การควบคุมความปลอดภัย สารสนเทศ ที่สำคัญ ของ CIS

เวอร์ชั่น 8.1

แปล โดย ศิริลักษณ์ สิทธิ์สกนธ์กุล

16 ธันวาคม 2567

ขอขอบคุณ

CIS ขอขอบคุณผู้เชี่ยวชาญด้านความปลอดภัยจำนวนมากที่อาสา สละเวลาและความสามารถของพวกเขาเพื่อสนับสนุน **CIS Critical Security Controls® (CIS Controls®)** และงานอื่น ๆ ของ CIS ผลิตภัณฑ์ของ CIS เกิดจากความร่วมมือของอาสาสมัครที่เปรียบเสมือนกองทัพจากทั่วทั้งอุตสาหกรรม โดยพวกเขาได้สละเวลาและความสามารถของตนอย่างใจกว้างเพื่อสร้างประสบการณ์ออนไลน์ที่ปลอดภัยยิ่งขึ้นสำหรับทุกคน.

การอนุญาตภายใต้ใบอนุญาต Creative Commons (Creative Commons License)

Contents

Overview

บทนำ

CIS Critical Security Controls® (CIS Controls®) เป็นแนวทางการปฏิบัติที่เป็นประโยชน์และสร้างสรรค์สำหรับผู้ป้องกันภัย จากนั้นจึงแบ่งปันข้อมูลเหล่านั้นให้กับกลุ่มผู้รับที่กว้างขึ้น โดยเริ่มต้นจากกิจกรรมเล็กๆ ที่เกิดขึ้นจากความร่วมมือในชุมชนเพื่อระบุการโจมตีทางไซเบอร์ที่พบได้บ่อยและสำคัญที่สุดซึ่งส่งผลกระทบต่อองค์กรในทุกๆ วัน และนำความรู้และประสบการณ์เหล่านั้นมาแปลง

เป้าหมายดั้งเดิมนั้นเรียบง่าย—เพื่อช่วยให้ผู้คนและองค์กรมุ่งเน้นความสนใจไปที่ขั้นตอนที่สำคัญที่สุดในการป้องกันตนเองจากการโจมตีที่มีความสำคัญและส่งผลกระทบโดยตรง.

นำโดยศูนย์ความปลอดภัยทางอินเทอร์เน็ต (Led by the Center for Internet Security® - CIS®)

CIS Controls ได้พัฒนาไปเป็นชุมชนระดับนานาชาติที่ประกอบด้วยอาสาสมัครทั้งในระดับบุคคลและสถาบัน โดยมีเป้าหมายสำคัญดังนี้:

- **แบ่งปันข้อมูลเชิงลึกเกี่ยวกับการโจมตีและผู้โจมตี:** ระบุสาเหตุที่แท้จริง และแปลงข้อมูลเหล่านั้นเป็นชุดของการป้องกันที่มีประสิทธิภาพ
- **สร้างและแบ่งปันเครื่องมือและแนวทางการทำงาน:** รวมถึงเรื่องราวเกี่ยวกับการนำไปใช้และการแก้ปัญหา
- **เชื่อมโยง CIS Controls กับกรอบงานด้านกฎระเบียบและการปฏิบัติตามข้อกำหนด:** เพื่อสร้างความสอดคล้องและนำไปสู่การจัดลำดับความสำคัญและความมุ่งเน้นร่วมกัน
- **ระบุปัญหาและอุปสรรคที่พบบ่อย:** เช่น การประเมินเริ่มต้นและการจัดทำแผนการดำเนินงาน พร้อมแก้ไขปัญหาเหล่านั้นในฐานะชุมชน

CIS Controls สะท้อนถึงความรู้รวมกันของผู้เชี่ยวชาญจากทุกส่วนของระบบนิเวศ (เช่น บริษัท รัฐบาล บุคคลทั่วไป) ที่มีบทบาทหลากหลาย (ผู้ตอบสนองต่อภัยคุกคาม นักวิเคราะห์ เทคโนโลยี ผู้ปฏิบัติงานด้าน IT ผู้ป้องกัน ผู้ค้นหาช่องโหว่ ผู้สร้างเครื่องมือ ผู้ให้บริการโซลูชัน ผู้ใช้งาน ผู้กำหนดนโยบาย ผู้ตรวจสอบ เป็นต้น) และครอบคลุมหลายภาคส่วน (เช่น รัฐบาล พลังงาน การป้องกันการโจมตี การเงิน การขนส่ง การศึกษา ที่ปรึกษา ความปลอดภัย IT เป็นต้น)

ทุกฝ่ายได้ร่วมมือกันเพื่อสร้าง นำไปใช้ และสนับสนุนการดำเนินงานของ **CIS Controls** อย่างต่อเนื่อง.

วิวัฒนาการของ CIS Controls (Evolution of the CIS Controls)

CIS Controls เริ่มต้นในลักษณะเดียวกับกิจกรรมอื่นๆ ที่คล้ายกัน โดยการรวมตัวของผู้เชี่ยวชาญเพื่อแลกเปลี่ยนความคิดเห็นและอภิปรายจนกว่าจะได้ข้อสรุปที่ทุกฝ่ายเห็นพ้องกัน กระบวนการนี้มีคุณค่าอย่างมาก ขึ้นอยู่กับคุณภาพของผู้เชี่ยวชาญที่มีส่วนร่วมและประสบการณ์ของพวกเขา

การจัดทำเอกสารและแบ่งปันผลลัพธ์ช่วยให้องค์กรต่างๆ ได้ประโยชน์จากความเชี่ยวชาญของผู้ที่พวกเขาไม่สามารถว่าจ้างหรือเข้าถึงได้ คุณสามารถปรับปรุงผลลัพธ์ (และเพิ่มความมั่นใจในผลลัพธ์) ได้โดยการเลือกผู้เชี่ยวชาญที่ครอบคลุมหลากหลายความรู้ นำกระบวนการที่สอดคล้องมาใช้ และใช้ข้อมูลที่ดีที่สุดเท่าที่จะหาได้ (โดยเฉพาะข้อมูลเกี่ยวกับการโจมตี) สุดท้ายแล้ว ผลลัพธ์จะขึ้นอยู่กับการตัดสินใจของกลุ่มผู้เชี่ยวชาญกลุ่มเล็กๆ ที่ได้รับการบันทึกไว้ในลักษณะที่ไม่เป็นทางการ

CIS Controls เวอร์ชัน 8.1 (CIS Controls v8.1)

ที่ CIS เราได้ใช้เวลาหลายปีในการปรับปรุงกระบวนการแนะนำแนวปฏิบัติที่ดีที่สุด (CIS Benchmarks™ และ CIS Controls) โดยมุ่งเน้นความเข้มงวด ความโปร่งใส และการใช้ข้อมูลที่เป็นพื้นฐานสำหรับวิทยาศาสตร์ด้านการป้องกันไซเบอร์

ในเวอร์ชันเริ่มแรกของ CIS Controls เราใช้รายการการโจมตีที่เป็นที่รู้จักทั่วไปเป็นตัวทดสอบอย่างง่ายเพื่อวัดประโยชน์ของคำแนะนำเฉพาะ ตั้งแต่ปี 2013 เป็นต้นมา เราได้ทำงานร่วมกับทีมรายงาน **Verizon Data Breach Investigations Report (DBIR)** เพื่อนำผลการวิเคราะห์ข้อมูลขนาดใหญ่ของพวกเขามาจับคู่กับ CIS Controls เพื่อสร้างโปรแกรมการปรับปรุงการป้องกันที่ได้มาตรฐาน

ล่าสุด **CIS** ได้เปิดตัว **Community Defense Model (CDM)** ซึ่งเป็นแนวทางที่ใช้ข้อมูลมากที่สุดของเรา ในเวอร์ชันเริ่มแรก CDM ใช้ข้อสรุปจาก DBIR ล่าสุด รวมกับข้อมูลจาก **Multi-State Information Sharing and Analysis Center® (MS-ISAC®)** เพื่อระบุประเภทการโจมตีที่สำคัญที่สุด 5 ประเภท

CDM และความสัมพันธ์กับ MITRE ATT&CK® Framework

CDM อธิบายการโจมตีเหล่านี้โดยใช้ **MITRE Adversarial Tactics, Techniques, and Common Knowledge® (MITRE ATT&CK®) Framework** เพื่อสร้างรูปแบบการโจมตี (หรือการรวมกันของกลยุทธ์และเทคนิคที่ใช้ในการโจมตี) วิธีนี้ช่วยให้เราวิเคราะห์คุณค่าของการดำเนินการป้องกัน (Safeguards) แต่ละรายการได้

ผลลัพธ์:

- ให้มุมมองที่สอดคล้องและอธิบายได้เกี่ยวกับคุณค่าความปลอดภัยของการป้องกันในทุกช่วงชีวิตของผู้โจมตี

- เป็นรากฐานสำหรับกลยุทธ์การป้องกันเชิงลึก (Defense-in-Depth)

รายละเอียดการวิเคราะห์นี้มีอยู่บนเว็บไซต์ของ CIS (https://www.cisecurity.org/controls/v8-1/)

แนวปฏิบัติด้านความปลอดภัยของ CIS (CIS Security Best Practices): CIS Controls และ CIS Benchmarks ไม่ใช่แค่รายการ "สิ่งที่ควรทำ" หรือ "สิ่งที่อาจช่วยได้" แต่เป็นชุดการดำเนินการที่ได้รับการจัดลำดับความสำคัญ และเน้นย้ำให้ใช้งานได้จริง มีเครือข่ายสนับสนุนจากชุมชนที่ช่วยให้สามารถนำไปใช้ได้ง่าย มีความสามารถในการขยายขอบเขต และสอดคล้องกับข้อกำหนดด้านความปลอดภัยของอุตสาหกรรมหรือรัฐบาลทั้งหมด.

เวอร์ชันนี้ของ CIS Controls

CIS Controls เวอร์ชัน 8.1 (v8.1) เป็นการปรับปรุงต่อเนื่องจากเวอร์ชัน 8.0 โดยในกระบวนการพัฒนา CIS Controls เราได้กำหนด **"หลักการออกแบบ" (Design Principles)** เพื่อเป็นแนวทางสำหรับการปรับปรุงทั้งเล็กและใหญ่ในเอกสาร หลักการออกแบบในเวอร์ชันนี้ประกอบด้วย **บริบท (Context)**, **ความชัดเจน (Clarity)**, และ **ความสม่ำเสมอ (Consistency)**

หลักการออกแบบสำหรับการปรับปรุงนี้:

บริบท (Context): ขยายขอบเขตและการประยุกต์ใช้ มาตรการป้องกัน ในทางปฏิบัติด้วยการเพิ่มตัวอย่างเฉพาะเจาะจงและคำอธิบายเพิ่มเติม เราได้อัปเดต CIS Controls ให้ครอบคลุม **ประเภททรัพย์สินใหม่ (Asset Classes)** เพื่อให้สอดคล้องกับโครงสร้างพื้นฐานขององค์กรในแต่ละส่วน นอกจากนี้ยังเพิ่มคำอธิบาย มาตรการป้องกัน บางรายการเพื่อให้ใช้งานได้จริงและชัดเจนยิ่งขึ้น

การอยู่ร่วมกัน (Coexistence): CIS Controls มีความสอดคล้องกับมาตรฐานและกรอบงานอุตสาหกรรมที่พัฒนาอย่างต่อเนื่อง และจะยังคงดำเนินการในลักษณะนี้ต่อไป เพื่อช่วยผู้ใช้งานทุกคนให้สามารถใช้งาน Controls ได้อย่างสะดวก การเผยแพร่ **NIST CSF 2.0** จำเป็นต้องมีการอัปเดตการจับคู่ฟังก์ชันความปลอดภัยและการปรับปรุงฟังก์ชันใหม่ๆ

ความสม่ำเสมอ (Consistency): ในการอัปเดตที่ต่อเนื่อง CIS Controls จะลดผลกระทบต่อผู้ใช้งานให้น้อยที่สุด ไม่มีการเปลี่ยนแปลง **กลุ่มการดำเนินการ (Implementation Groups)** ในการอัปเดตนี้ และจิตวิญญาณของ มาตรการป้องกันในแต่ละรายการยังคงเดิม นอกจากนี้ เราได้ปรับให้ประเภททรัพย์สินใหม่และคำจำกัดความมีความสอดคล้องทั่วทั้ง Controls และเพิ่มการอัปเดตเล็กน้อยในบางจุด

การอัปเดตสำคัญใน CIS Controls เวอร์ชัน 8.1:

- ปรับการจับคู่ฟังก์ชันความปลอดภัยของ **NIST CSF** ให้ตรงกับเวอร์ชัน **NIST CSF 2.0**

- เพิ่มและขยายคำจำกัดความในพจนานุกรมสำหรับคำที่ใช้งานใน Controls (เช่น **แผน (Plan)**, **กระบวนการ (Process)**, **ข้อมูลสำคัญ (Sensitive Data)**)
- ปรับปรุงประเภททรัพย์สิน (Asset Classes) และเพิ่มการจับคู่ใหม่สำหรับมาตรการป้องกัน
- แก้ไขข้อผิดพลาดเล็กน้อยในคำอธิบาย มาตรการป้องกัน
- เพิ่มคำชี้แจงให้ มาตรการป้องกัน ที่คำอธิบายเดิมอาจไม่ชัดเจน

การปรับปรุงสำคัญใน CIS Controls เวอร์ชัน 8.1

หนึ่งในการปรับปรุงสำคัญของการจับคู่ใน **CIS Controls v8.1** คือการเพิ่มฟังก์ชันความปลอดภัยด้าน **"การกำกับดูแล" (Governance)** ซึ่งเป็นโครงสร้างสำคัญที่ช่วยให้โปรแกรมความปลอดภัยทางไซเบอร์สามารถดำเนินไปสู่การบรรลุเป้าหมายขององค์กรได้

จุดเด่นของการปรับปรุงด้าน Governance:

- **ครอบคลุมและเฉพาะเจาะจง:** CIS Controls ถูกออกแบบให้ครอบคลุมพอที่จะปกป้องและสนับสนุนโปรแกรมความปลอดภัยทางไซเบอร์ในองค์กรทุกขนาด พร้อมทั้งมีความชัดเจนเพียงพอเพื่อให้การดำเนินการง่ายขึ้น
- ในเวอร์ชัน 8.1 หัวข้อด้านการกำกับดูแลได้รับการระบุอย่างชัดเจนว่าเป็นคำแนะนำที่สามารถนำไปปฏิบัติ เพื่อเสริมสร้างการกำกับดูแลในโปรแกรมความปลอดภัยทางไซเบอร์
- ช่วยให้ผู้ใช้งานสามารถระบุ ส่วนประกอบที่เกี่ยวข้องกับการกำกับดูแลในโปรแกรมได้ดียิ่งขึ้น และมอบหลักฐานที่จำเป็นสำหรับการแสดงความสอดคล้องกับข้อกำหนดต่างๆ

วัตถุประสงค์ของ CIS Controls:

- ออกแบบเพื่อช่วยให้องค์กรสามารถวางแผน ดำเนินการ วัดผล และจัดการความปลอดภัยได้อย่างเป็นระบบ
- ลดความซับซ้อนของภาษาเพื่อลดการซ้ำซ้อน
- เน้นที่การดำเนินการที่วัดผลได้ พร้อมเมตริกที่กำหนดไว้อย่างชัดเจน
- ทำให้ มาตรการป้องกัน มีความชัดเจนและกระชับ

CIS ยังคงสร้างสมดุลระหว่างการตอบสนองต่อความท้าทายด้านความปลอดภัยทางไซเบอร์ในปัจจุบันและการรักษากลยุทธ์ป้องกันที่มั่นคง โดยหลีกเลี่ยงการพึ่งพาเทคโนโลยีที่ซับซ้อนหรือเข้าถึงได้ยาก

การปรับตัวต่อการเปลี่ยนแปลงทางเทคโนโลยี:

- ทีมงาน CIS Controls ตระหนักถึงการพัฒนาของเทคโนโลยี เช่น **ปัญญาประดิษฐ์ (Artificial Intelligence)**, **ความจริงเสริม (Augmented Reality)**, และ **การประมวลผลรอบตัว (Ambient Computing)** ที่กำลังเปลี่ยนแปลงโครงสร้างพื้นฐานขององค์กรทั้งในแบบละเอียดอ่อนและแบบปฏิวัติ
- ขณะนี้ทีมงานกำลังพัฒนาแนวคิดสำหรับ **CIS Controls เวอร์ชัน 9** เพื่อเตรียมพร้อมสำหรับอนาคต

ระบบนิเวศของ CIS Controls (“ไม่ได้เป็นเพียงรายการเท่านั้น”)

ไม่ว่าคุณจะใช้ **CIS Controls** หรือวิธีการอื่นในการนำทางโปรแกรมปรับปรุงความปลอดภัยของคุณ สิ่งสำคัญที่ต้องตระหนักคือ **"ไม่ได้เป็นเพียงรายการ"** คุณสามารถหา "รายการ" คำแนะนำด้านความปลอดภัยที่น่าเชื่อถือจากแหล่งข้อมูลต่างๆ ได้มากมาย แต่ควรมองว่ารายการเหล่านั้นเป็นเพียงจุดเริ่มต้น สิ่งที่สำคัญยิ่งกว่าคือการมองหา **ระบบนิเวศที่เกิดขึ้นรอบๆ รายการ**

คำถามสำคัญที่ควรพิจารณา:

- ฉันจะหา **การฝึกอบรม** ข้อมูลเสริม หรือคำอธิบายได้จากที่ไหน?
- องค์กรอื่นได้นำคำแนะนำเหล่านี้ไปใช้และใช้งานอย่างไร?
- มีตลาดสำหรับเครื่องมือและบริการจากผู้ให้บริการหรือไม่?
- ฉันจะวัดความก้าวหน้า หรือระดับความสมบูรณ์ได้อย่างไร?
- สิ่งนี้สอดคล้องกับกรอบงานและข้อกำหนดด้านกฎระเบียบต่างๆ อย่างไร?

พลังที่แท้จริงของ CIS Controls:

ไม่ได้อยู่ที่การสร้าง "รายการที่ดีที่สุด" แต่คือการดึงประสบการณ์ของชุมชนทั้งในระดับบุคคลและองค์กร เพื่อปรับปรุงความปลอดภัยผ่านการแบ่งปันแนวคิด เครื่องมือ บทเรียน และการดำเนินการร่วมกัน

บทบาทของ CIS:

CIS ทำหน้าที่เป็นตัวกระตุ้นและศูนย์กลางข้อมูลเพื่อช่วยให้ทุกคนเรียนรู้จากกันและกัน ตั้งแต่เวอร์ชัน 6 มีการพัฒนาข้อมูลเสริม ผลิตภัณฑ์ และบริการที่เกี่ยวข้องจาก CIS และในอุตสาหกรรมโดยรวมอย่างมหาศาล

การสนับสนุนจาก CIS:

คุณสามารถติดต่อ controlsinfo@cisecurity.org เพื่อขอข้อมูลและเอกสารสนับสนุนต่างๆ ได้แก่:

- **การจับคู่ระหว่าง CIS Controls กับกรอบงานการบริหารความเสี่ยง** เช่น NIST®, Federal Information Security Modernization Act (FISMA), International Organization for Standardization (ISO) เป็นต้น
- **กรณีศึกษา** เกี่ยวกับการนำไปใช้ในองค์กร
- **รายการอ้างอิงที่เกี่ยวข้องกับ CIS Controls** ในมาตรฐานระดับชาติและนานาชาติ กฎหมายและกฎระเบียบในระดับรัฐและประเทศ รวมถึงสมาคมวิชาชีพ
- **ข้อมูลที่ปรับแต่งสำหรับองค์กรขนาดเล็กและขนาดกลาง**
- **การวัดผลและเมตริก** สำหรับ CIS Controls
- **เอกสารไวท์เปเปอร์** จากผู้ให้บริการและเอกสารอื่นๆ ที่สนับสนุน CIS Controls
- **เอกสารเกี่ยวกับการเชื่อมโยงกับ NIST® Cybersecurity Framework**

วิธีเริ่มต้นใช้งาน (How to Get Started)

ในอดีต **CIS Controls** ถูกจัดเรียงตามลำดับเพื่อช่วยมุ่งเน้นกิจกรรมด้านความปลอดภัยทางไซเบอร์ขององค์กร โดยมีชุดย่อยใน 6 รายการแรกที่เรียกว่า **“cyber hygiene”** อย่างไรก็ตาม วิธีการนี้กลับเรียบง่ายเกินไป องค์กรบางแห่ง โดยเฉพาะองค์กรขนาดเล็ก อาจพบว่าการปฏิบัติตาม **มาตรการป้องกัน** ในขั้นแรกเป็นเรื่องยากและอาจไม่สามารถดำเนินการตาม **CIS Controls** ขั้นถัดไปได้เลย (เช่น การมีกลยุทธ์สำรองข้อมูลเพื่อกู้คืนจากการโจมตีด้วย ransomware)

การเปลี่ยนแปลงในเวอร์ชัน 7.1:

ตั้งแต่ **CIS Controls เวอร์ชัน 7.1** เป็นต้นมา ได้มีการสร้าง **กลุ่มการดำเนินการตาม CIS Controls (Implementation Groups หรือ IGs)** เพื่อเป็นแนวทางใหม่ในการจัดลำดับความสำคัญในการนำไปใช้

CIS Controls Implementation Groups (IGs):

- **IGs คืออะไร:** IGs เป็นหมวดหมู่การประเมินด้วยตนเองสำหรับองค์กร แต่ละ IG ระบุชุดย่อยของ **CIS Controls** ซึ่งชุมชนได้ประเมินว่าเหมาะสมกับองค์กรที่มีโปรไฟล์ความเสี่ยง และทรัพยากรที่คล้ายคลึงกัน
- **แนวทางที่ปรับให้เหมาะกับแต่ละองค์กร:** IGs มองข้าม CIS Controls ในแนวนอน และปรับให้เหมาะกับประเภทขององค์กรที่แตกต่างกัน

การกำหนดกลุ่ม IGs: ดูข้อมูลเพิ่มเติมได้ที่นี่

1 IG1: เรียกว่า **“essential cyber hygiene”**เป็นชุดพื้นฐานของ มาตรการป้องกันด้านการป้องกันทางไซเบอร์ที่ทุกองค์กรควรใช้เพื่อป้องกันการโจมตีที่พบได้บ่อยที่สุด เหมาะสำหรับองค์กรขนาดเล็กที่มีทรัพยากรจำกัด

2 IG2: สร้างขึ้นบนฐานของ IG1 และเพิ่ม มาตรการป้องกัน สำหรับองค์กรที่มีความซับซ้อนมากขึ้น เหมาะสำหรับองค์กรขนาดกลางที่มีทรัพยากรเพิ่มขึ้น

3 IG3: ครอบคลุม มาตรการป้องกัน ทั้งหมดใน IG1 และ IG2 เหมาะสำหรับองค์กรขนาดใหญ่หรือองค์กรที่มีความต้องการด้านความปลอดภัยที่สูง

การใช้งานหรือเปลี่ยนจากเวอร์ชันก่อนหน้าของ CIS Controls

ในขณะที่ภัยคุกคามทางไซเบอร์มีการเปลี่ยนแปลงอย่างต่อเนื่อง เราเชื่อว่า **CIS Controls เวอร์ชัน 8** และการอัปเดตใดๆ ในอนาคต เป็นชุดการควบคุมที่ครอบคลุมและสมบูรณ์ที่สุดที่เราเคยพัฒนา

อย่างไรก็ตาม เราเข้าใจว่าองค์กรที่ใช้งานเวอร์ชันก่อนหน้า เช่น **CIS Controls เวอร์ชัน 7 หรือ 7.1** ในฐานะส่วนสำคัญของกลยุทธ์การป้องกันภัย อาจลังเลที่จะเปลี่ยนไปใช้เวอร์ชัน 8

คำแนะนำของเรา:

สำหรับผู้ที่ใช้งานเวอร์ชัน 7 หรือ 7.1:

- คุณกำลังใช้งานแผนความปลอดภัยที่มีประสิทธิภาพและใช้งานได้จริง
- ในระยะยาว เราแนะนำให้พิจารณาเปลี่ยนไปใช้เวอร์ชันล่าสุดเพื่อให้สอดคล้องกับแนวปฏิบัติที่ดีที่สุด

สำหรับผู้ที่ใช้งานเวอร์ชัน 6 (หรือต่ำกว่า): เราแนะนำให้เริ่มวางแผนการเปลี่ยนไปใช้ **CIS Controls เวอร์ชัน 8** โดยเร็วที่สุดเท่าที่จะเป็นไปได้

CIS Controls เวอร์ชัน 8 นำเสนอแนวทางการป้องกันภัยที่ทันสมัย ครอบคลุม และสามารถช่วยให้องค์กรตอบสนองต่อภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพมากขึ้นในยุคที่การโจมตีมีความซับซ้อนและพัฒนาอย่างรวดเร็ว.

การสนับสนุนการเปลี่ยนผ่านจากเวอร์ชันก่อนหน้าของ CIS Controls

ในเวอร์ชันก่อนหน้าของ **CIS Controls** เราสามารถให้ความช่วยเหลือในรูปแบบเครื่องมือที่ง่ายที่สุดเท่านั้น เช่น **บันทึกการเปลี่ยนแปลง (Change Log)** ที่ใช้สเปรดชีตเป็นหลัก

การเปลี่ยนแปลงในเวอร์ชัน 8:

สำหรับ **เวอร์ชัน 8** เราได้ใช้แนวทางที่ครอบคลุมมากขึ้น โดยทำงานร่วมกับพันธมิตรหลายรายเพื่อให้แน่ใจว่า **ระบบนิเวศของ CIS Controls** พร้อมสนับสนุนการเปลี่ยนผ่านของคุณอย่างเต็มที่

ดูรายละเอียดเพิ่มเติมเกี่ยวกับการเปลี่ยนผ่านและการสนับสนุนได้ที่:
https://www.cisecurity.org/controls/v8-1/

CIS Controls เวอร์ชัน 8 ออกแบบมาเพื่อให้การเปลี่ยนผ่านจากเวอร์ชันก่อนหน้าสะดวกและรองรับความต้องการขององค์กรทุกขนาด.

โครงสร้างของ CIS Controls

การนำเสนอแต่ละ Control ในเอกสารนี้ประกอบด้วยองค์ประกอบดังต่อไปนี้:

- **ภาพรวม (Overview):** คำอธิบายสั้นๆ เกี่ยวกับจุดมุ่งหมายของ Control และประโยชน์ของมันในฐานะมาตรการป้องกัน
- **เหตุใด Control นี้จึงสำคัญ (Why is this Control critical?):** อธิบายถึงความสำคัญของ Control นี้ในการป้องกัน ลดผลกระทบ หรือระบุการโจมตี พร้อมคำอธิบายว่าผู้โจมตีใช้ประโยชน์จากการไม่มี Control นี้อย่างไร
- **กระบวนการและเครื่องมือ (Procedures and tools):** คำอธิบายทางเทคนิคเพิ่มเติมเกี่ยวกับกระบวนการและเทคโนโลยีที่ช่วยในการนำ Control นี้ไปใช้และทำให้การทำงานเป็นอัตโนมัติ
- **คำอธิบาย มาตรการป้องกัน (Safeguard descriptions):** ตารางของการดำเนินการเฉพาะที่องค์กรควรปฏิบัติเพื่อให้สามารถนำ Control นี้ไปใช้ได้

กลุ่มการดำเนินการ (Implementation Groups)

IG1 (Implementation Group 1)

องค์กรในกลุ่ม IG1 เป็นองค์กรขนาดเล็กถึงขนาดกลางที่มีความเชี่ยวชาญด้าน IT และความปลอดภัยทางไซเบอร์ที่จำกัด ซึ่งสามารถจัดสรรเพื่อปกป้องทรัพย์สิน IT และบุคลากรได้

ความกังวลหลัก ขององค์กร IG1: มุ่งเน้นให้ธุรกิจดำเนินงานได้อย่างต่อเนื่อง เนื่องจากมีความอดทนต่อการหยุดทำงาน (Downtime) ที่จำกัดมาก

ข้อมูลที่ต้องการปกป้องมีความอ่อนไหวต่ำ โดยส่วนใหญ่เกี่ยวข้องกับข้อมูลพนักงานและข้อมูลทางการเงิน

มาตรการป้องกัน สำหรับ IG1:

- ควรสามารถนำไปใช้ได้ง่าย แม้มีความเชี่ยวชาญด้านความปลอดภัยทางไซเบอร์ที่จำกัด
- ออกแบบมาเพื่อป้องกันการโจมตีทั่วไปที่ไม่ได้มุ่งเป้าเฉพาะเจาะจง
- มักจะออกแบบให้ใช้งานร่วมกับฮาร์ดแวร์และซอฟต์แวร์สำเร็จรูปเชิงพาณิชย์ (Commercial Off-The-Shelf: COTS) ที่เหมาะสำหรับสำนักงานขนาดเล็กหรือที่บ้าน

IG2 (รวมถึง IG1)

องค์กรในกลุ่ม IG2 มีบุคลากรที่รับผิดชอบการจัดการและปกป้องโครงสร้างพื้นฐาน IT โดยองค์กรเหล่านี้มักประกอบด้วยหลายแผนกที่มีโปรไฟล์ความเสี่ยงแตกต่างกันตามบทบาทหน้าที่และภารกิจ

ลักษณะสำคัญขององค์กร IG2:

- หน่วยงานขนาดเล็กบางแห่งอาจมีภาระด้านการปฏิบัติตามข้อกำหนดด้านกฎระเบียบ
- มักมีการจัดเก็บและประมวลผลข้อมูลสำคัญของลูกค้าหรือองค์กร
- สามารถทนต่อการหยุดชะงักของบริการในช่วงสั้นๆ ได้
- ความกังวลหลักคือ **การสูญเสียความเชื่อมั่นจากสาธารณชน** หากเกิดการละเมิดข้อมูล

มาตรการป้องกัน สำหรับ IG2:

- ออกแบบมาเพื่อช่วยให้ทีมรักษาความปลอดภัยรับมือกับความซับซ้อนในการดำเนินงานที่เพิ่มขึ้น

- บาง มาตรการป้องกัน ต้องอาศัยเทคโนโลยีระดับองค์กร (Enterprise-grade Technology) และความเชี่ยวชาญเฉพาะทางเพื่อการติดตั้งและการกำหนดค่าอย่างเหมาะสม

IG3 (รวมถึง IG1 และ IG2)

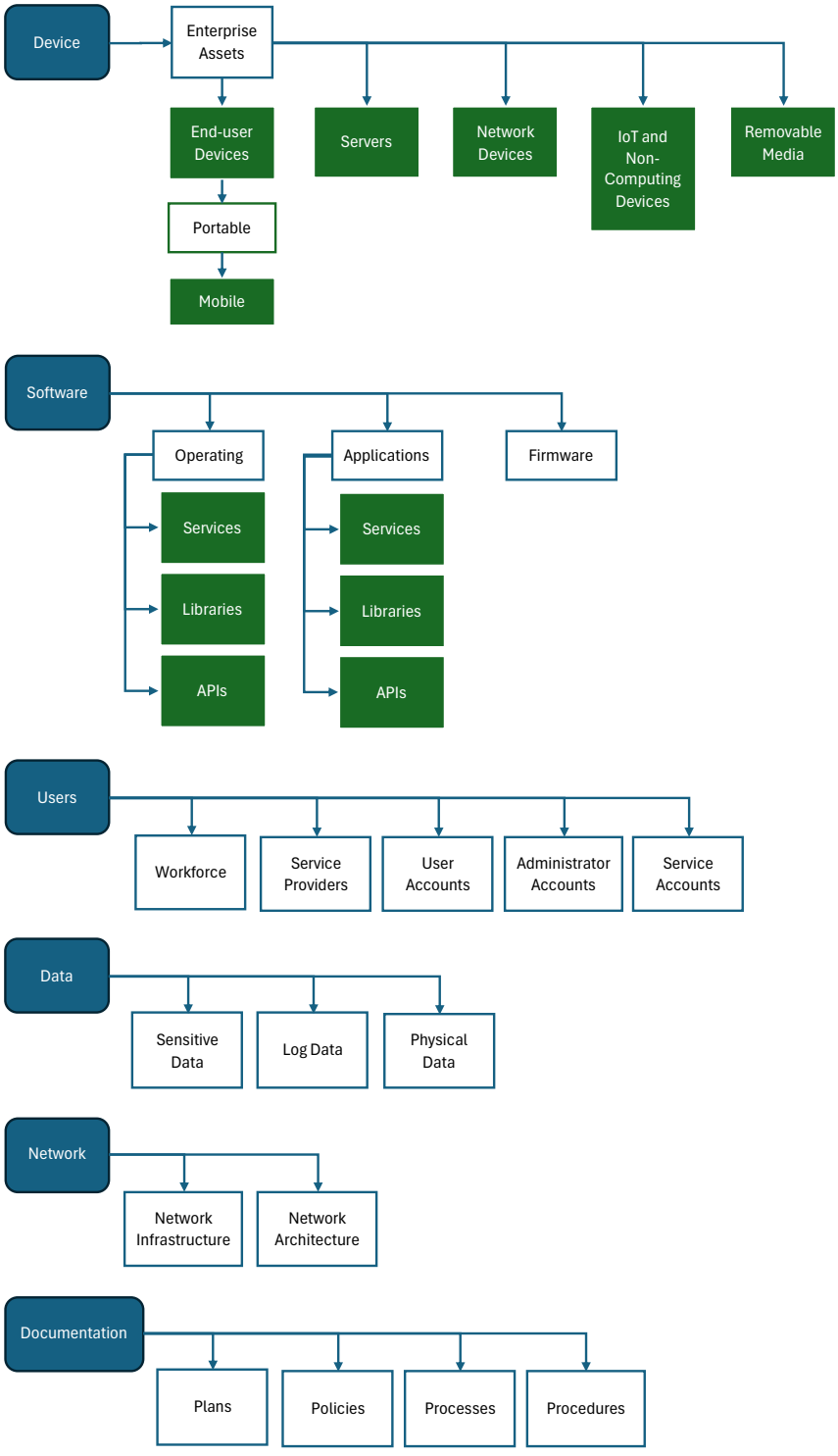
ลักษณะสำคัญขององค์กร IG3:

- ทรัพย์สินและข้อมูลของ IG3 ประกอบด้วยข้อมูลหรือฟังก์ชันที่มีความอ่อนไหวสูงและอยู่ภายใต้การกำกับดูแลด้านกฎระเบียบและการปฏิบัติตามข้อกำหนด
- องค์กรต้องให้ความสำคัญกับ **ความพร้อมใช้งานของบริการ (Availability)**, **ความลับ (Confidentiality)**, และ **ความสมบูรณ์ของข้อมูลที่อ่อนไหว (Integrity)**
- การโจมตีที่สำเร็จสามารถสร้างความเสียหายอย่างมากต่อสวัสดิภาพของสาธารณชน

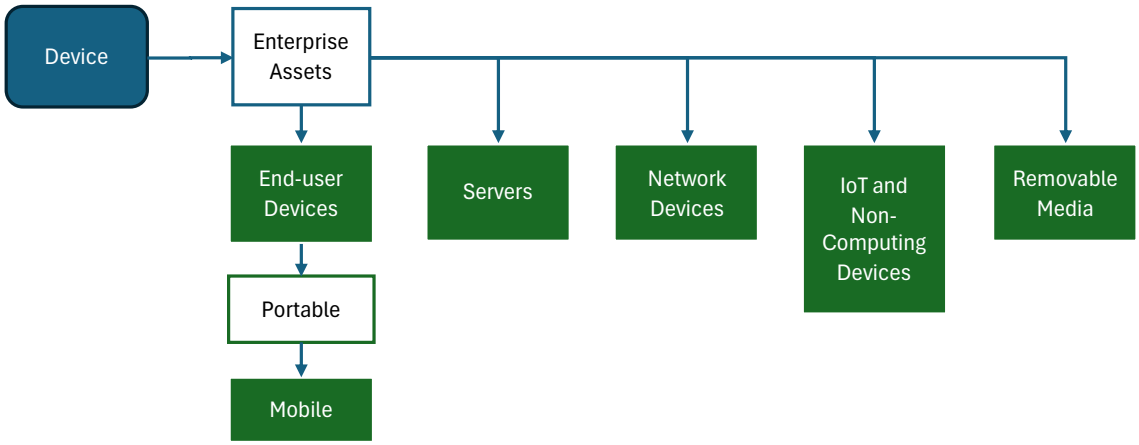
มาตรการป้องกัน สำหรับ IG3:

- ต้องออกแบบเพื่อป้องกันการโจมตีที่มีเป้าหมาย (Targeted Attacks) จากผู้โจมตีที่มีความเชี่ยวชาญสูง
- ลดผลกระทบจากการโจมตีในรูปแบบ Zero-Day ซึ่งเป็นช่องโหว่ที่ยังไม่มีการแก้ไข

Asset Classes



อุปกรณ์ (Devices)



อุปกรณ์สามารถอยู่ในพื้นที่ทางกายภาพ โครงสร้างพื้นฐานเสมือน (Virtual Infrastructure) หรือสภาพแวดล้อมบนคลาวด์ (Cloud-based Environments) นอกจากนี้ อุปกรณ์ยังสามารถเชื่อมต่อกับระบบเหล่านี้ได้จากระยะไกล

ทรัพย์สินขององค์กร (Enterprise Assets): ทรัพย์สินที่มีศักยภาพในการจัดเก็บหรือประมวลผลข้อมูล สำหรับเอกสารนี้ ทรัพย์สินขององค์กรรวมถึงอุปกรณ์ที่ใช้โดยผู้ใช้งานปลายทาง (End-user Devices), อุปกรณ์เครือข่าย (Network Devices), อุปกรณ์ที่ไม่ใช่คอมพิวเตอร์/อุปกรณ์ Internet of Things (IoT), และเซิร์ฟเวอร์ ซึ่งสามารถอยู่ในสภาพแวดล้อมเสมือน, บนคลาวด์, หรือในพื้นที่ทางกายภาพ

อุปกรณ์สำหรับผู้ใช้งานปลายทาง (End-user Devices): ทรัพย์สินด้านเทคโนโลยีสารสนเทศ (IT) ที่สมาชิกในองค์กรใช้ในช่วงเวลาทำงานหรือเวลาว่าง อุปกรณ์สำหรับผู้ใช้งานปลายทางประกอบด้วยคอมพิวเตอร์ตั้งโต๊ะ (Desktops), เวิร์กสเตชัน (Workstations), และอุปกรณ์พกพาหรือเคลื่อนที่ เช่น แล็ปท็อป สมาร์ทโฟน และแท็บเล็ต สำหรับเอกสารนี้ อุปกรณ์สำหรับผู้ใช้งานปลายทางเป็นส่วนย่อยของทรัพย์สินขององค์กร

อุปกรณ์พกพา (Portable Devices): อุปกรณ์ที่สามารถพกพาได้และมีความสามารถในการเชื่อมต่อเครือข่ายแบบไร้สาย อุปกรณ์พกพาสำหรับผู้ใช้งานปลายทางอาจรวมถึงแล็ปท็อปที่อาจต้องใช้อุปกรณ์เสริมภายนอกสำหรับการเชื่อมต่อ และอุปกรณ์เคลื่อนที่ เช่น สมาร์ทโฟนและแท็บเล็ต สำหรับเอกสารนี้ อุปกรณ์พกพาถือเป็นส่วนย่อยของอุปกรณ์สำหรับผู้ใช้งานปลายทาง

อุปกรณ์เคลื่อนที่ (Mobile Devices): อุปกรณ์ขนาดเล็กที่องค์กรออกให้สำหรับผู้ใช้งานปลายทาง โดยมีความสามารถในการเชื่อมต่อแบบไร้สายในตัว เช่น สมาร์ทโฟนและแท็บเล็ต สำหรับเอกสารนี้ อุปกรณ์เคลื่อนที่ถือเป็นส่วนย่อยของอุปกรณ์พกพา

เซิร์ฟเวอร์ (Servers): อุปกรณ์หรือระบบที่ให้ทรัพยากร ข้อมูล บริการ หรือโปรแกรมแก่เครื่องอื่นๆ เซิร์ฟเวอร์สามารถอยู่ในศูนย์ข้อมูล (Datacenters), สภาพแวดล้อมบนคลาวด์แบบสาธารณะ, ส่วนตัว, หรือแบบไฮบริด รวมถึงเครื่องเสมือน (Virtual

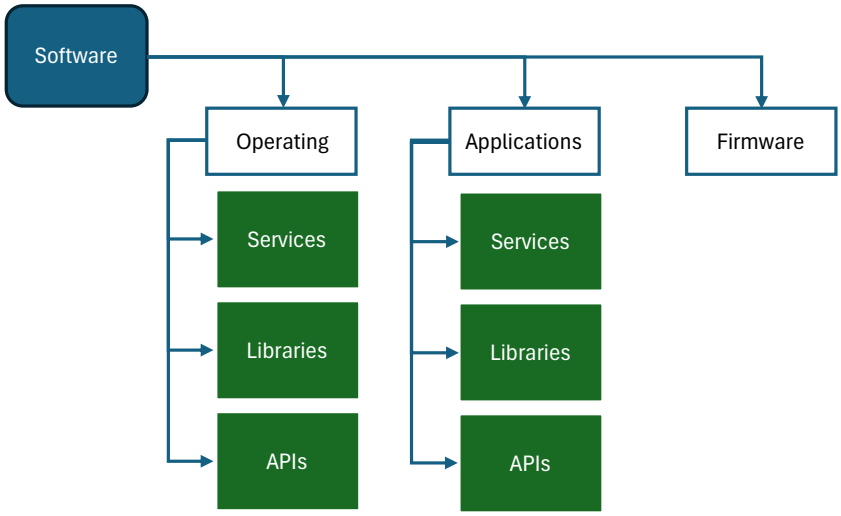
Machines), คอนเทนเนอร์ชั่วคราว (Temporal Containers), หรือเวิร์กโหลดแบบไม่มีเซิร์ฟเวอร์ (Serverless Workloads) ตัวอย่างของเซิร์ฟเวอร์ ได้แก่ เว็บเซิร์ฟเวอร์, แอปพลิเคชันเซิร์ฟเวอร์, เมลเซิร์ฟเวอร์, และไฟล์เซิร์ฟเวอร์ สำหรับเอกสารนี้ เซิร์ฟเวอร์ถือเป็นส่วนย่อยของทรัพย์สินขององค์กร

อุปกรณ์ Internet of Things (IoT) และอุปกรณ์ที่ไม่ใช่คอมพิวเตอร์ (Non-computing Devices): อุปกรณ์ที่ฝังตัวด้วยเซ็นเซอร์ ซอฟต์แวร์ และเทคโนโลยีอื่นๆ อุปกรณ์เหล่านี้สามารถเชื่อมต่อ จัดเก็บ และแลกเปลี่ยนข้อมูลกับอุปกรณ์หรือระบบอื่นๆ ได้ การเชื่อมต่อของอุปกรณ์กับอินเทอร์เน็ตอาจเป็นแบบต่อเนื่อง, ไม่ต่อเนื่อง, หรือไม่มีการเชื่อมต่อ ตัวอย่างอุปกรณ์เหล่านี้ ได้แก่ สมาร์ทวอทช์และอุปกรณ์สวมใส่อื่นๆ, เครื่องพิมพ์, จอภาพอัจฉริยะ, อุปกรณ์สมาร์ทโฮม, ลำโพง, ระบบควบคุมในอุตสาหกรรม, และเซ็นเซอร์ด้านความปลอดภัยทางกายภาพ สำหรับเอกสารนี้ อุปกรณ์ IoT และอุปกรณ์ที่ไม่ใช่คอมพิวเตอร์ถือเป็นส่วนย่อยของทรัพย์สินขององค์กร

อุปกรณ์เครือข่าย (Network Devices): อุปกรณ์อิเล็กทรอนิกส์ที่จำเป็นสำหรับการสื่อสารและการทำงานร่วมกันระหว่างอุปกรณ์ในเครือข่ายคอมพิวเตอร์ อุปกรณ์เครือข่ายรวมถึงจุดเชื่อมต่อไร้สาย (Wireless Access Points), ไฟร์วอลล์ (Firewalls), สวิตช์ (Switches), เราเตอร์ (Routers), และเกตเวย์ (Gateways) ทั้งแบบฮาร์ดแวร์และแบบเสมือน อุปกรณ์เหล่านี้ประกอบด้วยฮาร์ดแวร์ทางกายภาพ รวมถึงอุปกรณ์เสมือนและบนคลาวด์ สำหรับเอกสารนี้ อุปกรณ์เครือข่ายถือเป็นส่วนย่อยของทรัพย์สินขององค์กร โดยอุปกรณ์เครือข่ายมีบทบาทสองด้าน คือ เป็นทรัพย์สินขององค์กร และเป็นทรัพย์สินที่เกี่ยวข้องกับการสื่อสารในเครือข่าย

สื่อที่ถอดออกได้ (Removable Media): อุปกรณ์จัดเก็บข้อมูลทุกประเภทที่สามารถถอดออกจากคอมพิวเตอร์ขณะระบบยังทำงานอยู่ และช่วยให้สามารถย้ายข้อมูลระหว่างระบบ ตัวอย่างของสื่อที่ถอดออกได้ ได้แก่ ซีดี (CDs), ดีวีดี (DVDs), บลูเรย์ดิสก์ (Blu-ray Discs), ฮาร์ดไดรฟ์ภายนอก (External Hard Drives), การ์ด SD, เทปสำรองข้อมูล (Tape Backups), ดิสเก็ตต์ (Diskettes), และไดรฟ์ USB

ซอฟต์แวร์ (Software)



ชุดข้อมูลและคำสั่งที่ใช้ในการกำหนดทิศทางให้คอมพิวเตอร์ดำเนินงานเฉพาะ ซอฟต์แวร์ถือเป็นทรัพย์สินที่รวมถึงระบบปฏิบัติการและแอปพลิเคชัน ซึ่งอาจประกอบด้วยบริการ (Services), ไลบรารี (Libraries), หรืออินเทอร์เฟซการเขียนโปรแกรมแอปพลิเคชัน (APIs)

แอปพลิเคชัน (Applications): โปรแกรม หรือ กลุ่มของโปรแกรมที่ทำงานบนระบบปฏิบัติการซึ่งติดตั้งบนทรัพย์สินขององค์กร ตัวอย่างประเภทแอปพลิเคชัน ได้แก่ เว็บ, ฐานข้อมูล, บนคลาวด์, และมือถือ แอปพลิเคชันถือเป็นทรัพย์สินซอฟต์แวร์ในเอกสารนี้

ระบบปฏิบัติการ (Operating Systems): ซอฟต์แวร์บนทรัพย์สินขององค์กรที่จัดการทรัพยากรฮาร์ดแวร์และซอฟต์แวร์ และให้บริการพื้นฐานสำหรับโปรแกรมต่างๆ ตัวอย่างระบบปฏิบัติการ ได้แก่ Windows, Ubuntu, MacOS, Android, และ z/OS ระบบปฏิบัติการถือเป็นทรัพย์สินซอฟต์แวร์ในเอกสารนี้

บริการ (Services): โปรแกรมเฉพาะที่ทำงานสำหรับงานสำคัญของระบบปฏิบัติการ โดยบริการมักเริ่มต้นพร้อมกับระบบปฏิบัติการ ทำงานเบื้องหลัง และสามารถหยุดหรือเริ่มใหม่ได้โดยผู้ใช้ ตัวอย่างบริการ ได้แก่ การจัดการการสื่อสารเครือข่าย, ผู้ใช้งาน, สิทธิ์ไฟล์, ความปลอดภัยของระบบ, และการโต้ตอบกับอุปกรณ์

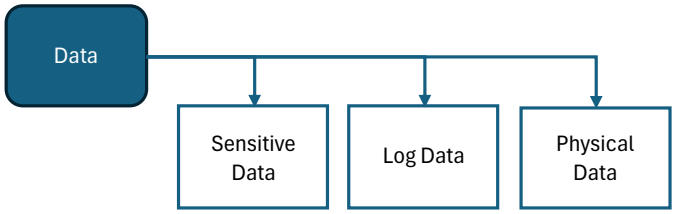
ไลบรารี (Library): ชุดโค้ดที่คอมไพล์ไว้ล่วงหน้าเพื่อแชร์และใช้งาน ประกอบด้วยคลาส, ขั้นตอนการทำงาน, สคริปต์, ข้อมูลการตั้งค่า และอื่นๆ ไลบรารีถูกออกแบบมาเพื่อช่วยผู้พัฒนาโปรแกรมและคอมไพเลอร์ในการสร้างและใช้งานซอฟต์แวร์ได้อย่างมีประสิทธิภาพมากขึ้น

อินเทอร์เฟซการเขียนโปรแกรมแอปพลิเคชัน (Application Programming Interface - API): ชุดกฎและอินเทอร์เฟซที่ช่วยให้ส่วนประกอบของซอฟต์แวร์

สามารถโต้ตอบกันได้ในรูปแบบมาตรฐาน APIs ช่วยให้แอปพลิเคชันสามารถเข้าถึงและสื่อสารกับทรัพยากรภายในและภายนอก

เฟิร์มแวร์ (Firmware): ซอฟต์แวร์ที่จัดเก็บในหน่วยความจำถาวรของอุปกรณ์ เช่น ROM หรือแฟลชเมมโมรี เฟิร์มแวร์ช่วยให้อุปกรณ์ฮาร์ดแวร์ประเภทต่างๆ สื่อสารกับระบบปฏิบัติการได้ เฟิร์มแวร์มักจะได้รับการอัปเดตแยกจากกระบวนการอัปเดตซอฟต์แวร์ระบบปฏิบัติการและแอปพลิเคชันขององค์กร

ข้อมูล (Data)



ข้อมูลคือชุดข้อเท็จจริงที่สามารถตรวจสอบ วิเคราะห์ และนำไปใช้ในการตัดสินใจได้ องค์กรมักจัดเก็บและประมวลผลข้อมูลที่สำคัญต่อการดำเนินงาน แต่ไม่ได้จัดว่าเป็นข้อมูลที่มีความอ่อนไหว อย่างไรก็ตาม ข้อมูลเหล่านี้ยังคงต้องได้รับการปกป้องอย่างเหมาะสม แม้ว่าข้อมูลอาจอยู่ในรูปแบบกายภาพ แต่ CIS Controls มุ่งเน้นการป้องกันข้อมูลดิจิทัลที่อาจถูกจัดเก็บ ส่งต่อ และประมวลผลโดยระบบคอมพิวเตอร์เป็นหลัก

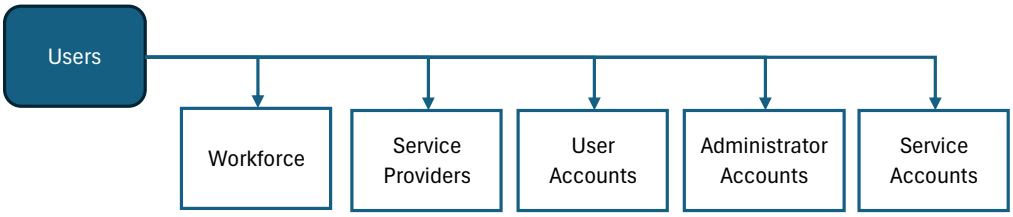
ข้อมูลที่มีความอ่อนไหว (Sensitive Data): ข้อมูลในรูปแบบกายภาพหรือดิจิทัลที่องค์กรจัดเก็บ ประมวลผล หรือจัดการ ซึ่งต้องเก็บไว้เป็นความลับ แม่นยำ เชื่อถือได้ และพร้อมใช้งาน หากข้อมูลนี้ถูกเปิดเผยหรือทำลายโดยไม่ได้รับอนุญาต อาจก่อให้เกิดความเสียหายต่อองค์กรหรือลูกค้า ความเสียหายดังกล่าวอาจเกิดจากการละเมิดข้อมูล (Data Breach) หรือการฝ่าฝืนนโยบาย สัญญา หรือข้อกำหนดทางกฎหมาย

ข้อมูลล็อก (Log Data): ไฟล์ข้อมูลที่สร้างโดยระบบคอมพิวเตอร์เพื่อบันทึกเหตุการณ์ที่เกิดขึ้นภายในองค์กร ตัวอย่างของล็อก ได้แก่:

- ล็อกของระบบปฏิบัติการ
- การตรวจจับมัลแวร์
- ฐานข้อมูล
- แอปพลิเคชัน
- เครือข่าย
- ไฟร์วอลล์
- เว็บเซิร์ฟเวอร์
- ล็อกการควบคุมการเข้าถึง (เช่น ล็อกอิเล็กทรอนิกส์, ระบบสัญญาณเตือน)

ข้อมูลกายภาพ (Physical Data): ข้อมูลที่จัดเก็บในเอกสารกายภาพ หรือในอุปกรณ์จัดเก็บข้อมูลแบบถอดออกได้ (Removable Devices) เช่น ไดรฟ์ USB, เทปสำรองข้อมูล ข้อมูลกายภาพอาจจัดว่าเป็นข้อมูลที่มีความอ่อนไหวหรือไม่ก็ได้

ผู้ใช้งาน (Users)



ผู้ใช้งานหมายถึงพนักงาน, ผู้ให้บริการจากบุคคลภายนอก, ผู้รับเหมา, ผู้ให้บริการ, ที่ปรึกษา หรือบุคคลอื่นๆ ที่ได้รับอนุญาตให้เข้าถึงทรัพย์สินขององค์กร รวมถึงบัญชีผู้ใช้งาน (User Accounts), บัญชีผู้ดูแลระบบ (Administrator Accounts), และบัญชีบริการ (Service Accounts)

บุคลากรในองค์กร (Workforce): บุคคลทั้งหมดที่ได้รับการว่าจ้างหรือมีส่วนร่วมกับองค์กร และมีสิทธิ์เข้าถึงระบบข้อมูล, ทรัพย์สิน, หรือทรัพยากรขององค์กร รวมถึงพนักงานที่ทำงานในสถานที่หรือระยะไกล ผู้รับเหมามักจะถือว่าเป็นส่วนหนึ่งของบุคลากรในองค์กร ขณะที่ที่ปรึกษาและผู้ให้บริการอาจไม่ใช่ ทั้งนี้ขึ้นอยู่กับข้อตกลงในสัญญา

ผู้ให้บริการ (Service Providers): ผู้ให้บริการคือหน่วยงานที่เสนอแพลตฟอร์ม, ซอฟต์แวร์, และบริการให้กับองค์กรอื่น ตัวอย่างได้แก่:

- ที่ปรึกษาด้าน IT
- ผู้ให้บริการที่มีการจัดการ (Managed Service Providers - MSPs)
- แพลตฟอร์ม Software as a Service (SaaS)
- ผู้ให้บริการคลาวด์
  ผู้ให้บริการบุคคลที่สามและผู้ขาย (Vendors) ก็ถือว่าเป็นผู้ให้บริการด้วยเช่นกัน บริการเหล่านี้อาจมีค่าใช้จ่ายหรือไม่มีความจำเป็นต้องมีสัญญา (Contract) หรือข้อตกลงระดับการให้บริการ (SLA)

บัญชีผู้ใช้งาน (User Accounts): ตัวตนที่ประกอบด้วยข้อมูลประจำตัว เช่น ชื่อผู้ใช้งานและรหัสผ่าน ใช้ในการระบุผู้ใช้งานในระบบคอมพิวเตอร์หรือเครือข่าย บัญชีผู้ใช้งานจะควบคุมข้อมูลและการตั้งค่าของผู้ใช้ รวมถึงการเข้าถึงไฟล์ โฟลเดอร์ และทรัพยากรต่างๆ ในเอกสารนี้ บัญชีผู้ใช้งานหมายถึงบัญชีผู้ใช้มาตรฐานที่มีสิทธิ์จำกัดและใช้สำหรับการดำเนินการทั่วไป

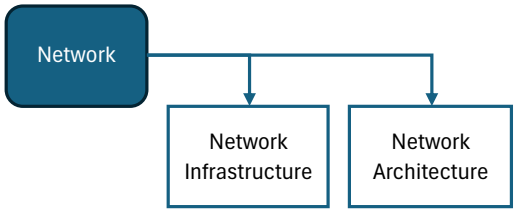
บัญชีผู้ดูแลระบบ (Administrator Accounts): บัญชีสำหรับผู้ใช้งานที่ต้องการสิทธิพิเศษระดับสูงเพื่อจัดการด้านต่างๆ ของคอมพิวเตอร์, โดเมน, หรือโครงสร้างพื้นฐาน IT

ทั้งหมดในองค์กร บัญชีผู้ดูแลระบบแต่ละบัญชีควรเชื่อมโยงกับผู้ใช้งานคนเดียว ประเภทของบัญชีผู้ดูแลระบบที่พบบ่อย ได้แก่:

- บัญชี Root
- บัญชีผู้ดูแลระบบท้องถิ่น
- บัญชีผู้ดูแลโดเมน
- บัญชีผู้ดูแลอุปกรณ์เครือข่ายหรือความปลอดภัย

บัญชีบริการ (Service Accounts): บัญชีที่สร้างขึ้นสำหรับการใช้งานแอปพลิเคชัน, บริการ, หรือกระบวนการอัตโนมัติบนระบบปฏิบัติการ บัญชีบริการอาจถูกสร้างขึ้นเพื่อครอบครองข้อมูลหรือไฟล์การตั้งค่าโดยเฉพาะ แต่ละบัญชีบริการควรใช้สำหรับบริการหรือฟังก์ชันเฉพาะ และควรมีเจ้าของที่รับผิดชอบในการใช้งานบัญชีนั้น บัญชีบริการไม่ควรใช้สำหรับงานคอมพิวเตอร์ทั่วไป

เครือข่าย (Network)



เครือข่ายคือกลุ่มของอุปกรณ์ที่เชื่อมต่อกันเพื่อแลกเปลี่ยนข้อมูล องค์กรอาจดำเนินการเครือข่ายหนึ่งเครือข่ายหรือมากกว่าที่จัดการร่วมกันหรือแยกออกจากกัน

โครงสร้างพื้นฐานเครือข่าย (Network Infrastructure): การรวบรวมทรัพยากรเครือข่ายที่ให้การเชื่อมต่อ การจัดการ การดำเนินงานทางธุรกิจ และการสื่อสาร ประกอบด้วยฮาร์ดแวร์ ซอฟต์แวร์ ระบบ และอุปกรณ์ต่างๆ ที่ช่วยให้เกิดการประมวลผลและการสื่อสารระหว่างผู้ใช้งาน บริการ แอปพลิเคชัน และกระบวนการ โครงสร้างพื้นฐานเครือข่ายสามารถอยู่ในรูปแบบคลาวด์ กายภาพ หรือเสมือน

สถาปัตยกรรมเครือข่าย (Network Architecture): หมายถึงการออกแบบเครือข่าย ทั้งในเชิงกายภาพและเชิงตรรกะ โดยกำหนดวิธีการจัดระเบียบเครือข่าย รวมถึงการเชื่อมต่อระหว่างอุปกรณ์และซอฟต์แวร์ ตลอดจนข้อมูลที่ส่งผ่านระหว่างกัน สิ่งนี้ควรรวมถึงแผนผังสถาปัตยกรรมเครือข่ายและแผนผังสถาปัตยกรรมความปลอดภัย

เอกสาร (Documentation)

เอกสารหมายถึง นโยบาย (Policies), กระบวนการ (Processes), ขั้นตอน (Procedures), แผนงาน (Plans), แผนผัง (Diagrams), และเอกสารอื่นๆ ทั้งในรูปแบบกายภาพและดิจิทัล เช่น รายงานการปฏิบัติตามข้อกำหนด

(Compliance Reports) ตัวอย่างเอกสารอาจรวมถึงวิธีการกำกับดูแลขององค์กร กระบวนการที่ผู้ใช้งานต้องปฏิบัติตาม หรือคำอธิบายเกี่ยวกับสถาปัตยกรรมเครือข่าย

แผนงาน (Plan): แผนงานเป็นการนำเอานโยบายไปใช้ปฏิบัติ ซึ่งอาจรวมถึงกลุ่มของนโยบาย กระบวนการ และขั้นตอนต่างๆ

นโยบาย (Policy): คำแถลงอย่างเป็นทางการขององค์กรที่กำหนดวัตถุประสงค์เฉพาะของโปรแกรมรักษาความปลอดภัยข้อมูล นโยบายอาจระบุการดำเนินการที่ต้องทำหรือการกระทำที่ต้องห้าม

กระบวนการ (Process): ชุดของงานทั่วไปและกิจกรรมที่ออกแบบมาเพื่อให้บรรลุเป้าหมายด้านความปลอดภัย กระบวนการควรถูกจัดทำเป็นเอกสาร ซึ่งสามารถรวมอยู่ในแผนงาน (Plan), นโยบาย (Policy), ขั้นตอน (Procedure) หรือเอกสารที่ไม่เป็นทางการ

ขั้นตอน (Procedure): ชุดของขั้นตอนที่จัดลำดับไว้สำหรับการดำเนินงานเฉพาะเจาะจง ให้แนวทางที่ได้รับการอนุมัติสำหรับการปฏิบัติในสภาพแวดล้อมทางเทคโนโลยีและองค์กรที่กำหนด

CIS Critical Security Controls

CONTROL 1

การจัดทำและควบคุมรายการทรัพย์สินขององค์กร Inventory and Control of Enterprise Assets

Safeguards: 5	IG1: 2/5	IG2: 4/5	IG3: 5/5

ภาพรวม (Overview):

การจัดการอย่างกระตือรือร้น (เช่น การสำรวจ, ติดตาม, และแก้ไข) ทรัพย์สินทั้งหมดขององค์กร (อุปกรณ์ผู้ใช้งานปลายทาง รวมถึงอุปกรณ์พกพาและเคลื่อนที่; อุปกรณ์เครือข่าย; อุปกรณ์ที่ไม่ใช่คอมพิวเตอร์/Internet of Things (IoT); และเซิร์ฟเวอร์) ที่เชื่อมต่อกับโครงสร้างพื้นฐาน ทั้งในเชิงกายภาพ, เสมือน, ระยะไกล, และในสภาพแวดล้อมบนคลาวด์ เพื่อให้ทราบถึงทรัพย์สินทั้งหมดที่ต้องได้รับการตรวจสอบและป้องกันในองค์กร การดำเนินการนี้ยังสนับสนุนการระบุทรัพย์สินที่ไม่ได้รับอนุญาตหรือไม่ได้รับการจัดการ เพื่อนำออกหรือแก้ไข

เหตุใดการควบคุมนี้จึงสำคัญ? (Why is this Control critical?)

องค์กรไม่สามารถป้องกันสิ่งที่พวกเขาไม่รู้ว่ามีอยู่ การควบคุมทรัพย์สินทั้งหมดขององค์กรมีบทบาทสำคัญใน:

- การเฝ้าระวังความปลอดภัย
- การตอบสนองต่อเหตุการณ์
- การสำรองและกู้คืนระบบ

องค์กรควรทราบว่าข้อมูลใดมีความสำคัญต่อพวกเขา การจัดการทรัพย์สินอย่างเหมาะสมจะช่วยระบุทรัพย์สินที่เกี่ยวข้องกับข้อมูลสำคัญเพื่อใช้มาตรการรักษาความปลอดภัยที่เหมาะสม

ภัยคุกคามที่สำคัญ:

- ผู้โจมตีจากภายนอกมักสแกนพื้นที่ที่อยู่ของอินเทอร์เน็ตเพื่อหาทรัพย์สินที่อาจไม่ได้รับการปกป้อง
- ผู้โจมตีสามารถใช้ประโยชน์จากทรัพย์สินใหม่ที่ยังไม่ได้กำหนดค่าความปลอดภัยอย่างเหมาะสม
- ทรัพย์สินที่ไม่ถูกระบุภายในองค์กรอาจมีการตั้งค่าความปลอดภัยที่อ่อนแอ ทำให้ง่ายต่อการถูกโจมตีด้วยมัลแวร์ผ่านเว็บหรืออีเมล

ตัวอย่างการป้องกันเพิ่มเติม:

- ทรัพย์สินเชื่อมต่อชั่วคราว เช่น ระบบทดสอบ หรือ เครือข่ายผู้เยี่ยมชม ควรได้รับการระบุและแยกเพื่อลดความเสี่ยง

กระบวนการ และเครื่องมือ (Procedures and Tools):

การควบคุมนี้ต้องใช้การดำเนินการทั้งในด้านเทคนิคและกระบวนการ ซึ่งรวมถึง:

- การสำรวจและจัดการข้อมูลสินทรัพย์ขององค์กรตลอดวงจรชีวิตของมัน
- เชื่อมโยงกับการกำกับดูแลธุรกิจโดยการกำหนดเจ้าของข้อมูล/ทรัพย์สินสำหรับแต่ละส่วนประกอบในกระบวนการธุรกิจ

องค์กรขนาดเล็ก:

- ใช้เครื่องมือความปลอดภัยที่มีอยู่ เช่น การสแกนเครือข่ายด้วยเครื่องมือตรวจหาช่องโหว่, ตรวจสอบล็อกจากโปรแกรมป้องกันมัลแวร์, ล็อกเครือข่ายจากสวิตช์, หรือล็อกการยืนยันตัวตน
- จัดการผลลัพธ์ในรูปแบบสเปรดชีตหรือฐานข้อมูล

องค์กรขนาดใหญ่:

ใช้ข้อมูลจากพอร์ทัลคลาวด์ และล็อกจากแพลตฟอร์มองค์กร เช่น:

- Active Directory (AD)
- Single Sign-On (SSO)
- Multi-Factor Authentication (MFA)
- Virtual Private Network (VPN)
- Intrusion Detection Systems (IDS)
- Mobile Device Management (MDM)
- เครื่องมือตรวจหาช่องโหว่

การบำรุงรักษา:

- การสำรวจทรัพย์สินองค์กรอย่างต่อเนื่องเป็นกระบวนการที่ต้องปรับปรุงอยู่เสมอ
- ใช้ฐานข้อมูลสินทรัพย์ การติดตามคำสั่งซื้อ และรายการสินค้าท้องถิ่น เพื่อกำหนดว่ามีอุปกรณ์ใดเชื่อมต่ออยู่

ผลประโยชน์เพิ่มเติม:

การจัดการทรัพย์สินอย่างสมบูรณ์ช่วยสนับสนุนการตอบสนองต่อเหตุการณ์ เช่น:

- การตรวจสอบแหล่งที่มาของทราฟฟิกเครือข่าย

- การระบุทรัพย์สินที่มีช่องโหว่หรือได้รับผลกระทบในเหตุการณ์เดียวกัน

วิธีการ และคำแนะนำเพิ่มเติม (Methods and Additional Guidance):

มีเครื่องมือและวิธีการที่ช่วยปรับข้อมูลให้เป็นมาตรฐานเพื่อระบุอุปกรณ์ที่มีลักษณะเฉพาะในแต่ละแหล่งข้อมูล

คู่มือแนะนำเฉพาะด้าน:

- **คำแนะนำสำหรับระบบคลาวด์ (Cloud-Specific Guidance):** ดูคู่มือ CIS Controls Cloud Companion Guide ได้ที่: https://www.cisecurity.org/controls/v8/
- **คำแนะนำสำหรับแท็บเล็ตและสมาร์ทโฟน (Tablet and Smartphone Guidance):** ดูคู่มือ CIS Controls Mobile Companion Guide ได้ที่: https://www.cisecurity.org/controls/v8/
- **คำแนะนำสำหรับ IoT (IoT Guidance):** ดูคู่มือ CIS Controls Internet of Things Companion Guide ได้ที่: https://www.cisecurity.org/controls/v8/
- **คำแนะนำสำหรับระบบควบคุมอุตสาหกรรม (Industrial Control Systems - ICS):** ดูคู่มือ CIS Controls ICS Implementation Guide https://www.cisecurity.org/controls/v8/ สำหรับรายละเอียดเพิ่มเติม

มาตรการป้องกัน (Safeguards)

มาตรการป้องกันที่ 1.1: การจัดตั้งและรักษารายการสินทรัพย์ขององค์กรอย่างละเอียด (Establish and Maintain Detailed Enterprise Asset Inventory)

Asset Type: Devices	Security Function: Identify		IG1 IG2 IG3

การจัดตั้งและรักษารายการสินทรัพย์ขององค์กร (Establish and Maintain an Accurate Enterprise Asset Inventory)

จัดตั้งและรักษารายการสินทรัพย์ขององค์กรที่ถูกต้อง ครบถ้วน และเป็นปัจจุบัน สำหรับสินทรัพย์ทั้งหมดที่มีศักยภาพในการจัดเก็บหรือประมวลผลข้อมูล รวมถึง:

- อุปกรณ์ผู้ใช้งานปลายทาง (End-user Devices) เช่น อุปกรณ์พกพาและเคลื่อนที่
- อุปกรณ์เครือข่าย (Network Devices)
- อุปกรณ์ที่ไม่ใช่คอมพิวเตอร์/IoT (Non-computing/IoT Devices)
- เซิร์ฟเวอร์ (Servers)

สิ่งที่ต้องบันทึกในรายการสินทรัพย์:

- ที่อยู่เครือข่าย (Network Address) หากเป็นแบบคงที่
- ที่อยู่ฮาร์ดแวร์ (Hardware Address)
- ชื่อเครื่อง (Machine Name)
- ชื่อเจ้าของสินทรัพย์ในองค์กร (Enterprise Asset Owner)
- แผนกที่สินทรัพย์นั้นสังกัด (Department)
- การอนุมัติการเชื่อมต่อเครือข่ายของสินทรัพย์แต่ละรายการ

สำหรับอุปกรณ์ผู้ใช้งานเคลื่อนที่ (Mobile End-user Devices): เครื่องมือประเภท Mobile Device Management (MDM) สามารถช่วยสนับสนุนกระบวนการนี้ได้เมื่อเหมาะสม

รายการสินทรัพย์ควรครอบคลุม:

สินทรัพย์ที่เชื่อมต่อกับโครงสร้างพื้นฐานในรูปแบบกายภาพ, เสมือน, ระยะไกล และในสภาพแวดล้อมคลาวด์

สินทรัพย์ที่เชื่อมต่อกับโครงสร้างพื้นฐานเครือข่ายขององค์กรอย่างสม่ำเสมอ แม้ว่าสินทรัพย์เหล่านี้อาจไม่ได้อยู่ภายใต้การควบคุมขององค์กร

ความถี่ในการอัปเดต: ตรวจสอบและอัปเดตรายการสินทรัพย์ขององค์กรทุก 6 เดือน หรือบ่อยกว่านั้น

การดำเนินการนี้ช่วยให้องค์กรจัดการสินทรัพย์ได้อย่างครอบคลุมและลดความเสี่ยงจากการละเมิดความปลอดภัยของระบบเครือข่าย.

มาตรการป้องกันที่ 1.2: การจัดการสินทรัพย์ที่ไม่ได้รับอนุญาต (Address Unauthorized Assets)

Asset Type: Devices	Security Function: Identify		IG1 IG2 IG3

กำหนดให้มี กระบวนการในการจัดการสินทรัพย์ที่ไม่ได้รับอนุญาต โดยดำเนินการตรวจสอบ และจัดการเป็นรายสัปดาห์ องค์กรสามารถเลือกวิธีการจัดการดังนี้:

- ถอดสินทรัพย์ออกจากเครือข่าย
- ปฏิเสธการเชื่อมต่อสินทรัพย์เข้ากับเครือข่ายจากระยะไกล
- แยกสินทรัพย์ออก (Quarantine)

เป้าหมาย: เพื่อป้องกันการเข้าถึงเครือข่ายโดยสินทรัพย์ที่ไม่ได้รับอนุญาต ซึ่งอาจนำไปสู่ความเสี่ยงด้านความปลอดภัยหรือการโจมตีทางไซเบอร์.

มาตรการป้องกันที่ 1.3: ใช้เครื่องมือค้นหาแบบแอคทีฟ (Utilize an Active Discovery Tool)

Asset Type: Devices	Security Function: Detect		IG2 IG3

ใช้ **เครื่องมือค้นหาแบบแอคทีฟ (Active Discovery Tool)** เพื่อตรวจสอบและระบุสินทรัพย์ที่เชื่อมต่อกับเครือข่ายขององค์กร

การดำเนินการ: กำหนดค่าเครื่องมือค้นหาแบบแอคทีฟให้ทำงาน รายวันหรือบ่อยกว่านั้น

เป้าหมาย: เพื่อให้สามารถตรวจสอบและติดตามสินทรัพย์ที่เชื่อมต่อกับเครือข่ายได้อย่างต่อเนื่อง ช่วยลดความเสี่ยงจากการมีสินทรัพย์ที่ไม่ได้รับการจัดการหรือไม่ได้รับอนุญาตในระบบ.

มาตรการป้องกันที่ 1.4: ใช้การบันทึก DHCP (Dynamic Host Configuration Protocol) เพื่ออัปเดตรายการสินทรัพย์ขององค์กร (Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory):

Asset Type: Devices	Security Function: Identify		IG2 IG3

ใช้การบันทึก DHCP บน เซิร์ฟเวอร์ DHCP หรือเครื่องมือการจัดการที่อยู่ IP (IP Address Management Tools) เพื่ออัปเดตรายการสินทรัพย์ขององค์กร

การดำเนินการ: ทบทวนและใช้บันทึก DHCP เพื่อนำข้อมูลมา อัปเดตรายการสินทรัพย์ขององค์กร ทุกสัปดาห์ หรือบ่อยกว่านั้น

เป้าหมาย: เพื่อให้สามารถติดตามและอัปเดตสินทรัพย์ที่เชื่อมต่อกับเครือข่ายได้อย่างแม่นยำและทันเวลาผ่านการใช้ข้อมูลจากการบันทึก DHCP.

มาตรการป้องกันที่ 1.5: ใช้ เครื่องมือค้นหาแบบพาสซีฟ (Use a Passive Asset Discovery Tool):

Asset Type: Devices	Security Function: Detect		IG3

ใช้ **เครื่องมือค้นหาแบบพาสซีฟ (Passive Discovery Tool)** เพื่อตรวจสอบและระบุสินทรัพย์ที่เชื่อมต่อกับเครือข่ายขององค์กร

การดำเนินการ: ทบทวนและใช้ผลการสแกนจากเครื่องมือค้นหาแบบพาสซีฟเพื่อ **อัปเดตรายการสินทรัพย์ขององค์กร** อย่างน้อย **สัปดาห์ละครั้ง** หรือบ่อยกว่านั้น

เป้าหมาย: เพื่อสนับสนุนการจัดการรายการสินทรัพย์ด้วยข้อมูลที่ได้จากการค้นหาแบบพาสซีฟ ซึ่งลดความเสี่ยงจากสินทรัพย์ที่ไม่ได้รับการตรวจสอบหรือควบคุม.

CONTROL 2

การจัดทำ และควบคุมรายการทรัพย์สินซอฟต์แวร์ (Inventory and Control of Software Assets Overview)

Safeguards: 7	IG1: 3/7	IG2: 6/7	IG3: 7/7

ภาพรวม (Overview):

จัดการอย่างกระตือรือร้น (สำรวจ, ติดตาม, และแก้ไข) ซอฟต์แวร์ทั้งหมด (ระบบปฏิบัติการและแอปพลิเคชัน) บนเครือข่าย เพื่อให้มั่นใจว่าเฉพาะซอฟต์แวร์ที่ได้รับอนุญาตเท่านั้นที่ติดตั้งและสามารถทำงานได้ และป้องกันไม่ให้ซอฟต์แวร์ที่ไม่ได้รับอนุญาตหรือตรวจสอบไม่ได้ถูกติดตั้งหรือทำงาน

เหตุใดการควบคุมนี้จึงสำคัญ? (Why is this Control critical?):

การจัดทำรายการซอฟต์แวร์ที่ครบถ้วนเป็นรากฐานสำคัญในการป้องกันการโจมตี

การป้องกันช่องโหว่:

- ผู้โจมตีมักสแกนหาเป้าหมายที่มีช่องโหว่ในซอฟต์แวร์เพื่อนำไปใช้โจมตี เช่น การเปิดเว็บไซต์หรือไฟล์แนบที่เป็นอันตรายผ่านเบราว์เซอร์ที่มีช่องโหว่ อาจทำให้ผู้โจมตีติดตั้งโปรแกรมที่ไม่พึงประสงค์ เช่น Backdoor หรือ Bot และใช้ช่องทางนี้เพื่อควบคุมระบบในระยะยาว

การอัปเดตและแพตช์:

- การอัปเดตและแพตช์ซอฟต์แวร์เป็นหนึ่งในวิธีป้องกันสำคัญ
- หากไม่มีรายการซอฟต์แวร์ครบถ้วน องค์กรไม่สามารถระบุได้ว่ามีซอฟต์แวร์ที่มีช่องโหว่หรือไม่ หรืออาจเกิดการละเมิดลิขสิทธิ์

การป้องกัน Zero-Day Exploits:

- การโจมตีด้วย Zero-Day Exploits ใช้ประโยชน์จากช่องโหว่ที่ยังไม่มีแพตช์
- หากองค์กรมีรายการซอฟต์แวร์ที่ครบถ้วน สามารถใช้มาตรการชั่วคราวเพื่อป้องกันการโจมตีจนกว่าแพตช์จะพร้อมใช้งาน

การลดความเสี่ยงที่ไม่จำเป็น:

- การจัดการซอฟต์แวร์ช่วยลดความเสี่ยงที่ไม่จำเป็น เช่น การลบซอฟต์แวร์เริ่มต้นที่ไม่มีความจำเป็นและเพิ่มความเสี่ยงด้านความปลอดภัย

กระบวนการและเครื่องมือ (Procedures and Tools):

การใช้ Allowlisting:

- ใช้เครื่องมือ Allowlisting เชิงพาณิชย์หรือเครื่องมือการป้องกันการทำงานของแอปพลิเคชันที่รวมอยู่ในซอฟต์แวร์ป้องกันมัลแวร์หรือระบบปฏิบัติการ

เครื่องมือจัดการซอฟต์แวร์:

- เครื่องมือเชิงพาณิชย์มีให้เลือกมากมายและสามารถตรวจสอบซอฟต์แวร์ทั่วไปในองค์กร
- ดึงข้อมูลระดับการอัปเดตของแต่ละโปรแกรมเพื่อตรวจสอบว่าเป็นเวอร์ชันล่าสุด

การกำหนด Allowlisting แบบกำหนดเอง:

- อนุญาตให้สร้าง Allowlisting ตามตำแหน่งไฟล์, แฮช (Hash), หรือกฎอื่นๆ
- สามารถตั้งค่ากฎเพื่อควบคุมการใช้งานซอฟต์แวร์ในช่วงเวลาหรือสำหรับผู้ใช้งานบางกลุ่ม

การจัดการแอปพลิเคชันที่ไม่ได้รับอนุมัติ:

- บางเครื่องมือสามารถแยกแอปพลิเคชันที่ไม่มีอันตรายแต่ไม่ได้รับอนุมัติ และให้ผู้ดูแลระบบตั้งค่ากฎเฉพาะ

การจัดทำรายการซอฟต์แวร์ที่ครบถ้วนและการใช้งานเครื่องมือที่เหมาะสมช่วยให้องค์กรลดความเสี่ยงด้านความปลอดภัยและป้องกันการโจมตีอย่างมีประสิทธิภาพ.

คำแนะนำเฉพาะด้าน (Specific Guidance):

- **คำแนะนำสำหรับระบบคลาวด์ (Cloud-Specific Guidance):**
  ดูคู่มือ CIS Controls Cloud Companion Guide ได้ที่:
  https://www.cisecurity.org/controls/v8/
- **คำแนะนำสำหรับแท็บเล็ตและสมาร์ทโฟน (Tablet and Smartphone Guidance):**
  ดูคู่มือ CIS Controls Mobile Companion Guide ได้ที่:
  https://www.cisecurity.org/controls/v8/
- **คำแนะนำสำหรับ IoT (IoT Guidance):**
  ดูคู่มือ CIS Controls Internet of Things Companion Guide ได้ที่:
  https://www.cisecurity.org/controls/v8/
- **คำแนะนำสำหรับระบบควบคุมในอุตสาหกรรม (Industrial Control Systems - ICS):**
  ดูคู่มือ CIS Controls ICS Implementation Guide ได้ที่:
  https://www.cisecurity.org/controls/v8/

มาตรการป้องกัน (Safeguards)

มาตรการป้องกันที่ 2.1: การจัดตั้งและรักษารายการซอฟต์แวร์ (Establish and Maintain a Software Inventory)

Asset Type: Software	Security Function: Identify		IG1 IG2 IG3

จัดตั้งและรักษารายการซอฟต์แวร์ที่ได้รับอนุญาตทั้งหมดที่ติดตั้งบนทรัพย์สินขององค์กร โดยรายการซอฟต์แวร์ต้องประกอบด้วยข้อมูลดังนี้:

- ชื่อซอฟต์แวร์ (Title)
- ผู้ผลิต (Publisher)
- วันที่ติดตั้งหรือเริ่มใช้งานครั้งแรก (Initial Install/Use Date)
- วัตถุประสงค์ทางธุรกิจ (Business Purpose)

ข้อมูลเพิ่มเติมที่ควรรวมไว้ (เมื่อเหมาะสม):

- Uniform Resource Locator (URL)
- แหล่งดาวน์โหลด (App Store)
- เวอร์ชัน (Version)
- กลไกการติดตั้ง (Deployment Mechanism)
- วันที่เลิกใช้งาน (Decommission Date)
- จำนวนใบอนุญาต (Number of Licenses)

ความถี่ในการอัปเดต: ตรวจสอบและอัปเดตรายการซอฟต์แวร์ทุก 6 เดือน หรือ บ่อยกว่านั้น

เป้าหมาย: เพื่อให้มั่นใจว่าซอฟต์แวร์ที่ใช้งานอยู่ได้รับการจัดการอย่างเหมาะสม ป้องกันการละเมิดลิขสิทธิ์ และลดความเสี่ยงจากซอฟต์แวร์ที่ไม่ได้รับการตรวจสอบ.

มาตรการป้องกันที่ 2.2: ตรวจสอบให้แน่ใจว่าซอฟต์แวร์ที่ได้รับอนุญาตยังคงได้รับการสนับสนุน (Ensure Authorized Software is Currently Supported)

Asset Type: Software	Security Function: Identify		IG1 IG2 IG3

ตรวจสอบให้แน่ใจว่าซอฟต์แวร์ที่ได้รับการกำหนดว่าได้รับอนุญาตในรายการซอฟต์แวร์ขององค์กร ยังคงเป็นซอฟต์แวร์ที่ได้รับการสนับสนุน:

กรณีซอฟต์แวร์ที่ไม่ได้รับการสนับสนุน แต่ยังจำเป็นต่อพันธกิจขององค์กร:

- จัดทำเอกสารข้อยกเว้น (Exception Documentation)
- ระบุมาตรการลดความเสี่ยง (Mitigating Controls)
- ยอมรับความเสี่ยงที่เหลืออยู่ (Residual Risk Acceptance)

กรณีซอฟต์แวร์ที่ไม่ได้รับการสนับสนุน และไม่มีเอกสารข้อยกเว้น:

- ระบุซอฟต์แวร์นั้นเป็น ไม่ได้รับอนุญาต (Unauthorized)

ความถี่ในการตรวจสอบ: ตรวจสอบรายการซอฟต์แวร์เพื่อยืนยันการสนับสนุนซอฟต์แวร์อย่างน้อย เดือนละครั้ง หรือ บ่อยกว่านั้น

เป้าหมาย:เพื่อป้องกันความเสี่ยงด้านความปลอดภัยที่เกิดจากซอฟต์แวร์ที่ไม่ได้รับการสนับสนุน และสนับสนุนการใช้งานซอฟต์แวร์ที่ปลอดภัยและทันสมัยในองค์กร.

มาตรการป้องกันที่ 2.3: การจัดการซอฟต์แวร์ที่ไม่ได้รับอนุญาต (Address Unauthorized Software)

Asset Type: Software	Security Function: Identify		IG1 IG2 IG3

ตรวจสอบให้แน่ใจว่าซอฟต์แวร์ที่ไม่ได้รับอนุญาตถูกดำเนินการจัดการดังนี้:

- นำออกจากการใช้งาน บนทรัพย์สินขององค์กร
- หรือ จัดทำเอกสารข้อยกเว้น (Documented Exception)

ความถี่ในการตรวจสอบ:ตรวจสอบซอฟต์แวร์ที่ไม่ได้รับอนุญาตอย่างน้อย เดือนละครั้ง หรือ บ่อยกว่านั้น

เป้าหมาย:เพื่อป้องกันการใช้งานซอฟต์แวร์ที่อาจก่อให้เกิดความเสี่ยงด้านความปลอดภัย และส่งเสริมการปฏิบัติตามมาตรฐานความปลอดภัยในองค์กร.

มาตรการป้องกันที่ 2.4: ใช้เครื่องมือการจัดทำรายการซอฟต์แวร์แบบอัตโนมัติ (Utilize Automated Software Inventory Tools)

Asset Type: Devices	Security Function: Detect		IG2 IG3

ใช้ เครื่องมือการจัดทำรายการซอฟต์แวร์แบบอัตโนมัติ (Automated Software Inventory Tools) ให้ครอบคลุมทั่วทั้งองค์กร เพื่อช่วยให้การค้นหาและบันทึกซอฟต์แวร์ที่ติดตั้งเป็นไปโดยอัตโนมัติ

เป้าหมาย: เพื่อเพิ่มความแม่นยำและประสิทธิภาพในการจัดการรายการซอฟต์แวร์ ลดความเสี่ยงจากข้อผิดพลาดที่อาจเกิดจากกระบวนการด้วยมือ และเพิ่มความสามารถในการติดตามซอฟต์แวร์ที่ติดตั้งในระบบอย่างต่อเนื่อง.

มาตรการป้องกันที่ 2.5: การกำหนดรายชื่อซอฟต์แวร์ที่ได้รับอนุญาต (Allowlist Authorized Software)

Asset Type: Devices	Security Function: Protect		IG2 IG3

ใช้ การควบคุมทางเทคนิค เช่น การกำหนดรายชื่อซอฟต์แวร์ที่ได้รับอนุญาต (Application Allowlisting) เพื่อให้แน่ใจว่ามีเพียงซอฟต์แวร์ที่ได้รับอนุญาตเท่านั้นที่สามารถทำงานหรือเข้าถึงได้

ความถี่ในการประเมิน: ประเมินรายการซอฟต์แวร์ที่ได้รับอนุญาตทุก 6 เดือน หรือบ่อยกว่านั้น

เป้าหมาย: เพื่อป้องกันการรันซอฟต์แวร์ที่ไม่ได้รับอนุญาต ลดความเสี่ยงจากมัลแวร์หรือการโจมตีทางไซเบอร์ และสนับสนุนความมั่นคงปลอดภัยของระบบโดยรวม.

มาตรการป้องกันที่ 2.6: การกำหนดรายชื่อไลบรารีที่ได้รับอนุญาต (Allowlist Authorized Libraries)

Asset Type: Devices	Security Function: Protect		IG2 IG3

ใช้ การควบคุมทางเทคนิค เพื่อให้มั่นใจว่าเฉพาะไลบรารีซอฟต์แวร์ที่ได้รับอนุญาต เช่น ไฟล์ .dll, .ocx, และ .so เท่านั้นที่สามารถโหลดเข้าสู่กระบวนการของระบบได้

บล็อกไลบรารีที่ไม่ได้รับอนุญาต ไม่ให้โหลดเข้าสู่กระบวนการของระบบ

ความถี่ในการประเมิน: ประเมินรายการไลบรารีที่ได้รับอนุญาตทุก 6 เดือน หรือ บ่อยกว่านั้น

เป้าหมาย: เพื่อป้องกันการรัน หรือโหลดไลบรารีที่อาจก่อให้เกิดความเสี่ยงด้านความปลอดภัย สนับสนุนการป้องกันระบบจากช่องโหว่และการโจมตีโดยใช้ไลบรารีที่ไม่ได้รับอนุญาต.

มาตรการป้องกันที่ 2.7: การกำหนดรายชื่อสคริปต์ที่ได้รับอนุญาต (Allowlist Authorized Scripts)

Asset Type: Devices	Security Function: Protect		IG3

ใช้ การควบคุมทางเทคนิค เช่น ลายเซ็นดิจิทัล (Digital Signatures) และ การควบคุมเวอร์ชัน (Version Control) เพื่อให้มั่นใจว่าเฉพาะสคริปต์ที่ได้รับอนุญาต เช่น ไฟล์ .ps1 และ .py เท่านั้นที่สามารถรันได้

บล็อกสคริปต์ที่ไม่ได้รับอนุญาต ไม่ให้รันในระบบ

ความถี่ในการประเมิน:ประเมินรายการสคริปต์ที่ได้รับอนุญาตทุก 6 เดือน หรือ บ่อยกว่านั้น

เป้าหมาย: เพื่อป้องกันการรันสคริปต์ที่อาจมีความเสี่ยงด้านความปลอดภัย ลดโอกาสที่ระบบจะถูกโจมตีผ่านสคริปต์ที่ไม่ได้รับอนุญาต และส่งเสริมการจัดการระบบที่ปลอดภัยและมีประสิทธิภาพ.

CONTROL 3

การปกป้องข้อมูล (Data Protection)

Safeguards: 5	IG1: 6/14	IG2: 12/14	IG3: 14/14

ภาพรวม (Overview):

จัดการอย่างกระตือรือร้น (สำรวจ, ติดตาม, และแก้ไข) ซอฟต์แวร์ทั้งหมด (ระบบปฏิบัติการและแอปพลิเคชัน) บนเครือข่าย เพื่อให้มั่นใจว่าเฉพาะซอฟต์แวร์ที่ได้รับอนุญาตเท่านั้นที่ติดตั้งและสามารถทำงานได้ และป้องกันไม่ให้ซอฟต์แวร์ที่ไม่ได้รับอนุญาตหรือตรวจสอบไม่ได้ถูกติดตั้งหรือทำงาน

เหตุใดการควบคุมนี้จึงสำคัญ? (Why is this Control critical?):

การจัดทำรายการซอฟต์แวร์ที่ครบถ้วนเป็นรากฐานสำคัญในการป้องกันการโจมตี

การป้องกันช่องโหว่:

- ผู้โจมตีมักสแกนหาเป้าหมายที่มีช่องโหว่ในซอฟต์แวร์เพื่อนำไปใช้โจมตี เช่น การเปิดเว็บไซต์หรือไฟล์แนบที่เป็นอันตรายผ่านเบราว์เซอร์ที่มีช่องโหว่ อาจทำให้ผู้โจมตีติดตั้งโปรแกรมที่ไม่พึงประสงค์ เช่น Backdoor หรือ Bot และใช้ช่องทางนี้เพื่อควบคุมระบบในระยะยาว

การอัปเดตและแพตช์:

- การอัปเดตและแพตช์ซอฟต์แวร์เป็นหนึ่งในวิธีป้องกันสำคัญ
- หากไม่มีรายการซอฟต์แวร์ครบถ้วน องค์กรไม่สามารถระบุได้ว่ามีซอฟต์แวร์ที่มีช่องโหว่หรือไม่ หรืออาจเกิดการละเมิดลิขสิทธิ์

การป้องกัน Zero-Day Exploits:

- การโจมตีด้วย Zero-Day Exploits ใช้ประโยชน์จากช่องโหว่ที่ยังไม่มีแพตช์
- หากองค์กรมีรายการซอฟต์แวร์ที่ครบถ้วน สามารถใช้มาตรการชั่วคราวเพื่อป้องกันการโจมตีจนกว่าแพตช์จะพร้อมใช้งาน

การลดความเสี่ยงที่ไม่จำเป็น:

- การจัดการซอฟต์แวร์ช่วยลดความเสี่ยงที่ไม่จำเป็น เช่น การลบซอฟต์แวร์เริ่มต้นที่ไม่มีความจำเป็นและเพิ่มความเสี่ยงด้านความปลอดภัย

กระบวนการและเครื่องมือ (Procedures and Tools):

การใช้ Allowlisting:

- ใช้เครื่องมือ Allowlisting เชิงพาณิชย์หรือเครื่องมือการป้องกันการทำงานของแอปพลิเคชันที่รวมอยู่ในซอฟต์แวร์ป้องกันมัลแวร์หรือระบบปฏิบัติการ

เครื่องมือจัดการซอฟต์แวร์:

- เครื่องมือเชิงพาณิชย์มีให้เลือกมากมายและสามารถตรวจสอบซอฟต์แวร์ทั่วไปในองค์กร
- ดึงข้อมูลระดับการอัปเดตของแต่ละโปรแกรมเพื่อตรวจสอบว่าเป็นเวอร์ชันล่าสุด

การกำหนด Allowlisting แบบกำหนดเอง:

- อนุญาตให้สร้าง Allowlisting ตามตำแหน่งไฟล์, แฮช (Hash), หรือกฎอื่นๆ
- สามารถตั้งค่ากฎเพื่อควบคุมการใช้งานซอฟต์แวร์ในช่วงเวลาหรือสำหรับผู้ใช้งานบางกลุ่ม

การจัดการแอปพลิเคชันที่ไม่ได้รับอนุมัติ:

- บางเครื่องมือสามารถแยกแอปพลิเคชันที่ไม่มีอันตรายแต่ไม่ได้รับอนุมัติ และให้ผู้ดูแลระบบตั้งค่ากฎเฉพาะ

แหล่งข้อมูลเพิ่มเติม:

NIST® SP 800-88r1 Guides for Media Sanitization:

ดาวน์โหลดเอกสาร

NIST® FIPS 140-2:

ดาวน์โหลดเอกสาร

NIST® FIPS 140-3:

ดาวน์โหลดเอกสาร

คู่มือคำแนะนำเฉพาะด้าน:

ระบบคลาวด์ (Cloud): CIS Controls Cloud Companion Guide

แท็บเล็ตและสมาร์ทโฟน: CIS Controls Mobile Companion Guide

มาตรการป้องกัน (Safeguards)

มาตรการป้องกันที่ 3.1: การจัดตั้งและรักษารายการซอฟต์แวร์ (Establish and Maintain a Software Inventory)

Asset Type: Data	Security Function: Govern		IG1 IG2 IG3

จัดตั้งและรักษากระบวนการจัดการข้อมูลที่มีการบันทึกไว้อย่างเป็นทางการ โดยในกระบวนการควรมีการกำหนดและระบุ:

- ความอ่อนไหวของข้อมูล (Data Sensitivity)
- เจ้าของข้อมูล (Data Owner)
- การจัดการข้อมูล (Handling of Data)
- ระยะเวลาการเก็บรักษาข้อมูล (Data Retention Limits)
- ข้อกำหนดในการกำจัดข้อมูล (Disposal Requirements)

กระบวนการนี้ควรเป็นไปตามมาตรฐานความอ่อนไหวและการเก็บรักษาขององค์กร

ความถี่ในการตรวจสอบและอัปเดต:ตรวจสอบและอัปเดตเอกสาร ทุกปี หรือเมื่อมีการเปลี่ยนแปลงสำคัญในองค์กรที่อาจส่งผลต่อมาตรการนี้

เป้าหมาย: เพื่อให้มั่นใจว่าข้อมูลได้รับการจัดการอย่างเหมาะสมและปลอดภัยตลอดวงจรชีวิต รวมถึงลดความเสี่ยงจากการละเมิดความปลอดภัยหรือการไม่ปฏิบัติตามกฎระเบียบ.

มาตรการป้องกันที่ 3.2: การจัดตั้งและรักษารายการข้อมูล (Establish and Maintain a Data Inventory)

Asset Type: Data	Security Function: Identify		IG1 IG2 IG3

จัดตั้งและรักษารายการข้อมูล (Data Inventory) ตามกระบวนการจัดการข้อมูลขององค์กร โดยให้ความสำคัญกับข้อมูลที่อ่อนไหว (Sensitive Data) อย่างน้อยที่สุด

ความถี่ในการตรวจสอบและอัปเดต: ตรวจสอบและอัปเดตรายการข้อมูล อย่างน้อยปีละครั้ง โดยให้ความสำคัญเป็นพิเศษกับข้อมูลที่อ่อนไหว

เป้าหมาย: เพื่อให้มั่นใจว่าข้อมูลขององค์กรได้รับการระบุและจัดการอย่างเหมาะสม โดยเฉพาะข้อมูลที่อ่อนไหว ลดความเสี่ยงจากการสูญเสียหรือการละเมิดข้อมูล.

มาตรการป้องกันที่ 3.3: การกำหนดรายการควบคุมการเข้าถึงข้อมูล (Configure Data Access Control Lists)

Asset Type: Data	Security Function: Protect		IG1 IG2 IG3

กำหนด รายการควบคุมการเข้าถึงข้อมูล (Data Access Control Lists) ตามหลักการความจำเป็นในการรู้ (Need to Know)

- ใช้รายการควบคุมการเข้าถึงข้อมูล หรือที่เรียกว่าการอนุญาตการเข้าถึง (Access Permissions)
- นำไปใช้กับระบบไฟล์ในเครื่อง (Local File Systems), ระบบไฟล์ระยะไกล (Remote File Systems), ฐานข้อมูล (Databases), และแอปพลิเคชัน (Applications)

เป้าหมาย: เพื่อจำกัดการเข้าถึงข้อมูลให้เฉพาะบุคคลที่มีความจำเป็นในการใช้งาน ลดความเสี่ยงจากการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต และเพิ่มความปลอดภัยให้กับข้อมูลในระบบ.

มาตรการป้องกันที่ 3.4: การบังคับใช้การเก็บรักษาข้อมูล (Enforce Data Retention)

Asset Type: Data	Security Function: Protect	IG1	IG2	IG3

เก็บรักษาข้อมูลตามกระบวนการจัดการข้อมูลที่มีการบันทึกไว้อย่างเป็นทางการขององค์กร โดยการเก็บรักษาข้อมูลต้องกำหนด:

- ระยะเวลาเก็บรักษาขั้นต่ำ (Minimum Retention Timelines)
- ระยะเวลาเก็บรักษาสูงสุด (Maximum Retention Timelines)

เป้าหมาย:

- เพื่อให้การเก็บรักษาข้อมูลสอดคล้องกับนโยบายขององค์กรและข้อกำหนดทางกฎหมาย ลดความเสี่ยงจากการเก็บข้อมูลเกินความจำเป็นหรือละเมิดกฎระเบียบเกี่ยวกับการเก็บรักษาข้อมูล.

มาตรการป้องกันที่ 3.5: การกำจัดข้อมูลอย่างปลอดภัย (Securely Dispose of Data)

Asset Type: Data	Security Function: Protect	IG1	IG2	IG3

กำจัดข้อมูลอย่างปลอดภัยตามที่ระบุไว้ในกระบวนการจัดการข้อมูลขององค์กรที่มีการบันทึกไว้อย่างเป็นทางการ โดย:

- มั่นใจว่ากระบวนการและวิธีการกำจัดข้อมูล สอดคล้องกับระดับความอ่อนไหวของข้อมูล

เป้าหมาย: เพื่อป้องกันข้อมูลที่ละเอียดอ่อนจากการถูกเข้าถึงหรือใช้งานโดยไม่ได้รับอนุญาตหลังจากถูกกำจัด ช่วยลดความเสี่ยงด้านความปลอดภัย และปฏิบัติตามข้อกำหนดด้านกฎหมายและกฎระเบียบ.

มาตรการป้องกันที่ 3.6: การเข้ารหัสข้อมูลในอุปกรณ์ผู้ใช้งาน (Encrypt Data on End-User Devices)

Asset Type: Data	Security Function: Protect	IG1	IG2	IG3

เข้ารหัสข้อมูลในอุปกรณ์ของผู้ใช้งาน (End-User Devices) ที่มีข้อมูลที่อ่อนไหว เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

ตัวอย่างการดำเนินการ:

- Windows BitLocker®
- Apple FileVault®
- Linux® dm-crypt

เป้าหมาย: เพื่อเพิ่มความปลอดภัยให้กับข้อมูลในอุปกรณ์ผู้ใช้งาน โดยเฉพาะข้อมูลที่อ่อนไหว ช่วยลดความเสี่ยงจากการโจรกรรมอุปกรณ์หรือการเข้าถึงโดยไม่ได้รับอนุญาต.

มาตรการป้องกันที่ 3.7: การจัดตั้งและรักษาระบบการจัดประเภทข้อมูล (Establish and Maintain a Data Classification Scheme)

Asset Type: Data	Security Function: Identify		IG2 IG3

จัดตั้งและรักษาระบบการจัดประเภทข้อมูล (Data Classification Scheme) สำหรับองค์กร โดยอาจใช้ป้ายกำกับ (Labels) เช่น:

- “Sensitive” (ข้อมูลอ่อนไหว)
- “Confidential” (ข้อมูลลับ)
- “Public” (ข้อมูลสาธารณะ)

การดำเนินการ:

- จัดประเภทข้อมูลตามป้ายกำกับที่กำหนด
- ทบทวนและปรับปรุงระบบการจัดประเภทข้อมูล ทุกปี หรือเมื่อมีการเปลี่ยนแปลงสำคัญในองค์กรที่อาจส่งผลต่อมาตรการนี้

เป้าหมาย: เพื่อสนับสนุนการจัดการข้อมูลให้เหมาะสมตามระดับความอ่อนไหวและความสำคัญ ลดความเสี่ยงจากการเข้าถึงหรือใช้งานข้อมูลโดยไม่ได้รับอนุญาต และปฏิบัติตามข้อกำหนดด้านความปลอดภัย.

มาตรการป้องกันที่ 3.8: การไหลของข้อมูลในเอกสาร (Document Data Flows)

Asset Type: Data	Security Function: Identify		IG2 IG3

บันทึกการไหลของข้อมูล (Data Flows) โดยการบันทึกนี้ควรรวมถึง:

- การไหลของข้อมูลที่เกี่ยวข้องกับผู้ให้บริการ (Service Provider Data Flows)
- อิงตามกระบวนการจัดการข้อมูลขององค์กร

ความถี่ในการตรวจสอบและอัปเดต:

- ทบทวนและปรับปรุงเอกสารการไหลของข้อมูล ทุกปี หรือ
- เมื่อมีการเปลี่ยนแปลงสำคัญในองค์กรที่อาจส่งผลต่อมาตรการนี้

เป้าหมาย: เพื่อให้เข้าใจถึงการเคลื่อนที่ของข้อมูลในระบบอย่างชัดเจน สนับสนุนการจัดการข้อมูลอย่างมีประสิทธิภาพ ลดความเสี่ยงจากการละเมิดข้อมูล และเสริมสร้างการปฏิบัติตามข้อกำหนดด้านความปลอดภัย.

มาตรการป้องกันที่ 3.9: การเข้ารหัสข้อมูลบนสื่อแบบถอดได้ (Encrypt Data on Removable Media)

Asset Type: Data	Security Function: Protect		IG2 IG3

ดำเนินการเข้ารหัสข้อมูลที่จัดเก็บอยู่บน สื่อแบบถอดได้ (Removable Media) เช่น USB Drives, External Hard Drives, SD Cards เป็นต้น

เป้าหมาย: เพื่อป้องกันการเข้าถึงข้อมูลที่ไม่ได้รับอนุญาต หากสื่อแบบถอดได้สูญหายหรือถูกโจรกรรม เพิ่มความปลอดภัยสำหรับข้อมูลที่อ่อนไหวและช่วยลดความเสี่ยงด้านความปลอดภัย.

มาตรการป้องกันที่ 3.10: การเข้ารหัสข้อมูลที่อ่อนไหวขณะส่งผ่าน (Encrypt Sensitive Data in Transit)

Asset Type: Data	Security Function: Protect		IG2 IG3

ดำเนินการเข้ารหัสข้อมูลที่อ่อนไหวขณะส่งผ่านระบบเครือข่าย (In Transit) เพื่อป้องกันการดักจับหรือการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

ตัวอย่างการดำเนินการ:

- Transport Layer Security (TLS)
- Open Secure Shell (OpenSSH)

เป้าหมาย: เพื่อเพิ่มความปลอดภัยสำหรับข้อมูลที่ส่งผ่านเครือข่าย ลดความเสี่ยงจากการโจมตีแบบดักจับข้อมูล (Man-in-the-Middle) และสนับสนุนการปฏิบัติตามข้อกำหนดด้านความปลอดภัยของข้อมูล.

มาตรการป้องกันที่ 3.11: การเข้ารหัสข้อมูลที่อ่อนไหวขณะจัดเก็บ (Encrypt Sensitive Data at Rest)

Asset Type: Data	Security Function: Protect		IG2 IG3

ดำเนินการเข้ารหัสข้อมูลที่อ่อนไหวขณะจัดเก็บ (At Rest) บนเซิร์ฟเวอร์, แอปพลิเคชัน , และฐานข้อมูล เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

ตัวอย่างการดำเนินการ:

- การเข้ารหัสในระดับชั้นจัดเก็บข้อมูล (Storage-Layer Encryption): หรือที่เรียกว่า การเข้ารหัสฝั่งเซิร์ฟเวอร์ (Server-Side Encryption) ซึ่งถือเป็นข้อกำหนดขั้นต่ำของมาตรการนี้
- การเข้ารหัสในระดับแอปพลิเคชัน (Application-Layer Encryption): หรือที่เรียกว่า การเข้ารหัสฝั่งไคลเอนต์ (Client-Side Encryption) ซึ่งป้องกันการเข้าถึงข้อมูลแบบ plain-text แม้จะสามารถเข้าถึงอุปกรณ์จัดเก็บข้อมูลได้

เป้าหมาย: เพื่อปกป้องข้อมูลที่อ่อนไหวขณะจัดเก็บ ลดความเสี่ยงจากการโจรกรรมข้อมูลหรือการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต และสนับสนุนการปฏิบัติตามข้อกำหนดด้านความปลอดภัยของข้อมูล..

มาตรการป้องกันที่ 3.12: แยกการประมวลผลและการจัดเก็บข้อมูลตามความอ่อนไหว (Segment Data Processing and Storage Based on Sensitivity)

Asset Type: Data	Security Function: Protect		IG2 IG3

แยกการประมวลผลและการจัดเก็บข้อมูลตามระดับความอ่อนไหวของข้อมูล (Data Sensitivity) โดย:

- หลีกเลี่ยงการประมวลผลข้อมูลที่อ่อนไหวบนทรัพย์สินขององค์กรที่ออกแบบมาสำหรับข้อมูลที่มีความอ่อนไหวต่ำกว่า

เป้าหมาย: เพื่อป้องกันความเสี่ยงจากการผสมข้อมูลที่มีระดับความอ่อนไหวต่างกัน ลดความเสี่ยงของการเข้าถึงข้อมูลที่ไม่ได้รับอนุญาต และเสริมสร้างการควบคุมด้านความปลอดภัยของข้อมูลในองค์กร.

มาตรการป้องกันที่ 3.13: การติดตั้งโซลูชันป้องกันการสูญหายของข้อมูล (Deploy a Data Loss Prevention Solution)

Asset Type: Data	Security Function: Protect		IG3

ติดตั้งเครื่องมืออัตโนมัติ เช่น โซลูชันป้องกันการสูญหายของข้อมูล (Host-Based Data Loss Prevention - DLP) เพื่อ:

- ระบุข้อมูลที่อ่อนไหวทั้งหมดที่ถูกจัดเก็บ, ประมวลผล หรือส่งผ่านทรัพย์สินขององค์กร
- ครอบคลุมทั้งข้อมูลที่อยู่ในองค์กรและข้อมูลที่ผู้ให้บริการระยะไกลจัดการ
- อัปเดตรายการข้อมูลขององค์กร (Data Inventory)

เป้าหมาย: เพื่อป้องกันการสูญหายของข้อมูลที่อ่อนไหวและเพิ่มความปลอดภัยในการจัดการข้อมูลสำคัญขององค์กร

มาตรการป้องกันที่ 3.14: การบันทึกการเข้าถึงข้อมูลที่อ่อนไหว (Log Sensitive Data Access)

Asset Type: Data	Security Function: Protect		IG3

บันทึกการเข้าถึงข้อมูลที่อ่อนไหว โดยรวมถึง:

- การแก้ไขข้อมูล
- การกำจัดข้อมูล

เป้าหมาย: เพื่อสนับสนุนการตรวจสอบและติดตามการเข้าถึงข้อมูลที่อ่อนไหว ลดความเสี่ยงจากการใช้งานโดยไม่ได้รับอนุญาต และเพิ่มความโปร่งใสในการจัดการข้อมูลขององค์กร.

CONTROL 4

การกำหนดค่าความปลอดภัยของทรัพย์สินและซอฟต์แวร์ขององค์กร (Secure Configuration of Enterprise Assets and Software)

Safeguards: 12	IG1: 7/12	IG2: 11/12	IG3: 12/12

ภาพรวม (Overview):

จัดตั้งและรักษาการกำหนดค่าความปลอดภัยของทรัพย์สินขององค์กร (อุปกรณ์ผู้ใช้งาน รวมถึงอุปกรณ์พกพาและมือถือ; อุปกรณ์เครือข่าย; อุปกรณ์ที่ไม่ใช่ระบบคอมพิวเตอร์/IoT; และเซิร์ฟเวอร์) และซอฟต์แวร์ (ระบบปฏิบัติการและแอปพลิเคชัน)

เหตุใดการควบคุมนี้จึงสำคัญ? (Why is this Control critical?):

1 การกำหนดค่าเริ่มต้น (Default Configurations):

อุปกรณ์และซอฟต์แวร์ที่ส่งมาจากผู้ผลิตหรือผู้จำหน่ายมักตั้งค่าเพื่อความสะดวกในการติดตั้งและใช้งาน แทนที่จะเน้นความปลอดภัย เช่น:

- เปิดใช้งานบริการและพอร์ตเริ่มต้น
- บัญชีหรือรหัสผ่านเริ่มต้น
- การตั้งค่า DNS ที่กำหนดไว้ล่วงหน้า
- การใช้งานโปรโตคอลรุ่นเก่า (ที่มีช่องโหว่)
- การติดตั้งซอฟต์แวร์ที่ไม่จำเป็น

2 การอัปเดตและการจัดการตลอดวงจรชีวิต (Lifecycle Management):

การอัปเดตการกำหนดค่าความปลอดภัยต้องถูกจัดการและบันทึกผ่านกระบวนการจัดการการกำหนดค่า (Configuration Management Workflow) เพื่อ:

- รักษาบันทึกสำหรับตรวจสอบความสอดคล้อง
- รองรับการตอบสนองต่อเหตุการณ์ (Incident Response)
- สนับสนุนการตรวจสอบ (Audit)

3 บทบาทของผู้ให้บริการ (Service Providers):

ผู้ให้บริการโครงสร้างพื้นฐานมักไม่ได้ตั้งค่าความปลอดภัยโดยค่าเริ่มต้น เพื่อให้ลูกค้าสามารถปรับใช้การตั้งค่าความปลอดภัยได้เอง ซึ่งอาจทำให้เกิดช่องโหว่ เช่น:

- บัญชีหรือรหัสผ่านเริ่มต้น
- การเข้าถึงที่มากเกินความจำเป็น

- บริการที่ไม่จำเป็น

4 การบำรุงรักษาความปลอดภัยอย่างต่อเนื่อง:

แม้จะมีการตั้งค่าความปลอดภัยที่แข็งแกร่งในตอนเริ่มต้น แต่ต้องมีการจัดการอย่างต่อเนื่องเพื่อหลีกเลี่ยงการลดระดับความปลอดภัยเมื่อ:

- มีการอัปเดตหรือแก้ไขซอฟต์แวร์
- รายงานช่องโหว่ใหม่
- มีการปรับเปลี่ยนการตั้งค่าเพื่อสนับสนุนซอฟต์แวร์ใหม่หรือข้อกำหนดทางปฏิบัติการ

กระบวนการและเครื่องมือ (Procedures and Tools):

องค์กรสามารถใช้ มาตรฐานความปลอดภัย (Security Baselines) ที่มีอยู่สำหรับแต่ละระบบ โดยเริ่มจาก คู่มือและรายการตรวจสอบความปลอดภัย (Security Benchmarks, Guides, or Checklists) ที่ได้รับการพัฒนา, ตรวจสอบ, และสนับสนุนในระดับสาธารณะ

ทรัพยากรที่แนะนำ:

โปรแกรม CIS Benchmarks™ และแนวทางการกำหนดค่าความปลอดภัย

- **CIS Benchmarks™ Program:** http://www.cisecurity.org/cis-benchmarks/
- **National Checklist Program Repository ของ NIST®:** https://nvd.nist.gov/ncp/repository

คำแนะนำในการปรับแต่งและการใช้งาน (Adjustment and Implementation):

องค์กรควรปรับปรุงหรือปรับแต่งมาตรฐานความปลอดภัยพื้นฐานเหล่านี้ (Security Baselines) ให้สอดคล้องกับ:

- นโยบายความปลอดภัยขององค์กร
- ข้อกำหนดของอุตสาหกรรม
- ข้อกำหนดด้านกฎระเบียบของรัฐบาล

หากมีการเบี่ยงเบนจากการกำหนดค่ามาตรฐาน ควรมีการบันทึกเหตุผลเพื่อใช้ในการตรวจสอบหรือการตรวจประเมินในอนาคต

องค์กรขนาดใหญ่หรือซับซ้อนมากขึ้น (Larger or More Complex Enterprises):

ในองค์กรที่ซับซ้อนอาจมีการกำหนดค่าพื้นฐานหลายรูปแบบขึ้นอยู่กับ:

- ข้อกำหนดด้านความปลอดภัย
- การจัดประเภทข้อมูลบนทรัพย์สินขององค์กร

ตัวอย่างขั้นตอนการสร้างรูปแบบการกำหนดค่าความปลอดภัยพื้นฐาน (Secure Baseline Image):

1. กำหนดความเสี่ยงของข้อมูลที่จัดการ/จัดเก็บ: เช่น ความเสี่ยงสูง, ปานกลาง, ต่ำ
2. สร้างสคริปต์การกำหนดค่าความปลอดภัย: เพื่อปรับการตั้งค่าระบบให้สอดคล้องกับข้อกำหนดด้านความปลอดภัย โดยใช้มาตรฐาน เช่น CIS Benchmarks
3. ติดตั้งระบบปฏิบัติการพื้นฐาน (Base OS):
4. อัปเดตแพตช์ระบบปฏิบัติการและความปลอดภัย:
5. ติดตั้งซอฟต์แวร์ แอปพลิเคชัน และเครื่องมือที่เหมาะสม:
6. อัปเดตซอฟต์แวร์ที่ติดตั้ง: จากขั้นตอนที่ 4
7. ติดตั้งสคริปต์การปรับแต่งท้องถิ่น:
8. รันสคริปต์ความปลอดภัยที่สร้างไว้ในขั้นตอนที่ 2: เพื่อปรับระดับความปลอดภัย

9. ใช้เครื่องมือบันทึก/วิเคราะห์การตั้งค่าระบบ (System Setting): สำหรับการตั้งค่าพื้นฐาน
10. ดำเนินการทดสอบคุณภาพด้านความปลอดภัย (QA Test):
11. บันทึกภาพพื้นฐานนี้ (Base Image) ไว้ในตำแหน่งที่ปลอดภัย:

เครื่องมือการจัดการการกำหนดค่า (Configuration Management Tools):

เครื่องมือการจัดการทั้งเชิงพาณิชย์และฟรี เช่น:

CIS Configuration Assessment Tool (CIS-CAT®):
https://learn.cisecurity.org/cis-cat-lite

ฟังก์ชันของเครื่องมือ:

- ตรวจสอบการตั้งค่าของระบบปฏิบัติการและแอปพลิเคชันในเครื่องที่ได้รับการจัดการ
- ระบุการเบี่ยงเบนจากการกำหนดค่าพื้นฐานมาตรฐาน

รูปแบบการใช้งาน:

- Agent-based: ติดตั้งตัวแทน (Agent) ในแต่ละระบบที่มีการจัดการ
- Agentless Inspection: เข้าสู่ระบบทรัพย์สินองค์กรระยะไกลด้วยข้อมูลรับรองผู้ดูแลระบบ
- Hybrid Approach: ใช้ตัวแทนชั่วคราวที่ติดตั้งและลบออกในระหว่างการสแกน

เป้าหมาย: เพื่อช่วยให้องค์กรสามารถรักษารูปแบบการกำหนดค่าความปลอดภัยที่มั่นคง ลดความเสี่ยงจากการโจมตี และสอดคล้องกับนโยบายความปลอดภัย.

มาตรการป้องกัน (Safeguards)

มาตรการป้องกันที่ 4.1: การจัดตั้งและรักษารายการซอฟต์แวร์ (Establish and Maintain a Software Inventory)

Asset Type: Documentation	Security Function: Govern		IG1 IG2 IG3

จัดตั้งและรักษากระบวนการกำหนดค่าความปลอดภัยที่บันทึกไว้อย่างเป็นทางการสำหรับ:

- ทรัพย์สินขององค์กร: เช่น อุปกรณ์ผู้ใช้งาน (รวมถึงอุปกรณ์พกพาและมือถือ), อุปกรณ์ที่ไม่ใช่ระบบคอมพิวเตอร์ (Non-computing/IoT Devices), และเซิร์ฟเวอร์
- ซอฟต์แวร์: เช่น ระบบปฏิบัติการ (Operating Systems) และแอปพลิเคชัน (Applications)

ความถี่ในการตรวจสอบและอัปเดต:

- ทบทวนและปรับปรุงเอกสาร ทุกปี หรือ
- เมื่อมีการเปลี่ยนแปลงสำคัญในองค์กรที่อาจส่งผลกระทบต่อมาตรการนี้

เป้าหมาย: เพื่อให้มั่นใจว่ากระบวนการกำหนดค่าความปลอดภัยขององค์กรได้รับการจัดการและปรับปรุงอย่างต่อเนื่อง รองรับการปฏิบัติตามข้อกำหนดด้านความปลอดภัย และลดความเสี่ยงจากการโจมตีหรือการกำหนดค่าที่ไม่เหมาะสม.

มาตรการป้องกันที่ 4.2: จัดตั้งและรักษากระบวนการกำหนดค่าความปลอดภัยสำหรับโครงสร้างพื้นฐานเครือข่าย (Establish and Maintain a Secure Configuration Process for Network Infrastructure)

Asset Type: Documentation	Security Function: Govern		IG1 IG2 IG3

จัดตั้งและรักษากระบวนการกำหนดค่าความปลอดภัยที่บันทึกไว้อย่างเป็นทางการสำหรับ อุปกรณ์เครือข่าย (Network Devices)

ความถี่ในการตรวจสอบและอัปเดต:

- ทบทวนและปรับปรุงเอกสาร ทุกปี หรือ
- เมื่อมีการเปลี่ยนแปลงสำคัญในองค์กรที่อาจส่งผลกระทบต่อมาตรการนี้

เป้าหมาย: เพื่อให้แน่ใจว่าอุปกรณ์เครือข่ายมีการตั้งค่าความปลอดภัยที่เหมาะสมและได้รับการปรับปรุงเพื่อลดความเสี่ยงด้านความปลอดภัย

มาตรการป้องกันที่ 4.3: กำหนดการล็อกเซสชันอัตโนมัติบนทรัพย์สินขององค์กร (Configure Automatic Session Locking on Enterprise Assets)

Asset Type: Documentation	Security Function: Govern		IG1 IG2 IG3

กำหนดให้มีการล็อกเซสชันอัตโนมัติบน ทรัพย์สินขององค์กร (Enterprise Assets) หลังจากไม่มีการใช้งานตามระยะเวลาที่กำหนด:

- ระบบปฏิบัติการทั่วไป: ระยะเวลาไม่เกิน 15 นาที
- อุปกรณ์ผู้ใช้งานแบบพกพา (Mobile End-User Devices): ระยะเวลาไม่เกิน 2 นาที

เป้าหมาย: เพื่อป้องกันการเข้าถึงอุปกรณ์โดยไม่ได้รับอนุญาตในกรณีที่ผู้ใช้งานปล่อยให้อุปกรณ์ว่างโดยไม่ได้ล็อกเซสชัน ช่วยลดความเสี่ยงด้านความปลอดภัยและสนับสนุนแนวทางปฏิบัติที่ปลอดภัยในองค์กร.

มาตรการป้องกันที่ 4.4: การติดตั้ง และจัดการไฟร์วอลล์บนเซิร์ฟเวอร์ (Implement and Manage a Firewall on Servers)

Asset Type: Documentation	Security Function: Protect		IG1 IG2 IG3

ติดตั้งและจัดการไฟร์วอลล์บน เซิร์ฟเวอร์ (Servers) โดยต้องรองรับการใช้งาน ซึ่งอาจรวมถึง:

- ไฟร์วอลล์เสมือน (Virtual Firewall)
- ไฟร์วอลล์ของระบบปฏิบัติการ (Operating System Firewall)
- ไฟร์วอลล์ของบุคคลที่สาม (Third-Party Firewall Agent)

เป้าหมาย: เพื่อป้องกันการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต และ เพิ่มระดับความปลอดภัยบนเซิร์ฟเวอร์ขององค์กร

มาตรการป้องกันที่ 4.5: การติดตั้ง และจัดการไฟร์วอลล์บนอุปกรณ์ผู้ใช้งาน (Implement and Manage a Firewall on End-User Devices)

Asset Type: Documentation	Security Function: Protect		IG1 IG2 IG3

ติดตั้งและจัดการ ไฟร์วอลล์แบบโฮสต์ (Host-Based Firewall) หรือ เครื่องมือกรองพอร์ต (Port-Filtering Tool) บนอุปกรณ์ผู้ใช้งาน (End-User Devices) พร้อมกำหนดกฎแบบ Default-Deny Rule ซึ่ง:

- บล็อกการรับส่งข้อมูลทั้งหมด
- อนุญาตเฉพาะบริการและพอร์ตที่ได้รับการกำหนดไว้อย่างชัดเจนเท่านั้น

เป้าหมาย:เพื่อควบคุมการรับส่งข้อมูลเครือข่าย ลดความเสี่ยงจากการโจมตีและการเข้าถึงโดยไม่ได้รับอนุญาต และเสริมสร้างความปลอดภัยบนอุปกรณ์ของผู้ใช้งานในองค์กร.

มาตรการป้องกันที่ 4.6: จัดการทรัพย์สิน และซอฟต์แวร์ขององค์กรอย่างปลอดภัย (Securely Manage Enterprise Assets and Software)

Asset Type: Documentation	Security Function: Protect		IG1 IG2 IG3

จัดการทรัพย์สินและซอฟต์แวร์ขององค์กรอย่างปลอดภัย ตัวอย่างการดำเนินการ:

ใช้ Infrastructure-as-Code (IaC) ที่ควบคุมด้วยระบบจัดการเวอร์ชัน (Version-Controlled)

เข้าถึงอินเทอร์เฟซ สำหรับผู้ดูแลระบบผ่านโปรโตคอลเครือข่ายที่ปลอดภัย เช่น:

- Secure Shell (SSH)
- Hypertext Transfer Protocol Secure (HTTPS)

หลีกเลี่ยงการใช้โปรโตคอลการจัดการที่ไม่ปลอดภัย เช่น:

- Telnet (Teletype Network)
- HTTP (ยกเว้นในกรณีที่มีความจำเป็นด้านการปฏิบัติการ)

เป้าหมาย: เพื่อป้องกันการเข้าถึงที่ไม่ได้รับอนุญาตและลดความเสี่ยงจากการใช้โปรโตคอลหรือวิธีการจัดการที่ไม่ปลอดภัย

มาตรการป้องกันที่ 4.7: จัดการบัญชีเริ่มต้นบนทรัพย์สินและซอฟต์แวร์ขององค์กร (Manage Default Accounts on Enterprise Assets and Software)

Asset Type: Documentation	Security Function: Protect		IG1 IG2 IG3

จัดการบัญชีผู้ใช้งานเริ่มต้น (Default Accounts) บนทรัพย์สินและซอฟต์แวร์ขององค์กร เช่น:

- บัญชี Root
- บัญชี Administrator
- บัญชีที่ตั้งค่ามาจากผู้ผลิต

ตัวอย่างการดำเนินการ:

- ปิดใช้งานบัญชีเริ่มต้น (Disable Default Accounts)
- ทำให้บัญชีเริ่มต้นไม่สามารถใช้งานได้ (Make Default Accounts Unusable)

เป้าหมาย: เพื่อป้องกันการใช้บัญชีเริ่มต้นที่มีความเสี่ยง ลดโอกาสที่ผู้ไม่ประสงค์ดีจะเข้าถึงระบบโดยใช้ข้อมูลประจำตัวที่ทราบล่วงหน้า.

มาตรการป้องกันที่ 4.8: ถอนการติดตั้ง หรือปิดใช้งานบริการที่ไม่จำเป็นบนทรัพย์สินและซอฟต์แวร์ขององค์กร (Uninstall or Disable Unnecessary Services on Enterprise Assets and Software)

Asset Type: Documentation	Security Function: Protect		IG1 IG2 IG3

ถอนการติดตั้งหรือปิดใช้งานบริการที่ไม่จำเป็นบน ทรัพย์สินและซอฟต์แวร์ขององค์กร เช่น:

- บริการแชร์ไฟล์ที่ไม่ได้ใช้งาน
- โมดูลของเว็บแอปพลิเคชันที่ไม่จำเป็น
- ฟังก์ชันของบริการที่ไม่ได้ถูกใช้งาน

เป้าหมาย: เพื่อป้องกันช่องโหว่ที่อาจเกิดจากบริการที่ไม่จำเป็น ลดความเสี่ยงที่ผู้ไม่ประสงค์ดีจะใช้บริการเหล่านี้เป็นจุดโจมตี และเพิ่มความปลอดภัยโดยรวมของระบบองค์กร.

มาตรการป้องกันที่ 4.9: กำหนดค่าเซิร์ฟเวอร์ DNS ที่เชื่อถือได้บนทรัพย์สินขององค์กร (Configure Trusted DNS Servers on Enterprise Assets)

Asset Type: Documentation	Security Function: Protect		IG1 IG2 IG3

กำหนดค่าเซิร์ฟเวอร์ DNS ที่เชื่อถือได้ บนโครงสร้างพื้นฐานเครือข่าย ตัวอย่างการดำเนินการ:

- ตั้งค่าอุปกรณ์เครือข่ายให้ใช้ เซิร์ฟเวอร์ DNS ที่ควบคุมโดยองค์กร
- ใช้ เซิร์ฟเวอร์ DNS ภายนอกที่เชื่อถือได้ และเข้าถึงได้

เป้าหมาย: เพื่อเพิ่มความปลอดภัยในการแก้ไขชื่อโดเมน ลดความเสี่ยงจากการถูกโจมตีด้วยการปลอมแปลง DNS (DNS Spoofing) และเพิ่มความมั่นคงปลอดภัยให้กับทรัพย์สินขององค์กร

มาตรการป้องกันที่ 4.10: บังคับการล็อกอุปกรณ์อัตโนมัติบนอุปกรณ์ผู้ใช้งานแบบพกพา (Enforce Automatic Device Lockout on Portable End-User Devices)

Asset Type: Documentation	Security Function: Protect		IG1 IG2 IG3

บังคับให้ อุปกรณ์ผู้ใช้งานแบบพกพา (Portable End-User Devices) ทำการล็อกอัตโนมัติหลังจากมีความพยายามยืนยันตัวตนล้มเหลวตามเกณฑ์ที่กำหนดไว้:

- สำหรับแล็ปท็อป (Laptops): ไม่เกิน 20 ครั้ง
- สำหรับแท็บเล็ตและสมาร์ทโฟน: ไม่เกิน 10 ครั้ง

ตัวอย่างการดำเนินการ:

- ใช้ Microsoft® InTune Device Lock
- ใช้ Apple® Configuration Profile maxFailedAttempts

เป้าหมาย: เพื่อป้องกันการเข้าถึงอุปกรณ์โดยไม่ได้รับอนุญาตหลังจากมีความพยายามยืนยันตัวตนล้มเหลวหลายครั้ง ลดความเสี่ยงจากการโจมตีด้วยวิธีเดาสุ่ม (Brute Force) และเสริมสร้างความปลอดภัยสำหรับอุปกรณ์พกพาขององค์กร.

มาตรการป้องกันที่ 4.11: บังคับใช้ความสามารถในการลบข้อมูลจากระยะไกลบนอุปกรณ์ผู้ใช้งานแบบพกพา (Enforce Remote Wipe Capability on Portable End-User Devices)

Asset Type: Documentation	Security Function: Protect		IG2 IG3

ลบข้อมูลขององค์กรจาก อุปกรณ์ผู้ใช้งานแบบพกพา (Portable End-User Devices) ที่องค์กรเป็นเจ้าของจากระยะไกลเมื่อมีความเหมาะสม เช่น:

- อุปกรณ์สูญหายหรือถูกขโมย
- ผู้ใช้งานไม่มีส่วนเกี่ยวข้องกับองค์กรอีกต่อไป

เป้าหมาย: เพื่อป้องกันข้อมูลขององค์กรจากการถูกเข้าถึงโดยไม่ได้รับอนุญาต เพิ่มความปลอดภัยให้กับข้อมูลในกรณีที่อุปกรณ์หลุดจากการควบคุมขององค์กร

มาตรการป้องกันที่ 4.12: แยกพื้นที่การทำงานขององค์กรบนอุปกรณ์ผู้ใช้งานมือถือ (Separate Enterprise Workspaces on Mobile End-User Devices)

Asset Type: Documentation	Security Function: Protect		IG3

แยกพื้นที่การทำงานขององค์กรออกจากพื้นที่ส่วนตัวบน อุปกรณ์ผู้ใช้งานมือถือ (Mobile End-User Devices) หากระบบรองรับ

ตัวอย่างการดำเนินการ:

- ใช้ Apple® Configuration Profile
- ใช้ Android™ Work Profile

วิธีเหล่านี้ช่วยแยกแอปพลิเคชันและข้อมูลขององค์กรออกจากแอปพลิเคชันและข้อมูลส่วนตัว

เป้าหมาย: เพื่อป้องกันการปะปนระหว่างข้อมูลส่วนตัวและข้อมูลขององค์กร ลดความเสี่ยงจากการรั่วไหลของข้อมูล เพิ่มความปลอดภัยในการใช้งานอุปกรณ์มือถือในงานขององค์กร.

CONTROL 5

การบริหารบัญชี (Account Management)

Safeguards: 6	IG1: 4/6	IG2: 6/6	IG3: 6/6

ภาพรวม (Overview):

ใช้กระบวนการและเครื่องมือเพื่อจัดการและกำหนดสิทธิ์การใช้งานให้กับข้อมูลประจำตัวของบัญชีผู้ใช้งาน (User Accounts) รวมถึงบัญชีผู้ดูแลระบบ (Administrator Accounts) และบัญชีบริการ (Service Accounts) สำหรับทรัพย์สินและซอฟต์แวร์ขององค์กร

เหตุผลที่การควบคุมนี้มีความสำคัญ (Why is this Control Critical?):

การเข้าถึงทรัพย์สินหรือข้อมูลขององค์กรโดยไม่ได้รับอนุญาตผ่าน ข้อมูลประจำตัวผู้ใช้งานที่ถูกต้อง ง่ายกว่าการ “แฮก” ระบบโดยตรง ซึ่งภัยคุกคามทั้งจากภายในและภายนอกสามารถใช้วิธีการหลากหลายเพื่อเข้าถึงบัญชีผู้ใช้งานอย่างลับๆ เช่น:

- รหัสผ่านที่อ่อนแอ
- บัญชีที่ยังคงใช้งานได้แม้ผู้ใช้งานจะออกจากองค์กรแล้ว
- บัญชีทดสอบที่ไม่ได้ถูกปิดการใช้งาน
- บัญชีที่ใช้งานร่วมกันเป็นเวลานานโดยไม่มีการเปลี่ยนรหัสผ่าน
- บัญชีบริการ (Service Accounts) ที่ถูกฝังในแอปพลิเคชันหรือสคริปต์
- ผู้ใช้งานที่ใช้รหัสผ่านเดียวกันกับบัญชีออนไลน์ที่ถูกแฮกและเผยแพร่สู่สาธารณะ
- Social Engineering: การล่อลวงให้ผู้ใช้งานเปิดเผยรหัสผ่าน
- การใช้มัลแวร์เพื่อดักจับรหัสผ่าน หรือโทเค็นในหน่วยความจำหรือผ่านเครือข่าย

บัญชีที่มีสิทธิ์สูง (Administrative Accounts) เป็นเป้าหมายสำคัญ เนื่องจากช่วยให้ผู้โจมตีสามารถ:

- เพิ่มบัญชีผู้ใช้งานใหม่
- เปลี่ยนแปลงทรัพย์สินให้ง่ายต่อการโจมตีในรูปแบบอื่นๆ

บัญชีบริการ (Service Accounts) ก็มีความอ่อนไหวเช่นกัน เพราะมักถูกใช้งานร่วมกันระหว่างทีมทั้งภายใน และภายนอกองค์กร และบางครั้งบัญชีเหล่านี้อาจไม่มีใครทราบถึงการมีอยู่ จนกระทั่งการตรวจสอบบัญชีในกระบวนการจัดการมาตรฐาน

สุดท้าย การบันทึกและการตรวจสอบบัญชีเป็นส่วนสำคัญของ การปฏิบัติการด้านความปลอดภัย (Security Operations) แม้ว่าหัวข้อนี้จะครอบคลุมใน CIS Control 8 (Audit Log Management) แต่ยังคงมีความสำคัญในบริบทของการพัฒนาโปรแกรม Identity and Access Management (IAM) ที่ครอบคลุม.

กระบวนการและเครื่องมือ (Procedures and Tools):

การติดตามบัญชี (Account Tracking):

- ต้องติดตามและตรวจสอบบัญชีผู้ใช้งานทั้งหมดในระบบ
- บัญชีที่ไม่ได้ใช้งาน (Dormant Accounts) ต้องถูกปิดการใช้งาน (Disabled) และในที่สุดต้องถูกลบออกจากระบบ

การตรวจสอบบัญชี (Account Audits):

- ดำเนินการตรวจสอบบัญชีเป็นระยะเพื่อให้แน่ใจว่าบัญชีที่ใช้งานอยู่ทั้งหมดมีความเชื่อมโยงกับผู้ใช้งานที่ได้รับอนุญาตของทรัพย์สินองค์กร
- ตรวจสอบบัญชีใหม่ที่ถูกเพิ่มเข้ามาตั้งแต่การตรวจสอบครั้งก่อน โดยเฉพาะบัญชีผู้ดูแลระบบ (Administrator Accounts) และ บัญชีบริการ (Service Accounts)

การจัดการบัญชีที่มีสิทธิ์สูง (Privileged Accounts Management):

- ผู้ใช้งานที่มีสิทธิ์ผู้ดูแลระบบ (Administrator) หรือสิทธิ์สูงอื่นๆ ควรมีบัญชีแยกสำหรับงานที่ต้องการสิทธิ์ดังกล่าว
- บัญชีที่มีสิทธิ์สูงเหล่านี้ควรใช้งานเฉพาะเมื่อปฏิบัติงานที่ต้องการสิทธิ์ระดับสูงหรือต้องเข้าถึงข้อมูลที่มีความอ่อนไหว
- บัญชีผู้ใช้งานปกติ (Base User Account) สำหรับงานประจำวันของผู้ใช้งานไม่ควรมีสิทธิ์สูง

Single Sign-On (SSO):

- การใช้ SSO เป็นวิธีที่สะดวกและปลอดภัยสำหรับองค์กรที่มีหลายแอปพลิเคชัน รวมถึงแอปพลิเคชันบนคลาวด์
- ช่วยลดจำนวนรหัสผ่านที่ผู้ใช้งานต้องจัดการ

ตัวจัดการรหัสผ่าน (Password Manager):

- แนะนำให้ผู้ใช้งานใช้ แอปพลิเคชันตัวจัดการรหัสผ่าน เพื่อเก็บรหัสผ่านอย่างปลอดภัย
- ห้ามเก็บรหัสผ่านในรูปแบบไฟล์ข้อความหรือสเปรดชีตในเครื่องคอมพิวเตอร์

การตรวจสอบแบบหลายปัจจัย (Multi-Factor Authentication - MFA):

- ควรใช้ MFA สำหรับการเข้าถึงระบบจากระยะไกล

การออกจากระบบอัตโนมัติ (Automatic Logout):

- ผู้ใช้งานต้องถูกออกจากระบบโดยอัตโนมัติหลังจากไม่มีการใช้งานในช่วงเวลาที่กำหนด
- ฝึกอบรมให้ผู้ใช้งานล็อกหน้าจอของตนเมื่อออกจากอุปกรณ์ เพื่อป้องกันการเข้าถึงโดยผู้อื่นที่อยู่ในบริเวณใกล้เคียง

เป้าหมาย:

- ลดความเสี่ยงจากการเข้าถึงระบบโดยไม่ได้รับอนุญาต
- ส่งเสริมการใช้งานระบบที่ปลอดภัยและปฏิบัติตามแนวทางปฏิบัติที่ดีในการจัดการบัญชีในองค์กร.

ทรัพยากรที่แนะนำ:

แนวทางการระบุตัวตนดิจิทัลของ NIST® (NIST Digital Identity Guidelines): เป็นแหล่งข้อมูลที่ยอดเยี่ยมสำหรับการจัดการและใช้งานระบบระบุตัวตนดิจิทัล https://pages.nist.gov/800-63-3/

คู่มือแนวทางนโยบายรหัสผ่านของ CIS (CIS Password Policy Guide): ให้คำแนะนำเกี่ยวกับการสร้างและการใช้งานรหัสผ่านที่ปลอดภัย สามารถเข้าถึงได้ที่: https://www.cisecurity.org/white-papers/cis-password-policy-guide

มาตรการป้องกัน (Safeguards)

มาตรการป้องกันที่ 5.1: จัดทำและดูแลรายการบัญชีผู้ใช้งาน (Establish and Maintain an Inventory of Accounts)

Asset Type: Users	Security Function: Identify		IG1 IG2 IG3

จัดทำและดูแลรายการบัญชีผู้ใช้งานทั้งหมดที่องค์กรจัดการ โดยในรายการบัญชีควรครอบคลุม:

- บัญชีผู้ใช้งานทั่วไป (User Accounts)
- บัญชีผู้ดูแลระบบ (Administrator Accounts)
- บัญชีบริการ (Service Accounts)

รายการบัญชีควรประกอบด้วยข้อมูลต่อไปนี้อย่างน้อย:

- ชื่อบุคคล
- ชื่อผู้ใช้งาน (Username)
- วันที่เริ่ม/หยุดใช้งาน (Start/Stop Dates)

- แผนกที่สังกัด (Department)

ดำเนินการตรวจสอบความถูกต้องของบัญชีที่ใช้งานอยู่ทั้งหมดเป็นประจำอย่างน้อยรายไตรมาส หรือบ่อยครั้งกว่านั้น หากจำเป็น

เป้าหมาย:

- เพื่อให้มั่นใจว่าบัญชีทั้งหมดในองค์กรได้รับการอนุญาตอย่างถูกต้อง
- ลดความเสี่ยงจากการใช้งานบัญชีที่ไม่ได้รับอนุญาต หรือบัญชีที่ไม่ได้ใช้งาน (Dormant Accounts)
- สนับสนุนการปฏิบัติการด้านความปลอดภัยด้วยการบริหารจัดการบัญชีอย่างมีระบบ.

มาตรการป้องกันที่ 5.2: ใช้รหัสผ่านที่ไม่ซ้ำกัน (Use Unique Passwords)

Asset Type: Users	Security Function: Identify		IG1 IG2 IG3

กำหนดให้ทุกบัญชีผู้ใช้งานบนทรัพย์สินขององค์กรต้องใช้ รหัสผ่านที่ไม่ซ้ำกัน (Unique Passwords)

แนวทางปฏิบัติที่ดีที่สุด (Best Practice):

- บัญชีที่ใช้ Multi-Factor Authentication (MFA): ใช้รหัสผ่านที่มีความยาวอย่างน้อย 8 ตัวอักษร
- บัญชีที่ไม่ใช้ Multi-Factor Authentication (MFA): ใช้รหัสผ่านที่มีความยาวอย่างน้อย 14 ตัวอักษร

เป้าหมาย:

- ลดความเสี่ยงจากการใช้รหัสผ่านซ้ำ ซึ่งอาจนำไปสู่การเข้าถึงระบบโดยไม่ได้รับอนุญาต
- เสริมสร้างความปลอดภัยให้กับระบบขององค์กรโดยใช้นโยบายรหัสผ่านที่แข็งแรงและปลอดภัย.

มาตรการป้องกันที่ 5.3: ปิดใช้งานบัญชีที่ไม่ได้ใช้งาน (Disable Dormant Accounts)

Asset Type: Users	Security Function: Protect		IG1 IG2 IG3

ลบหรือปิดใช้งานบัญชีที่ไม่ได้ใช้งาน (Dormant Accounts) หลังจากไม่มีการใช้งานเป็นระยะเวลา 45 วัน (ขึ้นอยู่กับความสามารถของระบบ)

มาตรการป้องกันที่ 5.4: จำกัดสิทธิ์ของผู้ดูแลระบบให้กับบัญชีผู้ดูแลระบบเท่านั้น (Restrict Administrator Privileges to Dedicated Administrator Accounts)

Asset Type: Users	Security Function: Identify		IG1 IG2 IG3

- จำกัดสิทธิ์ของผู้ดูแลระบบ (Administrator Privileges) ให้ใช้งานได้เฉพาะบัญชีผู้ดูแลระบบ (Dedicated Administrator Accounts) บนทรัพย์สินขององค์กรเท่านั้น
- กิจกรรมการคำนวณทั่วไป เช่น การท่องอินเทอร์เน็ต การใช้อีเมล และการใช้งานซอฟต์แวร์เพื่อเพิ่มประสิทธิภาพการทำงาน ควรดำเนินการจาก บัญชีหลักของผู้ใช้งาน (Primary Non-Privileged Account)

มาตรการป้องกันที่ 5.5: จัดทำและดูแลรายการบัญชีบริการ (Establish and Maintain an Inventory of Service Accounts)

Asset Type: Users	Security Function: Identify		IG2 IG3

จัดทำและดูแลรายการบัญชีบริการ (Service Accounts) โดยรายการบัญชีควรมีข้อมูลดังนี้อย่างน้อย:

- แผนกที่เป็นเจ้าของบัญชี (Department Owner)
- วันที่ตรวจสอบล่าสุด (Review Date)
- วัตถุประสงค์ของบัญชี (Purpose)

การตรวจสอบบัญชี:

- ดำเนินการตรวจสอบบัญชีบริการเป็นระยะเพื่อให้แน่ใจว่าบัญชีที่ใช้งานอยู่ทั้งหมดได้รับการอนุญาตอย่างถูกต้อง
- กำหนดการตรวจสอบอย่างน้อย รายไตรมาส หรือบ่อยครั้งกว่านั้น หากจำเป็น

มาตรการป้องกันที่ 5.6: รวมศูนย์การจัดการบัญชี (Centralize Account Management)

Asset Type: Users	Security Function: Govern		IG2 IG3

ดำเนินการรวมศูนย์การจัดการบัญชีผู้ใช้งานผ่านระบบ ไดเรกทอรี (Directory) หรือบริการจัดการข้อมูลประจำตัว (Identity Service) เพื่อให้การจัดการบัญชีเป็นระเบียบปลอดภัย และมีประสิทธิภาพมากขึ้น

CIS Center for Internet Security

CONTROL 6

การจัดการการควบคุมการเข้าถึง (Access Control Management)

Safeguards: 8	IG1: 5/8	IG2: 7/8	IG3: 8/8

ภาพรวม (Overview):

ใช้กระบวนการและเครื่องมือเพื่อสร้าง กำหนด จัดการ และเพิกถอนข้อมูลรับรองการเข้าถึง (Access Credentials) และสิทธิ์ (Privileges) สำหรับบัญชีผู้ใช้งาน บัญชีผู้ดูแลระบบ และบัญชีบริการบนทรัพย์สินและซอฟต์แวร์ขององค์กร

เหตุใดการควบคุมนี้จึงสำคัญ? (Why is this Control Critical?):

ในขณะที่ CIS Control 5 มุ่งเน้นที่การจัดการบัญชีผู้ใช้งาน CIS Control 6 เน้นการจัดการสิทธิ์การเข้าถึงของบัญชีเหล่านั้น

- ในเวอร์ชั่น 8.1 เราจะทำให้ มั่นใจว่าผู้ใช้งานสามารถเข้าถึงข้อมูลหรือทรัพย์สินขององค์กรได้เฉพาะที่เหมาะสมกับบทบาทของพวกเขาเท่านั้น
- ต้องมีการตรวจสอบและใช้การยืนยันตัวตนที่แข็งแกร่ง (Strong Authentication) สำหรับข้อมูลหรือฟังก์ชันที่สำคัญหรือมีความอ่อนไหว

หลักการสำคัญ:

- บัญชีผู้ใช้งานควรได้รับ สิทธิ์ที่น้อยที่สุด (Minimal Authorization) ที่จำเป็นสำหรับบทบาทหน้าที่ของพวกเขา
- การมอบสิทธิ์การเข้าถึงที่สอดคล้องกับบทบาทของแต่ละตำแหน่ง และกำหนดบทบาทเหล่านั้นให้กับผู้ใช้งาน เป็นวิธีปฏิบัติที่ดีที่สุด (Best Practice)
- การพัฒนาโปรแกรมที่สมบูรณ์สำหรับการจัดสรร (Provisioning) และการเพิกถอนสิทธิ์ (De-provisioning Access) เป็นสิ่งสำคัญ
- การรวมศูนย์การจัดการสิทธิ์การเข้าถึงเป็นสิ่งที่เหมาะสมที่สุด (Centralizing This Function is Ideal)

บางกิจกรรมของผู้ใช้งานอาจก่อให้เกิดความเสี่ยงต่อองค์กรมากขึ้น เนื่องจากสองปัจจัยหลัก:

- การเข้าถึงจากเครือข่ายที่ไม่น่าเชื่อถือ (Untrusted Networks)
- การดำเนินการในบทบาทของผู้ดูแลระบบ (Administrator Functions) ซึ่งเปิดโอกาสให้ผู้ใช้งานสามารถเพิ่ม เปลี่ยนแปลง หรือยกเลิกบัญชีผู้ใช้งานอื่น รวมถึงการเปลี่ยนแปลงการตั้งค่าระบบปฏิบัติการหรือแอปพลิเคชัน ซึ่งอาจลดความปลอดภัยของระบบได้

นี่จึงเน้นถึงความสำคัญของการใช้ การยืนยันตัวตนหลายปัจจัย (Multi-Factor Authentication - MFA) และเครื่องมือ การจัดการการเข้าถึงที่มีสิทธิพิเศษ (Privileged Access Management - PAM) เพื่อเพิ่มความปลอดภัย

กระบวนการและเครื่องมือ (Procedures and Tools)

การจัดการสิทธิ์ผู้ใช้งาน

ควรมีกระบวนการสำหรับการมอบสิทธิ์และเพิกถอนสิทธิ์สำหรับบัญชีผู้ใช้งาน โดยอ้างอิงจาก บทบาท (Role) และ ความจำเป็น (Need) ภายในองค์กรผ่านเทคนิคการเข้าถึงตามบทบาท (Role-Based Access)

Role-Based Access คือ วิธีการกำหนดและจัดการความต้องการในการเข้าถึงของแต่ละบัญชี โดยพิจารณาจาก:

- ความจำเป็นในการเข้าถึง (Need to Know)
- สิทธิ์น้อยที่สุด (Least Privilege)
- ความต้องการด้านความเป็นส่วนตัว (Privacy Requirements)
- การแยกหน้าที่และความรับผิดชอบ (Separation of Duties)

เครื่องมือเทคโนโลยีสามารถช่วยจัดการกระบวนการนี้ได้ แต่ในบางกรณีอาจต้องมีการกำหนดสิทธิ์ที่เฉพาะเจาะจงหรือชั่วคราวตามสถานการณ์

การยืนยันตัวตนหลายปัจจัย (MFA)

- MFA ควรใช้กับบัญชีที่มีสิทธิ์ระดับผู้ดูแล (Privileged) หรือบัญชีผู้ดูแลระบบ (Administrator Accounts)
- เครื่องมือส่วนใหญ่มีแอปพลิเคชันบนสมาร์ทโฟนที่ใช้งานง่าย และสามารถตั้งค่าการยืนยันตัวตนได้สะดวก
- การใช้ฟังก์ชัน Number Generator มีความปลอดภัยมากกว่าการส่งข้อความ SMS หรือการแจ้งเตือนแบบ “Push Alert” ให้ผู้ใช้งานยืนยัน อย่างไรก็ตาม วิธีดังกล่าวไม่แนะนำสำหรับบัญชีที่มีสิทธิ์ระดับสูง

การใช้เครื่องมือจัดการสิทธิ์ระดับสูง (Privileged Access Management - PAM):

- PAM สามารถจัดการบัญชีที่มีสิทธิ์ระดับสูงได้ โดยการสร้างรหัสผ่านแบบครั้งเดียว (One-Time Password) ที่ต้องตรวจสอบทุกครั้งก่อนใช้งาน
- สำหรับความปลอดภัยเพิ่มเติมในงานดูแลระบบ ควรใช้ Jump-Boxes หรือ Out of Band Terminal Connections

การเพิกถอนบัญชี (De-Provisioning):

- กระบวนการเพิกถอนบัญชีควรเป็นแบบมาตรฐานที่สามารถทำซ้ำได้ โดยเฉพาะเมื่อพนักงานออกจากองค์กร

- อย่างไรก็ตาม กระบวนการนี้มักไม่ครอบคลุมถึงผู้รับเหมาภายนอก (Contractors) ซึ่งต้องรวมอยู่ในขั้นตอนมาตรฐาน
- ควรจัดทำรายการและติดตามบัญชีบริการ (Service Accounts) เพื่อลดความผิดพลาด เช่น การทิ้งโทเค็นข้อความที่ชัดเจน (Clear Text Tokens) หรือรหัสผ่านในโค้ดที่เผยแพร่บนคลาวด์สาธารณะ

การใช้บัญชีที่มีสิทธิ์สูง:

- ไม่ควรใช้บัญชีที่มีสิทธิ์ระดับสูงสำหรับงานประจำวัน เช่น การท่องเว็บหรืออ่านอีเมล
- ผู้ดูแลระบบควรมีบัญชีที่ไม่มีสิทธิ์เพิ่มขึ้นสำหรับการใช้งานทั่วไป และเข้าสู่ระบบด้วยบัญชีที่มีสิทธิ์ระดับสูงเฉพาะเมื่อดำเนินการที่ต้องการการอนุญาตระดับดังกล่าว
- เจ้าหน้าที่ความปลอดภัยควรตรวจสอบกระบวนการที่กำลังทำงานอยู่เป็นระยะ เพื่อตรวจสอบว่ามีเบราว์เซอร์หรือโปรแกรมอ่านอีเมลใดที่ทำงานด้วยสิทธิ์ระดับสูงหรือไม่

ทรัพยากรเพิ่มเติม:

NIST® Digital Identity Guidelines: https://pages.nist.gov/800-63-3/

มาตรการป้องกัน (Safeguards)

มาตรการป้องกันที่ 6.1: จัดตั้งกระบวนการมอบสิทธิ์การเข้าถึง (Establish an Access Granting Process)

Asset Type: Documentation	Security Function: Govern	IG1	IG2	IG3

จัดตั้งและปฏิบัติตามกระบวนการที่มีการบันทึกไว้อย่างชัดเจน และควรเป็นแบบอัตโนมัติ (Automated) สำหรับการมอบสิทธิ์การเข้าถึงทรัพย์สินขององค์กรให้กับผู้ใช้งานใหม่ หรือเมื่อมีการเปลี่ยนแปลงบทบาทหน้าที่ของผู้ใช้งาน

มาตรการป้องกันที่ 6.2: จัดตั้งกระบวนการเพิกถอนสิทธิ์การเข้าถึง (Establish an Access Revoking Process)

Asset Type: Documentation	Security Function: Govern	IG1	IG2	IG3

จัดตั้งและปฏิบัติตามกระบวนการที่มีการบันทึกไว้อย่างชัดเจน และควรเป็นแบบอัตโนมัติ (Automated) สำหรับการเพิกถอนสิทธิ์การเข้าถึงทรัพย์สินขององค์กร โดยดำเนินการปิดใช้งานบัญชีทันทีเมื่อ:

- มีการเลิกจ้าง (Termination)
- มีการเพิกถอนสิทธิ์ (Rights Revocation)
- มีการเปลี่ยนบทบาทหน้าที่ของผู้ใช้งาน

การปิดใช้งานบัญชี (Disabling Accounts) แทนการลบบัญชีอาจจำเป็นในบางกรณีเพื่อรักษาร่องรอยการตรวจสอบ (Audit Trails)

มาตรการป้องกันที่ 6.3: บังคับใช้ MFA สำหรับแอปพลิเคชันที่เปิดเผยสู่ภายนอก (Require MFA for Externally-Exposed Applications)

Asset Type: User	Security Function: Protect		IG1	IG2	IG3

บังคับใช้การยืนยันตัวตนหลายปัจจัย (Multi-Factor Authentication - MFA) สำหรับแอปพลิเคชันขององค์กรหรือแอปพลิเคชันของบุคคลที่สามที่เปิดเผยต่อสาธารณะ ซึ่งรองรับ MFA

การบังคับใช้ MFA ผ่านบริการไดเรกทอรี (Directory Service) หรือผู้ให้บริการการลงชื่อเข้าใช้ครั้งเดียว (SSO) ถือว่าเป็นการปฏิบัติตามข้อกำหนดของ มาตรการป้องกันที่ นี้

มาตรการป้องกันที่ 6.4: บังคับใช้ MFA สำหรับการเข้าถึงเครือข่ายระยะไกล (Require MFA for Remote Network Access)

Asset Type: User	Security Function: Protect		IG1	IG2	IG3

กำหนดให้ผู้ใช้งานต้องใช้การยืนยันตัวตนหลายปัจจัย (Multi-Factor Authentication - MFA) สำหรับการเข้าถึงเครือข่ายขององค์กรจากระยะไกล

มาตรการป้องกันที่ 6.5: บังคับใช้ MFA สำหรับการเข้าถึงของผู้ดูแลระบบ (Require MFA for Administrative Access)

Asset Type: User	Security Function: Protect		IG1	IG2	IG3

กำหนดให้บัญชีที่มีสิทธิ์การเข้าถึงระดับผู้ดูแล (Administrative Access Accounts) ทุกบัญชี ต้องใช้การยืนยันตัวตนหลายปัจจัย (MFA) บนอุปกรณ์ทั้งหมดในองค์กร ไม่ว่าจะเป็นอุปกรณ์ที่จัดการในสถานที่ หรือผ่านผู้ให้บริการ

มาตรการป้องกันที่ 6.6: จัดตั้งและดูแลรายการระบบการตรวจสอบและอนุญาต (Establish and Maintain an Inventory of Authentication and Authorization Systems)

Asset Type: Software	Security Function: Identify			IG2	IG3

สร้างและรักษารายการระบบการตรวจสอบตัวตน (Authentication) และระบบอนุญาตการเข้าถึง (Authorization) ขององค์กร ซึ่งรวมถึงระบบที่โฮสต์ในสถานที่หรือผ่านผู้ให้บริการระยะไกล (Remote Service Provider)

- ทบทวนและอัปเดตรายการอย่างน้อยปีละหนึ่งครั้ง หรือบ่อยกว่านั้น

มาตรการป้องกันที่ 6.7: การรวมศูนย์การควบคุมการเข้าถึง (Centralize Access Control)

Asset Type: User	Security Function: Protect		IG2 IG3

รวมศูนย์การควบคุมการเข้าถึงทรัพย์สินทั้งหมดขององค์กรผ่านบริการไดเรกทอรี (Directory Service) หรือผู้ให้บริการ Single Sign-On (SSO) หากรองรับ

มาตรการป้องกันที่ 6.8: กำหนดและดูแลการควบคุมการเข้าถึงตามบทบาท (Define and Maintain Role-Based Access Control)

Asset Type: User	Security Function: Govern		IG3

กำหนดและดูแลการควบคุมการเข้าถึงตามบทบาท (Role-Based Access Control) โดยระบุและบันทึกสิทธิ์การเข้าถึงที่จำเป็นสำหรับแต่ละบทบาทในองค์กรเพื่อให้สามารถปฏิบัติหน้าที่ได้อย่างเหมาะสม

- ทำการทบทวนสิทธิ์การเข้าถึงทรัพย์สินองค์กรอย่างสม่ำเสมอ อย่างน้อยปีละหนึ่งครั้ง หรือบ่อยกว่านั้น เพื่อยืนยันว่าทุกสิทธิ์ที่มีการกำหนดนั้นได้รับการอนุญาตอย่างเหมาะสม

CONTROL 7

การจัดการช่องโหว่อย่างต่อเนื่อง (Continuous Vulnerability Management)

Safeguards: 7	IG1: 4/7	IG2: 7/7	IG3: 7/7

ภาพรวม (Overview):

พัฒนาแผนเพื่อประเมินและติดตามช่องโหว่บนทรัพย์สินทั้งหมดในโครงสร้างพื้นฐานขององค์กรอย่างต่อเนื่อง เพื่อแก้ไขและลดโอกาสของผู้โจมตีให้เหลือน้อยที่สุด รวมถึงตรวจสอบแหล่งข้อมูลสาธารณะและแหล่งข้อมูลเฉพาะอุตสาหกรรมสำหรับข้อมูลเกี่ยวกับภัยคุกคามและช่องโหว่ใหม่ ๆ

ทำไมการควบคุมนี้จึงสำคัญ?

นักป้องกันระบบไซเบอร์ต้องเผชิญกับความท้าทายอย่างต่อเนื่องจากผู้โจมตีที่มองหาช่องโหว่ในโครงสร้างพื้นฐานเพื่อใช้โจมตี และเข้าถึงระบบ ผู้ป้องกันต้องเข้าถึงข้อมูลภัยคุกคามได้อย่างทันเวลา รวมถึงข้อมูลเกี่ยวกับ:

- การอัปเดตซอฟต์แวร์
- แพตช์
- คำแนะนำด้านความปลอดภัย
- ข่าวสารเกี่ยวกับภัยคุกคาม

พวกเขาควรตรวจสอบสภาพแวดล้อมของตนอย่างสม่ำเสมอเพื่อระบุช่องโหว่เหล่านี้ก่อนที่ผู้โจมตีจะทำได้ การทำความเข้าใจและจัดการกับช่องโหว่เป็นกิจกรรมที่ต้องดำเนินการต่อเนื่อง ซึ่งต้องใช้เวลา ความใส่ใจ และทรัพยากร

ความท้าทายของการป้องกัน

- ผู้โจมตีสามารถเข้าถึงข้อมูลเดียวกันและมักจะใช้ประโยชน์จากช่องโหว่ได้เร็วกว่าที่องค์กรจะแก้ไข
- ช่องว่างเวลาระหว่างการที่ช่องโหว่ถูกค้นพบจนถึงเมื่อมันถูกแก้ไขเป็นสิ่งสำคัญ
- ผู้ป้องกันสามารถจัดลำดับความสำคัญของช่องโหว่ที่มีผลกระทบมากที่สุดต่อองค์กรหรือง่ายต่อการถูกโจมตี

ตัวอย่างเช่น เมื่อมีการรายงานช่องโหว่ใหม่ ผู้ผลิตจะต้องพัฒนา และส่งมอบแพตช์หรือเครื่องมือชี้วัดความผิดปกติ (Indicators of Compromise - IOCs) และการอัปเดต ผู้

ป้องกันต้องประเมินความเสี่ยงของช่องโหว่ใหม่ต่อองค์กร ทดสอบความเข้ากันได้ของแพตช์ และติดตั้งแพตช์

ข้อจำกัดในการป้องกัน

- Zero-Day Exploits: ผู้โจมตีอาจใช้ประโยชน์จากช่องโหว่ที่ยังไม่เป็นที่รู้จักในชุมชนด้านความปลอดภัย ช่องโหว่ดังกล่าวเรียกว่า "zero-day exploit"
- ช่องโหว่อาจเป็นที่รู้จักในกลุ่มชุมชนเฉพาะ (เช่น ผู้ผลิตยังคงพัฒนาแพตช์) นานเป็นสัปดาห์ เดือน หรือปี ก่อนที่จะถูกเปิดเผยต่อสาธารณะ
- บางครั้งผู้ป้องกันอาจทราบว่ามีช่องโหว่ที่ไม่สามารถแก้ไขได้ทันทีและต้องพึ่งพาการควบคุมอื่นเพื่อบรรเทาผลกระทบ

บทเรียนสำคัญ: การจัดการช่องโหว่เป็นกระบวนการต่อเนื่องที่จำเป็นต้องมีการติดตาม วิเคราะห์ และใช้มาตรการเชิงรุกอย่างต่อเนื่องเพื่อปกป้องค์กรจากการโจมตี.

องค์กรที่ไม่ประเมินโครงสร้างพื้นฐานของตนเพื่อหาช่องโหว่และไม่แก้ไขข้อบกพร่องที่ค้นพบอย่างเชิงรุก มีความเสี่ยงสูงที่ทรัพย์สินขององค์กรจะถูกบุกรุก ผู้ป้องกันต้องเผชิญกับความท้าทายที่สำคัญ เช่น

- การปรับขนาดกระบวนการแก้ไขให้ครอบคลุมทั่วทั้งองค์กร
- การจัดลำดับความสำคัญของการดำเนินการที่มีข้อขัดแย้ง
- การรักษาการดำเนินธุรกิจหรือภารกิจขององค์กรไม่ให้หยุดชะงัก

กระบวนการและเครื่องมือ (Procedures and Tools)

มีเครื่องมือสแกนหาช่องโหว่จำนวนมากที่สามารถใช้ประเมินการตั้งค่าความปลอดภัยของทรัพย์สินในองค์กรได้ องค์กรบางแห่งยังพบว่าบริการเชิงพาณิชย์ที่ใช้เครื่องสแกนระยะไกลที่บริหารจัดการโดยผู้ให้บริการภายนอกนั้นมีประสิทธิภาพ

เพื่อลดความซับซ้อนและมาตรฐานการจัดการช่องโหว่ในองค์กร ควรใช้เครื่องมือสแกนที่เชื่อมโยงช่องโหว่กับระบบการจัดหมวดหมู่และภาษาอุตสาหกรรมที่ได้รับการยอมรับ เช่น:

- Common Vulnerabilities and Exposures (CVE®)
- Common Configuration Enumeration (CCE)
- Open Vulnerability and Assessment Language (OVAL®)
- Common Platform Enumeration (CPE)
- Common Vulnerability Scoring System (CVSS)
- Extensible Configuration Checklist Description Format (XCCDF)

ข้อมูลเพิ่มเติมเกี่ยวกับ SCAP: NIST SP 800-126r3

การกำหนดความถี่ของการสแกน

ความถี่ในการสแกนควรเพิ่มขึ้นเมื่อความหลากหลายของทรัพย์สินในองค์กรเพิ่มขึ้น เพื่อรองรับรอบการอัปเดตแพตช์ของแต่ละผู้ผลิต

เครื่องมือสแกนช่องโหว่ขั้นสูงสามารถตั้งค่าด้วยข้อมูลรับรองผู้ใช้ (User Credentials) เพื่อทำการสแกนเชิงลึก ซึ่งเรียกว่า "การสแกนที่ผ่านการรับรอง" (Authenticated Scans)

การตรวจสอบการตั้งค่าความปลอดภัย

นอกจากเครื่องมือสแกนช่องโหว่ที่ตรวจสอบการตั้งค่าความปลอดภัยบนเครือข่ายแล้ว ยังมีเครื่องมือฟรีและเชิงพาณิชย์ที่สามารถตรวจสอบการตั้งค่าของทรัพย์สินในองค์กรได้ เครื่องมือเหล่านี้สามารถให้ข้อมูลเชิงลึกเกี่ยวกับ:

- การเปลี่ยนแปลงการตั้งค่าโดยไม่ได้รับอนุญาต
- การแนะนำข้อผิดพลาดด้านความปลอดภัยโดยไม่ตั้งใจจากผู้ดูแลระบบ

การเชื่อมโยงกับระบบบริหารจัดการปัญหา

องค์กรที่มีประสิทธิภาพจะเชื่อมโยงเครื่องมือสแกนช่องโหว่เข้ากับระบบบริหารจัดการปัญหา (Problem-Ticketing System) เพื่อ:

- ติดตามและรายงานความคืบหน้าในการแก้ไขช่องโหว่
- เน้นช่องโหว่ที่สำคัญต่อผู้บริหารระดับสูงเพื่อให้แน่ใจว่าได้รับการแก้ไข

การติดตามระยะเวลาแก้ไขช่องโหว่

- องค์กรสามารถติดตามระยะเวลาที่ใช้ในการแก้ไขช่องโหว่ หลังจากที่ระบุหรือมีการออกแพตช์แล้ว
- การดำเนินการนี้สามารถสนับสนุนข้อกำหนดด้านการปฏิบัติตามกฎระเบียบภายในหรืออุตสาหกรรม

องค์กรที่มีความพร้อม อาจนำเสนอรายงานเหล่านี้ในการประชุมคณะกรรมการกำกับดูแลความปลอดภัยด้าน IT ซึ่งรวบรวมผู้นำจาก IT และหน่วยธุรกิจเพื่อจัดลำดับความสำคัญของการแก้ไขตามผลกระทบทางธุรกิจ.

การเลือกแก้ไขช่องโหว่ และการติดตั้งแพตช์ (Selecting Vulnerabilities to Fix and Applying Patches)

การพิจารณาเลือกช่องโหว่ในการแก้ไข

องค์กรควรเสริม Common Vulnerability Scoring System (CVSS) ของ Forum of Incident Response and Security Teams, Inc. (FIRST) ด้วยข้อมูลเกี่ยวกับ:

- ความน่าจะเป็นของภัยคุกคาม (Likelihood): ความเป็นไปได้ที่ผู้ไม่หวังดีจะใช้ประโยชน์จากช่องโหว่
- ผลกระทบที่อาจเกิดขึ้น (Potential Impact): ความเสียหายที่อาจเกิดขึ้นต่อองค์กรหากช่องโหว่ถูกโจมตี

ข้อมูลเกี่ยวกับความน่าจะเป็นของการโจมตีควรถูกอัปเดตอย่างสม่ำเสมอ โดยใช้ข้อมูลภัยคุกคามล่าสุด เช่น:

- การปล่อยเครื่องมือโจมตี (Exploit) ใหม่
- ข้อมูลข่าวกรองเกี่ยวกับการใช้ช่องโหว่ในการโจมตี

สิ่งเหล่านี้สามารถเปลี่ยนลำดับความสำคัญของช่องโหว่ที่ต้องได้รับการแก้ไขหรือการติดตั้งแพตช์ใหม่ องค์กรสามารถใช้งานระบบเชิงพาณิชย์ต่างๆ เพื่อช่วยปรับปรุงและรักษากระบวนการนี้ให้สามารถขยายขนาดได้ตามความต้องการ.

การสแกนช่องโหว่เปรียบเทียบผลลัพธ์

เครื่องมือสแกนช่องโหว่ที่มีประสิทธิภาพมากที่สุดควรสามารถ:

- เปรียบเทียบผลลัพธ์ของการสแกนปัจจุบันกับการสแกนก่อนหน้า เพื่อดูการเปลี่ยนแปลงของช่องโหว่ในสภาพแวดล้อมตลอดเวลา
- คุณสมบัตินี้ช่วยให้เจ้าหน้าที่รักษาความปลอดภัยสามารถ วิเคราะห์แนวโน้มช่องโหว่ ได้ตั้งแต่เดือนต่อเดือน

กระบวนการตรวจสอบคุณภาพ

- ควรมีกระบวนการ ตรวจสอบคุณภาพ (Quality Assurance) เพื่อยืนยันว่าการอัปเดตการตั้งค่าหรือการติดตั้งแพตช์ได้ถูกดำเนินการอย่างถูกต้อง
- การตรวจสอบนี้ควรครอบคลุมทรัพย์สินทั้งหมดขององค์กรที่เกี่ยวข้อง

การบริหารจัดการช่องโหว่ที่มีประสิทธิภาพช่วยให้องค์กรสามารถตอบสนองต่อภัยคุกคามได้อย่างรวดเร็วและลดความเสี่ยงจากการถูกโจมตี.

มาตรการป้องกัน (Safeguards)

มาตรการป้องกันที่ 7.1: จัดตั้ง และรักษากระบวนการแก้ไขปัญหา (Establish and Maintain a Vulnerability Management Process)

Asset Type: Documentation	Security Function: Govern		IG1 IG2 IG3

จัดตั้งและรักษากระบวนการจัดการช่องโหว่ที่เป็นลายลักษณ์อักษรสำหรับทรัพย์สินขององค์กร

- ทบทวนและปรับปรุงเอกสาร อย่างน้อยปีละครั้ง หรือเมื่อมีการเปลี่ยนแปลงสำคัญในองค์กรที่อาจส่งผลกระทบต่อมาตรการนี้.

มาตรการป้องกันที่ 7.2: จัดตั้งและรักษากระบวนการแก้ไขปัญหา (Establish and Maintain a Remediation Process)

Asset Type: Documentation	Security Function: Govern	IG1	IG2	IG3

จัดตั้งและรักษากลยุทธ์การแก้ไขปัญหาที่ใช้หลักการประเมินความเสี่ยง และบันทึกในรูปแบบของกระบวนการแก้ไขปัญหา

- ทบทวนกระบวนการนี้ **อย่างน้อยเดือนละครั้ง** หรือบ่อยกว่านั้น.

มาตรการป้องกันที่ 7.3: ดำเนินการจัดการแพตช์ระบบปฏิบัติการอัตโนมัติ (Perform Automated Operating System Patch Management)

Asset Type: Software	Security Function: Protect	IG1	IG2	IG3

ดำเนินการอัปเดตระบบปฏิบัติการบนทรัพย์สินขององค์กรผ่านระบบจัดการแพตช์อัตโนมัติ

- ดำเนินการ อย่างน้อยเดือนละครั้ง หรือบ่อยกว่านั้น.

มาตรการป้องกันที่ 7.4: ดำเนินการจัดการแพตช์แอปพลิเคชันอัตโนมัติ (Perform Automated Application Patch Management)

Asset Type: Software	Security Function: Protect	IG1	IG2	IG3

ดำเนินการอัปเดตแอปพลิเคชันบนทรัพย์สินขององค์กรผ่านระบบจัดการแพตช์อัตโนมัติ

- ดำเนินการ อย่างน้อยเดือนละครั้ง หรือบ่อยกว่านั้น.

มาตรการป้องกันที่ 7.5: ดำเนินการสแกนช่องโหว่อัตโนมัติของทรัพย์สินภายในองค์กร (Perform Automated Vulnerability Scans of Internal Enterprise Assets)

Asset Type: Software	Security Function: Identify	IG2	IG3

ดำเนินการสแกนช่องโหว่อัตโนมัติของทรัพย์สินภายในองค์กร

- ดำเนินการ ทุกไตรมาส หรือบ่อยกว่านั้น.
- รวมทั้งการสแกนแบบ Authenticated และ Unauthenticated.

มาตรการป้องกันที่ 7.6: ดำเนินการสแกนช่องโหว่อัตโนมัติของทรัพย์สินที่เปิดเผยต่อภายนอก (Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets)

Asset Type: Software	Security Function: Identify	IG2	IG3

ดำเนินการสแกนช่องโหว่อัตโนมัติของทรัพย์สินที่เปิดเผยต่อภายนอกขององค์กร

- ดำเนินการ อย่างน้อยเดือนละครั้ง หรือบ่อยกว่านั้น.

มาตรการป้องกันที่ 7.7: แก้ไขช่องโหว่ที่ตรวจพบ (Remediate Detected Vulnerabilities)

Asset Type: Software	Security Function: Respond		IG2 IG3

แก้ไขช่องโหว่ที่ตรวจพบในซอฟต์แวร์ผ่านกระบวนการและเครื่องมือที่กำหนดไว้

- ดำเนินการ อย่างน้อยเดือนละครั้ง หรือบ่อยกว่านั้น โดยอิงตามกระบวนการแก้ไขที่กำหนด.

CONTROL 8

การจัดการช่องโหว่อย่างต่อเนื่อง (Continuous Vulnerability Management)

Safeguards: 12	IG1: 3/12	IG2: 11/12	IG3: 12/12

ภาพรวม (Overview):

รวบรวม, แจ้งเตือน, ตรวจสอบ, และจัดเก็บบันทึกการตรวจสอบของเหตุการณ์ต่าง ๆ ที่สามารถช่วยในการตรวจจับ, ทำความเข้าใจ, หรือกู้คืนจากการโจมตีได้.

ทำไมการควบคุมนี้จึงมีความสำคัญ?

การรวบรวมและการวิเคราะห์บันทึกการตรวจสอบ มีความสำคัญอย่างยิ่งต่อความสามารถขององค์กร ในการตรวจจับกิจกรรมที่เป็นอันตรายได้อย่างรวดเร็ว บางครั้ง บันทึกการตรวจสอบเป็นหลักฐานเพียงอย่างเดียวของการโจมตีที่ประสบความสำเร็จ ผู้โจมตีทราบว่าองค์กรหลายแห่งเก็บบันทึกการตรวจสอบเพื่อวัตถุประสงค์ด้านการปฏิบัติตามข้อกำหนด แต่แทบจะไม่เคยมีการวิเคราะห์บันทึกเหล่านี้เลย ผู้โจมตีใช้ความรู้นี้เพื่อซ่อนตำแหน่ง, ซอฟต์แวร์ที่เป็นอันตราย, และกิจกรรมต่าง ๆ บนเครื่องเหยื่อ เนื่องจากขาดการวิเคราะห์บันทึกที่มีประสิทธิภาพหรือไม่มีเลย ผู้โจมตีจึงสามารถควบคุมเครื่องของเหยื่อได้นานเป็นเดือนหรือเป็นปี โดยที่องค์กรเป้าหมายไม่รู้ตัว.

ประเภทของบันทึกการตรวจสอบ

บันทึกการตรวจสอบ (Logs) แบ่งออกเป็น 2 ประเภทหลักที่มักถูกจัดการและตั้งค่าแยกจากกัน ได้แก่ **บันทึกระบบ (System Logs)** และ **บันทึกการตรวจสอบ (Audit Logs)**

- **บันทึกระบบ (System Logs)**: บันทึกประเภทนี้ให้ข้อมูลเกี่ยวกับเหตุการณ์ระดับระบบ เช่น เวลาเริ่มต้น/สิ้นสุดของกระบวนการต่าง ๆ ของระบบ, การเกิดข้อขัดข้อง (Crash) เป็นต้น บันทึกเหล่านี้เป็นฟังก์ชันพื้นฐานที่ติดมากับระบบ และมักต้องการการตั้งค่าเปิดใช้งานน้อยกว่า.
- **บันทึกการตรวจสอบ (Audit Logs)**: บันทึกประเภทนี้ให้ข้อมูลเกี่ยวกับเหตุการณ์ระดับผู้ใช้ เช่น เวลาที่ผู้ใช้ล็อกอิน, การเข้าถึงไฟล์ เป็นต้น การตั้งค่าเพื่อเปิดใช้งานบันทึกการตรวจสอบต้องมีการวางแผนและดำเนินการมากกว่าบันทึกระบบ.

ความสำคัญของบันทึกการตรวจสอบในกระบวนการตอบสนองต่อเหตุการณ์ (Incident Response)

บันทึกการตรวจสอบมีบทบาทสำคัญในการตอบสนองต่อเหตุการณ์การโจมตี หลังจากตรวจพบการโจมตี การวิเคราะห์บันทึกสามารถช่วยให้องค์กรเข้าใจขอบเขตและผลกระทบของการโจมตีได้ บันทึกการตรวจสอบที่สมบูรณ์สามารถแสดงข้อมูล เช่น:

- เวลาที่การโจมตีเกิดขึ้น
- วิธีการที่ผู้โจมตีใช้ในการโจมตี
- ข้อมูลที่ถูกเข้าถึง
- ข้อมูลที่ถูกลักลอบนำออกไป (Exfiltrated)

การจัดเก็บบันทึกการตรวจสอบเป็นสิ่งสำคัญในกรณีที่ต้องมีการสอบสวนเพิ่มเติม หรือหากการโจมตียังคงไม่ถูกตรวจพบเป็นเวลานาน.

ขั้นตอนและเครื่องมือ (Process and Tools)

ขั้นตอนและเครื่องมือสำหรับการจัดการบันทึกการตรวจสอบ (Audit Log Management):

- การเปิดใช้งานการบันทึกในสินทรัพย์และซอฟต์แวร์: องค์กรควรเปิดใช้งานความสามารถในการบันทึกเหตุการณ์ (Logging) ในสินทรัพย์และซอฟต์แวร์ทุกประเภท ซึ่งรวมถึงระบบปฏิบัติการ, แอปพลิเคชัน, และซอฟต์แวร์รักษาความปลอดภัย.
- การจัดเก็บบันทึกในเซิร์ฟเวอร์กลาง (Centralized Logging Server): บันทึกที่สร้างจากอุปกรณ์ต่าง ๆ เช่น ไฟร์วอลล์, พร็อกซีเซิร์ฟเวอร์, และระบบเชื่อมต่อจากระยะไกล (VPN, Dial-up) ควรถูกส่งไปยังเซิร์ฟเวอร์จัดเก็บบันทึกแบบรวมศูนย์เพื่อให้ง่ายต่อการตรวจสอบและวิเคราะห์.
- การตั้งค่าให้บันทึกข้อมูลอย่างละเอียด (Verbose Logging): ในอุปกรณ์ที่เหมาะสม ควรตั้งค่าให้มีการบันทึกเหตุการณ์อย่างละเอียด (Verbose Logging) เพื่อเก็บข้อมูลที่มีประโยชน์ในการวิเคราะห์เหตุการณ์การโจมตี.
- การเก็บรักษาข้อมูลบันทึก (Log Retention): ควรกำหนดระยะเวลาในการเก็บรักษาบันทึกการตรวจสอบอย่างเหมาะสม เพื่อให้สามารถใช้บันทึกเหล่านี้ในการสอบสวนเหตุการณ์ได้ในอนาคต.
- การบันทึกการควบคุมการเข้าถึง (Access Control Logging): อุปกรณ์และซอฟต์แวร์ทั้งหมดควรถูกตั้งค่าให้บันทึกการควบคุมการเข้าถึง โดยเฉพาะเมื่อผู้ใช้พยายามเข้าถึงทรัพยากรที่ไม่มีสิทธิ์.
- การตรวจสอบบันทึกเป็นระยะ (Periodic Log Review): องค์กรควรทำการตรวจสอบบันทึกเป็นระยะ โดยเปรียบเทียบบันทึกกับรายการสินทรัพย์ที่

จัดทำไว้ใน CIS Control 1 เพื่อให้แน่ใจว่าสินทรัพย์ที่เชื่อมต่อกับเครือข่ายทุกชิ้นกำลังสร้างบันทึกอย่างสม่ำเสมอ.

การจัดการบันทึกการตรวจสอบที่มีประสิทธิภาพช่วยให้องค์กรสามารถตรวจจับและตอบสนองต่อการโจมตีได้อย่างรวดเร็ว อีกทั้งยังช่วยในการวิเคราะห์เหตุการณ์ย้อนหลังและรักษาความสอดคล้องตามข้อกำหนดและมาตรฐานความปลอดภัย.

มาตรการป้องกันที่ 8.1: จัดทำและดูแลกระบวนการจัดการบันทึกการตรวจสอบ (Establish and Maintain an Audit Log Management Process)

Asset Type: Documentation	Security Function: Govern		IG1 IG2 IG3

จัดทำและดูแลกระบวนการจัดการบันทึกการตรวจสอบ (Audit Log Management) ที่มีการกำหนดความต้องการการบันทึกขององค์กรอย่างชัดเจน ในกระบวนการนี้ควรครอบคลุมถึงการรวบรวม, การทบทวน, และการเก็บรักษาบันทึกการตรวจสอบสำหรับสินทรัพย์ขององค์กร อย่างน้อยที่สุด ควรมีการทบทวนและปรับปรุงเอกสารเป็นประจำทุกปี หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญในองค์กรที่อาจส่งผลกระทบต่อการควบคุมนี้.

มาตรการป้องกันที่ 8.2: รวบรวมบันทึกการตรวจสอบ (Collect Audit Logs)

Asset Type: Data	Security Function: Detect		IG1 IG2 IG3

รวบรวมบันทึกการตรวจสอบ (Audit Logs) ให้แน่ใจว่าการบันทึกเหตุการณ์ได้ถูกเปิดใช้งานในสินทรัพย์ขององค์กร ตามที่กำหนดไว้ใน กระบวนการจัดการบันทึกการตรวจสอบขององค์กร.

มาตรการป้องกันที่ 8.3: ให้แน่ใจว่ามีพื้นที่จัดเก็บบันทึกการตรวจสอบเพียงพอ (Ensure Adequate Audit Log Storage)

Asset Type: Data	Security Function: Protect		IG1 IG2 IG3

ให้แน่ใจว่าปลายทางการบันทึกมีพื้นที่จัดเก็บเพียงพอ เพื่อให้สอดคล้องกับกระบวนการจัดการบันทึกการตรวจสอบขององค์กร.

มาตรการป้องกันที่ 8.4: กำหนดมาตรฐานการซิงโครไนซ์เวลา (Standardize Time Synchronization)

Asset Type: Data	Security Function: Protect		IG1 IG2 IG3

กำหนดมาตรฐานการซิงโครไนซ์เวลา โดยการตั้งค่าให้มีแหล่งเวลาที่ซิงโครไนซ์กันอย่างน้อยสองแหล่งสำหรับสินทรัพย์ขององค์กร ในกรณีที่ระบบรองรับ.

มาตรการป้องกันที่ 8.5: เก็บบันทึกการตรวจสอบโดยละเอียด (Collect Detailed Audit Logs)

Asset Type: Data	Security Function: Detect		IG2 IG3

กำหนดการบันทึกการตรวจสอบโดยละเอียดสำหรับสินทรัพย์ขององค์กรที่มีข้อมูลที่มีความละเอียดอ่อน รวมถึงแหล่งที่มาของเหตุการณ์, วันที่, ชื่อผู้ใช้งาน, เวลาประทับ, ที่อยู่ต้นทาง, ที่อยู่ปลายทาง และองค์ประกอบอื่น ๆ ที่มีประโยชน์ในการตรวจสอบทางนิติวิทยาศาสตร์.

มาตรการป้องกันที่ 8.6: เก็บบันทึกการตรวจสอบคำขอ DNS (Collect DNS Query Audit Logs)

Asset Type: Data	Security Function: Detect		IG2 IG3

เก็บบันทึกการตรวจสอบคำขอ DNS บนอุปกรณ์ขององค์กรในกรณีที่เหมาะสมและรองรับการทำงานดังกล่าว.

มาตรการป้องกันที่ 8.7: เก็บบันทึกการตรวจสอบคำขอ URL (Collect URL Request Audit Logs)

Asset Type: Data	Security Function: Detect		IG2 IG3

เก็บบันทึกการตรวจสอบคำขอ URL บนอุปกรณ์ขององค์กรในกรณีที่เหมาะสมและรองรับการทำงานดังกล่าว.

มาตรการป้องกันที่ 8.8: เก็บบันทึกการตรวจสอบคำสั่งบรรทัดคำสั่ง (Collect Command-Line Audit Logs)

Asset Type: Data	Security Function: Detect		IG2 IG3

เก็บบันทึกการตรวจสอบคำสั่งบรรทัดคำสั่ง เช่น บันทึกคำสั่งจาก PowerShell®, BASH™, และเทอร์มินัลการจัดการระยะไกล.

มาตรการป้องกันที่ 8.9: รวมศูนย์การจัดเก็บบันทึกการตรวจสอบ (Centralize Audit Logs)

Asset Type: Data	Security Function: Detect		IG2 IG3

รวมศูนย์การเก็บ และ การจัดเก็บบันทึกการตรวจสอบจากสินทรัพย์ทั้งหมดขององค์กรตามกระบวนการจัดการบันทึกการตรวจสอบที่กำหนดไว้ ตัวอย่างการนำไปใช้ ได้แก่ การใช้เครื่องมือ SIEM ในการรวมศูนย์แหล่งข้อมูลบันทึกต่าง ๆ.

มาตรการป้องกันที่ 8.10: เก็บรักษาบันทึกการตรวจสอบ (Retain Audit Logs)

Asset Type: Data	Security Function: Protect		IG2 IG3

เก็บรักษาบันทึกการตรวจสอบจากสินทรัพย์ทั้งหมดขององค์กรเป็นระยะเวลาอย่างน้อย 90 วัน.

มาตรการป้องกันที่ 8.11: ดำเนินการทบทวนบันทึกการตรวจสอบ (Conduct Audit Log Reviews)

Asset Type: Data	Security Function: Protect		IG2 IG3

ดำเนินการทบทวนบันทึกการตรวจสอบเพื่อค้นหาความผิดปกติหรือเหตุการณ์ที่ไม่ปกติ ซึ่งอาจบ่งชี้ถึงภัยคุกคามที่อาจเกิดขึ้น ดำเนินการทบทวนเป็นรายสัปดาห์หรือบ่อยกว่านั้น.

มาตรการป้องกันที่ 8.12: เก็บบันทึกการให้บริการจากผู้ให้บริการ (Collect Service Provider Logs)

Asset Type: Data	Security Function: Protect		IG3

เก็บบันทึกการให้บริการจากผู้ให้บริการ ในกรณีที่รองรับ ตัวอย่างการนำไปใช้ ได้แก่ การเก็บบันทึกเหตุการณ์การยืนยันตัวตนและการให้สิทธิ์, เหตุการณ์การสร้างและการทำลายข้อมูล, และเหตุการณ์การจัดการผู้ใช้งาน.

CONTROL 9

การป้องกันอีเมลและเว็บเบราว์เซอร์ (Email and Web Browser Protections)

Safeguards: 7	IG1: 2/7	IG2: 6/7	IG3: 7/7

ภาพรวม (Overview):

เพิ่มการป้องกัน และการตรวจจับภัยคุกคาม จากช่องทางอีเมลและเว็บ เนื่องจากช่องทางเหล่านี้เป็นโอกาสสำหรับผู้โจมตีในการหลอกล่อหรือโน้มน้าวพฤติกรรมของมนุษย์ผ่านการติดต่อโดยตรง.

เหตุใดการควบคุมนี้จึงมีความสำคัญ?

เว็บเบราว์เซอร์ และ ไคลเอนต์อีเมลเป็นจุดเริ่มต้นที่พบได้บ่อยสำหรับผู้โจมตี เนื่องจากเป็นจุดที่มีการโต้ตอบกับผู้ใช้โดยตรงภายในองค์กร เนื้อหาสามารถถูกออกแบบมาเพื่อหลอกล่อ หรือ ปลอมแปลง เพื่อทำให้ผู้ใช้งานเปิดเผยข้อมูลรับรอง, ให้ข้อมูลที่ละเอียดอ่อน, หรือเปิดช่องทางให้ผู้โจมตีเข้าถึงระบบได้ จึงเพิ่มความเสี่ยงให้กับองค์กร.

เนื่องจากอีเมลและเว็บเป็นช่องทางหลักที่ผู้ใช้งานใช้ในการติดต่อกับผู้ใช้งานภายนอกและสภาพแวดล้อมที่ไม่น่าเชื่อถือ ช่องทางเหล่านี้จึงเป็นเป้าหมายหลักสำหรับการโจมตีด้วยโค้ดที่เป็นอันตรายและการหลอกลวงทางสังคม (Social Engineering) นอกจากนี้ เมื่อองค์กรเปลี่ยนไปใช้อีเมลบนเว็บหรือเข้าถึงอีเมลผ่านอุปกรณ์เคลื่อนที่ ผู้ใช้งานอาจไม่ได้ใช้ไคลเอนต์อีเมลแบบเต็มรูปแบบที่มีการควบคุมความปลอดภัยในตัว เช่น การเข้ารหัสการเชื่อมต่อ, การยืนยันตัวตนที่เข้มงวด, และปุ่มรายงานการฟิชชิง.

ขั้นตอนและเครื่องมือ

เว็บเบราว์เซอร์

อาชญากรไซเบอร์สามารถใช้ประโยชน์จากเว็บเบราว์เซอร์ได้หลายวิธี หากพวกเขามีช่องโหว่ที่ยังไม่ได้รับการแก้ไขในเบราว์เซอร์ พวกเขาสามารถสร้างหน้าเว็บที่เป็นอันตรายเพื่อโจมตีช่องโหว่เหล่านั้นเมื่อมีการใช้งานผ่านเบราว์เซอร์ที่ไม่ปลอดภัย หรือไม่ได้รับการอัปเดต นอกจากนี้ยังสามารถพุ่งเป้าไปที่ปลั๊กอินของเว็บเบราว์เซอร์จากผู้ผลิตบุคคลที่สาม ซึ่งอาจทำให้พวกเขาเข้าถึงเบราว์เซอร์หรือแม้กระทั่งระบบปฏิบัติการหรือแอปพลิเคชันได้โดยตรง

ปลั๊กอินเหล่านี้ เช่นเดียวกับซอฟต์แวร์อื่น ๆ ภายในระบบ จะต้องได้รับการตรวจสอบช่องโหว่ และต้องรักษาให้ทันสมัยด้วยแพตช์หรือเวอร์ชันล่าสุด และต้องมีการควบคุมอย่างเคร่งครัด ปลั๊กอินบางตัวมาจากแหล่งที่ไม่น่าเชื่อถือ และบางตัวถูกเขียนขึ้นมาเพื่อเป็นอันตราย ดังนั้น จึงควรป้องกันไม่ให้ผู้ใช้งานติดตั้งมัลแวร์โดยตั้งใจหรือไม่ตั้งใจ

ซึ่งอาจแฝงอยู่ในปลั๊กอิน ส่วนขยาย (Extensions) และแอดออน (Add-ons) การตั้งค่าเบราว์เซอร์อย่างง่ายสามารถทำให้การติดตั้งมัลแวร์ทำได้ยากขึ้น เช่น การลดความสามารถในการติดตั้งแอดออน/ปลั๊กอิน/ส่วนขยาย และป้องกันการทำงานของเนื้อหาบางประเภทโดยอัตโนมัติ

เบราว์เซอร์ยอดนิยมส่วนใหญ่มีฐานข้อมูลเว็บไซต์ฟิชชิงและ/หรือเว็บไซต์ที่มีมัลแวร์เพื่อป้องกันภัยคุกคามที่พบบ่อยที่สุด แนวทางปฏิบัติที่ดีที่สุด คือการเปิดใช้งานตัวกรองเนื้อหาเหล่านี้และเปิดใช้งานตัวบล็อกป๊อปอัป เนื่องจากป๊อปอัปไม่เพียงแต่น่ารำคาญแต่ยังสามารถฝังมัลแวร์โดยตรงหรือหลอกให้ผู้ใช้คลิกลิงก์ด้วยเทคนิคการหลอกลวงทางสังคม (Social Engineering) เพื่อบล็อกการเข้าถึงโดเมนที่เป็นอันตราย แนะนำให้สมัครใช้บริการกรอง DNS เพื่อบล็อกการเข้าถึงเว็บไซต์ที่เป็นอันตรายจากระดับเครือข่าย

อีเมล

อีเมลเป็นวิธีการทำงานที่มีปฏิสัมพันธ์สูงที่สุดวิธีหนึ่งระหว่างผู้ใช้กับทรัพย์สินขององค์กร การฝึกอบรมและกระตุ้นให้เกิดพฤติกรรมที่ถูกต้องจึงมีความสำคัญไม่แพ้การตั้งค่าทางเทคนิค อีเมลเป็นช่องทางการโจมตีที่พบได้บ่อยที่สุดในองค์กร โดยใช้กลยุทธ์ เช่น ฟิชชิง (Phishing) และ การโจมตีผ่านการปลอมแปลงอีเมลทางธุรกิจ (Business Email Compromise - BEC)

การใช้เครื่องมือกรองสแปมและการสแกนมัลแวร์ที่เกตเวย์อีเมล ช่วยลดจำนวนอีเมลและไฟล์แนบที่เป็นอันตรายที่เข้ามาในเครือข่ายขององค์กร การเปิดใช้งาน การตรวจสอบโดเมนอีเมลด้วย Domain-based Message Authentication, Reporting, and Conformance (DMARC) ช่วยลดการส่งสแปม และ กิจกรรมฟิชชิง การติดตั้งเครื่องมือเข้ารหัส (Encryption) เพื่อรักษาความปลอดภัยของอีเมลและการสื่อสารเป็นการเพิ่มอีกชั้นของการรักษาความปลอดภัยทั้งในระดับผู้ใช้และเครือข่าย

นอกจากนี้ การบล็อกไฟล์ตามผู้ส่ง ยังควรพิจารณาอนุญาตเฉพาะไฟล์ประเภทที่ผู้ใช้จำเป็นต้องใช้ในการทำงานเท่านั้น ซึ่งจำเป็นต้องประสานงานกับหน่วยธุรกิจต่าง ๆ เพื่อทำความเข้าใจว่าไฟล์ประเภทใดที่พวกเขามักได้รับผ่านอีเมล เพื่อให้มั่นใจว่าไม่มีการขัดจังหวะกระบวนการทำงานของพวกเขา

เนื่องจากเทคนิคการโจมตีฟิชชิงมีการพัฒนาอย่างต่อเนื่องเพื่อหลบเลี่ยงกฎการกรองสแปม การฝึกอบรมผู้ใช้ให้สามารถระบุอีเมลฟิชชิงได้ และแจ้งทีม IT Security เมื่อพบอีเมลที่น่าสงสัยจึงมีความสำคัญ มีแพลตฟอร์มหลายตัวที่สามารถทดสอบฟิชชิงกับผู้ใช้ช่วยให้พวกเขาเรียนรู้ตัวอย่างการโจมตีที่หลากหลาย และติดตามการพัฒนาความสามารถในการระบุฟิชชิงของพวกเขา การรวมความรู้จากผู้ใช้เพื่อแจ้งให้ทีม IT Security ทราบถึงการพบอีเมลฟิชชิง ช่วยเพิ่มประสิทธิภาพในการป้องกันและตรวจจับภัยคุกคามที่มาจากอีเมล

มาตรการป้องกันที่ 9.1: การใช้เฉพาะเว็บเบราว์เซอร์และไคลเอนต์อีเมลที่ได้รับการสนับสนุนเต็มรูปแบบ (Ensure Use of Only Fully Supported Browsers and Email Clients)

Asset Type: Software	Security Function: Protect	IG1	IG2	IG3

มั่นใจได้ว่าองค์กรใช้เฉพาะเว็บเบราว์เซอร์และไคลเอนต์อีเมลที่ได้รับการสนับสนุนอย่างเต็มรูปแบบ โดยใช้เฉพาะเวอร์ชันล่าสุดที่ผู้จัดจำหน่ายให้มาเท่านั้น

มาตรการป้องกันที่ 9.2: ใช้บริการกรอง DNS (Use DNS Filtering Services)

Asset Type: Software	Security Function: Protect	IG1	IG2	IG3

ใช้บริการกรอง DNS บนอุปกรณ์ผู้ใช้ทั้งหมด รวมถึงอุปกรณ์ระยะไกลและอุปกรณ์ในสถานที่ เพื่อบล็อกการเข้าถึงโดเมนที่เป็นอันตรายที่ทราบแล้ว

มาตรการป้องกันที่ 9.3: บำรุงรักษาและบังคับใช้การกรอง URL บนเครือข่าย (Maintain and Enforce Network-Based URL Filters)

Asset Type: Software	Security Function: Protect	IG2	IG3

บังคับใช้และอัปเดตการกรอง URL บนเครือข่ายเพื่อจำกัดการเชื่อมต่อของสินทรัพย์ในองค์กรกับเว็บไซต์ที่อาจเป็นอันตรายหรือไม่ได้รับอนุญาต การใช้งานตัวอย่าง ได้แก่ การกรองตามหมวดหมู่ การกรองตามความน่าเชื่อถือ หรือการใช้บัญชีบล็อก บังคับใช้การกรองสำหรับสินทรัพย์ในองค์กรทั้งหมด

มาตรการป้องกันที่ 9.4: จำกัดส่วนขยายของเว็บเบราว์เซอร์และไคลเอนต์อีเมลที่ไม่จำเป็นหรือไม่ได้รับอนุญาต (Restrict Unnecessary or Unauthorized Browser and Email Client Extensions)

Asset Type: Software	Security Function: Protect	IG2	IG3

จำกัดส่วนขยาย ปลั๊กอิน และแอปพลิเคชันเสริมของเว็บเบราว์เซอร์และไคลเอนต์อีเมลที่ไม่จำเป็นหรือไม่ได้รับอนุญาต โดยการถอนการติดตั้งหรือปิดการใช้งาน

มาตรการป้องกันที่ 9.5: ใช้การยืนยันตัวตน DMARC (Implement DMARC)

Asset Type: Software	Security Function: Protect	IG2	IG3

เพื่อให้ความเสี่ยงจากการปลอมแปลงหรือการดัดแปลงอีเมลจากโดเมนที่ถูกต้องลดลง ให้ใช้มาตรการยืนยันตัวตน DMARC โดยเริ่มจากการใช้มาตรฐาน Sender Policy Framework (SPF) และ DomainKeys Identified Mail (DKIM)

มาตรการป้องกันที่ 9.6: บล็อกประเภทไฟล์ที่ไม่จำเป็น DMARC (Block Unnecessary File Types)

Asset Type:	Security Function: Protect	IG2	IG3

Softwareบล็อกประเภทไฟล์ที่ไม่จำเป็นซึ่งพยายามเข้าสู่เกตเวย์อีเมลองค์กร

มาตรการป้องกันที่ 9.7: ติดตั้งและบำรุงรักษาการป้องกันมัลแวร์บนเซิร์ฟเวอร์อีเมล (Deploy and Maintain Email Server Anti-Malware Protections)

Asset Type: Software	Security Function: Protect		IG3

ติดตั้ง และบำรุงรักษาการป้องกันมัลแวร์ บนเซิร์ฟเวอร์อีเมล เช่น การสแกนไฟล์แนบ และ/หรือการใช้ระบบแซนด์บ็อกซ์ (Sandboxing)

CONTROL 10

การป้องกันมัลแวร์ (Malware Defenses)

Safeguards: 7	IG1: 3/7	IG2: 7/7	IG3: 7/7

ภาพรวม (Overview):

ป้องกันหรือควบคุมการติดตั้ง การแพร่กระจาย และการทำงานของแอปพลิเคชันมัลแวร์ โค้ด หรือสคริปต์ที่เป็นอันตรายบนสินทรัพย์ขององค์กร.

เหตุใดการควบคุมนี้จึงมีความสำคัญ?

มัลแวร์ (ซึ่งบางครั้งจัดประเภทเป็นไวรัส หรือโทรจัน) เป็นภัยคุกคามที่อันตรายและเป็นส่วนสำคัญของการโจมตีทางอินเทอร์เน็ต โดยมีวัตถุประสงค์ที่หลากหลาย เช่น การขโมยข้อมูลการเข้าสู่ระบบ การลักลอบขโมยข้อมูล การค้นหาเป้าหมายอื่น ๆ ภายในเครือข่าย และการเข้ารหัสหรือทำลายข้อมูล มัลแวร์มีการพัฒนาและปรับเปลี่ยนอยู่ตลอดเวลา โดยมัลแวร์รุ่นใหม่ ๆ ใช้เทคนิคการเรียนรู้ของเครื่อง (Machine Learning)

มัลแวร์สามารถเข้าสู่องค์กรผ่านช่องโหว่ต่าง ๆ ในอุปกรณ์ผู้ใช้งาน อีเมลแนบ ลิงก์เว็บไซต์ บริการคลาวด์ อุปกรณ์เคลื่อนที่ และสื่อบันทึกข้อมูลแบบถอดได้ มัลแวร์มักอาศัยพฤติกรรมการใช้งานที่ไม่ปลอดภัยของผู้ใช้ เช่น การคลิกลิงก์ การเปิดไฟล์แนบ การติดตั้งซอฟต์แวร์หรือโปรไฟล์ หรือการเสียบอุปกรณ์ USB โดยมัลแวร์สมัยใหม่ถูกออกแบบมาให้หลบเลี่ยง หลอกลวง หรือปิดการทำงานของระบบป้องกัน

ระบบป้องกันมัลแวร์ต้องสามารถทำงานได้อย่างมีประสิทธิภาพในสภาพแวดล้อมที่เปลี่ยนแปลงอย่างรวดเร็ว โดยอาศัยระบบอัตโนมัติ การอัปเดตอย่างรวดเร็วและทันท่วงที รวมถึงการผสานการทำงานกับกระบวนการอื่น ๆ เช่น การจัดการช่องโหว่และการตอบสนองต่อเหตุการณ์ นอกจากนี้ ระบบป้องกันมัลแวร์ต้องถูกใช้งานในทุกจุดที่มีความเสี่ยงและสินทรัพย์ขององค์กร เพื่อช่วยในการตรวจจับ ป้องกันการแพร่กระจาย และควบคุมการทำงานของซอฟต์แวร์หรือโค้ดที่เป็นอันตราย

ขั้นตอนและเครื่องมือ

การป้องกันมัลแวร์ที่มีประสิทธิภาพประกอบด้วยชุดเครื่องมือสำหรับการป้องกันและตรวจจับมัลแวร์แบบดั้งเดิมบนอุปกรณ์ปลายทาง (Endpoint). เพื่อให้มั่นใจได้ว่าข้อมูล Indicator of Compromise (IOC) สำหรับมัลแวร์มีการอัปเดตล่าสุด องค์กรสามารถรับการอัปเดตอัตโนมัติจากผู้ให้บริการ เพื่อเสริมความสมบูรณ์ของข้อมูลช่องโหว่หรือข้อมูลภัยคุกคามอื่น ๆ การจัดการเครื่องมือเหล่านี้ควรดำเนินการผ่านศูนย์กลาง เพื่อให้เกิดความสม่ำเสมอทั่วทั้งโครงสร้างพื้นฐาน

การปิดกั้นหรือระบุมัลแวร์เป็นเพียงส่วนหนึ่งของการควบคุมนี้ อีกส่วนหนึ่งคือการรวบรวมบันทึกการทำงานจากศูนย์กลาง เพื่อสนับสนุนการแจ้งเตือน การระบุ

เหตุการณ์ และการตอบสนองต่อเหตุการณ์ เมื่อผู้โจมตียังคงพัฒนากลยุทธ์การโจมตีอย่างต่อเนื่อง หลายคนใช้แนวทาง “Living-off-the-Land” (LotL) เพื่อหลีกเลี่ยงการถูกตรวจจับ ซึ่งเป็นพฤติกรรมของผู้โจมตีที่ใช้เครื่องมือหรือฟีเจอร์ที่มีอยู่แล้วในสภาพแวดล้อมเป้าหมาย

การเปิดใช้งานการบันทึกตามมาตรการป้องกันใน CIS Control 8 จะทำให้องค์กรติดตามเหตุการณ์ได้ง่ายขึ้นอย่างมาก เพื่อทำความเข้าใจว่าเกิดอะไรขึ้นและทำไมถึงเกิดเหตุการณ์ขึ้น

CIS จัดทำชุดคู่มือเพื่อช่วยทำความเข้าใจว่ามาตรการควบคุม CIS สามารถนำไปใช้กับเทคนิค “Living-off-the-Land” ที่พบได้บ่อยได้อย่างไร: https://www.cisecurity.org/white-papers/

มาตรการป้องกันที่ 10.1: ติดตั้งและบำรุงรักษาซอฟต์แวร์ป้องกันมัลแวร์ (Deploy and Maintain Anti-Malware Software)

Asset Type: Devices	Security Function: Detect		IG1 IG2 IG3

ติดตั้งและบำรุงรักษาซอฟต์แวร์ป้องกันมัลแวร์บนอุปกรณ์ทั้งหมดขององค์กร

มาตรการป้องกันที่ 10.2: ตั้งค่าให้ซอฟต์แวร์ป้องกันมัลแวร์อัปเดตฐานข้อมูลลายเซ็นอัตโนมัติ (Configure Automatic Anti-Malware Signature Updates)

Asset Type: Devices	Security Function: Protect		IG1 IG2 IG3

ตั้งค่าให้ซอฟต์แวร์ป้องกันมัลแวร์อัปเดตไฟล์ฐานข้อมูลลายเซ็นอัตโนมัติบนอุปกรณ์ทั้งหมดขององค์กร

มาตรการป้องกันที่ 10.3: ปิดการใช้งานฟังก์ชัน Autorun และ Autoplay สำหรับสื่อแบบถอดได้ (Disable Autorun and Autoplay for Removable Media)

Asset Type: Devices	Security Function: Protect		IG1 IG2 IG3

ปิดการใช้งานฟังก์ชันการทำงาน Autorun และ Autoplay สำหรับการทำงานอัตโนมัติเมื่อเชื่อมต่อสื่อแบบถอดได้

มาตรการป้องกันที่ 10.4: ตั้งค่าให้ซอฟต์แวร์ป้องกันมัลแวร์สแกนสื่อแบบถอดได้โดยอัตโนมัติ (Configure Automatic Anti-Malware Scanning of Removable Media)

Asset Type: Devices	Security Function: Detect		IG2 IG3

ตั้งค่าให้ซอฟต์แวร์ป้องกันมัลแวร์สแกนสื่อแบบถอดได้โดยอัตโนมัติทุกครั้งที่เชื่อมต่อกับอุปกรณ์

มาตรการป้องกันที่ 10.5: เปิดใช้งานฟีเจอร์ป้องกันการเอ็กซ์พลอยต์ (Enable Anti-Exploitation Features)

Asset Type: Devices	Security Function: Detect		IG2 IG3

เปิดใช้งานฟีเจอร์ป้องกันการเอ็กซ์พลอยต์บนอุปกรณ์และซอฟต์แวร์ขององค์กร เช่น Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), หรือ Apple® System Integrity Protection (SIP) และ Gatekeeper™

มาตรการป้องกันที่ 10.6: จัดการซอฟต์แวร์ป้องกันมัลแวร์จากศูนย์กลาง (Centrally Manage Anti-Malware Software)

Asset Type: Devices	Security Function: Protect		IG2 IG3

จัดการซอฟต์แวร์ป้องกันมัลแวร์จากศูนย์กลาง เพื่อให้การตั้งค่าและการควบคุมเป็นไปอย่างสอดคล้องและมีประสิทธิภาพ

มาตรการป้องกันที่ 10.7: ใช้ซอฟต์แวร์ป้องกันมัลแวร์ที่อิงตามพฤติกรรม (Use Behavior-Based Anti-Malware Software)

Asset Type: Devices	Security Function: Detect		IG2 IG3

ใช้ซอฟต์แวร์ป้องกันมัลแวร์ที่อิงตามการวิเคราะห์พฤติกรรมเพื่อระบุและตรวจจับกิจกรรมที่น่าสงสัยหรืออาจเป็นอันตราย

CONTROL 11

การกู้คืนข้อมูล (Data Recovery)

Safeguards: 5	IG1: 4/5	IG2: 5/5	IG3: 5/5

ภาพรวม (Overview):

จัดตั้งและรักษาแนวปฏิบัติในการกู้คืนข้อมูลที่เพียงพอสำหรับการกู้คืนสินทรัพย์ขององค์กรให้กลับสู่สถานะที่เชื่อถือได้ก่อนเกิดเหตุการณ์

เหตุใดการควบคุมนี้จึงมีความสำคัญ?

ในสามเสาหลักของความปลอดภัยไซเบอร์ ได้แก่ ความลับ (Confidentiality), ความสมบูรณ์ (Integrity), และ ความพร้อมใช้งาน (Availability) — ความพร้อมใช้งานของข้อมูลบางครั้งมีความสำคัญมากกว่าความลับของข้อมูลเองอีกด้วย องค์กรต้องใช้ข้อมูลหลายประเภทในการตัดสินใจทางธุรกิจ และหากข้อมูลนั้นไม่พร้อมใช้งานหรือไม่น่าเชื่อถือ อาจส่งผลกระทบต่อการดำเนินงานขององค์กร ตัวอย่างที่เห็นได้ง่ายคือข้อมูลสภาพอากาศสำหรับบริษัทขนส่ง

เมื่อผู้โจมตีเข้าควบคุมสินทรัพย์ พวกเขามักจะเปลี่ยนแปลงการตั้งค่า เพิ่มบัญชีผู้ใช้ใหม่ และติดตั้งซอฟต์แวร์หรือสคริปต์ที่เป็นอันตราย การเปลี่ยนแปลงเหล่านี้มักตรวจพบได้ยาก เพราะผู้โจมตีอาจทำการแทนที่แอปพลิเคชันที่เชื่อถือได้ด้วยเวอร์ชันที่เป็นอันตราย หรือเปลี่ยนแปลงบัญชีให้ดูเหมือนชื่อปกติ การเปลี่ยนแปลงการตั้งค่าอาจรวมถึงการเพิ่มหรือแก้ไขรีจิสทรี การเปิดพอร์ต ปิดบริการรักษาความปลอดภัย ลบล็อกไฟล์ หรือดำเนินการอื่นๆ ที่ทำให้ระบบไม่ปลอดภัย นอกจากนี้ การกระทำดังกล่าวไม่ได้เกิดจากการโจมตีเสมอไป ความผิดพลาดของมนุษย์ก็สามารถก่อให้เกิดปัญหาเช่นกัน ดังนั้น การมีแบคอัพหรือข้อมูลสำรองที่อัปเดตจึงเป็นสิ่งจำเป็นสำหรับการกู้คืนสินทรัพย์และข้อมูลกลับสู่สถานะที่น่าเชื่อถือ

ช่วงไม่กี่ปีที่ผ่านมา การโจมตีด้วยแรนซัมแวร์เพิ่มขึ้นอย่างรวดเร็ว แม้จะไม่ใช่ภัยคุกคามใหม่ แต่ถูกทำให้เป็นเชิงพาณิชย์และมีการจัดระเบียบมากขึ้นเพื่อใช้เป็นวิธีการทำเงินของผู้โจมตี หากแรนซัมแวร์ทำการเข้ารหัสข้อมูลขององค์กรและเรียกค่าไถ่ การมีข้อมูลสำรองล่าสุดเพื่อกู้คืนกลับสู่สถานะที่เชื่อถือได้จะช่วยแก้ไขปัญหาได้ อย่างไรก็ตาม แรนซัมแวร์ในปัจจุบันมีการขู่กรรโชกเพิ่มเติมโดยการขโมยข้อมูลก่อนเข้ารหัส จากนั้นจึงเรียกค่าไถ่ทั้งเพื่อกู้คืนข้อมูลและไม่ให้ข้อมูลถูกขายหรือเผยแพร่สู่สาธารณะ ในกรณีนี้ การกู้คืนข้อมูลจะช่วยฟื้นฟูระบบให้กลับมาดำเนินการได้ตามปกติเท่านั้น

การปฏิบัติตามแนวทางภายใน CIS Controls จะช่วยลดความเสี่ยงจากแรนซัมแวร์ได้ผ่านการรักษาความปลอดภัยที่ดีขึ้น เนื่องจากผู้โจมตีมักใช้ช่องโหว่เก่าหรือเทคนิคพื้นฐานบนระบบที่ไม่ปลอดภัย)

ขั้นตอนและเครื่องมือ

กระบวนการกู้คืนข้อมูลควรถูกกำหนดไว้ในกระบวนการจัดการข้อมูลที่อธิบายไว้ใน CIS Control 3: การปกป้องข้อมูล ซึ่งควรรวมถึงขั้นตอนการสำรองข้อมูลตามมูลค่าความละเอียดอ่อน หรือข้อกำหนดการเก็บรักษาข้อมูล การทำเช่นนี้จะช่วยในการกำหนดความถี่และประเภทของการสำรองข้อมูล (เช่น การสำรองข้อมูลเต็มรูปแบบหรือการสำรองข้อมูลแบบเพิ่มขึ้น)

อย่างน้อย หนึ่งครั้งต่อไตรมาส (หรือทุกครั้งที่มีการแนะนำกระบวนการหรือเทคโนโลยีการสำรองข้อมูลใหม่) ควรมีกลุ่มทดสอบทำการสุ่มตัวอย่างการสำรองข้อมูลและพยายามกู้คืนบนสภาพแวดล้อมทดสอบ หลังจากการกู้คืนเสร็จสิ้นแล้ว ควรทำการตรวจสอบว่าระบบปฏิบัติการ แอปพลิเคชัน และข้อมูลจากการสำรองข้อมูลทั้งหมดอยู่ในสภาพสมบูรณ์และทำงานได้อย่างถูกต้อง

ในกรณีที่มีการติดมัลแวร์ ขั้นตอนการกู้คืนควรใช้เวอร์ชันการสำรองข้อมูลที่เชื่อว่าเป็นเวอร์ชันที่สร้างขึ้นก่อนที่การติดมัลแวร์จะเกิดขึ้นครั้งแรก

มาตรการป้องกันที่ 11.1: จัดตั้งและดูแลกระบวนการกู้คืนข้อมูล (Establish and Maintain a Data Recovery Process)

Asset Type: Documentation	Security Function: Govern		IG1 IG2 IG3

จัดตั้ง และดูแลกระบวนการกู้คืน ข้อมูลที่มีการบันทึกเป็นลายลักษณ์อักษร ในกระบวนการนี้ ควรระบุขอบเขตของกิจกรรมการกู้คืนข้อมูล การจัดลำดับความสำคัญของการกู้คืน และการรักษาความปลอดภัยของข้อมูลสำรอง ทบทวนและอัปเดตเอกสารทุกปี หรือตามการเปลี่ยนแปลงที่สำคัญขององค์กรที่อาจส่งผลกระทบต่อการป้องกันนี้

มาตรการป้องกันที่ 11.2: ทำการสำรองข้อมูลโดยอัตโนมัติ (Perform Automated Backups)

Asset Type: Documentation	Security Function: Recover		IG1 IG2 IG3

ทำการสำรองข้อมูลโดยอัตโนมัติสำหรับสินทรัพย์ขององค์กรที่อยู่ในขอบเขต ดำเนินการสำรองข้อมูลทุกสัปดาห์ หรือตามความถี่ที่เหมาะสมตามความละเอียดอ่อนของข้อมูล

มาตรการป้องกันที่ 11.3: ปกป้องข้อมูลสำหรับการกู้คืน (Protect Recovery Data)

Asset Type: Documentation	Security Function: Protect		IG1 IG2 IG3

ปกป้องข้อมูลสำหรับการกู้คืนด้วยมาตรการควบคุมที่เทียบเท่ากับข้อมูลต้นฉบับ อ้างอิงถึงการเข้ารหัสหรือการแยกข้อมูลตามความต้องการขององค์กร

มาตรการป้องกันที่ 11.4: จัดตั้งและดูแลอินสแตนซ์ของข้อมูลกู้คืนที่แยกออกจากระบบ (Establish and Maintain an Isolated Instance of Recovery Data)

Asset Type: Documentation	Security Function: Recover		IG1 IG2 IG3

จัดตั้งและดูแลอินสแตนซ์ของข้อมูลกู้คืนที่แยกออกจากระบบตัวอย่างของการใช้งาน รวมถึง การควบคุมเวอร์ชันปลายทางการสำรองข้อมูลผ่านระบบออฟไลน์ คลาวด์ หรือบริการนอกสถานที่

มาตรการป้องกันที่ 11.5: ทดสอบการกู้คืนข้อมูล (Test Data Recovery)

Asset Type: Documentation	Security Function: Recover		IG2 IG3

ทดสอบการกู้คืนข้อมูลจากการสำรองอย่างน้อยทุกไตรมาส หรือบ่อยกว่านั้น โดยเลือกสุ่มทดสอบกับสินทรัพย์ขององค์กรที่อยู่ในขอบเขตการกู้คืนข้อมูล

CONTROL 12

การจัดการโครงสร้างพื้นฐานเครือข่าย (Network Infrastructure Management)

Safeguards: 8	IG1: 1/8	IG2: 7/8	IG3: 8/8

ภาพรวม (Overview):

จัดตั้ง ดำเนินการ และบริหารจัดการ (ติดตาม, รายงาน, แก้ไข) อุปกรณ์เครือข่ายอย่างจริงจัง เพื่อป้องกันไม่ให้ผู้โจมตีใช้ประโยชน์จากบริการเครือข่ายและจุดเชื่อมต่อที่มีช่องโหว่

เหตุใดการควบคุมนี้จึงมีความสำคัญ?

โครงสร้างพื้นฐานเครือข่ายที่ปลอดภัยเป็นการป้องกันที่สำคัญต่อการโจมตี ซึ่งรวมถึงการมีสถาปัตยกรรมความปลอดภัยที่เหมาะสม การแก้ไขช่องโหว่ที่มักเกิดขึ้นจากการตั้งค่าเริ่มต้น การตรวจสอบการเปลี่ยนแปลง และการประเมินค่าใหม่ของการตั้งค่าปัจจุบัน อุปกรณ์โครงสร้างพื้นฐานเครือข่ายประกอบด้วยอุปกรณ์ต่าง ๆ เช่น เกตเวย์แบบกายภาพและเสมือน ไฟร์วอลล์ จุดเชื่อมต่อไร้สาย เราเตอร์ และสวิตช์

การตั้งค่าเริ่มต้นสำหรับอุปกรณ์เครือข่ายมักเน้นที่ความสะดวกในการติดตั้งและใช้งานมากกว่าความปลอดภัย ช่องโหว่จากการตั้งค่าเริ่มต้นอาจรวมถึง:

- บริการและพอร์ตที่เปิดใช้งาน
- บัญชีผู้ใช้และรหัสผ่านเริ่มต้น (รวมถึงบัญชีบริการ)
- รองรับโปรโตคอลเก่าที่มีช่องโหว่
- การติดตั้งซอฟต์แวร์ที่ไม่จำเป็น

ผู้โจมตีจะค้นหาการตั้งค่าเริ่มต้นที่มีช่องโหว่ ช่องโหว่ในชุดกฎไฟร์วอลล์ เราเตอร์ และสวิตช์ และใช้ช่องโหว่เหล่านี้ในการเจาะระบบ พวกเขาจะใช้ข้อบกพร่องของอุปกรณ์เหล่านี้เพื่อเข้าถึงเครือข่าย เปลี่ยนเส้นทางการรับส่งข้อมูล และดักจับข้อมูลระหว่างการส่งผ่าน

ความปลอดภัยของเครือข่ายเป็นสภาพแวดล้อมที่เปลี่ยนแปลงตลอดเวลา ซึ่งจำเป็นต้องมีการประเมินแผนผังสถาปัตยกรรม การตั้งค่า การควบคุมการเข้าถึง และการอนุญาตการรับส่งข้อมูลอย่างสม่ำเสมอ ผู้โจมตีมักใช้ประโยชน์จากการตั้งค่าอุปกรณ์เครือข่ายที่ลดความปลอดภัยลงเมื่อเวลาผ่านไป เนื่องจากผู้ใช้งานต้องการข้อยกเว้นเพื่อตอบสนองความต้องการทางธุรกิจ ในบางครั้ง ข้อยกเว้นเหล่านี้ถูกนำไปใช้ แต่ไม่ได้ถูกยกเลิกเมื่อไม่จำเป็นอีกต่อไป บางกรณีความเสี่ยงจากข้อยกเว้น

ไม่ได้รับการวิเคราะห์หรือวัดเทียบกับความต้องการทางธุรกิจ และความเสี่ยงนั้นก็อาจเปลี่ยนแปลงไปตามเวลา

ขั้นตอนและเครื่องมือ

องค์กรควรตรวจสอบให้แน่ใจว่าโครงสร้างพื้นฐานเครือข่ายได้รับการบันทึกอย่างครบถ้วนและแผนผังสถาปัตยกรรมเครือข่ายมีการอัปเดตอยู่เสมอ การมีการสนับสนุนจากผู้จำหน่ายเพื่อการอัปเดตแพตช์และการอัปเกรดฟีเจอร์สำหรับองค์ประกอบที่สำคัญของโครงสร้างพื้นฐานเป็นสิ่งสำคัญ ควรอัปเกรดอุปกรณ์ที่หมดอายุการใช้งาน (End-of-Life - EOL) ก่อนวันที่จะไม่มีการสนับสนุน หรือใช้มาตรการควบคุมเพื่อลดความเสี่ยงโดยการแยกอุปกรณ์ออกจากเครือข่าย องค์กรต้องติดตามเวอร์ชันและการตั้งค่าโครงสร้างพื้นฐานเพื่อหาช่องโหว่ที่จำเป็นต้องอัปเกรดอุปกรณ์เครือข่ายเป็นเวอร์ชันที่ปลอดภัยและเสถียร โดยไม่กระทบต่อการทำงานของโครงสร้างพื้นฐาน

การมีแผนผังสถาปัตยกรรมเครือข่ายที่อัปเดต ซึ่งรวมถึงแผนผังสถาปัตยกรรมความปลอดภัย เป็นรากฐานสำคัญสำหรับการจัดการโครงสร้างพื้นฐาน ขั้นตอนถัดไปคือการจัดการบัญชีผู้ใช้งานเพื่อควบคุมการเข้าถึง การบันทึก (logging) และการเฝ้าตรวจสอบ (monitoring) นอกจากนี้ การดูแลระบบโครงสร้างพื้นฐานควรกระทำผ่านโปรโตคอลที่ปลอดภัยเท่านั้น โดยใช้การยืนยันตัวตนที่เข้มงวด (เช่น การยืนยันตัวตนหลายปัจจัย - MFA สำหรับการจัดการสิทธิ์พิเศษ - PAM) และจากอุปกรณ์ที่ใช้เฉพาะสำหรับการจัดการ หรือเครือข่ายที่อยู่นอกแถบ (out-of-band networks)

เครื่องมือเชิงพาณิชย์สามารถช่วยประเมินชุดกฎ (rule sets) ของอุปกรณ์กรองเครือข่ายเพื่อดูว่ามีความสอดคล้องหรือขัดแย้งกันหรือไม่ เครื่องมือเหล่านี้ช่วยตรวจสอบข้อผิดพลาดโดยอัตโนมัติในชุดกฎหรือรายการควบคุมการเข้าถึง (Access Control Lists - ACLs) ที่อาจอนุญาตให้บริการที่ไม่ต้องการผ่านอุปกรณ์เครือข่ายได้ ควรใช้เครื่องมือเหล่านี้ทุกครั้งที่มีการเปลี่ยนแปลงกฎไฟร์วอลล์, ACL ของเราเตอร์, หรือเทคโนโลยีกรองอื่น ๆ อย่างมีนัยสำคัญ

สำหรับคำแนะนำเกี่ยวกับการทำงานทางไกลและสำนักงานขนาดเล็ก สามารถอ้างอิงจาก CIS Controls Telework and Small Office Network Security Guide ได้ที่: https://www.cisecurity.org/controls/v8/

มาตรการป้องกันที่ 12.1: ตรวจสอบให้แน่ใจว่าโครงสร้างพื้นฐานเครือข่ายทันสมัยอยู่เสมอ (Ensure Network Infrastructure is Up-to-Date)

Asset Type: Network	Security Function: Protect		IG1	IG2	IG3

ตรวจสอบให้แน่ใจว่าโครงสร้างพื้นฐานเครือข่ายมีการอัปเดตอยู่เสมอ ตัวอย่างวิธีการใช้งานได้แก่ การใช้ซอฟต์แวร์เวอร์ชันล่าสุดที่เสถียร และ/หรือการใช้บริการเครือข่ายแบบ NaaS (Network as a Service) ที่ยังได้รับการสนับสนุน ตรวจสอบเวอร์ชัน

ซอฟต์แวร์เป็นรายเดือน หรือตรวจสอบบ่อยครั้งขึ้น เพื่อยืนยันว่าซอฟต์แวร์ยังคงได้รับการสนับสนุน

มาตรการป้องกันที่ 12.2: จัดทำและบำรุงรักษาสถาปัตยกรรมเครือข่ายที่ปลอดภัย (Establish and Maintain a Secure Network Architecture)

Asset Type: Network	Security Function: Protect		IG1 IG2 IG3

ออกแบบและบำรุงรักษาสถาปัตยกรรมเครือข่ายที่ปลอดภัย โดยต้องครอบคลุมการแบ่งส่วนเครือข่าย (segmentation), หลักการสิทธิ์ขั้นต่ำ (least privilege), และการรองรับการใช้งาน (availability) อย่างน้อยที่สุด ตัวอย่างการใช้งานประกอบไปด้วยการจัดทำเอกสาร, นโยบาย, และองค์ประกอบการออกแบบ

มาตรการป้องกันที่ 12.3: จัดการโครงสร้างพื้นฐานเครือข่ายอย่างปลอดภัย (Securely Manage Network Infrastructure)

Asset Type: Network	Security Function: Protect		IG2 IG3

จัดการโครงสร้างพื้นฐานเครือข่ายอย่างปลอดภัย ตัวอย่างการใช้งานประกอบไปด้วยการควบคุมเวอร์ชันการเขียนโค้ดโครงสร้างพื้นฐาน (Infrastructure-as-Code - IaC) และการใช้โปรโตคอลเครือข่ายที่ปลอดภัย เช่น SSH และ HTTPS

มาตรการป้องกันที่ 12.4: จัดทำและบำรุงรักษาแผนผังสถาปัตยกรรม (Establish and Maintain Architecture Diagram(s))

Asset Type: Documentation	Security Function: Govern		IG2 IG3

จัดทำและบำรุงรักษาแผนผังสถาปัตยกรรมและ/หรือเอกสารระบบเครือข่ายอื่น ๆ ตรวจสอบและอัปเดตเอกสารเป็นประจำทุกปี หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญในองค์กรที่อาจส่งผลกระทบต่อนโยบายนี้

มาตรการป้องกันที่ 12.5: รวมศูนย์การยืนยันตัวตน การอนุญาต และการตรวจสอบเครือข่าย (Centralize Network Authentication, Authorization, and Auditing (AAA))

Asset Type: Network	Security Function: Protect		IG2 IG3

รวมศูนย์การจัดการการยืนยันตัวตน (Authentication), การอนุญาต (Authorization), และการตรวจสอบ (Auditing) สำหรับเครือข่าย

มาตรการป้องกันที่ 12.6: ใช้โปรโตคอลการจัดการและการสื่อสารเครือข่ายที่ปลอดภัย (Use of Secure Network Management and Communication Protocols)

Asset Type: Network	Security Function: Protect		IG2 IG3

ใช้โปรโตคอลการจัดการและการสื่อสารเครือข่ายที่ปลอดภัย เช่น 802.1X, Wi-Fi Protected Access 2 (WPA2) Enterprise หรือระดับที่สูงกว่า

มาตรการป้องกันที่ 12.7: ตรวจสอบให้แน่ใจว่าอุปกรณ์ระยะไกลใช้ VPN และเชื่อมต่อกับโครงสร้างพื้นฐาน AAA ขององค์กร (Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise's AAA Infrastructure)

Asset Type: Network	Security Function: Protect		IG2 IG3

กำหนดให้ผู้ใช้ทำการยืนยันตัวตนผ่านบริการ VPN และระบบยืนยันตัวตน (AAA) ที่องค์กรจัดการ ก่อนที่จะเข้าถึงทรัพยากรขององค์กรจากอุปกรณ์ของผู้ใช้งาน

มาตรการป้องกันที่ 12.8: จัดทำและบำรุงรักษาทรัพยากรการประมวลผลเฉพาะสำหรับงานผู้ดูแลระบบ (Establish and Maintain Dedicated Computing Resources for All Administrative Work)

Asset Type: Network	Security Function: Protect		IG2 IG3

จัดทำและบำรุงรักษาทรัพยากรการประมวลผลที่ถูกแยกออกอย่างชัดเจน ทั้งในเชิงกายภาพหรือเชิงตรรกะ สำหรับงานผู้ดูแลระบบหรือการเข้าถึงที่ต้องใช้สิทธิ์ผู้ดูแล ทรัพยากรการประมวลผลเหล่านี้ควรถูกแบ่งแยกจากเครือข่ายหลักขององค์กรและไม่ควรได้รับอนุญาตให้เชื่อมต่ออินเทอร์เน็ต

CONTROL 13

การเฝ้าระวังและป้องกันเครือข่าย (Network Monitoring and Defense)

Safeguards: 11	IG1: 0/11	IG2: 6/11	IG3: 11/11

ภาพรวม (Overview):

ดำเนินกระบวนการและใช้เครื่องมือเพื่อสร้าง และ รักษาการเฝ้าระวังเครือข่ายอย่างครอบคลุม พร้อมกับการป้องกันภัยคุกคามด้านความปลอดภัยบนโครงสร้างพื้นฐานเครือข่ายและผู้ใช้งานภายในองค์กร

เหตุใดมาตรการนี้จึงมีความสำคัญ?

เราไม่สามารถพึ่งพา การป้องกันเครือข่าย ให้มีประสิทธิภาพสมบูรณ์ ได้เสมอไป เนื่องจากฝ่ายตรงข้ามมีการพัฒนาและปรับปรุงเทคนิคอย่างต่อเนื่อง โดยมีการแลกเปลี่ยนหรือขายข้อมูลเกี่ยวกับช่องโหว่และวิธีการหลบเลี่ยงการควบคุมความปลอดภัย แม้เครื่องมือรักษาความปลอดภัยจะทำงานได้ตามที่โฆษณาไว้ แต่การตั้งค่าและปรับแต่งให้เหมาะสมกับความเสี่ยงขององค์กรเป็นสิ่งจำเป็นเพื่อให้เกิดประสิทธิภาพสูงสุด

การตั้งค่าที่ผิดพลาดจากความผิดพลาดของมนุษย์หรือการขาดความรู้เกี่ยวกับความสามารถของเครื่องมือ อาจทำให้องค์กรรู้สึกปลอดภัยโดยไม่ถูกต้อง เครื่องมือรักษาความปลอดภัยจะมีประสิทธิภาพได้ก็ต่อเมื่อรองรับกระบวนการเฝ้าระวังอย่างต่อเนื่อง ซึ่งทำให้เจ้าหน้าที่สามารถรับการแจ้งเตือนและตอบสนองต่อเหตุการณ์ด้านความปลอดภัยได้อย่างรวดเร็ว

องค์กรที่เน้นการใช้เทคโนโลยีเพียงอย่างเดียว อาจพบปัญหาในการรับมือกับการแจ้งเตือนเท็จ เนื่องจากขาดการวิเคราะห์โดยมนุษย์ การระบุและตอบสนองต่อภัยคุกคามต้องอาศัยการมองเห็นได้ครอบคลุมทุกช่องทางในโครงสร้างพื้นฐาน และการใช้มนุษย์ในกระบวนการตรวจจับ การวิเคราะห์ และการตอบสนอง

สำหรับองค์กรขนาดใหญ่หรือองค์กรที่เป็นเป้าหมายหลัก จำเป็นต้องมีความสามารถในการปฏิบัติการด้านความปลอดภัย (Security Operations) เพื่อป้องกัน ตรวจจับ และตอบสนองต่อภัยคุกคามทางไซเบอร์อย่างรวดเร็ว ก่อนที่ภัยคุกคามจะส่งผลกระทบต่อองค์กร กระบวนการนี้จะสร้างรายงานกิจกรรมและตัวชี้วัดที่ช่วยปรับปรุงนโยบายความปลอดภัย และสนับสนุนการปฏิบัติตามกฎระเบียบขององค์กร

เหตุการณ์ในข่าวมักแสดงให้เห็นว่าองค์กรบางแห่งถูกเจาะระบบนานหลายสัปดาห์ หลายเดือน หรือหลายปีกว่าจะตรวจพบ การมีความตระหนักในสถานการณ์อย่างครอบคลุมช่วยลดเวลาการตรวจจับและการตอบสนองได้อย่างมาก ซึ่งเป็นสิ่งสำคัญในการลดผลกระทบเมื่อพบมัลแวร์ การขโมยข้อมูล หรือการรั่วไหลของข้อมูลที่ละเอียดอ่อน

การมีข้อมูลเชิงลึกเกี่ยวกับกลยุทธ์ เทคนิค และวิธีการ (TTPs) ของผู้โจมตี รวมถึงตัวบ่งชี้การโจมตี (IOCs) ช่วยให้องค์กรสามารถระบุภัยคุกคามในอนาคตได้อย่างรวดเร็วและสามารถกู้คืนระบบได้เร็วขึ้น ด้วยการมีข้อมูลที่ครบถ้วนเกี่ยวกับสภาพแวดล้อมและโครงสร้างขององค์กรเพื่อพัฒนากลยุทธ์การตอบสนองที่มีประสิทธิภาพ

ขั้นตอนและเครื่องมือ

องค์กรส่วนใหญ่ไม่จำเป็นต้องสร้างศูนย์ปฏิบัติการด้านความปลอดภัย (SOC) เพื่อให้มีการรับรู้สถานการณ์ด้านความปลอดภัย การเริ่มต้นทำได้โดยการทำความเข้าใจกับฟังก์ชันธุรกิจที่สำคัญ สถาปัตยกรรมเครือข่าย และ เซิร์ฟเวอร์ ข้อมูล และการไหลเวียนของข้อมูล การเชื่อมต่อบริการของผู้ขาย และ พันธมิตรทางธุรกิจ รวมถึงอุปกรณ์และบัญชีของผู้ใช้งาน ปัจจัยเหล่านี้ช่วยพัฒนาโครงสร้างความปลอดภัย การควบคุมทางเทคนิค การบันทึก การเฝ้าระวัง และขั้นตอนการตอบสนอง

หัวใจสำคัญของกระบวนการนี้ คือ การมีทีมที่ผ่านการฝึกอบรมและมีการจัดการอย่างเป็นระบบ เพื่อดำเนินกระบวนการตรวจจับ วิเคราะห์ และแก้ไขเหตุการณ์ด้านความปลอดภัย ความสามารถเหล่านี้สามารถทำได้ทั้งภายในองค์กรหรือจ้างที่ปรึกษาหรือผู้ให้บริการภายนอก (Managed Service Provider) องค์กรควรพิจารณากิจกรรมที่เกี่ยวข้องกับเครือข่าย สินทรัพย์ขององค์กร ข้อมูลประจำตัวผู้ใช้ และการเข้าถึงข้อมูล เทคโนโลยีมีบทบาทสำคัญในการรวบรวม วิเคราะห์ข้อมูล และเฝ้าระวังเครือข่ายและสินทรัพย์ขององค์กร ทั้งภายในและภายนอก นอกจากนี้ ควรรวมถึงการมองเห็นการทำงานบนแพลตฟอร์มคลาวด์ที่อาจไม่สอดคล้องกับเทคโนโลยีรักษาความปลอดภัยในสถานที่ขององค์กร

การส่งต่อบันทึกข้อมูลที่สำคัญทั้งหมดไปยังโปรแกรมการวิเคราะห์ เช่น ระบบจัดการข้อมูลเหตุการณ์ด้านความปลอดภัย (Security Information and Event Management - SIEM) สามารถเพิ่มมูลค่าได้ อย่างไรก็ตาม เครื่องมือเหล่านี้ไม่สามารถให้ภาพรวมที่สมบูรณ์ได้ การตรวจสอบบันทึกข้อมูลรายสัปดาห์เป็นสิ่งจำเป็นในการปรับแต่งเกณฑ์ และ ระบุเหตุการณ์ที่ผิดปกติ เครื่องมือการวิเคราะห์ความสัมพันธ์สามารถทำให้บันทึกการตรวจสอบ (Audit Logs) มีประโยชน์ยิ่งขึ้นสำหรับการตรวจสอบด้วยตนเองในภายหลัง แต่เครื่องมือเหล่านี้ไม่สามารถทดแทนผู้เชี่ยวชาญด้านความปลอดภัยสารสนเทศ และ ผู้ดูแลระบบได้ แม้จะมีเครื่องมือการวิเคราะห์บันทึกอัตโนมัติ แต่ความเชี่ยวชาญ และ สัญชาตญาณของมนุษย์ยังคงเป็นสิ่งจำเป็นในการระบุและทำความเข้าใจกับการโจมตี

เมื่อกระบวนการนี้พัฒนาไป องค์กรจะสร้าง และ รักษาคลังความรู้ที่ช่วยให้เข้าใจ และประเมินความเสี่ยงทางธุรกิจ รวมถึงพัฒนาขีดความสามารถด้านข่าวกรองภัยคุกคามภายใน ข่าวกรองภัยคุกคามคือการรวบรวมกลยุทธ์ เทคนิค และวิธีการ (TTPs) จากเหตุการณ์และฝ่ายตรงข้าม เพื่อให้บรรลุเป้าหมายนี้ โปรแกรมการรับรู้สถานการณ์จะกำหนดและประเมินแหล่งข้อมูลที่เกี่ยวข้องในการตรวจจับ รายงาน และจัดการการโจมตี องค์กรที่มีความพร้อมสามารถพัฒนาไปสู่การล่าภัยคุกคาม (Threat Hunting)

ซึ่งเจ้าหน้าที่ที่ได้รับการฝึกอบรมจะตรวจสอบบันทึกระบบและผู้ใช้งาน การไหลของข้อมูล และรูปแบบการรับส่งข้อมูลด้วยตนเองเพื่อค้นหาความผิดปกติ

มาตรการป้องกันที่ 13.1: การแจ้งเตือนเหตุการณ์ความปลอดภัยแบบรวมศูนย์ (Centralize Security Event Alerting)

Asset Type: Network	Security Function: Detect		IG2 IG3

ทำการแจ้งเตือนเหตุการณ์ความปลอดภัยแบบรวมศูนย์สำหรับสินทรัพย์ขององค์กร เพื่อการวิเคราะห์และการเชื่อมโยงบันทึกข้อมูล การใช้งานที่ดีที่สุดต้องใช้ระบบ SIEM ซึ่งรวมถึงการแจ้งเตือนการเชื่อมโยงเหตุการณ์ที่ผู้ขายกำหนดไว้ แพลตฟอร์มวิเคราะห์บันทึกข้อมูลที่กำหนดค่าด้วยการแจ้งเตือนการเชื่อมโยงที่เกี่ยวข้องกับความปลอดภัย ก็สามารถตอบสนองต่อการป้องกันนี้ได้เช่นกัน

มาตรการป้องกันที่ 13.2: ใช้ระบบตรวจจับการบุกรุกบนโฮสต์ (Deploy a Host-Based Intrusion Detection Solution)

Asset Type: Network	Security Function: Detect		IG2 IG3

ติดตั้งระบบตรวจจับการบุกรุกบนโฮสต์ (Host-Based Intrusion Detection Solution) ในสินทรัพย์ขององค์กร ตามความเหมาะสมและการรองรับ

มาตรการป้องกันที่ 13.3: ใช้ระบบตรวจจับการบุกรุกบนเครือข่าย (Deploy a Network Intrusion Detection Solution)

Asset Type: Network	Security Function: Detect		IG2 IG3

ติดตั้งระบบตรวจจับการบุกรุกบนเครือข่าย (Network Intrusion Detection Solution) ในสินทรัพย์ขององค์กร ตามความเหมาะสม ตัวอย่างการใช้งานรวมถึงระบบตรวจจับการบุกรุกบนเครือข่าย (NIDS) หรือบริการที่เทียบเท่าจากผู้ให้บริการคลาวด์ (CSP)

มาตรการป้องกันที่ 13.4: กรองการรับส่งข้อมูลระหว่างเซกเมนต์เครือข่าย (Perform Traffic Filtering Between Network Segments)

Asset Type: Network	Security Function: Protect		IG2 IG3

ดำเนินการกรองการรับส่งข้อมูลระหว่างเซกเมนต์เครือข่าย ตามความเหมาะสม เพื่อจำกัดการเคลื่อนย้ายของข้อมูลและลดโอกาสที่ผู้โจมตีจะเคลื่อนย้ายไปยังส่วนอื่นของเครือข่าย

มาตรการป้องกันที่ 13.5: จัดการการควบคุมการเข้าถึงสำหรับสินทรัพย์ระยะไกล (Manage Access Control for Remote Assets)

Asset Type: Network	Security Function: Protect		IG2 IG3

จัดการการควบคุมการเข้าถึงสำหรับอุปกรณ์ที่เชื่อมต่อกับทรัพยากรขององค์กรจากระยะไกล กำหนดระดับการเข้าถึงตาม: การติดตั้งซอฟต์แวร์ป้องกันมัลแวร์ที่ทันสมัย การปฏิบัติตามกระบวนการกำหนดค่าความปลอดภัยขององค์กร และการอัปเดตระบบปฏิบัติการและแอปพลิเคชันให้เป็นปัจจุบัน

มาตรการป้องกันที่ 13.6: เก็บบันทึกการไหลของข้อมูลเครือข่าย (Collect Network Traffic Flow Logs)

Asset Type: Network	Security Function: Detect		IG2 IG3

เก็บบันทึกการไหลของข้อมูลเครือข่ายและ/หรือข้อมูลการจราจรบนเครือข่ายเพื่อตรวจสอบและแจ้งเตือนจากอุปกรณ์เครือข่าย

มาตรการป้องกันที่ 13.7: ใช้ระบบป้องกันการบุกรุกบนโฮสต์ (Deploy a Host-Based Intrusion Prevention Solution)

Asset Type: Network	Security Function: Protect		IG3

ติดตั้งระบบป้องกันการบุกรุกบนโฮสต์ในสินทรัพย์ขององค์กร ตามความเหมาะสมและการรองรับ ตัวอย่างการใช้งาน ได้แก่ โปรแกรม Endpoint Detection and Response (EDR) หรือโฮสต์เบส IPS เอเจนต์

มาตรการป้องกันที่ 13.8: ใช้ระบบป้องกันการบุกรุกบนเครือข่าย (Deploy a Network Intrusion Prevention Solution)

Asset Type: Network	Security Function: Protect		IG3

ติดตั้งระบบป้องกันการบุกรุกบนเครือข่าย ตามความเหมาะสม ตัวอย่างการใช้งาน ได้แก่ระบบ Network Intrusion Prevention System (NIPS) หรือบริการที่เทียบเท่าจากผู้ให้บริการคลาวด์ (CSP)

มาตรการป้องกันที่ 13.9: ใช้การควบคุมการเข้าถึงในระดับพอร์ต (Deploy Port-Level Access Control)

Asset Type: Network	Security Function: Protect		IG3

ใช้การควบคุมการเข้าถึงในระดับพอร์ต โดยใช้โปรโตคอลการควบคุมการเข้าถึงเครือข่าย เช่น 802.1x หรือโปรโตคอลอื่น ๆ ที่คล้ายกัน ซึ่งอาจรวมถึงการยืนยันตัวตนของผู้ใช้และ/หรืออุปกรณ์

มาตรการป้องกันที่ 13.10: กรองข้อมูลที่ระดับเลเยอร์แอปพลิเคชัน (Perform Application Layer Filtering)

Asset Type: Network	Security Function: Protect		IG3

ทำการกรองข้อมูลที่ระดับเลเยอร์แอปพลิเคชัน ตัวอย่างการใช้งานได้แก่พร็อกซีกรองข้อมูล ไฟร์วอลล์ระดับเลเยอร์แอปพลิเคชัน หรือเกตเวย์

มาตรการป้องกันที่ 13.11: ปรับแต่งเกณฑ์การแจ้งเตือนเหตุการณ์ความปลอดภัย (Tune Security Event Alerting Thresholds)

Asset Type: Network	Security Function: Protect		IG3

ปรับแต่งเกณฑ์การแจ้งเตือนเหตุการณ์ความปลอดภัยเป็นรายเดือนหรือบ่อยกว่านั้น

CONTROL 14

การสร้างความตระหนักและการฝึกอบรมทักษะด้านความปลอดภัย(Security Awareness and Skills Training)

Safeguards: 9	IG1: 8/9	IG2: 9/9	IG3: 9/9

ภาพรวม (Overview):

จัดตั้งและรักษาโปรแกรมการสร้างความตระหนักด้านความปลอดภัย (Security Awareness) เพื่อปลูกฝังพฤติกรรมที่ตระหนักถึงความปลอดภัยในหมู่พนักงาน และให้พวกเขามีทักษะที่เหมาะสมในการลดความเสี่ยงทางไซเบอร์ขององค์กร

เหตุใดการควบคุมนี้จึงมีความสำคัญ?

การกระทำของผู้ใช้มีบทบาทสำคัญต่อความสำเร็จหรือความล้มเหลวของโปรแกรมรักษาความปลอดภัยขององค์กร การโน้มน้าวให้ผู้ใช้งานคลิกลิงก์หรือเปิดไฟล์แนบที่เป็นอันตราย เพื่อให้มัลแวร์เข้าสู่องค์กรนั้นง่ายกว่าการหาช่องโหว่เครือข่ายโดยตรง

ผู้ใช้งานอาจทำให้เกิดเหตุการณ์ความปลอดภัย ทั้งโดยตั้งใจและไม่ตั้งใจ เช่น:

- การจัดการข้อมูลที่ละเอียดอ่อนอย่างไม่เหมาะสม
- การส่งอีเมลที่มีข้อมูลที่ละเอียดอ่อนไปยังผู้รับผิดคน
- การทำอุปกรณ์พกพาหาย
- การใช้รหัสผ่านที่อ่อนแอหรือใช้รหัสผ่านเดียวกันกับเว็บไซต์สาธารณะ

ไม่มีโปรแกรมรักษาความปลอดภัยใดที่สามารถลดความเสี่ยงทางไซเบอร์ได้อย่างมีประสิทธิภาพ โดยไม่มีกระบวนการจัดการกับช่องโหว่ทางมนุษย์ ผู้ใช้งานในทุกระดับขององค์กรมีความเสี่ยงที่แตกต่างกัน ตัวอย่างเช่น:

- ผู้บริหาร มีการจัดการข้อมูลที่มีความละเอียดอ่อนมากขึ้น
- ผู้ดูแลระบบ มีสิทธิ์ควบคุมการเข้าถึงระบบและแอปพลิเคชัน
- ฝ่ายการเงิน ทรัพยากรมนุษย์ และฝ่ายสัญญา มีการเข้าถึงข้อมูลที่ทำให้พวกเขาเป็นเป้าหมายได้

การฝึกอบรมควรมีการอัปเดตเป็นประจำ เพื่อเพิ่มวัฒนธรรมความปลอดภัยและลดการใช้วิธีการทำงานที่มีความเสี่ยง.

ขั้นตอนและเครื่องมือสำหรับการสร้างความตระหนักและการฝึกอบรมทักษะด้านความปลอดภัย

การออกแบบโปรแกรมการฝึกอบรมที่มีประสิทธิภาพ

โปรแกรมฝึกอบรมความตระหนักด้านความปลอดภัยที่มีประสิทธิภาพควรเป็นมากกว่าการดูวิดีโอการฝึกอบรมปีละครั้ง ควรมีการสื่อสารข้อความและการแจ้งเตือนที่เกี่ยวข้องกับความปลอดภัยบ่อยขึ้น โดยเน้นหัวข้อที่สอดคล้องกับสถานการณ์ปัจจุบัน เช่น:

- การใช้รหัสผ่านที่แข็งแกร่ง เมื่อมีรายงานข่าวเกี่ยวกับการรั่วไหลของข้อมูลการเข้าสู่ระบบ
- การป้องกันฟิชชิง ในช่วงเวลาภาษี
- การรับรู้การหลอกลวง เกี่ยวกับการส่งพัสดุในช่วงเทศกาลวันหยุด

การฝึกอบรมที่สอดคล้องกับกฎระเบียบและภัยคุกคามเฉพาะขององค์กร

การฝึกอบรมควรพิจารณาถึงข้อกำหนดด้านกฎระเบียบและระดับภัยคุกคามเฉพาะขององค์กร เช่น:

- สถาบันการเงิน: เน้นการปฏิบัติตามข้อกำหนดในการจัดการและการใช้ข้อมูล
- องค์กรด้านการดูแลสุขภาพ: เน้นการจัดการข้อมูลสุขภาพ
- ผู้ค้าปลีก: เน้นการจัดการข้อมูลบัตรเครดิต

การฝึกอบรมเกี่ยวกับการโจมตีทางวิศวกรรมสังคม (Social Engineering)

การฝึกอบรมควรรวมถึงการทดสอบฟิชชิงและการรับรู้เทคนิคที่ใช้ในการโจมตีแบบเจาะจงตามบทบาท เช่น:

- ฝ่ายการเงิน: อาจได้รับอีเมลหลอกลวงแบบ BEC (Business Email Compromise) ที่ปลอมเป็นผู้บริหารสั่งให้โอนเงิน
- พนักงานทั่วไป: อาจได้รับอีเมลจากพันธมิตรหรือผู้ขายที่ถูกแฮก เพื่อขอเปลี่ยนแปลงข้อมูลบัญชีธนาคาร

แหล่งข้อมูลที่เป็นประโยชน์สำหรับการสร้างโปรแกรมการฝึกอบรม

NIST SP 800-50: การฝึกอบรมความตระหนักด้านความปลอดภัยข้อมูล

https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf

National Cyber Security Centre (UK): การศึกษาและการสร้างความตระหนักให้กับผู้ใช้

https://www.ncsc.gov.uk/guidance/10-steps-user-education-and-awareness

EDUCAUSE: แคมเปญการสร้างความตระหนักด้านความปลอดภัยทางไซเบอร์

https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program/awareness-campaigns

National Cyber Security Alliance (NCSA): ทรัพยากรสำหรับการรักษาความปลอดภัยออนไลน์

https://staysafeonline.org/

SANS: ทรัพยากรการฝึกอบรมความตระหนักด้านความปลอดภัย

https://www.sans.org/security-awareness-training/resources

CIS Telework and Small Office Network Security Guide: คำแนะนำในการตั้งค่าเราเตอร์ที่บ้าน

https://www.cisecurity.org/white-papers/cis-controls-telework-and-small-office-network-security-guide/

มาตรการป้องกัน (Safeguards)

มาตรการป้องกันที่ 14.1: จัดตั้งและดูแลโปรแกรมการสร้างความตระหนักด้านความปลอดภัย (Establish and Maintain a Security Awareness Program)

Asset Type: Documentation	Security Function: Govern		IG1 IG2 IG3

จัดตั้งและดูแลโปรแกรมการสร้างความตระหนักด้านความปลอดภัย เพื่อให้ความรู้แก่พนักงานเกี่ยวกับวิธีการใช้งานทรัพย์สินและข้อมูลขององค์กรอย่างปลอดภัย

- ดำเนินการฝึกอบรมในช่วงเริ่มงาน และอย่างน้อยปีละครั้ง
- ทบทวนและอัปเดตเนื้อหาการฝึกอบรมทุกปี หรือตามการเปลี่ยนแปลงสำคัญในองค์กรที่อาจส่งผลกระทบต่อนโยบายนี้

มาตรการป้องกันที่ 14.2: ฝึกอบรมพนักงานให้รู้จักการโจมตีทางวิศวกรรมสังคม (Train Workforce Members to Recognize Social Engineering Attacks)

Asset Type: Users	Security Function: Protect		IG1 IG2 IG3

ฝึกอบรมพนักงานให้สามารถระบุการโจมตีทางวิศวกรรมสังคมได้ เช่น:

- ฟิชชิง (Phishing)
- การหลอกลวงทางอีเมลธุรกิจ (Business Email Compromise - BEC)
- การหลอกถามข้อมูล (Pretexting)
- การตามคนเข้าไปในพื้นที่หวงห้าม (Tailgating)

มาตรการป้องกันที่ 14.3: ฝึกอบรมพนักงานเกี่ยวกับแนวปฏิบัติที่ดีที่สุดในการยืนยันตัวตน (Train Workforce Members on Authentication Best Practices)

Asset Type: Users	Security Function: Protect	IG1	IG2	IG3

ฝึกอบรมพนักงานเกี่ยวกับแนวปฏิบัติที่ดีที่สุดในการยืนยันตัวตน หัวข้อการฝึกอบรมอาจรวมถึง:

- การยืนยันตัวตนหลายปัจจัย (MFA)
- การสร้างรหัสผ่านที่ปลอดภัย
- การจัดการข้อมูลประจำตัว (Credential Management)

มาตรการป้องกันที่ 14.4: ฝึกอบรมพนักงานเกี่ยวกับแนวปฏิบัติที่ดีที่สุดในการจัดการข้อมูล (Train Workforce on Data Handling Best Practices)

Asset Type: Users	Security Function: Protect	IG1	IG2	IG3

ฝึกอบรมพนักงานเกี่ยวกับวิธีการระบุ จัดเก็บ โอนย้าย จัดเก็บถาวร และทำลายข้อมูลที่ละเอียดอ่อนอย่างถูกต้อง หัวข้อการฝึกอบรมควรรวมถึง:

- การปฏิบัติตามนโยบายหน้าจอและโต๊ะทำงานที่ชัดเจน (Clear Screen and Desk Policy) เช่น:
- ล็อกหน้าจอเมื่อเดินออกจากอุปกรณ์
- ลบข้อมูลบนกระดานไวท์บอร์ด ทั้งกายภาพ และดิจิทัลหลังการประชุม
- จัดเก็บข้อมูลและทรัพย์สินอย่างปลอดภัย

มาตรการป้องกันที่ 14.5: ฝึกอบรมพนักงานเกี่ยวกับสาเหตุของการเปิดเผยข้อมูลโดยไม่ตั้งใจ (Train Workforce Members on Causes of Unintentional Data Exposure)

Asset Type: Users	Security Function: Protect	IG1	IG2	IG3

ฝึกอบรมพนักงานให้ตระหนักถึงสาเหตุของการเปิดเผยข้อมูลโดยไม่ตั้งใจ ตัวอย่างหัวข้อการฝึกอบรม ได้แก่:

- การส่งข้อมูลที่ละเอียดอ่อนไปผิดผู้รับ
- การทำอุปกรณ์พกพาหาย
- การเผยแพร่ข้อมูลไปยังกลุ่มเป้าหมายที่ไม่ถูกต้อง

มาตรการป้องกันที่ 14.6: ฝึกอบรมพนักงานให้สามารถระบุและรายงานเหตุการณ์ด้านความปลอดภัย (Train Workforce Members on Recognizing and Reporting Security Incidents)

Asset Type: Users	Security Function: Protect	IG1	IG2	IG3

ฝึกอบรมพนักงานให้สามารถระบุเหตุการณ์ด้านความปลอดภัยที่อาจเกิดขึ้น และสามารถรายงานเหตุการณ์ดังกล่าวได้อย่างถูกต้อง

มาตรการป้องกันที่ 14.7: ฝึกอบรมพนักงานให้สามารถระบุและรายงานการขาดการอัปเดตความปลอดภัยในอุปกรณ์ขององค์กร (Train Workforce on How to Identify and Report if Their Enterprise Assets are Missing Security Updates)

Asset Type: Users	Security Function: Protect	IG1	IG2	IG3

ฝึกอบรมพนักงานให้เข้าใจวิธีการตรวจสอบและรายงานการขาดการอัปเดตซอฟต์แวร์หรือความล้มเหลวในกระบวนการและเครื่องมืออัตโนมัติ การฝึกอบรมควรรวมถึงการแจ้งให้ทีม IT ทราบหากพบความผิดพลาดในกระบวนการอัตโนมัติและเครื่องมือต่าง ๆ

มาตรการป้องกันที่ 14.8: ฝึกอบรมพนักงานเกี่ยวกับอันตรายจากการเชื่อมต่อและการส่งข้อมูลผ่านเครือข่ายที่ไม่ปลอดภัย (Train Workforce on the Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks)

Asset Type: Users	Security Function: Protect	IG1	IG2	IG3

ฝึกอบรมพนักงานเกี่ยวกับอันตรายจากการเชื่อมต่อและการส่งข้อมูลผ่านเครือข่ายที่ไม่ปลอดภัยสำหรับกิจกรรมขององค์กร

- สำหรับพนักงานที่ทำงานระยะไกล การฝึกอบรมควรรวมถึงคำแนะนำในการตั้งค่าเครือข่ายภายในบ้านให้ปลอดภัย

มาตรการป้องกันที่ 14.9: ดำเนินการฝึกอบรมความตระหนักและทักษะด้านความปลอดภัยตามบทบาทหน้าที่ (Conduct Role-Specific Security Awareness and Skills Training)

Asset Type: Users	Security Function: Protect	IG2	IG3

จัดให้มีการฝึกอบรมความตระหนักและทักษะด้านความปลอดภัยที่เหมาะสมกับบทบาทหน้าที่เฉพาะในองค์กร ตัวอย่างการใช้งาน ได้แก่:

- หลักสูตรการดูแลระบบอย่างปลอดภัย สำหรับผู้เชี่ยวชาญด้าน IT
- การฝึกอบรมความตระหนัก และการป้องกันช่องโหว่ OWASP® Top 10 สำหรับนักพัฒนาเว็บแอปพลิเคชัน
- การฝึกอบรมการรับรู้การโจมตีทางวิศวกรรมสังคมขั้นสูง สำหรับตำแหน่งที่มีความเสี่ยงสูง เช่น ผู้บริหารระดับสูง

CONTROL 15

การจัดการผู้ให้บริการ (Service Provider Management)

Safeguards: 7		IG1: 1/7	IG2: 4/7	IG3: 7/7

ภาพรวม (Overview):

พัฒนากระบวนการประเมินผู้ให้บริการที่จัดการข้อมูลที่ละเอียดอ่อน หรือรับผิดชอบแพลตฟอร์มและกระบวนการ IT ที่สำคัญขององค์กร เพื่อให้แน่ใจว่าผู้ให้บริการเหล่านี้มีมาตรการปกป้องแพลตฟอร์มและข้อมูลอย่างเหมาะสม

เหตุใดการควบคุมนี้จึงมีความสำคัญ?

ในยุคที่เชื่อมต่อกันอย่างกว้างขวาง องค์กรต้องพึ่งพาผู้ขายและพันธมิตรในการจัดการข้อมูลและโครงสร้างพื้นฐานสำหรับแอปพลิเคชันหรือฟังก์ชันที่สำคัญ

มีตัวอย่างมากมายที่การละเมิดข้อมูลจากบุคคลที่สามส่งผลกระทบต่อองค์กรโดยตรง เช่น:

- การรั่วไหลของข้อมูลบัตรเครดิต ในช่วงปลายยุค 2000 ที่เกิดจากการที่ผู้โจมตีเจาะระบบผู้ให้บริการขนาดเล็กในอุตสาหกรรมค้าปลีก
- การโจมตีแรนซัมแวร์ ที่ส่งผลกระทบต่อธุรกิจทางอ้อม เนื่องจากผู้ให้บริการถูกโจมตีจนไม่สามารถดำเนินการได้ ส่งผลให้ธุรกิจหยุดชะงัก
- ในกรณีที่แย่กว่านั้น การโจมตีแรนซัมแวร์สามารถเข้ารหัสข้อมูลในระบบหลักขององค์กรได้หากมีการเชื่อมต่อโดยตรงกับผู้ให้บริการที่ถูกโจมตี

ข้อกำหนดด้านความปลอดภัยและความเป็นส่วนตัว

กฎระเบียบด้านความปลอดภัยและความเป็นส่วนตัวหลายฉบับกำหนดให้องค์กรต้องขยายการปกป้องไปยังผู้ให้บริการ เช่น:

- HIPAA: สำหรับข้อตกลงกับผู้ร่วมธุรกิจในอุตสาหกรรมการดูแลสุขภาพ
- FFIEC: สำหรับข้อกำหนดในอุตสาหกรรมการเงิน
- Cyber Essentials (U.K.): สำหรับข้อกำหนดในสหราชอาณาจักร

การสร้างความไว้วางใจกับบุคคลที่สามเป็นหัวใจสำคัญของการจัดการความเสี่ยงและการปฏิบัติตามข้อกำหนด (Governance, Risk, and Compliance - GRC) เพราะความเสี่ยงที่ไม่ได้รับการจัดการภายในองค์กรจะถูกโอนไปยังหน่วยงานภายนอก

ความท้าทายในการประเมินผู้ให้บริการ

แม้จะมีการประเมินความปลอดภัยของผู้ให้บริการมานานหลายทศวรรษ แต่ยังไม่มีมาตรฐานสากลในการประเมินความปลอดภัย ส่งผลให้ผู้ให้บริการถูกลูกค้าตรวจสอบหลายครั้งในแต่ละเดือน ซึ่งกระทบต่อประสิทธิภาพการทำงานของผู้ให้บริการเอง

มาตรฐานในอุตสาหกรรมที่มีอยู่ ได้แก่:

- Shared Assessments Program สำหรับอุตสาหกรรมการเงิน
- Higher Education Community Vendor Assessment Toolkit (HECVAT) สำหรับการศึกษาระดับอุดมศึกษา
- บริษัทประกันภัยทางไซเบอร์ ก็มีเกณฑ์การวัดความปลอดภัยของตนเองเช่นกัน

ความเสี่ยงจากผู้ให้บริการขนาดเล็ก

แม้องค์กรจะให้ความสำคัญกับการตรวจสอบบริษัทผู้ให้บริการคลาวด์ขนาดใหญ่หรือผู้ให้บริการแอปพลิเคชันหลัก แต่ผู้ให้บริการขนาดเล็กกลับมีความเสี่ยงมากกว่า เนื่องจากผู้ให้บริการขนาดเล็กมักทำสัญญากับผู้ให้บริการเพิ่มเติม (เช่น ผู้ให้บริการชั้นที่สี่) เพื่อสนับสนุนการทำงานขององค์กรหลัก

การประเมินและการจัดการความเสี่ยงจากผู้ให้บริการจึงเป็นสิ่งสำคัญ เพื่อป้องกันภัยคุกคามที่อาจส่งผลกระทบต่อความปลอดภัยของข้อมูลและการดำเนินธุรกิจขององค์กร.

ขั้นตอนและเครื่องมือสำหรับการจัดการผู้ให้บริการ (Service Provider Management)

กระบวนการการประเมินและติดตามผู้ให้บริการ

การใช้รายการตรวจสอบมาตรฐาน (Standard Checklists)

- ใช้รายการตรวจสอบมาตรฐาน เช่น ISO 27001 หรือ CIS Controls เพื่อประเมินผู้ให้บริการ
- แม้การใช้สเปรดชีตเป็นวิธีดั้งเดิม แต่ปัจจุบันมีแพลตฟอร์มออนไลน์ที่ช่วยให้การจัดการเป็นระบบและเป็นศูนย์กลางมากขึ้น

การประเมินประสิทธิภาพของโปรแกรม

- เน้นที่พื้นฐานของโปรแกรม ไม่ใช่แค่การปฏิบัติตามรายการตรวจสอบ
- ทบทวนการประเมินเป็นประจำทุกปี เนื่องจากความสัมพันธ์และข้อมูลอาจมีการเปลี่ยนแปลง

การสร้างนโยบายและการติดตามความเสี่ยง

1. กำหนดนโยบายการตรวจสอบผู้ให้บริการ
   - สร้างนโยบายที่ชัดเจนเกี่ยวกับการประเมินและการตรวจสอบผู้ให้บริการ

2 การจัดทำรายการผู้ให้บริการ:

- จัดทำบัญชีรายชื่อผู้ให้บริการทั้งหมดที่องค์กรใช้
- กำหนด ระดับความเสี่ยง (Risk Rating) สำหรับผู้ให้บริการแต่ละราย โดยพิจารณาผลกระทบที่อาจเกิดขึ้นต่อธุรกิจหากมีเหตุการณ์ความปลอดภัย

3 การระบุข้อกำหนดในสัญญา

- ระบุภาษาหรือข้อกำหนดในสัญญาที่ทำให้ผู้ให้บริการต้องรับผิดชอบ หากเกิดเหตุการณ์ที่ส่งผลกระทบต่อองค์กร

การใช้แพลตฟอร์มประเมินผู้ให้บริการ

4 แพลตฟอร์มการประเมินจากบุคคลที่สาม (Third-Party Assessment Platforms)

- ใช้แพลตฟอร์มที่มีข้อมูลผู้ให้บริการหลายพันราย เพื่อให้เห็นภาพรวมของอุตสาหกรรมและตัดสินใจเกี่ยวกับความเสี่ยงได้ดีขึ้น
- แพลตฟอร์มเหล่านี้มักมีคะแนนความเสี่ยงแบบไดนามิก ซึ่งได้จากการประเมินทางเทคนิคเชิงรับ (Passive Technical Assessments) หรือข้อมูลเพิ่มเติมจากการประเมินของบริษัทอื่น ๆ

5 การเน้นการประเมินเฉพาะส่วนที่เกี่ยวข้อง

- ในการประเมิน ให้เน้นที่แผนกหรือบริการของผู้ให้บริการที่เกี่ยวข้องโดยตรงกับการสนับสนุนองค์กร

6 การลดความเสี่ยงผ่านบริการจัดการความปลอดภัย

- ผู้ให้บริการที่มีสัญญาบริการรักษาความปลอดภัย หรือมีการทำประกันภัยทางไซเบอร์ จะช่วยลดความเสี่ยงได้

การยกเลิกการใช้บริการอย่างปลอดภัย

กระบวนการ Decommission ผู้ให้บริการ

เมื่อสัญญาสิ้นสุดหรือต้องการยกเลิกบริการ ควรดำเนินการดังนี้:

- ปิดใช้งานบัญชีผู้ใช้งานและบัญชีบริการ
- ยุติการไหลของข้อมูล ระหว่างองค์กรกับผู้ให้บริการ
- ทำลายข้อมูลขององค์กรอย่างปลอดภัย ที่อยู่ในระบบของผู้ให้บริการ

การจัดการผู้ให้บริการอย่างมีประสิทธิภาพช่วยลดความเสี่ยงจากการละเมิดความปลอดภัยของบุคคลที่สาม และช่วยให้องค์กรสามารถควบคุมการปกป้องข้อมูลและระบบที่สำคัญได้อย่างเหมาะสม.

มาตรการป้องกัน (Safeguards)

มาตรการป้องกันที่ 15.1: จัดทำและดูแลรายการผู้ให้บริการ (Establish and Maintain an Inventory of Service Providers)

Asset Type: Users	Security Function: Identify		IG1 IG2 IG3

จัดทำและดูแลรายการผู้ให้บริการ โดยรายการต้องระบุผู้ให้บริการทั้งหมดที่ทราบ รวมถึงการจัดประเภทและข้อมูลการติดต่อภายในองค์กรสำหรับผู้ให้บริการแต่ละราย

- ทบทวนและอัปเดตรายการผู้ให้บริการทุกปี หรือเมื่อมีการเปลี่ยนแปลงสำคัญในองค์กรที่อาจส่งผลกระทบต่อนโยบายนี้

มาตรการป้องกันที่ 15.2: จัดทำและดูแลนโยบายการจัดการผู้ให้บริการ (Establish and Maintain a Service Provider Management Policy)

Asset Type: Users	Security Function: Govern		IG2 IG3

จัดทำและดูแลนโยบายการจัดการผู้ให้บริการ โดยนโยบายต้องครอบคลุม:

- การจัดประเภท
- การจัดทำบัญชีรายชื่อ
- การประเมิน
- การเฝ้าตรวจสอบ
- การยกเลิกการใช้บริการ (Decommissioning)
- ทบทวนและอัปเดตนโยบายทุกปี หรือเมื่อมีการเปลี่ยนแปลงสำคัญในองค์กรที่อาจส่งผลกระทบ

มาตรการป้องกันที่ 15.3: จัดประเภทผู้ให้บริการ (Classify Service Providers)

Asset Type: Users	Security Function: Govern		IG2 IG3

จัดประเภทผู้ให้บริการ โดยพิจารณาลักษณะต่าง ๆ เช่น:

- ความละเอียดอ่อนของข้อมูล
- ปริมาณข้อมูล
- ความต้องการความพร้อมใช้งาน
- ข้อกำหนดด้านกฎระเบียบ
- ความเสี่ยงโดยธรรมชาติ (Inherent Risk)
- ความเสี่ยงที่ถูกลดทอน (Mitigated Risk)

- ทบทวนและอัปเดตการจัดประเภททุกปี หรือเมื่อมีการเปลี่ยนแปลงสำคัญในองค์กร

มาตรการป้องกันที่ 15.4: ตรวจสอบให้แน่ใจว่าสัญญากับผู้ให้บริการรวมข้อกำหนดด้านความปลอดภัย (Ensure Service Provider Contracts Include Security Requirements)

Asset Type: Users	Security Function: Govern		IG2 IG3

ตรวจสอบให้แน่ใจว่าสัญญากับผู้ให้บริการมีข้อกำหนดด้านความปลอดภัย เช่น:

- ข้อกำหนดขั้นต่ำของโปรแกรมความปลอดภัย
- การแจ้งเตือนและการตอบสนองต่อเหตุการณ์ด้านความปลอดภัยและการละเมิดข้อมูล
- ข้อกำหนดการเข้ารหัสข้อมูล
- ข้อกำหนดการทำลายข้อมูลอย่างปลอดภัย
- ข้อกำหนดด้านความปลอดภัยต้องสอดคล้องกับนโยบายการจัดการผู้ให้บริการขององค์กร
- ทบทวนสัญญากับผู้ให้บริการทุกปี เพื่อให้แน่ใจว่าสัญญามีข้อกำหนดด้านความปลอดภัยครบถ้วนและเหมาะสม

มาตรการป้องกันที่ 15.5: ประเมินผู้ให้บริการ (Assess Service Providers)

Asset Type: Users	Security Function: Govern		IG3

ประเมินผู้ให้บริการตามนโยบายการจัดการผู้ให้บริการขององค์กร ขอบเขตการประเมินอาจแตกต่างกันไปตามการจัดประเภท และอาจรวมถึง:

- การตรวจสอบรายงานการประเมินมาตรฐาน เช่น Service Organization Control 2 (SOC 2) และ Payment Card Industry (PCI) Attestation of Compliance (AoC)
- แบบสอบถามที่ปรับแต่งเฉพาะองค์กร
- กระบวนการตรวจสอบที่เหมาะสมและเข้มงวด
- ทำการประเมินผู้ให้บริการอย่างน้อยปีละครั้ง หรือเมื่อมีการทำสัญญาใหม่หรือการต่ออายุสัญญา

มาตรการป้องกันที่ 15.6: เฝ้าตรวจสอบผู้ให้บริการ (Monitor Service Providers)

Asset Type: Users	Security Function: Govern		IG3

เฝ้าตรวจสอบผู้ให้บริการตามนโยบายการจัดการผู้ให้บริการขององค์กร การตรวจสอบอาจรวมถึง:

- การประเมินความสอดคล้องของผู้ให้บริการเป็นระยะ
- การติดตามการอัปเดตและบันทึกการเปลี่ยนแปลงจากผู้ให้บริการ (Release Notes)
- การเฝ้าระวังข้อมูลการละเมิดใน Dark Web

มาตรการป้องกันที่ 15.7: ยกเลิกการใช้บริการผู้ให้บริการอย่างปลอดภัย (Securely Decommission Service Providers)

Asset Type: Users	Security Function: Protect		IG3

ยกเลิกการใช้บริการผู้ให้บริการอย่างปลอดภัย ตัวอย่างการพิจารณา ได้แก่:

- การปิดใช้งานบัญชีผู้ใช้และบัญชีบริการ
- ยุติการไหลของข้อมูล ระหว่างองค์กรและผู้ให้บริการ
- การทำลายข้อมูลขององค์กรอย่างปลอดภัย ที่อยู่ในระบบของผู้ให้บริการ

CONTROL 16

ความปลอดภัยของซอฟต์แวร์แอปพลิเคชัน (Application Software Security)

Safeguards: 14	IG1: 0/14	IG2: 11/14	IG3: 14/14

ภาพรวม (Overview):

จัดการวงจรชีวิตความปลอดภัยของซอฟต์แวร์ที่พัฒนาเอง โฮสต์ หรือจัดหามาใช้ เพื่อป้องกัน ตรวจจับ และแก้ไขจุดอ่อนด้านความปลอดภัยก่อนที่จุดอ่อนเหล่านั้นจะส่งผลกระทบต่อองค์กร

เหตุใดการควบคุมนี้จึงมีความสำคัญ?

แอปพลิเคชันเป็นอินเทอร์เฟซที่ใช้งานง่ายสำหรับผู้ใช้ในการเข้าถึงและจัดการข้อมูลได้อย่างสอดคล้องกับฟังก์ชันธุรกิจ แอปพลิเคชันยังช่วยลดความซับซ้อนในการทำงานที่อาจเกิดข้อผิดพลาด เช่น การเข้าสู่ฐานข้อมูลเพื่อเพิ่มหรือแก้ไขไฟล์

องค์กรใช้แอปพลิเคชันเพื่อจัดการข้อมูลที่ละเอียดอ่อนและควบคุมการเข้าถึงทรัพยากรของระบบ ดังนั้นผู้โจมตีสามารถใช้จุดอ่อนของแอปพลิเคชันเพื่อโจมตีข้อมูลได้โดยตรง แทนที่จะต้องใช้การโจมตีเครือข่ายที่ซับซ้อนเพื่อลบหลีกการควบคุมความปลอดภัย

ความท้าทายในการรักษาความปลอดภัยแอปพลิเคชันในยุคปัจจุบัน

- สภาพแวดล้อมการพัฒนาที่ซับซ้อน: แอปพลิเคชันทำงานบนหลายแพลตฟอร์ม เช่น เว็บ, มือถือ, คลาวด์
- วงจรการพัฒนาที่สั้นลง: การพัฒนาเปลี่ยนจากการใช้ระเบียบวิธีแบบเดิม (Waterfall) มาเป็น DevOps ที่มีการอัปเดตโค้ดบ่อยครั้ง
- การผสมผสานโค้ด: แอปพลิเคชันมักประกอบจากเฟรมเวิร์ค ไลบรารี โค้ดเก่าและโค้ดใหม่
- การปฏิบัติตามกฎระเบียบ: กฎระเบียบการคุ้มครองข้อมูลที่ทันสมัย เช่น GDPR และกฎหมายภาคส่วนต่าง ๆ

ความเสี่ยงจากช่องโหว่ในแอปพลิเคชัน

ช่องโหว่ในแอปพลิเคชันอาจเกิดจาก:

- การออกแบบที่ไม่ปลอดภัย
- โครงสร้างพื้นฐานที่ไม่ปลอดภัย
- ความผิดพลาดในการเขียนโค้ด

- การยืนยันตัวตนที่อ่อนแอ
- การไม่ทดสอบเงื่อนไขที่ผิดปกติ

ตัวอย่างการโจมตีที่พบบ่อย

- บัฟเฟอร์โอเวอร์โฟลว์ (Buffer Overflow)
- SQL Injection
- Cross-Site Scripting (XSS)
- Cross-Site Request Forgery (CSRF)
- Click-Jacking

แอปพลิเคชันและเว็บไซต์ยังสามารถใช้เป็นเครื่องมือในการขโมยข้อมูลประจำตัว การดึงข้อมูล หรือการติดตั้งมัลแวร์บนเครื่องของผู้ใช้งานได้

ความท้าทายในการใช้ SaaS (Software as a Service)

การใช้แพลตฟอร์ม SaaS ซึ่งซอฟต์แวร์ถูกพัฒนาและจัดการโดยบุคคลที่สาม อาจเพิ่มความเสี่ยง เนื่องจากองค์กรอาจขาดความโปร่งใสเกี่ยวกับกระบวนการพัฒนาและมาตรการรักษาความปลอดภัยของผู้ให้บริการ

ขั้นตอนและเครื่องมือ

การพัฒนาเวอร์ชัน 8 ร่วมกับ SAFECode

ในเวอร์ชัน 8 ของ CIS Controls ได้มีการร่วมมือกับ SAFECode เพื่อช่วยพัฒนาขั้นตอนและมาตรการป้องกันสำหรับการควบคุมความปลอดภัยซอฟต์แวร์แอปพลิเคชันที่อัปเดตแล้ว อย่างไรก็ตาม ความปลอดภัยของซอฟต์แวร์แอปพลิเคชันเป็นหัวข้อที่กว้างมาก ดังนั้นจึงมุ่งเน้นเฉพาะมาตรการป้องกันที่สำคัญที่สุด ซึ่งได้มาจากเอกสารประกอบที่พัฒนาโดย SAFECode และสอดคล้องกับเนื้อหาที่มีอยู่ของ SAFECode

แนวทางการพัฒนาแบบสามระดับ (Three-Tiered Development Group Approach)

SAFECode ได้พัฒนาแนวทางการแบ่งกลุ่มการพัฒนาออกเป็นสามระดับ เพื่อช่วยให้องค์กรระบุได้ว่าตนเองอยู่ในกลุ่มใด โดยใช้ระดับความพร้อมในการดำเนินการ (Implementation Group - IG) ของ CIS Controls เป็นแรงบันดาลใจ ดังนี้:

กลุ่มการพัฒนา 1 (Development Group 1 - DG1)

ลักษณะของ DG1

- องค์กรพึ่งพาซอฟต์แวร์สำเร็จรูป (Off-the-Shelf) หรือซอฟต์แวร์โอเพ่นซอร์ส (OSS) เป็นหลัก
- มีการพัฒนาแอปพลิเคชันขนาดเล็กหรือการเขียนโค้ดเว็บไซต์เป็นครั้งคราว

- สามารถปฏิบัติตามแนวปฏิบัติที่ดีที่สุดในระดับพื้นฐาน ทั้งในเชิงปฏิบัติการและเชิงกระบวนการ
- สามารถจัดการความปลอดภัยของซอฟต์แวร์ที่ผู้ขายจัดหาให้ โดยการปฏิบัติตามคำแนะนำของ CIS Controls

แนวทางปฏิบัติที่สำคัญสำหรับ DG1

การใช้ซอฟต์แวร์จากแหล่งที่เชื่อถือได้

- ตรวจสอบให้แน่ใจว่าซอฟต์แวร์สำเร็จรูปและซอฟต์แวร์โอเพ่นซอร์สมาจากแหล่งที่มีความน่าเชื่อถือ

การติดตั้งการอัปเดตและแพตช์ความปลอดภัย

- ดำเนินการติดตั้งการอัปเดตและแพตช์ความปลอดภัยตามที่ผู้จัดจำหน่ายแนะนำ

การใช้แนวปฏิบัติที่ดีที่สุดในการกำหนดค่าและการใช้งานซอฟต์แวร์

- ปฏิบัติตามแนวปฏิบัติที่ดีที่สุดในการติดตั้งและกำหนดค่า เช่น การใช้การยืนยันตัวตนที่เข้มงวดและการจำกัดสิทธิ์การเข้าถึง

การประเมินความปลอดภัยของซอฟต์แวร์จากผู้ให้บริการ

- ประเมินซอฟต์แวร์ที่จัดหาโดยผู้ให้บริการตามมาตรฐานความปลอดภัย เช่น การขอรายงาน SOC 2 หรือการรับรองความปลอดภัยที่เกี่ยวข้อง

การทดสอบแอปพลิเคชันขนาดเล็ก

- สำหรับการพัฒนาแอปพลิเคชันขนาดเล็ก ควรทำการทดสอบช่องโหว่พื้นฐาน เช่น การทดสอบ SQL Injection และ Cross-Site Scripting (XSS)

กลุ่มการพัฒนา 2 (Development Group 2 - DG2)

ลักษณะของ DG2

- องค์กรพึ่งพาซอฟต์แวร์ที่พัฒนาขึ้นเอง (โดยทีมงานภายในหรือผู้รับจ้าง)
- ใช้แอปพลิเคชันที่เป็นเว็บและ/หรือเนทีฟโค้ดที่รวมกับคอมโพเนนต์ของบุคคลที่สาม
- แอปพลิเคชันทำงานบนระบบภายในองค์กร (On-Premises) หรือในคลาวด์
- มีทีมพัฒนาที่ใช้แนวปฏิบัติที่ดีที่สุดสำหรับการพัฒนาซอฟต์แวร์
- ให้ความสำคัญกับคุณภาพและการบำรุงรักษาซอฟต์แวร์โอเพ่นซอร์สหรือซอฟต์แวร์เชิงพาณิชย์ที่ใช้

กลุ่มการพัฒนา 3 (Development Group 3 - DG3)

ลักษณะของ DG3

- องค์กรลงทุนอย่างมากในการพัฒนาซอฟต์แวร์ที่ใช้ดำเนินธุรกิจและให้บริการลูกค้า
- โฮสต์ซอฟต์แวร์บนโครงสร้างพื้นฐานภายใน คลาวด์ หรือทั้งสองอย่าง
- มีการรวมคอมโพเนนต์ซอฟต์แวร์จากโอเพ่นซอร์สและเชิงพาณิชย์จำนวนมาก
- ซอฟต์แวร์ที่พัฒนาโดยผู้ขายและองค์กรที่ให้บริการ SaaS ควรปฏิบัติตามข้อกำหนดของกลุ่มนี้เป็นอย่างน้อย

แนวทางการรักษาความปลอดภัยสำหรับ DG2 และ DG3

- การจัดการช่องโหว่ (Vulnerability Management)
- ผสานกระบวนการจัดการช่องโหว่เข้ากับวงจรการพัฒนา (SDLC)
- ใช้การวิเคราะห์สาเหตุของปัญหา (Root Cause Analysis) เพื่อแก้ไขข้อบกพร่องพื้นฐานและลดช่องโหว่ในอนาคต
- กำหนดระดับความรุนแรง (Severity Rating) เพื่อจัดลำดับความสำคัญในการแก้ไขปัญหา

การฝึกอบรมความปลอดภัยสำหรับนักพัฒนา

- ฝึกอบรมนักพัฒนาเกี่ยวกับแนวคิดการรักษาความปลอดภัยแอปพลิเคชันและการเขียนโค้ดอย่างปลอดภัย
- รวมถึงกระบวนการประเมินและการจัดการซอฟต์แวร์จากบุคคลที่สาม เพื่อตรวจสอบว่าไม่มีช่องโหว่ด้านความปลอดภัย

การรักษาความปลอดภัยโครงสร้างพื้นฐาน

- ใช้แนวทาง CIS Controls 1-7, 12, และ 13 เพื่อลดพื้นที่เสี่ยงในการโจมตี (Attack Surface)
- รักษาความปลอดภัยเครือข่าย ระบบ และบัญชีผู้ใช้งานที่รองรับแอปพลิเคชัน

การแนะนำความปลอดภัยตั้งแต่ต้นใน SDLC

- ผสานการรักษาความปลอดภัยตั้งแต่ขั้นตอนการออกแบบ
- ใช้การทำ Threat Modeling เพื่อระบุและแก้ไขข้อบกพร่องในการออกแบบก่อนการเขียนโค้ด

การใช้โปรแกรม Bug Bounty

- สำหรับทีมพัฒนาขนาดใหญ่หรือทีมเชิงพาณิชย์ ควรพิจารณาใช้โปรแกรม Bug Bounty เพื่อจูงใจให้ผู้เชี่ยวชาญภายนอกค้นหาช่องโหว่

- โปรแกรม Bug Bounty ควรใช้เป็นส่วนเสริมของกระบวนการพัฒนาที่ปลอดภัย

แหล่งข้อมูลเพิ่มเติมสำหรับการรักษาความปลอดภัยแอปพลิเคชัน

SAFECode Application Security Addendum

 https://safecode.org/cis-controls/

NIST® Secure Software Development Framework (SSDF)

 https://csrc.nist.gov/News/2020/mitigating-risk-of-software-vulns-ssdf

The Software Alliance

 https://www.bsa.org/reports/updated-bsa-framework-for-secure-software

OWASP® (Open Web Application Security Project)

 https://owasp.org/

มาตรการป้องกันที่ 16.1: จัดทำและดูแลกระบวนการพัฒนาซอฟต์แวร์อย่างปลอดภัย (Establish and Maintain a Secure Application Development Process)

Asset Type: Users	Security Function: Govern		IG2 IG3

จัดทำและดูแลกระบวนการพัฒนาซอฟต์แวร์อย่างปลอดภัย โดยในกระบวนการนี้ควรรวมถึง:

- มาตรฐานการออกแบบแอปพลิเคชันอย่างปลอดภัย
- แนวปฏิบัติในการเขียนโค้ดอย่างปลอดภัย
- การฝึกอบรมนักพัฒนา
- การจัดการช่องโหว่
- การรักษาความปลอดภัยของโค้ดจากบุคคลที่สาม
- ขั้นตอนการทดสอบความปลอดภัยของแอปพลิเคชัน
- ทบทวนและอัปเดตเอกสารทุกปี หรือตามการเปลี่ยนแปลงสำคัญในองค์กรที่อาจส่งผลกระทบต่อมาตรการนี้

มาตรการป้องกันที่ 16.2: จัดทำและดูแลกระบวนการยอมรับและจัดการช่องโหว่ของซอฟต์แวร์ (Establish and Maintain a Process to Accept and Address Software Vulnerabilities)

Asset Type: Users	Security Function: Govern		IG2 IG3

จัดทำและดูแลกระบวนการสำหรับการยอมรับและจัดการรายงานช่องโหว่ของซอฟต์แวร์ ซึ่งรวมถึง:

- นโยบายการจัดการช่องโหว่ ที่ระบุขั้นตอนการรายงาน
- ผู้รับผิดชอบการจัดการรายงานช่องโหว่
- กระบวนการรับเรื่อง มอบหมาย แก้ไข และทดสอบการแก้ไข

ใช้ระบบติดตามช่องโหว่ที่รวมถึงการจัดระดับความรุนแรงและตัวชี้วัดสำหรับการวัดระยะเวลาในการระบุ วิเคราะห์ และแก้ไขช่องโหว่

- ทบทวนและอัปเดตเอกสารทุกปี หรือตามการเปลี่ยนแปลงสำคัญในองค์กร

หมายเหตุสำหรับนักพัฒนาซอฟต์แวร์บุคคลที่สาม: ควรพิจารณานโยบายนี้เป็นนโยบายที่เผยแพร่สู่ภายนอก เพื่อกำหนดความคาดหวังให้กับผู้มีส่วนได้ส่วนเสียภายนอก

มาตรการป้องกันที่ 16.3: ดำเนินการวิเคราะห์สาเหตุของช่องโหว่ด้านความปลอดภัย (Perform Root Cause Analysis on Security Vulnerabilities)

Asset Type: Users	Security Function: Protect		IG2 IG3

ดำเนินการวิเคราะห์สาเหตุของช่องโหว่ด้านความปลอดภัย (Root Cause Analysis) เมื่อทำการตรวจสอบช่องโหว่ โดยการวิเคราะห์สาเหตุจะช่วยให้ทีมพัฒนาสามารถระบุปัญหาพื้นฐานที่ทำให้เกิดช่องโหว่ และช่วยให้การแก้ไขปัญหาเป็นไปอย่างยั่งยืน แทนที่จะมุ่งแก้ไขเฉพาะช่องโหว่ที่พบในแต่ละครั้ง

มาตรการป้องกันที่ 16.4: จัดทำและจัดการรายการส่วนประกอบซอฟต์แวร์จากบุคคลที่สาม (Establish and Manage an Inventory of Third-Party Software Components)

Asset Type: Users	Security Function: Identify		IG2 IG3

จัดทำและดูแลรายการส่วนประกอบซอฟต์แวร์จากบุคคลที่สามที่ใช้ในการพัฒนา ซึ่งมักเรียกว่า “Bill of Materials (BOM)” รวมถึงส่วนประกอบที่วางแผนจะใช้ในอนาคต

- รายการนี้ต้องรวมถึงความเสี่ยงที่ส่วนประกอบแต่ละรายการอาจก่อให้เกิด
- ประเมินรายการอย่างน้อยเดือนละครั้ง เพื่อตรวจสอบการเปลี่ยนแปลงหรือการอัปเดต และยืนยันว่าส่วนประกอบยังได้รับการสนับสนุนอยู่

มาตรการป้องกันที่ 16.5: ใช้ส่วนประกอบซอฟต์แวร์จากบุคคลที่สามที่น่าเชื่อถือและทันสมัย (Use Up-to-Date and Trusted Third-Party Software Components)

Asset Type: Users	Security Function: Protect		IG2 IG3

ใช้ส่วนประกอบซอฟต์แวร์จากบุคคลที่สามที่น่าเชื่อถือและมีการอัปเดตล่าสุด

- เลือกใช้เฟรมเวิร์คและไลบรารีที่ได้รับการพิสูจน์แล้วว่ามีความปลอดภัย
- จัดหาส่วนประกอบเหล่านี้จากแหล่งที่เชื่อถือได้ หรือทำการประเมินหาช่องโหว่ก่อนการใช้งาน

มาตรการป้องกันที่ 16.6: จัดทำ และดูแลระบบการจัดอันดับความรุนแรง และกระบวนการสำหรับช่องโหว่ในแอปพลิเคชัน (Establish and Maintain a Severity Rating System and Process for Application Vulnerabilities)

Asset Type: Users	Security Function: Govern		IG2 IG3

จัดทำและดูแลระบบการจัดอันดับความรุนแรงและกระบวนการสำหรับช่องโหว่ในแอปพลิเคชัน เพื่อช่วยในการจัดลำดับความสำคัญในการแก้ไขช่องโหว่

- กำหนดระดับความปลอดภัยขั้นต่ำสำหรับการปล่อยโค้ดหรือแอปพลิเคชัน
- การจัดอันดับความรุนแรงช่วยให้การจัดการความเสี่ยงเป็นระบบและมั่นใจได้ว่าช่องโหว่ที่รุนแรงที่สุดจะถูกแก้ไขก่อน
- ทบทวนและอัปเดตระบบการจัดอันดับและกระบวนการนี้ทุกปี

มาตรการป้องกันที่ 16.7: ใช้แม่แบบการตั้งค่าความปลอดภัยมาตรฐานสำหรับโครงสร้างพื้นฐานแอปพลิเคชัน ประเภทสินทรัพย์: ซอฟต์แวร์ (Use Standard Hardening Configuration Templates for Application Infrastructure)

Asset Type: Users	Security Function: Protect		IG2 IG3

ใช้แม่แบบการตั้งค่าความปลอดภัยมาตรฐานจากอุตสาหกรรม (Standard Hardening Configuration Templates) สำหรับส่วนประกอบโครงสร้างพื้นฐานแอปพลิเคชัน เช่น:

- เซิร์ฟเวอร์ ฐานข้อมูล และเว็บเซิร์ฟเวอร์
- คอนเทนเนอร์บนคลาวด์
- ส่วนประกอบ Platform as a Service (PaaS)
- ส่วนประกอบ Software as a Service (SaaS)
- ห้ามให้ซอฟต์แวร์ที่พัฒนาเองทำให้การตั้งค่าความปลอดภัยที่แข็งแกร่ง (Hardening) อ่อนแอลง

มาตรการป้องกันที่ 16.8: แยกระบบการทำงานจริงและระบบทดสอบออกจากกัน (Separate Production and Non-Production Systems)

Asset Type: Users	Security Function: Protect		IG2 IG3

แยกสภาพแวดล้อมสำหรับระบบการทำงานจริง (Production) และระบบทดสอบ (Non-Production) ออกจากกัน เพื่อป้องกันความเสี่ยงที่อาจเกิดขึ้นจากการทดสอบหรือพัฒนาซอฟต์แวร์ที่อาจส่งผลกระทบต่อระบบการทำงานจริง

มาตรการป้องกันที่ 16.9: ฝึกอบรมนักพัฒนาเกี่ยวกับแนวคิดการรักษาความปลอดภัยแอปพลิเคชันและการเขียนโค้ดอย่างปลอดภัย (Train Developers in Application Security Concepts and Secure Coding)

Asset Type: Users	Security Function: Protect	IG2 IG3

มั่นใจว่านักพัฒนาซอฟต์แวร์ทุกคนได้รับการฝึกอบรมเกี่ยวกับการเขียนโค้ดอย่างปลอดภัย ตามสภาพแวดล้อมและบทบาทความรับผิดชอบของพวกเขา

- หัวข้อการฝึกอบรมอาจรวมถึงหลักการความปลอดภัยทั่วไปและแนวปฏิบัติมาตรฐานด้านความปลอดภัยของแอปพลิเคชัน
- ดำเนินการฝึกอบรมอย่างน้อยปีละครั้ง
- ออกแบบการฝึกอบรมเพื่อส่งเสริมวัฒนธรรมความปลอดภัยในทีมพัฒนา

มาตรการป้องกันที่ 16.10: ใช้หลักการออกแบบที่ปลอดภัยในสถาปัตยกรรมแอปพลิเคชัน (Apply Secure Design Principles in Application Architectures)

Asset Type: Users	Security Function: Protect	IG2 IG3

ใช้หลักการออกแบบที่ปลอดภัยในสถาปัตยกรรมแอปพลิเคชัน เช่น:

1. หลักการสิทธิ์ขั้นต่ำ (Least Privilege): ให้สิทธิ์เฉพาะที่จำเป็นเท่านั้น
2. การตรวจสอบอินพุตจากผู้ใช้ (Never Trust User Input): ตรวจสอบความถูกต้องของข้อมูลทุกครั้ง เช่น ขนาด ประเภทข้อมูล และรูปแบบที่ยอมรับได้
3. การลดพื้นที่เสี่ยงในการโจมตี (Attack Surface):
   - ปิดพอร์ตและบริการที่ไม่ปลอดภัย
   - ลบโปรแกรมและไฟล์ที่ไม่จำเป็น
   - เปลี่ยนชื่อหรือลบบัญชีผู้ใช้เริ่มต้น

มาตรการป้องกันที่ 16.11: ใช้โมดูลหรือบริการที่ผ่านการตรวจสอบสำหรับส่วนประกอบความปลอดภัยของแอปพลิเคชัน (Leverage Vetted Modules or Services for Application Security Components)

Asset Type: Users	Security Function: Identify	IG2 IG3

ใช้โมดูลหรือบริการที่ผ่านการตรวจสอบแล้วสำหรับส่วนประกอบความปลอดภัยของแอปพลิเคชัน เช่น:

- การจัดการข้อมูลประจำตัว (Identity Management)
- การเข้ารหัส (Encryption)
- การบันทึกและการตรวจสอบ (Auditing and Logging)

การใช้ฟีเจอร์แพลตฟอร์มที่มีอยู่สำหรับฟังก์ชันความปลอดภัยที่สำคัญจะช่วยลดภาระงานของนักพัฒนาและลดโอกาสเกิดข้อผิดพลาดในการออกแบบหรือการใช้งาน

- เลือกใช้เฉพาะอัลกอริทึมการเข้ารหัสที่เป็นมาตรฐาน ยอมรับในปัจจุบัน และผ่านการตรวจสอบอย่างกว้างขวาง
- ระบบปฏิบัติการสมัยใหม่มีเครื่องมือที่มีประสิทธิภาพสำหรับการยืนยันตัวตน การอนุญาต และการสร้างบันทึกการตรวจสอบที่ปลอดภัย

มาตรการป้องกันที่ 16.12: ดำเนินการตรวจสอบความปลอดภัยในระดับโค้ด (Implement Code-Level Security Checks)

Asset Type: Users	Security Function: Protect		IG2 IG3

ใช้เครื่องมือวิเคราะห์โค้ดทั้งแบบ Static Analysis (การวิเคราะห์แบบนิ่ง) และ Dynamic Analysis (การวิเคราะห์แบบไดนามิก) ภายในวงจรชีวิตการพัฒนาแอปพลิเคชัน เพื่อตรวจสอบว่ามีการปฏิบัติตามแนวปฏิบัติการเขียนโค้ดอย่างปลอดภัย

- Static Analysis: วิเคราะห์โค้ดโดยไม่ต้องรันแอปพลิเคชัน
- Dynamic Analysis: วิเคราะห์โค้ดในขณะที่แอปพลิเคชันกำลังทำงาน

มาตรการป้องกันที่ 16.13: ดำเนินการทดสอบเจาะระบบแอปพลิเคชัน (Conduct Application Penetration Testing)

Asset Type: Users	Security Function: Detect		IG2 IG3

ดำเนินการทดสอบเจาะระบบ (Penetration Testing) สำหรับแอปพลิเคชัน โดยเฉพาะสำหรับแอปพลิเคชันที่สำคัญ

- การทดสอบแบบ Authenticated Penetration Testing เหมาะสำหรับการค้นหาช่องโหว่ในตรรกะธุรกิจมากกว่าการสแกนโค้ดหรือการทดสอบอัตโนมัติ
- การทดสอบนี้อาศัยทักษะของผู้ทดสอบในการจำลองการโจมตีทั้งแบบ Authenticated (มีการยืนยันตัวตน) และ Unauthenticated (ไม่มีการยืนยันตัวตน)

มาตรการป้องกันที่ 16.14: ดำเนินการทำ Threat Modeling (Conduct Threat Modeling)

Asset Type: Users	Security Function: Protect		IG3

ดำเนินการทำ Threat Modeling ซึ่งเป็นกระบวนการระบุและแก้ไขข้อบกพร่องในการออกแบบความปลอดภัยของแอปพลิเคชันก่อนการเขียนโค้ด

- Threat Modeling ดำเนินการโดยผู้เชี่ยวชาญที่ได้รับการฝึกอบรมเฉพาะ
- ประเมินการออกแบบแอปพลิเคชันและประเมินความเสี่ยงด้านความปลอดภัยสำหรับแต่ละจุดเข้าใช้งานและระดับการเข้าถึง
- เป้าหมาย: ทำแผนที่แอปพลิเคชัน สถาปัตยกรรม และโครงสร้างพื้นฐานอย่างเป็นระบบเพื่อทำความเข้าใจจุดอ่อน

CONTROL 17

การจัดการการตอบสนองต่อเหตุการณ์ (Incident Response Management)

Safeguards: 9	IG1: 3/9	IG2:	IG3:

ภาพรวม (Overview):

จัดตั้งโปรแกรมเพื่อพัฒนาและรักษาความสามารถในการตอบสนองต่อเหตุการณ์ (เช่น นโยบาย, แผน, ขั้นตอนปฏิบัติ, บทบาทที่กำหนดไว้, การฝึกอบรม และการสื่อสาร) เพื่อเตรียมพร้อม ตรวจจับ และตอบสนองต่อการโจมตีได้อย่างรวดเร็ว

เหตุใดการควบคุมนี้จึงมีความสำคัญ?

โปรแกรมความปลอดภัยทางไซเบอร์ที่ครอบคลุมต้องมีทั้งการ ป้องกัน (Protection), การตรวจจับ (Detection), การตอบสนอง (Response) และ การกู้คืน (Recovery) อย่างไรก็ตาม ในหลายองค์กรที่ยังไม่เติบโตเต็มที่ มักจะละเลยการตอบสนองและการกู้คืน หรือใช้วิธีการตอบสนองที่ไม่เพียงพอ เช่น การฟื้นฟูระบบกลับสู่สถานะเดิมโดยไม่วิเคราะห์เหตุการณ์

เป้าหมายหลักของการตอบสนองต่อเหตุการณ์

- ระบุภัยคุกคาม ก่อนที่จะแพร่กระจาย
- ตอบสนองและแก้ไข ก่อนที่จะสร้างความเสียหาย
- เข้าใจขอบเขตของเหตุการณ์ เพื่อป้องกันไม่ให้เกิดซ้ำ

หากองค์กรไม่มีแผนที่เป็นลายลักษณ์อักษร ต่อให้มีบุคลากรที่มีความสามารถ ก็จะไม่สามารถดำเนินการตรวจสอบ, รายงาน, เก็บรวบรวมข้อมูล, กำหนดความรับผิดชอบทางกฎหมาย, และวางแผนการสื่อสารได้อย่างมีประสิทธิภาพ

ความสำคัญของการสื่อสาร

1. การสื่อสารกับผู้มีส่วนได้ส่วนเสีย เป็นหัวใจสำคัญในการลดผลกระทบจากเหตุการณ์ทางไซเบอร์
2. ผู้นำองค์กรจำเป็นต้องเข้าใจผลกระทบที่อาจเกิดขึ้น เพื่อช่วยจัดลำดับความสำคัญในการแก้ไขหรือกู้คืนระบบ
3. การตัดสินใจทางธุรกิจอาจขึ้นอยู่กับ:
   - การปฏิบัติตามข้อกำหนดทางกฎหมาย
   - กฎการเปิดเผยข้อมูล
   - ข้อตกลงระดับการให้บริการ (SLAs) กับพันธมิตรหรือลูกค้า
   - ผลกระทบต่อรายได้ หรือภารกิจขององค์กร

ความสำคัญของเวลาในการตรวจพบการโจมตี

- Dwell Time: ระยะเวลาที่ผู้โจมตีอยู่ในโครงสร้างพื้นฐานขององค์กรโดยไม่ถูกตรวจพบ อาจยาวนานหลายวัน หลายสัปดาห์ หรือหลายเดือน
- ยิ่งผู้โจมตีอยู่ได้นานเท่าไร ก็ยิ่งสามารถฝังตัวและสร้างวิธีการเข้าถึงแบบถาวรได้มากขึ้น
- แรนซัมแวร์: ผู้โจมตีมักจะขโมยข้อมูลก่อนทำการเข้ารหัสเพื่อเรียกค่าไถ่ ดังนั้นการลด Dwell Time จึงเป็นสิ่งสำคัญอย่างยิ่ง

ขั้นตอนและเครื่องมือ

การจัดทำแผนการตอบสนองต่อเหตุการณ์

1 จัดทำแผนการตอบสนองที่เป็นลายลักษณ์อักษร

แม้องค์กรจะไม่มีทรัพยากรสำหรับการตอบสนองภายใน ควรมีแผนที่กำหนดไว้ชัดเจน ซึ่งประกอบด้วย:

- แหล่งข้อมูลสำหรับการป้องกันและการตรวจจับภัยคุกคาม
- รายชื่อผู้ที่จะเรียกใช้ความช่วยเหลือจากภายนอก เช่น ผู้เชี่ยวชาญหรือที่ปรึกษาด้านความปลอดภัย
- แผนการสื่อสารเพื่อแจ้งข้อมูลแก่ผู้บริหาร พนักงาน หน่วยงานกำกับดูแล คู่ค้า และลูกค้า

การฝึกอบรมและการทดสอบแผนการตอบสนอง

2 การฝึกอบรมตามสถานการณ์ (Scenario-Based Training)

- ให้ทีมตบสนองต่อเหตุการณ์หรือผู้เชี่ยวชาญภายนอก ดำเนินการฝึกซ้อมตามสถานการณ์การโจมตีที่จำลองขึ้น
- สถานการณ์ควรปรับให้เหมาะกับภัยคุกคามและผลกระทบที่อาจเกิดขึ้นกับองค์กร
- การฝึกซ้อมช่วยให้ผู้บริหารและทีมเทคนิคเข้าใจบทบาทของตนในกระบวนการตอบสนอง

3 การระบุและแก้ไขช่องว่างในแผนการตอบสนอง

- การฝึกอบรมและการทดสอบมักจะพบช่องว่างในแผนและกระบวนการ รวมถึงการพึ่งพาที่ไม่คาดคิด
- ปรับปรุงแผนการตอบสนองตามผลการฝึกซ้อม

การเพิ่มความสามารถในการระบุภัยคุกคาม

4 การใช้ Threat Intelligence และ Threat Hunting

- องค์กรที่มีความพร้อมสูงควรผสาน Threat Intelligence (ข่าวกรองภัยคุกคาม) และ Threat Hunting (การล่าภัยคุกคาม) ในกระบวนการตอบสนอง
- ระบุผู้โจมตีหลักหรือกลุ่มผู้โจมตีที่มุ่งเป้าไปยังอุตสาหกรรมขององค์กร
- มุ่งเน้นการตรวจจับและกำหนดขั้นตอนการตอบสนองเพื่อระบุและแก้ไขปัญหาได้รวดเร็วขึ้น

ขั้นตอนที่แนะนำจาก CIS Control 17

มาตรการป้องกันใน CIS Control 17 ให้ขั้นตอนที่มีความสำคัญสูงที่สามารถเพิ่มความปลอดภัยให้กับองค์กร และควรรวมไว้ในแผนการตอบสนองที่ครอบคลุม

แหล่งข้อมูลเพิ่มเติมที่แนะนำ

CREST Cyber Security Incident Response Guide

- Council of Registered Security Testers (CREST) ให้คำแนะนำ มาตรฐาน และความรู้ในหลากหลายหัวข้อด้านการป้องกันทางไซเบอร์

ลิงก์สำหรับดาวน์โหลดคู่มือ:

https://www.crest-approved.org/wp-content/uploads/2022/04/CSIR-Procurement-Guide-1.pdf

ประโยชน์ของการปฏิบัติตามแนวทางเหล่านี้

- เพิ่มความพร้อมในการรับมือกับเหตุการณ์: ช่วยให้ทีมสามารถตรวจจับและตอบสนองต่อการโจมตีได้อย่างรวดเร็วและมีประสิทธิภาพ
- ปรับปรุงกระบวนการอย่างต่อเนื่อง: การฝึกอบรมและการทดสอบช่วยให้สามารถปรับปรุงแผนให้เหมาะสมกับภัยคุกคามที่เปลี่ยนแปลง
- การสื่อสารที่มีประสิทธิภาพ: ช่วยให้การสื่อสารกับผู้มีส่วนได้ส่วนเสียในช่วงวิกฤตเป็นไปอย่างราบรื่น
- ลด Dwell Time: ลดระยะเวลาที่ผู้โจมตีแฝงตัวอยู่ในระบบ

การมีแผนการตอบสนองต่อเหตุการณ์ที่ชัดเจน ช่วยให้การจัดการภัยคุกคามเป็นไปอย่างมีประสิทธิภาพและสร้างความมั่นใจให้กับองค์กรในการรับมือกับความเสี่ยงทางไซเบอร์.

มาตรการป้องกัน (Safeguards)

มาตรการป้องกันที่ 17.1: กำหนดบุคลากรที่รับผิดชอบการจัดการเหตุการณ์ (Conduct Application Penetration Testing)

Asset Type: Users	Security Function: Respond		IG1 IG2 IG3

กำหนดบุคคลหลัก 1 คน และผู้สำรองอย่างน้อย 1 คน เพื่อจัดการกระบวนการตอบสนองต่อเหตุการณ์ในองค์กร

- บุคลากรที่ได้รับมอบหมายมีหน้าที่ในการประสานงานและจัดทำเอกสารการตอบสนองและการกู้คืนจากเหตุการณ์
- อาจเป็นพนักงานภายในองค์กร ผู้ให้บริการจากภายนอก หรือรูปแบบผสม
- หากใช้ผู้ให้บริการภายนอก ให้กำหนดบุคคลภายในองค์กรอย่างน้อย 1 คนเพื่อดูแลการทำงานของผู้ให้บริการ
- ทบทวนเป็นประจำทุกปี หรือเมื่อมีการเปลี่ยนแปลงสำคัญในองค์กรที่อาจส่งผลกระทบต่อมาตรการนี้

มาตรการป้องกันที่ 17.2: จัดทำและดูแลข้อมูลการติดต่อสำหรับการรายงานเหตุการณ์ความปลอดภัย (Establish and Maintain Contact Information for Reporting Security Incidents)

Asset Type: Documentation	Security Function: Govern		IG1	IG2	IG3

จัดทำและดูแลข้อมูลการติดต่อสำหรับฝ่ายที่ต้องได้รับแจ้งเมื่อเกิดเหตุการณ์ความปลอดภัย

ผู้ติดต่ออาจรวมถึง:

- พนักงานภายใน
- ผู้ให้บริการภายนอก
- หน่วยงานบังคับใช้กฎหมาย
- บริษัทประกันภัยทางไซเบอร์
- หน่วยงานรัฐบาลที่เกี่ยวข้อง
- พันธมิตร ISAC (Information Sharing and Analysis Center)
- ผู้มีส่วนได้ส่วนเสียอื่น ๆ
- ตรวจสอบข้อมูลการติดต่อเป็นประจำทุกปี เพื่อให้แน่ใจว่าข้อมูลเป็นปัจจุบัน

มาตรการป้องกันที่ 17.3: จัดทำและดูแลกระบวนการรายงานเหตุการณ์ขององค์กร (Establish and Maintain an Enterprise Process for Reporting Incidents)

Asset Type: Documentation	Security Function: Govern		IG1	IG2	IG3

จัดทำและดูแลกระบวนการที่ชัดเจนสำหรับให้พนักงานรายงานเหตุการณ์ความปลอดภัย ซึ่งควรรวมถึง:

- กรอบเวลาการรายงาน

- บุคคลที่ต้องรายงานเหตุการณ์
- ช่องทางการรายงาน
- ข้อมูลขั้นต่ำที่ต้องรายงาน
- กระบวนการนี้ต้องเผยแพร่ให้พนักงานทุกคนทราบ
- ทบทวนเป็นประจำทุกปี หรือเมื่อมีการเปลี่ยนแปลงสำคัญในองค์กร

มาตรการป้องกันที่ 17.4: จัดทำและดูแลกระบวนการตอบสนองต่อเหตุการณ์ (Establish and Maintain an Incident Response Process)

Asset Type: Documentation	Security Function: Govern		IG2 IG3

จัดทำและดูแลกระบวนการตอบสนองต่อเหตุการณ์ที่เป็นลายลักษณ์อักษร โดยควรครอบคลุม:

- บทบาทและความรับผิดชอบ
- ข้อกำหนดการปฏิบัติตามกฎระเบียบ
- แผนการสื่อสาร
- ทบทวนเป็นประจำทุกปี หรือเมื่อมีการเปลี่ยนแปลงสำคัญในองค์กร

มาตรการป้องกันที่ 17.5: มอบหมายบทบาท และความรับผิดชอบหลัก (Assign Key Roles and Responsibilities)

Asset Type: Users	Security Function: Respond		IG2 IG3

มอบหมายบทบาทและความรับผิดชอบหลักสำหรับการตอบสนองต่อเหตุการณ์ ซึ่งควรรวมถึง:

- ทีมตอบสนองต่อเหตุการณ์
- นักวิเคราะห์ความปลอดภัย
- ผู้ให้บริการภายนอกที่เกี่ยวข้อง
- ทบทวนเป็นประจำทุกปี หรือเมื่อมีการเปลี่ยนแปลงสำคัญในองค์กรก

มาตรการป้องกันที่ 17.6: กำหนดกลไกการสื่อสารระหว่างการตอบสนองต่อเหตุการณ์ (Define Mechanisms for Communicating During Incident Response)

Asset Type: Users	Security Function: Respond		IG2 IG3

กำหนดกลไกหลัก และกลไกรอง สำหรับการสื่อสารและการรายงานในระหว่างเกิดเหตุการณ์ความปลอดภัย

กลไกการสื่อสารที่สามารถใช้ได้ เช่น:

- เบอร์โทรศัพท์
- อีเมล
- แชทที่ปลอดภัย (Secure Chat)
- จดหมายแจ้งเตือน

พิจารณาว่ากลไกบางอย่าง เช่น อีเมล อาจได้รับผลกระทบระหว่างเกิดเหตุการณ์

ทบทวนเป็นประจำทุกปี หรือเมื่อมีการเปลี่ยนแปลงสำคัญในองค์กรที่อาจส่งผลกระทบต่อมาตรการนี้:

มาตรการป้องกันที่ 17.7: ดำเนินการฝึกซ้อมการตอบสนองต่อเหตุการณ์เป็นประจำ (Conduct Routine Incident Response Exercises)

Asset Type: Users	Security Function: Respond		IG2 IG3

วางแผนและดำเนินการฝึกซ้อมการตอบสนองต่อเหตุการณ์และสถานการณ์จำลองสำหรับบุคลากรหลักที่เกี่ยวข้อง

การฝึกซ้อมควรทดสอบ:

- ช่องทางการสื่อสาร
- การตัดสินใจ
- ขั้นตอนการทำงาน
- ดำเนินการฝึกซ้อมอย่างน้อยปีละครั้ง

มาตรการป้องกันที่ 17.8: ดำเนินการทบทวนหลังเหตุการณ์ (Conduct Post-Incident Reviews)

Asset Type: Users	Security Function: Respond		IG2 IG3

ดำเนินการทบทวนหลังเกิดเหตุการณ์ (Post-Incident Review) เพื่อป้องกันการเกิดซ้ำของเหตุการณ์

การทบทวนควรมุ่งเน้นที่:

- บทเรียนที่ได้เรียนรู้ (Lessons Learned)
- การดำเนินการติดตามผล (Follow-Up Actions)

มาตรการป้องกันที่ 17.9: จัดทำและดูแลเกณฑ์สำหรับการระบุเหตุการณ์ความปลอดภัย (Establish and Maintain Security Incident Thresholds)

Asset Type: Users	Security Function: Respond		IG3

จัดทำและดูแลเกณฑ์สำหรับการระบุเหตุการณ์ความปลอดภัย โดยแยกแยะระหว่างเหตุการณ์ (Incident) และ เหตุการณ์ปกติ (Event)

ตัวอย่างเกณฑ์การระบุเหตุการณ์ ได้แก่:

- กิจกรรมผิดปกติ (Abnormal Activity)
- ช่องโหว่ด้านความปลอดภัย (Security Vulnerability)
- จุดอ่อนด้านความปลอดภัย (Security Weakness)
- การละเมิดข้อมูล (Data Breach)
- เหตุการณ์ด้านความเป็นส่วนตัว (Privacy Incident)
- ทบทวนเกณฑ์เป็นประจำทุกปี หรือเมื่อมีการเปลี่ยนแปลงสำคัญในองค์กร

CONTROL 18

การทดสอบเจาะระบบ (Penetration Testing)

Safeguards: 5	IG1: 0/5	IG2: 3/5	IG3: 5/5

ภาพรวม (Overview):

ทดสอบประสิทธิภาพ และความยืดหยุ่นของสินทรัพย์ ในองค์กรโดยการระบุและใช้ประโยชน์จากจุดอ่อนในการควบคุม (ทั้งในแง่ของบุคลากร กระบวนการ และเทคโนโลยี) พร้อมจำลองวัตถุประสงค์และการกระทำของผู้โจมตี

เหตุใดการควบคุมนี้จึงมีความสำคัญ?

การป้องกันที่มีประสิทธิภาพต้องประกอบด้วย:

- นโยบายและการกำกับดูแลที่รัดกุม
- การป้องกันทางเทคนิคที่แข็งแกร่ง
- การปฏิบัติที่เหมาะสมจากบุคลากร

อย่างไรก็ตาม ในสภาพแวดล้อมที่ซับซ้อน เทคโนโลยีเปลี่ยนแปลงอยู่ตลอดเวลา และเทคนิคการโจมตีใหม่ ๆ เกิดขึ้นอย่างต่อเนื่อง การทดสอบเจาะระบบเป็นระยะช่วยให้องค์กรสามารถ:

- ระบุช่องโหว่ และ
- ประเมินความยืดหยุ่นของการควบคุมความปลอดภัย

การทดสอบเจาะระบบสามารถดำเนินการจากมุมมองต่าง ๆ เช่น:

- เครือข่ายภายนอก
- เครือข่ายภายใน
- แอปพลิเคชัน
- ระบบหรืออุปกรณ์
- การโจมตีทางวิศวกรรมสังคม (Social Engineering)
- การเลี่ยงการควบคุมการเข้าถึงทางกายภาพ (Physical Access Control Bypass)

วัตถุประสงค์ของการทดสอบเจาะระบบ

1 การสาธิตการโจมตีอย่างชัดเจน

- เพื่อโน้มน้าวผู้ตัดสินใจให้เห็นถึงจุดอ่อนขององค์กร

2 การทดสอบการทำงานของการป้องกัน (Verification)

- ตรวจสอบว่าการป้องกันทำงานได้ถูกต้อง

3 การตรวจสอบการออกแบบการป้องกัน (Validation)

- ตรวจสอบว่าองค์กรสร้างระบบป้องกันที่เหมาะสมตั้งแต่แรกหรือไม่

ประโยชน์ของการทดสอบเจาะระบบ

- ระบุช่องโหว่ในระบบและบุคลากร
- ประเมินประสิทธิภาพของการป้องกัน
- ค้นหาจุดอ่อนในกระบวนการ เช่น การจัดการการตั้งค่าที่ไม่สมบูรณ์ หรือการฝึกอบรมผู้ใช้งานที่ไม่เพียงพอ

ความแตกต่างระหว่างการทดสอบเจาะระบบและการทดสอบช่องโหว่

4 การทดสอบช่องโหว่ (Vulnerability Testing)

- ตรวจหาช่องโหว่ที่ทราบแล้วโดยใช้การสแกนอัตโนมัติ
- บางครั้งมีการตรวจสอบข้อผิดพลาด (False Positives) ด้วยมือ

5 การทดสอบเจาะระบบ (Penetration Testing)

- ระบุช่องโหว่และพยายามใช้ช่องโหว่นั้นเพื่อดูว่าผู้โจมตีสามารถทำอะไรได้บ้าง
- ต้องการการวิเคราะห์และการมีส่วนร่วมจากมนุษย์มากขึ้น

Red Team Exercises

- คล้ายกับการทดสอบเจาะระบบ แต่เน้นการจำลองการโจมตีจาก Tactics, Techniques, and Procedures (TTPs) ของผู้โจมตีเฉพาะกลุ่ม
- ประเมินความสามารถขององค์กรในการรับมือกับการโจมตีจากคู่ต่อสู้ที่เจาะจง

บทสรุป

การทดสอบเจาะระบบเป็นส่วนสำคัญของโปรแกรมการรักษาความปลอดภัยที่ครอบคลุม ช่วยให้องค์กรสามารถ:

- ระบุจุดอ่อนที่อาจถูกใช้ประโยชน์
- ปรับปรุงการป้องกันอย่างต่อเนื่อง
- สร้างความตระหนักรู้ในระดับผู้บริหารและทีมเทคนิค

การทดสอบเจาะระบบช่วยให้องค์กรเตรียมพร้อมรับมือกับภัยคุกคามได้ดียิ่งขึ้น และลดความเสี่ยงจากการถูกโจมตีทางไซเบอร์.

ขั้นตอนและเครื่องมือ

ขั้นตอนในการทดสอบเจาะระบบ

1 การสืบค้นข้อมูล (Reconnaissance)

- เริ่มต้นด้วยการรวบรวมข้อมูลเกี่ยวกับองค์กรและสภาพแวดล้อม
- ใช้เครื่องมือและเทคนิคเพื่อค้นหาเป้าหมายและข้อมูลที่เกี่ยวข้อง

2 การสแกนเพื่อระบุช่องโหว่ (Scanning for Vulnerabilities)

- ระบุช่องโหว่ที่สามารถใช้เป็นช่องทางเข้าสู่องค์กร
- ตรวจสอบให้แน่ใจว่าสินทรัพย์ที่อยู่ในขอบเขตทั้งหมดถูกค้นพบ ไม่ควรพึ่งพารายการสินทรัพย์ที่อาจล้าสมัยหรือไม่ครบถ้วน

3 การใช้ประโยชน์จากช่องโหว่ (Exploitation)

- ดำเนินการโจมตีช่องโหว่เพื่อแสดงให้เห็นว่าผู้โจมตีสามารถ:
- ล้มล้างวัตถุประสงค์ด้านความปลอดภัยขององค์กร (เช่น การปกป้องข้อมูลที่ละเอียดอ่อน)
- บรรลุวัตถุประสงค์ของผู้โจมตี (เช่น การสร้าง Command and Control (C2) ที่ซ่อนเร้น)

4 การวิเคราะห์และรายงานผลลัพธ์

- รายงานผลการทดสอบโดยระบุช่องโหว่และความเสี่ยงที่ตรวจพบ
- อธิบายวิธีการที่ใช้ในการโจมตี และผลกระทบที่อาจเกิดขึ้น

ข้อควรระวังในการทดสอบเจาะระบบ

ความเสี่ยงในการทดสอบ:

- อาจทำให้ระบบหยุดทำงานโดยไม่คาดคิด
- อาจทำให้ข้อมูลหรือการตั้งค่าถูกลบหรือเสียหาย
- รายงานผลการทดสอบต้องมีการปกป้อง เนื่องจากมีข้อมูลขั้นตอนการเจาะระบบที่ละเอียดอ่อน

ความชำนาญของผู้ทดสอบ:

- การทดสอบเจาะระบบควรดำเนินการโดยผู้เชี่ยวชาญจากบริษัทที่มีชื่อเสียง

การกำหนดขอบเขตและกฎการทำงาน (Scope and Rules of Engagement)

5 ขอบเขตการทดสอบ

- ระบุสินทรัพย์ที่มีข้อมูลหรือฟังก์ชันการทำงานที่มีมูลค่าสูง
- พิจารณาทดสอบระบบที่มีมูลค่าต่ำกว่าเพื่อดูว่าสามารถใช้เป็นจุดเชื่อม (Pivot Points) เพื่อโจมตีเป้าหมายที่มีมูลค่าสูงได้หรือไม่

กฎการทำงาน

- กำหนดเวลาที่จะทำการทดสอบ
- ระยะเวลาของการทดสอบ
- วิธีการทดสอบ
- กำหนดผู้รับผิดชอบหลักในกรณีที่เกิดปัญหา

การรักษาความลับ

- ควรมีเพียงไม่กี่คนในองค์กรที่ทราบว่ากำลังมีการทดสอบเจาะระบบ
- การใช้ที่ปรึกษากฎหมายภายนอกในการดูแลการทดสอบ ช่วยปกป้องรายงานจากการเปิดเผย

แหล่งข้อมูลแนะนำสำหรับการวางแผนและจัดการการทดสอบเจาะระบบ

- OWASP Penetration Testing Methodologies

https://www.owasp.org/index.php/Penetration_testing_methodologies

- PCI Security Standards Council – Penetration Testing Guidance

https://www.pcisecuritystandards.org/documents/Penetration-Testing-Guidance-v1_1.pdf

มาตรการป้องกันที่ 18.1: จัดทำและดูแลโปรแกรมการทดสอบเจาะระบบ (Establish and Maintain a Penetration Testing Program)

Asset Type: Documentation	Security Function: Govern		IG2 IG3

จัดทำและดูแลโปรแกรมการทดสอบเจาะระบบที่เหมาะสมกับขนาด ความซับซ้อน อุตสาหกรรม และความพร้อมขององค์กร

ลักษณะของโปรแกรม ควรรวมถึง:

- ขอบเขต: เครือข่าย, แอปพลิเคชันเว็บ, API, บริการที่โฮสต์, การควบคุมทางกายภาพ
- ความถี่ในการทดสอบ
- ข้อจำกัด: ช่วงเวลาที่อนุญาตและประเภทการโจมตีที่ยกเว้น
- ข้อมูลติดต่อ ของผู้รับผิดชอบ
- การแก้ไขปัญหา: วิธีการส่งต่อผลการทดสอบภายในองค์กร
- ข้อกำหนดการทบทวนย้อนหลัง

มาตรการป้องกันที่ 18.2: ดำเนินการทดสอบเจาะระบบภายนอกเป็นระยะ (Perform Periodic External Penetration Tests)

Asset Type: Network	Security Function: Detect		IG2 IG3

ดำเนินการทดสอบเจาะระบบจากภายนอกตามข้อกำหนดของโปรแกรม อย่างน้อยปีละครั้ง

การทดสอบภายนอกควรรวมถึง:

- การสืบค้นข้อมูล (Reconnaissance) เพื่อค้นหาข้อมูลที่สามารถใช้ประโยชน์ในการโจมตี
- การทดสอบต้องดำเนินการโดยผู้เชี่ยวชาญที่มีคุณสมบัติเหมาะสม
- การทดสอบอาจเป็นแบบ Clear Box (ทราบข้อมูลระบบ) หรือ Opaque Box (ไม่ทราบข้อมูลระบบ)ล

มาตรการป้องกันที่ 18.3: ดำเนินการตรวจสอบความปลอดภัยในระดับโค้ด (Implement Code-Level Security Checks)

Asset Type: Network	Security Function: Protect		IG2 IG3

แก้ไขปัญหาที่พบจากการทดสอบเจาะระบบตามกระบวนการแก้ไขช่องโหว่ขององค์กรกำหนด:

- ระยะเวลาในการแก้ไข
- ระดับความพยายาม ตามผลกระทบและความสำคัญของช่องโหว่ที่พบ

มาตรการป้องกันที่ 18.4: ตรวจสอบความถูกต้องของมาตรการรักษาความปลอดภัย (Validate Security Measures)

Asset Type: Network	Security Function: Protect		IG3

ตรวจสอบความถูกต้องของมาตรการรักษาความปลอดภัยหลังจากการทดสอบเจาะระบบ หากจำเป็น ให้ปรับเปลี่ยน:

- กฎการป้องกัน (Rulesets)
- ความสามารถในการตรวจจับ ให้เหมาะสมกับเทคนิคที่ใช้ในการทดสอบ

มาตรการป้องกันที่ 18.5: ดำเนินการทดสอบเจาะระบบภายในเป็นระยะ (Perform Periodic Internal Penetration Tests)

Asset Type: Network	Security Function: Detect		IG3

ดำเนินการทดสอบเจาะระบบจากภายในตามข้อกำหนดของโปรแกรม อย่างน้อยปีละครั้ง การทดสอบอาจเป็นแบบ:

- Clear Box: มีข้อมูลภายในระบบ
- Opaque Box: ไม่มีข้อมูลภายในระบบบ

Appendix

Acronyms and Abbreviations

AAA	Authentication, Authorization, and Auditing
ACL	Access Control List
AD	Active Directory
AoC	Attestation of Compliance
API	Application Programming Interface
BEC	Business Email Compromise
C2	Command and Control
CCE	Common Configuration Enumeration
CDM	Community Defense Model
CIA	Confidentiality, Integrity, and Availability
CIS	Center for Internet Security
CIS-CAT	CIS Configuration Assessment Tool
COTS	Commercial off-the-Shelf
CPE	Common Platform Enumeration
CREST	Council of Registered Security Testers
CSA	Cloud Security Alliance
CSP	Cloud Service Provider
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DBIR	Data Breach Investigations Report
DEP	Data Execution Prevention
DG	Development Group
DHCP	Dynamic Host Configuration Protocol
DKIM	DomainKeys Identified Mail
DLP	Data Loss Prevention
DMARC	Domain-based Message Authentication, Reporting, and Conformance
DMS	Database Management System
DNS	Domain Name System
DPI	Deep Packet Inspection
EDR	Endpoint Detection and Response
EOL	End of Life
FFIEC	Federal Financial Institutions Examination Council
FIRST	Forum of Incident Response and Security Teams, Inc.
FISMA	Federal Information Security Modernization Act
GRC	Governance Risk and Compliance
HECVAT	Higher Education Community Vendor Assessment Toolkit
HIPAA	Health Insurance Portability and Accountability Act
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IaaS	Infrastructure as a Service
IaC	Infrastructure as Code
IAM	Identity and Access Management
IDS	Intrusion Detection System
IG	Implementation Group
IOCs	Indicators of Compromise
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
ISAC	Information Sharing and Analysis Center
ISO	International Organization for Standardization
IT	Information Technology
LotL	Living off the Land
MDM	Mobile Device Management
MFA	Multi-Factor Authentication
MITRE ATT&C	MITRE Adversarial Tactics, Techniques, andCommon Knowledge®
MS-ISAC	Multi-State Information Sharing and Analysis Center
NaaS	Network as a Service
NCSA	National Cyber Security Alliance
NIDS	Network Intrusion Detection System
NIST	National Institute of Standards and Technology
OS	Operating System
OSS	Open Source Software
OVAL	Open Vulnerability and Assessment Language
OWASP	Open Web Application Security Project
PaaS	Platform as a Service
PAM	Privileged Access Management
PCI	Payment Card Industry
SaaS	Software as a Service
SAFECode	Software Assurance Forum for Excellence in Code
SCADA	Supervisory Control and Data Acquisition
SIEM	Security Information and Event Management
SIP	System Integrity Protection
SMS	Short Messaging Service
SOC	Security Operations Center
SOC 2	Service Organization Control 2
SPF	Sender Policy Framework
SQL	Structured Query Language
SSDF	Secure Software Development Framework
SSH	Secure Shell
SSO	Single Sign-On Telnet Teletype Network
TLS	Transport Layer Security
TTPs	Tactics, Techniques, and Procedures
U.K.	United Kingdom
URL	Uniform Resource Locator
USB	Universal Serial Bus
VPN	Virtual Private Network
WDEG	Windows Defender Exploit Guard
WPA2	Wi-Fi Protected Access 2
XCCDF	Extensible Configuration Checklist Description Format

Accounts บัญชีผู้ใช้งาน

บัญชีผู้ใช้งาน หมายถึงโปรไฟล์, ตัวตน (Identity), หรือการเป็นสมาชิกที่สร้างขึ้นสำหรับบุคคล กลุ่ม หรือเอนทิตีเครื่องจักร ซึ่งให้สิทธิ์การเข้าถึงทรัพยากรหรือฟังก์ชันต่าง ๆ ภายในระบบคอมพิวเตอร์หรือเครือข่าย

ความสำคัญของระบบบัญชีผู้ใช้งาน

ระบบบัญชีผู้ใช้งานมีความสำคัญในการจัดการ การอนุญาต (Permissions) และ ระดับความปลอดภัย (Security Levels) ภายในองค์กร แต่ละบุคคลอาจมีบัญชีหลายบัญชี ขึ้นอยู่กับ:

- บทบาทงาน (Job Roles)
- ข้อกำหนดด้านความปลอดภัย (Security Requirements)

ประเภทของบัญชีผู้ใช้งาน

1. บัญชีผู้ใช้งานทั่วไป (User Accounts)
   - สำหรับบุคคลทั่วไป
   - กำหนดสิทธิ์การเข้าถึงตามบทบาทและความรับผิดชอบที่เฉพาะเจาะจง
2. บัญชีผู้ดูแลระบบ (Administrator Accounts)
   - สำหรับผู้ดูแลระบบที่ต้องการสิทธิ์การเข้าถึงในระดับสูง
   - สามารถจัดการและเปลี่ยนแปลงการตั้งค่าของระบบหรือเครือข่ายได้
3. บัญชีบริการ (Service Accounts)
   - สำหรับการใช้งานโดยบริการ, แอปพลิเคชัน, หรือกระบวนการอัตโนมัติ
   - มักใช้สำหรับการทำงานเฉพาะเจาะจง เช่น การเข้าถึงฐานข้อมูลหรือการรันสคริปต์

Administrator Accounts บัญชีผู้ดูแลระบบ

บัญชีผู้ดูแลระบบ คือบัญชีที่ให้สิทธิ์การเข้าถึงในระดับสูงสำหรับผู้ใช้งานที่ต้องการความสามารถในการจัดการระบบต่าง ๆ ภายในองค์กร เช่น คอมพิวเตอร์ โดเมน หรือโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศทั้งหมด

ลักษณะของบัญชีผู้ดูแลระบบ

- สิทธิ์การเข้าถึงขั้นสูง (Escalated Privileges): สามารถติดตั้งซอฟต์แวร์, ปรับแต่งการตั้งค่า, และจัดการการควบคุมความปลอดภัยได้ ใช้สำหรับการบริหารจัดการระบบ, แก้ไขปัญหา, และการบำรุงรักษา
- การกำหนดเฉพาะบุคคล: แต่ละบัญชีผู้ดูแลระบบควรกำหนดให้กับผู้ใช้เพียงคนเดียว เพื่อลดความเสี่ยงจากการใช้สิทธิ์โดยไม่ได้รับอนุญาต

ประเภทของบัญชีผู้ดูแลระบบ

1. บัญชีรูท (Root Accounts)
   - มีสิทธิ์สูงสุดในระบบปฏิบัติการ เช่น Linux หรือ Unix
2. บัญชีผู้ดูแลระบบท้องถิ่น (Local Administrator)
   - สำหรับการจัดการเครื่องคอมพิวเตอร์เฉพาะเครื่องนั้น ๆ
3. บัญชีผู้ดูแลระบบโดเมน (Domain Administrator)
   - สำหรับการจัดการโดเมนภายในเครือข่ายขององค์กร เช่น Active Directory
4. บัญชีผู้ดูแลอุปกรณ์เครือข่ายและความปลอดภัย (Network or Security Appliance Administrator)
   - สำหรับการจัดการอุปกรณ์เครือข่าย เช่น เราเตอร์, สวิตช์, ไฟร์วอลล์, และอุปกรณ์รักษาความปลอดภัยอื่น ๆ

Application Programming Interface: API อินเทอร์เฟซการเขียนโปรแกรมแอปพลิเคชัน

API คือชุดของกฎและอินเทอร์เฟซที่ช่วยให้ส่วนประกอบของซอฟต์แวร์สามารถสื่อสารและทำงานร่วมกันได้ในลักษณะที่เป็นมาตรฐาน

การใช้งานของ API

1. การเข้าถึงทรัพยากรภายใน (Internal Resources) แอปพลิเคชันใช้ API เพื่อดึงข้อมูลหรือฟังก์ชันจากภายในระบบ เช่น การดึงข้อมูลจากฐานข้อมูลภายใน
2. การสื่อสารกับทรัพยากรภายนอก (External Resources) แอปพลิเคชันใช้ API เพื่อโต้ตอบกับบริการจากภายนอก เช่น บริการบนคลาวด์, ระบบการชำระเงินออนไลน์, หรือแพลตฟอร์มโซเชียลมีเดีย

ตัวอย่างการใช้งาน API

- API ของบริการแผนที่ (Mapping Services API): ให้แอปพลิเคชันสามารถแสดงแผนที่จากบริการ เช่น Google Maps
- API ของระบบชำระเงิน (Payment Gateway API): เชื่อมต่อกับระบบชำระเงิน เช่น PayPal หรือ Stripe
- API โซเชียลมีเดีย (Social Media API): ช่วยให้แอปพลิเคชันโพสต์ข้อความหรือดึงข้อมูลจากแพลตฟอร์ม เช่น Facebook หรือ Twitter

ข้อดีของการใช้ API

- ความยืดหยุ่น (Flexibility)ทำให้แอปพลิเคชันสามารถเชื่อมต่อกับบริการต่าง ๆ ได้อย่างสะดวก
- ประสิทธิภาพ (Efficiency) ลดเวลาการพัฒนา โดยใช้ฟังก์ชันที่มีอยู่แล้วผ่าน API
- ความสามารถในการขยาย (Scalability) สามารถเพิ่มความสามารถให้แอปพลิเคชันโดยการเชื่อมต่อกับบริการใหม่ ๆ

Applications แอปพลิเคชัน

แอปพลิเคชัน หมายถึงโปรแกรมหรือกลุ่มของโปรแกรมที่ทำงานอยู่บนระบบปฏิบัติการ ซึ่งโฮสต์อยู่บนสินทรัพย์ขององค์กร (Enterprise Asset)

ประเภทของแอปพลิเคชัน

1. แอปพลิเคชันเว็บ (Web Applications) แอปพลิเคชันที่เข้าถึงผ่านเว็บเบราว์เซอร์ ตัวอย่าง: เว็บไซต์อีคอมเมิร์ซ, ระบบจัดการเนื้อหา (CMS)
2. แอปพลิเคชันฐานข้อมูล (Database Applications) แอปพลิเคชันที่ใช้จัดการและประมวลผลข้อมูลในฐานข้อมูล ตัวอย่าง: ระบบการจัดการฐานข้อมูล (DBMS) เช่น MySQL, Oracle

3. แอปพลิเคชันบนคลาวด์ (Cloud-Based Applications) แอปพลิเคชันที่ทำงานผ่านโครงสร้างพื้นฐานคลาวด์ ตัวอย่าง: บริการจัดเก็บข้อมูลบนคลาวด์ เช่น Google Drive, Microsoft 365
4. แอปพลิเคชันบนอุปกรณ์เคลื่อนที่ (Mobile Applications) แอปพลิเคชันที่ออกแบบมาให้ทำงานบนอุปกรณ์เคลื่อนที่ เช่น สมาร์ทโฟนและแท็บเล็ต ตัวอย่าง: แอปพลิเคชันธนาคารบนมือถือ, แอปโซเชียลมีเดีย

แอปพลิเคชันในฐานะสินทรัพย์ซอฟต์แวร์ (Software Asset)

การจัดการแอปพลิเคชัน:

- การควบคุมการติดตั้ง, การอัปเดต, และการถอนการติดตั้ง
- การรักษาความปลอดภัยและการตรวจสอบการใช้งาน

การรักษาความปลอดภัยของแอปพลิเคชัน:

- การตรวจสอบช่องโหว่และการแก้ไขช่องโหว่
- การเข้ารหัสข้อมูลและการควบคุมสิทธิ์การเข้าถึง

Asset Class คลาสของสินทรัพย์

คลาสของสินทรัพย์ (Asset Class) หมายถึง กลุ่มของสินทรัพย์ข้อมูลที่ถูกประเมินร่วมกันเป็นชุดเดียวกัน โดยอ้างอิงจากความคล้ายคลึงกันของสินทรัพย์ในกลุ่มนั้น

ตัวอย่างคลาสของสินทรัพย์

1. อุปกรณ์ (Devices) สินทรัพย์ที่มีความสามารถในการจัดเก็บหรือประมวลผลข้อมูล ตัวอย่าง: เดสก์ท็อป, แล็ปท็อป, สมาร์ทโฟน, แท็บเล็ต, อุปกรณ์ IoT
2. ซอฟต์แวร์ (Software)โปรแกรมและระบบปฏิบัติการที่ใช้บนสินทรัพย์ต่าง ๆ ตัวอย่าง: แอปพลิเคชัน, ระบบปฏิบัติการ, ไลบรารี, API ข้อมูล (Data) ชุดของข้อเท็จจริงที่ใช้ในการตัดสินใจหรือดำเนินการ ตัวอย่าง: ข้อมูลทางการเงิน, ข้อมูลลูกค้า, ข้อมูลบันทึกการใช้งาน (Log Data)
3. ผู้ใช้งาน (Users) บุคคลหรือกลุ่มที่ได้รับอนุญาตให้เข้าถึงสินทรัพย์ ตัวอย่าง: พนักงาน, ผู้ดูแลระบบ, ผู้ให้บริการภายนอก
4. เครือข่าย (Network) ทรัพยากรที่เกี่ยวข้องกับการสื่อสารและการเชื่อมต่อระหว่างอุปกรณ์ ตัวอย่าง: เราเตอร์, สวิตช์, ไฟร์วอลล์, จุดเชื่อมต่อเครือข่าย
5. เอกสาร (Documentation) ข้อมูลที่เป็นลายลักษณ์อักษรเกี่ยวกับนโยบาย, กระบวนการ, และการตั้งค่า ตัวอย่าง: นโยบายความปลอดภัย, แผนผังเครือข่าย, คู่มือการใช้งาน

ประโยชน์ของการจัดกลุ่มสินทรัพย์เป็นคลาส

- การจัดการที่มีประสิทธิภาพ: ช่วยให้สามารถบริหารจัดการสินทรัพย์ที่คล้ายกันได้อย่างเป็นระบบ
- การรักษาความปลอดภัยที่เหมาะสม: สามารถใช้มาตรการรักษาความปลอดภัยที่เหมาะสมกับสินทรัพย์แต่ละคลาส
- การประเมินความเสี่ยง: ช่วยให้การประเมินความเสี่ยงทำได้ง่ายขึ้นโดยการวิเคราะห์ตามกลุ่มสินทรัพย์
- การปฏิบัติตามข้อกำหนด: ช่วยให้มั่นใจว่าสินทรัพย์ทุกประเภทได้รับการดูแลและปกป้องตามข้อกำหนดที่เกี่ยวข้อง

Authentication Systems ระบบการยืนยันตัวตน

ระบบการยืนยันตัวตน คือระบบหรือกลไกที่ใช้ในการระบุตัวตนผู้ใช้งาน โดยการเชื่อมโยงคำขอที่เข้ามากับชุดของข้อมูลระบุตัวตน (Credentials) ซึ่งข้อมูลดังกล่าวจะถูกเปรียบเทียบกับข้อมูลที่จัดเก็บไว้ในฐานข้อมูลของผู้ใช้งานที่ได้รับอนุญาต ไม่ว่าจะอยู่ในระบบปฏิบัติการ, บริการไดเรกทอรีผู้ใช้งาน, หรือเซิร์ฟเวอร์การยืนยันตัวตน

กระบวนการยืนยันตัวตน

1. การส่งข้อมูลรับรองตัวตน (Credentials): ผู้ใช้ส่งข้อมูลรับรอง เช่น ชื่อผู้ใช้และรหัสผ่าน
2. การเปรียบเทียบข้อมูล: ระบบตรวจสอบข้อมูลที่ได้รับกับข้อมูลที่จัดเก็บไว้ในฐานข้อมูลผู้ใช้งานที่ได้รับอนุญาต
3. การยืนยันสิทธิ์: หากข้อมูลตรงกัน ระบบจะอนุญาตให้เข้าถึงทรัพยากรหรือฟังก์ชันที่ร้องขอ

ตัวอย่างระบบการยืนยันตัวตน

1. Active Directory (AD) บริการไดเรกทอรีที่ใช้จัดการบัญชีผู้ใช้งานและสิทธิ์การเข้าถึงในเครือข่าย Windows
2. การยืนยันตัวตนหลายปัจจัย (Multi-Factor Authentication: MFA)การยืนยันตัวตนที่ต้องใช้ข้อมูลมากกว่า 1 ปัจจัย เช่น:
   - รหัสผ่าน (สิ่งที่คุณรู้)
   - โทเค็น (สิ่งที่คุณมี)
   - ลายนิ้วมือ (สิ่งที่คุณเป็น)
3. ไบโอเมตริกส์ (Biometrics) การใช้คุณลักษณะทางกายภาพหรือพฤติกรรม เช่น ลายนิ้วมือ, การจดจำใบหน้า, การสแกนม่านตา
4. โทเค็น (Tokens) อุปกรณ์หรือซอฟต์แวร์ที่สร้างรหัสผ่านแบบใช้ครั้งเดียว (One-Time Password: OTP) สำหรับการยืนยันตัวตน

ประโยชน์ของระบบการยืนยันตัวตน

- เพิ่มความปลอดภัย: ป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต
- ควบคุมการเข้าถึง: กำหนดสิทธิ์การเข้าถึงตามบทบาทและความรับผิดชอบ
- ความยืดหยุ่น: รองรับการยืนยันตัวตนหลายรูปแบบ เช่น MFA และไบโอเมตริกส์
- การปฏิบัติตามข้อกำหนด:ช่วยให้สอดคล้องกับมาตรฐานความปลอดภัยและข้อกำหนดทางกฎหมาย

ระบบการยืนยันตัวตนเป็นส่วนสำคัญในการรักษาความปลอดภัยของข้อมูลและทรัพยากรในองค์กร โดยการยืนยันสิทธิ์การเข้าถึงอย่างถูกต้องและปลอดภัย ช่วยลดความเสี่ยงจากการโจมตีและการเข้าถึงโดยไม่ได้รับอนุญาต.

Authorization Systems ระบบการอนุญาต

ระบบการอนุญาต (Authorization System) คือระบบหรือกลไกที่ใช้ในการกำหนดระดับการเข้าถึงหรือสิทธิ์ ของผู้ใช้/ลูกค้าสำหรับทรัพยากรในระบบ ซึ่งรวมถึงไฟล์, บริการ, โปรแกรมคอมพิวเตอร์, ข้อมูล, และฟีเจอร์ต่าง ๆ ของแอปพลิเคชัน โดยระบบการอนุญาตจะให้หรือปฏิเสธการเข้าถึงตาม ตัวตนของผู้ใช้

กระบวนการทำงานของระบบการอนุญาต

- การยืนยันตัวตน (Authentication): ก่อนที่จะมีการอนุญาต ผู้ใช้ต้องผ่านการยืนยันตัวตนก่อน
- การกำหนดสิทธิ์ (Authorization): ระบบตรวจสอบว่าผู้ใช้มีสิทธิ์อะไร และตัดสินใจให้หรือปฏิเสธการเข้าถึงทรัพยากร
- การบังคับใช้กฎการเข้าถึง (Access Enforcement): ระบบใช้กฎที่กำหนดไว้เพื่อควบคุมการเข้าถึงทรัพยากร เช่น ไฟล์, โฟลเดอร์, หรือฟีเจอร์ต่าง ๆ

ตัวอย่างระบบการอนุญาต

- Active Directory (AD) ระบบไดเรกทอรีที่ช่วยจัดการสิทธิ์การเข้าถึงของผู้ใช้ในเครือข่าย Windows สามารถกำหนดสิทธิ์การเข้าถึงตามบทบาทหรือกลุ่มผู้ใช้
- Access Control Lists (ACLs) รายการที่กำหนดสิทธิ์การเข้าถึงทรัพยากร เช่น ไฟล์หรือโฟลเดอร์ ระบุว่าใครบ้างที่สามารถอ่าน, เขียน, หรือแก้ไขทรัพยากรได้
- Role-Based Access Control (RBAC) การควบคุมการเข้าถึงตามบทบาทของผู้ใช้ ตัวอย่าง: ผู้ใช้ในบทบาท "ผู้ดูแลระบบ" (Admin) จะมีสิทธิ์สูงกว่าผู้ใช้ในบทบาท "ผู้ใช้งานทั่วไป" (User)

ประโยชน์ของระบบการอนุญาต

- เพิ่มความปลอดภัย จำกัดการเข้าถึงเฉพาะผู้ใช้ที่มีสิทธิ์เท่านั้น ลดความเสี่ยงจากการเข้าถึงโดยไม่ได้รับอนุญาต
- การจัดการสิทธิ์ที่มีประสิทธิภาพ สามารถกำหนดสิทธิ์การเข้าถึงตามบทบาทและความรับผิดชอบของผู้ใช้
- ความยืดหยุ่นในการใช้งาน รองรับการกำหนดสิทธิ์แบบละเอียดสำหรับการเข้าถึงทรัพยากรที่หลากหลาย
- การปฏิบัติตามกฎระเบียบช่วยให้องค์กรปฏิบัติตามมาตรฐานความปลอดภัยและข้อกำหนดทางกฎหมาย

Bi-Annually ทุกหกเดือน

Bi-Annually หมายถึง การดำเนินการใด ๆ ที่ต้องทำ ทุกหกเดือน (ปีละสองครั้ง)

แนวทางปฏิบัติสำหรับงานที่ต้องทำ Bi-Annually

1. การดำเนินการตามกำหนดเวลา: งานที่ต้องดำเนินการเป็นประจำทุกหกเดือน เช่น การตรวจสอบความปลอดภัย, การอัปเดตข้อมูลสินทรัพย์, หรือการทบทวนการกำหนดค่าเครือข่าย
2. การดำเนินการเมื่อมีการเปลี่ยนแปลงสำคัญ: นอกเหนือจากการทำตามกำหนดเวลา ควรดำเนินการซ้ำเมื่อเกิดการเปลี่ยนแปลงที่สำคัญซึ่งอาจส่งผลกระทบต่อเครือข่ายหรืออุปกรณ์ เช่น:
   - การอัปเกรดฮาร์ดแวร์
   - การควบรวมกิจการ (Mergers and Acquisitions)
   - การเปลี่ยนแปลงโครงสร้างพื้นฐานเครือข่าย

ตัวอย่างงานที่ควรทำ Bi-Annually

- การตรวจสอบสินทรัพย์ขององค์กร (Enterprise Asset Inventory)ทบทวนและอัปเดตรายการสินทรัพย์ เช่น อุปกรณ์เครือข่าย, ซอฟต์แวร์, และข้อมูลผู้ใช้งาน
- การตรวจสอบการกำหนดค่าเครือข่าย (Network Configuration Review) ตรวจสอบการตั้งค่าเครือข่ายเพื่อให้มั่นใจว่าไม่มีช่องโหว่และการตั้งค่าที่ไม่จำเป็น
- การทบทวนสิทธิ์การเข้าถึง (Access Control Review) ตรวจสอบสิทธิ์การเข้าถึงของผู้ใช้และผู้ดูแลระบบ
- การทดสอบเจาะระบบ (Penetration Testing) ดำเนินการทดสอบเจาะระบบเพื่อค้นหาช่องโหว่และจุดอ่อน

Breach การละเมิดข้อมูล

การละเมิดข้อมูล (Breach) หมายถึง การสูญเสียการควบคุม, การถูกล้วงข้อมูล, การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต, การได้มาซึ่งข้อมูลโดยไม่ได้รับอนุญาต หรือเหตุการณ์ใด ๆ ที่คล้ายกัน ซึ่งมีลักษณะดังต่อไปนี้:

- บุคคลที่ไม่ได้รับอนุญาต เข้าถึงหรือมีโอกาสเข้าถึงข้อมูลที่ละเอียดอ่อนหรือข้อมูลที่เป็นความลับ
- ผู้ใช้ที่ได้รับอนุญาต ใช้ข้อมูลที่ละเอียดอ่อนหรือข้อมูลที่เป็นความลับในทางที่ไม่ได้รับอนุญาต

ตัวอย่างการละเมิดข้อมูล

- การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต แฮกเกอร์เข้าถึงฐานข้อมูลที่มีข้อมูลลูกค้า
- การเปิดเผยข้อมูลโดยไม่ได้ตั้งใจ การส่งอีเมลที่มีข้อมูลละเอียดอ่อนไปยังผู้รับผิดคน
- การล้วงข้อมูลภายในองค์กร พนักงานที่เข้าถึงข้อมูลสำหรับการใช้งานที่ไม่ได้รับอนุญาต เช่น การขโมยข้อมูลเพื่อนำไปขายต่อ
- การได้มาซึ่งข้อมูลโดยไม่ได้รับอนุญาต การขโมยข้อมูลจากอุปกรณ์ที่สูญหายหรือถูกขโมย เช่น แล็ปท็อปหรือฮาร์ดไดรฟ์

ผลกระทบจากการละเมิดข้อมูล

- ความเสียหายทางการเงิน ค่าปรับจากการละเมิดกฎระเบียบ, ค่าฟื้นฟูระบบ, และค่าชดเชยลูกค้า
- ความเสียหายต่อชื่อเสียง สูญเสียความไว้วางใจจากลูกค้าและคู่ค้า
- ผลกระทบทางกฎหมาย การละเมิดกฎหมายและข้อบังคับด้านความปลอดภัยของข้อมูล เช่น GDPR, HIPAA
- การหยุดชะงักทางธุรกิจ กระทบต่อการดำเนินงานขององค์กร

วิธีการป้องกันการละเมิดข้อมูล

- การเข้ารหัสข้อมูล (Encryption) เข้ารหัสข้อมูลทั้งขณะจัดเก็บและขณะส่งผ่านเครือข่าย
- การยืนยันตัวตนหลายปัจจัย (MFA) เพิ่มระดับความปลอดภัยในการยืนยันตัวตน
- การตรวจสอบการเข้าถึง (Access Control) กำหนดสิทธิ์การเข้าถึงข้อมูลตามบทบาทของผู้ใช้งาน
- การฝึกอบรมความปลอดภัย (Security Awareness Training) ให้ความรู้แก่พนักงานเกี่ยวกับการปกป้องข้อมูลและการปฏิบัติตามนโยบายความปลอดภัย

Cloud Environment สภาพแวดล้อมคลาวด์

สภาพแวดล้อมคลาวด์ (Cloud Environment) คือสภาพแวดล้อมเสมือนที่ให้การเข้าถึงเครือข่ายแบบออนดีมานด์สำหรับทรัพยากรที่สามารถกำหนดค่าได้อย่างหลากหลาย เช่น เครือข่าย, การประมวลผล, พื้นที่จัดเก็บข้อมูล, แอปพลิเคชัน และบริการต่าง ๆ

ลักษณะสำคัญ 5 ประการของสภาพแวดล้อมคลาวด์

- การบริการตนเองแบบออนดีมานด์ (On-Demand Self-Service) ผู้ใช้สามารถขอ และจัดการทรัพยากรได้เองโดยไม่ต้องผ่านผู้ให้บริการ
- การเข้าถึงผ่านเครือข่ายอย่างกว้างขวาง (Broad Network Access) สามารถเข้าถึงทรัพยากรผ่านเครือข่ายจากอุปกรณ์ที่หลากหลาย เช่น คอมพิวเตอร์, สมาร์ทโฟน, และแท็บเล็ต
- การรวมทรัพยากร (Resource Pooling) ทรัพยากรต่าง ๆ จะถูกรวมและแบ่งปันให้กับผู้ใช้หลายราย โดยระบบสามารถจัดสรรทรัพยากรได้ตามความต้องการ

- ความยืดหยุ่นในการปรับขนาด (Rapid Elasticity) สามารถเพิ่มหรือลดทรัพยากรได้อย่างรวดเร็วตามความต้องการใช้งาน
- การวัดและคิดค่าบริการตามการใช้งาน (Measured Service) การใช้งานทรัพยากรถูกติดตามและวัดผลอย่างชัดเจน เพื่อให้สามารถเรียกเก็บค่าบริการตามการใช้งานจริง

ประเภทของบริการในสภาพแวดล้อมคลาวด์

- ซอฟต์แวร์เป็นบริการ (Software as a Service: SaaS) ให้บริการซอฟต์แวร์สำเร็จรูปผ่านอินเทอร์เน็ต ตัวอย่าง: Google Workspace, Microsoft 365, Salesforce
- แพลตฟอร์มเป็นบริการ (Platform as a Service: PaaS) ให้แพลตฟอร์มสำหรับการพัฒนาและทดสอบแอปพลิเคชัน ตัวอย่าง: Microsoft Azure App Services, Google App Engine, AWS Elastic Beanstalk
- โครงสร้างพื้นฐานเป็นบริการ (Infrastructure as a Service: IaaS)ให้บริการโครงสร้างพื้นฐานเสมือน เช่น เซิร์ฟเวอร์, ระบบจัดเก็บข้อมูล, และเครือข่าย ตัวอย่าง: Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP)

ประโยชน์ของสภาพแวดล้อมคลาวด์

- ความคุ้มค่าในการลงทุน (Cost Efficiency) ลดค่าใช้จ่ายในการจัดการและบำรุงรักษาโครงสร้างพื้นฐาน
- ความยืดหยุ่น (Scalability) รองรับการขยายหรือลดขนาดทรัพยากรได้ตามความต้องการ
- ความสะดวกในการเข้าถึง (Accessibility) สามารถเข้าถึงบริการได้จากทุกที่ ทุกเวลา ผ่านอินเทอร์เน็ต
- การฟื้นฟูจากภัยพิบัติ (Disaster Recovery) ระบบสำรองข้อมูลและการกู้คืนข้อมูลที่มีประสิทธิภาพ
- การอัปเดตอัตโนมัติ (Automatic Updates) ผู้ให้บริการดูแลการอัปเดตซอฟต์แวร์และความปลอดภัย

Data ข้อมูล

ข้อมูล (Data) หมายถึง ชุดของข้อเท็จจริงที่สามารถตรวจสอบ, วิเคราะห์, และนำมาใช้ในการตัดสินใจได้ แม้ว่าข้อมูลอาจอยู่ในรูปแบบกายภาพ แต่ใน CIS Controls การปกป้องข้อมูลจะมุ่งเน้นไปที่ ข้อมูลดิจิทัล เป็นหลัก ซึ่งสามารถ:

- จัดเก็บ (Stored)
- ถ่ายโอน (Transferred)
- ประมวลผล (Processed)

ประเภทของข้อมูลดิจิทัล

- ข้อมูลที่จัดเก็บ (Stored Data) ข้อมูลที่จัดเก็บในอุปกรณ์ต่าง ๆ เช่น เซิร์ฟเวอร์, ฮาร์ดไดรฟ์, และคลาวด์ ตัวอย่าง: ไฟล์เอกสาร, ฐานข้อมูล
- ข้อมูลที่กำลังถ่ายโอน (Data in Transit) ข้อมูลที่กำลังถูกส่งผ่านเครือข่าย ตัวอย่าง: การส่งอีเมล, การถ่ายโอนไฟล์ผ่านเครือข่าย
- ข้อมูลที่กำลังประมวลผล (Data in Use) ข้อมูลที่กำลังถูกใช้งานหรือประมวลผลโดยแอปพลิเคชัน ตัวอย่าง: การแก้ไขไฟล์, การประมวลผลธุรกรรมทางการเงิน

การปกป้องข้อมูลตาม CIS Controls

- การเข้ารหัส (Encryption) เข้ารหัสข้อมูลทั้งขณะจัดเก็บและขณะถ่ายโอนเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต
- การควบคุมการเข้าถึง (Access Control) กำหนดสิทธิ์การเข้าถึงข้อมูลตามบทบาทและความจำเป็นในการใช้งาน
- การจัดการข้อมูลอย่างปลอดภัย (Secure Data Handling) การจัดเก็บ, ถ่ายโอน, และกำจัดข้อมูลอย่างปลอดภัยตามนโยบายขององค์กร
- การตรวจสอบและติดตาม (Logging and Monitoring) บันทึกการเข้าถึงข้อมูลเพื่อระบุและตรวจสอบกิจกรรมที่ผิดปกติ

Data Exposure การเปิดเผยข้อมูลโดยไม่ตั้งใจ

การเปิดเผยข้อมูลโดยไม่ตั้งใจ (Data Exposure) หมายถึง การรั่วไหลหรือการเปิดเผยข้อมูลที่เป็นความลับหรือข้อมูลที่ละเอียดอ่อนโดยไม่ได้เจตนา ซึ่งอาจนำไปสู่การละเมิดความปลอดภัยของข้อมูล

สาเหตุของการเปิดเผยข้อมูลโดยไม่ตั้งใจ

- การกำหนดสิทธิ์การเข้าถึงผิดพลาด ให้สิทธิ์การเข้าถึงข้อมูลกับผู้ใช้ที่ไม่ควรมีสิทธิ์
- การส่งข้อมูลผิดพลาด ส่งอีเมลหรือเอกสารไปยังผู้รับผิดคน
- การกำหนดค่าความปลอดภัยผิดพลาด การตั้งค่าความปลอดภัยในฐานข้อมูลหรือคลาวด์ไม่เหมาะสม เช่น เปิดให้สาธารณะเข้าถึงได้
- อุปกรณ์สูญหายหรือถูกขโมย แล็ปท็อป, สมาร์ทโฟน, หรือสื่อจัดเก็บข้อมูลที่มีข้อมูลสำคัญถูกทำหายหรือถูกขโมย
- การแชร์ข้อมูลผ่านช่องทางที่ไม่ปลอดภัย แชร์ข้อมูลผ่านเครือข่ายหรือแอปพลิเคชันที่ไม่มีการเข้ารหัส

วิธีป้องกันการเปิดเผยข้อมูลโดยไม่ตั้งใจ

- การควบคุมการเข้าถึง (Access Control) กำหนดสิทธิ์การเข้าถึงข้อมูลอย่างเหมาะสม
- การเข้ารหัสข้อมูล (Data Encryption) เข้ารหัสข้อมูลทั้งขณะจัดเก็บและขณะถ่ายโอน
- การฝึกอบรมพนักงาน (Security Awareness Training) ให้ความรู้เกี่ยวกับวิธีการจัดการและส่งข้อมูลอย่างปลอดภัย
- การตรวจสอบการตั้งค่า (Configuration Audits) ตรวจสอบการตั้งค่าความปลอดภัยของระบบและฐานข้อมูลอย่างสม่ำเสมอ
- การสำรองข้อมูล (Data Backup) สำรองข้อมูลเพื่อป้องกันการสูญหายจากเหตุการณ์ไม่คาดคิด

Database ฐานข้อมูล

ฐานข้อมูล (Database) หมายถึงการรวบรวมข้อมูลที่มีการจัดระเบียบอย่างเป็นระบบ ซึ่งโดยทั่วไปจะถูกจัดเก็บและเข้าถึงได้ในรูปแบบอิเล็กทรอนิกส์ผ่านระบบคอมพิวเตอร์

ลักษณะของฐานข้อมูล

1. การจัดระเบียบอย่างเป็นระบบ ข้อมูลถูกจัดเก็บในรูปแบบที่สามารถเข้าถึงและเรียกใช้ได้อย่างมีประสิทธิภาพ เช่น ตาราง, ฟิลด์, และเรกคอร์ด
2. การเข้าถึงแบบอิเล็กทรอนิกส์ สามารถเข้าถึงได้ผ่านระบบคอมพิวเตอร์ โดยใช้คำสั่งหรือโปรแกรมเฉพาะ
3. ที่ตั้งของฐานข้อมูล

- บนเซิร์ฟเวอร์ภายในองค์กร (On-Site)
- บนคลาวด์หรือเซิร์ฟเวอร์ระยะไกล (Remote/Cloud-Based)

ระบบจัดการฐานข้อมูล (Database Management Systems: DBMS)

- DBMS คือระบบที่ใช้ในการดูแลและจัดการฐานข้อมูล เช่น การสร้าง, การอัปเดต, การค้นหา, และการรักษาความปลอดภัยของข้อมูล
- ในบริบทของเอกสารนี้ DBMS จะไม่ถือเป็นส่วนหนึ่งของฐานข้อมูล

Devices อุปกรณ์

อุปกรณ์ (Devices) หมายถึงสินทรัพย์ขององค์กรที่ใช้ในการประมวลผลและจัดเก็บข้อมูล ซึ่งครอบคลุมประเภทต่าง ๆ ได้แก่:

- อุปกรณ์สำหรับผู้ใช้งานปลายทาง (End-User Devices)
- อุปกรณ์พกพา (Portable Devices)
- อุปกรณ์เคลื่อนที่ (Mobile Devices)
- เซิร์ฟเวอร์ (Servers)
- อุปกรณ์ Internet of Things (IoT) และอุปกรณ์ที่ไม่ใช่คอมพิวเตอร์ (Non-Computing Devices)
- อุปกรณ์เครือข่าย (Network Devices)
- สื่อจัดเก็บข้อมูลแบบถอดได้ (Removable Media)

ลักษณะของอุปกรณ์

- สถานที่ติดตั้ง:สามารถอยู่ในพื้นที่จริง (Physical Spaces), โครงสร้างพื้นฐานเสมือน (Virtual Infrastructure), หรือบนคลาวด์ (Cloud-Based Environments)
- การเชื่อมต่อระยะไกล: อุปกรณ์สามารถเชื่อมต่อกับระบบต่าง ๆ ได้จากระยะไกล

ประเภทของอุปกรณ์

- อุปกรณ์สำหรับผู้ใช้งานปลายทาง (End-User Devices) เดสก์ท็อป, แล็ปท็อป, เวิร์กสเตชัน
- อุปกรณ์พกพา (Portable Devices) อุปกรณ์ที่สามารถเคลื่อนย้ายได้ง่ายและเชื่อมต่อเครือข่ายแบบไร้สาย เช่น แล็ปท็อป, สมาร์ทโฟน, แท็บเล็ต
- อุปกรณ์เคลื่อนที่ (Mobile Devices) สมาร์ทโฟน, แท็บเล็ตที่มีความสามารถในการเชื่อมต่อไร้สายในตัว
- เซิร์ฟเวอร์ (Servers) เครื่องแม่ข่ายที่ให้บริการข้อมูล, แอปพลิเคชัน, หรือทรัพยากรอื่น ๆ เช่น เว็บเซิร์ฟเวอร์, เมลเซิร์ฟเวอร์
- อุปกรณ์ IoT และอุปกรณ์ที่ไม่ใช่คอมพิวเตอร์ (IoT and Non-Computing Devices) อุปกรณ์ที่ฝังเซ็นเซอร์และซอฟต์แวร์ เช่น สมาร์ทวอทช์, เครื่องพิมพ์, จอแสดงผลอัจฉริยะ, ระบบควบคุมโรงงาน
- อุปกรณ์เครือข่าย (Network Devices) อุปกรณ์ที่ใช้เชื่อมต่อและจัดการเครือข่าย เช่น เราเตอร์, สวิตช์, ไฟร์วอลล์, จุดเชื่อมต่อเครือข่าย
- สื่อจัดเก็บข้อมูลแบบถอดได้ (Removable Media) อุปกรณ์จัดเก็บข้อมูลที่สามารถถอดออกได้ เช่น USB แฟลชไดรฟ์, ฮาร์ดไดรฟ์แบบพกพา, การ์ด SD

Documentation เอกสาร

เอกสาร (Documentation) หมายถึง นโยบาย, กระบวนการ, ขั้นตอนปฏิบัติ, แผนงาน, แผนผัง, และข้อมูลที่เป็นลายลักษณ์อักษรอื่น ๆ ซึ่งอาจอยู่ในรูปแบบกายภาพหรือดิจิทัล

ประเภทของเอกสาร

- นโยบาย (Policies) คำประกาศอย่างเป็นทางการที่กำหนดวัตถุประสงค์และแนวทางปฏิบัติด้านความปลอดภัย
- ตัวอย่าง: นโยบายความปลอดภัยของข้อมูล, นโยบายการจัดการความเสี่ยง
- กระบวนการ (Processes) ชุดของขั้นตอนและกิจกรรมที่ต้องปฏิบัติเพื่อให้บรรลุเป้าหมายที่เกี่ยวข้องกับความปลอดภัย ตัวอย่าง: กระบวนการควบคุมการเข้าถึงข้อมูล, กระบวนการจัดการการเปลี่ยนแปลง
- ขั้นตอนปฏิบัติ (Procedures) ขั้นตอนที่กำหนดไว้อย่างชัดเจนสำหรับการดำเนินการงานเฉพาะ ตัวอย่าง: ขั้นตอนการสำรองข้อมูล, ขั้นตอนการตอบสนองต่อเหตุการณ์ความปลอดภัย
- แผนงาน (Plans) การวางแผนปฏิบัติการที่ระบุถึงวิธีการดำเนินการตามนโยบาย ตัวอย่าง: แผนการกู้คืนระบบหลังภัยพิบัติ (Disaster Recovery Plan), แผนการตอบสนองต่อเหตุการณ์ (Incident Response Plan)
- แผนผัง (Diagrams) แผนผังที่แสดงภาพรวมของสถาปัตยกรรมระบบเครือข่าย, ระบบความปลอดภัย, และการเชื่อมต่อระหว่างองค์ประกอบต่าง ๆ ตัวอย่าง: แผนผังโครงสร้างเครือข่าย, แผนผังการไหลของข้อมูล (Data Flow Diagram) รายงานการปฏิบัติตามข้อกำหนด (Compliance Reports) รายงานที่แสดงถึงการปฏิบัติตามกฎระเบียบและมาตรฐาน ตัวอย่าง: รายงานการตรวจสอบความปลอดภัย, รายงานการปฏิบัติตามข้อกำหนด GDPR

ตัวอย่างการใช้งานเอกสาร

- วิธีการบริหารจัดการองค์กร (Governance Methods) แนวทางและกฎระเบียบในการควบคุมการดำเนินงานและความปลอดภัย
- กระบวนการที่ผู้ใช้งานต้องปฏิบัติตาม (User Processes) ข้อกำหนดที่ผู้ใช้งานต้องทำตามในการเข้าถึงและจัดการข้อมูล
- คำอธิบายโครงสร้างเครือข่าย (Network Architecture) แผนผังที่แสดงการเชื่อมต่อและการตั้งค่าเครือข่ายขององค์กร

ประโยชน์ของเอกสาร

- ความชัดเจนและความโปร่งใส ช่วยให้ทุกคนในองค์กรเข้าใจแนวทางปฏิบัติและนโยบายที่ชัดเจน
- การปฏิบัติตามข้อกำหนด (Compliance) สนับสนุนการปฏิบัติตามมาตรฐานและกฎระเบียบต่าง ๆ เช่น ISO 27001, GDPR
- การจัดการและควบคุมความปลอดภัย ช่วยให้สามารถตรวจสอบ, บริหารจัดการ, และปรับปรุงความปลอดภัยได้อย่างมีประสิทธิภาพ

- การฝึกอบรมและการเรียนรู้ เป็นแหล่งข้อมูลสำหรับการฝึกอบรมพนักงานและสร้างความเข้าใจในกระบวนการทำงาน

Dwell Time เวลาการฝังตัว

Dwell Time หมายถึง ระยะเวลาระหว่างการโจมตีครั้งแรกกับการตรวจพบการบุกรุก ซึ่งในช่วงเวลานี้ ผู้โจมตีสามารถเข้าถึงข้อมูลและสภาพแวดล้อมภายในโดยไม่ได้รับอนุญาต

องค์ประกอบของ Dwell Time

- การโจมตีครั้งแรก (Initial Attack) ช่วงเวลาที่ผู้โจมตีเริ่มเจาะระบบหรือใช้ช่องโหว่เพื่อเข้าถึงเครือข่ายหรือข้อมูลขององค์กร
- การเข้าถึงโดยไม่ได้รับอนุญาต (Unauthorized Access) ผู้โจมตีสามารถควบคุมหรือขโมยข้อมูลภายในระบบได้โดยไม่ถูกตรวจพบ
- การตรวจพบการบุกรุก (Intrusion Detection) เวลาที่ระบบรักษาความปลอดภัยหรือทีมงานตรวจพบกิจกรรมที่ผิดปกติและบ่งชี้ถึงการบุกรุก

ตัวอย่างของ Dwell Time

- กรณีโจมตีด้วยมัลแวร์ (Malware): ผู้โจมตีติดตั้งมัลแวร์ในระบบและฝังตัวอยู่เป็นเวลาหลายสัปดาห์ก่อนที่ระบบตรวจจับได้
- การบุกรุกบัญชีผู้ดูแลระบบ (Administrator Account Compromise): ผู้โจมตีเข้าถึงบัญชีผู้ดูแลระบบและใช้สิทธิ์ในการขโมยข้อมูลเป็นเวลาหลายเดือนก่อนการตรวจพบ

ความสำคัญของการลด Dwell Time

- จำกัดความเสียหาย ยิ่งตรวจพบการโจมตีได้เร็วเท่าใด ความเสียหายก็จะยิ่งน้อยลงเท่านั้น
- ป้องกันการสูญหายของข้อมูล ลดโอกาสที่ข้อมูลจะถูกขโมยหรือถูกทำลาย
- รักษาชื่อเสียงองค์กร การตอบสนองอย่างรวดเร็วช่วยลดผลกระทบต่อชื่อเสียงและความไว้วางใจจากลูกค้า
- ลดต้นทุนการกู้คืนระบบ การตรวจพบการโจมตีได้เร็วช่วยลดต้นทุนในการกู้คืนและแก้ไขระบบ

วิธีลด Dwell Time

- ระบบตรวจจับการบุกรุก (Intrusion Detection Systems: IDS) ใช้ IDS และ SIEM เพื่อตรวจจับกิจกรรมที่ผิดปกติอย่างรวดเร็ว
- การเฝ้าระวังอย่างต่อเนื่อง (Continuous Monitoring) ตรวจสอบเครือข่ายและระบบอย่างสม่ำเสมอเพื่อตรวจหาพฤติกรรมที่น่าสงสัย
- การวิเคราะห์ภัยคุกคาม (Threat Hunting) ดำเนินการค้นหาภัยคุกคามเชิงรุกภายในเครือข่าย
- การฝึกอบรมทีมรักษาความปลอดภัย ให้ทีมรักษาความปลอดภัยมีความสามารถในการระบุและตอบสนองต่อการโจมตีอย่างรวดเร็ว

End-User Devices อุปกรณ์สำหรับผู้ใช้งานปลายทาง

อุปกรณ์สำหรับผู้ใช้งานปลายทาง (End-User Devices) หมายถึง สินทรัพย์เทคโนโลยีสารสนเทศ (IT Assets) ที่สมาชิกในองค์กรใช้งานทั้งในช่วงเวลาทำงานและนอกเวลาทำงาน

ประเภทของอุปกรณ์สำหรับผู้ใช้งานปลายทาง

- เดสก์ท็อปและเวิร์กสเตชัน (Desktops and Workstations) เครื่องคอมพิวเตอร์ตั้งโต๊ะและเวิร์กสเตชันสำหรับการทำงานภายในสำนักงาน เหมาะสำหรับการทำงานที่ต้องการประสิทธิภาพสูงและการประมวลผลที่ต่อเนื่อง
- อุปกรณ์พกพา (Portable Devices) อุปกรณ์ที่สามารถเคลื่อนย้ายได้ง่ายและมีความสามารถในการเชื่อมต่อเครือข่าย ตัวอย่าง: แล็ปท็อป (Laptops)
- อุปกรณ์เคลื่อนที่ (Mobile Devices) อุปกรณ์ขนาดเล็กที่มีความสามารถในการเชื่อมต่อไร้สาย ตัวอย่าง: สมาร์ทโฟน (Smartphones), แท็บเล็ต (Tablets)

ลักษณะการใช้งาน

- การใช้งานภายในองค์กร (On-Site Use) ใช้งานในสำนักงาน เช่น การทำงานบนเวิร์กสเตชันหรือเดสก์ท็อป
- การใช้งานนอกสถานที่ (Remote Use) ใช้งานขณะทำงานจากระยะไกลหรือที่บ้าน ผ่านอุปกรณ์พกพาหรืออุปกรณ์เคลื่อนที่
- การใช้งานระหว่างเดินทาง (Mobile Workforce) การทำงานที่ต้องการความยืดหยุ่นสูง เช่น การใช้สมาร์ทโฟนและแท็บเล็ตเพื่อเข้าถึงข้อมูลและบริการขององค์กร

ความสำคัญของการจัดการอุปกรณ์สำหรับผู้ใช้งานปลายทาง

- การรักษาความปลอดภัย (Security) ป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตและการสูญหายของข้อมูล
- การจัดการสินทรัพย์ (Asset Management) ติดตามและดูแลอุปกรณ์ที่ใช้งานในองค์กรอย่างมีประสิทธิภาพ
- การสำรองข้อมูล (Data Backup) ปกป้องข้อมูลที่จัดเก็บในอุปกรณ์พกพาและอุปกรณ์เคลื่อนที่
- การอัปเดตและแพตช์ (Updates and Patching) ตรวจสอบและติดตั้งการอัปเดตซอฟต์แวร์เพื่อปิดช่องโหว่ด้านความปลอดภัย

Enterprise องค์กร

องค์กร (Enterprise) หมายถึง ธุรกิจหรือหน่วยงานใด ๆ ที่มีการใช้ระบบคอมพิวเตอร์, เครือข่าย, และอุปกรณ์ต่าง ๆ ในการดำเนินงาน

ลักษณะขององค์กร

- ธุรกิจเชิงพาณิชย์ (Commercial Business) บริษัทที่ดำเนินงานเพื่อแสวงหากำไร ตัวอย่าง: บริษัทเอกชน, ร้านค้าปลีก, สตาร์ทอัพ
- หน่วยงานภาครัฐ (Government Organizations) หน่วยงานของรัฐที่ให้บริการสาธารณะ ตัวอย่าง: กระทรวง, หน่วยงานท้องถิ่น, โรงเรียนของรัฐ
- องค์กรไม่แสวงหากำไร (Non-Profit Organizations) องค์กรที่มีวัตถุประสงค์เพื่อการกุศลหรือสังคม ตัวอย่าง: มูลนิธิ, สมาคมการกุศล, องค์กรการกุศล
- สถาบันการศึกษา (Educational Institutions) องค์กรที่มุ่งเน้นการศึกษาและวิจัย ตัวอย่าง: โรงเรียน, มหาวิทยาลัย, ศูนย์วิจัย

บทบาทของเทคโนโลยีในองค์กร

- การสื่อสารและการทำงานร่วมกัน (Communication and Collaboration) ใช้เครือข่ายและซอฟต์แวร์เพื่อการสื่อสารภายในและภายนอกองค์กร
- การจัดการข้อมูล (Data Management) การจัดเก็บ, วิเคราะห์, และปกป้องข้อมูลที่สำคัญ
- การดำเนินธุรกิจ (Business Operations) ระบบไอทีสนับสนุนการดำเนินงานในทุกภาคส่วนของธุรกิจ
- ความปลอดภัยทางไซเบอร์ (Cybersecurity) การปกป้องระบบและข้อมูลจากการโจมตีทางไซเบอร์

Enterprise Assets สินทรัพย์ขององค์กร

สินทรัพย์ขององค์กร (Enterprise Assets) หมายถึงทรัพยากรที่มีศักยภาพในการจัดเก็บหรือประมวลผลข้อมูล ซึ่งครอบคลุมอุปกรณ์และระบบที่ใช้ในสภาพแวดล้อมการทำงานทั้งแบบเสมือน, คลาวด์, และกายภาพ

ประเภทของสินทรัพย์ขององค์กร

- อุปกรณ์สำหรับผู้ใช้งานปลายทาง (End-User Devices) อุปกรณ์ที่ใช้โดยพนักงานในการทำงานตัวอย่าง: เดสก์ท็อป, แล็ปท็อป, สมาร์ทโฟน, แท็บเล็ต
- อุปกรณ์เครือข่าย (Network Devices) อุปกรณ์ที่ใช้ในการเชื่อมต่อและจัดการเครือข่าย ตัวอย่าง: เราเตอร์, สวิตช์, ไฟร์วอลล์, จุดเชื่อมต่อเครือข่าย
- อุปกรณ์ที่ไม่ใช่คอมพิวเตอร์/อุปกรณ์ IoT (Non-Computing/Internet of Things Devices) อุปกรณ์ที่เชื่อมต่อกับเครือข่ายแต่ไม่ใช่คอมพิวเตอร์ทั่วไป ตัวอย่าง: เครื่องพิมพ์, กล้องวงจรปิด, อุปกรณ์ควบคุมอุณหภูมิ, เซ็นเซอร์อัจฉริยะ
- เซิร์ฟเวอร์ (Servers) อุปกรณ์หรือระบบที่ให้บริการข้อมูล, แอปพลิเคชัน, หรือทรัพยากรแก่เครือข่าย ตัวอย่าง: เว็บเซิร์ฟเวอร์, เมลเซิร์ฟเวอร์, เซิร์ฟเวอร์ฐานข้อมูล

สภาพแวดล้อมของสินทรัพย์ขององค์กร

- สภาพแวดล้อมกายภาพ (Physical Environments) สินทรัพย์ที่ติดตั้งในสถานที่ทำงาน เช่น ศูนย์ข้อมูล (Data Center) หรือสำนักงาน
- สภาพแวดล้อมเสมือน (Virtual Environments) สินทรัพย์ที่ทำงานในรูปแบบเสมือน เช่น เครื่องเสมือน (Virtual Machines)
- สภาพแวดล้อมบนคลาวด์ (Cloud-Based Environments) สินทรัพย์ที่โฮสต์บนแพลตฟอร์มคลาวด์ เช่น Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP)

Externally-Exposed Applications แอปพลิเคชันที่เปิดเผยสู่ภายนอก

แอปพลิเคชันที่เปิดเผยสู่ภายนอก (Externally-Exposed Applications) หมายถึงแอปพลิเคชัน ที่สามารถเข้าถึงได้จากอินเทอร์เน็ตสาธารณะ และสามารถถูกตรวจพบได้จากการสแกนเครือข่ายหรือการทำ reconnaissance โดยบุคคลภายนอกเครือข่ายขององค์กร

ตัวอย่างแอปพลิเคชันที่เปิดเผยสู่ภายนอก

- เว็บไซต์องค์กร (Corporate Websites) หน้าเว็บที่ให้ข้อมูลเกี่ยวกับองค์กรหรือบริการ
- แอปพลิเคชันบนคลาวด์ (Cloud-Based Applications) แอปพลิเคชันที่โฮสต์บนบริการคลาวด์ เช่น SaaS (Software as a Service)
- เว็บเซิร์ฟเวอร์ (Web Servers) เซิร์ฟเวอร์ที่ให้บริการเว็บเพจหรือ API
- พอร์ทัลการเข้าถึงระยะไกล (Remote Access Portals) ระบบที่อนุญาตให้พนักงานหรือผู้ใช้งานภายนอกเชื่อมต่อกับทรัพยากรขององค์กร

ความเสี่ยงที่เกี่ยวข้องกับแอปพลิเคชันที่เปิดเผยสู่ภายนอก

- การโจมตีทางไซเบอร์ (Cyber Attacks) การถูกโจมตีจากภายนอก เช่น การโจมตีแบบ DDoS, การโจมตีช่องโหว่ของแอปพลิเคชัน
- การขโมยข้อมูล (Data Breach) การเข้าถึงข้อมูลที่ละเอียดอ่อนโดยไม่ได้รับอนุญาต
- การเจาะระบบผ่านช่องโหว่ (Exploitation of Vulnerabilities) การใช้ประโยชน์จากช่องโหว่ของซอฟต์แวร์หรือการตั้งค่าที่ไม่ปลอดภัย

วิธีป้องกันแอปพลิเคชันที่เปิดเผยสู่ภายนอก

- การรักษาความปลอดภัยแอปพลิเคชัน (Application Security) ตรวจสอบช่องโหว่และแพตช์ซอฟต์แวร์อย่างสม่ำเสมอ
- การใช้ไฟร์วอลล์เว็บแอปพลิเคชัน (Web Application Firewall: WAF) กรองและป้องกันการโจมตีที่มุ่งเป้าไปยังแอปพลิเคชัน
- การยืนยันตัวตนหลายปัจจัย (Multi-Factor Authentication: MFA) เพิ่มความปลอดภัยในการเข้าถึงแอปพลิเคชัน
- การตรวจสอบและเฝ้าระวัง (Monitoring and Logging) บันทึกและตรวจสอบกิจกรรมที่น่าสงสัยอย่างต่อเนื่อง

Externally-Exposed Enterprise Assets สินทรัพย์ขององค์กรที่เปิดเผยสู่ภายนอก

สินทรัพย์ขององค์กรที่เปิดเผยสู่ภายนอก (Externally-Exposed Enterprise Assets) หมายถึง สินทรัพย์ขององค์กรที่สามารถเข้าถึงได้จากอินเทอร์เน็ตสาธารณะ และสามารถถูกค้นพบได้จากการทำ Domain Name System (DNS) Reconnaissance และการสแกนเครือข่ายโดยบุคคลภายนอกเครือข่ายขององค์กร

ตัวอย่างสินทรัพย์ที่เปิดเผยสู่ภายนอก

- เว็บเซิร์ฟเวอร์ (Web Servers) เซิร์ฟเวอร์ที่โฮสต์เว็บไซต์หรือบริการออนไลน์ขององค์กร
- อีเมลเซิร์ฟเวอร์ (Email Servers) เซิร์ฟเวอร์ที่ให้บริการอีเมลแก่พนักงานและลูกค้า
- บริการเข้าถึงระยะไกล (Remote Access Services) เช่น VPN Gateways, Remote Desktop Services
- แอปพลิเคชันคลาวด์ (Cloud-Based Applications) บริการและแอปพลิเคชันที่โฮสต์บนคลาวด์ เช่น SaaS (Software as a Service)

- เซิร์ฟเวอร์ฐานข้อมูล (Database Servers) เซิร์ฟเวอร์ที่สามารถเข้าถึงได้จากภายนอก หากไม่ได้กำหนดค่าความปลอดภัยอย่างเหมาะสม
- อุปกรณ์เครือข่าย (Network Devices) เช่น ไฟร์วอลล์, เราเตอร์, และจุดเชื่อมต่อเครือข่าย (Access Points)

ความเสี่ยงที่เกี่ยวข้องกับสินทรัพย์ที่เปิดเผยสู่ภายนอก

- การโจมตีทางไซเบอร์ (Cyber Attacks) โอกาสถูกโจมตีจากแฮกเกอร์ เช่น การโจมตีแบบ DDoS, การเจาะระบบผ่านช่องโหว่
- การรั่วไหลของข้อมูล (Data Breaches) ข้อมูลที่ถูกขโมยหรือรั่วไหลจากการตั้งค่าความปลอดภัยที่ไม่เหมาะสม
- ช่องโหว่จากการตั้งค่าเริ่มต้น (Default Configurations) การใช้การตั้งค่าเริ่มต้นที่ไม่ปลอดภัย เช่น บัญชีผู้ใช้งานและรหัสผ่านเริ่มต้น
- การเข้าถึงโดยไม่ได้รับอนุญาต (Unauthorized Access) การเข้าถึงทรัพยากรที่ไม่ควรเปิดเผยต่อสาธารณะ

วิธีป้องกันสินทรัพย์ที่เปิดเผยสู่ภายนอก

- การตรวจสอบสินทรัพย์ (Asset Inventory Management) จัดทำและทบทวนรายการสินทรัพย์ที่เปิดเผยสู่ภายนอกอย่างสม่ำเสมอ
- การใช้ไฟร์วอลล์และระบบกรองการเข้าถึง (Firewalls and Access Controls) ควบคุมการเข้าถึงด้วยไฟร์วอลล์และกฎการกรองการเข้าถึงเครือข่าย
- การอัปเดตและแพตช์ซอฟต์แวร์ (Patch Management) ติดตั้งแพตช์และอัปเดตซอฟต์แวร์อย่างสม่ำเสมอเพื่อลดช่องโหว่
- การยืนยันตัวตนหลายปัจจัย (Multi-Factor Authentication: MFA) เพิ่มการรักษาความปลอดภัยด้วยการยืนยันตัวตนหลายปัจจัยสำหรับการเข้าถึงจากภายนอก
- การตรวจสอบและเฝ้าระวัง (Monitoring and Logging) เฝ้าระวังการใช้งานและบันทึกกิจกรรมเพื่อตรวจจับพฤติกรรมที่ผิดปกติ

Firmware เฟิร์มแวร์

เฟิร์มแวร์ (Firmware) หมายถึง ซอฟต์แวร์ที่จัดเก็บอยู่ในหน่วยความจำถาวร (Non-Volatile Memory) ของอุปกรณ์ เช่น ROM (Read-Only Memory) หรือแฟลชเมมโมรี (Flash Memory) เฟิร์มแวร์ทำหน้าที่เป็นสะพานเชื่อมระหว่างฮาร์ดแวร์และระบบปฏิบัติการ ช่วยให้ฮาร์ดแวร์สามารถทำงานร่วมกับซอฟต์แวร์ได้อย่างราบรื่น

ลักษณะของเฟิร์มแวร์

1. อยู่ในหน่วยความจำถาวร (Non-Volatile Memory) ข้อมูลในเฟิร์มแวร์ไม่สูญหายแม้จะปิดเครื่อง
2. ควบคุมการทำงานของฮาร์ดแวร์ (Hardware Control) ให้คำสั่งพื้นฐานสำหรับการทำงานของฮาร์ดแวร์
3. อัปเดตได้แยกจากระบบปฏิบัติการ (OS) การอัปเดตเฟิร์มแวร์มักทำผ่านกระบวนการเฉพาะ ไม่รวมอยู่ในการอัปเดตระบบปฏิบัติการหรือซอฟต์แวร์ทั่วไป

ตัวอย่างการใช้งานเฟิร์มแวร์

- BIOS (Basic Input/Output System) เฟิร์มแวร์สำหรับการเริ่มต้นการทำงานของคอมพิวเตอร์และตรวจสอบฮาร์ดแวร์ก่อนโหลดระบบปฏิบัติการ
- เฟิร์มแวร์ของเราเตอร์ (Router Firmware) ควบคุมการทำงานและการเชื่อมต่อเครือข่าย
- เฟิร์มแวร์ในสมาร์ทโฟน ช่วยควบคุมการทำงานของฮาร์ดแวร์ต่าง ๆ เช่น กล้อง, หน้าจอสัมผัส, และการเชื่อมต่อเครือข่าย
- เฟิร์มแวร์ของเครื่องพิมพ์ (Printer Firmware) ช่วยให้เครื่องพิมพ์ทำงานร่วมกับระบบปฏิบัติการและซอฟต์แวร์การพิมพ์ได้

ความสำคัญของเฟิร์มแวร์

- การทำงานร่วมกันระหว่างฮาร์ดแวร์และซอฟต์แวร์ ช่วยให้ฮาร์ดแวร์สามารถสื่อสารและทำงานร่วมกับระบบปฏิบัติการได้อย่างมีประสิทธิภาพ
- ความปลอดภัยและการอัปเดต การอัปเดตเฟิร์มแวร์ช่วยแก้ไขช่องโหว่ด้านความปลอดภัยและเพิ่มประสิทธิภาพในการทำงาน
- ความเสถียรของระบบ เฟิร์มแวร์ที่เหมาะสมช่วยให้ระบบทำงานได้อย่างเสถียรและลดปัญหาการทำงานผิดพลาดของฮาร์ดแวร์

Govern การกำกับดูแล

ตามนิยามของ NIST CSF 2.0 Security Function การกำกับดูแล (Govern) หมายถึงการกำหนด, สื่อสาร, และติดตามกลยุทธ์การจัดการความเสี่ยงด้านความปลอดภัยทางไซเบอร์, ความคาดหวัง, และนโยบายขององค์กร การกำกับดูแลนี้ช่วยให้มั่นใจได้ว่าองค์กรสามารถดำเนินการและจัดลำดับความสำคัญของการบรรลุเป้าหมายในฟังก์ชันอื่น ๆ ทั้งห้าได้อย่างเหมาะสม โดยสอดคล้องกับพันธกิจและความคาดหวังของผู้มีส่วนได้ส่วนเสีย

บทบาทของการกำกับดูแลในความปลอดภัยทางไซเบอร์

1. การเข้าใจบริบทขององค์กร (Organizational Context) ประเมินปัจจัยภายในและภายนอกที่อาจมีผลกระทบต่อกลยุทธ์ความปลอดภัยทางไซเบอร์
2. การกำหนดกลยุทธ์ความปลอดภัยทางไซเบอร์ (Cybersecurity Strategy) วางแผนและกำหนดทิศทางในการป้องกันและจัดการความเสี่ยงด้านความปลอดภัย
3. การจัดการความเสี่ยงในห่วงโซ่อุปทาน (Cybersecurity Supply Chain Risk Management) บริหารจัดการความเสี่ยงที่เกี่ยวข้องกับซัพพลายเออร์และพันธมิตรที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์
4. การกำหนดบทบาทและความรับผิดชอบ (Roles, Responsibilities, and Authorities) ระบุและกำหนดหน้าที่ความรับผิดชอบของบุคลากรในการรักษาความปลอดภัยทางไซเบอร์
5. การพัฒนานโยบาย (Policy Development) จัดทำและเผยแพร่นโยบายความปลอดภัยที่ชัดเจนและเหมาะสมกับบริบทขององค์กร
6. การติดตามและกำกับดูแลกลยุทธ์ความปลอดภัย (Oversight of Cybersecurity Strategy) ตรวจสอบและประเมินความก้าวหน้าในการดำเนินงานด้านความปลอดภัยอย่างสม่ำเสมอ

ความสำคัญของการกำกับดูแล (Governance)

- บูรณาการความปลอดภัยกับการจัดการความเสี่ยงขององค์กร (Enterprise Risk Management - ERM) ช่วยให้การจัดการความเสี่ยงทางไซเบอร์เป็นส่วนหนึ่งของกลยุทธ์การจัดการความเสี่ยงโดยรวมขององค์กร
- การสื่อสารและการกำหนดความคาดหวัง (Communication and Expectation Setting) สร้างความเข้าใจร่วมกันในทุกระดับขององค์กรเกี่ยวกับการรักษาความปลอดภัยทางไซเบอร์
- การกำหนดลำดับความสำคัญ (Prioritization) ช่วยในการจัดลำดับความสำคัญของการดำเนินการด้านความปลอดภัยให้สอดคล้องกับพันธกิจขององค์กร

Internal Enterprise Assets สินทรัพย์ภายในองค์กร

สินทรัพย์ภายในองค์กร (Internal Enterprise Assets) หมายถึง สินทรัพย์ขององค์กรที่ไม่ได้เปิดเผยต่อสาธารณะ และสามารถถูกค้นพบได้ผ่านการสแกนเครือข่ายหรือการทำ Reconnaissance ภายในเครือข่ายขององค์กร โดยการเข้าถึงที่ได้รับอนุญาต ไม่ว่าจะเป็นการยืนยันตัวตนหรือไม่ก็ตาม

ตัวอย่างของสินทรัพย์ภายในองค์กร

- เซิร์ฟเวอร์ภายใน (Internal Servers) เซิร์ฟเวอร์ที่ใช้สำหรับระบบการจัดการภายใน เช่น เซิร์ฟเวอร์ไฟล์, เซิร์ฟเวอร์ฐานข้อมูล
- อุปกรณ์เครือข่ายภายใน (Internal Network Devices) เช่น สวิตช์, เราเตอร์, ไฟร์วอลล์ ที่ใช้ภายในเครือข่ายองค์กร
- อุปกรณ์สำหรับผู้ใช้งานปลายทาง (End-User Devices) เดสก์ท็อป, แล็ปท็อป, และเวิร์กสเตชันที่เชื่อมต่ออยู่ภายในเครือข่าย
- เครื่องพิมพ์และอุปกรณ์ IoT ภายใน (Internal Printers and IoT Devices) อุปกรณ์ที่เชื่อมต่อและใช้งานเฉพาะภายในองค์กร
- แอปพลิเคชันภายใน (Internal Applications) ซอฟต์แวร์หรือระบบที่ออกแบบมาให้ใช้งานภายในเท่านั้น เช่น ระบบ HR หรือ ERP

Internet of Things: IoT อินเทอร์เน็ตของสรรพสิ่ง

อินเทอร์เน็ตของสรรพสิ่ง (Internet of Things: IoT) หมายถึงอุปกรณ์ที่ฝังตัวเซ็นเซอร์, ซอฟต์แวร์, และเทคโนโลยีอื่น ๆ ซึ่งสามารถเชื่อมต่อ, จัดเก็บ, และแลกเปลี่ยนข้อมูลกับอุปกรณ์และระบบอื่น ๆ ได้ การเชื่อมต่อกับอินเทอร์เน็ตของอุปกรณ์ IoT อาจเป็นแบบชั่วคราว (Intermittent), ไม่มีการเชื่อมต่อ (Non-Existent), หรือเชื่อมต่ออย่างต่อเนื่อง (Persistent)

ลักษณะของอุปกรณ์ IoT

- การฝังเซ็นเซอร์และซอฟต์แวร์ (Embedded Sensors and Software) มีเซ็นเซอร์และซอฟต์แวร์สำหรับเก็บข้อมูลและประมวลผลข้อมูล
- การเชื่อมต่อเครือข่าย (Network Connectivity) สามารถเชื่อมต่ออินเทอร์เน็ตหรือเครือข่ายท้องถิ่นได้
- การแลกเปลี่ยนข้อมูล (Data Exchange) สามารถแลกเปลี่ยนข้อมูลกับอุปกรณ์หรือระบบอื่น ๆ ได้
- ความยืดหยุ่นในการเชื่อมต่อ (Flexible Connectivity) การเชื่อมต่อสามารถเป็นแบบต่อเนื่อง, ไม่ต่อเนื่อง, หรือไม่มีการเชื่อมต่อเลย

ตัวอย่างของอุปกรณ์ IoT

- อุปกรณ์สวมใส่อัจฉริยะ (Smart Wearables) ตัวอย่าง: สมาร์ทวอทช์, สายรัดข้อมือเพื่อสุขภาพ
- เครื่องพิมพ์อัจฉริยะ (Smart Printers) สามารถเชื่อมต่อเครือข่ายเพื่อสั่งพิมพ์งานจากระยะไกล
- หน้าจออัจฉริยะ (Smart Screens) จอแสดงผลที่สามารถเชื่อมต่ออินเทอร์เน็ตและแสดงข้อมูลแบบโต้ตอบ
- อุปกรณ์สมาร์ทโฮม (Smart Home Devices) ตัวอย่าง: หลอดไฟอัจฉริยะ, กล้องวงจรปิดอัจฉริยะ, ลำโพงอัจฉริยะ
- ระบบควบคุมอุตสาหกรรม (Industrial Control Systems) ใช้ในโรงงานและกระบวนการผลิต เช่น ระบบ SCADA (Supervisory Control and Data Acquisition)
- เซ็นเซอร์ความปลอดภัย (Physical Security Sensors) ตัวอย่าง: เซ็นเซอร์ตรวจจับการเคลื่อนไหว, ระบบตรวจจับควันไฟ

ความเสี่ยงและการรักษาความปลอดภัยสำหรับอุปกรณ์ IoT

- ช่องโหว่ด้านความปลอดภัย (Security Vulnerabilities) อุปกรณ์ที่ไม่ได้รับการอัปเดตอาจถูกโจมตีได้
- การเข้าถึงโดยไม่ได้รับอนุญาต (Unauthorized Access) อุปกรณ์ที่มีการตั้งค่าความปลอดภัยไม่ดีอาจถูกเข้าถึงโดยไม่ได้รับอนุญาต
- การรั่วไหลของข้อมูล (Data Breaches) ข้อมูลที่จัดเก็บหรือส่งผ่านอุปกรณ์อาจถูกขโมยได้
- มัลแวร์และการโจมตี (Malware and Attacks) การโจมตีที่มุ่งเป้าไปที่อุปกรณ์ IoT เพื่อสร้างความเสียหายหรือหยุดการทำงาน

Library ไลบรารี

ไลบรารี (Library) หมายถึง โค้ดที่ถูกคอมไพล์ไว้ล่วงหน้าและสามารถนำมาใช้ซ้ำได้ ประกอบไปด้วยคลาส (Classes), กระบวนการ (Procedures), สคริปต์ (Scripts), ข้อมูลการตั้งค่า (Configuration Data) และอื่น ๆ ซึ่งใช้ในการพัฒนาโปรแกรมและแอปพลิเคชันซอฟต์แวร์

วัตถุประสงค์ของไลบรารี

- ช่วยนักพัฒนาโปรแกรม (Assist Programmers) ลดความซ้ำซ้อนในการเขียนโค้ดและช่วยให้นักพัฒนาทำงานได้รวดเร็วขึ้น
- สนับสนุนตัวคอมไพเลอร์ (Support Compilers) ช่วยให้คอมไพเลอร์ทำงานได้มีประสิทธิภาพในการสร้างและรันซอฟต์แวร์
- เพิ่มประสิทธิภาพการพัฒนา (Enhance Development Efficiency) ทำให้การพัฒนาโปรแกรมสะดวกและรวดเร็วขึ้นโดยใช้ฟังก์ชันหรือโมดูลที่มีอยู่แล้ว

ส่วนประกอบของไลบรารี

- คลาส (Classes) โครงสร้างที่รวบรวมฟังก์ชันและข้อมูลเข้าด้วยกัน เพื่อการเขียนโปรแกรมเชิงวัตถุ (OOP)

- กระบวนการ (Procedures) ฟังก์ชันหรือเมทอดที่สามารถเรียกใช้เพื่อทำงานเฉพาะเจาะจง
- สคริปต์ (Scripts) ชุดคำสั่งที่สามารถทำงานได้โดยอัตโนมัติ
- ข้อมูลการตั้งค่า (Configuration Data) ข้อมูลที่ใช้ตั้งค่าเพื่อควบคุมการทำงานของโปรแกรม

ประเภทของไลบรารี

- ไลบรารีมาตรฐาน (Standard Libraries) ไลบรารีที่มาพร้อมกับภาษาการเขียนโปรแกรม เช่น stdlib ใน Python หรือ java.lang ใน Java
- ไลบรารีจากบุคคลที่สาม (Third-Party Libraries) ไลบรารีที่พัฒนาขึ้นโดยนักพัฒนาภายนอก เช่น NumPy สำหรับ Python หรือ Lodash สำหรับ JavaScript
- ไลบรารีเฉพาะงาน (Specialized Libraries) ไลบรารีที่ออกแบบมาสำหรับงานเฉพาะ เช่น การประมวลผลภาพ, การจัดการฐานข้อมูล, หรือการเรียนรู้ของเครื่อง (Machine Learning)

Log Data ข้อมูลล็อก

ข้อมูลล็อก (Log Data) หมายถึงไฟล์ข้อมูลที่สร้างขึ้นโดยระบบคอมพิวเตอร์เพื่อบันทึกเหตุการณ์ต่าง ๆ ที่เกิดขึ้นภายในองค์กร ข้อมูลล็อกช่วยในการติดตามการทำงานของระบบ, การตรวจสอบความปลอดภัย, และการวิเคราะห์ปัญหาที่เกิดขึ้น

ลักษณะของข้อมูลล็อก

- บันทึกเหตุการณ์ (Event Recording) บันทึกข้อมูลเกี่ยวกับการทำงานของระบบ, การเข้าถึงทรัพยากร, และเหตุการณ์ที่เกี่ยวข้องกับความปลอดภัย
- สร้างโดยอัตโนมัติ (Computer-Generated) ระบบคอมพิวเตอร์สร้างข้อมูลล็อกขึ้นโดยอัตโนมัติเมื่อมีการกระทำหรือเหตุการณ์เกิดขึ้น
- เชื่อถือได้ (Reliable) เป็นหลักฐานที่เชื่อถือได้ในการตรวจสอบเหตุการณ์ย้อนหลัง

ตัวอย่างข้อมูลล็อก

- ล็อกระบบปฏิบัติการ (Operating System Logs) บันทึกการทำงานและข้อผิดพลาดของระบบปฏิบัติการ เช่น Windows Event Logs, Linux Syslog
- ล็อกการตรวจจับมัลแวร์ (Anti-Malware Detection Logs) บันทึกการตรวจพบมัลแวร์และการดำเนินการตอบสนอง
- ล็อกฐานข้อมูล (Database Logs) บันทึกการเข้าถึงฐานข้อมูล , การเปลี่ยนแปลงข้อมูล, และข้อผิดพลาดที่เกิดขึ้น
- ล็อกแอปพลิเคชัน (Application Logs) บันทึกการทำงานและการใช้งานแอปพลิเคชัน เช่น การล็อกอิน, การประมวลผลคำสั่ง
- ล็อกเครือข่าย (Network Logs) บันทึกการรับ-ส่งข้อมูลในเครือข่าย เช่น การเชื่อมต่อเครือข่าย, การรับส่งแพ็กเก็ตข้อมูล
- ล็อกไฟร์วอลล์ (Firewall Logs) บันทึกการปิดกั้นหรืออนุญาตการเชื่อมต่อเครือข่ายผ่านไฟร์วอลล์
- ล็อกเว็บเซิร์ฟเวอร์ (Web Server Logs) บันทึกการเข้าถึงเว็บไซต์ เช่น การร้องขอไฟล์, การตอบสนองเซิร์ฟเวอร์, และข้อผิดพลาด HTTP
- ล็อกการควบคุมการเข้าถึง (Access Control Logs) บันทึกการเข้าถึงระบบหรือพื้นที่ควบคุม เช่น ระบบล็อกประตูอิเล็กทรอนิกส์, ระบบสัญญาณเตือนภัย

ประโยชน์ของข้อมูลล็อก

- การตรวจสอบและวิเคราะห์ความปลอดภัย (Security Auditing and Analysis) ช่วยในการตรวจจับการบุกรุก, การโจมตีทางไซเบอร์, และพฤติกรรมที่น่าสงสัย
- การแก้ไขปัญหา (Troubleshooting) ใช้ในการวิเคราะห์และแก้ไขปัญหาการทำงานของระบบหรือแอปพลิเคชัน
- การปฏิบัติตามข้อกำหนด (Compliance) สนับสนุนการปฏิบัติตามมาตรฐานความปลอดภัย เช่น ISO 27001, GDPR, และ HIPAA
- การเฝ้าระวังและติดตามการทำงาน (Monitoring and Tracking) ช่วยให้ผู้ดูแลระบบติดตามการทำงานและประสิทธิภาพของระบบได้อย่างต่อเนื่อง
- การสืบสวนเหตุการณ์ (Incident Investigation) เป็นหลักฐานสำคัญในการสืบสวนเหตุการณ์ความปลอดภัยและการกู้คืนระบบหลังการโจมตี

Mobile Devices อุปกรณ์เคลื่อนที่

อุปกรณ์เคลื่อนที่ (Mobile Devices) หมายถึงอุปกรณ์สำหรับผู้ใช้งานปลายทางขนาดเล็ก ที่องค์กรจัดหาให้ ซึ่งมีความสามารถในการเชื่อมต่อแบบไร้สายในตัว โดยทั่วไปจะหมายถึงสมาร์ทโฟนและแท็บเล็ต

ลักษณะสำคัญของอุปกรณ์เคลื่อนที่

- ขนาดเล็กและพกพาง่าย (Small and Portable) สะดวกต่อการพกพาและใช้งานได้ทุกที่
- การเชื่อมต่อไร้สาย (Intrinsic Wireless Capability) มีความสามารถในการเชื่อมต่อผ่าน Wi-Fi, บลูทูธ, หรือเครือข่ายมือถือ (4G/5G)
- จัดหาโดยองค์กร (Enterprise-Issued) อุปกรณ์ที่องค์กรจัดหาให้เพื่อใช้ในการทำงาน
- เป็นส่วนย่อยของอุปกรณ์พกพา (Subset of Portable Devices) อุปกรณ์เคลื่อนที่ถือเป็นกลุ่มย่อยของอุปกรณ์พกพาที่สามารถเชื่อมต่อเครือข่ายได้

ตัวอย่างอุปกรณ์เคลื่อนที่

- สมาร์ทโฟน (Smartphones) อุปกรณ์โทรศัพท์มือถือที่มีความสามารถในการประมวลผลและเชื่อมต่ออินเทอร์เน็ต
- แท็บเล็ต (Tablets) อุปกรณ์ที่มีหน้าจอขนาดใหญ่กว่าสมาร์ทโฟน เหมาะสำหรับการทำงานและการอ่านข้อมูล

ความเสี่ยงด้านความปลอดภัยของอุปกรณ์เคลื่อนที่

- การสูญหายหรือถูกขโมย (Loss or Theft) ความเสี่ยงจากข้อมูลที่อาจรั่วไหลหากอุปกรณ์สูญหาย
- มัลแวร์และการโจมตีทางไซเบอร์ (Malware and Cyber Attacks) การติดตั้งแอปพลิเคชันที่ไม่ปลอดภัยหรือการโจมตีจากเครือข่ายที่ไม่ปลอดภัย
- การเชื่อมต่อเครือข่ายที่ไม่ปลอดภัย (Insecure Network Connections) การเชื่อมต่อ Wi-Fi สาธารณะอาจทำให้ข้อมูลถูกดักจับได้

แนวทางการรักษาความปลอดภัย

- การเข้ารหัสข้อมูล (Data Encryption) เข้ารหัสข้อมูลทั้งในขณะจัดเก็บและขณะส่งผ่านเครือข่าย
- การยืนยันตัวตนหลายปัจจัย (Multi-Factor Authentication: MFA) เพิ่มระดับความปลอดภัยในการเข้าถึงอุปกรณ์
- การจัดการอุปกรณ์เคลื่อนที่ (Mobile Device Management: MDM) ใช้เครื่องมือในการควบคุม, ตรวจสอบ, และลบข้อมูลจากระยะไกลเมื่อจำเป็น
- การอัปเดตซอฟต์แวร์ (Software Updates) ติดตั้งการอัปเดตระบบปฏิบัติการและแอปพลิเคชันอย่างสม่ำเสมอ

Multi-Factor Authentication: MFA การยืนยันตัวตนหลายปัจจัย

การยืนยันตัวตนหลายปัจจัย (Multi-Factor Authentication: MFA) หมายถึงกระบวนการยืนยันตัวตนที่ใช้ปัจจัยตั้งแต่สองประเภทขึ้นไปในการยืนยันตัวตนของผู้ใช้งาน โดยปัจจัยเหล่านี้ประกอบด้วยสิ่งที่ผู้ใช้รู้, สิ่งที่ผู้ใช้อยู่ในครอบครอง, และสิ่งที่บ่งบอกความเป็นตัวตนของผู้ใช้

ประเภทของปัจจัยการยืนยันตัวตน

1. สิ่งที่คุณรู้ (Something You Know) ข้อมูลที่ผู้ใช้จำได้ เช่น
   - PIN (Personal Identification Number)
   - รหัสผ่าน (Password)
   - คำถามเพื่อความปลอดภัย (Security Questions)
2. สิ่งที่คุณมี (Something You Have) อุปกรณ์หรือสิ่งที่ผู้ใช้มีอยู่ เช่น
   - อุปกรณ์ระบุตัวตนดิจิทัล (Cryptographic Identification Device)
   - โทเคน (Token)
   - แอปพลิเคชันยืนยันตัวตน (Authenticator Apps) เช่น Google Authenticator
3. สิ่งที่คุณเป็น (Something You Are) ลักษณะทางกายภาพเฉพาะตัวของผู้ใช้ เช่น
   - การสแกนลายนิ้วมือ (Fingerprint Scanning)
   - การจดจำใบหน้า (Facial Recognition)
   - การจดจำม่านตา (Iris Recognition)

Network เครือข่าย

เครือข่าย (Network) หมายถึง กลุ่มของอุปกรณ์ที่เชื่อมต่อถึงกันเพื่อแลกเปลี่ยนข้อมูลระหว่างกัน โดยเครือข่ายถือเป็นกลุ่มรวมที่ประกอบไปด้วยโครงสร้างพื้นฐานเครือข่าย (Network Infrastructure) และสถาปัตยกรรมเครือข่าย (Network Architecture)

องค์ประกอบหลักของเครือข่าย

1. โครงสร้างพื้นฐานเครือข่าย (Network Infrastructure) รวมฮาร์ดแวร์ และซอฟต์แวร์ ที่จำเป็นสำหรับการสื่อสารและการจัดการเครือข่าย ตัวอย่าง:
   - เราเตอร์ (Routers)
   - สวิตช์ (Switches)
   - ไฟร์วอลล์ (Firewalls)
   - จุดเชื่อมต่อไร้สาย (Wireless Access Points)
2. สถาปัตยกรรมเครือข่าย (Network Architecture) การออกแบบและการจัดระเบียบเครือข่ายทั้งในเชิงกายภาพและเชิงตรรกะ

Network Architecture สถาปัตยกรรมเครือข่าย

สถาปัตยกรรมเครือข่าย (Network Architecture) หมายถึงการออกแบบเครือข่ายทั้งในเชิงกายภาพและเชิงตรรกะ ซึ่งกำหนดวิธีการจัดระเบียบเครือข่าย, การเชื่อมต่อระหว่างอุปกรณ์และซอฟต์แวร์, และการส่งผ่านข้อมูลระหว่างอุปกรณ์ต่าง ๆ โดยควรรวมถึงแผนผังสถาปัตยกรรมเครือข่ายและแผนผังสถาปัตยกรรมความปลอดภัยด้วย

องค์ประกอบของสถาปัตยกรรมเครือข่าย

- การออกแบบกายภาพ (Physical Design) การเชื่อมต่อทางกายภาพของอุปกรณ์ต่าง ๆ ในเครือข่าย ตัวอย่าง: การเชื่อมต่อด้วยสายเคเบิล, ตำแหน่งของเราเตอร์และสวิตช์
- การออกแบบเชิงตรรกะ (Logical Design) การกำหนดการทำงาน, เส้นทางการส่งข้อมูล, และกฎการควบคุมการเข้าถึง ตัวอย่าง: VLANs (Virtual LANs), การกำหนด IP Address, Routing Protocols
- การแบ่งส่วนเครือข่าย (Network Segmentation) การแบ่งเครือข่ายออกเป็นส่วนย่อยเพื่อเพิ่มความปลอดภัยและประสิทธิภาพ ตัวอย่าง: เครือข่ายสำหรับพนักงาน, เครือข่ายสำหรับแขก, เครือข่ายสำหรับเซิร์ฟเวอร์
- ความปลอดภัยเครือข่าย (Network Security) มาตรการและการควบคุมเพื่อปกป้องเครือข่ายจากการโจมตี ตัวอย่าง: ไฟร์วอลล์, การเข้ารหัส, ระบบป้องกันการบุกรุก (IDS/IPS)

ประเภทของสถาปัตยกรรมเครือข่าย

- เครือข่ายแบบดาว (Star Topology) อุปกรณ์ทั้งหมดเชื่อมต่อกับศูนย์กลาง เช่น สวิตช์หรือเราเตอร์
- เครือข่ายแบบตาข่าย (Mesh Topology) อุปกรณ์แต่ละตัวเชื่อมต่อกันโดยตรงหลายเส้นทาง ช่วยเพิ่มความทนทาน
- เครือข่ายแบบบัส (Bus Topology) อุปกรณ์ทั้งหมดเชื่อมต่อกับสายกลางเส้นเดียว
- เครือข่ายแบบวงแหวน (Ring Topology) อุปกรณ์เชื่อมต่อกันเป็นวงกลม ข้อมูลไหลในทิศทางเดียวหรือสองทิศทาง

แผนผังสถาปัตยกรรมเครือข่าย

- แผนผังสถาปัตยกรรมเครือข่าย (Network Architecture Diagram) แสดงการเชื่อมต่อระหว่างอุปกรณ์เครือข่าย
- แผนผังสถาปัตยกรรมความปลอดภัย (Security Architecture Diagram) แสดงการควบคุมความปลอดภัย เช่น ตำแหน่งของไฟร์วอลล์, การแบ่งเครือข่ายเพื่อความปลอดภัย

ความสำคัญของสถาปัตยกรรมเครือข่าย

- เพิ่มประสิทธิภาพในการทำงาน (Performance Optimization) ช่วยให้การส่งข้อมูล ทำได้รวดเร็วและมีประสิทธิภาพ
- ความปลอดภัย (Security) ออกแบบให้สามารถควบคุม และป้องกันการโจมตีทางเครือข่ายได้
- การขยายเครือข่าย (Scalability) รองรับการขยายตัวของเครือข่ายในอนาคต
- การจัดการและการแก้ไขปัญหา (Manageability and Troubleshooting) ช่วยให้ผู้ดูแลระบบเข้าใจโครงสร้างเครือข่ายและแก้ไขปัญหาได้ง่ายขึ้น

Network Asset ทรัพย์สินเครือข่าย

ทรัพย์สินเครือข่าย (Network Asset) หมายถึงกลุ่มของอุปกรณ์ที่เชื่อมต่อถึงกันและสามารถแลกเปลี่ยนข้อมูลระหว่างกันได้ องค์กรอาจมีการจัดการเครือข่ายหนึ่งเครือข่ายหรือหลายเครือข่าย โดยแต่ละเครือข่ายสามารถถูกจัดการร่วมกันหรือแยกกันอย่างอิสระ

Network Devices อุปกรณ์เครือข่าย

อุปกรณ์เครือข่าย (Network Devices) หมายถึง อุปกรณ์อิเล็กทรอนิกส์ที่จำเป็นสำหรับการสื่อสาร และ การเชื่อมต่อระหว่างอุปกรณ์ต่าง ๆ ภายในเครือข่ายคอมพิวเตอร์ อุปกรณ์เหล่านี้ประกอบไปด้วยฮาร์ดแวร์ที่เป็นรูปธรรม, อุปกรณ์เสมือน, และอุปกรณ์ที่อยู่ในคลาวด์

ตัวอย่างอุปกรณ์เครือข่าย

- จุดเชื่อมต่อไร้สาย (Wireless Access Points) ให้การเชื่อมต่อเครือข่ายไร้สายสำหรับอุปกรณ์ต่าง ๆ เช่น แล็ปท็อป , สมาร์ทโฟน, และแท็บเล็ต
- ไฟร์วอลล์ (Firewalls) กำหนดและควบคุมการอนุญาตหรือปิดกั้นการรับ-ส่งข้อมูล เพื่อปกป้องเครือข่ายจากการโจมตี
- เกตเวย์ (Gateways) เป็นจุดเชื่อมต่อระหว่างเครือข่ายที่ต่างกัน เช่น เครือข่ายภายในและอินเทอร์เน็ต
- เราเตอร์ (Routers) จัดการการส่งข้อมูลระหว่างเครือข่ายต่าง ๆ และกำหนดเส้นทางการเดินทางของข้อมูล
- สวิตช์ (Switches) เชื่อมต่ออุปกรณ์หลาย ๆ ตัวในเครือข่ายเดียวกันและจัดการการส่งข้อมูลระหว่างอุปกรณ์เหล่านั้น

ประเภทของอุปกรณ์เครือข่าย

- อุปกรณ์ฮาร์ดแวร์ (Physical Hardware) อุปกรณ์จับต้องได้ เช่น เราเตอร์, สวิตช์, และไฟร์วอลล์
- อุปกรณ์เสมือน (Virtual Devices) อุปกรณ์ที่ทำงานในสภาพแวดล้อมเสมือน เช่น Virtual Routers, Virtual Firewalls
- อุปกรณ์ในคลาวด์ (Cloud-Based Devices) บริการเครือข่ายที่จัดการผ่านคลาวด์ เช่น Cloud Firewalls, Cloud Gateways

Network Infrastructure โครงสร้างพื้นฐานเครือข่าย

โครงสร้างพื้นฐานเครือข่าย (Network Infrastructure) หมายถึงทรัพยากรทั้งหมดในเครือข่ายที่ทำให้การเชื่อมต่อกับเครือข่ายหรืออินเทอร์เน็ต, การจัดการ, การดำเนินธุรกิจ, และการสื่อสารเป็นไปได้ ประกอบด้วยฮาร์ดแวร์, ซอฟต์แวร์, ระบบ, และอุปกรณ์ต่าง ๆ ซึ่งทำหน้าที่สนับสนุนการประมวลผลและการสื่อสารระหว่างผู้ใช้งาน, บริการ, แอปพลิเคชัน, และกระบวนการต่าง ๆ

องค์ประกอบของโครงสร้างพื้นฐานเครือข่าย

ฮาร์ดแวร์ (Hardware) อุปกรณ์เครือข่ายที่จับต้องได้ เช่น

- เราเตอร์ (Routers)
- สวิตช์ (Switches)
- ไฟร์วอลล์ (Firewalls)
- จุดเชื่อมต่อไร้สาย (Wireless Access Points)
- เซิร์ฟเวอร์ (Servers)
- ซอฟต์แวร์ (Software)

ซอฟต์แวร์ที่ควบคุมและจัดการการทำงานของเครือข่าย เช่น

- ระบบปฏิบัติการเครือข่าย (Network Operating Systems)
- ซอฟต์แวร์การจัดการเครือข่าย (Network Management Software)
- ระบบควบคุมการเข้าถึง (Access Control Systems)

ระบบและกระบวนการ (Systems and Processes)

กระบวนการและระบบที่ใช้ในการจัดการเครือข่าย เช่น

- ระบบตรวจสอบและเฝ้าระวัง (Monitoring Systems)
- ระบบตรวจจับและป้องกันการบุกรุก (IDS/IPS)
- ระบบจัดการการจราจรในเครือข่าย (Traffic Management Systems)

การเชื่อมต่อและการสื่อสาร (Connectivity and Communication)

ช่องทางและเทคโนโลยีสำหรับการเชื่อมต่อ เช่น

- สายเคเบิลเครือข่าย (Ethernet Cables)
- การเชื่อมต่อไร้สาย (Wi-Fi, Bluetooth)
- การเชื่อมต่อคลาวด์ (Cloud Connectivity)

Non-Computing/Internet of Things: IoT Devices อุปกรณ์ที่ไม่ใช่คอมพิวเตอร์/อินเทอร์เน็ตของสรรพสิ่ง

อุปกรณ์ที่ไม่ใช่คอมพิวเตอร์/อินเทอร์เน็ตของสรรพสิ่ง (Non-Computing/IoT Devices) หมายถึงอุปกรณ์ที่ฝังตัวเซ็นเซอร์, ซอฟต์แวร์, และเทคโนโลยีอื่น ๆ โดยมีวัตถุประสงค์เพื่อการเชื่อมต่อ, การจัดเก็บ, และการแลกเปลี่ยนข้อมูลกับอุปกรณ์และระบบอื่น ๆ ผ่านอินเทอร์เน็ต แม้อุปกรณ์เหล่านี้จะไม่ได้ใช้สำหรับการประมวลผลเชิงคอมพิวเตอร์โดยตรง แต่มีบทบาทในการสนับสนุนกระบวนการทำงานขององค์กร

Operating System ระบบปฏิบัติการ

หน้าที่หลักของระบบปฏิบัติการ

- การจัดการฮาร์ดแวร์ (Hardware Management) ควบคุมการทำงานของอุปกรณ์ฮาร์ดแวร์ เช่น ซีพียู, หน่วยความจำ, ฮาร์ดดิสก์, และอุปกรณ์ต่อพ่วง
- การจัดการซอฟต์แวร์ (Software Management) ควบคุมการติดตั้ง, การรัน, และการจัดการซอฟต์แวร์ต่าง ๆ
- การจัดการไฟล์และข้อมูล (File and Data Management) จัดการการอ่าน, การเขียน, และการจัดเก็บไฟล์ข้อมูลในระบบ
- การให้บริการพื้นฐาน (Common Services) ให้บริการต่าง ๆ ที่จำเป็น เช่น การรักษาความปลอดภัย, การควบคุมการเข้าถึง, และการเชื่อมต่อเครือข่าย
- การจัดการกระบวนการ (Process Management) จัดการการทำงานของโปรแกรมและกระบวนการที่รันอยู่ในระบบ

ตัวอย่างระบบปฏิบัติการยอดนิยม

- Windows ระบบปฏิบัติการสำหรับเครื่องคอมพิวเตอร์ตั้งโต๊ะและแล็ปท็อปที่พัฒนาโดย Microsoft
- Ubuntu ระบบปฏิบัติการแบบโอเพนซอร์สที่ใช้กับเซิร์ฟเวอร์และเครื่องเดสก์ท็อป
- MacOS ระบบปฏิบัติการสำหรับเครื่องคอมพิวเตอร์ของ Apple เช่น MacBook และ iMac
- Android ระบบปฏิบัติการสำหรับอุปกรณ์เคลื่อนที่ เช่น สมาร์ทโฟนและแท็บเล็ต

ประเภทของระบบปฏิบัติการ

- ระบบปฏิบัติการสำหรับเดสก์ท็อป (Desktop Operating Systems)เช่น Windows, MacOS, Ubuntu
- ระบบปฏิบัติการสำหรับเซิร์ฟเวอร์ (Server Operating Systems) เช่น Windows Server, Red Hat Enterprise Linux, z/OS
- ระบบปฏิบัติการสำหรับอุปกรณ์เคลื่อนที่ (Mobile Operating Systems) เช่น Android, iOS
- ระบบปฏิบัติการแบบฝังตัว (Embedded Operating Systems) ใช้ในอุปกรณ์ IoT, เครื่องใช้ไฟฟ้า, และระบบควบคุมในโรงงาน
- z/OS ระบบปฏิบัติการสำหรับเมนเฟรมคอมพิวเตอร์ที่พัฒนาโดย IBM

Phishing ฟิชชิง

ฟิชชิง (Phishing) คือ เทคนิคที่ใช้ในการหลอกลวงเพื่อให้ได้มาซึ่งข้อมูลสำคัญ เช่น หมายเลขบัญชีธนาคาร, รหัสผ่าน, หรือข้อมูลส่วนบุคคล โดยการส่งข้อความที่ดูเหมือนมาจากธุรกิจที่น่าเชื่อถือหรือบุคคลที่น่าไว้วางใจ ผ่านทางอีเมลหรือเว็บไซต์ปลอม

วิธีการฟิชชิงที่พบบ่อย

- ฟิชชิงผ่านอีเมล (Email Phishing) ผู้โจมตีส่งอีเมลที่แอบอ้างว่าเป็นองค์กรที่น่าเชื่อถือ เช่น ธนาคาร, บริษัทบัตรเครดิต หรือหน่วยงานราชการ เพื่อหลอกให้ผู้รับคลิกลิงก์หรือดาวน์โหลดไฟล์แนบที่เป็นอันตราย
- ฟิชชิงผ่านเว็บไซต์ (Website Phishing) การสร้างเว็บไซต์ปลอมที่มีหน้าตาเหมือนเว็บไซต์จริง เพื่อหลอกให้กรอกข้อมูลสำคัญ เช่น ชื่อผู้ใช้, รหัสผ่าน หรือหมายเลขบัตรเครดิต
- สเปียร์ฟิชชิง (Spear Phishing) การโจมตีที่เฉพาะเจาะจงโดยผู้โจมตีจะศึกษาข้อมูลของเป้าหมายเพื่อสร้างข้อความที่เหมือนกับการติดต่อจากคนรู้จักหรือหน่วยงานที่เกี่ยวข้อง
- วาฬฟิชชิง (Whale Phishing) การหลอกลวงผู้บริหารระดับสูงหรือผู้ที่มีอำนาจตัดสินใจในองค์กร โดยมักใช้เทคนิคการแอบอ้างที่มีความซับซ้อน
- สมิชชิง (Smishing) การหลอกลวงผ่านข้อความ SMS โดยมีลิงก์หรือข้อความที่หลอกให้ผู้ใช้ดำเนินการบางอย่าง
- วิชชิง (Vishing) การหลอกลวงผ่านการโทรศัพท์ โดยแอบอ้างเป็นเจ้าหน้าที่หรือบุคคลที่น่าเชื่อถือเพื่อให้เหยื่อเปิดเผยข้อมูล

ลักษณะของฟิชชิง

- ข้อความเร่งด่วน (Sense of Urgency) ข้อความที่สร้างความรู้สึกเร่งด่วน เช่น "บัญชีของคุณจะถูกระงับหากไม่ดำเนินการภายใน 24 ชั่วโมง"
- ข้อเสนอที่ดูดีเกินจริง (Too Good to Be True) ข้อเสนอที่ดูน่าสนใจเกินไป เช่น รางวัลเงินสดหรือสิทธิพิเศษ
- ลิงก์ปลอม (Fake Links) ลิงก์ที่ดูเหมือนจะเป็นของจริง แต่เมื่อคลิกแล้วจะนำไปยังเว็บไซต์ปลอม
- ไฟล์แนบอันตราย (Malicious Attachments) ไฟล์แนบที่มีมัลแวร์ซ่อนอยู่ เช่น ไฟล์ PDF, Word, หรือ ZIP
- การสะกดผิดหรือข้อความแปลก ๆ (Spelling Errors or Odd Language) ข้อความที่มีการสะกดผิดหรือการใช้ภาษาที่ไม่เป็นทางการ

วิธีป้องกันการฟิชชิง

- ตรวจสอบที่อยู่อีเมล (Verify Email Address) ตรวจสอบว่าที่อยู่อีเมลผู้ส่งตรงกับหน่วยงานที่อ้างหรือไม่
- หลีกเลี่ยงการคลิกลิงก์โดยตรง (Avoid Clicking Direct Links) พิมพ์ URL ด้วยตนเองแทนการคลิกลิงก์จากอีเมล
- ใช้การยืนยันตัวตนหลายปัจจัย (Enable Multi-Factor Authentication) เพิ่มชั้นความปลอดภัยในการเข้าสู่ระบบ
- ติดตั้งโปรแกรมป้องกันไวรัส (Install Anti-Malware Software) ใช้ซอฟต์แวร์ป้องกันไวรัสที่ทันสมัยและอัปเดตอยู่เสมอ
- ฝึกอบรมพนักงาน (Employee Training) ให้ความรู้แก่พนักงานเกี่ยวกับการระบุและป้องกันการฟิชชิง
- รายงานการฟิชชิง (Report Phishing) หากพบการโจมตีฟิชชิง ควรรายงานไปยังฝ่ายไอทีหรือหน่วยงานที่เกี่ยวข้องทันที

Physical Data ข้อมูลแบบกายภาพ

ข้อมูลแบบกายภาพ (Physical Data) หมายถึง ข้อมูลที่จัดเก็บในเอกสารที่จับต้องได้หรือจัดเก็บในอุปกรณ์จัดเก็บข้อมูลแบบถอดได้ทางกายภาพ เช่น แฟลชไดรฟ์ USB, เทปสำรองข้อมูล เป็นต้น ข้อมูลแบบกายภาพอาจเป็นข้อมูลที่มีความละเอียดอ่อนหรือไม่ก็ได้

ตัวอย่างของข้อมูลแบบกายภาพ

1. เอกสารกระดาษ (Paper Documents) เช่น สัญญา, ใบแจ้งหนี้, รายงานทางการเงิน, บันทึกการประชุม
2. อุปกรณ์จัดเก็บข้อมูลแบบถอดได้ (Removable Storage Devices)เช่น
   - แฟลชไดรฟ์ (USB Drives)
   - ฮาร์ดไดรฟ์ภายนอก (External Hard Drives)
   - การสำรองข้อมูลบนเทป (Tape Backups)
   - ซีดีและดีวีดี (CDs/DVDs)
   - รูปถ่ายหรือฟิล์ม (Photographs or Film) ภาพถ่ายทางกายภาพที่มีข้อมูลหรือหลักฐานสำคัญ

ลักษณะของข้อมูลแบบกายภาพ

- จับต้องได้ (Tangible) สามารถมองเห็นและสัมผัสได้ เช่น กระดาษและอุปกรณ์จัดเก็บข้อมูล
- เสี่ยงต่อการสูญหายหรือถูกขโมย (Prone to Loss or Theft) การทำหายหรือถูกขโมยทำให้ข้อมูลรั่วไหลได้ง่าย
- จำเป็นต้องมีการรักษาความปลอดภัย (Requires Physical Security)ต้องเก็บรักษาในพื้นที่ปลอดภัย เช่น ตู้เซฟ, ห้องควบคุมการเข้าถึง

วิธีการปกป้องข้อมูลแบบกายภาพ

- การเข้ารหัสข้อมูล (Data Encryption) เข้ารหัสข้อมูลบนอุปกรณ์จัดเก็บแบบถอดได้ เช่น แฟลชไดรฟ์ USB
- การควบคุมการเข้าถึง (Access Control) จำกัดการเข้าถึงเอกสารและอุปกรณ์ให้เฉพาะผู้ที่ได้รับอนุญาต
- การจัดเก็บในที่ปลอดภัย (Secure Storage) เก็บเอกสารในตู้ล็อกหรือพื้นที่ที่มีระบบรักษาความปลอดภัย
- การทำลายข้อมูลอย่างปลอดภัย (Secure Data Destruction) ทำลายเอกสารหรืออุปกรณ์ที่ไม่ใช้งานแล้วโดยการย่อยเอกสารหรือทำลายอุปกรณ์

- การสำรองข้อมูล (Data Backup) สำรองข้อมูลในสถานที่หรือสื่อที่ปลอดภัย

ความเสี่ยงที่เกี่ยวข้องกับข้อมูลแบบกายภาพ

- การสูญหาย (Loss) เอกสารหรืออุปกรณ์จัดเก็บข้อมูลสูญหายจากความประมาท
- การโจรกรรม (Theft) ข้อมูลอาจถูกขโมยจากการเข้าถึงโดยไม่ได้รับอนุญาต
- ความเสียหายทางกายภาพ (Physical Damage) น้ำท่วม, ไฟไหม้, หรือความเสียหายจากการใช้งานทำให้ข้อมูลสูญหายได้
- การรั่วไหลของข้อมูล (Data Breach) การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาตอาจนำไปสู่การรั่วไหลของข้อมูลสำคัญ

Physical Environment สภาพแวดล้อมทางกายภาพ

สภาพแวดล้อมทางกายภาพ (Physical Environment) หมายถึง ส่วนประกอบฮาร์ดแวร์ที่จับต้องได้ซึ่งเป็นส่วนหนึ่งของเครือข่าย รวมถึงสายเคเบิลและเราเตอร์ ฮาร์ดแวร์เหล่านี้จำเป็นสำหรับการสื่อสารและการเชื่อมต่อระหว่างอุปกรณ์ต่าง ๆ ในเครือข่าย

Plan แผน

แผน (Plan) หมายถึง เอกสารหรือแนวทางปฏิบัติที่จัดทำขึ้นเพื่อดำเนินการตามนโยบายที่กำหนดไว้ โดยแผนอาจประกอบด้วยกลุ่มของนโยบาย, กระบวนการ (Processes), และขั้นตอนการปฏิบัติ (Procedures) ที่มีการกำหนดไว้อย่างชัดเจน

Policy นโยบาย

นโยบาย (Policy) หมายถึง แถลงการณ์การกำกับดูแลอย่างเป็นทางการ ซึ่งกำหนดวัตถุประสงค์เฉพาะของโปรแกรมการรักษาความปลอดภัยของข้อมูล (Information Security Program) นโยบายทำหน้าที่เป็นแนวทางปฏิบัติและกำหนดขอบเขตสำหรับการจัดการและปกป้องทรัพยากรขององค์กร

Portable Devices อุปกรณ์พกพา

อุปกรณ์พกพา (Portable Devices) หมายถึง อุปกรณ์สำหรับผู้ใช้งานที่สามารถเคลื่อนย้ายได้และมีความสามารถในการเชื่อมต่อเครือข่ายแบบไร้สาย อุปกรณ์เหล่านี้เป็นส่วนหนึ่งของอุปกรณ์สำหรับผู้ใช้งาน (End-User Devices)

Pretexting การหลอกลวงโดยการสร้างเรื่อง

การหลอกลวงโดยการสร้างเรื่อง (Pretexting) เป็นเทคนิคหนึ่งในการโจมตีแบบวิศวกรรมสังคม (Social Engineering) ซึ่งผู้โจมตีสร้างสถานการณ์หรือเรื่องราวขึ้นมาเพื่อหลอกล่อให้เหยื่อยอมเปิดเผยข้อมูลที่ไม่ควรเปิดเผย เป้าหมายของการหลอกลวงประเภทนี้คือการทำให้เหยื่อเชื่อมั่นว่าการสื่อสารนั้นถูกต้องและมาจากแหล่งที่น่าเชื่อถือ การหลอกลวงสามารถเกิดขึ้นได้ผ่านวิธีการสื่อสารหรือสื่อใด ๆ ก็ได้ เช่น โทรศัพท์, อีเมล, ข้อความ, หรือการสนทนาต่อหน้า

ลักษณะสำคัญของการหลอกลวงโดยการสร้างเรื่อง

- การสร้างเรื่องราวที่น่าเชื่อถือ (Believable Scenario) ผู้โจมตีคิดค้นสถานการณ์หรือเรื่องราวที่ทำให้เหยื่อเชื่อว่าเป็นการติดต่อที่ถูกต้อง
- การแอบอ้างบุคคลหรือหน่วยงาน (Impersonation) แอบอ้างเป็นบุคคลที่มีอำนาจ, หน่วยงานที่เชื่อถือได้, หรือคนรู้จักของเหยื่อ
- การใช้วิธีการสื่อสารที่หลากหลาย (Multiple Communication Methods) การหลอกลวงสามารถเกิดขึ้นผ่านการโทรศัพท์, อีเมล, ข้อความ, หรือการพูดคุยแบบตัวต่อตัว

ตัวอย่างการหลอกลวงโดยการสร้างเรื่อง

- แอบอ้างเป็นเจ้าหน้าที่ฝ่ายไอที (IT Department Impersonation) ผู้โจมตีโทรหาเหยื่อโดยอ้างว่าเป็นเจ้าหน้าที่ฝ่ายไอทีและขอให้เหยื่อให้ข้อมูลรหัสผ่านเพื่อแก้ไขปัญหาในระบบ
- การปลอมเป็นเจ้าหน้าที่ธนาคาร (Bank Officer Impersonation) ผู้โจมตีอ้างว่าเป็นเจ้าหน้าที่ธนาคารและแจ้งเหยื่อว่าบัญชีมีปัญหา พร้อมขอข้อมูลบัญชีเพื่อยืนยันตัวตน
- แอบอ้างเป็นผู้จัดการฝ่ายบุคคล (HR Department Impersonation) ส่งอีเมลแจ้งว่ามีการอัปเดตข้อมูลพนักงานและขอให้เหยื่อยืนยันข้อมูลส่วนตัวผ่านลิงก์ปลอม

วัตถุประสงค์ของการหลอกลวงโดยการสร้างเรื่อง

- ขโมยข้อมูลส่วนบุคคล (Stealing Personal Information) เช่น รหัสผ่าน, หมายเลขบัตรเครดิต, หรือข้อมูลบัญชีธนาคาร
- เข้าถึงระบบเครือข่าย (Gaining Network Access) หลอกให้เหยื่อมอบข้อมูลที่ใช้ในการเข้าสู่ระบบหรือการควบคุมเครือข่าย
- การหลอกลวงทางการเงิน (Financial Fraud) หลอกให้เหยื่อทำธุรกรรมทางการเงินหรือโอนเงินให้ผู้โจมตี

วิธีป้องกันการหลอกลวงโดยการสร้างเรื่อง

- ตรวจสอบแหล่งที่มา (Verify Source) ตรวจสอบให้แน่ใจว่าผู้ติดต่อเป็นบุคคลหรือหน่วยงานที่ถูกต้อง
- หลีกเลี่ยงการให้ข้อมูลทางโทรศัพท์หรืออีเมล (Avoid Sharing Sensitive Information) อย่าให้ข้อมูลที่ละเอียดอ่อนผ่านช่องทางที่ไม่ปลอดภัยหรือไม่ได้รับการยืนยัน
- ฝึกอบรมพนักงาน (Employee Training) ให้ความรู้เกี่ยวกับการโจมตีแบบวิศวกรรมสังคมและวิธีการรับมือ
- ใช้การยืนยันตัวตนหลายปัจจัย (Multi-Factor Authentication: MFA) เพิ่มความปลอดภัยในการเข้าถึงระบบหรือบัญชี
- ตั้งข้อสงสัยกับการขอข้อมูล (Be Skeptical of Requests for Information) หากมีการขอข้อมูลที่ผิดปกติ ให้สงสัยไว้ก่อนและตรวจสอบให้แน่ใจ

ขั้นตอนปฏิบัติ (Procedure)

ขั้นตอนปฏิบัติ (Procedure) หมายถึง ชุดของขั้นตอนที่เรียงลำดับอย่างชัดเจน ซึ่งต้องปฏิบัติตามเพื่อให้บรรลุงานเฉพาะที่กำหนดไว้ โดยขั้นตอนปฏิบัตินี้จะระบุวิธีการปฏิบัติที่ได้รับการอนุมัติสำหรับการดำเนินการในสภาพแวดล้อมทางเทคโนโลยีและองค์กร

ลักษณะสำคัญของขั้นตอนปฏิบัติ

- เรียงลำดับอย่างชัดเจน (Sequential Steps) ระบุขั้นตอนการปฏิบัติงานอย่างเป็นลำดับเพื่อความชัดเจนและหลีกเลี่ยงความสับสน

- เฉพาะเจาะจง (Specific) มุ่งเน้นไปที่การปฏิบัติงานเฉพาะเรื่อง เช่น การติดตั้งซอฟต์แวร์หรือการสำรองข้อมูล
- ได้รับการอนุมัติ (Approved) ขั้นตอนปฏิบัติต้องผ่านการอนุมัติจากผู้มีอำนาจภายในองค์กร
- สามารถทำซ้ำได้ (Repeatable) สามารถปฏิบัติซ้ำได้อย่างสม่ำเสมอเพื่อให้ได้ผลลัพธ์ที่คาดหวัง
- อ้างอิงได้ง่าย (Documented and Accessible) มีการบันทึกไว้เป็นลายลักษณ์อักษรและสามารถเข้าถึงได้ง่าย

Process กระบวนการ

กระบวนการ (Process) หมายถึง ชุดของงาน และกิจกรรมทั่วไปที่ดำเนินการเพื่อให้บรรลุเป้าหมายที่เกี่ยวข้องกับความปลอดภัย กระบวนการมักกำหนดลำดับขั้นตอนการทำงานที่ชัดเจนเพื่อให้มั่นใจว่างานที่เกี่ยวข้องกับความปลอดภัยดำเนินไปอย่างมีประสิทธิภาพและสอดคล้องกับนโยบายขององค์กร

Remote Devices อุปกรณ์ระยะไกล

อุปกรณ์ระยะไกล (Remote Devices) หมายถึง สินทรัพย์ขององค์กรที่สามารถเชื่อมต่อกับเครือข่ายจากระยะไกล โดยปกติผ่านทางอินเทอร์เน็ตสาธารณะ ซึ่งครอบคลุมถึงอุปกรณ์ต่าง ๆ เช่น อุปกรณ์สำหรับผู้ใช้งาน (End-User Devices), อุปกรณ์เครือข่าย (Network Devices), อุปกรณ์ที่ไม่ใช่คอมพิวเตอร์/อินเทอร์เน็ตของสรรพสิ่ง (Non-Computing/IoT Devices), และเซิร์ฟเวอร์ (Servers)

Remote File Systems ระบบไฟล์ระยะไกล

ระบบไฟล์ระยะไกล (Remote File Systems) หมายถึง ระบบที่ช่วยให้อุปกรณ์ในองค์กร (Enterprise Asset) สามารถเข้าถึงไฟล์ที่จัดเก็บอยู่ในอุปกรณ์อื่นผ่านเครือข่าย ระบบไฟล์ระยะไกลมักทำให้อุปกรณ์อื่น ๆ เช่น อุปกรณ์ที่ไม่ใช่คอมพิวเตอร์ (Non-Computing Devices) สามารถเข้าถึงได้จากอุปกรณ์ที่กำหนดไว้ การเข้าถึงไฟล์ระยะไกลนี้ดำเนินการผ่านเครือข่าย เช่น เครือข่ายท้องถิ่น (LAN), เครือข่ายกว้าง (WAN), การเชื่อมต่อแบบจุดต่อจุด (Point-to-Point Link), หรือวิธีการสื่อสารอื่น ๆ ระบบไฟล์ประเภทนี้มักเรียกว่า ระบบไฟล์เครือข่าย (Network File Systems) หรือ ระบบไฟล์แบบกระจาย (Distributed File Systems)

ตัวอย่างระบบไฟล์ระยะไกล

- Network File System (NFS) โปรโตคอลที่ใช้กันอย่างแพร่หลายในระบบปฏิบัติการ UNIX/Linux สำหรับการแชร์ไฟล์ระหว่างเครื่องคอมพิวเตอร์ผ่านเครือข่าย
- Server Message Block (SMB)/Common Internet File System (CIFS) โปรโตคอลที่ใช้ในระบบปฏิบัติการ Windows สำหรับการแชร์ไฟล์, เครื่องพิมพ์, และทรัพยากรอื่น ๆ ผ่านเครือข่าย
- Distributed File System (DFS) ระบบไฟล์ที่ช่วยให้สามารถจัดการไฟล์ที่กระจายอยู่ในหลายเครื่องได้อย่างเป็นระบบ
- File Transfer Protocol (FTP) โปรโตคอลสำหรับการถ่ายโอนไฟล์ระหว่างไคลเอนต์และเซิร์ฟเวอร์ผ่านเครือข่าย
- WebDAV (Web Distributed Authoring and Versioning) ส่วนขยายของ HTTP ที่ช่วยให้สามารถสร้าง, แก้ไข, และจัดการไฟล์ในเซิร์ฟเวอร์ระยะไกลได้

Removable Media สื่อแบบถอดได้

สื่อแบบถอดได้ (Removable Media) หมายถึง อุปกรณ์จัดเก็บข้อมูลที่สามารถถอดออกจากคอมพิวเตอร์ได้ในขณะที่ระบบยังคงทำงานอยู่ และสามารถใช้ในการย้ายข้อมูลจากระบบหนึ่งไปยังอีกระบบหนึ่งได้

ตัวอย่างของสื่อแบบถอดได้

- ซีดี (CDs) แผ่นดิสก์ที่ใช้จัดเก็บข้อมูล เช่น เพลงหรือไฟล์ข้อมูล
- ดีวีดี (DVDs) แผ่นดิสก์ที่สามารถจัดเก็บข้อมูลได้มากกว่า CD และมักใช้ในการเก็บภาพยนตร์หรือข้อมูลปริมาณมาก
- บลูเรย์ดิสก์ (Blu-ray Discs) แผ่นดิสก์ที่มีความจุสูง เหมาะสำหรับการจัดเก็บวิดีโอความละเอียดสูง
- ฮาร์ดไดรฟ์ภายนอก (External Hard Drives) อุปกรณ์จัดเก็บข้อมูลความจุสูงที่เชื่อมต่อผ่าน USB หรือ eSATA
- การ์ด SD (SD Cards) การ์ดหน่วยความจำขนาดเล็กที่ใช้ในกล้องถ่ายรูป, สมาร์ทโฟน และอุปกรณ์พกพาอื่น ๆ
- เทปสำรองข้อมูล (Tape Backups) สื่อจัดเก็บข้อมูลแบบแม่เหล็กที่ใช้สำหรับการสำรองข้อมูลปริมาณมาก
- ฟลอปปี้ดิสก์ (Diskettes) สื่อจัดเก็บข้อมูลแบบเก่าที่ใช้กับคอมพิวเตอร์รุ่นเก่า
- แฟลชไดรฟ์ (USB Drives) อุปกรณ์จัดเก็บข้อมูลขนาดเล็กที่เชื่อมต่อผ่านพอร์ต USB

ลักษณะสำคัญของสื่อแบบถอดได้

- เคลื่อนย้ายได้ง่าย (Portability) สามารถพกพาและถ่ายโอนข้อมูลระหว่างอุปกรณ์ได้สะดวก
- ใช้งานร่วมกับหลายอุปกรณ์ (Compatibility) สามารถใช้งานร่วมกับคอมพิวเตอร์และอุปกรณ์หลากหลายประเภท
- ความจุหลากหลาย (Variety of Storage Capacity) มีความจุให้เลือกตั้งแต่ไม่กี่เมกะไบต์ไปจนถึงหลายเทราไบต์
- ใช้งานขณะระบบทำงานอยู่ (Hot-Swappable) สามารถเชื่อมต่อและถอดออกได้โดยไม่ต้องปิดระบบ

ความเสี่ยงและข้อควรระวังในการใช้สื่อแบบถอดได้

- การติดมัลแวร์ (Malware Infections) สื่อแบบถอดได้อาจนำไวรัสหรือมัลแวร์เข้าสู่ระบบได้หากไม่มีการสแกนก่อนใช้งาน
- การสูญหายหรือถูกขโมย (Loss or Theft) ความเสี่ยงจากการสูญหายหรือถูกขโมยทำให้ข้อมูลรั่วไหล
- การรั่วไหลของข้อมูล (Data Leakage) ข้อมูลที่จัดเก็บในสื่อแบบถอดได้อาจถูกเข้าถึงโดยไม่ได้รับอนุญาต
- ความเสียหายทางกายภาพ (Physical Damage) สื่อแบบถอดได้มีความเสี่ยงต่อการเสียหายจากการกระแทก, ความชื้น, หรือความร้อน

แนวทางการรักษาความปลอดภัยสำหรับสื่อแบบถอดได้

- การเข้ารหัสข้อมูล (Data Encryption) เข้ารหัสข้อมูลที่จัดเก็บเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต
- การสแกนมัลแวร์ (Malware Scanning) สแกนหามัลแวร์ทุกครั้งก่อนใช้งาน
- ควบคุมการใช้งาน (Usage Control) กำหนดนโยบายควบคุมการใช้สื่อแบบถอดได้ในองค์กร
- การทำลายข้อมูลอย่างปลอดภัย (Secure Data Destruction) ทำลายข้อมูลในสื่ออย่างปลอดภัยก่อนทิ้งหรือใช้งานซ้ำ

- ติดตามและบันทึกการใช้งาน (Logging and Monitoring) บันทึกการใช้งานสื่อแบบถอดได้เพื่อการตรวจสอบและติดตาม

Script สคริปต์

สคริปต์ (Script) หมายถึง โค้ดที่ยังไม่ได้ถูกคอมไพล์ ซึ่งต้องการสภาพแวดล้อมของซอฟต์แวร์ในการประมวลผลและทำงาน โดยสคริปต์มักใช้ในการทำงานอัตโนมัติ (Automation), การประมวลผลข้อมูล, และการควบคุมการทำงานของโปรแกรมต่าง ๆ

ลักษณะสำคัญของสคริปต์

- ไม่ต้องคอมไพล์ (Interpreted) สคริปต์จะถูกตีความ (Interpret) และประมวลผลในขณะรันไทม์ โดยไม่ต้องคอมไพล์เป็นไฟล์ปฏิบัติการล่วงหน้า
- ต้องการสภาพแวดล้อมในการทำงาน (Execution Environment) ต้องทำงานภายใต้สภาพแวดล้อมเฉพาะ เช่น โปรแกรมแปลภาษา, อินเทอร์พรีเตอร์, หรือเครื่องมือที่รองรับสคริปต์
- ง่ายต่อการแก้ไข (Easy to Edit) สามารถแก้ไขและปรับปรุงได้ง่ายโดยไม่ต้องคอมไพล์ใหม่
- เหมาะสำหรับงานอัตโนมัติ (Automation) ใช้สำหรับการทำงานซ้ำ ๆ หรือการเขียนงานที่ต้องการความยืดหยุ่นสูง

Sensitive Data ข้อมูลที่อ่อนไหว

ข้อมูลที่อ่อนไหว (Sensitive Data) หมายถึง ข้อมูลทั้งในรูปแบบกายภาพและดิจิทัลที่จัดเก็บ, ประมวลผล, หรือถูกจัดการโดยองค์กร ซึ่งต้องมีการรักษาความเป็นส่วนตัว, ความถูกต้อง, ความน่าเชื่อถือ, และความพร้อมใช้งาน หากข้อมูลดังกล่าวถูกเปิดเผยหรือถูกทำลายโดยไม่ได้รับอนุญาต อาจก่อให้เกิดความเสียหายต่อองค์กรหรือผู้ใช้บริการขององค์กร

ตัวอย่างของข้อมูลที่อ่อนไหว

- ข้อมูลส่วนบุคคล (Personal Information) เช่น ชื่อ, ที่อยู่, หมายเลขบัตรประชาชน, หมายเลขโทรศัพท์
- ข้อมูลการเงิน (Financial Information) เช่น หมายเลขบัตรเครดิต, รายการธุรกรรม, ข้อมูลบัญชีธนาคาร
- ข้อมูลทางการแพทย์ (Medical Records) เช่น ประวัติการรักษา, โรคประจำตัว, ข้อมูลการประกันสุขภาพ
- ข้อมูลทางธุรกิจ (Business Data) เช่น แผนกลยุทธ์, ข้อมูลลูกค้า, รายงานทางการเงิน
- ข้อมูลทรัพย์สินทางปัญญา (Intellectual Property) เช่น สิทธิบัตร, เครื่องหมายการค้า, ข้อมูลการวิจัยและพัฒนา

Servers เซิร์ฟเวอร์

เซิร์ฟเวอร์ (Servers) หมายถึง อุปกรณ์หรือระบบที่ทำหน้าที่ให้บริการทรัพยากร, ข้อมูล, บริการ, หรือโปรแกรมแก่เครื่องอื่น ๆ บนเครือข่ายท้องถิ่น (Local Area Network: LAN) หรือเครือข่ายกว้าง (Wide Area Network: WAN) เซิร์ฟเวอร์สามารถให้บริการและใช้ทรัพยากรจากระบบอื่นได้พร้อมกัน

ลักษณะสำคัญของเซิร์ฟเวอร์

- การให้บริการ (Service Provision) ให้บริการต่าง ๆ เช่น การประมวลผลข้อมูล, การจัดเก็บไฟล์, การประมวลผลอีเมล และการโฮสต์เว็บไซต์
- ทำงานในเครือข่าย (Network-Based) ทำงานภายในเครือข่ายท้องถิ่น (LAN) หรือเครือข่ายกว้าง (WAN)
- รองรับการใช้งานร่วมกัน (Shared Access) ให้บริการแก่หลายอุปกรณ์และผู้ใช้พร้อมกัน
- การจัดการทรัพยากร (Resource Management) จัดการการใช้ทรัพยากร เช่น พื้นที่จัดเก็บข้อมูลและหน่วยประมวลผล

ประเภทของเซิร์ฟเวอร์

- เว็บเซิร์ฟเวอร์ (Web Server) ให้บริการโฮสต์เว็บไซต์และเว็บแอปพลิเคชัน ตัวอย่าง: Apache, Nginx, Microsoft IIS
- แอปพลิเคชันเซิร์ฟเวอร์ (Application Server) ให้บริการและประมวลผลแอปพลิเคชันต่าง ๆ ตัวอย่าง: JBoss, Tomcat, WebSphere
- เมลเซิร์ฟเวอร์ (Mail Server) ให้บริการรับ-ส่งและจัดเก็บอีเมล ตัวอย่าง: Microsoft Exchange, Postfix, Sendmail
- ไฟล์เซิร์ฟเวอร์ (File Server) ให้บริการจัดเก็บและแชร์ไฟล์ในเครือข่าย ตัวอย่าง: Windows File Server, Samba
- ฐานข้อมูลเซิร์ฟเวอร์ (Database Server) จัดการและให้บริการฐานข้อมูล ตัวอย่าง: MySQL, Microsoft SQL Server, Oracle Database
- DNS เซิร์ฟเวอร์ (DNS Server) แปลงชื่อโดเมนเป็นที่อยู่ IP ตัวอย่าง: BIND, Microsoft DNS Server
- เสมือนเซิร์ฟเวอร์ (Virtual Server) เซิร์ฟเวอร์ที่จำลองขึ้นภายในเครื่องจริง ตัวอย่าง: VMware, Hyper-V

สภาพแวดล้อมของเซิร์ฟเวอร์

- ดาต้าเซ็นเตอร์ (Datacenter) ศูนย์กลางที่เก็บเซิร์ฟเวอร์หลายเครื่องเพื่อให้บริการต่าง ๆ
- คลาวด์สาธารณะ (Public Cloud) เซิร์ฟเวอร์ที่ให้บริการผ่านผู้ให้บริการคลาวด์ เช่น AWS, Microsoft Azure, Google Cloud
- คลาวด์ส่วนตัว (Private Cloud) เซิร์ฟเวอร์ที่ให้บริการเฉพาะในองค์กร
- คลาวด์ผสม (Hybrid Cloud) การผสมผสานระหว่างคลาวด์สาธารณะและคลาวด์ส่วนตัว
- คอนเทนเนอร์ชั่วคราว (Temporal Containers) เซิร์ฟเวอร์ที่ทำงานในสภาพแวดล้อมคอนเทนเนอร์ เช่น Docker
- เวิร์กโหลดแบบไร้เซิร์ฟเวอร์ (Serverless Workloads) การประมวลผลที่ไม่ต้องจัดการเซิร์ฟเวอร์โดยตรง เช่น AWS Lambda

บทบาทของเซิร์ฟเวอร์ในองค์กร

- สนับสนุนการทำงานร่วมกัน (Collaboration Support) ให้บริการแชร์ไฟล์และการทำงานร่วมกันในทีม
- โฮสต์แอปพลิเคชันทางธุรกิจ (Business Application Hosting) รองรับแอปพลิเคชันที่จำเป็นต่อการดำเนินธุรกิจ
- การจัดเก็บข้อมูล (Data Storage) จัดเก็บข้อมูลที่สำคัญและสามารถเข้าถึงได้อย่างปลอดภัย
- การประมวลผลและวิเคราะห์ข้อมูล (Data Processing and Analysis) ประมวลผลข้อมูลขนาดใหญ่และการวิเคราะห์ข้อมูล

- การรักษาความปลอดภัย (Security) ให้บริการด้านความปลอดภัย เช่น การยืนยันตัวตนและการสำรองข้อมูล

Service Accounts บัญชีบริการ

บัญชีบริการ (Service Accounts) หมายถึง บัญชีที่สร้างขึ้นโดยเฉพาะเพื่อใช้ในการรันแอปพลิเคชัน, บริการ, และงานอัตโนมัติต่าง ๆ บนระบบปฏิบัติการ นอกจากนี้ บัญชีบริการยังอาจถูกสร้างขึ้นเพื่อเป็นเจ้าของข้อมูลและไฟล์การกำหนดค่า (Configuration Files) โดยเฉพาะ

ลักษณะสำคัญของบัญชีบริการ

- ใช้สำหรับงานเฉพาะเจาะจง (Specific Purpose) บัญชีบริการถูกสร้างขึ้นเพื่อทำงานเฉพาะ เช่น การรันบริการหรือแอปพลิเคชันใดแอปพลิเคชันหนึ่ง
- มีเจ้าของที่รับผิดชอบ (Assigned Owner) ควรกำหนดผู้รับผิดชอบบัญชีบริการแต่ละบัญชี เพื่อควบคุมและดูแลการใช้งาน
- ไม่ใช่สำหรับการใช้งานทั่วไป (Not for General Use) ไม่ควรใช้บัญชีบริการสำหรับการใช้งานทั่วไป เช่น การล็อกอินเพื่อท่องเว็บหรือใช้แอปพลิเคชันประจำวัน
- การควบคุมสิทธิ์ (Permission Control) กำหนดสิทธิ์การเข้าถึงเฉพาะที่จำเป็นสำหรับการทำงานของบริการนั้น ๆ เพื่อลดความเสี่ยงด้านความปลอดภัย
- การทำงานอัตโนมัติ (Automation) บัญชีบริการมักถูกใช้ในการทำงานอัตโนมัติ เช่น การสำรองข้อมูล, การประมวลผลตามเวลาที่กำหนด (Scheduled Tasks)

ตัวอย่างการใช้งานบัญชีบริการ

- การรันเว็บเซิร์ฟเวอร์ (Web Server Service) บัญชีที่ใช้สำหรับการรันบริการเว็บเซิร์ฟเวอร์ เช่น Apache หรือ IIS
- การสำรองข้อมูลอัตโนมัติ (Automated Backup Service) บัญชีที่ใช้สำหรับสคริปต์หรือโปรแกรมสำรองข้อมูลตามเวลาที่กำหนด
- การจัดการฐานข้อมูล (Database Management Service) บัญชีที่ใช้สำหรับการเชื่อมต่อและจัดการฐานข้อมูล เช่น MySQL หรือ SQL Server
- การประมวลผลงานตามเวลาที่กำหนด (Scheduled Tasks) บัญชีที่ใช้ในการรันงานที่ตั้งเวลาไว้ เช่น การอัปเดตซอฟต์แวร์อัตโนมัติ

แนวทางการจัดการบัญชีบริการอย่างปลอดภัย

- กำหนดสิทธิ์ขั้นต่ำ (Least Privilege) ให้สิทธิ์การเข้าถึงเฉพาะที่จำเป็นสำหรับการทำงานเท่านั้น
- กำหนดรหัสผ่านที่ปลอดภัย (Strong Passwords) ใช้รหัสผ่านที่ซับซ้อนและยากต่อการคาดเดา และเปลี่ยนรหัสผ่านเป็นระยะ
- เปิดใช้งานการยืนยันตัวตนหลายปัจจัย (Enable Multi-Factor Authentication: MFA) เพิ่มความปลอดภัยโดยใช้การยืนยันตัวตนหลายปัจจัยสำหรับบัญชีบริการที่สำคัญ
- บันทึกและตรวจสอบการใช้งาน (Logging and Monitoring) เปิดการบันทึกกิจกรรมของบัญชีบริการและตรวจสอบอย่างสม่ำเสมอ
- ไม่ใช้บัญชีร่วมกัน (Avoid Shared Accounts) หลีกเลี่ยงการใช้บัญชีบริการร่วมกัน เพื่อให้สามารถติดตามและระบุผู้ใช้งานได้อย่างชัดเจน
- การจัดการวงจรชีวิตบัญชี (Lifecycle Management) ปิดหรือลบบัญชีบริการที่ไม่ใช้งานเพื่อลดความเสี่ยงด้านความปลอดภัย
- การทบทวนบัญชีเป็นประจำ (Regular Reviews) ตรวจสอบบัญชีบริการเป็นระยะเพื่อให้แน่ใจว่ายังจำเป็นและใช้งานอย่างเหมาะสม

Services บริการ

บริการ (Services) หมายถึง โปรแกรมเฉพาะทางที่ทำงานเพื่อดำเนินการตามภารกิจสำคัญสำหรับระบบปฏิบัติการ โดยบริการเหล่านี้มักเริ่มทำงานพร้อมกับการบูตระบบปฏิบัติการ ทำงานอยู่เบื้องหลัง (Background Processes) และสามารถหยุดหรือเริ่มการทำงานใหม่ได้ตามการควบคุมของผู้ใช้

ลักษณะสำคัญของบริการ

- ทำงานอยู่เบื้องหลัง (Background Execution) บริการทำงานโดยไม่แสดงผลบนหน้าจอผู้ใช้โดยตรง และดำเนินการในเบื้องหลังเพื่อสนับสนุนการทำงานของระบบ
- เริ่มทำงานพร้อมระบบปฏิบัติการ (System Startup) บริการจำนวนมากถูกตั้งค่าให้เริ่มทำงานโดยอัตโนมัติเมื่อระบบปฏิบัติการบูตขึ้น
- ควบคุมได้โดยผู้ใช้ (User-Controlled) สามารถเริ่ม, หยุด, หรือรีสตาร์ทบริการได้ตามความต้องการผ่านเครื่องมือการจัดการระบบ
- ทำงานเฉพาะด้าน (Specialized Tasks) แต่ละบริการถูกออกแบบมาเพื่อทำงานเฉพาะ เช่น การจัดการเครือข่าย, การรักษาความปลอดภัย, หรือการจัดการผู้ใช้

ตัวอย่างของบริการ

- บริการจัดการเครือข่าย (Network Services) จัดการการสื่อสารระหว่างอุปกรณ์ในเครือข่าย เช่น DHCP, DNS, และไฟล์แชร์
- บริการจัดการผู้ใช้ (User Management Services) จัดการการยืนยันตัวตนและสิทธิ์ของผู้ใช้ เช่น Active Directory หรือ Local User Management
- บริการจัดการสิทธิ์ไฟล์ (File Permission Services) ควบคุมการเข้าถึงไฟล์และโฟลเดอร์ เช่น NTFS Permissions บน Windows
- บริการรักษาความปลอดภัย (Security Services) ให้การป้องกันไวรัส, การตรวจจับการบุกรุก เช่น Windows Defender หรือ Firewall
- บริการจัดการอุปกรณ์ (Device Interaction Services) จัดการการเชื่อมต่อและการทำงานของฮาร์ดแวร์ เช่น การจัดการเครื่องพิมพ์หรืออุปกรณ์จัดเก็บข้อมูล

การจัดการบริการในระบบปฏิบัติการ

- Windows Services จัดการผ่านเครื่องมือ Services.msc ตัวอย่าง: Windows Update, Print Spooler, Remote Desktop Services

- Linux Services จัดการผ่านคำสั่ง systemctl หรือ service ตัวอย่าง: sshd, cron, nginx, apache2
- macOS Services จัดการผ่าน launchctl หรือ System Preferences ตัวอย่าง: AirPort, File Sharing, Time Machine

แนวทางปฏิบัติที่ดีในการจัดการบริการ

- ปิดใช้งานบริการที่ไม่จำเป็น (Disable Unnecessary Services) ลดช่องโหว่และประหยัดทรัพยากรโดยปิดบริการที่ไม่ได้ใช้งาน
- อัปเดตบริการอย่างสม่ำเสมอ (Regular Updates) อัปเดตซอฟต์แวร์และบริการเพื่อปิดช่องโหว่ด้านความปลอดภัย
- ตรวจสอบการทำงานของบริการ (Monitor Services) ใช้เครื่องมือเพื่อตรวจสอบสถานะและประสิทธิภาพของบริการ
- จำกัดสิทธิ์การเข้าถึง (Limit Access Permissions) ให้สิทธิ์เฉพาะผู้ดูแลระบบในการจัดการบริการ

Service Provider ผู้ให้บริการ

ผู้ให้บริการ (Service Provider) หมายถึง หน่วยงานหรือองค์กรที่ให้บริการแพลตฟอร์ม, ซอฟต์แวร์, และบริการต่าง ๆ แก่องค์กรอื่น ๆ ซึ่งอาจรวมถึงบริการด้านไอที, การจัดการระบบ, หรือโซลูชันคลาวด์

ตัวอย่างผู้ให้บริการ

- ผู้รับเหมาด้านไอที (IT Contractors) ผู้เชี่ยวชาญด้านไอทีที่ให้บริการตามสัญญา เช่น การติดตั้งระบบเครือข่าย การพัฒนาซอฟต์แวร์
- ผู้ให้บริการจัดการระบบ (Managed Service Providers: MSPs) บริษัทที่ดูแลและจัดการโครงสร้างพื้นฐานด้านไอที เช่น การสำรองข้อมูล, การรักษาความปลอดภัยเครือข่าย
- ผู้ให้บริการคลาวด์ (Cloud Service Providers) บริษัทที่ให้บริการโซลูชันคลาวด์ เช่น Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS) ตัวอย่าง: Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP)
- ผู้ให้บริการซอฟต์แวร์ (Software Providers) บริษัทที่ให้บริการซอฟต์แวร์สำเร็จรูปหรือซอฟต์แวร์แบบกำหนดเอง
- ผู้ให้บริการศูนย์ข้อมูล (Datacenter Providers) ผู้ให้บริการพื้นที่จัดเก็บข้อมูลและการประมวลผลในศูนย์ข้อมูล

ประเภทของผู้ให้บริการ

- ผู้ให้บริการโครงสร้างพื้นฐาน (Infrastructure Providers) ให้บริการฮาร์ดแวร์, เซิร์ฟเวอร์, และการจัดการศูนย์ข้อมูล
- ผู้ให้บริการแพลตฟอร์ม (Platform Providers) ให้บริการแพลตฟอร์มสำหรับการพัฒนาและการใช้งานแอปพลิเคชัน
- ผู้ให้บริการซอฟต์แวร์ (Software Providers) ให้บริการซอฟต์แวร์ที่พร้อมใช้งาน เช่น ERP, CRM
- ผู้ให้บริการความปลอดภัย (Security Service Providers) ให้บริการด้านการรักษาความปลอดภัย เช่น การตรวจจับการบุกรุก, การจัดการความเสี่ยง

บทบาทของผู้ให้บริการในองค์กร

- สนับสนุนการทำงานด้านไอที (IT Support) ให้การสนับสนุนด้านเทคนิคและการจัดการระบบไอที
- เพิ่มประสิทธิภาพการทำงาน (Efficiency Improvement) ช่วยให้กระบวนการทำงานราบรื่นและลดภาระงานของทีมไอทีภายในองค์กร
- ลดต้นทุน (Cost Reduction) ลดค่าใช้จ่ายในการจ้างพนักงานประจำหรือการลงทุนในโครงสร้างพื้นฐาน
- เสริมความปลอดภัย (Enhanced Security) จัดการความปลอดภัยของข้อมูลและเครือข่ายอย่างมืออาชีพ
- การสำรองข้อมูลและกู้คืน (Backup and Recovery) ให้บริการสำรองข้อมูลและกู้คืนข้อมูลเมื่อเกิดเหตุฉุกเฉิน

ข้อควรพิจารณาในการเลือกผู้ให้บริการ

- ความน่าเชื่อถือ (Reliability) ตรวจสอบประวัติและชื่อเสียงของผู้ให้บริการ
- การรักษาความปลอดภัย (Security Practices) ผู้ให้บริการควรมีมาตรการรักษาความปลอดภัยที่เหมาะสม
- การปฏิบัติตามกฎระเบียบ (Compliance) ตรวจสอบว่าผู้ให้บริการปฏิบัติตามมาตรฐานและข้อบังคับ เช่น ISO 27001, GDPR
- ข้อตกลงการให้บริการ (Service Level Agreements: SLAs) กำหนดระดับการให้บริการและเงื่อนไขการรับประกัน
- การสนับสนุนลูกค้า (Customer Support) มีการให้บริการลูกค้าอย่างต่อเนื่องและมีประสิทธิภาพ

Social Engineering วิศวกรรมสังคม

วิศวกรรมสังคม (Social Engineering) หมายถึง กลยุทธ์ในการโจมตีทางไซเบอร์ที่ใช้ปฏิสัมพันธ์ระหว่างบุคคลบนแพลตฟอร์มต่าง ๆ เช่น อีเมล, โทรศัพท์, โซเชียลมีเดีย โดยอาศัยการชักจูงทางจิตวิทยาเพื่อหลอกล่อให้เหยื่อตัดสินใจผิดพลาดด้านความปลอดภัย หรือเปิดเผยข้อมูลที่เป็นความลับโดยไม่รู้ตัว

เป็นเทคนิคการโจมตีที่อาศัยความผิดพลาดของมนุษย์มากกว่าความล้มเหลวของเทคโนโลยี การตระหนักรู้, การฝึกอบรมอย่างต่อเนื่อง, และการมีมาตรการรักษาความปลอดภัยที่รัดกุม จะช่วยลดความเสี่ยงจากการถูกโจมตีด้วยวิศวกรรมสังคมได้อย่างมีประสิทธิภาพ.

ลักษณะสำคัญของวิศวกรรมสังคม

- การชักจูงทางจิตวิทยา (Psychological Manipulation) หลอกล่อให้เหยื่อทำตามความต้องการของผู้โจมตีโดยใช้จิตวิทยา
- การใช้ความน่าเชื่อถือ (Exploiting Trust) แอบอ้างเป็นบุคคลหรือองค์กรที่เหยื่อไว้ใจ เช่น เพื่อนร่วมงาน, ผู้ดูแลระบบ, หรือหน่วยงานราชการ
- การโจมตีผ่านช่องทางต่าง ๆ (Multi-Platform Attacks) ใช้ช่องทางหลากหลาย เช่น อีเมล, โทรศัพท์, โซเชียลมีเดีย, หรือการพบเจอในชีวิตจริง
- การหลอกลวงข้อมูล (Information Extraction) มีเป้าหมายเพื่อให้ได้ข้อมูลที่อ่อนไหว เช่น รหัสผ่าน, ข้อมูลการเงิน, หรือข้อมูลส่วนตัว

ตัวอย่างการโจมตีด้วยวิศวกรรมสังคม

- ฟิชชิง (Phishing) การส่งอีเมลหลอกลวงให้เหยื่อคลิกลิงก์ปลอมเพื่อขโมยข้อมูล
- วอทซ์ฟิชชิง (Vishing) การหลอกลวงผ่านทางโทรศัพท์ โดยแอบอ้างเป็นบุคคลที่น่าเชื่อถือ เช่น เจ้าหน้าที่ธนาคาร

- สเมชชิง (Smishing) การส่งข้อความ SMS หลอกลวงเพื่อให้เหยื่อคลิกลิงก์หรือเปิดเผยข้อมูลส่วนตัว
- พรีเท็กซ์ติ้ง (Pretexting) การสร้างเรื่องราวสมมติขึ้นมาเพื่อหลอกให้เหยื่อเปิดเผยข้อมูลที่เป็นความลับ
- เบทเทอร์ริ่ง (Baiting) การหลอกล่อให้เหยื่อดาวน์โหลดมัลแวร์ผ่านสิ่งของที่ดูน่าสนใจ เช่น แฟลชไดรฟ์ที่ถูกทิ้งไว้
- เทลเกทติ้ง (Tailgating) การตามบุคคลที่ได้รับอนุญาตเข้าไปในพื้นที่ปลอดภัย โดยไม่ต้องมีสิทธิ์เข้าด้วยตนเอง

ขั้นตอนการโจมตีด้วยวิศวกรรมสังคม

- การรวบรวมข้อมูล (Information Gathering) ผู้โจมตีศึกษาข้อมูลเกี่ยวกับเหยื่อจากแหล่งต่าง ๆ เช่น โซเชียลมีเดีย, เว็บไซต์บริษัท
- การสร้างความน่าเชื่อถือ (Building Trust) ผู้โจมตีแอบอ้างเป็นบุคคลที่เหยื่อไว้ใจเพื่อเพิ่มโอกาสสำเร็จในการโจมตี
- การหลอกล่อให้เกิดความผิดพลาด (Exploitation) หลอกล่อให้เหยื่อทำสิ่งที่ผิดพลาด เช่น คลิกลิงก์ปลอม, ให้ข้อมูลสำคัญ , หรือดาวน์โหลดไฟล์อันตราย
- การถอนตัว (Exit Strategy) ผู้โจมตีถอนตัวจากสถานการณ์หลังจากได้ข้อมูลที่ต้องการ โดยไม่ให้เหยื่อสงสัย

วิธีป้องกันการโจมตีด้วยวิศวกรรมสังคม

- การฝึกอบรมพนักงาน (Employee Training) ให้ความรู้และฝึกอบรมเกี่ยวกับวิธีการระบุและป้องกันการโจมตีทางวิศวกรรมสังคม
- การตรวจสอบแหล่งที่มา (Verify Sources) ตรวจสอบความถูกต้องของคำขอข้อมูลจากบุคคลหรือองค์กรที่น่าสงสัย
- การใช้การยืนยันตัวตนหลายปัจจัย (Multi-Factor Authentication: MFA) เพิ่มชั้นความปลอดภัยในการยืนยันตัวตน
- การไม่เปิดเผยข้อมูลส่วนตัว (Limit Personal Information Disclosure) หลีกเลี่ยงการให้ข้อมูลส่วนตัวหรือข้อมูลที่ละเอียดอ่อนผ่านช่องทางที่ไม่ปลอดภัย
- การรายงานเหตุการณ์ที่น่าสงสัย (Report Suspicious Activity) แจ้งทีมรักษาความปลอดภัยทันทีเมื่อพบความผิดปกติหรือการโจมตีที่สงสัยว่าเป็นการหลอกลวง
- การใช้ซอฟต์แวร์รักษาความปลอดภัย (Security Software) ติดตั้งซอฟต์แวร์ป้องกันไวรัสและมัลแวร์ที่มีประสิทธิภาพ

Software ซอฟต์แวร์

ซอฟต์แวร์ (Software) หมายถึง ชุดของข้อมูลและคำสั่งที่ใช้ในการควบคุมการทำงานของคอมพิวเตอร์เพื่อให้ดำเนินการตามภารกิจที่กำหนด ซอฟต์แวร์เป็นทรัพย์สินทางเทคโนโลยีที่ประกอบไปด้วยระบบปฏิบัติการและแอปพลิเคชัน ซึ่งอาจรวมถึงบริการ (Services), ไลบรารี (Libraries), และอินเทอร์เฟซโปรแกรมประยุกต์ (APIs)

ประเภทของซอฟต์แวร์

- ระบบปฏิบัติการ (Operating Systems) ซอฟต์แวร์ที่ทำหน้าที่จัดการทรัพยากรของคอมพิวเตอร์และเป็นพื้นฐานสำหรับการรันแอปพลิเคชันอื่น ๆ ตัวอย่าง: Windows, macOS, Linux, Android, iOS
- แอปพลิเคชัน (Applications) โปรแกรมที่ทำหน้าที่เฉพาะสำหรับผู้ใช้ เช่น การประมวลผลคำ, การจัดการฐานข้อมูล, หรือการท่องอินเทอร์เน็ต ตัวอย่าง: Microsoft Word, Google Chrome, Zoom
- ไลบรารี (Libraries) ชุดของโค้ดที่สามารถนำกลับมาใช้ซ้ำได้เพื่อช่วยในการพัฒนาซอฟต์แวร์ ตัวอย่าง: DLL (Dynamic Link Library) ใน Windows, .so ไฟล์ใน Linux
- บริการ (Services) โปรแกรมเฉพาะทางที่ทำงานในพื้นหลังเพื่อสนับสนุนการทำงานของระบบ ตัวอย่าง: Network Services, Security Services
- อินเทอร์เฟซโปรแกรมประยุกต์ (APIs) ชุดของกฎและอินเทอร์เฟซที่ช่วยให้ซอฟต์แวร์สามารถสื่อสารและทำงานร่วมกันได้ ตัวอย่าง: REST API, GraphQL API

บทบาทของซอฟต์แวร์ในองค์กร

- การจัดการงานและการดำเนินธุรกิจ (Business Operations) ช่วยให้การดำเนินงานต่าง ๆ เป็นไปอย่างมีประสิทธิภาพ เช่น ระบบบัญชี, ระบบการจัดการลูกค้า (CRM)
- การเพิ่มประสิทธิภาพการทำงาน (Productivity Enhancement) ซอฟต์แวร์ช่วยให้พนักงานทำงานได้เร็วขึ้น เช่น โปรแกรมประมวลผลคำ, โปรแกรมตารางคำนวณ
- การจัดการข้อมูล (Data Management) ซอฟต์แวร์ช่วยจัดเก็บ, วิเคราะห์, และประมวลผลข้อมูลปริมาณมาก เช่น ระบบฐานข้อมูล
- การรักษาความปลอดภัย (Security Management) ซอฟต์แวร์ป้องกันไวรัส, ระบบตรวจจับการบุกรุก และเครื่องมือการเข้ารหัสข้อมูล
- การทำงานร่วมกัน (Collaboration) ซอฟต์แวร์สำหรับการสื่อสารและการทำงานเป็นทีม เช่น โปรแกรมประชุมออนไลน์, ระบบแชร์ไฟล์

ความสำคัญของการจัดการซอฟต์แวร์

- การอัปเดตและแพตช์ความปลอดภัย (Security Updates and Patches) ป้องกันช่องโหว่ด้านความปลอดภัยโดยการติดตั้งอัปเดตเป็นประจำ
- การควบคุมสิทธิ์การใช้งาน (License Management) ตรวจสอบและจัดการสิทธิ์การใช้งานซอฟต์แวร์ให้ถูกต้องตามกฎหมาย
- การสำรองข้อมูล (Data Backup) สำรองข้อมูลที่สำคัญจากซอฟต์แวร์เพื่อป้องกันการสูญหาย
- การจัดการสินทรัพย์ซอฟต์แวร์ (Software Asset Management: SAM) การติดตามและควบคุมการใช้งานซอฟต์แวร์ในองค์กร

ข้อควรระวังในการใช้ซอฟต์แวร์

- ความเสี่ยงด้านความปลอดภัย (Security Risks) ซอฟต์แวร์ที่ไม่ได้อัปเดตอาจมีช่องโหว่ให้ถูกโจมตี
- การละเมิดลิขสิทธิ์ (License Violations) การใช้ซอฟต์แวร์ละเมิดลิขสิทธิ์อาจทำให้เกิดปัญหาทางกฎหมาย

- ซอฟต์แวร์ที่ไม่จำเป็น (Unnecessary Software) ซอฟต์แวร์ที่ไม่จำเป็นอาจทำให้ระบบทำงานช้าลงและเพิ่มความเสี่ยงด้านความปลอดภัย
- การติดมัลแวร์ (Malware Infections) ซอฟต์แวร์ที่ดาวน์โหลดจากแหล่งที่ไม่น่าเชื่อถืออาจมีมัลแวร์แฝงอยู่

Tailgating การลักลอบติดตาม

การลักลอบติดตาม (Tailgating) หมายถึง ปัญหาด้านความปลอดภัยทางกายภาพที่เกิดขึ้นเมื่อบุคคลหนึ่งแอบติดตามบุคคลอื่นเข้าไปในพื้นที่ปลอดภัย โดยไม่ได้ผ่านการยืนยันตัวตนหรือไม่ปฏิบัติตามมาตรการและขั้นตอนที่กำหนดไว้สำหรับการเข้า-ออกพื้นที่นั้น ๆ การลักลอบติดตาม (Tailgating) เป็นปัญหาความปลอดภัยทางกายภาพที่เกิดขึ้นจากการไม่ปฏิบัติตามมาตรการควบคุมการเข้า-ออกพื้นที่ การป้องกันและจัดการความเสี่ยงนี้ต้องอาศัยการใช้เทคโนโลยีควบคุมการเข้า-ออก, การเฝ้าระวังอย่างต่อเนื่อง, และการสร้างวัฒนธรรมความปลอดภัยในองค์กร เพื่อให้มั่นใจว่าพื้นที่ปลอดภัยได้รับการปกป้องอย่างเหมาะสม.

ลักษณะของการลักลอบติดตาม

- การผ่านเข้าโดยไม่ได้รับอนุญาต (Unauthorized Entry) บุคคลที่ไม่มีสิทธิ์ติดตามบุคคลที่ได้รับอนุญาตเข้าไปในพื้นที่ที่มีการควบคุม
- การไม่ยืนยันตัวตน (Lack of Authentication) ไม่มีการใช้บัตรผ่าน, การสแกนลายนิ้วมือ, หรือการยืนยันตัวตนอื่น ๆ ตามที่กำหนด
- การละเลยขั้นตอนการรักษาความปลอดภัย (Bypassing Security Protocols) ไม่ปฏิบัติตามขั้นตอนที่ออกแบบมาเพื่อควบคุมการเข้า-ออกพื้นที่

ตัวอย่างสถานการณ์การลักลอบติดตาม

- การตามคนผ่านประตู (Following Through Doors) บุคคลที่ไม่มีบัตรผ่านเดินตามพนักงานที่เปิดประตูด้วยบัตรผ่านของตนเอง
- การเข้าไปในลิฟต์ควบคุมพิเศษ (Restricted Elevators) บุคคลที่ไม่ได้รับอนุญาตแอบเข้าไปในลิฟต์ที่ต้องมีการยืนยันตัวตนเฉพาะ
- การตามคนผ่านประตูหมุน (Turnstiles) แอบตามหลังบุคคลที่ใช้ประตูหมุนเพื่อเข้าไปในพื้นที่ควบคุม

มาตรการป้องกันการลักลอบติดตาม

- การติดตั้งระบบควบคุมการเข้า-ออก (Access Control Systems) ใช้ระบบควบคุมการเข้า-ออก เช่น บัตร RFID, การสแกนลายนิ้วมือ, และการจดจำใบหน้า
- การใช้ประตูล็อกอัตโนมัติ (Man-Trap Doors) ประตูที่ล็อกอัตโนมัติและอนุญาตให้บุคคลผ่านได้ครั้งละหนึ่งคน
- การฝึกอบรมพนักงาน (Employee Training) ให้ความรู้พนักงานเกี่ยวกับความเสี่ยงจากการลักลอบติดตามและวิธีการป้องกัน
- การเฝ้าระวังและตรวจสอบ (Surveillance and Monitoring) ใช้กล้องวงจรปิด (CCTV) และการตรวจตราจากเจ้าหน้าที่รักษาความปลอดภัย
- การรายงานเหตุการณ์ที่น่าสงสัย (Incident Reporting) ส่งเสริมให้พนักงานรายงานเมื่อพบเห็นพฤติกรรมที่น่าสงสัย
- การใช้ระบบเตือนภัย (Alarm Systems) ติดตั้งระบบเตือนภัยเมื่อมีการพยายามผ่านเข้าโดยไม่ได้รับอนุญาต

Third-Party Provider ผู้ให้บริการบุคคลที่สาม

ผู้ให้บริการบุคคลที่สาม (Third-Party Provider) หมายถึงหน่วยงานหรือองค์กรภายนอกที่ให้บริการแพลตฟอร์ม, ซอฟต์แวร์, โครงสร้างพื้นฐาน, หรือบริการอื่น ๆ แก่องค์กรที่ใช้บริการ โดยผู้ให้บริการบุคคลที่สามมีบทบาทเหมือนกับ ผู้ให้บริการ (Service Provider)

Users ผู้ใช้

ผู้ใช้ (Users) หมายถึง พนักงาน, ผู้ให้บริการบุคคลที่สาม, ผู้รับเหมา, ผู้ให้บริการ, ที่ปรึกษา, หรือบุคคลอื่น ๆ ที่ได้รับอนุญาตให้เข้าถึงทรัพยากรขององค์กร นอกจากนี้ยังครอบคลุมถึงบัญชีผู้ใช้ (User Accounts), บัญชีผู้ดูแลระบบ (Administrator Accounts), และบัญชีบริการ (Service Accounts) อีกด้วย

User Accounts บัญชีผู้ใช้

บัญชีผู้ใช้ (User Accounts) หมายถึง ชุดข้อมูลระบุตัวตนที่ประกอบด้วยข้อมูลรับรอง เช่น ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ซึ่งใช้เพื่อยืนยันตัวตนของผู้ใช้ในระบบคอมพิวเตอร์หรือเครือข่าย บัญชีผู้ใช้ช่วยจัดเก็บข้อมูลและการตั้งค่าของผู้ใช้ ควบคุมการเข้าถึงไฟล์, โฟลเดอร์, ทรัพยากร และกำหนดสิทธิ์ในการปฏิบัติงานต่าง ๆ

บัญชีผู้ใช้ (User Accounts) เป็นองค์ประกอบสำคัญในการจัดการสิทธิ์และการรักษาความปลอดภัยในระบบ การใช้บัญชีผู้ใช้อย่างเหมาะสมและปฏิบัติตามแนวทางความปลอดภัย จะช่วยปกป้องข้อมูลและทรัพยากรขององค์กรได้อย่างมีประสิทธิภาพ.

ลักษณะสำคัญของบัญชีผู้ใช้

- ข้อมูลรับรอง (Credentials) ประกอบด้วยชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อยืนยันตัวตน
- การตั้งค่าส่วนบุคคล (User Settings) จัดเก็บการตั้งค่าเฉพาะบุคคล เช่น ธีม, ภาษาที่ใช้, และการตั้งค่าโปรแกรม
- การควบคุมการเข้าถึง (Access Control) กำหนดสิทธิ์การเข้าถึงไฟล์, โฟลเดอร์, และทรัพยากรต่าง ๆ ตามบทบาทของผู้ใช้
- สิทธิ์จำกัด (Limited Privileges) บัญชีผู้ใช้มาตรฐานมีสิทธิ์จำกัด เหมาะสำหรับการทำงานทั่วไป เช่น การใช้งานซอฟต์แวร์และการเข้าถึงข้อมูลที่ไม่ละเอียดอ่อน
- ติดตามกิจกรรม (Activity Tracking) ระบบสามารถบันทึกกิจกรรมที่ดำเนินการโดยบัญชีผู้ใช้ เพื่อการตรวจสอบและรักษาความปลอดภัย

แนวทางปฏิบัติที่ดีในการจัดการบัญชีผู้ใช้

- การใช้รหัสผ่านที่แข็งแรง (Strong Passwords) ใช้รหัสผ่านที่ซับซ้อนและเปลี่ยนรหัสผ่านเป็นระยะ
- การเปิดใช้งานการยืนยันตัวตนหลายปัจจัย (Multi-Factor Authentication: MFA) เพิ่มความปลอดภัยในการยืนยันตัวตน
- การจำกัดสิทธิ์ (Least Privilege) ให้สิทธิ์เฉพาะที่จำเป็นสำหรับการทำงานเท่านั้น
- การปิดบัญชีที่ไม่ใช้งาน (Disable Inactive Accounts) ปิดบัญชีที่ไม่ได้ใช้งานเกิน 30-45 วัน เพื่อลดความเสี่ยง

- การตรวจสอบกิจกรรม (Audit and Monitoring) ตรวจสอบกิจกรรมของบัญชีผู้ใช้อย่างสม่ำเสมอ

Virtual Environment สภาพแวดล้อมเสมือน

สภาพแวดล้อมเสมือน (Virtual Environment) หมายถึง การจำลองฮาร์ดแวร์เพื่อให้ซอฟต์แวร์สามารถทำงานได้โดยไม่ต้องใช้ฮาร์ดแวร์จริงจำนวนมาก สภาพแวดล้อมเสมือนช่วยให้ทรัพยากรจำนวนเล็กน้อยสามารถทำงานเสมือนเป็นทรัพยากรจำนวนมาก โดยมีความสามารถในการประมวลผล, หน่วยความจำ, การจัดเก็บข้อมูล, และเครือข่ายที่เพียงพอ

ลักษณะสำคัญของสภาพแวดล้อมเสมือน

- การจำลองฮาร์ดแวร์ (Hardware Simulation) จำลองทรัพยากรฮาร์ดแวร์ เช่น CPU, RAM, และพื้นที่จัดเก็บข้อมูลเพื่อให้ระบบปฏิบัติการและแอปพลิเคชันทำงานได้
- การแบ่งปันทรัพยากร (Resource Pooling) ใช้ทรัพยากรร่วมกันเพื่อเพิ่มประสิทธิภาพ เช่น เซิร์ฟเวอร์เดียวสามารถโฮสต์หลาย ๆ เครื่องเสมือน (VM)
- การขยายตัวอย่างยืดหยุ่น (Scalability) สามารถเพิ่มหรือลดขนาดของทรัพยากรตามความต้องการ
- ประสิทธิภาพการใช้ทรัพยากร (Resource Efficiency) ลดความจำเป็นในการใช้ฮาร์ดแวร์จริงจำนวนมาก ช่วยประหยัดค่าใช้จ่ายและพื้นที่
- การแยกสภาพแวดล้อม (Isolation) เครื่องเสมือนแต่ละเครื่องทำงานแยกจากกัน ช่วยเพิ่มความปลอดภัยและความยืดหยุ่น

ประเภทของสภาพแวดล้อมเสมือน

- การจำลองเซิร์ฟเวอร์ (Server Virtualization) แบ่งเซิร์ฟเวอร์กายภาพให้เป็นเซิร์ฟเวอร์เสมือนหลายเครื่อง ตัวอย่าง: VMware vSphere, Microsoft Hyper-V, Citrix Hypervisor
- การจำลองเดสก์ท็อป (Desktop Virtualization) ให้ผู้ใช้เข้าถึงเดสก์ท็อปเสมือนจากอุปกรณ์ต่าง ๆ ตัวอย่าง: VMware Horizon, Citrix Virtual Apps and Desktops
- การจำลองเครือข่าย (Network Virtualization) จำลองเครือข่ายเพื่อจัดการการเชื่อมต่อและการรักษาความปลอดภัย ตัวอย่าง: Cisco ACI, VMware NSX
- การจำลองพื้นที่จัดเก็บข้อมูล (Storage Virtualization) รวมพื้นที่จัดเก็บข้อมูลจากหลายแหล่งให้เป็นระบบเดียว ตัวอย่าง: VMware vSAN, Dell EMC VPLEX
- การจำลองแอปพลิเคชัน (Application Virtualization) รันแอปพลิเคชันในสภาพแวดล้อมเสมือนโดยไม่ต้องติดตั้งบนเครื่องจริง ตัวอย่าง: Microsoft App-V, Citrix Virtual Apps

บทบาทของสภาพแวดล้อมเสมือนในคลาวด์คอมพิวติ้ง

- พื้นฐานของคลาวด์ (Foundation of Cloud Computing) การจำลองเสมือนช่วยให้คลาวด์สามารถให้บริการ Infrastructure as a Service (IaaS), Platform as a Service (PaaS), และ Software as a Service (SaaS)
- การขยายทรัพยากรแบบไดนามิก (Dynamic Resource Scaling) สามารถขยายหรือลดทรัพยากรได้ตามความต้องการของผู้ใช้
- การสำรองและกู้คืนข้อมูล (Backup and Disaster Recovery) ทำให้สามารถกู้คืนข้อมูลและระบบได้รวดเร็วเมื่อเกิดเหตุฉุกเฉิน
- การทดสอบและพัฒนา (Testing and Development) ช่วยให้สามารถสร้างและทดสอบแอปพลิเคชันในสภาพแวดล้อมที่หลากหลายโดยไม่ต้องใช้ฮาร์ดแวร์จริง

ประโยชน์ของสภาพแวดล้อมเสมือน

- ลดต้นทุน (Cost Reduction) ลดค่าใช้จ่ายในการซื้อและบำรุงรักษาฮาร์ดแวร์
- เพิ่มความยืดหยุ่น (Flexibility) สามารถปรับแต่งและจัดสรรทรัพยากรได้ตามความต้องการ
- การกู้คืนระบบรวดเร็ว (Rapid Recovery) สามารถกู้คืนระบบได้อย่างรวดเร็วเมื่อเกิดปัญหา
- การจัดการง่ายขึ้น (Simplified Management) บริหารจัดการทรัพยากรและระบบได้ง่ายผ่านเครื่องมือควบคุมแบบรวมศูนย์

ข้อควรระวังในการใช้สภาพแวดล้อมเสมือน

- ประสิทธิภาพลดลง (Performance Overhead) การจำลองเสมือนอาจทำให้เกิดความหน่วง (Latency) หากทรัพยากรถูกใช้งานเกินขีดจำกัด
- ความปลอดภัย (Security Risks) การจัดการเครื่องเสมือนที่ไม่เหมาะสมอาจทำให้เกิดความเสี่ยงด้านความปลอดภัย
- การจัดการซับซ้อน (Complex Management) การจัดการสภาพแวดล้อมเสมือนจำนวนมากอาจซับซ้อนและต้องการทักษะเฉพาะ

Workforce พนักงานและบุคลากร

พนักงานและบุคลากร (Workforce) หมายถึง บุคคลทั้งหมดที่ได้รับการว่าจ้างหรือมีส่วนร่วมกับองค์กร และมีสิทธิ์เข้าถึงระบบสารสนเทศ, ทรัพยากร, หรือทรัพย์สินขององค์กร ซึ่งรวมถึงพนักงานที่ทำงานในสถานที่ปฏิบัติงาน (On-Site) และพนักงานที่ทำงานทางไกล (Remote) โดยไม่นับรวมผู้ให้บริการ (Service Providers) และผู้รับเหมา (Contractors)

ศูนย์ความปลอดภัยทางอินเทอร์เน็ต (Center for Internet Security, Inc. - CIS®)

CIS® เป็นองค์กรไม่แสวงหาผลกำไรที่ขับเคลื่อนโดยชุมชน มีพันธกิจในการทำให้โลกออนไลน์ปลอดภัยยิ่งขึ้นสำหรับผู้คน ธุรกิจ และรัฐบาล ด้วยความเชี่ยวชาญหลักในด้าน **ความร่วมมือ** และ **นวัตกรรม**

ภารกิจของ CIS®:

- **CIS Critical Security Controls® และ CIS Benchmarks™:**
  แนวปฏิบัติที่ได้รับการยอมรับในระดับสากลสำหรับการรักษาความปลอดภัยของระบบ IT และข้อมูล
- เป็นผู้นำชุมชนผู้เชี่ยวชาญด้าน IT ระดับโลกในการพัฒนามาตรฐานความปลอดภัยให้ทันสมัยและสอดคล้องกับภัยคุกคามใหม่ๆ
- **CIS Hardened Images®:**
  บริการสภาพแวดล้อมการประมวลผลบนคลาวด์ที่ปลอดภัย พร้อมปรับขนาดได้ตามความต้องการ

ศูนย์ข้อมูลและการแบ่งปันข้อมูล:

- **Multi-State Information Sharing and Analysis Center® (MS-ISAC®):**
  แหล่งข้อมูลที่เชื่อถือได้สำหรับการป้องกัน การตอบสนอง และการฟื้นฟูภัยคุกคามทางไซเบอร์สำหรับหน่วยงานรัฐในสหรัฐฯ รวมถึงรัฐบาลท้องถิ่น ชนเผ่า และดินแดน
- **Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC®):**
  สนับสนุนความต้องการด้านความปลอดภัยทางไซเบอร์ที่เปลี่ยนแปลงอย่างรวดเร็วของสำนักงานการเลือกตั้งในสหรัฐฯ

เรียนรู้เพิ่มเติม:

- เยี่ยมชมเว็บไซต์: CISecurity.org
- ติดตามบน Twitter: @CISecurity

CIS® มุ่งมั่นในการเป็นผู้นำด้านความปลอดภัยไซเบอร์ ด้วยการสนับสนุนชุมชนโลกในการป้องกันภัยคุกคามที่กำลังเกิดขึ้น และสร้างความปลอดภัยในโลกออนไลน์สำหรับทุกคน.