สำนักงานพัฒนารัฐบาลดิจิทัล
(องค์การมหาชน)
TDGA
THAILAND DIGITAL GOVERNMENT DEVELOPMENT AGENCY

ความมั่นคงปลอดภัยทางไซเบอร์เบื้องต้น

Basic Cybersecurity Series

แนวทางการรักษาความมั่นคงปลอดภัยทางไซเบอร์ 6 หัวข้อ

1 การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ Risk Assessment

ไม่เสี่ยง | เสี่ยงเล็กน้อย | เสี่ยงปานกลาง | เสี่ยงสูง | เสี่ยงสูงมาก

กระบวนการบริหารความเสี่ยงตามมาตรฐาน COSO ERM

1. กำหนดวัตถุประสงค์
2. ระบุความเสี่ยง
3. ประเมินความเสี่ยง
4. ประเมินมาตรฐานการควบคุม / การจัดการความเสี่ยง
5. รายงานผล
6. การติดตามและทบทวน

2 ความสามารถในการเตรียมตัวและตอบสนองต่อภัยคุกคามทางไซเบอร์ Cyber Resilience

หลัก CIA Security Model

C Confidentiality
การรักษาความลับ
- ป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต
- คุ้มครองข้อมูลให้เป็นความลับ

I Integrity
ความถูกต้องครบด้วน
- ข้อมูลถูกต้อง ไม่ถูกแก้ไขโดยไม่ได้รับอนุญาต
- เชื่อถือได้ น่าเชื่อถือ

A Availability
ความพร้อมใช้
- ระบบและข้อมูลพร้อมใช้งานเสมอ
- เข้าถึงได้เมื่อต้องการใช้งาน

3 กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ Cybersecurity Framework

NIST Cybersecurity Framework ประกอบด้วย 5 ส่วน

1. **Identify** ระบุและทำความเข้าใจความเสี่ยง
2. **Protect** ปกป้องระบบและข้อมูล
3. **Detect** ตรวจจับภัยคุกคามและเหตุผิดปกติ
4. **Respond** ตอบสนองต่อเหตุการณ์
5. **Recover** ฟื้นฟูระบบและบริการ

4 การประเมินช่องโหว่ Vulnerability Assessment

ประโยชน์

- 4.1 ช่วยประเมินความเสี่ยงที่เกิดจากช่องโหว่
- 4.2 ช่วยการสร้างรายงานที่รวบรวมข้อมูลเกี่ยวกับช่องโหว่
- 4.3 ช่วยตรวจสอบว่าระบบสอดคล้องกับมาตรฐาน
- 4.4 ช่วยค้นพบและแก้ไขช่องโหว่และปัญหาความปลอดภัย

5 การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ Detect

วัตถุประสงค์

- ลดความเสียหาย
- ลดโอกาสและระยะเวลาโจมตี
- สามารถให้ข้อมูลที่เป็นประโยชน์กระบวนการตอบสนองต่อเหตุการณ์

เครื่องมือที่ใช้ในการเฝ้าระวัง

ระบบเรวจจับการบุกรุก (IDS)	ระบบป้องกันการบุกรุก (IPS)	ระบบบริหารจัดการข้อมูลความปลอดภัยและเหตุการณ์ (SIEM)	ระบบตรวจจับและตอบสนองปลายทาง (EDR)
IDS	IPS		

6 การเผชิญเหตุภัยคุกคามทางไซเบอร์ Respond และการฟื้นฟูความเสียหายจากภัยคุกคามทางไซเบอร์ Recover

ขั้นตอนการรับมือภัยคุกคามทางไซเบอร์

1. **เตรียมการ** จัดทำแผนการรับมือ / ตั้งที่มตอบสนองต่อเหตุการณ์
2. **ระบุภัยคุกคาม** ตรวจจับเหตุการณ์ ค้นหาความปลอดภัย
3. **การควบคุม** การจัดการเบื้องต่อกับระบบหรือภัย
4. **การกำจัด** เช่น การลบไฟล์ Malware

นางสาวพรสุวรรณ โพธิ์สุวรรณ์ นักทรัพยากรบุคคลปฏิบัติการ
กลุ่มงานจริยธรรม กองการเจ้าหน้าที่
กันยายน 2569