แผนรับมือภัยคุกคามทางไซเบอร์
สำนักงานขับเคลื่อนการปฏิรูปประเทศ ยุทธศาสตร์ชาติ และการสร้างความสามัคคีปรองดอง

๑. หลักการและเหตุผล

ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๔๔ กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร็ว ซึ่งประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างน้อยต้องประกอบด้วยเรื่องดังต่อไปนี้

๑.๑ แผนการตรวจสอบและประเมินความเสียงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจประเมินผู้ตรวจสอบภายใน หรือผู้ตรวจสอบอิสระจากภายนอก อย่างน้อยปีละหนึ่งครั้ง

๑.๒ แผนรับมือภัยคุกคามทางไซเบอร์

เพื่อดำเนินการตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๔๔ สำนักงานขับเคลื่อนการปฏิรูปประเทศ ยุทธศาสตร์ชาติ และการสร้างความสามัคคีปรองดอง (สำนักงาน ป.ย.ป.) จึงได้จัดทำแผนรับมือภัยคุกคามทางไซเบอร์ขึ้นเพื่อรับมือกับภัยคุกคามทางไซเบอร์ ที่มาในรูปแบบไวรัสคอมผิวเตอร์ และ การโจมตีระบบเครือข่ายคอมพิวเตอร์กลางของสำนักงาน ป.ย.ป. โดยการดำเนินงานตามแผนจะมุ่งเน้นในการ ตรวจสอบ ควบคุม ป้องกันและแก้ไขปัญหาที่เกิดจากภัยคุกคามทางไซเบอร์ รวมถึงการกู้คืนระบบเครือข่ายคอมพิวเตอร์กลางให้สามารถใช้งานได้

๒. วัตถุประสงค์

๒.๑ เพื่อกำหนดวิธีการในการตรวจสอบ ควบคุม ป้องกัน และแก้ไขปัญหาที่เกิดจากภัยคุกคามทางไซเบอร์ เพื่อป้องกันและลดความเสียหายที่เกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ

๒.๒ เพื่อกำหนดวิธีการกู้คืนระบบเครือข่ายคอมพิวเตอร์กลางของสำนักงาน ป.ย.ป. ให้สามารถใช้งานได้

๒.๓ เพื่อเตรียมความพร้อมด้านบุคลากรของสำนักงาน ป.ย.ป. ในการรับมือกับปัญหาภัยคุกคามทางไซเบอร์

๓. รูปแบบภัยคุกคามไซเบอร์

๓.๑ ซอฟต์แวร์ประสงค์ร้าย (Malicious Software) หรือที่เรียกโดยทั่วไปว่ามัลแวร์ (Malware) ซึ่งเป็นโปรแกรมที่มีการทำงานที่มุ่งประสงค์ร้ายต่อคอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์

๓.๒ ไวรัสคอมพิวเตอร์ (Computer Virus) เป็นมัลแวร์ชนิดหนึ่ง ที่สามารถคัดลอกตัวเองติดตั้งตัวเองในเครื่องคอมพิวเตอร์อื่น ๆ โดยที่เจ้าของเครื่องคอมผิวเตอร์ไม่นุญาต ซึ่งไวรัสคอมพิวเตอร์จะแพร่กระจายตัวเองไปสู่เครื่องคอมพิวเตอร์เครื่องอื่น ๆ โดยใช้พาหะ เช่น แฟลชไดร์ติดไวรัส หรือไฟล์คอมพิวเตอร์ติดไวรัส เป็นต้น

๓.๓ หนอนคอมพิวเตอร์ (computer worm) เป็นมัลแวร์ชนิดหนึ่ง สามารถคัดลอกตัวเองติดตั้งตัวเองในเครื่องคอมพิวเตอร์อื่น ๆ โดยที่เจ้าของเครื่องคอมพิวเตอร์ไม่อนุญาต โดยหนอนคอมพิวเตอร์จะต่างกับไวรัสตรงที่ไวรัสจะแพร่กระจายตัวเองไปสู่คอมพิวเตอร์เครื่องอื่น ๆ โดยอาศัยพาหะ แต่หนอนคอมพิวเตอร์จะใช้วิธีสแกน

เครื่องคอมพิวเตอร์ที่อยู่ในระบบเครือข่ายและตรวจหาช่องโหว่ของระบบปฏิบัติการหรือช่องโหว่ของแอพพลิเคชั่น จากนั้นจึงทำการคัดลอกตัวเองเข้าไปฝังตัวโดยใช้ช่องโหว่ดังกล่าว

๓.๔ โทรจัน (Trojan) เป็นมัลแวร์ชนิดหนึ่ง ที่มีจุดประสงค์เพื่อบุกรุก เข้าถึง และควบคุมเครื่องคอมพิวเตอร์จากระยะไกล ดำเนินการเปลี่ยนแปลง ทำลายไฟล์ข้อมูลสำคัญ หรือทำการคัดลอกข้อมูลดังกล่าวส่งให้แก่ผู้คุกคามผ่านระบบเครือข่ายอินเทอร์เน็ต ซึ่งข้อมูลสำคัญที่ผู้คุกคามต้องการอาจเป็น ชื่อผู้ใช้ รหัสผ่าน เลขที่บัญชีธนาคาร และข้อมูลส่วนบุคคล

๓.๕ สปายแวร์ (Spyware) เป็นมัลแวร์ชนิดหนึ่งที่มีวัตถุประสงค์เพื่อบันทึกการกระทำของผู้ใช้บนเครื่องคอมพิวเตอร์และส่งผ่านอินเทอร์เน็ตโดยที่ผู้ใช้ไม่ได้รับทราบ โปรแกรมแอบดักข้อมูลนั้นสามารถรวบรวมข้อมูล สถิติการใช้งานจากผู้ใช้ได้หลายอย่างขึ้นอยู่กับการออกแบบของโปรแกรม

๓.๖ ซอฟต์แวร์เรียกค่าไถ่ (ransomware) เป็นมัลแวร์ชนิดหนึ่ง ที่มีพฤติกรรมเข้ารหัสไฟล์ต่าง ๆ ที่อยู่บนเครื่องคอมพิวเตอร์ ไม่ว่าจะเป็นฟล์เอกสาร รูปภาพ วิดีโอ ผู้ใช้งานจะไม่สามารถปิดไฟล์ใด ๆ ได้เลยหากไฟล์เหล่านั้นถูกเข้ารหัส ซึ่งผู้ใช้งานจะต้องทำการจ่ายเงินตามข้อความ "เรียกค่าไถ่" ที่ปรากฏจึงจะได้รหัสเพื่อปลดล็อคข้อมูลและสามารถกู้ข้อมูลกลับมาได้

๓.๗ การโจมตีแบบ DOS/DDOS มีจุดประสงค์เพื่อทำให้เครื่องคอมพิวเตอร์แม่ข่าย (Server) หยุดทำงาน หากเครื่องคอมพิวเตอร์ที่โจมตี มีเครื่องเดียว เรียกว่าการโจมตีแบบ Denial of Service (DoS) แต่หากมีเครื่องคอมพิวเตอร์ที่โจมตีมีมากกว่า ๑ เครื่องและกระทำพร้อมๆ กัน ไม่ว่าจะโดยตั้งใจหรือไม่ตั้งใจ จะเรียกว่า การโจมตีแบบ Distributed Denial of Service (DDoS)

๓.๘ Botnet เป็นกลุ่มของอุปกรณ์ที่ติดมัลแวร์และถูกเปลี่ยนเป็น Bot (ย่อมาจาก Robot) ไม่ว่าจะเป็นอุปกรณ์คอมพิวเตอร์ เว็บแคม เราท์เตอร์ หรืออุปกรณ์ IoT อื่นๆ เพื่อรอรับคำสั่งจากผู้บุกรุก (Hacker) โดยผู้บุกรุก (Hacker) จะนำ Botnet ที่มีไปใช้ในการโจมตีขนาดใหญ่ เช่นการทำ DDOS เป็นต้น

๓.๙ Spam Mail หรืออีเมล์ขยะ เป็นขยะออนไลน์ที่ส่งตรงถึงผู้รับ โดยที่ผู้รับสารนั้นไม่ต้องการ และสร้างความเดือดร้อน รำคาญให้กับผู้รับได้ในลักษณะของการโฆษณาสินค้าหรือบริการ การชักชวนเข้า ไปยังเว็บไซต์ต่าง ๆ ซึ่งอาจมีภัยคุกคามชนิด phishing แฝงเข้ามาด้วย ด้วยเหตุนี้จึงควรติดตั้งระบบ anti spam หรือหากใช้ฟรีอีเมล์ก็จะมีโปรแกรมคัดกรองอีเมล์ขยะในชั้นหนึ่งแล้ว

๓.๑๐ Phishing คือการหลอกลวงทางอินเทอร์เน็ต เพื่อขอข้อมูลที่สำคัญเช่น รหัสผ่าน หรือหมายเลขบัตรเครดิต โดยการส่งข้อความผ่านทางอีเมลหรือเมสเซนเจอร์ ตัวอย่างของการฟิชชิง เช่น การบอกแก่ผู้รับปลายทางว่าเป็นธนาคารหรือบริษัทที่น่าเชื่อถือ และแจ้งว่ามีสาเหตุทให้คุณต้องเข้าสู่ระบบและ ใส่ข้อมูลที่สำคัญใหม่ โดยเว็บไซต์ที่ลิงก์ไปนั้นจะมีหน้าตาคล้ายคลึงกับเว็บที่กล่าวถึง Phishing

๓.๑๑ Sniffing เป็นการดักข้อมูลที่ส่งจากคอมพิวเตอร์เครื่องหนึ่ง ไปยังอีกเครื่องหนึ่ง หรือจากเครือข่ายหนึ่งไปยังอีกเครือข่ายหนึ่ง เป็นวิธีการหนึ่งที่ผู้บุกรุกระบบนิยมใช้

๓.๑๒ Hacking เป็นการเจาะระบบเครือข่ายคอมพิวเตอร์ไม่ว่าจะกระทำด้วยมนุษย์หรืออาศัยโปรแกรมด้วยวัตถุประสงค์ต่าง ๆ กัน ทั้งนี้โดยทั่วไปแล้วการ Hacking เป็นสิ่งที่ผิดกฎหมาย แต่อย่างไรก็ตามหากได้รับอนุญาตก็ไม่ใช่สิ่งผิดกฎหมาย โดยตัวอย่างของการ Hacking อย่างถูกกฎหมาย เช่น การเจาะระบบเพื่อประเมินความเสี่ยงของระบบคอมพิวเตอร์ และทดสอบระบบการรักษาความปลอดภัยเครือข่ายขององค์กร

๓.๑๓ ผู้บุกรุก (Hacker) หมายถึง ผู้ที่ไม่ได้รับอนุญาตในการใช้งานระบบ แต่พยายามลักลอบเข้ามาใช้งานด้วยวัตถุประสงค์ต่าง ๆ ไม่ว่าจะเพื่อโจรกรรมข้อมูล ผลกำไร หรือความพอใจส่วนบุคคลก็ตาม ความเสียหาย จากผู้บุกรุกเป็นภัยคุกตามที่หนัก

๔. การเตรียมความพร้อมในการรับมือปัญหาภัยคุกคามทางไซเบอร์

เพื่อให้สำนักงาน ป.ย.ป. มีความพร้อมในการรับมือปัญหาภัยคุกคามทางไซเบอร์ตามระบุในข้อ ๓ มีความจำเป็นต้องดำเนินการเตรียมความพร้อมในด้านต่าง ๆ ดังนี้

๔.๑ การเตรียมพร้อมด้านอุปกรณ์

เพื่อให้ระบบเครือข่ายคอมพิวเตอร์กลางของสำนักงาน ป.ย.ป. สามารถรับมือกับภัยคุกคามทางไซเบอร์ได้ สำนักงาน ป.ย.ป. จึงจัดหาอุปกรณ์และซอฟต์แวร์ที่จำเป็นดังนี้

(๑) อุปกรณ์ป้องกันระบบเครือข่าย (Next Generation Firewall) ใช้สำหรับป้องกันภัยคุกคามทางไซเบอร์ประเภท DoS/DDOS BOTNET Phishing Sniffing Hacker ทั้งนี้อุปกรณ์ป้องกันระบบเครือข่ายที่จัดหานอกจากความสามารถในการเป็น Firewall แล้วยังต้องมีความสามารถอื่น ๆ เพิ่มเติม ซึ่งได้แก่ความสามารถในด้านการตรวจจับการบุกรุก (IPS) ความสามารถในการคัดกรองเว็บไซต์อันตราย (Web filtering) และ การควบคุมการใช้งานซอฟต์แวร์ (Application Control) เป็นอย่างน้อย

(๒) ระบบสำรองข้อมูล ใช้สำหรับกระบวนการสำรองข้อมูล และ การกู้ข้อมูล ของระบบเครือข่ายคอมพิวเตอร์ของสำนักงาน ป.ย.ป. รวมทั้งยังสามารถสำรองข้อมูลแบบเข้ารหัสได้ โดยดำเนินการเก็บข้อมูลไว้ที่ฐานข้อมูลของโครงการพัฒนาระบบคลาวด์กลางภาครัฐ (GDCC) ซึ่งมีความปลอดภัยสูงมาก

(๓) ซอฟต์แวร์ป้องกันไวรัสคอมพิวเตอร์แบบคอร์ปอเรต (Corporate Antivirus Software) ใช้สำหรับติดตั้งบนเครื่องคอมพิวเตอร์ (PC) เครื่องคอมพิวเตอร์พกพา (Notebook) และเครื่องคอมพิวเตอร์แม่ข่าย ของสำนักงาน ป.ย.ป. ซึ่งสามารถป้องกันภัยคุกคามไซเบอร์ประเภท Malware, Computer Virus ,Computer worm ,Trojan ,Spyware smw ,BOTET ได้

๔.๒ แผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

เพื่อให้ระบบเครือข่ายคอมพิวเตอร์กลางของสำนักงาน ป.ย.ป. สามารถรับมือกับภัยคุกคามทางไซเบอร์ที่มีการพัฒนาขึ้นตลอดเวลา สำนักงาน ป.ย.ป. จะพิจารณาจ้างบริษัทผู้เชี่ยวชาญในการประเมินความเสี่ยงการรักษาความมั่นคงปลอดภัยไซเบอร์มาตรวจสอบ อย่างน้อยปีละ ๑ ครั้ง ซึ่งในการตรวจสอบและประเมินความเสี่ยงนี้อาจสามารถค้นหาภัยคุกคามไซเบอร์ประเภท Backdoor ที่ถูกซ่อนเอาไว้จากขั้นตอนการพัฒนาระบบงานคอมพิวเตอร์ได้

๔.๓ การเตรียมพร้อมด้านบุคลากร

๔.๓.๑ การให้ความรู้

เพื่อให้บุคลากรของสำนักงาน ป.ย.ป. มีความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ สำนักงาน ป.ย.ป. จึงได้ให้บุคลากรที่เกี่ยวข้องกับภารกิจงานด้านการดูแลความมั่นคงปลอดภัยไซเบอร์เข้าร่วมการฝึกอบรมเพื่อพัฒนาองค์ความรู้ให้ทันต่อการเปลี่ยนแปลงของเทคโนโลยีอยู่เสมอ

๔.๓.๒ การแจ้งรายชื่อเจ้าหน้าที่ สำหรับประสานงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตาม พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตราที่ ๔๖ กำหนดให้หน่วยงานภาครัฐแจ้งรายชื่อเจ้าหน้าที่ระดับบริหารและระดับปฏิบัติการ เพื่อประสานงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ไปยังสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยสำนักงาน ป.ย.ป. ได้มีคำสั่งสำนักงาน ป.ย.ป. ที่ ๕๖/๒๕๖๕ เรื่อง แต่งตั้งคณะกรรมการเทคโนโลยีดิจิทัล และกำกับดูแลข้อมูลของสำนักงาน ป.ย.ป. แล้ว

๔.๓.๓ มีผู้ดูแลด้านการรักษาความมั่นคงปลอดภัยเครือข่าย และ ผู้ดูแลระบบเครือข่ายคอมพิวเตอร์กลางของสำนักงาน ป.ย.ป. (ดูแลโดย GDCC)

๔.๔ การเตรียมพร้อมด้านการสำรองข้อมูลและระบบคอมพิวเตอร์สำรอง

ในกรณีที่ภัยคุกคามทางไซเบอร์ก่อเกิดความเสียหายแก่ระบบเครือข่ายคอมพิวเตอร์กลางของสำนักงาน ป.ย.ป. อย่างมากจนไม่สามารถทำงานได้เป็นเวลานาน สำนักงาน ป.ย.ป. จะพิจารณาทางเลือกในการแก้ไขปัญหาโดยวิธีการกู้คืนข้อมูลที่เสียหาย หรือปิดใช้งานระบบฐานข้อมูลเพื่อป้องกันการถูกโจมตีที่จะสร้างความเสียหายเป็นวงกว้าง จากนั้นจึงให้ผู้เชี่ยวชาญทำการกู้ระบบกลับคืน โดยมีเป้าหมายเพื่อให้ระบบเครือข่ายคอมพิวเตอร์กลางของสำนักงาน ป.ย.ป. สามารถใช้งานได้อย่างรวดเร็วที่สุด

๕. การเตรียมพร้อมรับมือภัยคุกคามทางไซเบอร์ในส่วนบุคลากรของสำนักงาน ป.ย.ป.

เมื่อเกิดการคุกคามทางไซเบอร์และผลกระทบที่เกิดขึ้นอาจส่งผลให้การทำงานของเครื่องคอมพิวเตอร์ของบุคลากรของสำนักงาน ป.ย.ป. ทำงานผิดพลาดหรือล่าช้าลง หรือส่งผลให้ไฟล์ข้อมูลที่ถูกจัดเก็บเอาไว้ในเครื่องคอมพิวเตอร์ไม่สามารถใช้งานได้ และยากต่อการกู้คืนให้เป็นปกติ ดังนั้นบุคลากรของสำนักงาน ป.ย.ป. ควรดำเนินการเตรียมพร้อมรับมือภัยคุกคามทางไซเบอร์ดังนี้

๕.๑ ดำเนินการตามนโยบายการใช้งานระบบป้องกันไวรัสสำหรับเครื่องคอมพิวเตอร์อย่างเคร่งครัด

๕.๒ ดำเนินการตามนโยบายการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล และ นโยบายการใช้งานเครื่องคอมพิวเตอร์แบบพกพาอย่างเคร่งครัด โดยสำนักงาน ป.ย.ป. จะดำเนินการสนับสนุนการเตรียมพร้อมรับมือภัยคุกคามทางไซเบอร์ ดังนี้

(๑) ดำเนินการจัดหาซอฟต์แวร์ป้องกันไวรัสคอมพิวเตอร์แบบคอร์ปอเรต (Corporate Antivirus Software) ให้เพียงพอต่อจำนวนบุคลากรของสำนักงาน ป.ย.ป.

(๒) ดำเนินการจัดเตรียมพื้นที่จัดเก็บข้อมูลส่วนกลาง โดยทำการเก็บข้อมูลทั้งหมดไว้ที่ฐานข้อมูลของ GDCC โดยปัจจุบันมีขนาดการเก็บที่ ๕๐๐ GB และจะมีการสำรองข้อมูลจากพื้นที่จัดเก็บข้อมูลส่วนกลางทุกวัน (วันละ ๑ ครั้ง) เพื่อป้องกันเหตุฉุกเฉินก็จะสามารถสำเนาข้อมูลสำคัญที่เก็บอยู่บนพื้นที่จัดเก็บข้อมูลส่วนกลางกลับมาได้