ความมั่นคงปลอดภัยไซเบอร์พื้นฐาน

ความรู้เกี่ยวกับการรักษาความปลอดภัยระบบสารสนเทศขององค์กรและกฎหมายที่เกี่ยวข้องในหน่วยงานภาครัฐ

ความปลอดภัยไซเบอร์ หมายถึง การปกป้องระบบเครือข่าย คอมพิวเตอร์ โปรแกรม และข้อมูลจากการโจมตี การเข้าถึงโดยไม่ได้รับอนุญาต ความเสียหาย หรือการรบกวนการทำงาน โดยมีเป้าหมายเพื่อให้ระบบสารสนเทศมีความ มั่นคงปลอดภัย และสามารถใช้งานได้อย่างต่อเนื่อง

หลักสำคัญของความปลอดภัยไซเบอร์มักอิงตามหลัก CIA Triad ประกอบด้วย

1.) Confidentiality (ความลับของข้อมูล)

2.) Integrity (ความถูกต้องครบถ้วนของข้อมูล)

3.) Availability (ความพร้อมใช้งานของระบบ)

มาตราสำคัญพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA)

มาตรา 3 – คำนิยามที่สำคัญ

กำหนดนิยามของคำว่า “ข้อมูลส่วนบุคคล”, “เจ้าของข้อมูล”, “ผู้ควบคุมข้อมูล”, และ “ผู้ประมวลผลข้อมูล” ข้อมูลส่วนบุคคล หมายถึง ข้อมูลเกี่ยวกับบุคคลที่สามารถระบุตัวตนได้โดยตรงหรือโดยอ้อ

มาตรา 19 – การขอความยินยอม

ผู้ควบคุมข้อมูลต้องขอ ความยินยอมอย่างชัดเจน จากเจ้าของข้อมูล ก่อนเก็บ ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ห้ามใช้ความยินยอมที่คลุมเครือ หรือมีการบังคับ

มาตรา 26 – ข้อมูลอ่อนไหว

- ข้อมูลที่ต้องได้รับการคุ้มครองเป็นพิเศษ เช่น เชื้อชาติ ศาสนา ความคิดเห็นทางการเมือง ข้อมูลสุขภาพ พฤติกรรมทางเพศ ฯลฯ ต้องได้รับ ความยินยอมเป็นลายลักษณ์อักษร และมีเหตุอันสมควรในการประมวลผล

DMR

มาตรา 27 – การเก็บข้อมูลต้องมีวัตถุประสงค์

- ห้ามเก็บข้อมูลเกินความจำเป็น และต้องแจ้งวัตถุประสงค์อย่างชัดเจน
- ใช้ข้อมูลได้เฉพาะตามวัตถุประสงค์ที่แจ้งไว้เท่านั้น

มาตรา 28-29 – สิทธิของเจ้าของข้อมูล

<u>เจ้าของข้อมูลมีสิทธิ</u>

- ขอเข้าถึงข้อมูล
- ขอให้แก้ไขข้อมูล
- ถอนความยินยอม
- ขอให้ลบข้อมูล
- ขอระงับการใช้ข้อมูล

มาตรา 37 – หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคล

- ต้องรักษาความมั่นคงปลอดภัยของข้อมูล
- ต้องแจ้งเหตุละเมิดข้อมูลภายใน 72 ชั่วโมง
- ต้องแต่งตั้งเจ้าหน้าที่คุ้มครองข้อมูล (DPO) หากเข้าข่ายตามที่กำหนด

มาตรา 72 – โทษทางอาญา

การเปิดเผยข้อมูลส่วนบุคคลโดยมิชอบ อาจมีโทษ จำคุกไม่เกิน 1 ปี หรือปรับไม่เกิน 1 ล้านบาท หรือทั้งจำทั้งปรับ

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

1.) เป็นกฎหมายเพื่อ ป้องกันและรับมือภัยคุกคามไซเบอร์ ที่อาจกระทบต่อความมั่นคงของประเทศ

2.) เน้นคุ้มครอง โครงสร้างพื้นฐานสำคัญทางสารสนเทศ เช่น พลังงาน การเงิน โทรคมนาคม ฯลฯ

3.) ตั้งหน่วยงานหลัก กมช (คณะกรรมการฯ) กำหนดนโยบาย และ สำนักงานไซเบอร์แห่งชาติ (สศก.) ปฏิบัติงานและประสานงาน

4.) ให้อำนาจเจ้าหน้าที่ในการ ตรวจสอบ เข้าถึงข้อมูล หรือระบบคอมพิวเตอร์ (กรณีจำเป็น)

5.) หน่วยงานรัฐ เอกชนต้อง รายงานเหตุไซเบอร์ และมี แผนป้องกันความเสี่ยง

6.) โทษ: ผู้ไม่ปฏิบัติตามคำสั่งอาจถูกปรับ หรือดำเนินคดีตามกฎหมาย

ความรู้เบื้องต้น ในแนวความคิด Zero Trust

Zero Trust คือแนวคิดด้านความปลอดภัยไซเบอร์ที่ว่า "ไม่เชื่อถือใครโดยอัตโนมัติ ไม่ว่าจะอยู่ใน หรืออยู่นอกระบบ“ ทุกการเข้าถึงต้อง ยืนยันตัวตน ตรวจสอบสิทธิ์ และจำกัดการเข้าถึงการเชื่อมโยงข้อมูล

DMR

แนวปฏิบัติจริงของ Zero Trust สำหรับการประยุกต์ใช้ในองค์กร

1.) ยืนยันตัวตนอย่างเข้มงวด (Strong Authentication)

- ใช้ระบบ Multi-Factor Authentication (MFA) กับผู้ใช้ทุกคน
- ควบคุมการเข้าสู่ระบบด้วย Single Sign-On (SSO) ที่ปลอดภัย

2.) จำกัดสิทธิ์การเข้าถึง (Least Privilege Access)

- ให้สิทธิ์การเข้าถึงเฉพาะข้อมูล/ระบบที่จำเป็นต่อหน้าที่
- ใช้ Role-Based Access Control (RBAC) หรือ Policy-Based Access

3.) แบ่งโซนเครือข่าย (Network Segmentation)

- แยกระบบสำคัญออกจากกันเพื่อลดความเสียหายหากถูกเจาะ
- ใช้ Firewall หรือ Zero Trust Network Architecture (ZTNA)

4.) ตรวจสอบและติดตามแบบเรียลไทม์ (Continuous Monitoring)

- ใช้ระบบ SIEM, EDR หรือ XDR เพื่อตรวจจับพฤติกรรมผิดปกติ
- บันทึก log และวิเคราะห์เหตุการณ์อย่างต่อเนื่อง

5.) ควบคุมอุปกรณ์และปลายทาง (Endpoint Security)

- ตรวจสอบความปลอดภัยของอุปกรณ์ก่อนอนุญาตให้เชื่อมต่อ
- ใช้ระบบ Mobile Device Management (MDM)

6.) ตรวจสอบแอปและข้อมูล (Application & Data Security)

- จำกัดการเข้าถึงข้อมูลสำคัญ เช่น การเข้ารหัสไฟล์
- ควบคุมการใช้งานแอปพลิเคชันโดยนโยบาย Zero Trust

7.) ทบทวนและอัปเดตนโยบายความปลอดภัยเป็นประจำ

- ตรวจสอบบัญชีผู้ใช้ที่ไม่ได้ใช้งาน

- ปรับปรุงสิทธิ์และนโยบายตามโครงสร้างองค์กรที่เปลี่ยนแปลง

ประโยชน์และความสำคัญของการใช้แนวคิด Zero Trust

ความสำคัญ

- เพราะภัยคุกคามไซเบอร์มีความซับซ้อนมากขึ้น
- การทำงานแบบ Remote / Cloud / Mobile เพิ่มความเสี่ยง
- ระบบเดิมที่ "ไว้ใจภายในองค์กร" ไม่เพียงพออีกต่อไป

จึงต้องใช้แนวคิด “ไม่ไว้ใจใครโดยอัตโนมัติ” เพื่อป้องกันตั้งแต่ต้นทาง

ประโยชน์ของ Zero Trust

1.) ลดความเสี่ยงจากการถูกเจาะระบบ (Breach)

- ทุกการเข้าถึงต้องผ่านการตรวจสอบอย่างเข้มงวด

2.) จำกัดผลกระทบเมื่อระบบถูกโจมตี

- ผู้โจมตีไม่สามารถเคลื่อนย้ายภายในเครือข่ายได้ง่าย

3.) ปกป้องข้อมูลสำคัญได้ดีขึ้น

- ด้วยการควบคุมการเข้าถึงและการเข้ารหัสข้อมูล

4.) เพิ่มความมั่นใจด้านความปลอดภัย

- ทั้งสำหรับองค์กรเองและผู้มีส่วนได้ส่วนเสีย (ลูกค้า/พาร์ตเนอร์)

5.) สอดคล้องกับกฎหมายและมาตรฐานสากล

- เช่น PDPA, ISO/IEC 27001, NIST

รูปแบบภัยคุกคามไซเบอร์ (cyber security awareness) และตัวอย่างการโจมตีประเภทต่างๆ

1.) **Phishing** (ฟิชชิง) การหลอกให้คลิกลิงก์ หรือกรอกข้อมูลผ่านอีเมล/เว็บไซต์ปลอม เช่น อีเมลปลอมจากธนาคาร/หน่วยงาน

2.) **Malware** (มัลแวร์) โปรแกรมแฝงตัว เช่น ไวรัส โทรจัน สปายแวร์

อันตราย: ทำลายข้อมูล ดักจับรหัสผ่าน

3.) **Ransomware** (แรนซัมแวร์) มัลแวร์ที่ล็อกไฟล์เรียกค่าไถ่

อันตราย: ข้อมูลถูกเข้ารหัส ต้องจ่ายเงินเพื่อปลดล็อก

4.) **Social Engineering** (วิศวกรรมสังคม) การหลอกลวงทางจิตวิทยาให้เปิดเผยข้อมูลหรือรหัส เช่น แอบอ้างเป็น IT/ผู้บริหาร โทรมาขอรหัส

5.) Password Attack (เจาะรหัสผ่าน) การเดารหัสผ่าน หรือใช้เครื่องมือถอดรหัส

แนวทางป้องกัน: ตั้งรหัสให้รัดกุมและไม่ซ้ำกัน

6.) Insider Threat (ภัยจากคนใน) พนักงาน/ผู้เกี่ยวข้องที่มีสิทธิ์เข้าถึงข้อมูล ใช้ข้อมูลผิดวัตถุประสงค์

อันตราย: ข้อมูลรั่วไหลจากภายใน

7.) DDoS Attack การยิงข้อมูลจำนวนมากใส่ระบบเพื่อให้ระบบล่ม

ผลกระทบ: บริการใช้งานไม่ได้ชั่วคราว

DMR

ข้อควรปฏิบัติสำหรับบุคลากร

1.) อย่าคลิกลิงก์หรือเปิดไฟล์แนบที่ไม่น่าเชื่อถือ

2.) ใช้รหัสผ่านที่รัดกุม และเปิดใช้ 2FA (Two-Factor Authentication)

การรักษาความปลอดภัยของเครื่องคอมพิวเตอร์ส่วนบุคคล

แนวปฏิบัติพื้นฐานเพื่อความปลอดภัย

1.) ติดตั้งโปรแกรมแอนติไวรัส (Antivirus)

- เพื่อป้องกันมัลแวร์ ไวรัส และภัยคุกคามต่าง ๆ

2.) อัปเดตระบบปฏิบัติการและซอฟต์แวร์สม่ำเสมอ

- เพื่อปิดช่องโหว่ด้านความปลอดภัย

3.) ตั้งรหัสผ่านให้รัดกุม

- ควรใช้รหัสผ่านที่เดายาก และไม่ใช้ซ้ำในหลายบัญชี

การรักษาความปลอดภัยของเครื่องคอมพิวเตอร์ส่วนบุคคล

แนวปฏิบัติพื้นฐานเพื่อความปลอดภัย

4.) เปิดใช้งาน Firewall

- เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต

5.) ระวังการใช้งานอินเทอร์เน็ต

- หลีกเลี่ยงการคลิกลิงก์แปลก ๆ หรือดาวน์โหลดจากแหล่งที่ไม่น่าเชื่อถือ

6.) สำรองข้อมูล (Backup) อย่างสม่ำเสมอ

- เพื่อป้องกันข้อมูลสูญหายจากมัลแวร์หรือฮาร์ดแวร์เสีย

การรักษาความปลอดภัยของเครื่องคอมพิวเตอร์ส่วนบุคคล

แนวปฏิบัติพื้นฐานเพื่อความปลอดภัย

7.) ล็อกหน้าจอเมื่อไม่ใช้งาน

- เพื่อป้องกันผู้อื่นเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

8.) หลีกเลี่ยงการใช้ Wi-Fi สาธารณะโดยไม่เข้ารหัส VPN

- ป้องกันการดักจับข้อมูลระหว่างทาง

สรุป : "การรักษาความปลอดภัยคอมพิวเตอร์ส่วนบุคคล คือด่านแรกในการปกป้องข้อมูลของคุณ และองค์กร"

การรักษาความปลอดภัยของโทรศัพท์มือถือ แนวปฏิบัติพื้นฐานเพื่อความปลอดภัย

1.) ตั้งรหัสผ่านหรือระบบยืนยันตัวตน

- เช่น PIN, ลายนิ้วมือ, Face ID เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

2.) อัปเดตระบบปฏิบัติการและแอปพลิเคชันเสมอ

- เพื่อปิดช่องโหว่ที่อาจถูกใช้โจมตี

3.) หลีกเลี่ยงการติดตั้งแอปจากแหล่งไม่ปลอดภัย

- ดาวน์โหลดจาก App Store หรือ Play Store เท่านั้น

การรักษาความปลอดภัยของโทรศัพท์มือถือ แนวปฏิบัติพื้นฐานเพื่อความปลอดภัย

4.) ระมัดระวังการคลิกลิงก์ เปิดไฟล์แนบ

- ป้องกันฟิชชิงหรือมัลแวร์แฝง

5.) เปิดใช้การเข้ารหัสข้อมูล (Encryption)

- เพื่อป้องกันการอ่านข้อมูลเมื่อเครื่องถูกขโมย

6.) ติดตั้งแอปความปลอดภัยหรือแอนติไวรัส

- เพื่อตรวจจับพฤติกรรมหรือแอปต้องสงสัย

การรักษาความปลอดภัยของโทรศัพท์มือถือ แนวปฏิบัติพื้นฐานเพื่อความปลอดภัย

7.) สำรองข้อมูลเป็นประจำ

- ป้องกันข้อมูลสูญหายจากเหตุฉุกเฉิน

8.) ไม่ใช้ Wi-Fi สาธารณะโดยไม่เข้ารหัส VPN

- ลดความเสี่ยงถูกดักจับข้อมูล

สรุป : มือถือเป็นเหมือนคอมพิวเตอร์พกพา - ต้องดูแลให้ปลอดภัยไม่แพ้อุปกรณ์อื่น ๆ

การรักษาความปลอดภัยของอินเทอร์เน็ต

แนวปฏิบัติพื้นฐานเพื่อความปลอดภัย

1.) ใช้รหัสผ่านที่รัดกุม

- ผสมตัวอักษร ตัวเลข และสัญลักษณ์
- หลีกเลี่ยงการใช้รหัสเดียวกันทุกเว็บไซต์

2.) ไม่คลิกลิงก์แปลกปลอม

- โดยเฉพาะลิงก์ในอีเมล ข้อความ หรือโฆษณาที่ไม่น่าเชื่อถือ

3.) ติดตั้งโปรแกรมแอนติไวรัส/Firewall

- ช่วยป้องกันมัลแวร์ที่มาทางเว็บ

การรักษาความปลอดภัยของอินเทอร์เน็ต

แนวปฏิบัติพื้นฐานเพื่อความปลอดภัย

4.) เปิดใช้งาน HTTPS เมื่อเข้าชมเว็บไซต์

- เว็บไซต์ที่ปลอดภัยควรขึ้นต้นด้วย “https://”

5.) อัปเดตซอฟต์แวร์และเบราว์เซอร์เป็นประจำ

- ลดช่องโหว่ที่อาจถูกใช้โจมตีผ่านอินเทอร์เน็ต

6.) ระวังการใช้ Wi-Fi สาธารณะ

- หลีกเลี่ยงการทำธุรกรรมสำคัญ หากไม่ใช้ VPN

การรักษาความปลอดภัยของอินเทอร์เน็ต

แนวปฏิบัติพื้นฐานเพื่อความปลอดภัย

7.) ไม่แชร์ข้อมูลส่วนตัวผ่านเว็บไซต์ไม่ปลอดภัย

- เช่น หมายเลขบัตรประชาชน, บัญชีธนาคาร ฯลฯ

8.) ใช้การยืนยันตัวตนแบบ 2 ชั้น (2FA)

- เพิ่มความปลอดภัยเมื่อเข้าสู่ระบบออนไลน์

สรุป : ใช้อินเทอร์เน็ตอย่างรู้เท่าทัน = ลดความเสี่ยงจากภัยไซเบอร์

DMR

กรมทรัพยากรธรณี