เรียบเรียง : อนงค์นาฏ ศรีรัตนา ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
ข้อมูล : วรวุฒิ อ้อยหวาน ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

การยกระดับ ความมั่นคงปลอดภัยไซเบอร์ ตอนที่ 1

กรมส่งเสริมการเกษตร ได้เห็นความสำคัญในด้านภัยคุกคามไซเบอร์ที่เกิดขึ้นอย่างต่อเนื่องและต้องเร่งตรวจสอบแก้ไขให้สอดคล้องและเป็นไปตาม ***พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562*** ซึ่งมีผลบังคับใช้ เมื่อวันที่ 28 พฤษภาคม 2562 เพื่อป้องกันความเสี่ยงจากภัยคุกคามทางไซเบอร์อันอาจกระทบ ต่อความมั่นคงของรัฐ และความสงบเรียบร้อยภายในประเทศ

การดำเนินการของกรมส่งเสริมการเกษตร

1. แต่งตั้งผู้บริหารความมั่นคงปลอดภัยสารสนเทศ ของกรมส่งเสริมการเกษตร (Chief Information Security Officer: CISO) โดย นางอัญชลี สุวจิตตานนท์ รองอธิบดีกรมส่งเสริมการเกษตร ด้านบริหาร เป็นผู้บริหารความมั่นคงปลอดภัยสารสนเทศ ของกรมส่งเสริมการเกษตร เมื่อวันที่ 15 กันยายน 2566

2. แต่งตั้งคณะกรรมการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เมื่อวันที่ 15 กันยายน 2566 ซึ่งมีผู้บริหารความมั่นคงปลอดภัยสารสนเทศของกรมส่งเสริมการเกษตร เป็นประธาน ผู้อำนวยการกอง/สำนัก (ส่วนกลาง) ผู้อำนวยการสำนักงานส่งเสริมและพัฒนาการเกษตรที่ 1 – 6 เกษตรกรุงเทพมหานคร เป็นกรรมการ ผู้อำนวยการเทคโนโลยีสารสนเทศและการสื่อสาร เป็นกรรมการและเลขานุการ และผู้อำนวยการกลุ่มระบบเครือข่ายคอมพิวเตอร์และความมั่นคงปลอดภัยทางไซเบอร์ เป็นกรรมการและผู้ช่วยเลขานุการ เพื่อ

- กำหนดนโยบายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ของกรมส่งเสริมการเกษตร
- พิจารณาทบทวนนโยบายความมั่นคงปลอดภัยไซเบอร์ตามที่คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) ประกาศใช้
- กำหนดกรอบมาตรฐานและแนวทางส่งเสริมการพัฒนาระบบการให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ของกรมส่งเสริมการเกษตร
- พิจารณาให้ความเห็นชอบแผนปฏิบัติการการรักษาความมั่นคงปลอดภัยไซเบอร์ ของกรมส่งเสริมการเกษตร สำหรับเป็นแนวทางในการรักษาความมั่นคงปลอดภัยไซเบอร์ในสถานการณ์ปกติและในสถานการณ์ที่อาจจะเกิดขึ้น หรือเกิดภัยคุกตามทางไซเบอร์

โดยจะต้องสอดคล้องกับนโยบาย ยุทธศาสตร์และแผนระดับชาติ และกรอบนโยบายและแผนแม่บทที่เกี่ยวกับการรักษาความมั่นคงของสภาความมั่นคงแห่งชาติ

3. แต่งตั้งผู้ประสานงานด้านการรักษาความปลอดภัยไซเบอร์ในการประสานงานกับสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เพื่อประโยชน์ในการรักษาความมั่นคงปลอดภัยไซเบอร์ จำนวน 2 รายดังนี้

- ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
- ผู้อำนวยการกลุ่มระบบเครือข่ายคอมพิวเตอร์และความมั่นคงปลอดภัยทางไซเบอร์

การป้องกันและรับมือภัยคุกคามไซเบอร์ด้วย NIST Cybersecurity Framework และ พรบ.ไซเบอร์ พ.ศ. 2562

1. การป้องกันและรับมือภัยคุกคามไซเบอร์ด้วย NIST Cybersecurity Framework

NIST Cybersecurity Framework เป็นกรอบแนวทางปฏิบัติที่ดีที่สุดสำหรับการป้องกันและรับมือกับภัยคุกคามไซเบอร์ รวมถึงการบริหารจัดการความเสี่ยง มีอยู่ 5 ขั้น ดังนี้

1) การระบุ (Identify) เป็นขั้นตอนแรกในการศึกษาทำความเข้าใจบริบท ทรัพยากร และกิจกรรมงานสำคัญ เพื่อบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่มีต่อระบบ ทรัพย์สิน ข้อมูล และ ขีดความสามารถ

2) การป้องกัน (Protect) เป็นการดำเนินการตามมาตรการป้องกันที่เหมาะสมสำหรับการให้บริการโครงสร้างพื้นฐาน โดยมีวัตถุประสงค์เพื่อลดผลกระทบของเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ ครอบคลุมการฝึกอบรมด้านความตระหนัก มาตรการควบคุมการเข้าถึง และมาตรการด้านความมั่นคงปลอดภัยต่าง ๆ ทั้งกระบวนการและวิธีปฏิบัติ ตลอดจนเทคโนโลยี

3) การตรวจจับ (Detect) เป็นการดำเนินการเพื่อเฝ้าระวังเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ที่อาจเกิดขึ้น ครอบคลุมถึงกระบวนการเฝ้าระวังหรือตรวจติดตามต่อเนื่อง

4) การตอบสนอง (Respond) เป็นการดำเนินการเพื่อตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์ที่ตรวจพบ ครอบคลุมถึงการวางแผนรับมือ การสื่อสาร การวิเคราะห์ การลดความเสี่ยง และการปรับปรุง

5) การคืนสภาพ (Recover) เป็นการดำเนินการตามแผนงานเพื่อรองรับการดำเนินงานต่อเนื่อง รวมถึงแผนการกู้คืนทั้งด้านขีดความสามารถและบริการให้ได้ตามที่กำหนด

> การขับเคลื่อนการป้องกันและรับมือ (Incidence and Response) ภัยคุกคามไซเบอร์ ด้วย NIST Cybersecurity Framework ให้ได้มาตรฐานเป็นที่ยอมรับตามแบบสากล เพื่อยกระดับการให้บริการด้านดิจิทัลให้พร้อมใช้งานอย่างมีประสิทธิภาพ

2. พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

มีการกำหนดวิธีการและมาตรฐานไว้ในพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มาตรา 13 สอดคล้องกับ NIST Cybersecurity Framework ตามแนวทางของกรมส่งเสริมการเกษตรในการดำเนินการ ดังนี้

1) การระบุความเสี่ยงที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล

2) มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น

3) มาตรการตรวจสอบและเฝ้าระหวังภัยคุกคามทางไซเบอร์

4) มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์

5) มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์

ติดตามต่อในฉบับหน้าเจาะลึกถึงขั้นตอนการปฏิบัติตามแนวทางพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ของกรมส่งเสริมการเกษตรว่ามีวิธีดำเนินการเตรียมพร้อมรับมือกับความเสี่ยงอย่างไรหากต้องเผชิญภัยคุกคามทางไซเบอร์ ✤