอร์เน็ต ซึ่งข้อมูลสำคัญที่ผู้คุกคามต้องการอาจเป็น ชื่อผู้ใช้ รหัสผ่าน เลขที่บัญชีธนาคาร และข้อมูลส่วนบุคคลอื่น ๆ ลักษณะของการติดตั้งม้าโทรจันจะเหมือนกับไวรัสคอมพิวเตอร์ คือ อาศัยพาหนะ ซึ่งอาจมาจากแฟลชไดรว์ หรือทางอีเมล

๗.๕ สปายแวร์ (Spyware) เป็นมัลแวร์ชนิดหนึ่งที่มีวัตถุประสงค์เพื่อบันทึกการกระทำของผู้ใช้บนเครื่องคอมพิวเตอร์และส่งผ่านอินเทอร์เน็ต โดยที่ผู้ใช้ไม่ได้รับทราบ โปรแกรมแอบดักข้อมูลนั้นสามารถรวบรวมข้อมูล สถิติการใช้งานจากผู้ใช้ได้หลายอย่างขึ้นกับการออกแบบของโปรแกรม

๗.๖ ซอฟต์แวร์เรียกค่าไถ่ (Ransomware) เป็นมัลแวร์ชนิดหนึ่งที่มีพฤติกรรมเข้ารหัสไฟล์ต่าง ๆ ที่อยู่บนเครื่องคอมพิวเตอร์ไม่ว่าจะเป็นไฟล์เอกสาร รูปภาพ วิดีโอ ผู้ใช้งานจะไม่สามารถเปิดไฟล์ใด ๆ ได้เลย หากไฟล์เหล่านั้นถูกเข้ารหัส ซึ่งการถูกเข้ารหัสก็หมายความว่าจะต้องใช้คีย์ในการปลดล็อคเพื่อกู้ข้อมูลคืนกลับมา ผู้ใช้งานจะต้องทำการจ่ายเงินตามข้อความ เรียกค่าไถ่ ที่ปรากฏ

๗.๗ ประตูหลัง (Backdoor) เป็นช่องทางพิเศษที่ใช้เข้าถึงระบบงานคอมพิวเตอร์ โดยที่ไม่ต้องผ่านการพิสูจน์ทราบตัวตน ซึ่งส่วนใหญ่เมื่อผู้บุกรุกสามารถเจาะเข้าระบบได้แล้ว ก็จะสร้างประตูหลังเอาไว้เพื่อใช้ในการบุกรุกเข้าสู่ระบบงานคอมพิวเตอร์ในภายหลัง

๗.๘ Rootkit เป็นโปรแกรมที่ถูกพัฒนาขึ้นมาเพื่อควบคุมระบบหรือขโมยข้อมูลที่อยู่ในระบบคอมพิวเตอร์ ทั้งนี้ นอกจากใช้สำหรับบุกรุกเข้าสู่ระบบงานแล้ว Rootkit ยังอาจใช้เพื่อดูแลหรือตรวจสอบระบบคอมพิวเตอร์ได้ด้วย

๗.๙ การโจมตีแบบ DoS/DDoS มีจุดประสงค์เพื่อทำให้เครื่องคอมพิวเตอร์แม่ข่าย (Server) หยุดทำงาน หากเครื่องคอมพิวเตอร์ที่โจมตี มีเครื่องเดียวเรียกว่า การโจมตีแบบ Denial of Service (DoS) แต่หากมีเครื่องคอมพิวเตอร์ที่โจมตีมีมากกว่า ๑ เครื่องและกระทำพร้อม ๆ กัน ไม่ว่าจะโดยตั้งใจหรือไม่ตั้งใจจะเรียกว่า การโจมตีแบบ Distributed Denial of Service (DDoS)

๗.๑๐ Botnet เป็นกลุ่มของอุปกรณ์ที่ติดมัลแวร์และถูกเปลี่ยนเป็น Bot (ย่อมาจาก Robot) ไม่ว่าจะเป็นอุปกรณ์คอมพิวเตอร์ เว็บแคม เราท์เตอร์ หรืออุปกรณ์ IoT อื่น ๆ เพื่อรอรับคำสั่งจากผู้บุกรุก (Hacker) โดยผู้บุกรุกจะนำ Botnet ที่มีไปใช้ในการโจมตีขนาดใหญ่ เช่น การทำ DDoS เป็นต้น

๗.๑๑ Spam Mail หรืออีเมลขยะ เป็นขยะออนไลน์ที่ส่งตรงมาถึงผู้รับ โดยที่ผู้รับสารนั้นไม่ต้องการและสร้างความเดือนร้อน รำคาญให้กับผู้รับได้ในลักษณะของการโฆษณาสินค้าหรือบริการ การชักชวนเข้าไปยังเว็บไซต์ต่าง ๆ ซึ่งอาจมีภัยคุกคามชนิด Phishing แฝงเข้ามาด้วย ด้วยเหตุนี้จึงควรติดตั้งระบบ AntiSpam หรือหากใช้ฟรีอีเมลก็จะมีโปรแกรมคัดกรองอีเมลขยะในชั้นหนึ่งแล้ว

๗.๑๒ Phishing คือ การหลอกลวงทางอินเทอร์เน็ต เพื่อขอข้อมูลที่สำคัญ เช่น รหัสผ่าน หรือหมายเลขบัตรเครดิต โดยการส่งข้อความผ่านทางอีเมลหรือเมสเซนเจอร์ ตัวอย่างของการ Phishing เช่น การบอกแก่ผู้รับปลายทางว่าเป็นธนาคารหรือบริษัทที่น่าเชื่อถือ และแจ้งว่ามีสาเหตุทำให้คุณต้องเข้าสู่ระบบและใส่ข้อมูลที่สำคัญใหม่ โดยเว็บไซต์ที่ลิงค์ไปนั้น จะมีหน้าตาคล้ายคลึงกับเว็บที่กล่าวถึง

๗.๑๓ Sniffing เป็นการดักข้อมูลที่ส่งมาจากคอมพิวเตอร์เครื่องหนึ่งไปยังอีกเครื่องหนึ่ง หรือจากเครือข่ายหนึ่งไปยังอีกเครือข่ายหนึ่ง เป็นวิธีการหนึ่งที่ผู้บุกรุกระบบนิยมใช้

๗.๑๔ Hacking เป็นการเจาะระบบเครือข่ายคอมพิวเตอร์ไม่ว่าจะกระทำด้วยมนุษย์หรืออาศัยโปรแกรมด้วยวัตถุประสงค์ต่าง ๆ กัน ทั้งนี้โดยทั่วไปแล้วการ Hacking เป็นส่งที่ผิดกฎหมาย แต่อย่างไรก็ตาม หากได้รับอนุญาตก็ไม่ใช่สิ่งผิดกฎหมาย โดยตัวอย่างของการ Hacking อย่างถูกกฎหมาย เช่น การเจาะระบบเพื่อประเมินความเสียหายของระบบคอมพิวเตอร์ และทดสอบระบบการรักษาความมั่นคงปลอดภัยเครือข่ายขององค์กร

๗.๑๕ ผู้บุกรุก (Hacker) หมายถึง ผู้ที่ไม่ได้รับอนุญาตในการใช้งานระบบ แต่พยายามลักลอบเข้ามาใช้งานด้วยวัตถุประสงค์ต่าง ๆ ไม่ว่าจะเพื่อโจรกรรมข้อมูล ผลกำไร หรือความพอใจส่วนบุคคลก็ตาม ความเสียหายจากผู้บุกรุกเป็นภัยคุกคามที่หนัก

๘. การเตรียมความพร้อมในการรับมือปัญหาภัยคุกคาทางไซเบอร์

เพื่อให้กรมอุตสาหกรรมพื้นฐานและการเหมืองแร่ มีความพร้อมในการรับมือปัญหาภัยคุกคามทางไซเบอร์ จะดำเนินการเตรียมความพร้อมในด้านต่าง ๆ ดังนี้

๘.๑ การเตรียมความพร้อมด้านอุปกรณ์

เพื่อให้ระบบเครือข่ายคอมพิวเตอร์ของกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่ สามารถรับมือกับภัยคุกคามทางไซเบอร์ได้ จึงควรจัดหาอุปกรณ์และซอฟต์แวร์ที่จำเป็น ดังนี้

(๑) อุปกรณ์ป้องกันระบบเครือข่าย (Next Generation Firewall) ใช้สำหรับป้องกันภัยคุกคามทางไซเบอร์ประเภท DoS/DDoS Botnet Phishing Sniffing Hacker ทั้งนี้อุปกรณ์ป้องกันระบบเครือข่ายที่จัดหานอกจากความสามารถในการเป็น Firewall แล้วยังต้องมีความสามารถอื่น ๆ เพิ่มเติม ได้แก่ ความสามารถในด้านการตรวจจับการบุกรุก (IPS) ความสามารถในการคัดกรองของเว็บไซต์อันตราย (Web Filtering) และการควบคุมการใช้งานซอฟต์แวร์ (Application Control) เป็นอย่างน้อย

(๒) ซอฟต์แวร์ตรวจสอบประสิทธิภาพระบบเครือข่าย (Network Monitoring Software) ใช้สำหรับตรวจจับความผิดปกติที่เกิดขึ้นกับระบบเครือข่ายคอมพิวเตอร์ของกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่

(๓) อุปกรณ์ Web Application Firewall ใช้สำหรับป้องกันภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับระบบงานคอมพิวเตอร์ของกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่ ที่พัฒนาขึ้นมาให้บริการผ่าน Web Browser ได้แก่ การคุกคามทางไซเบอร์ประเภท Hacker โดยสามารถป้องกันเทคนิคการบุกรุก เช่น Cross-site Scripting และ SQL Injection ได้เป็นอย่างน้อย

(๔) ซอฟต์แวร์สำรองข้อมูล ใช้สำหรับกระบวนการสำรองข้อมูล และการกู้ข้อมูลของระบบเครือข่ายคอมพิวเตอร์ชองหน่วยงาน รวมทั้งยังสามารถสำรองข้อมูลแบบเข้ารหัสได้

(๕) อุปกรณ์จัดเก็บข้อมูลภายนอก (SAN Storage) เป็นอุปกรณ์ที่ใช้สำหรับติดตั้งระบบงานคอมพิวเตอร์ของกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่ และในการรับมือทางไซเบอร์อุปกรณ์จัดเก็บข้อมูลภายนอกยังสามารถลดผลกระทบที่เกิดจาก Ransomware ได้ โดยหน่วยงานจะใช้อุปกรณ์จัดเก็บข้อมูลภายนอกดังกล่าวจัดทำพื้นที่จัดเก็บข้อมูลส่วนกลาง โดยกำหนดให้แต่ละกองมีพื้นที่จัดเก็บข้อมูล ๕๐ GB และจะมีการสำรองข้อมูลจากพื้นที่จัดเก็บข้อมูลส่วนกลางอย่างสม่ำเสมอ ซึ่งหากกองต่าง ๆ นำไฟล์สำคัญมาจัดเก็บเอาไว้ที่พื้นที่จัดเก็บข้อมูลส่วนกลางแล้วแม้ว่าจะเกิดภัยคุกคามไซเบอร์ประเภท Ransomware ก็จะสามารถสำเนาข้อมูลสำคัญที่เก็บอยู่บนพื้นที่จัดเก็บส่วนกลางกลับมาได้

(๖) ระบบงานคอมพิวเตอร์สำรอง ใช้ในกรณีที่ไม่สามารถกู้ระบบงานคอมพิวเตอร์ขึ้นมาได้

(๗) อุปกรณ์จัดเก็บ Log file ใช้สำหรับจัดเก็บข้อมูลจราจรคอมพิวเตอร์ที่เกิดขึ้นจากการใช้งานเครือข่ายคอมพิวเตอร์ของกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่

(๘) อุปกรณ์วิเคราะห์ Log file ใช้สำหรับวิเคราะห์ข้อมูลจราจรคอมพิวเตอร์ที่เกิดขึ้นจากการใช้งานเครือข่ายคอมพิวเตอร์ของกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่ ซึ่งข้อมูลที่ถูกวิเคราะห์ดังกล่าวจะช่วยระบุถึงหมายเลข IP Address ของผู้โจมตี และลักษณะภัยคุกคามไซเบอร์ที่โจมตีระบบเครือข่ายคอมพิวเตอร์ของหน่วยงาน และใช้ประกอบการทำรายงานให้แก่คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์

(๙) ซอฟต์แวร์ป้องกันไวรัสคอมพิวเตอร์แบบคอร์ปอเรต (Corporate Antivirus Software) ใช้สำหรับติดตั้งบนเครื่องคอมพิวเตอร์ตั้งโต๊ะ เครื่องคอมพิวเตอร์พกพา และเครื่องคอมพิวเตอร์แม่ข่ายของหน่วยงาน ซึ่งสามารถป้องกันภัยคุกคามไซเบอร์ประเภท Malware, Computer Virus, Computer Worm, Trojan, Spyware, Ransomware, Botnet, Spam Mail

๘.๒ แผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

เพื่อให้ระบบเครือข่ายคอมพิวเตอร์ของหน่วยงานสามารถรับมือกับภัยคุกคามทางไซเบอร์ที่มีการพัฒนาขึ้นตลอดเวลา กรมอุตสาหกรรมพื้นฐานและการเหมืองแร่จะพิจารณาจ้างบริษัทผู้เชี่ยวชาญในการประเมินความเสี่ยงการรักษาความมั่นคงปลอดภัยไซเบอร์มาตรวจสอบ โดยจะมีจำนวนครั้งในการตรวจสอบอย่างน้อยปีละ ๑ ครั้ง ซึ่งในการตรวจสอบและประเมินความเสี่ยงนี้ อาจสามารถค้นหาภัยคุกคามทางไซเบอร์ประเภท Backdoor ที่ถูกซ่อนเอาไว้จากขั้นตอนการพัฒนาระบบงานคอมพิวเตอร์ได้

๘.๓ การเตรียมพร้อมด้านบุคลากร

(๑) การให้ความรู้

เพื่อให้บุคลากรของหน่วยงานมีความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ กรมอุตสาหกรรมพื้นฐานและการเหมืองแร่จะพิจารณาจ้างบริษัทผู้เชี่ยวชาญในการประเมินความเสี่ยงการรักษาความมั่นคงปลอดภัยไซเบอร์ดำเนินการจัดฝึกอบรมให้ความรู้แก่บุคลากรของหน่วยงาน

(๒) การแจ้งรายชื่อเจ้าหน้าที่สำหรับประสานงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๔๖ กำหนดให้หน่วยงานภาครัฐแจ้งรายชื่อเจ้าหน้าที่ระดับบริหารและระดับปฏิบัติการ เพื่อประสานงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ไปยังสำนักงานคณะกรรมการการรักษาความมันคงปลอดภัยไซเบอร์ โดยกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่จะกำหนดระดับภัยคุกคามทางไซเบอร์ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๖๐ และจะแจ้งรายชื่อเจ้าหน้าที่เพื่อประสานงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับภัยคุกคามต่าง ๆ

(๓) มีผู้ดูแลด้านการรักษาความมั่นคงปลอดภัยเครือข่าย และผู้ดูแลระบบเครือข่ายคอมพิวเตอร์ของหน่วยงาน

๘.๔ การเตรียมพร้อมด้านการสำรองข้อมูลและระบบคอมพิวเตอร์สำรอง

ในกรณีที่ภัยคุกคามทางไซเบอร์ ก่อเกิดความเสียหายแก่ระบบเครือข่ายคอมพิวเตอร์ของหน่วยงานอย่างมากจนไม่สามารถทำงานได้เป็นเวลานาน กรมอุตสาหกรรมพื้นฐานและการเหมืองแร่จะพิจารณาทางเลือกในการแก้ไขปัญหา โดยวิธีการกู้คืนข้อมูลที่เสียหาย หรือเปิดใช้ระบบคอมพิวเตอร์สำรอง โดยมีเป้าหมายเพื่อให้ระบบเครือข่ยคอมพิวเตอร์ของหน่วยงานสามารถใช้งานได้อย่างรวดเร็วที่สุด ทั้งนี้แนวทาง

ในการกู้คืนข้อมูล และการใช้ระบบคอมพิวเตอร์สำรองจะกำหนดอยู่ในเอกสารแผนสำรองข้อมูลและกู้คืนระบบของหน่วยงาน

๙. ขั้นตอนการปฏิบัติเมื่อเกิดภัยคุกคามทางไซเบอร์

ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๔๔ กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร็ว

ทั้งนี้ กรมอุตสาหกรรมพื้นฐานและการเหมืองแร่ ได้มีมาตรการสำหรับรับมือกับภัยคุกคามทางไซเบอร์ ๓ มาตรการ ดังนี้

๙.๑ มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect) มีการดำเนินการ ดังนี้

การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring) มีขั้นตอนดำเนินการ ดังนี้

(๑) การตรวจจับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ทั้งหมดที่เกี่ยวข้องกับบริการที่สำคัญของกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่

(๒) การจัดประเภทและวิเคราะห์เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่ตรวจพบ

(๓) การระบุว่ามีภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวกับบริการที่สำคัญของกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่

๙.๒ มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Response) มีขั้นตอนดำเนินการ ดังนี้

(๑) แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity incident Response Plan) ต้องมีการจัดทำ สื่อสาร ฝึกซ้อม ทบทวน และปรับปรุงแผนการรับมือภัยคุกคามทางไซเบอร์ตามที่ระบุไว้ในประมวลแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ ครั้ง เพื่อให้แน่ใจว่า แผนการรับมือภัยคุกคามทางไซเบอร์สามารถดำเนินการได้อย่างมีประสิทธิภาพและประสิทธิผล

(๒) แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)

- ต้องจัดทำแผนการสื่อสารในภาวะวิกฤต เพื่อตอบสนองต่อวิกฤตที่เกิดจากเหตุการณ์
- ต้องตรวจสอบให้แน่ใจว่า แผนการสื่อสารในภาวะวิกฤต มีการดำเนินการต่อไปนี้
  - จัดตั้งทีมการสื่อสารในภาวะวิกฤต เพื่อเปิดใช้งานในช่วงวิกฤต
  - ระบุสถานการณ์จำลองเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เป็นไปได้และแผนดำเนินการที่เกี่ยวข้อง
  - ระบุกลุ่มเป้าหมาย และผู้มีส่วนได้ส่วนเสียสำหรับสถานการณ์จำลองเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์แต่ละประเภท
  - ระบุผู้แทนหน่วยงานหลักและผู้เชี่ยวชาญด้านเทคนิคที่จะเป็นตัวแทนขององค์กรเมื่อกล่าวแถลงกับสื่อมวลชน
  - ระบุแพลตฟอร์ม ช่องทางการเผยแพร่ที่เหมาะสม เช่น โซเชียลมีเดียสำหรับการเผยแพร่ข้อมูล

- ต้องตรวจสอบให้แน่ใจว่าแผนการสื่อสารในภาวะวิกฤต รวมถึงการประสานงานระหว่างทุกฝ่ายที่ได้รับผลกระทบมีการตอบสนองที่ประสานกันและสอดคล้องกันในช่วงวิกฤต
- ต้องดำเนินการฝึกซ้อมแผนการสื่อสารในภาวะวิกฤตอย่างน้อยปี ๑ ครั้ง เพื่อให้แน่ใจว่าสามารถสื่อสารและเผยแพร่ข้อมูลได้อย่างทันท่วงทีและมีประสิทธิผลในช่วงวิกฤตอันเนื่องมาจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

(๓) การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise)

- หน่วยงานต้องมีส่วนร่วมในการฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์ หากได้รับคำสั่งเป็นลายลักษณ์อักษรให้ทำโดยคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ อาจดำเนินการได้ทั้งในระดับชาติ หรือระดับภาคส่วน หน่วยงานต้องตรวจสอบให้แน่ใจว่าบุคลากรที่เกี่ยวข้องที่ระบุไว้ในแผนการรับมือภัยคุกคามทางไซเบอร์มีส่วนร่วมในการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ดังกล่าว
- หน่วยงานต้องปฏิบัติตามคำขอใด ๆ ของคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เพื่อให้ข้อมูลที่เกี่ยวข้องกับบริการที่สำคัญของกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่เป็นไปตามวัตถุประสงค์ในการวางแผนและดำเนินการฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์ข้อมูลที่คณะกรรมการอาจร้องขอ รวมถึงแผนการรับมือภัยคุกคามทางไซเบอร์และแผนการสื่อสารในภาวะวิกฤต และขั้นตอนการปฏิบัติงานมาตรฐานที่เกี่ยวข้องกับการดำเนินงานของบริการที่สำคัญของหน่วยงาน

๙.๓ มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recovery)

(๑) หน่วยงานต้องจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP) เพื่อให้แน่ใจว่าบริการที่สำคัญของหน่วยงานสามารถให้บริการที่จำเป็นต่อไปได้ในกรณีที่เกิดการหยุดชะงัก เนื่องจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ เพื่อให้สามารถใช้ปฏิบัติงานได้จริง รวมถึงสอบทานแผนของผู้ให้บริการภายนอก เพื่อพิจารณาความสอดคล้องกับแผนงานของหน่วยงานของรัฐ

(๒) หน่วยงานตรวจสอบให้แน่ใจว่ามีการฝึกซ้อมแผนความต่อเนื่องทางธุรกิจ (BCP) อย่างน้อยปีละ ๑ ครั้ง เพื่อประเมินประสิทธิภาพของแผน (BCP) ต่อภัยคุกคามทางไซเบอร์และเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

กรมอุตสาหกรรมพื้นฐานและการเหมืองแร่ ได้จัดทำขั้นตอนการปฏิบัติเบื้องต้น เมื่อเกิดภัยคุกคามทางไซเบอร์ โดยมีขั้นตอน ดังนี้

ขั้นตอน	รายละเอียด
ตรวจพบภัยคุกคามทางไซเบอร์	มีการแจ้งเหตุจากผู้ใช้งาน หรือตรวจจับการคุกคามทางไซเบอร์ได้จากอุปกรณ์ป้องกันระบบเครือข่าย หรือเครื่องมือต่าง ๆ ตามที่กำหนดในข้อ ๗ ที่ช่วยให้สามารถตรวจพบการคุกคามทางไซเบอร์อย่างรวดเร็ว
ตรวจสอบภัยคุกคามทางไซเบอร์	ตรวจสอบข้อมูลของภัยคุกคามทางไซเบอร์ และประเมินระดับภัยคุกคามตามที่กำหนดใน พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๖๒
การควบคุมภัยคุกคามทางไซเบอร์	ดำเนินการควบคุมภัยคุกคามทางไซเบอร์ ให้ส่งผลกระทบน้อยที่สุด และป้องกันไม่ให้เกิดการแพร่กระจายไปยังส่วนอื่น ๆ ซึ่งในกรณีที่เร่งด่วนกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่จะทำการปิดระบบ หรือตัดการเชื่อมต่อของระบบคอมพิวเตอร์ชั่วคราว
แก้ไขได้ / แก้ไขปัญหา / แก้ไขไม่ได้	ดำเนินการแก้ไขหรือกำจัดภัยคุกคามทางไซเบอร์ในเบื้องต้นในทันที
ติดต่อศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (Thaicert) หรือสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์	ในกรณีที่ไม่สามารถแก้ไขปัญหาได้จะดำเนินการติดต่อศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (Thaicert) หรือสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เพื่อขอคำแนะนำหรือขอความช่วยเหลือ
การแก้ไขปัญหาสำเร็จและดำเนินการหาวิธีป้องกันการเกิดภัยคุกคามไซเบอร์ในลักษณะเดิม	หลังจากแก้ไขปัญหาภัยคุกคามไซเบอร์แล้ว กรมอุตสาหกรรมพื้นฐานและการเหมืองแร่จะดำเนินการตรวจหาช่องโหว่ โดยอุปกรณ์ตรวจสอบช่องโหว่ระบบเครือข่าย หรือเครื่องมืออื่น ๆ และหาวิธีเพื่อป้องกันการเกิดภัยคุกคามไซเบอร์ในลักษณะเดิม
ระบบทำงานปกติ / ทดสอบระบบ / ระบบทำงานไม่ปกติ	ตรวจสอบการทำงานของโครงสร้างพื้นฐานสำคัญทางสารสนเทศของหน่วยงาน ว่าสามารถทำงานได้หรือไม่ ในกรณีที่พบว่าการทำงานไม่สมบูรณ์ หรือข้อมูลสำคัญสูญหายไปจะดำเนินการกู้คืนระบบงาน
กู้คืนระบบ	ดำเนินการตามขั้นตอนการกู้คืนข้อมูลตามที่ระบุในแผนการสำรองและกู้คืนระบบ ในกรณีที่กู้คืนระบบไม่ได้ กรมอุตสาหกรรมพื้นฐานและการเหมืองแร่จะพิจารณาเปิดใช้ระบบคอมพิวเตอร์สำรองและเร่งกู้ระบบงานคอมพิวเตอร์หลัก
ระบบสามารถใช้งานได้ตามปกติ	เมื่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศของกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่สามารถทำงานได้ตามปกติแล้ว หน่วยงานที่ดูแลรับผิดชอบด้านโครงข่ายระบบสารสนเทศของหน่วยงานจะดำเนินการสรุปผลในการดำเนินการรับมือภัยคุกคามไซเบอร์
สรุปผลในการดำเนินการรับมือภัยคุกคามไซเบอร์และจัดทำรายงาน	สรุปผลในการรับมือภัยคุกคามไซเบอร์ และแจ้งผลการดำเนินงานให้แก่ผู้เกี่ยวข้อง เช่น ผู้อำนวยการศูนย์ ผู้บริการระดับสูงด้านสารสนเทศ

๑๐ การเตรียมพร้อมรับมือภัยคุกคามทางไซเบอร์ในส่วนของเจ้าหน้าที่

เมื่อเกิดการคุกคามทางไซเบอร์แล้ว ในบางครั้งผลกระทบที่เกิดขึ้นอาจส่งผลให้การทำงานของเครื่องคอมพิวเตอร์ของเจ้าหน้าที่ทำงานผิดพลาดหรือล่าช้าลง หรือส่งผลให้ไฟล์ข้อมูลที่ถูกจัดเก็บเอาไว้ในเครื่องคอมพิวเตอร์ไม่สามารถใช้งานได้ และยากต่อการกู้คืนให้เป็นปกติได้โดยเร็ว ดังนั้นเจ้าหน้าที่ของกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่ ควรดำเนินการเตรียมพร้อมรับมือภัยคุกคามทางไซเบอร์ ดังนี้

(๑) ดำเนินการตามนโยบายการใช้งานระบบป้องกันไวรัสสำหรับเครื่องคอมพิวเตอร์อย่างเคร่งครัด

(๒) ดำเนินการตามนโยบายการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล และนโยบายการใช้งานเครื่องคอมพิวเตอร์แบบพกพาอย่างเคร่งครัด

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กรมอุตสาหกรรมพื้นฐานและการเหมืองแร่ จะดำเนินการสนับสนุนการเตรียมพร้อมรับมือภัยคุกคามทางไซเบอร์ ดังนี้

(๑) ดำเนินการจัดหาซอฟต์แวร์ป้องกันไวรัสคอมพิวเตอร์แบบคอร์ปอเรต (Corporate Antivirus Software) ให้เพียงพอต่อจำนวนเจ้าหน้าที่ของกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่

(๒) ดำเนินการจัดเตรียมพื้นที่จัดเก็บข้อมูลส่วนกลาง โดยกำหนดให้แต่ละกองมีพื้นที่จัดเก็บข้อมูล ๕๐ GB และจะมีการสำรองข้อมูลจากพื้นที่จัดเก็บข้อมลส่วนกลางอย่างสม่ำเสมอ ซึ่งหากกองต่าง ๆ นำไฟล์สำคัญมาจัดเก็บเอาไว้ที่พื้นที่จัดเก็บข้อมูลส่วนกลางแล้วแม้ว่าจะเกิดภัยคุกคามไซเบอร์ประเภท Ransomware ก็จะสามารถสำเนาข้อมูลสำคัญที่เก็บอยู่บนพื้นที่จัดเก็บข้อมูลส่วนกลางกลับมาได้

๑๑. โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team : CIRT)

กรมอุตสาหกรรมพื้นฐานและการเหมืองแร่ใช้โมเดลโครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ในลักษณะแบบรวมศูนย์ ประกอบด้วย

ลำดับที่	ชื่อ นามสกุล รายละเอียดการติดต่อ	หน้าที่	ความรับผิดชอบ	การติดต่อสื่อสาร
๑	นางสาวพรชลันพักษ์ เพ็ญคุณาพร	หัวหน้าทีมรับมือเหตุการณ์ (Team Manager)	ทำหน้าที่สื่อสารกับผู้บริหารของหน่วยงาน	02-430-6848 ต่อ 4800
๒	นายผดุงศักดิ์ โนจิตร	รองหัวหน้าทีมรับมือเหตุการณ์ (Deputy Team Manager)	ทำหน้าที่แทนกรณีหัวหน้าทีมรับมือฯ ไม่อยู่/ไม่สามารถปฏิบัติงานได้	02-430-6848 ต่อ 4811
๓	นางสาวลลิดา จันทราธนากุล	เจ้าหน้าที่รับมือเหตุการณ์ (Incident Lead)	ทำหน้าที่ช่วยเหลือ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ให้สามารถควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์ได้	02-430-6848 ต่อ 4811

ลำดับที่	ชื่อ นามสกุล รายละเอียดการติดต่อ	หน้าที่	ความรับผิดชอบ	การติดต่อสื่อสาร
๔	นายธนาคาร ละครแก้ว	เจ้าหน้าที่เทคนิค (Technical Lead)	ทำหน้าที่ให้ความเห็นเกี่ยวกับแนวทางที่เหมาะสมในการควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์	02-430-6848 ต่อ 4811

ทั้งนี้ นอกจากทีมรับมือเหตุการณ์ดังกล่าวข้างต้น ให้มีบุคคลดังต่อไปนี้ ทำหน้าที่สนับสนุนการดำเนินการของแผนการรับมือภัยคุกคามทางไซเบอร์ฉบับนี้ ดังนี้

ลำดับที่	ชื่อ นามสกุล	หน้าที่	ความรับผิดชอบ	การติดต่อสื่อสาร
๑	นางสาวกนกวรรณ สวัสดิวงศ์	เจ้าหน้าที่ควบคุมผลกระทบ	ทำหน้าที่ควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์	02-430-6848 ต่อ 4831
๒	นางทัศนีย์ เจิมประสาทสิทธิ์	เจ้าหน้าที่ด้านการปฏิบัติตามกฎหมาย (Compliance)	ทำหน้าที่ตามนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กพร.	02-430-6848 ต่อ 4811
๓	นายปิยวัชร ประมวลรัตน์	ผู้ทดสอบเจาะระบบ	ทำหน้าที่ตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กพร.	02-430-6848 ต่อ 4831
๔	นายอภิชัย ปวรางกูร	ผู้เชี่ยวชาญด้านกฎหมาย	ทำหน้าที่ตามคำสั่งคณะทำงานข้อมูลข่าวสารและความมั่นคงปลอดภัยข้อมูลข่าวสาร กพร.	02-430-6848 ต่อ 4821
๕	นางสาวทัศนีย์ สุขมาก	ผู้บริหารจัดการความเสี่ยง	ทำหน้าที่ตามคำสั่งคณะทำงานข้อมูลข่าวสารและความมั่นคงปลอดภัยข้อมูลข่าวสาร กพร.	02-430-6849 ต่อ 4900
๖	นายธวัชพล รุ่งศรีทอง	ผู้รับผิดชอบด้านสื่อสารองค์กร	ทำหน้าที่ตามคำสั่งคณะทำงานข้อมูลข่าวสารและความมั่นคงปลอดภัยข้อมูลข่าวสาร กพร.	02-430-6840 ต่อ 4041

๑๒. ขั้นตอนการรับมือภัยคุกคาม

แผนการรับมือภัยคุกคามทางไซเบอร์ฉบับนี้ ประกอบด้วยขั้นตอนการรับมือเหตุภัยคุกคามทางไซเบอร์ตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔ และประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ รวมถึง นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์และนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านด้านสารสนเทศของกรมอุตสาหกรรมพื้นฐานและการเหมืองแร่ ดังนี้

๑๒.๑ ขั้นการเตรียมการ เป็นการดำเนินการมาตรการเพื่อเตรียมการและป้องกันการเกิดภัยคุกคามทางไซเบอร์ (Preparation) เป็นสิ่งที่จะต้องดำเนินการในระยะเริ่มต้น เพื่อเตรียมความพร้อมเมื่อต้องเผชิญเหตุ ได้แก่ การจัดเตรียมข้อมูลให้พร้อม การจัดตั้งและฝึกอบรมบุคลากรหรือทีมงาน การจัดหาเครื่องมือและทรัพยากรต่าง ๆ ที่จำเป็น การตั้งค่าระบบต่าง ๆ ให้ปลอดภัย การจัดทำนโยบาย แผนงาน และกระบวนการที่เกี่ยวข้อง รวมถึงการสร้างเครือข่ายความร่วมมือ ประกอบด้วยการดำเนินการในเรื่อง ดังต่อไปนี้

(๑) กำหนดโครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT) รายละเอียดตามข้อ ๑๑

(๒) กำหนดโครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure) ซึ่งกำหนดว่าหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจะปฏิบัติตามภาระหน้าที่ในการรายงานภายใต้พระราชบัญญัติ และกฎหมายย่อยใด ๆ ที่ทำขึ้นภายใต้กฎหมายดังกล่าว ตลอดจนภาระหน้าที่ในการรายงานภายใต้กฎหมาย และข้อกำหนดด้านกฎระเบียบที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(๓) กำหนดเกณฑ์และขั้นตอนในการเรียกใช้งาน (Activate) การตอบสนองต่อเหตุการณ์และการสร้างทีมรับมือเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ (CIRT)

(๔) ดำเนินการตามเอกสารแนบท้ายในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔

๑๒.๒ ขั้นการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ เป็นการดำเนินการในการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (Detection and Analysis) ซึ่งเป็นสิ่งจำเป็นที่จะช่วยให้หน่วยงานสามารถบรรเทาความเสี่ยงที่ยังคงเหลืออยู่ และสามารถแจ้งเตือนได้อย่างทันท่วงที เมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น ประกอบด้วยการดำเนินการตามเอกสารแนบท้ายในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔

๑๒.๓ ขั้นการระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคาม ทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ เป็นการดำเนินการเพื่อระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคามทาง

ไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ (Containment, Eradication, and Recovery) โดยการดำเนินการดังกล่าว ควรกำหนดให้สอดคล้องกับความรุนแรงและระดับของภัยคุกคามทางไซเบอร์ในแต่ละระดับ จนกระทั่งสามารถกู้คืนทรัพย์สินสำคัญทางสารสนเทศให้กลับมาดำเนินงานหรือให้บริการได้ตามปกติ ซึ่งการดำเนินการในขั้นตอนนี้อาจจะต้องกระทำควบคู่ไปกับการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ที่อาจมีการลุกลาม หรือทวีความรุนแรงมากขึ้น เพื่อให้การระงับและการปราบปรามภัยคุกคามทางไซเบอร์ตลอดจนการฟื้นฟูระบบงานที่ได้รับผลกระทบจากการเกิดภัยคุกคามทางไซเบอร์ สอดคล้องกับสถานการณ์ที่เปลี่ยนแปลงไป ประกอบด้วยการดำเนินการในเรื่อง ดังต่อไปนี้

(๑) จำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

(๒) เรียกใช้งานกระบวนการกู้คืน (Recovery Process)

(๓) ดำเนินการสอบสวน (Investigate) สาเหตุและผลกระทบของเหตุการณ์

(๔) เก็บรักษาหลักฐาน (Preservation of Evidence) ก่อนเริ่มกระบวนการกู้คืนซึ่งรวมถึงการได้มาของบันทึกการยึดหลักฐานคอมพิวเตอร์ที่ได้มา หรืออุปกรณ์อื่น ๆ เพื่อสนับสนุนการสอบสวน

(๕) ดำเนินการตามระเบียบวิธีการมีส่วนร่วม (Engagement Protocols) กับบุคคลภายนอกหรือแนวปฏิบัติการบริหารจัดการบุคคลภายนอก ซึ่งรวมถึงรายละเอียดการติดต่อ ตัวอย่างเช่น ผู้ขายสำหรับบริการด้านนิติวิทยาศาสตร์ การกู้คืน และการบังคับใช้กฎหมายเพื่อดำเนินคดี

(๖) ดำเนินการตามเอกสารแนบท้ายในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔

๑๒.๔ ขั้นการดำเนินการภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ เป็นการดำเนินการที่เกี่ยวข้องภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ (Post-Incident Activity) นั้น หน่วยงานควรกำหนดขั้นตอนวิธีปฏิบัติ หรือกำหนดนโยบายภายในที่เกี่ยวข้อง เพื่อให้มีแนวทางที่ชัดเจน ซึ่งการปฏิบัติตามมาตรการดังกล่าวจะช่วยให้หน่วยงานสามารถเรียนรู้จากเหตุภัยคุกคามทางไซเบอร์ที่ผ่านมา และสามารถหาแนวทางเพื่อแก้ไขจุดบกพร่องและพัฒนาแนวทางรับมือกับภัยคุกคามทางไซเบอร์ต่อไปในอนาคต นอกจากนี้หน่วยงานต้องเก็บรักษาข้อมูลและพยานหลักฐานที่จำเป็น เพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์ หรือใช้ในกรณีที่ต้องการร้องทุกข์หรือดำเนินคดี เนื่องจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้นนั้น อาจเข้าลักษณะเป็นความผิดตามประมวลกฎหมายอาญา หรือพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐ และที่แก้ไขเพิ่มเติม (ถ้ามี) หรือกฎหมายอื่น ๆ ที่เกี่ยวข้อง ประกอบด้วยการดำเนินการในเรื่อง ดังต่อไปนี้

(๑) ทบทวนหลังการดำเนินการ (After-Action Review Process) เพื่อระบุและแนะนำให้ปรับปรุงการดำเนินการเพื่อป้องกันการเกิดซ้ำ

(๒) ดำเนินการตามเอกสารแนบท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔

แหล่งที่มา

- ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔
- ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔
- NIST SP 800-61r2 Computer Security Incident Handling Guide

ตารางแสดงความสอดคล้องกับประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔

ประกาศ กกม. เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานฯ พ.ศ. ๒๕๖๔	แผนรับมือฯ ฉบับนี้
๑๙.๑ ต้องจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) ที่กำหนดว่าควรตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์อย่างไร โดยแผนการรับมือภัยคุกคามทางไซเบอร์ต้องมีรายละเอียดอย่างน้อย ดังต่อไปนี้	
(ก) โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT) รวมถึงบทบาทและความรับผิดชอบที่กำหนดไว้อย่างชัดเจนของสมาชิกในทีมแต่ละคนและรายละเอียดการติดต่อ	ข้อที่ ๘
(ข) โครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure) ซึ่งกำหนดว่าหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจะปฏิบัติตามภาระหน้าที่ในการรายงานภายใต้พระราชบัญญัติ และกฎหมายย่อยใด ๆ ที่ทำขึ้นภายใต้กฎหมายดังกล่าว ตลอดจนภาระหน้าที่ในการรายงานภายใต้กฎหมาย และข้อกำหนดด้านกฎระเบียบที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ	ข้อที่ ๙.๑ (๒)
(ค) เกณฑ์และขั้นตอนในการเรียกใช้งาน (Activate) การตอบสนองต่อเหตุการณ์และ CIRT	ข้อที่ ๙.๑ (๓)
(ง) ขั้นตอนจำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์	ข้อที่ ๙.๓ (๑)
(จ) การเรียกใช้งานกระบวนการกู้คืน (Recovery Process)	ข้อที่ ๙.๓ (๒)
(ฉ) ขั้นตอนในการสอบสวน (Investigate) สาเหตุและผลกระทบของเหตุการณ์	ข้อที่ ๙.๓ (๓)
(ช) ขั้นตอนการเก็บรักษาหลักฐาน (Preservation of Evidence) ก่อนเริ่มกระบวนการกู้คืนซึ่งรวมถึงการได้มาของบันทึกการยึดหลักฐานคอมพิวเตอร์ที่ได้มา หรืออุปกรณ์อื่น ๆ เพื่อสนับสนุนการสอบสวน	ข้อที่ ๙.๓ (๔)
(ซ) ระเบียบวิธีการมีส่วนร่วม (Engagement Protocols) กับบุคคลภายนอกหรือแนวปฏิบัติการบริหารจัดการบุคคลภายนอก ซึ่งรวมถึงรายละเอียดการติดต่อ ตัวอย่างเช่น ผู้ขายสำหรับบริการด้านนิติวิทยาศาสตร์/การกู้คืนและการบังคับใช้กฎหมายเพื่อดำเนินคดี และ	ข้อที่ ๙.๓ (๕)
(ฌ) กระบวนการทบทวนหลังการดำเนินการ (After-Action Review Process) เพื่อระบุและแนะนำให้ปรับปรุงการดำเนินการเพื่อป้องกันการเกิดซ้ำ	ข้อที่ ๙.๔ (๑)