

สรุปรายงานผลการพัฒนาความรู้ของข้าราชการ
สถานีพัฒนาที่ดินปราจีนบุรี สำนักงานพัฒนาที่ดินเขต ๒ กรมพัฒนาที่ดิน
รอบการประเมินที่ ๒/๒๕๖๙ ตั้งแต่วันที่ ๑ เมษายน ๒๕๖๙ - ๓๐ กันยายน ๒๕๖๙
ประจำปีงบประมาณ ๒๕๖๙

ชื่อ-นามสกุล นายสาโรช ดรงค์กาญจน์ ตำแหน่ง นักวิชาการเกษตรชำนาญการ
หน่วยงาน ฝ่ายวิชาการเพื่อการพัฒนาที่ดินที่ ๓ สถานีพัฒนาที่ดินปราจีนบุรี สำนักงานพัฒนาที่ดินเขต ๒
หัวข้อการพัฒนา "ทักษะด้านความมั่นคงปลอดภัยทางไซเบอร์เบื้องต้น : Basic Cybersecurity Serie"
วิธีการพัฒนา การเรียนรู้ผ่านการพัฒนาทางไกลด้วยระบบอิเล็กทรอนิกส์ TDGA e-Learning
วันที่ ๖-๙ กรกฎาคม ๒๕๖๙ สถานที่ สถานีพัฒนาที่ดินปราจีนบุรี
หน่วยงานที่จัดอบรม สถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล (Thailand Digital Government Academy : TDGA)

วัตถุประสงค์

๑. ได้รับความรู้เกี่ยวกับการตระหนักและทราบถึงวิธีการป้องกันภัยทางไซเบอร์ (Cybersecurity)
๒. ได้รับความรู้ความเข้าใจความหมาย และเห็นความสำคัญของการประยุกต์การใช้งานความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity)

สรุปสาระสำคัญ

"ทักษะด้านความมั่นคงปลอดภัยทางไซเบอร์เบื้องต้น : Basic Cybersecurity Serie"

แนวทางการรักษาความมั่นคงปลอดภัยทางไซเบอร์

๑. การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Risk Assessment)

ความเสี่ยง (Risk) หมายถึง ความเป็นไปได้ที่เหตุการณ์หนึ่งจะเกิดขึ้นและส่งผลกระทบต่อเป้าหมายหรือผลลัพธ์ที่คาดหวัง โดยอาจเป็นผลกระทบเชิงลบ เช่น ความเสียหาย ขาดทุน หรือการหยุดชะงัก แต่บางครั้งก็อาจมีผลเชิงบวก เช่น โอกาสทางธุรกิจใหม่ ๆ

การบริหารความเสี่ยง (Risk Management) หมายถึง กระบวนการอย่างเป็นระบบในการระบุ วิเคราะห์ ประเมิน และจัดการความเสี่ยง เพื่อให้สามารถควบคุมหรือบรรเทาผลกระทบที่อาจเกิดขึ้นต่อเป้าหมายขององค์กร โครงการ หรือกิจกรรมต่าง ๆ

๒. กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Framework)

CIA Model หรือ CIA Triad คือกรอบแนวคิดพื้นฐานด้านความมั่นคงปลอดภัยสารสนเทศ ประกอบด้วย ๓ เสาหลัก: Confidentiality (การรักษาความลับ), Integrity (ความถูกต้องครบถ้วน), และ Availability (ความพร้อมใช้งาน) ซึ่งใช้เป็นมาตรฐานสากลในการออกแบบและประเมินระบบความปลอดภัยทางไซเบอร์

กรอบมาตรฐานหลักที่นิยมใช้ในประเทศไทยมี ๒ กรอบมาตรฐาน

(๑) NIST Cybersecurity Framework (CSF) ๒.๐

National Institute of Standard and Technology ประกอบด้วยฟังก์ชันหลัก ๖ ด้าน: Identify, Protect, Detect, Respond, Recover และ Govern (เพิ่มใหม่ในปี ๒๐๒๔) เน้นการบริหารความเสี่ยงเชิงองค์กรและซัพพลายเชน ใช้ได้กับทุกขนาดองค์กร ตั้งแต่ภาครัฐจนถึงธุรกิจเอกชน

(๒) ISO/IEC ๒๗๐๐๑:๒๐๒๒

International Organization for Standardization (ISO) ใช้หลักการ การประเมินความเสี่ยง, การจัดการความเสี่ยง, การป้องกันความเสี่ยง, การลดความเสี่ยง และความปลอดภัยของข้อมูลสารสนเทศ

๓. การป้องกันความเสี่ยง (Protect) โดยการประเมินช่องโหว่ (Vulnerability Assessment - VA)

เพื่อให้ระบบสารสนเทศมีความมั่นคงปลอดภัย โดยเน้นการค้นหาและจัดลำดับความรุนแรงของช่องโหว่ ก่อนที่ผู้โจมตีจะใช้ประโยชน์จากมัน โดยมีแนวทางการประเมินช่องโหว่ (VA) ดังนี้

(๑) การระบุช่องโหว่ (Identify Vulnerabilities)

- ใช้เครื่องมือสแกน เช่น Nessus, OpenVAS, Qualys
- ตรวจสอบระบบปฏิบัติการ, แอปพลิเคชัน, และการตั้งค่าที่ไม่ปลอดภัย

(๒) การวิเคราะห์และจัดลำดับความเสี่ยง (Analyze & Prioritize)

- ประเมิน CVSS Score (Common Vulnerability Scoring System)
- จัดลำดับความสำคัญตามผลกระทบและความน่าจะเป็น

(๓) การจัดการและแก้ไข (Mitigation & Remediation)

- อัปเดตแพตช์ (Patch Management)
- ปรับปรุงการตั้งค่า (Configuration Hardening)
- ใช้มาตรการเสริม เช่น Firewall, IDS/IPS

(๔) การติดตามและทบทวน (Monitoring & Review)

- ทำการสแกนอย่างต่อเนื่อง (Continuous Vulnerability Management)
- บันทึกและรายงานผลเพื่อปรับปรุงกระบวนการ

๔. การตรวจสอบ และเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)

ช่วยให้องค์กรสามารถ ระบุและแจ้งเตือนภัยคุกคามได้อย่างทันที่ ก่อนที่จะสร้างความเสียหายรุนแรง โดยใช้อุปกรณ์และเครื่องมือหลักในการเฝ้าระวังภัยคุกคามไซเบอร์ ดังนี้

(๑) ระบบตรวจจับและป้องกันการบุกรุก (IDS/IPS)

- IDS (Intrusion Detection System): ตรวจจับการโจมตีหรือการเข้าถึงที่ผิดปกติ
- IPS (Intrusion Prevention System): บล็อกการโจมตีทันทีที่ตรวจพบ
- เหมาะสำหรับองค์กรที่ต้องการป้องกันการบุกรุกเครือข่ายโดยตรง

(๒) ระบบจัดการข้อมูลเหตุการณ์ด้านความปลอดภัย (SIEM)

- รวบรวมและวิเคราะห์ข้อมูลจากหลายแหล่ง เช่น Network Logs, Server Logs,
- ตรวจจับพฤติกรรมผิดปกติและแจ้งเตือนแบบเรียลไทม์

(๓) Endpoint Detection and Response (EDR/XDR)

- ตรวจสอบการทำงานของอุปกรณ์ปลายทาง เช่น PC, Laptop, Mobile
- สามารถตรวจจับมัลแวร์, Ransomware และการเข้าถึงที่ผิดปกติ

(๔) ระบบวิเคราะห์พฤติกรรม (UBA/Behavioral Analytics)

- วิเคราะห์พฤติกรรมผู้ใช้และอุปกรณ์เพื่อหาความผิดปกติ

(๕) เครื่องมือ AI และแพลตฟอร์มอัจฉริยะ

- Darktrace: ใช้ AI ตรวจจับความผิดปกติในเครือข่าย
- Vectra AI: วิเคราะห์พฤติกรรมและจัดลำดับความสำคัญของภัยคุกคาม
- Cylance: ใช้ AI คาดการณ์และป้องกันมัลแวร์

๕. การเผชิญเหตุภัยคุกคามภัยคุกคามทางไซเบอร์ (Respond) และการฟื้นฟูความเสียหายจากภัยคุกคามทางไซเบอร์ (Recover)

(๑) การเผชิญเหตุ (Respond) คือ ลดผลกระทบและควบคุมสถานการณ์ทันทีที่ตรวจพบภัยคุกคาม

- Incident Response Plan (IRP) จัดทำแผนรับมือเหตุการณ์ไซเบอร์
- การแจ้งเตือนและสื่อสาร (Communication) แจ้งทีมงานผู้บริหาร และผู้มีส่วนได้ส่วนเสีย
- การกักกัน (Containment) แยกระบบที่ถูกโจมตีออกจากเครือข่าย
- การแก้ไข (Eradication) ลบมัลแวร์ ปิดช่องโหว่ และปรับปรุงการตั้งค่า
- การบันทึกและวิเคราะห์ (Documentation & Forensics) เก็บหลักฐานดิจิทัลเพื่อหา

สาเหตุและป้องกันซ้ำ

(๒) การฟื้นฟู (Recover) คือ ทำให้ระบบกลับมาใช้งานได้ตามปกติและเสริมความมั่นคงในอนาคต

- การกู้คืนข้อมูล (Data Recovery) ใช้ Backup และระบบ Disaster Recovery
- การทดสอบระบบ (System Validation) ตรวจสอบความปลอดภัยก่อนเปิดใช้งาน
- การปรับปรุงมาตรการ (Improvement)
- การสื่อสารภายนอก (External Communication) แจ้งลูกค้า หน่วยงานกำกับดูแล หรือ

สาธารณะตามข้อกำหนด

- การเรียนรู้และพัฒนา (Lessons Learned) ใช้เหตุการณ์เป็นบทเรียนเพื่อเสริม

มาตรการป้องกัน

สิ่งที่สำคัญสำหรับการป้องกันภัยทางไซเบอร์ขั้นพื้นฐาน

๑. การปกป้องข้อมูลส่วนตัว การปกป้องข้อมูลส่วนตัวเป็นเรื่องสำคัญมากในยุคดิจิทัล เพราะข้อมูลของเรา เช่น ชื่อ ที่อยู่ เบอร์โทรศัพท์ รหัสผ่าน หรือแม้กระทั่งพฤติกรรมการใช้งานออนไลน์ สามารถถูกนำไปใช้โดยไม่ได้รับอนุญาตได้ หากไม่มีมาตรการป้องกันที่ดี

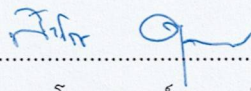
๒. การป้องกันการโจมตีทางไซเบอร์ (Cyber Attack Prevention) เป็นหัวใจสำคัญของ Cybersecurity Framework เพราะช่วยลดความเสี่ยงที่จะเกิดการสูญเสียข้อมูล ความเสียหายต่อระบบ และผลกระทบต่องค์กรหรือบุคคล

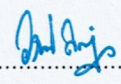
๓. การรับมือกับเหตุการณ์ภัยคุกคามทางไซเบอร์ (Cyber Incident Response) เป็นขั้นตอนสำคัญที่ช่วยให้องค์กรหรือบุคคลสามารถ ลดผลกระทบ ฟื้นฟูระบบ และป้องกันไม่ให้เกิดเหตุการณ์เกิดซ้ำ ได้อย่างมีประสิทธิภาพ

๔. การสร้างความเชื่อมั่นและความเชื่อถือ (Trust & Confidence) เป็นรากฐานสำคัญทั้งในด้านความมั่นคงปลอดภัยไซเบอร์ และ การทำงานร่วมกันในสังคม/องค์กร เพราะไม่ว่าระบบจะปลอดภัยแค่ไหน หากผู้ใช้หรือประชาชนไม่เชื่อมั่น ก็จะไม่เกิดการยอมรับและใช้งานอย่างเต็มที่

ประโยชน์ที่ได้รับจากการพัฒนาความรู้

มีความรู้ความเข้าใจเกี่ยวกับแนวทางการรักษาความมั่นคงปลอดภัยทางไซเบอร์ การประเมินความเสี่ยง กรอบมาตรฐานด้านความมั่นคง การประเมินช่องโหว่ การป้องกันภัยคุกคาม การเผชิญภัยคุกคามและการฟื้นฟู หลังโดนภัยคุกคามทางไซเบอร์ สามารถนำไปสื่อสารให้แก่ผู้อื่นได้

ลงนาม 
(นายสาโรช ดุรงค์กาญจน์)
ตำแหน่ง นักวิชาการเกษตรชำนาญการ

ลงนาม 
(นางสาววรรัตน์ สิวรางกุล)
ตำแหน่ง ผู้อำนวยการสถานีพัฒนาที่ดินปราจีนบุรี

1. การประเมินความเสี่ยง (Risk Assessment)

- [ระบุทรัพย์สินสำคัญ]
- [วิเคราะห์โอกาสและผลกระทบ]
- [กำหนดระดับความเสี่ยง]

2. กรอบมาตรฐาน (Cybersecurity Framework)

- [ใช้มาตรฐาน ISO 27001]
- [อ้างอิง NIST CSF]
- [กำหนดนโยบายความปลอดภัย]

แนวทางการรักษา ความมั่นคงปลอดภัย ทางไซเบอร์

3. การป้องกันความเสี่ยง (Protect - VA)

- [ตรวจสอบช่องโหว่
(Vulnerability Assessment)]
- [อัปเดต Patch เสมอ]
- ติดตั้ง Firewall / Antivirus

4. การตรวจสอบ ฝ้าระวัง (Detect)

- [ติดตาม Real-time (SOC)]
- [ตรวจพบสิ่งผิดปกติ]
- [แจ้งเตือนภัยคุกคาม]

5. เผชิญเหตุ และฟื้นฟู (Respond & Recover)

- [หยุดยั้งการโจมตี]
- [กู้คืนข้อมูลและระบบ]
- [ถอดบทเรียนหลังเหตุการณ์]



1. ปกป้องข้อมูลส่วนตัว (Data Privacy)

- ชื่อ/ที่อยู่/เบอร์โทร
- รหัสผ่านการเข้าถึง
- พฤติกรรมออนไลน์



2. ป้องกันการโจมตี (Attack Prevention)

- หัวใจหลัก Framework
- ลดความเสี่ยงข้อมูลรั่ว
- ป้องกันบุคคลและองค์กร



3. รับมือเหตุฉุกเฉิน (Incident Response)

- ลดผลกระทบ/ความเสียหาย
- ฟื้นฟูระบบอย่างรวดเร็ว
- ป้องกันไม่ให้เกิดซ้ำ



4. สร้างความเชื่อมั่น (Trust & Confidence)

- รากฐานความปลอดภัย
- เกิดการยอมรับใช้งาน
- ร่วมมือในสังคม/องค์กร

4 เสาหลักป้องกัน ภัยไซเบอร์