เรียบเรียง : อนงค์นาฏ ศรีรัตนา ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
ข้อมูล : วรวุฒิ อ้อยหวาน ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

การยกระดับความมั่นคงปลอดภัยไซเบอร์

ตอนที่ 2 (ตอนจบ)

จากบทความการยกระดับความมั่นคงปลอดภัยไซเบอร์ ตอนที่ 1 กล่าวถึงการปฏิบัติตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ในด้านนโยบายและกรอบแนวทางการปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์ไปแล้ว ตอนที่ 2 ซึ่งเป็นตอนจบนี้ จะกล่าวถึงขั้นตอนการปฏิบัติตามกรอบแนวทางดังกล่าว เพื่อยกระดับความมั่นคงปลอดภัยทางไซเบอร์ของกรมส่งเสริมการเกษตรอย่างมีประสิทธิภาพ

การควบคุมข้อมูลที่ไหลผ่านเข้า-ออกบนระบบเครือข่าย (Network Traffic)

ด้วยระบบควบคุมทราฟฟิกเครือข่ายเทคโนโลยีปัญญาประดิษฐ์ที่สามารถระบุความเสี่ยงของภัยคุกคาม ป้องกันความเสี่ยง ตรวจสอบและเฝ้าระวังสามารถเผชิญเหตุการณ์ภัยคุกคามในทุกระดับ เพื่อสร้างความมั่นคงปลอดภัยทางไซเบอร์ให้กับการดำเนินงานขับเคลื่อนไปสู่การให้บริการดิจิทัลได้อย่างมั่นคงปลอดภัย มีองค์ประกอบของระบบ ดังนี้

1. Next Generation Firewall (NGFW)

คือ อุปกรณ์ Firewall ที่มีเทคโนโลยีปัญญาประดิษฐ์ (AI) ที่นำมาใช้ตรวจจับภัยคุกคามขั้นสูงที่ไม่สามารถตรวจพบได้ด้วยอุปกรณ์ทั่วไปเพื่อจัดการกับภัยคุกคามไซเบอร์ ด้วยโมเดลการเรียนรู้ของเครื่องและอัลกอริทึมของAI สามารถป้องกันภัยคุกคามขั้นสูงแบบ Advanced Persistent Threat (APT) การป้องกันภัยจากช่องโหว่และความเสี่ยงของภัยคุกคามที่ไม่เคยค้นพบมาก่อน (Zero-day) โดยหลังจากการนำระบบดังกล่าวมาใช้ทำให้ตรวจพบเหตุการณ์โจมตีในระบบเครือข่ายของกรมส่งเสริมการเกษตร

2. Web Application Firewall (WAF)

เทคโนโลยี Web Application Firewall (WAF) ใช้จัดการความมั่นคงปลอดภัยสำหรับการให้บริการเว็บไซต์ เว็บแอปพลิเคชัน หรือเว็บ API โดยเฉพาะ ซึ่งจะสามารถป้องกันการเขียนโปรแกรมคำสั่งฐานข้อมูลที่ไม่ปลอดภัย (SQL Injection) การป้องกันการเปลี่ยนแปลงหน้าเว็บด้วยเทคนิคการขโมย Session (Cross site scripting) การป้องกันข้อผิดพลาดในการตรวจสอบสิทธิ์การเข้าถึงที่ไม่ปลอดภัย (Insecure Direct Object References) การป้องกันการตั้งค่าที่ผิดพลาดบนโปรแกรมเว็บเซิร์ฟเวอร์ (Security misconfiguration) ป้องกันการเข้าถึงระดับของสิทธิ์ที่ผิดพลาด (Missing Function Level Access Control) ป้องกันการเขียนโปรแกรมปลอมแปลงสิทธิ์ (Cross site request forgery) การป้องกันการเปลี่ยนเส้นทางไปยังเว็บไซต์อันตราย (Unvalidated Redirects and Forwards Unvalidated) และที่สำคัญสามารถป้องกันภัยคุกคามตามมาตรฐานสำคัญในการป้องกันด้านเว็บไซต์โดยเฉพาะ และครอบคลุมการป้องกันภัยคุกคามไซเบอร์เว็บไซต์ตามเอกสารมาตรฐานสิ่งที่ต้องคำนึงและให้ความสำคัญในความเสี่ยงด้านความมั่นคงปลอดภัยของเว็บ (OWASP Top 10) สำหรับผู้พัฒนาระบบเว็บไซต์

“

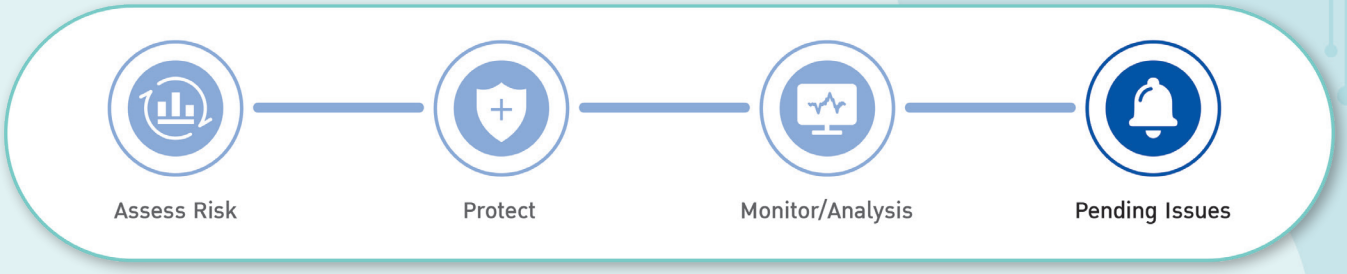
ศูนย์ SOC สนับสนุนการตรวจสอบ
และแก้ไขปัญหาของเจ้าหน้าที่รักษาความมั่นคงปลอดภัยไซเบอร์
ซึ่งสามารถระบุสถานะของภัยคุกคาม
ตอบสนองได้ง่ายและรวดเร็วขึ้น

”

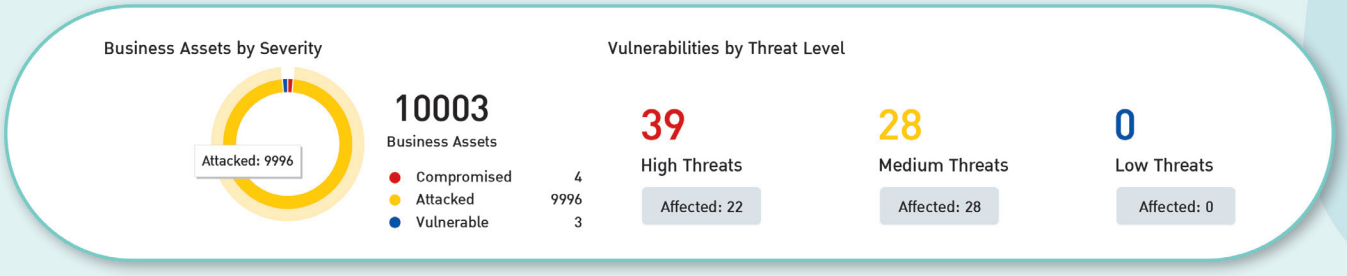
3. Security Operation Center (SOC)

ระบบการเฝ้าระวังแบบ Security Operation Center หรือศูนย์ SOC สนับสนุนการตรวจสอบและแก้ไขปัญหาของเจ้าหน้าที่รักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งสามารถระบุสถานะของภัยคุกคามตอบสนองได้ง่ายและรวดเร็วขึ้น พร้อมแนวทางและวิธีการแก้ไขต่อภัยคุกคามที่ตรวจพบ อาทิ

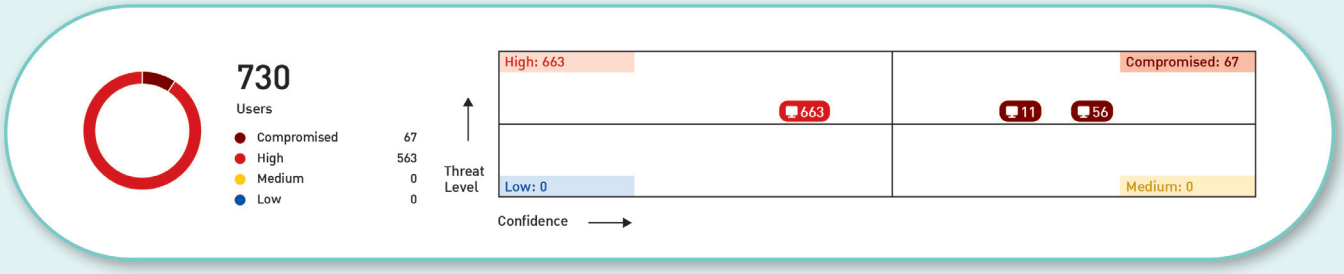
1) การปฏิบัติการด้านความมั่นคงปลอดภัยอย่างเป็นขั้นตอน ประกอบด้วย การประเมินความเสี่ยง (Access Risk) การป้องกันจากการประเมินความเสี่ยง (Protected) การตรวจติดตามและวิเคราะห์ (Monitor/Analysis) และประเด็นภัยคุกคามที่ตรวจพบและรอพิจารณา (Pending Issues)



2) การตรวจสอบอุปกรณ์ให้บริการ (Business Asset Security) ผ่านเว็บไซต์ โดเมน หรือหมายเลขไอพี วิเคราะห์ข้อมูลที่วิ่งไหลเข้าออกภายในระบบเครือข่ายคอมพิวเตอร์ ทำให้ทราบสถานะภัยคุกคาม (Compromised, Attacked, Vulnerable) และระดับความรุนแรงของภัยคุกคามที่ได้ (High, Medium, Low)



3) การตรวจสอบผู้ใช้งาน (User Security by Severity) เป็นการตรวจจับภัยคุกคามที่เกิดขึ้นบนเครื่อง ลูกข่ายและระดับความรุนแรงที่ตรวจพบ (Compromised, High, Medium, Low)



> “บุคลากรทุกท่านควรมีความตระหนักรู้ ถึงแนวทางและวิธีการป้องกันตัวเอง เพื่อความมั่นคงปลอดภัยของข้อมูล และสารสนเทศของกรมส่งเสริมการเกษตร และตัวท่านเอง”

4. ภัยคุกคามขั้นสูง Advance Persistent Threat (APT)

โดยการนำใช้เทคโนโลยี AI เข้ามาวิเคราะห์พฤติกรรม (Behavior Analysis) การโจมตี ช่องโหว่ แต่ละแบบจากฐานข้อมูลภัยคุกคามทั่วโลก (Global Threat Intelligence) เมื่อตรวจพบภัยคุกคามแล้วสามารถจัดการภัยคุกคามเหล่านั้นได้แบบอัตโนมัติตามนโยบายที่ถูกกำหนดไว้ในระบบบริหารจัดการ สามารถยับยั้งการเข้าถึงเว็บไซต์ที่ต้องสงสัยว่ามีอันตรายต่อเครื่องคอมพิวเตอร์ในเครือข่ายจากที่อยู่โดเมนที่ไม่ปลอดภัย (Suspicious DNS address) ที่ได้รับจากอีเมลหรือลิงค์เว็บไซต์ (Backlink)

5. การป้องกันภัยคุกคามอุปกรณ์ปลายทาง (Endpoint Security)

5.1 ความมั่นคงปลอดภัยอุปกรณ์ปลายทาง (Endpoint)

โดยมีการติดตั้งโปรแกรมป้องกันไวรัสให้กับเครื่องคอมพิวเตอร์โน้ตบุ๊ค 932 เครื่องและ เครื่องคอมพิวเตอร์ 219 เครื่อง รวม 1,151 เครื่องของหน่วยงานในสังกัดกรมฯ สามารถยับยั้งการแพร่กระจายของภัยคุกคามร้ายแรงโดยเฉพาะโปรแกรมไวรัสเรียกค่าไถ่ (Ransomware) โดยปีงบประมาณ พ.ศ. 2567 ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารอยู่ระหว่างการเสนอของบประมาณรายจ่ายประจำปี เพื่อขยายผลการตรวจสอบและจัดการความมั่นคงปลอดภัยไปยังอุปกรณ์ปลายทางบนระบบเครือข่ายของกรมส่งเสริมการเกษตร ยกระดับระบบรักษาความปลอดภัยไซเบอร์ได้อย่างครอบคลุมยิ่งขึ้น

5.2 การตรวจสอบและควบคุมอุปกรณ์ปลายทางให้ลดความเสี่ยงและช่องโหว่

1) สำหรับระบบปฏิบัติ windows ทั่วไป ผู้ใช้งาน ทำการ Update Patch ที่สำคัญเป็นประจำ เพื่อความปลอดภัยของระบบปฏิบัติการ แต่สำหรับเครื่องที่ติดตั้ง Endpoint การปรับปรุงความปลอดภัย เสริมจากระบบปฏิบัติการ ส่วนควบคุมกลางสามารถสั่ง Update ระบบปฏิบัติการได้

2) การป้องกันมัลแวร์ที่มาจากการติดตั้งซอฟแวร์ไม่ถูกต้องหรือไม่ถูกลิขสิทธิ์ ทำให้ระบบการทำงานของเครื่องปลายทางเกิดช่องโหว่ ทำงานผิดปกติ และข้อมูลรั่วไหลหรือเสียหาย รวมถึงเครื่องที่ถูกยึดครอง (Command & Control) อาจถูกใช้เพื่อกระจายมัลแวร์ไปยังเครื่องอื่นผ่านเครือข่ายภายในและภายนอกหน่วยงานส่งผลถึงความน่าเชื่อถือ (Reputition) ของหน่วยงานในการสื่อสารผ่านระบบเครือข่ายอินเทอร์เน็ตได้

6. การฟื้นฟูและคืนสภาพแพลตฟอร์มและบริการดิจิทัล (Digital Platform and Service Resilient)

เมื่อเกิดโจมตีระบบทำให้ไม่สามารถให้บริการได้แล้ว กรมส่งเสริมการเกษตรได้ให้ความสำคัญและมีแนวทางการดังนี้

6.1 การสำรองและกู้คืนแบบเบ็ดเสร็จอัตโนมัติ

มีการสำรองและกู้คืนแบบเบ็ดเสร็จอัตโนมัติ ด้วยเทคโนโลยีลดความซ้ำซ้อน (Deduplication) มาใช้ในการจัดเก็บข้อมูล ทำให้การสำรองข้อมูลมีประสิทธิภาพ ใช้ระยะเวลาน้อยลง และการกู้คืนทำได้อย่างรวดเร็ว ซึ่งสามารถดึงข้อมูลย้อนหลังได้ 30 วัน หรือ 1 เดือนได้เป็นอย่างน้อย

6.2 การตรวจจับมัลแวร์ (Malware)

มีกระบวนการตรวจสอบก่อนและหลังในการการสำรองข้อมูลในทุกประเภทข้อมูล เพื่อให้มั่นใจได้ว่า จะสามารถควบคุมไม่ให้เกิดภัยคุกคามร้ายแรงหรือการแพร่กระจายของมัลแวร์ลงไปสู่ข้อมูลที่สำรองเก็บไว้

6.3 การป้องกันภัยคุกคามต่อการเรียกค่าไถ่ (Ransomware)

เมื่อเกิดกรณีการคุกคามด้วย มัลแวร์เรียกค่าไถ่ ทำให้ไม่สามารถนำข้อมูลสารสนเทศมาใช้งานได้ จึงมีความจำเป็นต้องนำข้อมูลที่สำรองไว้มาใช้งานแทน แต่หากระบบการสำรองข้อมูลไม่สามารถป้องกัน Ransomware ทำให้ข้อมูลที่สำรองไว้ซึ่งถือเป็นข้อมูลชุดสุดท้ายไม่สามารถนำมากู้คืนใช้งาน ย่อมสร้างความเสียหายต่อการดำเนินการต่าง ๆ ที่ต้องใช้ข้อมูลสารสนเทศเหล่านั้น

6.4 นโยบายการสำรองระบบแพลตฟอร์มและข้อมูล กำหนดไว้ดังนี้

1) กลุ่มฐานข้อมูล (Database server) สำรองข้อมูลทุกวันจันทร์ – ศุกร์ ย้อนหลังได้ 1 เดือน

2) กลุ่มระบบแพลตฟอร์ม (Application server) สำรองข้อมูลทุกวันเสาร์ ย้อนหลังได้ 1 เดือน

3) กลุ่มไฟล์เอกสารและไฟล์รูปภาพ (Application server) สำรองข้อมูลทุกวันย้อนหลังได้ 1 เดือน

ภัยคุกคามทางไซเบอร์ ไม่ใช่เรื่องไกลตัว ทุกวันนี้มีการล่อลวงจากมิจฉาชีพ การโจมตีระบบเครือข่าย เพื่อหยุดยั้งการทำงานหรือการขโมยข้อมูลส่วนบุคคลตลอดเวลา แม้กรมส่งเสริมการเกษตรจะมีนโยบายและกรอบแนวทางการปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์อย่างรัดกุม และแน่นหนาเพียงใด ภัยคุกคามที่ควบคุมได้ยากที่สุด คือ ภัยคุกคามโดยบุคลากรภายในหน่วยงานเอง ซึ่งอาจจะเกิดขึ้นโดยความตั้งใจหรือไม่ตั้งใจ ดังนั้น บุคลากรทุกท่านควรมีความตระหนักรู้ถึงแนวทางและวิธีการป้องกันตัวเองเพื่อความมั่นคงปลอดภัยของข้อมูลและสารสนเทศของกรมส่งเสริมการเกษตรและตัวท่านเอง ✣