

ความมั่นคงปลอดภัยทางไซเบอร์กับภัยคุกคามทางดิจิทัล

(Cyber Security and Digital Awareness)

หลักการของความมั่นคงปลอดภัยทางไซเบอร์ หรือที่เรียกว่า CIA Triad คือ Confidentiality การรักษาความลับของข้อมูล, Integrity การรักษาความถูกต้องของข้อมูล ไม่มีใครเข้าไปแก้ไขข้อมูลได้ และ Availability ความพร้อมใช้งานของข้อมูล

การรักษาความมั่นคงปลอดภัยทางไซเบอร์ ใช้ 3 คุณสมบัติหลักข้างต้น (CIA Triad) ในกระบวนการนี้ต้องให้ความรู้ เสริมความเข้าใจและมีการบริหารจัดการที่ดีจึงจะสามารถรับมือกับภัยคุกคามต่างๆ ที่เข้ามาได้ ซึ่งไม่ใช่หน้าที่ของใครคนใดคนหนึ่ง นับเป็นหน้าที่ของทุกคนที่จะรักษาความปลอดภัยของข้อมูล ทั้งส่วนตัวและขององค์กร ซึ่งควรมีการช่วยเหลือ ป้องกัน ดูแล เฝ้าระวัง และต้องทำอย่างต่อเนื่อง

เครื่องมือที่นิยมใช้เพื่อบริหารจัดการด้านความมั่นคงปลอดภัยทางไซเบอร์

1. NIST 2.0

- Identity จัดลำดับความสำคัญ เสียหายส่วนไหนส่งผลกับการทำงาน/ให้บริการมากที่สุด
- Protect การป้องกัน ลดความเสี่ยงในด้านต่างๆ ใช้ Password ที่คาดเดายาก
- Detect เฝ้าระวัง มีการตรวจสอบผู้เข้ามาในระบบอย่างเข้มงวด
- Respond ตอบสนอง เตรียมแผนในการรับมือรูปแบบต่างๆ
- Recover วิธีการฟื้นฟูการแก้ปัญหาที่เด็ดขาด
- Govern กลไกควบคุมกำกับดูแล พัฒนานโยบาย กรอบการบริหาร มาตรฐาน เพื่อให้แน่ใจว่ามีการบริหารจัดการไซเบอร์อย่างดี

2. ISO/IEC 27001 คือมาตรฐานสากลสำหรับ ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System: ISMS) ที่ช่วยให้องค์กรประเมินความเสี่ยง ควบคุม และปกป้องข้อมูลสำคัญไม่ให้สูญหาย ถูกโจรกรรม หรือถูกเข้าถึงโดยไม่ได้รับอนุญาต

หมวดการควบคุมหลัก (เวอร์ชัน ISO/IEC 27001:2022) แบ่งมาตรการควบคุมออกเป็น 4 กลุ่มหลัก (รวม 93 มาตรการ):

- **Organizational Controls:** การกำหนดนโยบายความปลอดภัย การจัดสรรบทบาทหน้าที่ และการบริหารจัดการทรัพยากรข้อมูล
- **People Controls:** การคัดกรองบุคลากรก่อนรับเข้าทำงาน และการอบรมสร้างความตระหนักรู้ด้านภัยไซเบอร์
- **Physical Controls:** การควบคุมการเข้า-ออกอาคาร การรักษาความปลอดภัยห้องเซิร์ฟเวอร์ และอุปกรณ์ต่างๆ
- **Technological Controls:** การเข้ารหัสข้อมูล (Encryption), การจัดทำสำรองข้อมูล (Backup) และการตรวจจับภัยคุกคามในระบบ networks

ภัยคุกคามรูปแบบต่างๆ ที่ควรระวัง

1. Malware คือซอฟต์แวร์ที่ไม่ดี ไวรัสต่างๆ
2. Phishing คือ การหลอกลวงส่งข้อความหลอกลวง
3. Ran Somewhere คือเข้าระบบเราเข้าไฟล์เราให้เราใช้งานไม่ได้
4. D dos จำลองเหมือนเป็นผู้ใช้งานมาเข้าเว็บไซต์เดียวกันในเวลาเดียวกันทำให้เว็บไซต์ให้บริการไม่ได้
5. Man in the middle Attack คือการเข้าใช้ wifi ฟรี อาจจะโดนแฮกข้อมูลทำให้ข้อมูลเราถูกโจรกรรมหรือเปลี่ยนแปลงไปจากความจริง
6. Zero Day Attack คือมาโจมตีโดยอาศัยช่องโหว่ที่เรายังไม่สามารถป้องกันได้
7. Social Engineer หรือวิศวกรรมทางสังคม ไม่ได้โจมตีที่ฮาร์ดแวร์หรือซอฟต์แวร์แต่โจมตีที่ผู้ใช้งาน ทั้งจากการตั้งใจโจรกรรมข้อมูลหรือจากการกดที่ผิดพลาดไปปามัลแวร์เข้ามาในระบบ ทำให้เกิดความเสียหายในหลายระบบ

สรุปเนื้อหาโดย

นางวิมลภัทร์ งามจรัสวานิชย์

นักสำรวจดินชำนาญการพิเศษ

กลุ่มวางแผนการใช้ที่ดิน สำนักงานพัฒนาที่ดินเขต 3



สำนักงานคณะกรรมการข้าราชการพลเรือน
ขอมอบประกาศนียบัตรฉบับนี้ให้เพื่อแสดงว่า

นางวิมลภัทร จามจรัสวานิชย์

ได้ผ่านการพัฒนาทางไกลด้วยระบบอิเล็กทรอนิกส์

วิชา ความมั่นคงปลอดภัยทางไซเบอร์กับภัยคุกคามทางดิจิทัล
[Cyber Security and Digital Awareness]

[รวมระยะเวลาทั้งสิ้น 3 ชั่วโมง]
ให้ไว้ ณ วันที่ 19 สิงหาคม พ.ศ. 2569

(นายปิยวัฒน์ ศิวรักษ์)
เลขาธิการคณะกรรมการข้าราชการพลเรือน

