หลักสูตร

การบริหารจัดการความมั่นคงปลอดภัยสารสนเทศในระดับองค์กร

Information Security Management for Enterprise

ส่วนที่ 1
แนะนำหลักสูตร

หลักการเหตุผลความจำเป็น

ปี 2024 แนวโน้มความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity) ทั้งในระดับโลกและในประเทศไทยกำลังเผชิญกับความท้าทายที่เพิ่มขึ้นอย่างต่อเนื่อง โดย World Economic Forum คาดการณ์ว่ามูลค่าความเสียหายจากการถูกโจมตีทางไซเบอร์ทั่วโลกจะสูงถึง 8 ล้านล้านดอลลาร์สหรัฐฯ ในปี 2566 สำหรับประเทศไทย ประสบกับการโจมตีทางเว็บไซต์เพิ่มขึ้นมากถึง 40-60% ของเหตุการณ์ทั้งหมด ส่งผลให้องค์กรไทยต้องเร่งยกระดับความมั่นคงปลอดภัยทางไซเบอร์ของตนเอง

โดยองค์กรต้องเตรียมตัวรับมือ และปรับตัวเข้ากับแนวโน้มด้านความมั่นคงปลอดภัยทางไซเบอร์ตามแนวทางการปฏิบัติ 3 ด้าน ดังนี้ 1) ด้านกลยุทธ์องค์กร (Organization Strategy) ควรออกแบบแนวทางปฏิบัติด้านความมั่นคงปลอดภัยทางไซเบอร์โดยคำนึงถึงผู้ใช้งานเป็นศูนย์กลาง (Human-Centric) เพื่อลดความขัดแย้งระหว่างความปลอดภัยและการใช้งาน และส่งเสริมให้พนักงานทุกระดับมีส่วนร่วมในการรักษาความปลอดภัยขององค์กร 2) ด้านเทคโนโลยี (Technology) ควรนำ AI และ Machine Learning รวมถึงเครื่องมือตรวจสอบและป้องกันการโจมตีบน Cloud และ IoT มาช่วยในการตรวจจับและป้องกันภัยคุกคาม 3) บทบาทและความรับผิดชอบ (Role & Responsibility) องค์กรควรปรับเปลี่ยนบทบาทของ CISO จากเดิมที่เน้นการควบคุมและบังคับใช้มาตรการความปลอดภัย มาเป็นผู้ให้คำปรึกษาและสนับสนุน (Facilitator) รวมถึงให้คำแนะนำในการใช้เทคโนโลยีอย่างปลอดภัยและมีประสิทธิภาพ อีกทั้งควรมีการจัดให้มีการฝึกอบรมและกิจกรรมเสริมสร้างความตระหนักรู้เกี่ยวกับภัยคุกคามรูปแบบต่าง ๆ เพื่อให้พนักงานสามารถรับมือกับภัยคุกคามที่เปลี่ยนแปลงไปได้อย่างทันท่วงทีและมีประสิทธิภาพ

หลักสูตรการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศในระดับองค์กร จัดทำขึ้นเพื่อพัฒนา และยกระดับทักษะด้านการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศให้แก่บุคลากรในสายอาชีพ หรือผู้ที่มีความสนใจในเรื่องของความมั่นคงปลอดภัยสารสนเทศและไซเบอร์ เพื่อสามารถบริหารจัดการความมั่นคงปลอดภัยในการใช้เทคโนโลยีประกอบการทำงานในองค์กร รวมถึงมีความรู้และความสามารถในการจัดการรับมือภัยคุกคามทางสารสนเทศและไซเบอร์ที่อาจเกิดขึ้นในองค์กรได้อย่างรวดเร็ว ถูกต้อง ปลอดภัย และมีประสิทธิภาพ

คำอธิบายหลักสูตรโดยสังเขป

หลักสูตร “การบริหารจัดการความมั่นคงปลอดภัยสารสนเทศในระดับองค์กร” นี้ถูกออกแบบมาเพื่อเพิ่มพูนความรู้และทักษะในการบริหารจัดการความมั่นคงปลอดภัยทางไซเบอร์ โดยเน้นการทำความเข้าใจหลักการพื้นฐานของการจัดการความมั่นคงปลอดภัยสารสนเทศ การวิเคราะห์และประเมินความเสี่ยง การพัฒนานโยบายความปลอดภัย การตอบสนองต่อเหตุการณ์ภัยคุกคาม และการกู้คืนระบบหลังเกิดเหตุ โดยผู้เข้าร่วมหลักสูตรจะได้เรียนรู้ทั้งในภาคทฤษฎีและการปฏิบัติ ผ่านกรณีศึกษาจริงและกิจกรรมเชิงปฏิบัติการ เพื่อตอบสนองต่อความต้องการขององค์กรในการเสริมสร้างความมั่นคงปลอดภัยสารสนเทศอย่างมีประสิทธิภาพในยุคดิจิทัลที่ท้าทายมากขึ้น

กลุ่มเป้าหมาย

ผู้เข้ารับการพัฒนาทักษะ

01

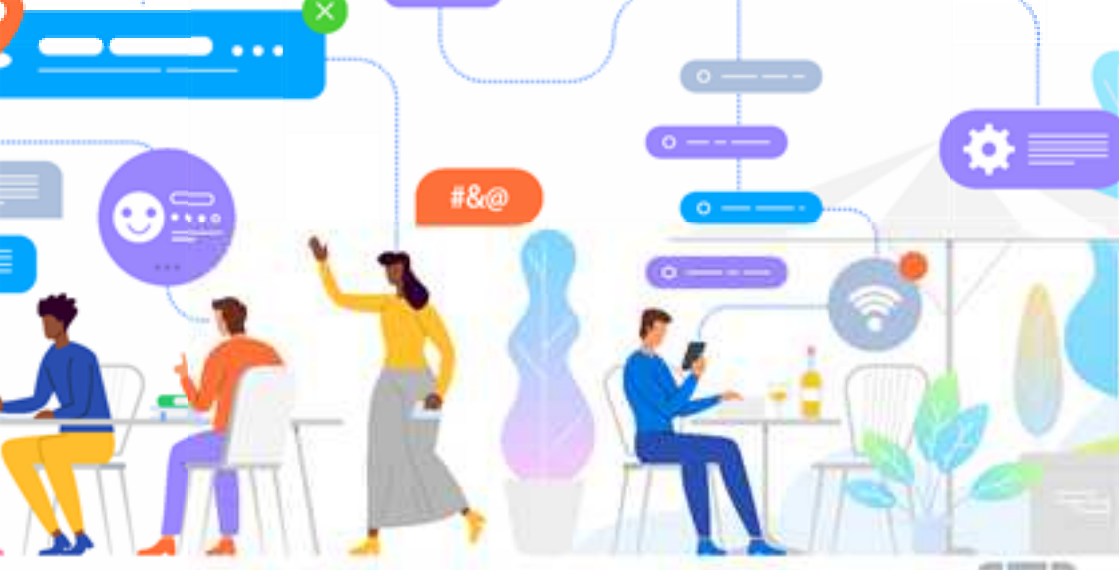
ผู้ปฏิบัติงานด้านความมั่นคงปลอดภัยสารสนเทศ
อาทิ นักบริหารจัดการความมั่นคงปลอดภัยข้อมูล (CISO),
ผู้จัดการ IT, นักจัดการข้อมูลส่วนบุคคล

02

แรงงานอิสระ/แรงงานทั่วไปที่มีความสนใจ
ด้านการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

ความรู้ขั้นพื้นฐาน ที่ผู้เข้ารับการพัฒนาทักษะต้องมี

1. มีประสบการณ์การทำงาน หรือมีความต้องการประกอบอาชีพที่เกี่ยวข้องกับหลักสูตรี
2. เป็นผู้ปฏิบัติงานในตำแหน่งการบริหารจัดการ การกำกับดูแลระบบเทคโนโลยีสารสนเทศ (IT) หรือที่เกี่ยวข้องอย่างน้อย 1 ปี
3. ผ่านการอบรมจากหลักสูตร Cybersecurity and Network Protection, Basic Cybersecurity หรือหลักสูตรความมั่นคงปลอดภัยทางไซเบอร์อื่น ๆ ของ DSD Online



คุณสมบัติของวิทยากร

1. มีประสบการณ์ในสายงานด้านการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศหรือไซเบอร์
2. มีความรู้ลึกซึ้งเกี่ยวกับมาตรฐานและแนวปฏิบัติที่เกี่ยวข้อง เช่น NIST Cybersecurity Framework, ISO/IEC 27001 และกฎหมายที่เกี่ยวข้อง
3. มีทักษะการใช้เครื่องมือที่เกี่ยวข้องกับการบริหารจัดการความเสี่ยงทางไซเบอร์ เช่น การวิเคราะห์ภัยคุกคาม การตอบสนองต่อเหตุการณ์ และการฟื้นฟูระบบ

รูปแบบการพัฒนาทักษะที่สามารถใช้ในการพัฒนาทักษะ

การเรียนอิเล็กทรอนิกส์ (e-Learning)

การพัฒนาทักษะเชิงปฏิบัติการ (Workshop)

การพัฒนาทักษะผ่านระบบ Webinar

ส่วนที่ 2
รายละเอียดหลักสูตร

วัตถุประสงค์

เพื่อให้ผู้รับการพัฒนาทักษะมีความรู้ ทักษะ และมีทัศนคติที่ดีในการปฏิบัติงานด้านการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ โดยสามารถ

1. **ทำความเข้าใจหลักการพื้นฐาน** ของการจัดการความมั่นคงปลอดภัยสารสนเทศ
2. **พัฒนาและดำเนินการนโยบายและขั้นตอน** การบริหารจัดการความมั่นคงปลอดภัยสารสนเทศอย่างมีประสิทธิภาพ
3. **ประเมินและลดความเสี่ยง** ด้านความมั่นคงปลอดภัยสารสนเทศ
4. **สร้างและรักษากรอบการกำกับดูแล** บริหารจัดการความมั่นคงปลอดภัยสารสนเทศได้อย่างมีประสิทธิภาพ
5. **ดำเนินการและจัดการปฏิบัติตามมาตรฐาน** การจัดการความมั่นคงปลอดภัยสารสนเทศ
6. **ประยุกต์ใช้ทักษะจากการอบรม** ในการปฏิบัติงานผ่านสถานการณ์และตัวอย่างจากกรณีศึกษาจริง

ระยะเวลาการพัฒนาทักษะ

ผู้รับการพัฒนาทักษะจะต้องฝึกภาคทฤษฎีด้วยตนเองบนระบบการฝึกทักษะออนไลน์ของกรมพัฒนาฝีมือแรงงาน **โดยมีระยะเวลาการพัฒนาทักษะทั้งหมด 10 ชั่วโมง**

คุณสมบัติของผู้รับการพัฒนาทักษะ

1. มีประสบการณ์การทำงาน หรือมีความต้องการประกอบอาชีพที่เกี่ยวข้องกับหลักสูตร
2. มีอายุตั้งแต่ 15 ปี ขึ้นไป
3. มีความรู้ไม่ต่ำกว่าระดับประกาศนียบัตรวิชาชีพ (ปวช.)
4. ผ่านการอบรมจากหลักสูตร Basic Cybersecurity หรือหลักสูตรความมั่นคงปลอดภัยทางไซเบอร์อื่น ๆ จากระบบการฝึกทักษะออนไลน์ของกรมพัฒนาฝีมือแรงงาน
5. กรณีผู้เข้ารับการพัฒนาทักษะเป็นแรงงานในสถานประกอบกิจการต้องเป็นผู้ปฏิบัติงานในตำแหน่งการบริหารจัดการ การกำกับดูแลระบบเทคโนโลยีสารสนเทศ (IT) หรือที่เกี่ยวข้องอย่างน้อย 1 ปี

วุฒิบัตร

ผู้เข้ารับการพัฒนาทักษะจะต้องฝึกอบรมภาคทฤษฎีบนระบบการฝึกทักษะออนไลน์ของกรมพัฒนาฝีมือแรงงาน และผ่านการประเมินผลตามเกณฑ์ไม่น้อยกว่าร้อยละ 70 จะได้รับวุฒิบัตรจากกรมพัฒนาฝีมือแรงงาน

หัวข้อวิชา

โมดูล	หัวข้อวิชา	ชั่วโมง
1	บทนำการบริหารจัดการความเสี่ยงทางสารสนเทศ และการระบุความเสี่ยง	2.30
2	การป้องกันสารสนเทศและการสร้างความตระหนักรู้ ด้านความปลอดภัยสารสนเทศ	1.45
3	การตรวจจับภัยคุกคามและเหตุการณ์ด้านความมั่นคงปลอดภัย สารสนเทศ	1.45
4	การตอบสนองต่อเหตุการณ์ภัยคุกคามทางสารสนเทศ	1.30
5	การกู้คืนทางสารสนเทศหลังเกิดเหตุการณ์ด้านความมั่นคงปลอดภัย	0.30
6	การกำกับดูแลความมั่นคงปลอดภัยสารสนเทศ	2
รวม (ชั่วโมง)		10

หมายเหตุ: ทั้งนี้ กรณีที่ผู้ประกอบกิจการตามพระราชบัญญัติส่งเสริมการพัฒนาฝีมือแรงงาน พ.ศ. 2545 ส่งลูกจ้างของตนเข้ารับการฝึกอบรมหรือจัดฝึกอบรมให้กับลูกจ้างของตน ตามคุณสมบัติของผู้รับการฝึกถือเป็นการฝึกตามพระราชบัญญัติส่งเสริมการพัฒนาฝีมือแรงงาน พ.ศ. 2545

สารบัญ

Chapter 3: แนวทางการวิเคราะห์และการจัดการความเสี่ยง

- วิธีการประเมินความเสี่ยงเชิงคุณภาพ และเชิงปริมาณ
  - การประเมินความเสี่ยงเชิงคุณภาพ (Qualitative Risk Assessment)
  - การประเมินความเสี่ยงเชิงปริมาณ (Quantitative Risk Assessment)
- กระบวนการวิเคราะห์ความเสี่ยง (Risk Analysis) เช่น การระบุสินทรัพย์และภัยคุกคาม การประเมินช่องโหว่ การประเมินความเสี่ยง การจัดลำดับความเสี่ยง
- การประเมินความเสี่ยงโดยใช้เมทริกซ์ความเสี่ยง (Risk Matrix) เช่น วิธีการประเมินความเสี่ยงโดยใช้เมทริกซ์ความเสี่ยง ข้อควรระวัง
- การบริหารจัดการความเสี่ยง (Risk Management) เช่น แนวคิดการจัดการความเสี่ยงทางสารสนเทศกระบวนการ/วิธีการจัดการความเสี่ยง
- การติดตาม ทบทวน และปรับปรุงกระบวนการจัดการความเสี่ยง (Risk Monitoring, Review and Improvement)

MODULE 2

การป้องกันสารสนเทศและการสร้างความตระหนักรู้ด้านความปลอดภัยสารสนเทศ (Information Security Protection and Awareness)

MODULE 3 การตรวจจับภัยคุกคามและเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Threat and Incident Detection)

Chapter 6: การระบุภัยคุกคามและการประเมินช่องโหว่ 125

- ประเภทของภัยคุกคามทางไซเบอร์ (Cyber Threat) เช่น มัลแวร์ (Malware) ฟิชชิ่ง (Phishing), แรนซัมแวร์ (Ransomware) วิศวกรรมสังคม (Social Engineering)
- ตัวอย่างการโจมตีทางไซเบอร์ที่เกิดขึ้นจริงในภาคอุตสาหกรรม
- ภัยคุกคามจากภายใน (Insider Threat)
- ความเสี่ยงด้านความปลอดภัยบนคลาวด์ (Cloud Security)
- เทคโนโลยีใหม่ ๆ เช่น IoT และ AI ที่อาจเป็นช่องโหว่ของระบบ
- วิธีการระบุภัยคุกคาม
- ทำความรู้จักข้อมูลเบื้องต้นของระบบการสแกนช่องโหว่ (Vulnerability Scanner) แบ่งออกเป็น Open Source เช่น OpenVAS, Nikto, Kali Linux, Nmap, Metasploit และแบบ Commercial เช่น QualysGuard และ Nessus
- วิธีการประเมินช่องโหว่ (Vulnerability Assessment) เช่น การสแกนช่องโหว่ การทดสอบการเจาะระบบ การตรวจสอบช่องโหว่ด้วยตนเอง การตรวจสอบโค้ด
- การทดสอบการเจาะระบบ (Penetration Testing) เช่น ความสามารถของระบบในการต้านการโจมตี ประเภทของการทดสอบการเจาะระบบ ขั้นตอนการทดสอบการเจาะระบบ การจำลองการโจมตีระบบเพื่อทดสอบประสิทธิภาพของมาตรการรักษาความปลอดภัย
- ค่า CVE และ CVSS

Chapter 7: การตรวจสอบทรัพย์สินสารสนเทศ 176

- การตรวจสอบทรัพย์สินสารสนเทศ
- ความสำคัญของการตรวจสอบทรัพย์สินสารสนเทศ
- วิธีการตรวจสอบอย่างต่อเนื่อง เช่น การตรวจสอบระบบ การตรวจสอบแอปพลิเคชัน การตรวจสอบเครือข่าย การตรวจสอบบล็อก และการตรวจสอบโดยใช้เครื่องมือ

MODULE 4

การตอบสนองต่อเหตุการณ์คุกคามทางสารสนเทศ (Information Security Incident Response)

Chapter 8: การตอบสนองต่อเหตุการณ์ 184

- กระบวนการและขั้นตอนการตอบสนองต่อเหตุการณ์ (Incident Response)
- การทำ Log Management
- การใช้ระบบในการตอบสนองและรับมือต่อเหตุการณ์
  - ระบบ SIEM กับการตอบสนองและรับมือต่อเหตุการณ์
  - ระบบ SOAR กับการตอบสนองและรับมือต่อเหตุการณ์
  - ระบบ XDR กับการตอบสนองและรับมือต่อเหตุการณ์
  - ขั้นตอนการทำ Incident Response
- กรณีศึกษา: การจำลองสถานการณ์การโจมตีด้วย Ransomware และการฝึกซ้อมแผน Incident Response
- การทำDigital Forensics ในการสืบสวนเหตุการณ์

MODULE 5

การกู้คืนทางสารสนเทศหลังเกิดเหตุการณ์ด้านความมั่นคงปลอดภัย (Information Security Incident Recovery)

Chapter 9: การกู้คืนทรัพย์สินและการดำเนินงาน 213

- จุดประสงค์และปัจจัยการกู้คืนทรัพย์สินในระบบสารสนเทศ
- ระยะของการกู้คืนระบบ (Disaster Recovery Phases)
- แผนฟื้นฟูภัยพิบัติ/แผนการกู้คืนจากภัยคุกคามทางไซเบอร์ (Disaster Recovery Plan - DRP)
- การสำรองข้อมูล (Backup)
  - ประเภทการสำรองข้อมูล
  - กลยุทธ์การสำรองข้อมูล
  - แนวทางปฏิบัติการสำรองข้อมูล
- แหล่งกู้คืนภัยพิบัติ (Disaster Recovery Sites)
- แผนการสื่อสารช่วงกู้คืนภัยพิบัติ (Disaster Recovery Communication Plan)

MODULE **6**

การกำกับดูแลความมั่นคงปลอดภัยสารสนเทศ (Information Security Governance)

MODULE 01

บทนำการบริหารจัดการความเสี่ยงทางสารสนเทศและการระบุความเสี่ยง

(Foundation of Information Security Management and Risk Identify)
#Identify

วัตถุประสงค์

เพื่อให้ผู้เข้ารับการพัฒนาทักษะมีความรู้ความเข้าใจเกี่ยวกับหลักการพื้นฐานของการจัดการความมั่นคงปลอดภัยสารสนเทศ แนวคิดและมาตรฐานที่เกี่ยวข้อง ภัยคุกคามและแนวโน้ม กฎหมายและข้อบังคับต่าง ๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศในประเทศไทยและต่างประเทศ โดยสามารถนำความรู้จากบทเรียนไปประยุกต์ใช้ในการออกแบบนโยบายการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

CHAPTER 1 ความรู้พื้นฐานและกฎหมายที่เกี่ยวข้องกับการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

ความหมายของ Information Security Management (ISM):

Information Security Management คืออะไร

ความหมาย

ข้อมูลเป็นสินทรัพย์สำคัญ ที่ต้องดูแลบำรุงรักษาและป้องกันอย่างดี โดยการจัดการความปลอดภัยของข้อมูล (Information Security Management) เป็นกระบวนการในการปกป้องข้อมูลที่สำคัญขององค์กรจากภัยคุกคามและช่องโหว่ โดยใช้ชุดของนโยบาย กระบวนการและเครื่องมือที่กำหนดขึ้นเพื่อรักษาความลับ (Confidentiality) ความถูกต้อง (Integrity) และความพร้อมใช้งาน (Availability) ของข้อมูล ระบบการจัดการความปลอดภัยของข้อมูล (ISMS) เป็นส่วนสำคัญในการจัดการนี้ โดยมุ่งเน้นที่การระบุและประเมินความเสี่ยง พร้อมกับดำเนินการควบคุมเพื่อลดความเสี่ยงเหล่านั้น

องค์ประกอบ

องค์ประกอบสามประการ (CIA) ของการจัดการความปลอดภัยของข้อมูล (Information Security Management) คือ

1. ความลับ (Confidentiality): การรักษาความลับของข้อมูลเพื่อให้แน่ใจว่าเฉพาะบุคคลที่ได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงหรือแก้ไขข้อมูลได้ โดยอาจมีการจัดหมวดหมู่ข้อมูลตามความเสี่ยงและผลกระทบที่คาดว่าจะเกิดขึ้น

2. ความถูกต้อง (Integrity): การรักษาความถูกต้องและความสม่ำเสมอของข้อมูลตลอดอายุการใช้งาน โดยป้องกันการแก้ไขหรือการลบข้อมูลโดยไม่ได้รับอนุญาต ด้วยมาตรการเช่น การควบคุมการเข้าถึงและการตรวจสอบความถูกต้องของข้อมูล

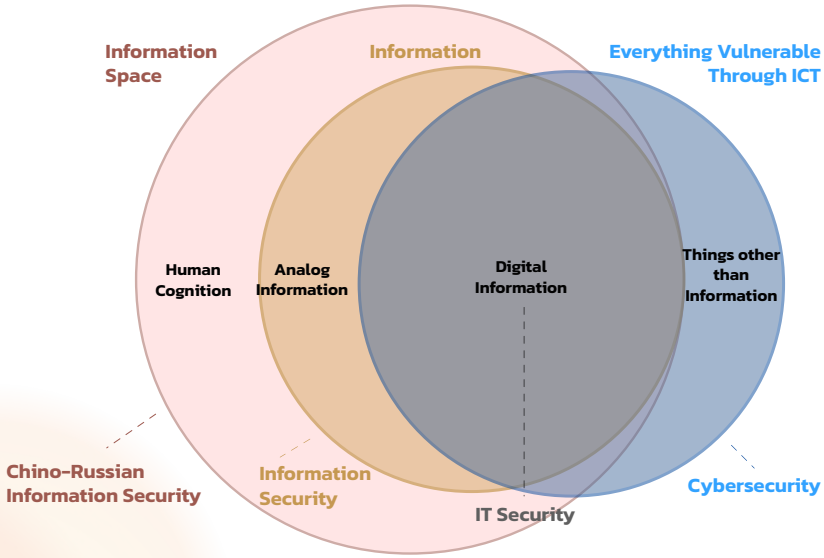
3. ความพร้อมใช้งาน (Availability): การทำให้แน่ใจว่าข้อมูลสำคัญสามารถเข้าถึงได้โดยผู้ใช้ที่ได้รับอนุญาตเมื่อจำเป็น ผ่านกระบวนการบำรุงรักษาและการตอบสนองต่อเหตุการณ์เพื่อป้องกันการสูญหายของข้อมูล

ความแตกต่างระหว่าง Information Security, Cybersecurity และ IT Management

Information Security เน้นการปกป้องข้อมูลทั้งในรูปแบบดิจิทัลและที่ไม่ใช่ดิจิทัลจากการเข้าถึง การใช้ การเปิดเผย การขัดขวาง การเปลี่ยนแปลงหรือการทำลายที่ไม่ได้รับอนุญาต ความปลอดภัยข้อมูลครอบคลุมถึงการรักษาความลับ (Confidentiality) ความสมบูรณ์ (Integrity) และความพร้อมใช้งาน (Availability) ของข้อมูลเพื่อให้มั่นใจว่าข้อมูลได้รับการปกป้องจากความเสี่ยงต่าง ๆ นอกจากนี้ยังรวมถึงการจัดการความเสี่ยง การปฏิบัติตามกฎหมายและข้อบังคับ และการควบคุมการเข้าถึงข้อมูลในทุก ๆ รูปแบบ ไม่ว่าจะเป็นกระดาษหรือดิจิทัล

IT Security (Information Technology Security) เน้นการปกป้องระบบเทคโนโลยีสารสนเทศ รวมถึงฮาร์ดแวร์ ซอฟต์แวร์ และเครือข่ายที่ใช้ในการเก็บรักษาและประมวลผลข้อมูล IT Security คล้ายคลึงกับ InfoSec แต่เน้นที่การปกป้องทรัพยากรทางเทคโนโลยี โดยครอบคลุมการรักษาความปลอดภัยเครือข่าย การควบคุมการเข้าถึงและการจัดการความเสี่ยงทางเทคโนโลยี เพื่อป้องกันการโจมตีและการเข้าถึงที่ไม่ได้รับอนุญาต

Cybersecurity เป็นส่วนหนึ่งของ IT Security ที่เน้นการปกป้องระบบคอมพิวเตอร์และเครือข่ายจากการโจมตีทางไซเบอร์ มุ่งเน้นการป้องกัน การตรวจจับ และการตอบสนองต่อภัยคุกคามทางไซเบอร์ เช่น มัลแวร์ ฟิชชิ่ง การโจมตีแบบ DDoS และการโจมตีทางไซเบอร์อื่น ๆ Cybersecurity ใช้เครื่องมือและเทคนิคต่าง ๆ เพื่อป้องกันการโจมตีจากภายนอก และรักษาความปลอดภัยของข้อมูลและระบบในเครือข่าย



แผนภูมิแสดงถึงองค์ประกอบต่าง ๆ ที่เกี่ยวข้อง ที่มา: ivezic.com

ทั้งสามสาขานี้มีความสัมพันธ์กันและมุ่งเน้นไปที่การปกป้องข้อมูลและระบบ ในมิติที่แตกต่างกัน Information Security เน้นการปกป้องข้อมูลทั้งหมด IT Security เน้นการปกป้องทรัพยากรทางเทคโนโลยีที่ใช้ในการเก็บรักษาและประมวลผลข้อมูล และ Cybersecurity เน้นการปกป้องระบบคอมพิวเตอร์และเครือข่ายจากการโจมตีทางไซเบอร์

ทำไมองค์กรควรให้ความสำคัญและต้องทำ Information Security Management

ในยุคดิจิทัลปัจจุบัน การจัดการความปลอดภัยของข้อมูล (Information Security Management) เป็นสิ่งสำคัญที่องค์กรทุกแห่งควรให้ความสำคัญ การรักษาความปลอดภัยของข้อมูลไม่เพียงแค่ปกป้องข้อมูลที่มีค่า แต่ยังช่วยเสริมสร้างความน่าเชื่อถือ ลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ และสร้างวัฒนธรรมความปลอดภัยภายในองค์กรด้วย

ปกป้องข้อมูลที่มีค่า

ข้อมูลที่สำคัญ เช่น ข้อมูลลูกค้า ข้อมูลทางการเงิน และทรัพย์สินทางปัญญา มีมูลค่าสูง หากข้อมูลเหล่านี้ถูกเข้าถึงหรือรั่วไหลอาจทำให้องค์กรประสบความเสียหายทางการเงิน และเสียชื่อเสียง การจัดการความปลอดภัยของข้อมูลช่วยปกป้องข้อมูลเหล่านี้จากการเข้าถึงที่ไม่ได้รับอนุญาต

เพิ่มความน่าเชื่อถือ

องค์กรที่มีมาตรการความปลอดภัยจะได้รับความไว้วางใจจากลูกค้าและพันธมิตร ลูกค้าจะมั่นใจได้ว่าข้อมูลส่วนตัว และข้อมูลทางการเงินของพวกเขาจะได้รับการปกป้องอย่างเหมาะสม ความไว้วางใจนี้ผลให้ความสัมพันธ์ทางธุรกิจดีขึ้นและมีโอกาสในการร่วมมือทางธุรกิจในอนาคต

ลดความเสี่ยงจากภัยคุกคามทางไซเบอร์

ภัยคุกคามทางไซเบอร์ เช่น มัลแวร์ แรนซัมแวร์ และการโจมตีแบบฟิชชิ่ง มีการพัฒนาอย่างต่อเนื่อง การจัดการความปลอดภัยของข้อมูลที่มีประสิทธิภาพช่วยให้องค์กรสามารถตรวจจับ ป้องกัน และตอบสนองต่อภัยคุกคามเหล่านี้ได้ ลดค่าใช้จ่ายในการฟื้นฟูระบบและการกู้คืนข้อมูลที่เสียหาย

สร้างวัฒนธรรมความปลอดภัยภายในองค์กร

การให้ความรู้และฝึกอบรมพนักงานเกี่ยวกับการรักษาความปลอดภัยของข้อมูล ทำให้พนักงานเข้าใจและมีความรับผิดชอบร่วมกันในการปกป้องข้อมูลขององค์กร วัฒนธรรมความปลอดภัยนี้ช่วยเสริมสร้างการป้องกันภัยคุกคามจากภายในองค์กรเอง

กรอบมาตรฐานการปฏิบัติงานที่เป็นที่นิยม

NIST Cybersecurity Framework (CSF): CSF 2.0

NIST Cybersecurity Framework (CSF) เป็นกรอบการทำงานลดความเสี่ยงจากภัยคุกคามหรือภัยอันตรายทางไซเบอร์ ที่ถูกสร้างขึ้นโดยในนามของ National Institute of Standards and Technology ซึ่งเป็นหน่วยงานภายใต้กระทรวงพาณิชย์ของประเทศสหรัฐอเมริกา กรอบการทำงานนี้เป็นที่ยอมรับและใช้งานอย่างแพร่หลายในระดับสากล โดยในเดือนกุมภาพันธ์ ปี ค.ศ. 2024 ได้มีการประกาศฉบับปรับปรุงซึ่งก็คือ CSF 2.0 เพื่อเพิ่มประสิทธิภาพของกรอบการทำงานนี้จากกรอบการทำงานเดิมก่อนหน้านี้ กรอบการทำงาน CSF จะมุ่งเน้นไปที่โครงสร้างพื้นฐานสำคัญของประเทศ เช่น เครือข่ายโทรคมนาคม หรือโรงพยาบาล แต่ในปัจจุบัน CSF 2.0 ได้ถูกออกแบบมาเพื่อนำไปประยุกต์ใช้ในองค์กรทุกประเภท ทุกอุตสาหกรรม ทุกระดับไม่ว่าจะเป็นโรงเรียนขนาดเล็ก องค์กรไม่แสวงหาผลกำไร ไปจนถึงองค์กรขนาดใหญ่ โดยไม่คำนึงถึงระดับความล้ำสมัยของเทคโนโลยีที่นำไปใช้ในองค์กรนั้น ๆ นอกจากนี้ CSF 2.0 ได้มีการเพิ่มฟังก์ชัน Govern (กำกับดูแล) เข้าไปในแก่นกลางของกรอบการทำงาน โดยเพิ่มการให้ความสำคัญกับการกำกับดูแล (Governance) และห่วงโซ่อุปทาน (Supply chain)

แกนหลัก CSF 2.0 (CSF 2.0 Core)
ที่มา: https://www.darkreading.com/cybersecurity-operations/whats-new-in-nist-cybersecurity-framework-2-0

CSF Core – ฟังก์ชัน (Functions)

แกนหลักของ CSF (CSF Core) เป็นการแบ่งประเภทกระบวนการลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ซึ่งประกอบด้วย 6 กระบวนการหรือฟังก์ชัน คือ Govern, Identify, Protect, Detect, Respond และ Recover โดยที่มีฟังก์ชัน Govern อยู่ตรงกลาง เป็นตัวกำหนดการดำเนินงานของฟังก์ชันที่เหลือ ฟังก์ชัน Govern, Identify, Protect มีหน้าที่ในการป้องกันและเตรียมรับมือกับภัยคุกคาม ส่วนฟังก์ชัน Detect, Respond และ Recover ใช้สำหรับการตรวจพบและบริหารเหตุการณ์ภัยคุกคามทางไซเบอร์ ฟังก์ชันของกรอบการทำงานนี้สามารถแบ่งออกเป็นหมวดหมู่และหมวดหมู่ย่อยได้เพิ่มเติม ซึ่งเป็นส่วนอธิบายรายละเอียดของฟังก์ชันให้ลึกมากยิ่งขึ้นแกนหลักของ CSF เป็นเพียงการนำเสนอให้เห็นถึงแนวทางการลดความเสี่ยง แต่ไม่ได้กล่าวให้ทราบถึงวิธีการลดความเสี่ยงโดยชัดเจน ซึ่งแต่ละองค์กรสามารถนำเอาแนวทางการลดความเสี่ยงดังกล่าวไปกำหนดวิธีการลดความเสี่ยงที่ชัดเจนตามบริบทของแต่ละองค์กร

Govern (กำกับดูแล)

สำหรับการกำกับดูแลความมั่นคงปลอดภัยทางไซเบอร์ให้ได้สำเร็จ จำเป็นต้องอาศัยความเข้าใจบริบทขององค์กร การกำหนดระดับความเสี่ยงที่ยอมรับได้ การกำหนดหน้าที่และความรับผิดชอบของบุคลากรที่เกี่ยวข้องต่อการรักษาความมั่นคงปลอดภัยทางไซเบอร์อย่างชัดเจน และบังคับใช้นโยบายการกำกับดูแลความมั่นคงปลอดภัยทางไซเบอร์อย่างสม่ำเสมอ สิ่งที่ท้าทายของฟังก์ชันนี้คือความซับซ้อนในการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ให้สอดคล้องกับวัตถุประสงค์ขององค์กร และการจัดการความเสี่ยงที่เกิดจากผู้ให้บริการภายนอก รวมไปถึงการควบคุมกำกับดูแลทั้งองค์กรอย่างทั่วถึง นี่จึงเป็นเหตุผลที่ต้องมีมาตรการควบคุมที่มีประสิทธิภาพ เพื่อส่งเสริมความรับผิดชอบและผลักดันให้เกิดการปรับปรุงอย่างต่อเนื่องในการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

Identify (ระบุ)

องค์กรต้องจัดทำรายงานเพื่อระบุความเสี่ยงของอุปกรณ์ต่างๆ จัดลำดับความสำคัญของสินทรัพย์ทางสารสนเทศภายในองค์กร และมีกระบวนการจัดการสินทรัพย์ตั้งแต่เริ่มต้นจนถึงวันที่หมดอายุการใช้งานของสินทรัพย์ (Asset Life Management – ALM) นอกจากนี้ยังต้องตรวจสอบและรวบรวมข้อมูลข่าวกรองด้านภัยคุกคามเพื่อใช้ประเมินความเสี่ยงขององค์กร ณ เวลาปัจจุบัน

Protect (ป้องกัน)

การใช้มาตรการรักษาความปลอดภัยเพื่อปกป้องระบบหรือข้อมูลขององค์กร เช่น การกำหนดสิทธิ์การเข้าถึง การใช้เทคโนโลยีป้องกันระบบ และการจัดอบรมเพื่อเพิ่มความตระหนักรู้เกี่ยวกับภัยคุกคามทางไซเบอร์ให้กับพนักงาน

Detect (ตรวจจับ)

องค์กรต้องมีกระบวนการติดตามสถานะของสินทรัพย์อย่างต่อเนื่องเพื่อตรวจจับสิ่งผิดปกติและสัญญาณของภัยคุกคาม รวมถึงความสามารถในการวิเคราะห์เหตุการณ์ที่น่าสงสัยหรืออาจก่อให้เกิดอันตรายอย่างรวดเร็ว เพื่อระบุและตรวจพบพฤติกรรมหรือสถานการณ์ที่ผิดปกติของระบบ ซึ่งอาจเป็นสัญญาณของการถูกคุกคามทางไซเบอร์ การมีกระบวนการตรวจจับที่มีประสิทธิภาพจะช่วยให้องค์กรสามารถระบุภัยคุกคามทางไซเบอร์ได้อย่างรวดเร็ว และนำไปสู่การตอบสนองและแก้ไขปัญหาได้ทันท่วงที ช่วยลดผลกระทบที่อาจเกิดขึ้น

Respond (ตอบสนอง)

องค์กรต้องจัดทำแผนรับมือเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ (Incident Response Plan) อย่างเป็นระบบ เพื่อรับมือกับภัยคุกคามที่อาจเกิดขึ้น โดยกำหนดนโยบาย ขั้นตอน และระบุหน้าที่ความรับผิดชอบของผู้เกี่ยวข้องอย่างชัดเจน แผนนี้จะช่วยให้องค์กรสามารถตอบสนองต่อเหตุการณ์ได้อย่างรวดเร็วและมีประสิทธิภาพ ลดความเสี่ยงและผลกระทบที่อาจเกิดขึ้น

Recover (กู้คืน)

ปฏิบัติตามแผนการกู้คืนระบบที่จัดเตรียมไว้อย่างเป็นขั้นตอน ตรวจสอบความครบถ้วนของข้อมูลสำรองที่ใช้ในการกู้คืน จัดทำแผนการสื่อสารเพื่อแจ้งความคืบหน้าให้บุคคลที่เกี่ยวข้องทราบ เพื่อให้สามารถวางแผนการดำเนินงานได้อย่างต่อเนื่องโดยไม่หยุดชะงัก รวมไปถึงการจัดทำเอกสารบันทึกรายละเอียดเหตุการณ์ ปัญหาที่พบและวิธีการแก้ไข เพื่อใช้ข้อมูลนี้ในการวิเคราะห์และประเมินสำหรับปรับปรุงแนวปฏิบัติและแผนรับมือเหตุการณ์ในอนาคต

CSF Core – หมวดหมู่ (Categories):

แต่ละฟังก์ชันประกอบด้วยหมวดหมู่ที่ให้รายละเอียดเพิ่มเติมเกี่ยวกับกิจกรรมและผลลัพธ์ที่ต้องการ

Govern (กำกับดูแล)

Organizational Context (บริบทขององค์กร) องค์กรควรเข้าใจบริบทของตนว่า ณ ปัจจุบัน ตัวองค์กรมีพันธกิจ และความคาดหวังจากผู้มีส่วนได้ส่วนเสียอย่างไร สถานะขององค์กร ณ ปัจจุบันว่าต้องพึ่งพาอาศัยใครและกฎหมายที่ต้องปฏิบัติตาม ซึ่งบริบทเหล่านี้ส่งผลต่อการตัดสินใจขององค์กรในการบริหารจัดการภัยอันตรายทางไซเบอร์

Risk Management Strategy (กลยุทธ์การบริหารความเสี่ยง) ในการบริหารความเสี่ยงขององค์กร องค์กรควรทราบถึงสิ่งที่องค์กรให้ความสำคัญเป็นลำดับต้น ๆ ข้อจำกัดขององค์กร และระดับความเสี่ยงที่สามารถยอมรับได้ เพื่อนำข้อมูลเหล่านี้สื่อสารกับบุคคลที่เกี่ยวข้องและไปประกอบการตัดสินใจในการรักษาความมั่นคงปลอดภัยทางไซเบอร์

Roles, Responsibilities, and Authorities (หน้าที่ ความรับผิดชอบ และอำนาจหน้าที่) เนื่องด้วยการรักษาความมั่นคงปลอดภัยทางไซเบอร์ องค์กรสามารถกำหนดหน้าที่และความรับผิดชอบของพนักงานในองค์กร และแต่งตั้งบุคคลซึ่งมีอำนาจหน้าที่ส่งเสริมให้พนักงานในองค์กรมีความรับผิดชอบ ประเมินความสามารถของตน และพัฒนาทักษะของตนอย่างต่อเนื่อง หลังจากที่กำหนดเรื่องนี้เสร็จสิ้นแล้ว องค์กรต้องสามารถสื่อสารให้บุคคลที่เกี่ยวข้องกับเรื่องนี้รับทราบ

Policy (กฎระเบียบ) ในส่วนนี้องค์กรสามารถกำหนด สื่อสาร และบังคับใช้กฎระเบียบในการรักษาความมั่นคงปลอดภัยทางไซเบอร์

Oversight (ควบคุม) หลังจากที่องค์กรรับทราบถึงผลลัพธ์การใช้มาตราการบริหารความเสี่ยงต่อการเกิดภัยอันตรายทางไซเบอร์ องค์กรมีหน้าที่นำผลลัพธ์นี้ไปใช้ปรับปรุงพัฒนากลยุทธ์การบริหารความเสี่ยงให้ดียิ่งขึ้น

Cybersecurity Supply Chain Risk Management (การบริหารความเสี่ยงของห่วงโซ่อุปทานในบริบทของการรักษาความมั่นคงปลอดภัยทางไซเบอร์) ผู้มีส่วนได้ส่วนเสียขององค์กรสามารถระบุ กำหนด จัดการ ควบคุม และปรับปรุง กระบวนการการบริหารความเสี่ยงของห่วงโซ่อุปทานในบริบทการรักษาความมั่นคงปลอดภัยทางไซเบอร์

Identify (ระบุ)

Asset Management (การจัดการทรัพย์สิน) องค์กรสามารถระบุทรัพย์สินของตนที่นำไปสู่การบรรลุเป้าหมายในการบริหารความเสี่ยงต่อการเกิดภัยอันตรายทางไซเบอร์ เช่น ข้อมูล ฮาร์ดแวร์ ซอฟต์แวร์ ระบบ สิ่งอำนวยความสะดวก บริการและบุคคลต่าง ๆ และบริหารจัดการทรัพย์สินเหล่านี้ตามความสำคัญของทรัพย์สินต่อเป้าหมายและกลยุทธ์บริหารความเสี่ยงขององค์กรโดยรวม

Risk Assessment (การประเมินความเสี่ยง) องค์กรเข้าใจความเสี่ยงต่อภัยอันตรายทางไซเบอร์ที่ส่งผลกระทบต่อตัวองค์กร สินทรัพย์ขององค์กร และบุคคลต่าง ๆ

Improvement (การปรับปรุง) องค์กรสามารถระบุได้ถึงแนวทางการปรับปรุงกระบวนการและกิจกรรมในการบริหารความเสี่ยงต่อภัยอันตรายทางไซเบอร์ของทุกฟังก์ชันในกรอบการดำเนินงาน CSF นี้

Protect (ป้องกัน)

Identify Management, Authentication, and Access Control (การระบุการจัดการพิสูจน์ตัวตน และควบคุมการเข้าถึง) ทำให้การเข้าถึงทรัพย์สินทำได้เฉพาะบุคคล บริการ และฮาร์ดแวร์ที่ได้รับอนุญาตเท่านั้น รวมทั้งเรียงลำดับความสำคัญในการบริหารทรัพย์สินจากระดับความเสี่ยงของสินทรัพย์นั้น ๆ ต่อการเข้าถึงโดยไม่ได้รับอนุญาต

Awareness and Training (การสร้างความตระหนักและการฝึกอบรม) การฝึกอบรมและสร้างความตระหนักรู้ให้แก่บุคลากรเพื่อให้บุคลากรมีความสามารถในการปฏิบัติหน้าที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์

Data Security (การรักษาความปลอดภัยของข้อมูล) การบริหารจัดการข้อมูลให้สอดคล้องกับกลยุทธ์การบริหารความเสี่ยงขององค์กรเพื่อรักษาความลับ (Confidentiality) ความถูกต้อง (Integrity) และความพร้อมใช้ของข้อมูล (Availability)

Platform Security (ความปลอดภัยของแพลตฟอร์ม) การบริหารจัดการฮาร์ดแวร์ ซอฟท์แวร์ (เช่น เฟิร์มแวร์ ระบบปฏิบัติการแอปพลิเคชัน) และบริการแพลตฟอร์มทางออฟไลน์และออนไลน์ให้สอดคล้องกับกลยุทธ์การบริหารความเสี่ยงขององค์กรเพื่อรักษาความลับความถูกต้อง และความพร้อมใช้ของข้อมูล

Technology Infastructure Resillience (ความแข็งแกร่งของเทคโนโลยีสารสนเทศ) การบริหารสถาปัตยกรรมด้านความมั่นคงปลอดภัยให้สอดคล้องกับกลยุทธ์ด้านความเสี่ยงขององค์กรเพื่อป้องกันความลับ ความถูกต้อง และความพร้อมใช้ของทรัพย์สินขององค์กร และมีความยืดหยุ่นที่จะสามารถรับมือกับทั้งภัยคุกคามทางไซเบอร์และภัยพิบัติต่าง ๆ ได้

Detect (ตรวจจับ)

Security Continuous Monitoring (การตรวจสอบความปลอดภัยอย่างต่อเนื่อง) ทรัพย์สินต้องมีการเฝ้าระวังเพื่อตรวจหาความผิดปกติ IoC (Indicators of Compromise เป็นสิ่งที่ให้สัญญาณว่าระบบอาจจะถูกละเมิดความปลอดภัย) และเหตุการณ์ที่ผิดปกติอื่น ๆ

Awareness and Training (การสร้างความตระหนัก และการฝึกอบรม) ความผิดปกติ IoC และเหตุการณ์ที่ผิดปกติอื่น ๆ มีความจำเป็นต้องได้รับการวิเคราะห์เพื่อกำหนดคุณลักษณะของเหตุการณ์ และตรวจจับเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์

Respond (ตอบสนอง)

Incident Management (การบริหารจัดการเหตุการณ์) บริหารจัดการการตอบสนองต่อเหตุการณ์ภัยอันตรายทางไซเบอร์

Incident Analysis (การวิเคราะห์เหตุการณ์) การดำเนินการการสอบสวนเหตุการณ์เพื่อให้มั่นใจถึงประสิทธิภาพการรับมือต่อเหตุการณ์ภัยคุกคามทางไซเบอร์ สนับสนุนกิจกรรมการกู้คืนข้อมูลและนิติวิทยาศาสตร์ที่เกี่ยวข้อง

Incident Response Reporting and Communication (การรายงานและสื่อสารข้อมูลเกี่ยวกับเหตุการณ์) กิจกรรมการรับมือต่อเหตุการณ์ภัยคุกคามทางไซเบอร์ต้องมีการประสานงานกับผู้มีส่วนได้ส่วนเสียทั้งภายในและภายนอกตามที่กฎหมาย กฎระเบียบ หรือนโยบายได้กำหนดไว้

Incident Mitigation (การบรรเทาผลกระทบของเหตุการณ์) ดำเนินกิจกรรมเพื่อป้องกันการขยายวงกว้างและลดผลกระทบของเหตุการณ์ที่เกิดขึ้น

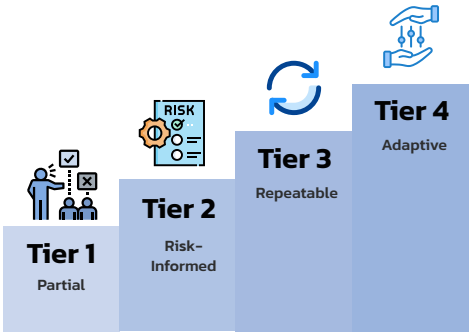
Recover (ตอบสนอง)

Incident Recovery Plan Execution (แผนการกู้คืนสถานการณ์) ดำเนินกิจกรรมการกู้คืนข้อมูลเพื่อให้มั่นใจถึงความพร้อมใช้งานของระบบและบริการต่าง ๆ ที่ได้รับผลกระทบจากเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์

Incident Recovery Communication (การสื่อสารข้อมูลเกี่ยวกับการกู้คืนสถานการณ์) กิจกรรมการกู้คืนต้องได้รับการประสานงานกับผู้มีส่วนได้ส่วนเสียทั้งภายในและภายนอกได้ทราบ

ระดับขั้น (Tiers):

ระดับขั้น (Tiers) เป็นตัวชี้วัดความเข้มงวดขององค์กรต่อการกำกับดูแล (Govern ใน CSF Core) และบริหารความเสี่ยงความมั่นคงปลอดภัยทางไซเบอร์ (Identify, Protect, Detect, Respond และ Recover ใน CSF Core) นอกจากนี้ระดับชั้นนี้ยังสามารถให้บริบทเกี่ยวกับมุมมองขององค์กรต่อความเสี่ยงทางด้านการรักษาความปลอดภัยทางไซเบอร์และกระบวนการขององค์กรในการบริหารความเสี่ยงนี้ ซึ่งระดับชั้นมีอยู่ทั้งหมด 4 ระดับ ได้แก่



ระดับ (Tier) ใน CSF 2.0
ที่มา: https://csf.tools/reference/nist-cybersecurity-framework/v2-0/

ระดับการใช้งาน (Tiers)	การกำกับดูแล	การบริหารความเสี่ยง
ระดับขั้นที่ 1: Partial	นำกลยุทธ์การบริหารความเสี่ยงมาประยุกต์ใช้ตามสถานการณ์ ไม่ได้นำมาใช้ล่วงหน้า	การรับรู้อย่างจำกัดเกี่ยวกับความเสี่ยงด้านความปลอดภัยทางไซเบอร์ในระดับองค์กร
ระดับขั้นที่ 2: Risk informed	มาตราการบริหารความเสี่ยงอนุมัติโดยบุคลากรด้านบริหารแล้ว แต่อาจไม่ได้ประกาศใช้กับองค์กรโดยรวม	มีการรับรู้ความเสี่ยงด้านความปลอดภัยทางไซเบอร์ในระดับองค์กร แต่ยังไม่ได้ดำเนินการจัดตั้งแนวทางในการบริหารจัดการความเสี่ยงขององค์กร
ระดับขั้นที่ 3: Repeatable	แนวปฏิบัติในการจัดการความเสี่ยงขององค์กรได้รับการอนุมัติอย่างเป็นทางการและออกประกาศใช้เป็นนโยบาย	องค์กรมีวิธีการจัดการความเสี่ยงทางไซเบอร์ในระดับทั่วทั้งองค์กร และมีการแบ่งปันข้อมูลด้านความปลอดภัยทางไซเบอร์อย่างสม่ำเสมอภายในองค์กร
ระดับขั้นที่ 4: Adaptative	องค์กรใช้วิธีการจัดการความเสี่ยงทางไซเบอร์ในระดับทั่วทั้งองค์กร โดยใช้นโยบาย กระบวนการ และขั้นตอนเพื่อรับมือกับเหตุการณ์ความปลอดภัยที่เป็นไปได้	องค์กรปรับพฤติกรรมการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์ตามกิจกรรมการรักษาความมั่นคงปลอดภัยทางไซเบอร์ในอดีตและปัจจุบัน รวมถึงตามบทเรียนขององค์กรในอดีต และตัวชี้วัดการคาดการณ์

ISO/IEC 27001:2022 มาตรฐานการจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS)

ตราสัญลักษณ์ของมาตราฐาน ISO 27001
ที่มา: https://www.davidfroud.com/iso-27001-certification-really-worth/

ISO/IEC 27001 เป็นมาตรฐานสากลที่ถูกพัฒนาระหว่างองค์กรระหว่างประเทศว่าด้วยมาตรฐาน (International Organization for Standardization) และคณะกรรมาธิการระหว่างประเทศว่าด้วยมาตรฐานสาขาอิเล็กทรอนิกส์ (International Electrotechnical Commission – IEC) ที่ได้รับการปรับเปลี่ยนจากเวอร์ชัน ISO/IEC 20071:2013 เป็น ISO/IEC 20071:2022 ในเดือนตุลาคม ปี ศ.ค. 2022 มาตรฐานนี้ได้รับการยอมรับเป็นอย่างมากสำหรับระบบจัดการความมั่นคงปลอดภัยของข้อมูล (Information Security Management System - ISMS) โดยช่วยให้องค์กรทุกขนาดและทุกประเภทสามารถปกป้องข้อมูลสำคัญได้อย่างเป็นระบบและมีประสิทธิภาพ ISMS เป็นระบบการจัดการข้อมูลที่ออกนโยบาย ขั้นตอนปฏิบัติ และมาตรการควบคุมเพื่อบริหารความเสี่ยงการรักษาความปลอดภัยของข้อมูลตามความเสี่ยงและความต้องการของแต่ละองค์กร

ความสำคัญและประโยชน์ของมาตรฐาน ISO/IEC 27001

มาตรฐาน ISO/IEC 27001 ขับเคลื่อนให้องค์กรบริหารและรักษาข้อมูลที่มีความละเอียดอ่อนให้ปลอดภัย โดยป้องกันการเข้าถึงของข้อมูลและการโจมตีทางไซเบอร์ นี้ยังช่วยให้องค์กรสามารถเตรียมตัว รับมือ และแก้ไขสถานการณ์ภัยอันตรายทางไซเบอร์ (Cyber Resilience) และสร้างความน่าเชื่อถือให้กับผู้มีส่วนได้ส่วนเสียว่าข้อมูลของพวกเขาจะถูกรักษาอย่างปลอดภัย

หลักการเบื้องหลังมาตรฐาน ISO 27001

มีหลักการภายใต้การทำให้ข้อมูลเป็นความลับ (Confidentiality) ครบถ้วนและถูกต้อง (Integrity) และสามารถเข้าถึงได้ (Availability) ดำเนินการโดยใช้วิธี PDCA (Plan-Do-Check-Act) ซึ่งเป็นกระบวนการปรับปรุงอย่างต่อเนื่อง โดยมีรายละเอียดดังนี้

Plan (วางแผน): ระบุความเสี่ยงด้านความปลอดภัยสารสนเทศ และกำหนดวัตถุประสงค์และมาตรการควบคุมของ ISMS

Do (ปฏิบัติ): ดำเนินการตามมาตรการควบคุมของ ISMS ที่ได้กำหนดไว้

Check (ตรวจสอบ): ตรวจสอบและประเมินผลการดำเนินงานของ ISMS

Act (ปรับปรุง): ปรับปรุง ISMS อย่างต่อเนื่อง เพื่อเพิ่มประสิทธิภาพ

ข้อกำหนดหรือองค์ประกอบหลักของ ISMS ใน ISO 27001:2022

Context of the Organization (บริบทขององค์กร):

- เข้าใจสภาพแวดล้อมทั้งภายในและภายนอกขององค์กร
- กำหนดสิ่งที่จำเป็นของผู้ที่เกี่ยวข้องและความคาดหวังของพวกเขา
- กำหนดขอบเขต ISMS และคิดค้น ISMS ที่สามารถนำไปปรับใช้กับวิธี PDCA

Leadership (ความเป็นผู้นำ):

- ผู้บริหารระดับสูงต้องแสดงความเป็นผู้นำและให้ความสำคัญกับการดำเนินงานด้านความปลอดภัยสารสนเทศ
- กำหนดนโยบายการบริหารความมั่นคงปลอดภัยสารสนเทศ
- มอบหมายความรับผิดชอบและอำนาจหน้าให้ผู้คนในแต่ละบทบาทในองค์กร และสื่อสารเรื่องนี้ภายในองค์กร

Planning (การวางแผน):

- วางแผนจัดการกับความเสี่ยงและโอกาสของความมั่นคงปลอดภัยสารสนเทศ
- กำหนดวัตถุประสงค์และแผนการบรรลุวัตถุประสงค์เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศ
- วางแผนรับมือกับความต้องการเปลี่ยนแปลง ISMS

Support (การสนับสนุน):

- จัดสรรทรัพยากรที่จำเป็นต่อการทำ PDCA
- กำหนดสมรรถนะของบุคลากร ใช้วิธีต่าง ๆ เช่นการฝึกอบรมหรือมอบหมายงานเพื่อสร้างสมรรถนะที่กำหนดมาแล้วให้กับบุคลากร และเก็บหลักฐานที่แสดงให้เห็นถึงสมรรถนะของบุคลากร
- สร้างความตระหนักรู้เรื่องนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ ส่วนร่วมของบุคลากรในการบรรลุตามเป้าหมายด้านความมั่นคงปลอดภัยสารสนเทศ และผลลัพธ์จากการบรรลุวัตถุประสงค์และไม่บรรลุวัตถุประสงค์
- กำหนดรายละเอียดการสื่อสารเกี่ยวกับการรักษาความมั่นคงปลอดภัยสารสนเทศขององค์กรซึ่งประกอบด้วย เนื้อหาในการสื่อสาร ช่วงเวลาที่สื่อสาร บุคคลใดที่ต้องสื่อสารให้ทราบ และวิธีการสื่อสาร
- สร้างและปรับปรุงสารสนเทศที่เป็นลายลักษณ์อักษร และควบคุมสารสนเทศที่เป็นลายลักษณ์อักษรให้มีความปลอดภัย

Operation (การดำเนินการ):

- วางแผนการดำเนินการและการควบคุมเกี่ยวกับการรักษาความมั่นคงปลอดภัยสารสนเทศ ควบคุมการรักษาความมั่นคงปลอดภัยสารสนเทศการทำ PDCA
- ประเมินความเสี่ยงด้านความมั่นคงปลอดภัยทางสารสนเทศเมื่อถึงรอบเวลาที่กำหนด หรือเมื่อมีเหตุการณ์ที่จำเป็นต้องเร่งสอบสวนประเมินความเสี่ยง หรือจากเกณฑ์ความเสี่ยงขององค์กรต่อระบบสารสนเทศ
- ดำเนินการปฏิบัติตามแผนการจัดการความเสี่ยงที่ได้จัดทำไว้

Performance Evaluation (การประเมินผลการปฏิบัติงาน):

ตรวจสอบและประเมินผลการดำเนินงานของ ISMS

- เฝ้าระวัง วัดผล วิเคราะห์ และประเมินผลการรักษาความมั่นคงปลอดภัยทางไซเบอร์
- ทำการตรวจประเมินภายใน (Internal Audit)
- ผู้บริหารทบทวน ISMS ขององค์กรตามรอบการทบทวน

Improvement (การปรับปรุง): ปรับปรุง ISMS อย่างต่อเนื่อง

- ใช้ข้อมูลจากบททบทวนผู้บริหาร การประเมินผล และการตรวจประเมินภายในมาปรับปรุง ISMS อย่างต่อเนื่อง
- ดำเนินการแก้ไขความไม่สอดคล้องที่ส่งผลกระทบกับ ISMS

Annex A controls (มาตรการควบคุม Annex A)

Annex A controls เป็นมาตรการควบคุมที่ใช้ลดความเสี่ยงด้านความปลอดภัยทางไซเบอร์ให้กับองค์กร ซึ่งมีทั้งหมด 93 ข้อ แบ่งออกเป็น 4 หมวดหมู่ ได้แก่ Organizational (มาตรการขององค์กร) People (มาตรการด้านบุคลากร) Physical (มาตรการด้านกายภาพ) และTechnological (มาตรการด้านเทคโนโลยี) ซึ่งแต่ละองค์กรสามารถเลือกใช้มาตรการต่าง ๆ ตามการบริหารจัดการความเสี่ยงของตน โดยไม่จำเป็นต้องเลือกใช้ทุกมาตรการที่มีอยู่ทั้งหมด 93 ข้อ

Organizational controls (จำนวน 37 มาตรการ): เป็นมาตรการระดับองค์กรโดยใช้นโยบาย ขั้นตอนการปฏิบัติ การกำหนดความรับผิดชอบของบุคลากรที่เกี่ยวข้อง และอื่น ๆ ที่องค์กรใช้ปกป้องข้อมูลให้มีความปลอดภัย ซึ่งครอบคลุมในประเด็นเรื่องนโยบายการรักษาข้อมูลให้ปลอดภัย การบริหารจัดการทรัพย์สินทางสารสนเทศ การควบคุมการเข้าถึงข้อมูล เป็นต้น

People controls (จำนวน 8 มาตรการ): เป็นมาตรการบริหารบุคลากรขององค์กรในการรักษาความปลอดภัยของข้อมูล โดยคำนึงถึงการที่บุคลากรกับข้อมูลมีการโต้ตอบกัน ซึ่งมาตรการนี้ครอบคลุมในประเด็นเรื่องการจัดการทรัพยากรบุคคล

Physical controls (จำนวน 14 มาตรการ): เป็นมาตรการสำหรับรักษาความปลอดภัยของทรัพย์สินที่จับต้องได้ ที่จำเป็นต่อการปกป้องข้อมูลที่เป็นความลับ มาตรการชุดนี้ครอบคลุมในประเด็น เช่น การควบคุมการเข้าออกทางกายภาพ (Physical Entry) การบำรุงรักษาอุปกรณ์ และการเฝ้าระวังด้านความมั่นคงปลอดภัยทางกายภาพ

Technological controls (จำนวน 34 มาตรการ): มาตรการทางดิจิทัลซึ่งรักษาความปลอดภัยโครงสร้างพื้นฐานทางสารสนเทศ โดยครอบคลุมในประเด็นเช่น การพิสูจน์ตัวตนที่มีความมั่นคงปลอดภัย การป้องกันจากโปรแกรมไม่พึงประสงค์ และการสำรองข้อมูล

กฎหมายความมั่นคงปลอดภัยสารสนเทศ

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562:

แหล่งที่มา: https://www.getinvoice.net/security_cyber_2562/

วัตถุประสงค์และขอบเขตของกฎหมาย

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 เป็นกฎหมายที่เริ่มบังคับใช้ในวันที่ 28 พฤษภาคม พ.ศ. 2562 โดยมีวัตถุประสงค์เพื่อกำกับดูแลหน่วยงานภาครัฐและเอกชนในการป้องกัน รับมือ และ ลดความเสี่ยงของภัยคุกคามทางไซเบอร์ที่อาจส่งผลกระทบต่อความมั่นคงของภาครัฐและความสงบเรียบร้อยภายในบ้านเมือง ซึ่งภัยคุกคามทางไซเบอร์ คือการกระทำที่ใช้คอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือโปรแกรมที่ไม่ปลอดภัยเพื่อสร้างความเสียหายให้กับข้อมูลและการสื่อสารที่เชื่อมต่อกันโดยทั่วไปในระบบอินเทอร์เน็ต ในเครือข่ายคอมพิวเตอร์ในโครงข่ายโทรคมนาคม หรือ ในระบบปกติของดาวเทียม

บทบาทและหน้าที่ของหน่วยงานที่เกี่ยวข้อง เช่น สำนักคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.), ศูนย์ประสานการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (ThaiCERT)

ThaiCERT
Thailand Computer Emergency Response Team
By NCSA Thailand

แหล่งที่มา https://www.thaicert.or.th/

สำนักคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เป็นหน่วยงานที่มีความสำคัญในพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มีหน้าที่สร้างความร่วมมือในการทำงานระหว่างภาครัฐและเอกชน ทั้งในสถานการณ์ปกติและสถานการณ์ที่ส่งผลกระทบต่อความมั่นคงอย่างรุนแรง และกำหนดแผนปฏิบัติการและมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ที่เป็นหนึ่งเดียวและต่อเนื่องขึ้นมา เพื่อจัดการกับภัยคุกคามทางไซเบอร์อย่างมีประสิทธิภาพ นอกจากนี้ สกมช. ได้มีการจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (ThaiCERT) ตามที่พระราชบัญญัติกำหนดเพื่อเฝ้าระวังความเสี่ยงจากภัยคุกคามทางไซเบอร์ รวมถึงติดตาม วิเคราะห์ และประมวลผลข้อมูล พร้อมทั้งแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์

ความผิดและบทลงโทษที่เกี่ยวข้องกับการโจมตีทางไซเบอร์

ผู้กระทำความผิดในกฎหมายฉบับนี้สามารถเป็นได้ทั้งพนักงานเจ้าหน้าที่ ซึ่งรัฐมนตรีได้กำหนดให้ปฏิบัติตามข้อกำหนดต่าง ๆ ในกฎหมาย หน่วยงานโครงสร้างพื้นฐานทางสารสนเทศที่ใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์ ในเรื่องที่เกี่ยวข้องกับการรักษาความปลอดภัยทางไซเบอร์ ผู้ซึ่งทำการโจมตีทางไซเบอร์หรือล่วงรู้ข้อมูลและเจ้าของคอมพิวเตอร์ที่สงสัยว่าอาจถูกการโจมตีทางไซเบอร์ โดยโทษทางกฎหมายจะมีทั้งโทษจำคุกและโทษปรับเงิน

พฤติกรรมที่ต้องได้รับการลงโทษ

พนักงานเจ้าหน้าที่: การนำข้อมูลในระบบคอมพิวเตอร์ไปเผยแพร่ต่อผู้อื่นโดยตั้งใจหรือประมาท

หน่วยงานโครงสร้างพื้นฐานทางสารสนเทศ: ไม่ปฏิบัติตามกฎเกณฑ์การรักษาความมั่นคงปลอดภัยทางไซเบอร์ที่ได้กล่าวไว้ในกฎหมาย เช่น ไม่รายงานเหตุการณ์ภัยคุกคามทางไซเบอร์ต่อหน่วยงานที่เกี่ยวข้อง

ผู้ซึ่งทำการโจมตีทางไซเบอร์: ล่วงรู้ข้อมูลเกี่ยวกับคอมพิวเตอร์

เจ้าของคอมพิวเตอร์: ปฏิเสธคำสั่งในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ เช่น ไม่ให้ตรวจสอบคอมพิวเตอร์เพื่อหาจุดเสี่ยง วิเคราะห์ และประเมินผลกระทบต่อการเกิดภัยคุกคามทางไซเบอร์

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA):

แหล่งที่มา: https://www.acisonline.net/?page_id=8726

วัตถุประสงค์และหลักการของ PDPA

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 หรือ Personal Data Protection Act (PDPA) เป็นกฎหมายซึ่งปกป้องข้อมูลส่วนบุคคลให้เก็บรักษาในพื้นที่ที่ปลอดภัย ได้มาตรฐาน และไม่เกิดการรั่วไหล นอกจากนี้ การเก็บและนำข้อมูลส่วนบุคคลไปใช้จะต้องได้รับความยินยอมจากเจ้าของข้อมูล และเจ้าของข้อมูลมีสิทธิทำการแก้ไขและลบข้อมูลส่วนบุคคลที่เคยให้ไว้กับหน่วยงานต่าง ๆ

คำนิยามของข้อมูลส่วนบุคคล

ข้อมูลส่วนบุคคล คือข้อมูลที่สามารถระบุตัวตนของเจ้าของข้อมูลได้ไม่ว่าทางตรงหรือทางอ้อม เช่น เลขบัตรประจำตัวประชาชน ชื่อนามสกุล ที่อยู่ อีเมล เบอร์โทรศัพท์ หรือแม้กระทั่งรูปภาพ ข้อมูลส่วนบุคคลยังประกอบไปด้วยข้อมูลที่มีความละเอียดอ่อน (Sensitive data) ซึ่งข้อมูลประเภทนี้เมื่อถูกการละเมิดแล้วจะสร้างผลกระทบในด้านการทำงาน สังคม และชีวิตความเป็นอยู่ที่รุนแรงกว่าข้อมูลส่วนบุคคลทั่วไป และอาจนำไปสู่การเลือกปฏิบัติต่อเจ้าของข้อมูลส่วนบุคคลเมื่อทราบว่าเจ้าของข้อมูลส่วนบุคคลมีลักษณะอย่างไร ตัวอย่างของข้อมูลที่มีความละเอียดอ่อนเช่น เชื้อชาติ เผ่าพันธุ์ ข้อมูลสุขภาพ พฤติกรรมทางเพศ ความคิดเห็นทางการเมือง ประวัติอาชญากรรม เป็นต้น

สิทธิของเจ้าของข้อมูลส่วนบุคคล

1. การรับทราบรายละเอียดเกี่ยวกับการเก็บรวบรวมใช้ข้อมูลส่วนบุคคล (Right to be informed)
2. การเข้าถึงข้อมูลส่วนบุคคล (Right to access)
3. การขอให้โอนข้อมูลส่วนบุคคล (Right to data portability)
4. การคัดค้านการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล (Right to object)
5. การขอให้ลบหรือทำลาย หรือทำให้ข้อมูลส่วนบุคคลไม่สามารถระบุตัวตนได้ (Right to erase or to be unidentified)
6. การขอให้หยุดใช้ข้อมูลส่วนบุคคล (Right to restrict processing)
7. การขอแก้ไขข้อมูลส่วนบุคคล (Right to rectification)

หน้าที่ของผู้ควบคุมข้อมูลส่วนบุคคลและผู้ประมวลผลข้อมูลส่วนบุคคล

ผู้ที่เกี่ยวข้องกับกฎหมาย PDPA นี้มีทั้งหมด 3 กลุ่มด้วยกันดังนี้

1. **เจ้าของข้อมูลส่วนบุคคล (Data Subject):** ผู้ซึ่งมีข้อมูลที่ถูกระบุตัวตนไว้ว่าข้อมูลนั้นเป็นของตน
2. **ผู้ควบคุมข้อมูลส่วนบุคคล (Data Controller):** บุคคลหรือองค์กรซึ่งเป็นผู้ตัดสินใจในเรื่องของการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ผู้ควบคุมข้อมูลส่วนบุคคลมีหน้าที่เช่น จัดให้มีมาตราการรักษาความปลอดภัยของข้อมูล ป้องกันไม่ให้ข้อมูลส่วนบุคคลถูกล่วงละเมิด และมีระบบการลบหรือทำลายข้อมูลหลังจากครบกำหนดระยะเวลาการเก็บรักษา เป็นต้น
3. **ผู้ประมวลผลข้อมูลส่วนบุคคล (Data Processor):** บุคคลหรือองค์กรที่ปฏิบัติตามคำสั่งหรือเป็นตัวแทนของผู้ควบคุมข้อมูลส่วนบุคคลในการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูล ผู้ประมวลผลข้อมูลมีหน้าที่เช่น การจัดให้มีมาตราการรักษาความปลอดภัยของข้อมูล รวมถึงแจ้งเมื่อเกิดเหตุการณ์การละเมิดข้อมูลให้ผู้ควบคุมข้อมูลส่วนบุคคลทราบ และเมื่อทำการประมวลผลเก็บข้อมูลในแต่ละครั้งเสร็จเรียบร้อยแล้ว ให้ผู้ประมวลผลข้อมูลส่วนบุคคลบันทึกรายการการประมวล และเก็บรักษาบันทึกนี้ไว้

การบังคับใช้ PDPA ในองค์กร

1. การบังคับใช้ในฐานะ Data Controller

Data Controller มีบทบาทในการกำหนดวัตถุประสงค์และวิธีการในการประมวลผลข้อมูลส่วนบุคคล ซึ่งการบังคับใช้ PDPA ในองค์กรในฐานะ Data Controller มีขั้นตอนสำคัญดังนี้

- **กำหนดนโยบายคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy):** องค์กรต้องจัดทำนโยบายที่ชัดเจนเกี่ยวกับการเก็บรวบรวม การใช้ และการเปิดเผยข้อมูลส่วนบุคคล โดยนโยบายนี้ต้องสอดคล้องกับข้อกำหนดของ PDPA และเผยแพร่ให้ผู้เกี่ยวข้องทราบ
- **ขอความยินยอม (Consent):** ก่อนที่จะเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล องค์กรต้องขอความยินยอมจากเจ้าของข้อมูลและต้องสามารถพิสูจน์ได้ว่ามีการขอความยินยอมอย่างชัดเจนและเป็นธรรม
- **สิทธิของเจ้าของข้อมูล (Data Subject Rights):** องค์กรต้องจัดให้มีวิธีการที่ชัดเจนและสะดวกในการให้เจ้าของข้อมูลสามารถใช้สิทธิของตน เช่น การขอเข้าถึงข้อมูล การแก้ไขข้อมูล การลบข้อมูล เป็นต้น
- **การจัดการความเสี่ยงและการกำหนดมาตรการรักษาความปลอดภัย (Risk Management and Security Measures):** องค์กรต้องประเมินความเสี่ยงที่อาจเกิดขึ้นจากการประมวลผลข้อมูลและ กำหนดมาตรการที่เหมาะสมในการป้องกัน เช่น การเข้ารหัสข้อมูล การจำกัดการเข้าถึงข้อมูล
- **การแจ้งเตือนการละเมิดข้อมูล (Data Breach Notification):** หากเกิดการละเมิดข้อมูลส่วนบุคคล องค์กรต้องมีระบบในการแจ้งเตือนผู้เกี่ยวข้องตามข้อกำหนดของ PDPA ภายในระยะเวลาที่กำหนด

2. การบังคับใช้ในฐานะ Data Processor

Data Processor เป็นผู้ที่ทำหน้าที่ประมวลผลข้อมูลส่วนบุคคลตามคำสั่งของ Data Controller ซึ่งการบังคับใช้ PDPA ในฐานะ Data Processor มีขั้นตอนสำคัญดังนี้

- **ปฏิบัติตามคำสั่งของ Data Controller:** Data Processor ต้องปฏิบัติตามคำสั่งของ Data Controller อย่างเคร่งครัดและไม่ประมวลผลข้อมูลส่วนบุคคลนอกเหนือจากที่ได้รับคำสั่ง

- **รักษาความปลอดภัยของข้อมูล:** Data Processor ต้องใช้มาตรการรักษาความปลอดภัยที่เหมาะสมเพื่อป้องกันการเข้าถึง การใช้ การเปิดเผย หรือการทำลายข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต
- **รักษาความปลอดภัยของข้อมูล:** Data Processor ต้องใช้มาตรการรักษาความปลอดภัยที่เหมาะสมเพื่อป้องกันการเข้าถึง การใช้ การเปิดเผย หรือการทำลายข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาต
- **ทำสัญญาการประมวลผลข้อมูล (Data Processing Agreement):** องค์กรในฐานะ Data Processor ต้องทำสัญญากับ Data Controller โดยสัญญานี้ต้องระบุถึงรายละเอียดของการประมวลผลข้อมูล ความรับผิดชอบของทั้งสองฝ่าย และมาตรการรักษาความปลอดภัย
- **การแจ้งเตือน Data Controller:** ในกรณีที่เกิดการละเมิดข้อมูลส่วนบุคคล Data Processor ต้องแจ้งให้ Data Controller ทราบทันทีเพื่อให้สามารถดำเนินการตามข้อกำหนดของ PDPA

การบังคับใช้ PDPA ทั้งในฐานะ Data Controller และ Data Processor จำเป็นต้องมีการทำความเข้าใจอย่างลึกซึ้งถึงบทบาทและความรับผิดชอบของแต่ละฝ่าย เพื่อให้การปฏิบัติงานเป็นไปตามกฎหมายและปกป้องข้อมูลส่วนบุคคลได้อย่างมีประสิทธิภาพ

บทลงโทษสำหรับการละเมิด PDPA

การลงโทษผู้กระทำความผิดใน PDPA สามารถแบ่งออกได้เป็น 3 ส่วนดังนี้

1. โทษทางแพ่ง: การชดใช้ค่าสินไหมทดแทนหรือการชดใช้เงินให้กับเจ้าของข้อมูลซึ่งได้รับความเสียหายจากการละเมิดข้อมูลส่วนบุคคล ตามมูลค่าของความเสียหายที่เกิดขึ้นจริง นอกจากนี้ ทางศาลอาจมีการเรียกให้ชดใช้ค่าสินไหมทดแทนเพิ่มอีกไม่เกินสองเท่าของมูลค่าค่าเสียหายที่เกิดขึ้นจริงกับเจ้าของข้อมูล

2. โทษทางอาญา: เป็นการลงโทษทั้งโดยการปรับเงินและจำคุก ซึ่งเป็นเหตุมาจากการใช้หรือเปิดเผยข้อมูลส่วนบุคคลที่ละเอียดอ่อนให้กับผู้อื่น หรือโอนย้ายข้อมูลส่วนบุคคลไปยังผู้อื่นในต่างประเทศ โทษทางอาญาได้กล่าวไว้ว่า ในกรณีที่ผู้กระทำความผิดเป็นนิติบุคคล อาจทำการดำเนินคดีกับกรรมการ ผู้บริหาร หรือผู้ที่มีส่วนรับผิดชอบในการดำเนินงานบริษัท

3. โทษทางปกครอง: เป็นโทษปรับเงินเนื่องจากการไม่ปฏิบัติตามหรือฝ่าฝืนกฎใน PDPA เช่น ละเลยการแจ้งเงื่อนไขการเก็บข้อมูลส่วนบุคคลต่อเจ้าของข้อมูล หรือการไม่อนุญาตให้เจ้าของข้อมูลเข้าถึงข้อมูลที่เคยให้ความยินยอมเก็บ รวบรวม ใช้

กรณีศึกษา:
การละเมิดข้อมูลส่วนบุคคลในประเทศไทย

แหล่งที่มา: https://www.naewna.com/local/743987

เมื่อวันที่ 15 ก.ค. 2566 ตำรวจได้จับกุม ผู้ต้องหาตามหมายจับศาลในข้อหา:

1. ทุจริตหลอกลวง นำข้อมูลคอมพิวเตอร์ที่บิดเบือนหรือปลอมเข้าสู่ระบบ
2. จัดให้มีการเล่นพนัน หรือชักชวนให้เล่นพนัน
3. ล่วงรู้และเปิดเผยข้อมูลส่วนบุคคลของผู้อื่น (พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 80)

โดยมีการกล่าวเพิ่มเติมว่า การกระทำดังกล่าวเป็นการกระทำที่ผิดกฎหมายหลายบท ซึ่งมีอัตราโทษจำคุกสูงสุดถึง 5 ปี อย่างเช่น พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 (PDPA) ซึ่งเป็นกฎหมายที่ป้องกันการละเมิดข้อมูลส่วนบุคคล รวมถึงการจัดเก็บและนำข้อมูลไปใช้โดยไม่ได้แจ้งให้ทราบและไม่ได้รับความยินยอมจากเจ้าของข้อมูลก่อน

กฎหมายคุ้มครองข้อมูลส่วนบุคคลของสหภาพยุโรป (General Data Protection Regulation: GDPR)

วัตถุประสงค์และหลักการของ GDPR

GDPR เป็นกฎหมายการคุ้มครองข้อมูลส่วนบุคคลในสหภาพยุโรปหรือ EU ซึ่งเป็นการคุ้มครองข้อมูล ความเป็นส่วนตัว และเศรษฐกิจในยุโรป กฎหมายนี้มีวัตถุประสงค์โดยรวมเพื่อปกป้องพลเมืองสภาพยุโรปจากการโดนละเมิดความเป็นส่วนตัว ทั้งนี้ยังมีวัตถุประสงค์ให้บริษัทมีความรับผิดชอบ ต่อการครอบครองและใช้ข้อมูลส่วนบุคคลของผู้บริโภค GDPR ถือได้ว่าเป็นกฎหมายด้านความเป็นส่วนตัวและความปลอดภัยที่เข้มงวดมากที่สุดในโลก และประเทศไทยได้นำแนวทางของ GDPR ในการกำหนดกฎหมาย PDPA ของประเทศ GDPR มีผลต่อใครหรือหน่วยงานใดก็ได้ทั่วโลกที่มีการเก็บข้อมูลของบุคคลในสหภาพยุโรป เนื่องด้วยอินเตอร์เน็ตที่ทำให้ผู้คนจากทั่วทุกมุมโลกเชื่อมต่อกันได้ง่ายยิ่งขึ้น กฎหมาย GDPR จึงมีโอกาสเกี่ยวข้องกับผู้คนต่าง ๆ ทั่วโลกได้มาก

การเปรียบเทียบระหว่าง PDPA และ GDPR

ด้านการเปรียบเทียบ	PDPA	GDPR
บุคคลที่กฎหมายบังคับใช้	เจ้าของข้อมูลในไทย และผู้ประมวลผลข้อมูลที่อยู่ในไทยและต่างประเทศ	การรับรู้อย่างจำกัดเกี่ยวกับความเสี่ยงด้านความปลอดภัยทางไซเบอร์ในระดับองค์กร
การบังคับใช้กฎหมาย	ยกเว้นบังคับใช้กับองค์กรนิติบัญญัติ เช่น วุฒิสภา สภาผู้แทนราษฎร	มีการรับรู้ความเสี่ยงด้านความปลอดภัยทางไซเบอร์ในระดับองค์กรแต่ยังไม่ได้ดำเนินการจัดตั้งแนวทางในการบริหารจัดการความเสี่ยงขององค์กร
คำจำกัดความของข้อมูลส่วนบุคคล และข้อมูลนิรนาม	• ไม่ได้ระบุว่าข้อมูลทางออนไลน์ อย่าง IP address Cookies เป็นข้อมูลส่วนบุคคล • กฎหมายกล่าวไว้ว่าเจ้าของข้อมูลส่วนบุคคลมีสิทธิขอให้ข้อมูลส่วนบุคคลของตนไม่สามารถระบุตัวตนได้ แต่ไม่ได้กล่าวว่า ข้อมูลที่ไม่สามารถระบุตัวตนจะถูกคุ้มครองหรือไม่	• ข้อมูลทางออนไลน์ อย่าง IP address Cookies ถือว่าเป็นข้อมูลส่วนบุคคล • กฎหมายไม่บังคับใช้กับข้อมูลที่ไม่สามารถระบุตัวตนได้
ข้อมูลส่วนบุคคลของผู้เยาว์	ไม่ได้คุ้มครองข้อมูลส่วนบุคคลของผู้เยาว์เป็นพิเศษ	คุ้มครองข้อมูลส่วนบุคคลของผู้เยาว์เป็นพิเศษ เช่นการเก็บข้อมูลของผู้เยาว์เพื่อวัตถุประสงค์ทางการตลาด
บันทึกการประมวลข้อมูล	ระบุว่าการทำและเก็บบันทึกรายการการประมวลผลข้อมูลเป็นไปตามที่คณะกรรมการประกาศ	มีการระบุสิ่งที่จะต้องอยู่ในบันทึกประมวลผลข้อมูล
บทลงโทษ	• ลงโทษทางแพ่งและปกครอง (เฉพาะค่าปรับ) • ลงโทษทางอาญา (มีทั้งแบบค่าปรับและแบบจำคุก)	มีโทษระดับรุนแรงและรุนแรงน้อยลงโดยระดับรุนแรงจะมีการปรับเงินมากกว่าระดับรุนแรงน้อยลง

ใน GDPR ค่าปรับจะขึ้นอยู่กับข้อกำหนดที่องค์กรละเมิดในกฎหมาย โดยที่การละเมิดความมั่นคงปลอดภัยข้อมูลจะตกอยู่ในโทษระดับที่ต่ำกว่า (ระดับรุนแรงน้อยลง) ในขณะที่การละเมิดสิทธิส่วนบุคคลต้องได้รับค่าปรับในระดับที่สูงขึ้น (ระดับรุนแรง)

กรณีศึกษา: การละเมิดข้อมูลส่วนบุคคล

ในเดือนพฤษภาคม ค.ศ. 2023 คณะกรรมการคุ้มครองข้อมูลของไอร์แลนด์ได้สั่งปรับผู้ให้บริการแพลตฟอร์มด้านโซเชียลมีเดียเป็นจำนวนเงิน 1.2 พันล้านดอลลาร์ เนื่องจากการโอนข้อมูลผู้ใช้ในยุโรปไปยังสหรัฐอเมริกาโดยไม่มีการป้องกันที่เพียงพอ นอกจากนี้ ยังถูกสั่งให้ระงับการโอนข้อมูลผู้ใช้ระหว่างสหภาพยุโรปและสหรัฐอเมริกาเป็นระยะเวลาหกเดือน

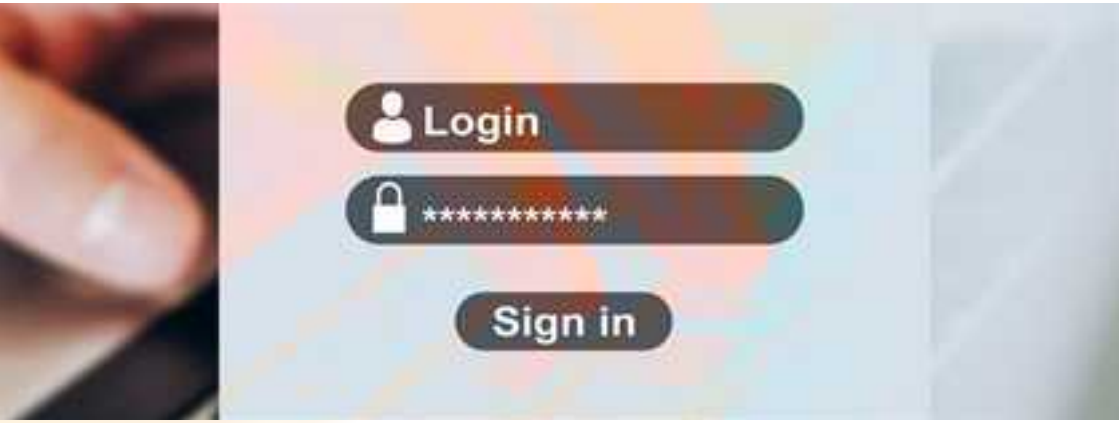
พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 (ฉบับที่ 2)

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 (ฉบับที่ 2) หรือพ.ร.บ.คอมพิวเตอร์ เป็นกฎหมายที่กำกับดูแลการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ซึ่งคำว่าคอมพิวเตอร์ ณ ที่นี้ สามารถประกอบไปด้วยคอมพิวเตอร์ตั้งโต๊ะ คอมพิวเตอร์โน้ตบุ๊ก สมาร์ตโฟน รวมถึงระบบต่าง ๆ ที่ถูกควบคุมด้วยระบบคอมพิวเตอร์ กฎหมายนี้มีจุดประสงค์เพื่อป้องกันและควบคุมการกระทำผิดที่เกิดขึ้นได้จากการใช้คอมพิวเตอร์ หากใครกระทำความผิดตามพ.ร.บ.คอมพิวเตอร์นี้ จะต้องได้รับการลงโทษตามที่กฎหมายได้กำหนดเอาไว้

ตัวอย่างการกระทำความผิดใน พ.ร.บ คอมพิวเตอร์

การเข้าถึงระบบคอมพิวเตอร์ของผู้อื่นในทางมิชอบ เช่น การแฮกเข้าไปดูข้อมูลของผู้อื่นหรือการล็อกอินเข้าสู่ระบบของผู้อื่น (ใส่ username และ password ของผู้นั้น) โดยไม่ได้รับอนุญาต

การนำไฟล์อันตรายเข้าสู่คอมพิวเตอร์ จนทำให้คอมพิวเตอร์เกิดความเสียหาย ยกตัวอย่าง การนำไวรัสเข้าสู่คอมพิวเตอร์ จึงทำให้เครื่องคอมพิวเตอร์เสียหาย



แหล่งที่มา: https://pixabay.com/photos/registration-log-in-keyboard-hand-3938434/

พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์เป็นกฎหมายกลางที่อนุญาตให้ข้อมูลทางอิเล็กทรอนิกส์มีผลบังคับใช้ได้ทางกฎหมาย โดยยึดตามหลักการความเท่าเทียมกัน (Functional Equivalence) ซึ่งมีความหมายว่า เอกสารในรูปแบบกระดาษและอิเล็กทรอนิกส์สามารถมีการบังคับใช้ได้ตามกฎหมายเหมือนกัน หลักความเป็นกลางทางเทคโนโลยี (Technological Neutrality) แปลว่า ถึงแม้ในอนาคตจะมีเทคโนโลยีดิจิทัลเกิดขึ้นใหม่ แต่กฎหมายนี้ก็ยังสามารถบังคับใช้กับเทคโนโลยีเหล่านั้นได้ และหลักเสรีภาพการแสดงเจตนา (Party Autonomy) ของคู่สัญญา

กฎหมายนี้เป็นส่วนหนึ่งของกฎหมายดิจิทัลในประเทศไทย โดยมีหน้าที่ในการออกนโยบายด้านดิจิทัล สร้างมาตรฐานและการอำนวยความสะดวกด้านดิจิทัล และสร้างระบบนิเวศที่น่าเชื่อถือและมั่นคงปลอดภัย

กฎหมายทรัพย์สินทางปัญญาที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศในประเทศไทย

ทรัพย์สินทางปัญญา คือ ผลงานที่เกิดจากการประดิษฐ์ คิดค้น หรือสร้างสรรค์ของมนุษย์ เน้นที่ผลผลิตของสติปัญญาและความชำนาญ ซึ่งสามารถเป็นได้ทั้งสิ่งที่จับต้องได้ เช่น สินค้า หรือสิ่งที่จับต้องไม่ได้ เช่น บริการ แนวคิดธุรกิจ หรือกรรมวิธีการผลิตในอุตสาหกรรม ทรัพย์สินทางปัญญาสามารถแบ่งออกได้เป็น 2 ประเภทได้แก่ ทั้ง 2 ประเภทมีกฎหมายในประเทศไทยคุ้มครอง

ลิขสิทธิ์

1. สิทธิพิเศษของเจ้าของลิขสิทธิ์ที่จะกระทำการใด ๆ กับงานที่สร้างสรรค์ขึ้น โดยไม่คำนึงถึงรูปแบบการแสดงออกของงานนั้น ประเภทของงานที่ได้รับการคุ้มครองลิขสิทธิ์ตามกฎหมาย ได้แก่ วรรณกรรม (รวมถึงโปรแกรมคอมพิวเตอร์) นาฏกรรม ศิลปกรรม ดนตรีกรรม โสตทัศนวัสดุ ภาพยนตร์ สิ่งบันทึกเสียง งานแพร่เสียงแพร่ภาพ งานอื่นใดในแผนกวรรณคดี แผนกวิทยาศาสตร์ หรือแผนกศิลปะ อายุการคุ้มครองลิขสิทธิ์ทั่วไป คือ ตลอดชีวิตของผู้สร้างสรรค์และอีก 50 ปีหลังจากผู้สร้างสรรค์เสียชีวิต

2. ในกรณีที่นิติบุคคลเป็นผู้สร้างสรรค์ ลิขสิทธิ์จะมีอายุ 50 ปีนับจากวันที่สร้างสรรค์งาน

3. ในกรณีที่ผู้สร้างสรรค์ใช้นามแฝงหรือไม่ปรากฏชื่อ ลิขสิทธิ์จะมีอายุ 50 ปีนับจากวันที่สร้างสรรค์งานนั้น

ที่มา: https://turnto10.com/news/entertainment/things-i-loved-in-2020-movies-books-music

ทรัพย์สินทางอุตสาหกรรม

1. ความคิดสร้างสรรค์ของมนุษย์ที่เกี่ยวกับสินค้าอุตสาหกรรมครอบคลุมทั้งการประดิษฐ์คิดค้นใหม่ ๆ การปรับปรุงกระบวนการหรือเทคนิคในการผลิต การออกแบบผลิตภัณฑ์ รวมถึงเครื่องหมายการค้า ความลับทางการค้า การคุ้มครองพันธุ์พืช แบบผังภูมิของวงจรรวม และสิ่งบ่งชี้ทางภูมิศาสตร์ ทรัพย์สินทางอุตสาหกรรมสามารถแบ่งออกได้หลายประเภท

- อายุการคุ้มครองเครื่องหมายการค้าที่จดทะเบียนแล้ว: 10 ปี ตั้งแต่วันที่ยื่นขอจดทะเบียน แล้วยังสามารถต่ออายุได้คราวละ 10 ปี

- อายุการคุ้มครองความลับทางการค้า: ระยะเวลาไม่ได้จำกัด ตราบเท่าที่ยังคงสภาพเป็นความลับทางการค้า

เครื่องหมายทางการค้า

ที่มา: https://research.mcmaster.ca/mcmaster-industry-liaison-office-milo/ip-education/intellectual-property-guides/what-is-a-trademark/

ตัวอย่างความลับทางการค้า: สูตรอาหาร

ที่มา: https://www.bbcgoodfood.com/recipes/collection/one-pot-recipes

เนื่องด้วยทรัพย์สินทางปัญญาต่าง ๆ สามารถอยู่ในรูปแบบของไฟล์บนระบบคอมพิวเตอร์ได้ การทราบถึงข้อมูลทางกฎหมายเบื้องต้นของทรัพย์สินทางปัญญา จะทำให้ผู้บริหารจัดการข้อมูลทางสารสนเทศทราบถึงขอบเขตของการกระทำต่อทรัพย์สินทางปัญญาโดยเบื้องต้นที่กฎหมายกำหนดไว้

สรุปท้ายบท Chapter 1

ความรู้พื้นฐานและกฎหมายที่เกี่ยวข้อง กับการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

ความสำคัญของ ISM ในยุคดิจิทัลที่ความปลอดภัยทางสารสนเทศเป็นสิ่งที่หลีกเลี่ยงไม่ได้ องค์ประกอบหลักของ ISM ได้แก่ ความลับ (Confidentiality) ความครบถ้วน (Integrity) และความพร้อมใช้งาน (Availability) ถูกนำเสนอเป็นส่วนสำคัญที่ต้องคำนึงถึงในการบริหารจัดการสารสนเทศ

นอกจากนี้ ยังได้กล่าวถึงมาตรฐานและกรอบการทำงานที่สำคัญ เช่น NIST Cybersecurity Framework และ ISO 27001 ซึ่งเป็นแนวทางปฏิบัติที่ช่วยให้องค์กรสามารถสร้างระบบความปลอดภัยสารสนเทศที่แข็งแกร่ง รวมถึงกฎหมายที่เกี่ยวข้องอย่างพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ และ PDPA ที่มีผลต่อการปฏิบัติในองค์กร

การระบุสินทรัพย์สารสนเทศและการจัดการความเสี่ยงเป็นอีกส่วนที่สำคัญ การรู้จักสินทรัพย์สารสนเทศทั้งประเภทและมูลค่าของมันช่วยให้องค์กรสามารถวางแผนและจัดการความเสี่ยงได้อย่างมีประสิทธิภาพ การประเมินความเสี่ยงทั้งเชิงคุณภาพและเชิงปริมาณ รวมถึงการจัดลำดับความเสี่ยง ทำให้สามารถบริหารจัดการความเสี่ยงได้ตรงจุดและมีประสิทธิผล

CHAPTER
2

การระบุสินทรัพย์สารสนเทศ

ทบทวนองค์ความรู้เรื่องสินทรัพย์สารสนเทศ (Information Asset)

สินทรัพย์สารสนเทศ (Information Asset) หมายถึงทรัพยากรต่าง ๆ ที่มีมูลค่าและสำคัญต่อการดำเนินธุรกิจขององค์กร ในยุคดิจิทัล สินทรัพย์สารสนเทศมีบทบาทสำคัญในการสร้างความได้เปรียบทางการแข่งขันและการรักษาความปลอดภัยของข้อมูล ประเภทของสินทรัพย์สารสนเทศที่องค์กรต้องให้ความสำคัญและจัดการอย่างมีประสิทธิภาพมีดังนี้

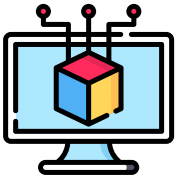
ข้อมูล (Data)

ข้อมูลเป็นสินทรัพย์ที่สำคัญที่สุดในหลายองค์กร ประกอบด้วย:

- **ข้อมูลส่วนบุคคล:** ข้อมูลเช่น ชื่อ ที่อยู่ เบอร์โทรศัพท์ เลขบัตรประชาชน หรือข้อมูลที่สามารถระบุตัวตนได้
- **ข้อมูลทางการเงิน:** ข้อมูลเกี่ยวกับการเงินขององค์กร เช่น รายงานการเงิน ข้อมูลการทำธุรกรรม บัญชีธนาคาร
- **ข้อมูลลูกค้า:** ข้อมูลเกี่ยวกับลูกค้า เช่น ประวัติการซื้อสินค้า ความต้องการ และข้อมูลติดต่อ

ซอฟต์แวร์ (Software)

ซอฟต์แวร์เป็นสินทรัพย์ที่สำคัญในการดำเนินงานขององค์กร ประกอบด้วย

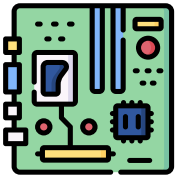


ระบบปฏิบัติการ: ระบบปฏิบัติการที่ใช้ในการจัดการและควบคุมการทำงานของฮาร์ดแวร์และซอฟต์แวร์อื่น ๆ

โปรแกรมประยุกต์: โปรแกรมที่ใช้ในการทำงานประจำวันเช่น ซอฟต์แวร์สำนักงาน ซอฟต์แวร์ทางธุรกิจ ระบบจัดการฐานข้อมูล

ฮาร์ดแวร์ (Hardware)

ฮาร์ดแวร์คืออุปกรณ์ทางกายภาพที่จำเป็นในการจัดเก็บและประมวลผลข้อมูล ประกอบด้วย



เซิร์ฟเวอร์: อุปกรณ์ที่ใช้ในการจัดเก็บข้อมูลและรันซอฟต์แวร์สำหรับองค์กร

คอมพิวเตอร์: อุปกรณ์ที่ใช้ในการทำงานประจำวันของพนักงาน

อุปกรณ์เครือข่าย: อุปกรณ์ที่ใช้ในการเชื่อมต่อและส่งข้อมูล เช่น เราเตอร์ สวิตช์

บริการ (Services)

บริการทางสารสนเทศเป็นองค์ประกอบสำคัญในการสนับสนุนการดำเนินงาน ประกอบด้วย

เว็บไซต์: แพลตฟอร์มออนไลน์ที่ใช้ในการสื่อสารและให้บริการกับลูกค้า

อีเมล: ระบบการสื่อสารที่ใช้ในการติดต่อประสานงานภายในและภายนอกองค์กร

บริการคลาวด์: การจัดเก็บและประมวลผลข้อมูลผ่านอินเทอร์เน็ต เช่น การสำรองข้อมูลและบริการซอฟต์แวร์บนคลาวด์

บุคลากร (People)

บุคลากรเป็นทรัพยากรที่สำคัญที่สุดในการจัดการและใช้ประโยชน์จากสินทรัพย์สารสนเทศ ประกอบด้วย

พนักงาน: บุคลากรภายในองค์กรที่มีบทบาทในการจัดการและใช้งานสินทรัพย์สารสนเทศ

ผู้รับเหมา: บุคคลภายนอกที่ได้รับการว่าจ้างให้ทำงานเฉพาะทาง เช่น การพัฒนาและบำรุงรักษาระบบ

การจัดการและปกป้องสินทรัพย์สารสนเทศเหล่านี้อย่างมีประสิทธิภาพเป็นสิ่งสำคัญในการรักษาความมั่นคงและความต่อเนื่องของธุรกิจ รวมถึงการรักษาความเชื่อมั่นจากลูกค้าและผู้มีส่วนได้ส่วนเสียอื่น ๆ ในยุคดิจิทัลนี้

วิธีการระบุและจัดประเภทสิน ทรัพย์สารสนเทศ

การระบุและจัดประเภทสินทรัพย์สารสนเทศ มีขั้นตอนดังนี้

1). การจัดหมวดหมู่และจัดทำป้ายชื่อข้อมูล

จัดทำทะเบียนข้อมูลสินทรัพย์สารสนเทศทั้งหมดที่องค์กรมี แบ่งตามหมวดหมู่ของสารสนเทศประเภทต่าง ๆ

2). การกำหนดชั้นความลับของสารสนเทศ

กำหนดเกณฑ์ในการจำแนกระดับชั้นความลับของข้อมูล โดยคำนึงถึงมูลค่า กฎหมาย และความละเอียดอ่อน พร้อมทั้งกำหนดรูปแบบในการจัดการให้เหมาะสมกับระดับชั้นความลับ

ลำดับชั้นความลับของข้อมูล สามารถจัดแบ่งได้ดังนี้

1. ข้อมูลลับที่สุด หมายถึง ข้อมูลที่หากเปิดเผยทั้งหมดหรือเพียงบางส่วน จะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด

2. ข้อมูลลับมาก หมายถึง ข้อมูลที่หากเปิดเผยทั้งหมดหรือเพียงบางส่วน จะก่อให้เกิดความเสียหายอย่างร้ายแรง

3. ข้อมูลลับ หมายถึง ข้อมูลที่หากเปิดเผยทั้งหมดหรือเพียงบางส่วน จะก่อให้เกิดความเสียหาย

4. ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

3). การกำหนดหน้าที่ความรับผิดชอบต่อสินทรัพย์องค์กร

ระบุผู้รับผิดชอบในการดูแลรักษาและปกป้องสินทรัพย์ข้อมูลแต่ละรายการ เพื่อควบคุมทะเบียนข้อมูลของสินทรัพย์ พร้อมทั้งรายงานการเคลื่อนย้าย หรือเปลี่ยนแปลงของสินทรัพย์

4). การจัดการและควบคุมการเข้าถึงสินทรัพย์

ข้อมูลลับจะต้องไม่ถูกเปิดเผยแก่บุคคลอื่น ยกเว้นในกรณีที่จำเป็นสำหรับการปฏิบัติงานเท่านั้น

ผู้ใช้งานต้องตระหนักถึงความสำคัญของการรักษาความปลอดภัย ของข้อมูลที่เก็บไว้ในเครื่องคอมพิวเตอร์ โดยเฉพาะอย่างยิ่งเครื่องที่ใช้งานร่วมกัน ข้อมูลลับเหล่านี้ต้องได้รับการปกป้องด้วยการเข้ารหัสหรือวิธีการอื่น ๆ ที่เหมาะสมจากระบบปฏิบัติการหรือระบบสารสนเทศ

เอกสารลับและสื่อบันทึกข้อมูลที่มีข้อมูลลับควรจัดเก็บในตู้ที่สามารถล็อกได้เมื่อไม่ใช้งาน โดยเฉพาะเมื่ออยู่นอกเวลาทำการ หรือเมื่อต้องทิ้งเอกสารหรือสื่อไว้โดยไม่มีการดูแล

ข้อมูลลับต้องถูกนำออกจากอุปกรณ์ประมวลผลต่าง ๆ เช่น เครื่องพิมพ์ เครื่องโทรสาร และเครื่องถ่ายเอกสาร ทันทีหลังจากใช้งานเสร็จ

เจ้าหน้าที่ต้องไม่เปิดเผยข้อมูลลับต่อบุคคลภายนอก ยกเว้นในกรณีที่การเปิดเผยนั้นอยู่ภายใต้ข้อตกลงการไม่เปิดเผยข้อมูล (NDA)

เจ้าหน้าที่ต้องหลีกเลี่ยงการพูดคุยหรือใช้งานข้อมูลลับ ในพื้นที่สาธารณะ เช่น ลิฟต์ หรือร้านอาหาร

สื่อบันทึกข้อมูลและอุปกรณ์คอมพิวเตอร์พกพาต่าง ๆ (เช่น PDA, USB-Drive, CD-ROM) ที่มีข้อมูลลับบันทึกอยู่ ต้องได้รับการดูแลรักษาและใช้งานอย่างระมัดระวัง

5). การจัดการสื่อที่ใช้บันทึกข้อมูล

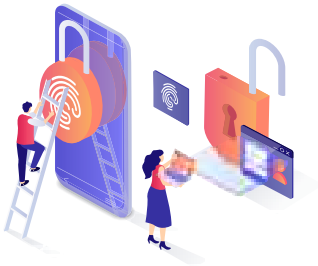
กำหนดให้มีกระบวนการจัดการสื่อบันทึกข้อมูล โดยมีการควบคุม การจัดเก็บ การเคลื่อนย้าย และการทำลายสื่อบันทึกข้อมูล

การบริหารจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้: ต้องมีการจัดทำขั้นตอนที่สอดคล้องกับวิธีการจัดชั้นความลับของสารสนเทศที่องค์กรกำหนดไว้ โดยสื่อบันทึกข้อมูลต้องได้รับการป้องกันจากการเข้าถึงโดยไม่ได้รับอนุญาต การนำไปใช้ผิดวัตถุประสงค์ หรือความเสียหายระหว่างการส่งหรือขนย้าย และต้องปฏิบัติตามเอกสารคู่มือการปฏิบัติงานเรื่องการลงทะเบียนสื่อเคลื่อนที่และสอบทานการใช้งาน

การเคลื่อนย้ายสื่อบันทึกข้อมูล: ต้องมีวิธีการจัดส่งสื่อบันทึกข้อมูลให้มีความมั่นคงปลอดภัย โดยปฏิบัติตามวิธีปฏิบัติงานเรื่องการส่งผ่านสื่อบันทึกข้อมูล (Physical Media In Transit)

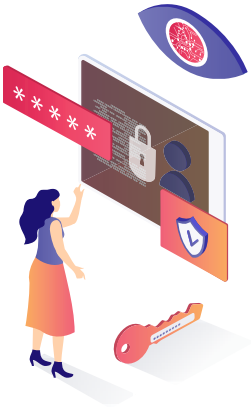
การทำลายสื่อบันทึกข้อมูล: ปฏิบัติตามวิธีปฏิบัติงานเรื่องการทำลายสื่อบันทึกข้อมูลและข้อมูลบนสื่อบันทึกข้อมูล (Disposal of media procedure) ซึ่งการทำลายเอกสารและสื่อที่ใช้ในการบันทึกข้อมูลจะต้องได้รับการอนุมัติจากเจ้าของข้อมูล และควรทำลายภายใต้สิ่งแวดล้อมที่มีการควบคุม

การประเมินมูลค่าและความสำคัญของสินทรัพย์สารสนเทศ



การประเมินมูลค่า

กระบวนการที่กำหนดมูลค่าทางการเงินหรือมูลค่าทางธุรกิจของสินทรัพย์นั้น ๆ เพื่อช่วยให้องค์กรสามารถจัดการทรัพยากรได้อย่างมีประสิทธิภาพ



การประเมินมูลค่าทางบัญชี: พิจารณามูลค่าทางบัญชีของสินทรัพย์ตามราคาซื้อขายและการเสื่อมราคา

การประเมินมูลค่าตลาด: พิจารณามูลค่าของสินทรัพย์หากมีการซื้อขายในตลาด

การประเมินมูลค่าทางการเงิน: พิจารณามูลค่าทางการเงินที่สินทรัพย์นั้นสร้างให้กับองค์กร เช่น รายได้หรือการลดค่าใช้จ่าย

การวิเคราะห์ต้นทุน-ผลประโยชน์: เปรียบเทียบต้นทุนของการป้องกันและรักษาความปลอดภัยสินทรัพย์กับผลประโยชน์ที่ได้รับจากการป้องกัน

การประเมินความสำคัญ

การพิจารณาถึงบทบาทและผลกระทบของสินทรัพย์นั้นต่อการดำเนินงานขององค์กร โดยมีขั้นตอนดังนี้

การจัดลำดับความสำคัญ: จัดลำดับสินทรัพย์สารสนเทศตามความสำคัญต่อธุรกิจ เช่น ข้อมูลที่สำคัญต่อการดำเนินงานประจำวัน ข้อมูลที่ต้องปฏิบัติตามข้อกำหนดทางกฎหมาย และข้อมูลที่มีมูลค่าทางการเงินสูง

การประเมินผลกระทบทางธุรกิจ (Business Impact Analysis): ประเมินผลกระทบต่อธุรกิจหากสินทรัพย์สารสนเทศถูกทำลาย สูญหาย หรือถูกโจมตี

การประเมินความสำคัญเชิงกลยุทธ์: พิจารณาบทบาทของสินทรัพย์ในแผนการระยะยาวและกลยุทธ์ขององค์กร

การพิจารณาผลกระทบ

การประเมินผลกระทบที่อาจเกิดขึ้นหากสินทรัพย์ข้อมูลสูญหาย ถูกทำลาย หรือถูกเปิดเผย มีขั้นตอนดังนี้

การวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis - BIA): วิเคราะห์และประเมินผลกระทบที่เกิดขึ้นต่อการดำเนินธุรกิจขององค์กร เช่นผลกระทบทางการเงิน ผลกระทบต่อภาพลักษณ์ขององค์กร และผลกระทบต่อการปฏิบัติตามข้อกำหนดทางกฎหมาย

การวิเคราะห์ความเสี่ยง (Risk Analysis): ประเมินโอกาสที่สินทรัพย์จะถูกโจมตีหรือสูญหาย รวมถึงผลกระทบที่จะเกิดขึ้นเมื่อเกิดเหตุการณ์ไม่พึงประสงค์

การกำหนดมาตรการป้องกันและลดความเสี่ยง: กำหนดมาตรการเพื่อป้องกันและลดความเสี่ยงที่เกี่ยวข้องกับสินทรัพย์สารสนเทศ เช่น การใช้ระบบสำรองข้อมูล การรักษาความปลอดภัยเครือข่าย และการอบรมพนักงานเกี่ยวกับการรักษาความปลอดภัยข้อมูล

การจัดทำแผนบริหารความต่อเนื่อง (Business Continuity Plan - BCP): จัดทำแผนฟื้นฟูความสามารถในการดำเนินงานเมื่อเกิดเหตุการณ์ที่มีผลกระทบต่อสินทรัพย์สารสนเทศ เช่น การกู้คืนข้อมูลและระบบภายในระยะเวลาที่กำหนด

การจัดทำทะเบียนสินทรัพย์สารสนเทศ (Asset Inventory)

วัตถุประสงค์ของการทำ Asset Inventory

ยืนยันการมีอยู่จริงของสินทรัพย์: การจัดทำทะเบียนสินทรัพย์แสดงให้เห็นว่ากิจการมีระบบควบคุมสินทรัพย์ที่มีประสิทธิภาพ โดยควรมีการตรวจนับสินทรัพย์อย่างน้อยปีละครั้ง เพื่อเสริมสร้างระบบการควบคุมภายในที่ดี

ป้องกันการทุจริตและปรับปรุงทะเบียนสินทรัพย์ให้ตรงกับความเป็นจริง: การจัดทำและตรวจนับสินทรัพย์ตามทะเบียนช่วยป้องกันการทุจริตหรือการสูญหายของสินทรัพย์ อีกทั้งยังแสดงถึงการใช้งานสินทรัพย์ที่เกี่ยวข้องกับกิจการ

อำนวยความสะดวกในการตรวจสอบและค้นหาสินทรัพย์: การระบุตำแหน่งที่ตั้งของสินทรัพย์ในทะเบียน ทำให้การค้นหาและนำมาใช้สะดวกยิ่งขึ้น

ความถูกต้องในการคำนวณค่าเสื่อมราคา: การจัดทำทะเบียนและตรวจนับสินทรัพย์อย่างครบถ้วน ช่วยให้การคำนวณค่าเสื่อมราคามีความถูกต้องลดความผิดพลาดและปัญหาที่อาจเกิดขึ้นในภายหลัง

องค์ประกอบของทะเบียนสินทรัพย์สารสนเทศ

ที่มา: prosofterp, ขึ้นทะเบียนทรัพย์สิน

ชื่อสินทรัพย์: รายละเอียดของสินทรัพย์ เช่น ชื่อหรือหมายเลข
ประเภทของสินทรัพย์: เช่น ฮาร์ดแวร์ ซอฟต์แวร์ ข้อมูล หรือทรัพยากรอื่น ๆ
ตำแหน่งที่ตั้ง: ที่อยู่ทางกายภาพหรือที่ตั้งในเครือข่าย
เจ้าของสินทรัพย์: บุคคลหรือหน่วยงานที่รับผิดชอบต่อสินทรัพย์นั้น
วันเริ่มต้นและวันหมดอายุ: วันที่เริ่มใช้งานและวันที่คาดว่าจะหมดอายุ
สถานะของสินทรัพย์: เช่น กำลังใช้งาน ไม่ได้ใช้งาน กำลังบำรุงรักษา ฯลฯ
มูลค่าของสินทรัพย์: ราคาหรือมูลค่าที่ประเมินไว้
ข้อมูลการบำรุงรักษา: ประวัติการบำรุงรักษาและการซ่อมแซม
การรับประกัน: ข้อมูลเกี่ยวกับการรับประกันของสินทรัพย์
หมายเหตุเพิ่มเติม: ข้อมูลเพิ่มเติมที่เกี่ยวข้องกับสินทรัพย์

วิธีการจัดทำทะเบียนสินทรัพย์สารสนเทศ

จัดสินทรัพย์ตามประเภทและกำหนดรหัสสินทรัพย์: เริ่มต้นโดยการจัดกลุ่มสินทรัพย์ตามประเภท (Fixed Asset Group) และกำหนดรหัสสินทรัพย์ (Fixed Asset Number) โดยระบุทั้งกลุ่มสินทรัพย์และ Running Number ตามลำดับวันที่ซื้อสินทรัพย์

ระบุข้อมูลสำคัญของสินทรัพย์: ระบุชื่อสินทรัพย์ (Asset Name) ชื่อย่อหรือนามแฝง (Asset Name Alias) สถานที่ตั้งของสินทรัพย์ (Location) และผู้รับผิดชอบสินทรัพย์ เพื่อให้สะดวกต่อการค้นหาเมื่อมีการตรวจนับ

บันทึกข้อมูลการใช้งานและค่าเสื่อมราคา: บันทึกวันที่เริ่มใช้งานสินทรัพย์ สถานะของสินทรัพย์ ข้อมูลการบำรุงรักษา อ้างอิงเลขที่เอกสารใบแจ้งหนี้ที่ซื้อสินทรัพย์ วิธีคิดค่าเสื่อมราคา อัตราค่าเสื่อมราคา วันที่เริ่มคิดค่าเสื่อมราคา ราคาทุนของสินทรัพย์ รวมถึงค่าเสื่อมราคาและค่าเสื่อมราคาสะสม

คำนวณมูลค่าตามบัญชีคงเหลือ: คำนวณมูลค่าตามบัญชีคงเหลือ (Net Book Value) โดยหักค่าเสื่อมราคาสะสมจากราคาทุน ซึ่งมูลค่าตามบัญชีคงเหลือในทะเบียนสินทรัพย์ทั้งหมดควรเท่ากับมูลค่าตามบัญชีคงเหลือในบัญชีแยกประเภท เพื่อยืนยันความครบถ้วนของการบันทึกบัญชี

จัดทำฉลากและรายงานแสดงข้อมูลสินทรัพย์: จัดทำฉลาก (Tags) ติดกำกับที่สินทรัพย์ เพื่ออำนวยความสะดวกในการค้นหาและตรวจสอบสินทรัพย์

กำหนดการตรวจนับสินทรัพย์ประจำปี: กำหนดให้มีการตรวจนับสินทรัพย์อย่างน้อยปีละหนึ่งครั้ง เพื่อยืนยันความมีตัวตนของสินทรัพย์และเสริมสร้างระบบการควบคุมภายในที่ดี

การปรับปรุง Asset Inventory

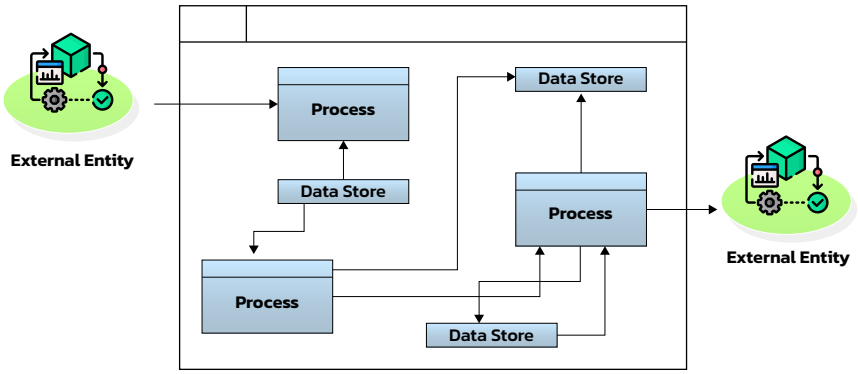
ตรวจนับสินทรัพย์เป็นประจำ: ดำเนินการตรวจนับสินทรัพย์อย่างสม่ำเสมออย่างน้อยปีละหนึ่งครั้ง เพื่ออัปเดตข้อมูลในทะเบียนให้ถูกต้องและเป็นปัจจุบัน

แก้ไขข้อมูลที่ผิดพลาด: ตรวจสอบและแก้ไขข้อมูลที่ผิดพลาด พร้อมทั้งปรับปรุงรายละเอียดของสินทรัพย์ที่มีการเปลี่ยนแปลง

เพิ่มและลบข้อมูลสินทรัพย์: บันทึกข้อมูลสินทรัพย์ใหม่ที่ได้รับเข้ามาในระบบและลบข้อมูลสินทรัพย์ที่ได้จำหน่ายออกไป

การทำแผนผังความสัมพันธ์ของสินทรัพย์ข้อมูล (Data Flow Diagram)

แผนผังความสัมพันธ์ของสินทรัพย์ข้อมูล (Data Flow Diagram) คืออะไร



ที่มา: www.eternalsunshineoftheismind.wordpress.com, Data Flow Diagrams

Data Flow Diagram (DFD) คือ แผนภาพที่ใช้แสดงการไหลของข้อมูลภายในระบบ โดยจะแสดงแหล่งที่มาของข้อมูล จุดที่ข้อมูลถูกส่งไป กิจกรรมที่เกิดขึ้นกับข้อมูลในแต่ละขั้นตอนของระบบ และจุดที่ข้อมูลถูกนำไปจัดเก็บ DFD เป็นเครื่องมือที่ช่วยให้เห็นภาพรวมการไหลของข้อมูลเพื่อใช้ในการวิเคราะห์และออกแบบระบบอย่างมีประสิทธิภาพ

ประโยชน์ของ Data Flow Diagram

สามารถใช้งานได้อย่างอิสระโดยไม่ต้องพึ่งพาเทคนิคอื่น ๆ เนื่องจากสามารถใช้สัญลักษณ์ต่าง ๆ แทนสิ่งที่วิเคราะห์มา

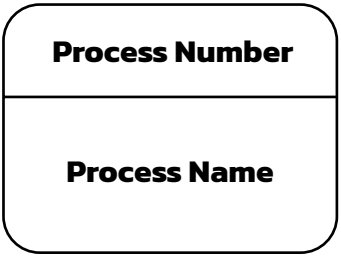
เป็นสื่อที่ง่ายต่อการแสดงความสัมพันธ์ระหว่างระบบใหญ่ และระบบย่อย โดยแสดงข้อมูลที่ซับซ้อนในรูปแบบแผนภาพที่เข้าใจง่าย ทำให้ผู้ที่ไม่เชี่ยวชาญด้านเทคนิคสามารถเข้าใจได้ดี

ช่วยในการวิเคราะห์ระบบได้อย่างง่ายดายและชัดเจน โดยสร้างความเข้าใจตรงกันระหว่างผู้วิเคราะห์ระบบ โปรแกรมเมอร์ และผู้ใช้

ช่วยกำหนดขอบเขต จุดเริ่มต้น และจุดสิ้นสุดของระบบ ทำให้สามารถวางแผนและจัดการระบบได้อย่างมีประสิทธิภาพ

สัญลักษณ์ที่ใช้ใน Data Flow Diagram

การประมวลผล (Process)



การประมวลผล (Process) คือ กระบวนการทำงานของระบบ หรือขั้นตอนการดำเนินงาน เพื่อตอบสนองข้อมูลที่รับเข้า (Input) หรือเงื่อนไขที่เกิดขึ้น เป็นการเปลี่ยนแปลงข้อมูลจากรูปแบบหนึ่ง (Input) ไปเป็นอีกรูปแบบหนึ่ง (Output) อาจดำเนินการทำงานจากบุคคล หน่วยงาน หุ่นยนต์ หรือเครื่องคอมพิวเตอร์ เป็นต้น

การใช้สัญลักษณ์

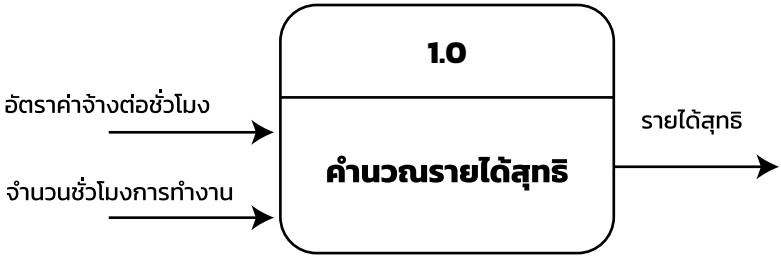
1. ต้องใช้สัญลักษณ์การประมวลผล (Process) คู่กับ สัญลักษณ์กระแสข้อมูล (Data Flow) เสมอ โดยที่ลูกศรชี้เข้าหมายถึงเป็นข้อมูลนำเข้า (Input) ลูกศรชี้ออกหมายถึงเป็นข้อมูลออกจากการประมวลผล (Output) ซึ่ง 1 Process สามารถมีข้อมูลนำเข้ามากกว่า 1 เส้น หรือข้อมูลออกมากกว่า 1 เส้นได้

2. การตั้งชื่อของ Process ควรเป็นวลีเดียวที่อธิบายการทำงานทั้งหมดได้ และควรอธิบายการทำงานอย่างใดอย่างหนึ่งโดยเฉพาะมากกว่าที่จะอธิบายการทำงานอย่างกว้าง ๆ

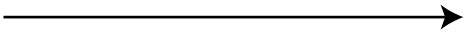
3. แต่ละ Process จะมีแต่ข้อมูลเข้าอย่างเดียว หรือข้อมูลออกอย่างเดียวไม่ได้

ตัวอย่าง

การคำนวณรายได้สุทธิของลูกจ้างรายวัน จะต้องประกอบด้วยข้อมูลนำเข้าที่เป็น “อัตราค่าจ้างต่อชั่วโมง” และ “จำนวนชั่วโมงการทำงาน” เมื่อผ่านการประมวลผลแล้วจะได้ “รายได้สุทธิ”

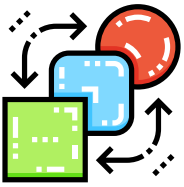


กระแสข้อมูล (Data Flow)



กระแสข้อมูล (Data Flow) เป็นเส้นทางในการไหลของข้อมูลจากส่วนหนึ่งไปยังอีกส่วนหนึ่งของระบบสารสนเทศ โดยจะมีลูกศรแสดงการไหลจากปลายลูกศรไปยังหัวลูกศรซึ่งข้อมูลที่ปรากฏบนเส้นนี้จะเป็นได้ทั้งข้อความ ตัวเลข รายการเรคคอร์ดที่ระบบคอมพิวเตอร์สามารถนำไปประมวลผลได้

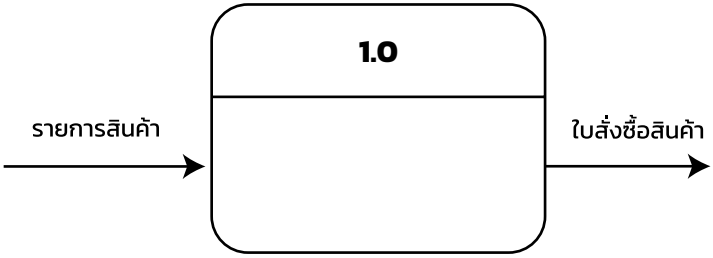
การใช้สัญลักษณ์



1. การตั้งชื่อกระแสข้อมูล โดยทั่วไปจะตั้งด้วยคำเพียงคำเดียวที่มีความหมายชัดเจนและเข้าใจง่าย ควรกำกับชื่อบนเส้นด้วยคำนาม เช่น เวลาทำงาน ใบสั่งซื้อสินค้า เป็นต้น
2. กระแสข้อมูลที่ผ่านการประมวลผลแล้วจะมีการเปลี่ยนแปลงไป ดังนั้นจึงควรตั้งชื่อให้แตกต่างกัน

ตัวอย่าง

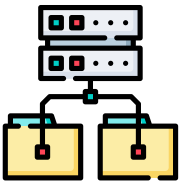
กระแสข้อมูลนำเข้า คือ “รายการสินค้า” และกระแสข้อมูลหลังผ่านการประมวณผล คือ “ใบสั่งซื้อสินค้า”



แหล่งจัดเก็บข้อมูล (Data Store)

แหล่งจัดเก็บข้อมูล (Data Store) เป็นส่วนที่ใช้แทนชื่อไฟล์หรือแฟ้ม ที่ใช้จัดเก็บข้อมูลในฐานข้อมูลเพื่อนำไปใช้ภายหลัง แหล่งจัดเก็บข้อมูลจะต้องมีทั้งข้อมูลเข้าและข้อมูลออก โดยข้อมูลที่ไหลออกจะอยู่ในลักษณะที่ถูกอ่านขึ้นมา ส่วนข้อมูลที่ไหลเข้าจะอยู่ในรูปของการบันทึก การเพิ่ม-ลบ แก้ไข

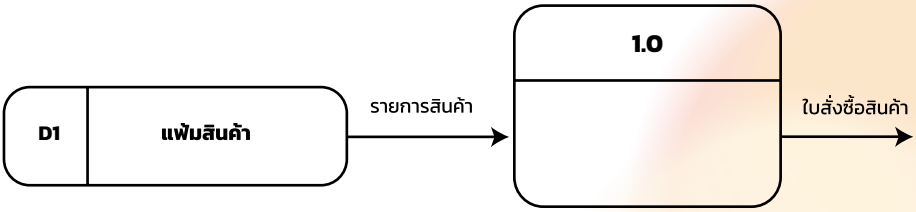
การใช้สัญลักษณ์



1. Data Store ต้องเชื่อมต่อ การประมวลผล (Process) เสมอ โดยเชื่อมผ่าน กระแสข้อมูล (Data Flow)
2. ใช้อักษรย่อ D1, D2 เป็นต้น เขียนด้านซ้ายมือของสัญลักษณ์ เพื่อแสดงว่าเป็นแหล่งเก็บข้อมูลอันที่เท่าใด โดยสามารถเขียนซ้ำในระดับต่าง ๆ ของแผนภาพกระแสข้อมูลได้

ตัวอย่าง:

“รายการสินค้า” (Data Flow) ถูกอ่านขึ้นมาจาก “แฟ้มสินค้า” (Data Store)



สิ่งที่อยู่ภายนอก (External Entity)

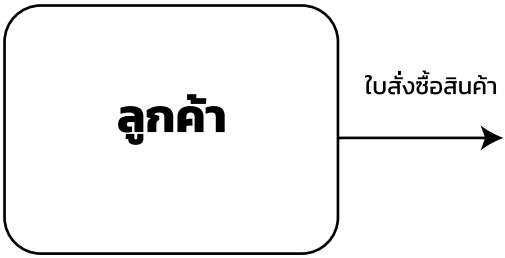
External Entity หมายถึง บุคคล หน่วยงานภายในองค์กร หน่วยงานภายนอกองค์กร หรือระบบงานอื่นที่อยู่ภายนอกขอบเขตของระบบงาน แต่มีความสัมพันธ์กับระบบ มีการส่งข้อมูลเข้าระบบเพื่อดำเนินงาน รับข้อมูลที่ผ่านการดำเนินงานจากระบบ เป็นต้น

การใช้สัญลักษณ์

1. ข้อมูลจาก External Entity หนึ่งไม่สามารถส่งไปยังอีก External Entity หนึ่งโดยตรงได้ ต้องผ่าน Process ก่อน
2. ต้องใช้คำนามในการตั้งชื่อ External Entity เสมอ

ตัวอย่าง:

“ลูกค้า” เป็นบุคคลภายนอกที่มีความสัมพันธ์กับระบบ



วิธีการสร้างแผนผังความสัมพันธ์ของสินทรัพย์ข้อมูล

1. กำหนดรายการกิจกรรมของธุรกิจ: รวบรวมและจำแนกรายการกิจกรรมต่าง ๆ ของธุรกิจ โดยระบุว่ากิจกรรมเหล่านั้นอยู่ในรูปแบบใด เช่น External Entities, Data Flows, Processes หรือ Data Stores

2. สร้างแผนภาพระดับสูงสุด (Context Diagram): แสดง External Entities และข้อมูลที่ไหลเข้าและออกจากระบบหลัก โดยไม่สนใจแหล่งเก็บข้อมูล

3. สร้างแผนภาพระดับถัดไป (Diagram 0 หรือ Parent Diagram): แสดง Process ต่าง ๆ ที่มีอยู่ในรูปแบบทั่วไป พร้อมแสดง Data Stores ในระดับนี้ด้วย

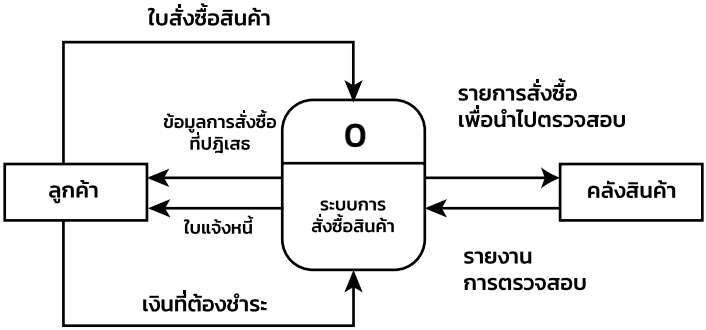
4. สร้างแผนภาพระดับลูกของแต่ละ Process ใน Diagram 0 (Level-1 Diagram): หากมีรายละเอียดของการทำงานย่อยในระดับนี้ ให้สร้างแผนภาพกระแสข้อมูลในระดับถัดไป เช่น Level-2 Diagram, Level-3 Diagram จนกระทั่งครบทุกระดับ

5. ตรวจสอบข้อผิดพลาด: ตรวจสอบคำกำกับบนเส้น Data Flow และ Process แต่ละอันว่า มีความหมายและถูกต้องหรือไม่

6. ตรวจสอบสมดุลข้อมูล: ตรวจสอบสมดุลระหว่างข้อมูลเข้าและออกของแผนภาพ DFD กับ Context Diagram

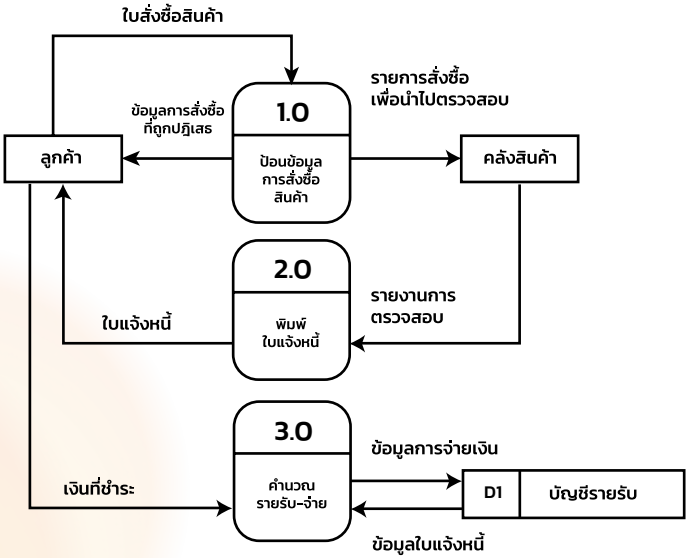
กรณีศึกษา: การสร้าง Data Flow Diagram สารสนเทศ/ข้อมูลขององค์กร

ตัวอย่างการเขียน Context Diagram ของระบบการสั่งซื้อสินค้า



ที่มา: Chiang Mai University, บทที่ 4 แผนภาพกระแสข้อมูล (Data Flow Diagram)

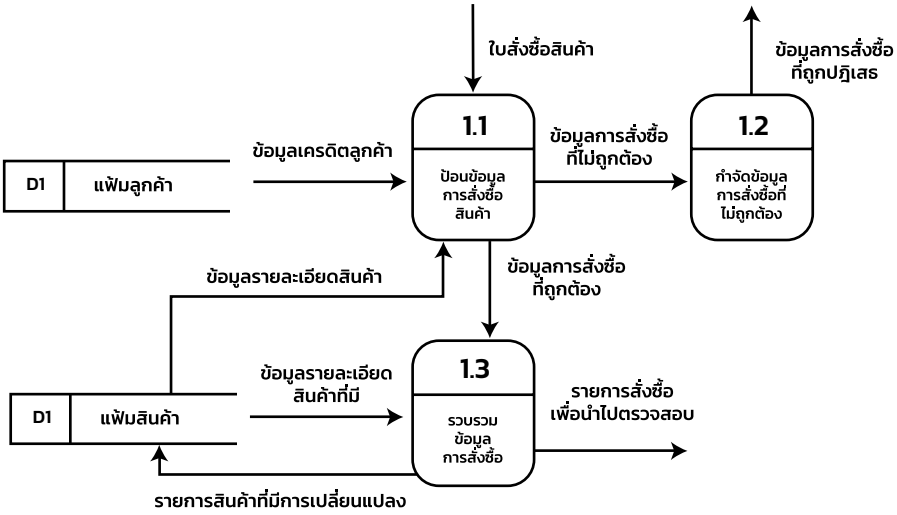
ตัวอย่างการเขียน Level-0 Diagram ของระบบการสั่งซื้อสินค้า



ที่มา: Chiang Mai University, บทที่ 4 แผนภาพกระแสข้อมูล (Data Flow Diagram)

ตัวอย่างการเขียน Child Diagram (Level-1) ของ Process 1.0

การป้อนข้อมูลการสั่งซื้อ



ที่มา: Chiang Mai University, บทที่ 4 แผนภาพกระแสข้อมูล (Data Flow Diagram)

หลังจากการสร้าง Data Flow Diagram (DFD) เสร็จสิ้น เราจะมีภาพรวมที่ชัดเจนเกี่ยวกับการไหลของข้อมูลภายในองค์กร DFD ช่วยให้เราเข้าใจว่าข้อมูลถูกประมวลผลที่ใด แหล่งข้อมูลมาจากไหน และข้อมูลถูกส่งต่อไปยังที่ใด การมีแผนภาพนี้ไม่เพียงแต่ช่วยให้เรามองเห็นกระบวนการและช่องทางการไหลของข้อมูล แต่ยังช่วยระบุจุดที่อาจเป็นช่องโหว่หรือมีความเสี่ยงได้อย่างชัดเจน

การระบุพื้นผิวการโจมตีขององค์กร (Attack Surface)

ด้วยข้อมูลจากการระบุสินทรัพย์และ DFD เราจึงสามารถดำเนินการสู่ขั้นตอนต่อไปที่สำคัญ นั่นคือ การระบุพื้นผิวการโจมตีขององค์กร ซึ่งจะช่วยให้เราทราบถึงจุดที่อาจเป็นช่องโหว่และมีความเสี่ยงต่อการถูกโจมตี รวมถึงการเตรียมมาตรการในการป้องกันและลดความเสี่ยงจากภัยคุกคามต่าง ๆ

พื้นผิวการโจมตีแบ่งออกเป็น 2 ส่วนคือ

1. ภายนอก: ครอบคลุมสถานะออนไลน์ขององค์กร เช่น เว็บไซต์ เว็บแอปพลิเคชัน และระบบที่เชื่อมต่ออินเทอร์เน็ตอื่น ๆ ซึ่งเป็นจุดเริ่มต้นที่เป็นไปได้สำหรับการโจมตีไซเบอร์

2. ภายใน: ประกอบด้วยระบบเครือข่าย เซิร์ฟเวอร์ อุปกรณ์ปลายทาง แอปพลิเคชัน และฐานข้อมูลทั้งหมดในองค์กร ช่องโหว่ในส่วนประกอบเหล่านี้อาจถูกใช้เพื่อเข้าถึงข้อมูลสำคัญ

ทรัพย์สินเฉพาะที่เป็นส่วนหนึ่งของพื้นผิวการโจมตีขององค์กรได้แก่:

ที่มา: https://sellaismk.shop/product_details/9931692.html

1. ที่อยู่ IP สาธารณะและโดเมน
2. เซิร์ฟเวอร์อีเมลและบัญชีผู้ใช้
3. VPN และระบบการเข้าถึงระยะไกล
4. ไฟร์วอลล์ เราเตอร์ และโครงสร้างพื้นฐานเครือข่าย
5. ระบบควบคุมการเข้าออกทางกายภาพ
6. อุปกรณ์ปลายทางของพนักงาน เช่น แล็ปท็อป เดสก์ท็อป และอุปกรณ์เคลื่อนที่
7. แอปพลิเคชันภายในและฐานข้อมูล
8. โครงสร้างพื้นฐานและบริการคลาวด์
9. อุปกรณ์ IoT และ OT

สรุปท้ายบท Chapter 2

การระบุสินทรัพย์สารสนเทศ

การอธิบายความหมายของสินทรัพย์สารสนเทศ ประเภทของสินทรัพย์สารสนเทศ เช่น ข้อมูล (Data) ซอฟต์แวร์ (Software) ฮาร์ดแวร์ (Hardware) วิธีการระบุและจัดประเภทสินทรัพย์สารสนเทศ การประเมินมูลค่าและความสำคัญของสินทรัพย์ การจัดทำทะเบียนสินทรัพย์สารสนเทศ (Asset Inventory) และการทำแผนผังความสัมพันธ์ของสินทรัพย์สารสนเทศ (Data Flow Diagram)

โดยการระบุและการจัดการสินทรัพย์สารสนเทศอย่างมีประสิทธิภาพช่วยให้องค์กรสามารถรักษาความปลอดภัยของข้อมูลสำคัญ ป้องกันการรั่วไหลของข้อมูล และลดความเสี่ยงที่เกี่ยวข้องกับการดำเนินธุรกิจ นอกจากนี้ยังเป็นพื้นฐานที่สำคัญในการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศในองค์กรอย่างมีประสิทธิภาพ โดยเน้นถึงความสำคัญของการทำทะเบียนสินทรัพย์สารสนเทศ (Asset Inventory) และการทำแผนผังความสัมพันธ์ของสินทรัพย์สารสนเทศ

CHAPTER
3

แนวทางการวิเคราะห์และการจัดการความเสี่ยง

แนวทางการประเมินความเสี่ยง (Risk Assessment)

ความเสี่ยง (Risk) = ความรุนแรง (Impact) x ความเป็นไปได้ (Likelihood)

แนวทางการประเมินความเสี่ยง คือ แนวทางการวิเคราะห์และจัดลำดับความเสี่ยงที่จะเกิดขึ้น โดยพิจารณาจากโอกาสที่จะเกิดความเสี่ยง และความรุนแรงของผลกระทบจากความเสี่ยงที่จะเกิดขึ้น ต่อการบรรลุวัตถุประสงค์ของกระบวนการทำงานขององค์กรหรือหน่วยงานนั้น ๆ โดยแนวทางการประเมินเพื่อระบุความเสี่ยงสามารถแบ่งได้เป็น 2 ประเภท ดังนี้

วิธีการประเมินความเสี่ยง แบ่งออกเป็น 2 ประเภท คือ เชิงคุณภาพและเชิงปริมาณ

การประเมินความเสี่ยงเชิงคุณภาพ (Qualitative Risk Assessment)

การประเมินความเสี่ยงเชิงคุณภาพคืออะไร

การประเมินความเสี่ยงเชิงคุณภาพ คือ การระบุและประเมินความเสี่ยงโดยใช้การตัดสินและประสบการณ์ของผู้เชี่ยวชาญ เน้นการอธิบายปรากฏการณ์ทางสังคมศาสตร์และมานุษยวิทยา โดยมุ่งเน้นความหลากหลายและความครอบคลุมของข้อมูลและวิธีการเข้าถึงข้อมูล แทนที่จะใช้การตรวจวัดทางวิทยาศาสตร์หรือการเก็บข้อมูลสถิติเชิงตัวเลข กระบวนการเก็บข้อมูลทางสังคมที่ใช้ประกอบด้วย:

1. การสัมภาษณ์เจาะลึก (In-depth Interview)
2. การสัมภาษณ์เฉพาะกลุ่ม (Focus Group Interview)
3. การใช้แบบสอบถาม (Questionnaire)
4. การศึกษาแบบมีส่วนร่วม (Participatory Action Research)

การประเมินความเสี่ยงเชิงคุณภาพมักจะมีการกำหนดค่าตัวเลขให้กับระดับความเสี่ยงที่แตกต่างกัน เช่น การใช้เมทริกซ์ความเสี่ยง ซึ่งวิธีนี้ไม่ได้เปลี่ยนการประเมินความเสี่ยงเชิงคุณภาพให้เป็นการประเมินเชิงปริมาณ หากการประเมินความเสี่ยงยังคงขึ้นอยู่กับวิจารณญาณของผู้ประเมินในการกำหนดค่าความเสี่ยง ก็ยังคงถือเป็นการประเมินเชิงคุณภาพอยู่

วิธีการประเมินความเสี่ยงเชิงคุณภาพ

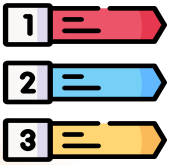
การประเมินความเสี่ยงเชิงคุณภาพจะมีการจัดลำดับความเสี่ยงตามระดับความรุนแรง เช่น สูง ปานกลาง ต่ำ โดยพิจารณาจากผลกระทบอันเนื่องมาจากความเสี่ยง (Impact) และโอกาสที่จะเกิดเหตุการณ์ความเสี่ยง (Likelihood) ตามวิจารณญาณส่วนบุคคลและความเชี่ยวชาญของผู้ประเมิน

ตัวอย่าง ระดับโอกาสในการเกิดเหตุการณ์ต่างๆ (Likelihood) เชิงคุณภาพ		
ระดับ	โอกาสที่จะเกิด	คำอธิบาย
1.	สูงมาก	มีโอกาสในการเกิดเกือบทุกครั้ง
2.	สูง	มีโอกาสในการเกิดค่อนข้างสูงหรือบ่อย ๆ
3.	ปานกลาง	มีโอกาสเกิดบางครั้ง
4.	น้อย	อาจมีโอกาสเกิด แต่นาน ๆ ครั้ง
5.	น้อยมาก	มีโอกาสเกิดในกรณียกเว้น

ตัวอย่าง: การประเมินความเสี่ยงจากการโจมตีแบบ Phishing โดยพิจารณาจากความน่าจะเป็นที่จะเกิดขึ้นและผลกระทบต่อชื่อเสียงขององค์กร

ตัวอย่างการใช้งาน

ระดับความน่าจะเป็น

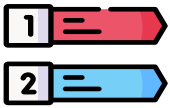


(สูงมาก): มีอีเมลฟิชชิงส่งเข้ามาทุกวัน
(สูง): มีอีเมลฟิชชิงส่งเข้ามาทุกสัปดาห์
(ปานกลาง): มีอีเมลฟิชชิงส่งเข้ามาทุกเดือน
(น้อย): มีอีเมลฟิชชิงส่งเข้ามาทุกไตรมาส
(น้อยมาก): มีอีเมลฟิชชิงส่งเข้ามาทุกปี

ระดับผลกระทบ

(สูงมาก): ทำให้ชื่อเสียงองค์กรเสียหายอย่างรุนแรง และต้องมีการกู้คืนข้อมูลที่เสียหาย
(สูง): มีการละเมิดข้อมูลบางส่วนและเกิดความเสียหาย ต่อชื่อเสียงองค์กร
(ปานกลาง): มีการละเมิดข้อมูลเล็กน้อยและเกิดผลกระทบต่อชื่อเสียงบางส่วน
(น้อย): มีการละเมิดข้อมูลแต่ไม่มีผลกระทบต่อชื่อเสียง
(น้อยมาก): ไม่มีการละเมิดข้อมูลและไม่มีผลกระทบต่อชื่อเสียง

การประเมิน:



ความน่าจะเป็น: 4 (สูง) – มีอีเมลฟิชชิงส่งเข้ามาทุกสัปดาห์

ผลกระทบ: 5 (สูงมาก) – ทำให้ชื่อเสียงองค์กรเสียหายอย่างรุนแรง

ผลการประเมิน:

ความเสี่ยงจากการโจมตีแบบ Phishing นี้จะถูกจัดอยู่ในระดับ สูง เนื่องจากมีโอกาสเกิดขึ้นสูงและส่งผลกระทบมากต่อชื่อเสียงองค์กร

มาตรการควบคุม:

- อบรมพนักงานเรื่องการตรวจจับอีเมลฟิชชิง
- ใช้ระบบกรองอีเมลที่มีประสิทธิภาพ
- ทำการทดสอบ Phishing Simulation เป็นระยะ

การประเมินความเสี่ยงเชิงปริมาณ (Quantitative Risk Assessment)

การประเมินความเสี่ยงเชิงปริมาณคืออะไร

การประเมินความเสี่ยงเชิงปริมาณเป็นการประเมินที่อาศัยข้อมูลเชิงสถิติและหลักการทางวิทยาศาสตร์ โดยใช้ค่าตัวเลขในการอธิบายความเสี่ยงต่าง ๆ ตามข้อมูลที่สามารถวัดได้ เช่น ต้นทุน การขนส่ง ระยะเวลาที่ใช้ในการดำเนินงาน และวันลาป่วยของพนักงาน เป็นต้น การประเมินความเสี่ยงเชิงปริมาณนี้มักจะดำเนินการหลังจากการประเมินความเสี่ยงเชิงคุณภาพ เพื่อเป็นวิธีการเพิ่มเติมในการประเมินความเสี่ยงที่มีความสำคัญสูงสุด

การใช้แนวทางเชิงวิทยาศาสตร์นี้ช่วยให้การตัดสินใจใด ๆ สามารถอธิบายและชี้แจงให้ผู้มีส่วนได้ส่วนเสียเข้าใจได้ง่ายขึ้น นอกจากนี้ความชัดเจนของการจัดอันดับเชิงตัวเลขยังทำให้สามารถวางแผนและคำนวณต้นทุนได้อย่างแม่นยำและมีประสิทธิภาพมากยิ่งขึ้นอีกด้วย

วิธีการประเมินความเสี่ยงเชิงปริมาณ

การประเมินความเสี่ยงเชิงปริมาณเป็นกระบวนการที่ใช้สูตรต่าง ๆ เพื่อคำนวณค่าความเสี่ยง ซึ่งสามารถทำได้ด้วยวิธีการต่าง ๆ ดังนี้:

1. Single Loss Expectancy (SLE)

SLE หมายถึง มูลค่าการสูญเสียที่คาดว่าจะเกิดขึ้นต่อครั้งหากเกิดเหตุการณ์ความเสี่ยงนั้น ๆ ขึ้น

สูตรคำนวณ: SLE = Asset Value (ค่าทรัพย์สิน) × Exposure Factor (อัตราความเสี่ยงที่ถูกกำหนด)

2. Annual Loss Expectancy (ALE)

ALE หมายถึง มูลค่าความสูญเสียที่คาดว่าจะเกิดขึ้นต่อปีจากเหตุการณ์ความเสี่ยงนั้น ๆ

สูตรคำนวณ: ALE = SLE × Annual Rate of Occurrence (อัตราการเกิดเหตุต่อปี)

ตัวอย่าง: การประเมินความเสี่ยงจากการเกิดไฟไหม้ในศูนย์ข้อมูล โดยคำนวณความน่าจะเป็นที่จะเกิดขึ้นและมูลค่าความเสียหายที่อาจเกิดขึ้น

ตัวอย่างการใช้งาน

สมมติว่าค่าทรัพย์สิน (Asset Value) คือ 30,000,000 บาท
อัตราความเสี่ยงที่ถูกกำหนด (Exposure Factor) คือ 50% (หรือ 0.5)
อัตราการเกิดเหตุต่อปี (Annual Rate of Occurrence, ARO) คือ 0.05 (หรือ 5% หรือ 1 เหตุการณ์ต่อปี)

ขั้นตอนการคำนวณ

1. คำนวณ SLE: SLE = 30,000,000 × 0.5 = 15,000,000 บาท

2. คำนวณ ALE: ALE = 15,000,000 × 0.05 = 750,000 บาท

ดังนั้น ALE ในกรณีนี้คือ 750,000 ซึ่งหมายถึงค่าความสูญเสียที่องค์กรคาดว่าจะเสียไปในแต่ละปี หากเกิดเหตุการณ์ที่เสียหายขึ้น การคำนวณนี้ช่วยให้ผู้บริหารสามารถประเมินความเสี่ยงทางการเงินและวางแผนการจัดการความเสี่ยงได้อย่างมีระบบและเป็นรูปธรรมในองค์กร

กระบวนการวิเคราะห์ความเสี่ยง (Risk Analysis)

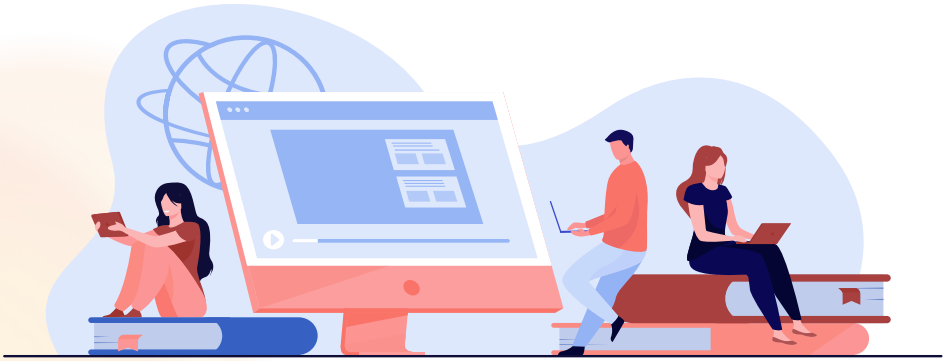
การระบุสินทรัพย์: ระบุสินทรัพย์ข้อมูลที่สำคัญและประเมินมูลค่า เพื่อให้เข้าใจถึงความสำคัญและคุณค่าของสินทรัพย์เหล่านั้นในบริบทขององค์กร โดยคำนึงถึงทั้งข้อมูลที่จับต้องได้ เช่น ฮาร์ดแวร์ และข้อมูลที่จับต้องไม่ได้ เช่น ข้อมูลทางการเงินหรือข้อมูลลูกค้า

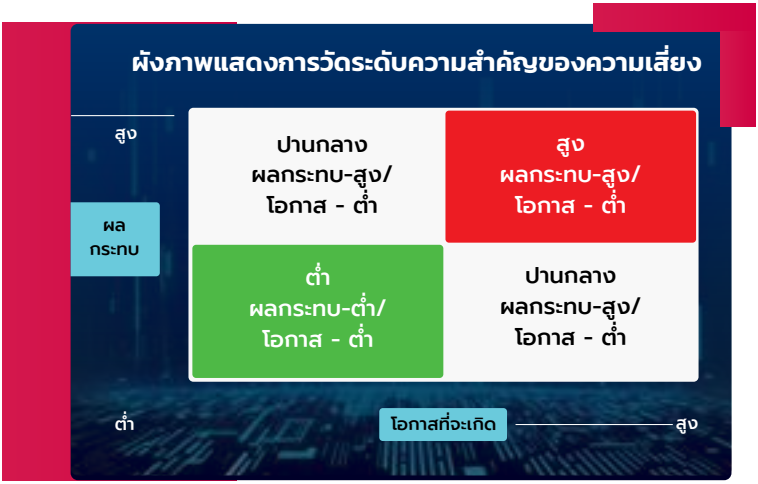
การระบุภัยคุกคาม: ระบุภัยคุกคามที่อาจเกิดขึ้นกับสินทรัพย์ ซึ่งอาจมาจากหลายแหล่ง ทั้งภัยคุกคามภายในองค์กร เช่น การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต หรือภัยคุกคามภายนอก เช่น การโจมตีจากแฮกเกอร์ โดยการวิเคราะห์ภัยคุกคามนี้ควรอิงตามข้อมูลที่เป็นปัจจุบันและเหตุการณ์จริงที่เคยเกิดขึ้น

การประเมินช่องโหว่: ประเมินจุดอ่อนในระบบหรือกระบวนการที่อาจถูกภัยคุกคามใช้ประโยชน์ โดยการตรวจสอบและวิเคราะห์ช่องโหว่ควรครอบคลุมทั้งด้านเทคนิค เช่น การตั้งค่าระบบที่ไม่ปลอดภัย และด้านกระบวนการ เช่น ขั้นตอนการจัดการข้อมูลที่ไม่รัดกุม

การประเมินความเสี่ยง: ประเมินโอกาสที่จะเกิดความเสี่ยงและผลกระทบที่อาจเกิดขึ้น เพื่อให้ทราบถึงระดับความเสี่ยงที่แต่ละภัยคุกคามนำมาสู่ โดยใช้วิธีการวิเคราะห์เชิงปริมาณและเชิงคุณภาพในการประเมิน เพื่อให้ได้ข้อมูลที่แม่นยำและสามารถนำไปใช้ได้จริง

การจัดลำดับความเสี่ยง: จัดลำดับความเสี่ยงตามระดับความสำคัญและผลกระทบ เพื่อวางแผนการจัดการความเสี่ยงอย่างมีประสิทธิภาพและเน้นการป้องกันความเสี่ยงที่มีความสำคัญสูงสุดก่อน การจัดลำดับนี้ ควรใช้เครื่องมืออย่าง Risk Matrix เพื่อให้สามารถมองเห็นและจัดการความเสี่ยงได้อย่างชัดเจนและเป็นระบบ





ที่มา: SlidePlayer, วัตถุประสงค์ในการเรียนรู้

การจัดลำดับความเสี่ยงตามระดับความสำคัญ สามารถแบ่งออกเป็น 4 ระดับ ดังนี้

E-Extreme Risk: ความเสี่ยงระดับสูงสุดต้องมีแผนการจัดการที่แน่นอนไว้รองรับ

H-High Risk: ความเสี่ยงระดับสูง ต้องมีการเตรียมการ เตรียมแผนการจัดการไว้รองรับ

M-Moderate Risk: ความเสี่ยงระดับกลาง ควรติดตามความเสี่ยงเป็นระยะ เพื่อวางแผนการจัดการ

L-Low Risk: ความเสี่ยงระดับต่ำ อาจยอมรับความเสี่ยงไว้ได้ หรือคอยติดตามระบุระดับความเสี่ยงเป็นระยะ เพราะความเสี่ยงระดับต่ำอาจเพิ่มระดับความรุนแรงกลายเป็นความเสี่ยงระดับกลางหรือสูงได้

การประเมินความเสี่ยงโดยใช้เมทริกซ์ความเสี่ยง (Risk Matrix)

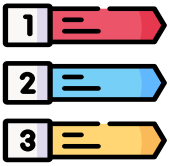
เมทริกซ์ความเสี่ยงคืออะไร

เมทริกซ์ความเสี่ยง หรือ Risk Matrix คือ ตารางที่ใช้เป็นเครื่องมือประเมินระดับความเสี่ยง โดยพิจารณาจากปัจจัยด้านโอกาสในการเกิดความเสี่ยงและความรุนแรงจากผลของความเสี่ยง เพื่อจัดลำดับความรุนแรงความเสี่ยงที่องค์กรต้องเผชิญและช่วยเลือกวิธีการบริหารความเสี่ยงที่เหมาะสมกับแต่ละปัจจัยต่อไป

วิธีการประเมินความเสี่ยงโดยใช้เมทริกซ์ความเสี่ยง

1. พิจารณาโอกาสที่จะเกิด (Likelihood) ผลกระทบ (Impact) และระดับความเสี่ยง (Degree of Risk) ของความเสี่ยงนั้น ๆ

โอกาสที่จะเกิด (Likelihood: L) หมายถึง ความถี่หรือโอกาสที่จะเกิดเหตุการณ์ความเสี่ยง ซึ่งจำแนกเป็น 5 ระดับ คือ



ระดับ 1 หมายถึง ความเสี่ยงนั้นมีโอกาสการเกิดน้อยมาก
ระดับ 2 หมายถึง ความเสี่ยงนั้นมีโอกาสการเกิดน้อย
ระดับ 3 หมายถึง ความเสี่ยงนั้นมีโอกาสการเกิดปานกลาง
ระดับ 4 หมายถึง ความเสี่ยงนั้นมีโอกาสการเกิดสูง
ระดับ 5 หมายถึง ความเสี่ยงนั้นมีโอกาสการเกิดสูงมาก

ผลกระทบ (Impact: I) หมายถึง ขนาดความรุนแรงของความเสียหายที่จะเกิดขึ้นหากเกิดเหตุการณ์ความเสี่ยง จำแนกเป็น 5 ระดับ คือ

ระดับ 1 หมายถึง ผลกระทบของความเสี่ยงต่อองค์กรมีน้อยมาก
ระดับ 2 หมายถึง ผลกระทบของความเสี่ยงต่อองค์กรมีน้อย
ระดับ 3 หมายถึง ผลกระทบของความเสี่ยงต่อองค์กรมีปานกลาง
ระดับ 4 หมายถึง ผลกระทบของความเสี่ยงต่อองค์กรมีสูง
ระดับ 5 หมายถึง ผลกระทบของความเสี่ยงต่อองค์กรมีสูงมาก

ระดับความเสี่ยง (Degree of Risk: D) หมายถึง สถานะของความเสี่ยงที่ได้จากการประเมินโอกาสและผลกระทบของแต่ละปัจจัยเสี่ยง

คำนวณได้จากสูตรดังต่อไปนี้:

ระดับความเสี่ยง (D) = ระดับผลกระทบ (I) x ระดับโอกาสที่จะเกิด (L)

ซึ่งระดับความเสี่ยงแบ่งตามความสำคัญเป็น 4 ระดับ ดังนี้

ระดับความเสี่ยง	ระดับคะแนน	ความหมาย
สูงมาก (Extreme)	17-25	ระดับที่ไม่สามารถยอมรับได้ จำเป็นต้องเร่งจัดการความเสี่ยงในทันทีเพื่อให้ความเสี่ยงต่ำลง และอยู่ในระดับที่ยอมรับได้ในที่สุด
สูง (High)	10-16	ระดับที่ไม่สามารถยอมรับได้ โดยต้องระเฝ้าระวัง และจัดการความเสี่ยงเพื่อให้อยู่ในระดับที่ยอมรับได้ต่อไป
ปานกลาง (Medium)	6-9	ระดับที่พอยอมรับได้ แต่ต้องใช้ความพยายามที่จะลดความเสี่ยงที่จะลดความเสี่ยงให้อยู่ในระดับที่น้อยลงต่อไป
น้อย (Low)	1-5	ระดับที่ยอมรับได้ โดยใช้วิธีควบคุมปกติในขั้นตอนการปฏิบัติงานที่กำหนด และติดตามระดับความเสี่ยงตลอดระยะเวลาการปฏิบัติงาน

ที่มา: depa, การประเมินความเสี่ยงและการจัดการความเสี่ยง ประจำปี 2564

2. จัดวางแต่ละความเสี่ยงลงใน Risk Matrix ซึ่งจะช่วยให้สามารถมองเห็นระดับความเสี่ยงได้ชัดเจนขึ้น เป็นประโยชน์ในการวางแผนจัดการและลดความเสี่ยงตามลำดับความสำคัญ นอกจากนี้ยังช่วยในการวิเคราะห์ความเสี่ยงเพื่อหาแนวทางเตรียมรับมือก่อนที่ความเสี่ยงนั้นจะเกิดขึ้นจริง

ผลกระทบ \ โอกาส	เกิดขึ้นยาก (1)	เกิดขึ้นน้อย (2)	เกิดขึ้นบ้าง (3)	เกิดขึ้นสูง (4)	เกิดขึ้นสูงมาก (5)	
สูงมาก (5)	5	10	15	20	25	ระดับความเสี่ยงที่ไม่สามารถยอมรับได้
สูง (4)	4	8	12	16	20	
ปลานกลาง (3)	3	6	9	12	15	
น้อย (2)	2	4	6	9	10	มาตรการควบคุมความเสี่ยง
น้อยมาก (1)	1	2	3	4	5	ยอมรับได้

	ระดับความเสี่ยง 17-25 คะแนน	(สูงมาก)	ต้องกำกับดูแลอย่างใกล้ชิด
	ระดับความเสี่ยง 10-16 คะแนน	(สูง)	ต้องเฝ้าระวัง
	ระดับความเสี่ยง 6-9 คะแนน	(ปลานกลาง)	ต้องกำกับดูแลอย่างใกล้ชิด
	ระดับความเสี่ยง 1-5 คะแนน	(ต่ำ)	ต้องกำกับดูแลอย่างใกล้ชิด

ที่มา: depa, การประเมินความเสี่ยงและการจัดการความเสี่ยง ประจำปี 2564

จากตัวอย่าง ความเสี่ยงตั้งแต่ระดับคะแนน 10 - 25 จะได้รับพิจารณาคัดเลือกเพื่อนำมาเข้าสู่กระบวนการบริหารจัดการความเสี่ยง เพื่อจัดการและควบคุมความเสี่ยงให้ลดลง ส่วนความเสี่ยงในระดับคะแนน 9 และต่ำกว่า จะถือว่าเป็นความเสี่ยงที่สามารถยอมรับได้

การบริหารจัดการความเสี่ยง (Risk Management)

ความหมายของการบริหารจัดการความเสี่ยงในบริบทของความมั่นคงปลอดภัยสารสนเทศ

การบริหารจัดการความเสี่ยงในบริบทของความมั่นคงปลอดภัยสารสนเทศ หมายถึง กระบวนการหรือกิจกรรมที่เน้นการรับรู้ การประเมิน การทบทวน และการจัดการความเสี่ยงที่เกี่ยวข้องกับความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศภายในองค์กร เป็นกระบวนการที่ช่วยสร้างความสมดุลของต้นทุนเชิงเศรษฐศาสตร์และการดำเนินธุรกิจ ระหว่างมาตรการในการป้องกันและการบรรลุผลสำเร็จของพันธกิจ ด้วยการปกป้องระบบเทคโนโลยีสารสนเทศและข้อมูลสำคัญ ซึ่งจะช่วยสนับสนุนความสำเร็จของการบรรลุพันธกิจขององค์กร

กระบวนการการจัดการความเสี่ยง

การลดและควบคุมความเสี่ยง (Risk Reduction, Control):

การลดความเสี่ยง หรือการควบคุมความเสี่ยง เป็นการปรับปรุงระบบการทำงานหรือการออกแบบวิธีการทำงานใหม่ เพื่อลดโอกาสที่จะเกิดหรือลดผลกระทบให้อยู่ในระดับที่องค์กรยอมรับได้ เช่น การจัดทำคู่มือการปฏิบัติงาน การฝึกอบรมบุคลากรให้มีความรู้เพียงพอ การติดตั้งเครื่องดับเพลิง การ back up ข้อมูลเป็นระยะ ๆ การมี server สำรอง เป็นต้น

การกระจายและถ่ายโอนความเสี่ยง (Risk Sharing, Transfer):

การกระจายความเสี่ยง หรือการโอนความเสี่ยง เป็นการให้ผู้อื่นช่วยแบ่งเบาความรับผิดชอบในความเสี่ยงไป เช่น การจ้างบุคคลภายนอกดำเนินการแทน (Outsource) การซื้อกรมธรรม์ประกันภัย การจ้างเหมาและเหมาช่วง เป็นต้น

กระกระทำนี้ไม่ได้เป็นการลดความเสี่ยงที่จะเกิดขึ้น แต่เป็นการรับประกันว่าเมื่อเกิดความเสียหายขึ้น องค์กรจะได้รับการชดใช้จากผู้อื่น

การหลีกเลี่ยงความเสี่ยง (Risk Avoidance):
การหลีกเลี่ยงความเสี่ยง คือการหลีกเลี่ยงหรือหยุดการกระทำที่ก่อให้เกิดความเสี่ยง เช่น งานส่วนใดที่องค์กรไม่ถนัด อาจหลีกเลี่ยงหรือหยุดการทำงานในส่วนนั้น และอาจใช้การ Outsource แทน
ข้อเสียคือ อาจส่งผลกระทบให้เกิดการเปลี่ยนแปลงในแผนงานขององค์กรมากจนเกินไปจนไม่สามารถมุ่งไปสู่เป้าหมายที่วางไว้ได้

การยอมรับความเสี่ยง (Risk Acceptance):
หากความเสียหายจากปัจจัยเสี่ยงมีระดับต่ำพอที่จะยอมรับได้ หรือหากพบว่าไม่มีวิธีการจัดการความเสี่ยงใดที่เหมาะสม เนื่องจากต้นทุนหรือค่าใช้จ่ายในการจัดการความเสี่ยงมีราคาสูงกว่าประโยชน์ที่ได้รับ อาจจะต้องยอมรับความเสี่ยงนั้น แต่ควรมีมาตรการติดตามอย่างใกล้ชิดเพื่อรองรับผลกระทบที่อาจเกิดขึ้นได้

ตัวอย่าง: กรณีศึกษาเรื่องการจัดการความเสี่ยงของธุรกิจปริวรรตเงินตราต่างประเทศในจังหวัดสงขลา

ตัวอย่างความเสี่ยงที่มีระดับความเสี่ยงอยู่ในระดับมาก ซึ่งเป็นความเสี่ยงที่น่าสนใจและควรได้รับการควบคุม เพื่อไม่ให้ส่งผลเสียหายกับกิจการเพิ่มขึ้น สามารถอธิบายได้ ดังนี้

1. ความเสี่ยงจากคู่แข่งขันทางธุรกิจ เดิมกิจการส่วนใหญ่ใช้วิธีการยอมรับความเสี่ยงที่จะเกิดขึ้น

คำแนะนำ: กิจการสามารถควบคุมความเสี่ยงโดยสร้างสัมพันธ์ที่ดีกับคู่ค้า เพื่อเป็นการสร้างเครือข่ายความสัมพันธ์ และมีกลยุทธ์ในการดึงดูดลูกค้า เช่น เสนอขายเงินตราต่างประเทศ กรณีลูกค้าต้องการเดินทางไปต่างประเทศเพื่อประหยัดเวลา

2. ความเสี่ยงด้านความปลอดภัยของเงินสดและทรัพย์สิน เดิมกิจการควบคุมความเสี่ยงโดยการติดกล้องวงจรปิด เก็บเงินเข้าตู้นิรภัย และทำลูกกรงเหล็กเพื่อป้องกันการโจรกรรมเป็นบางราย

คำแนะนำ: กิจการควรแบ่งแยกหน้าที่ความรับผิดชอบในการรับเงินและการบันทึกบัญชีให้ชัดเจน กำหนดให้มีการตรวจยอดเงินกับหลักฐานการรับเงินทุกครั้ง วิธีการเก็บเงินเข้าตู้นิรภัยต้องมีลูกกุญแจอย่างน้อยสองดอก และตั้งอยู่ในที่ลับตาคน หรือในบางกิจการจะใช้วิธีการฝากเงินเข้าธนาคารเพื่อลดความเสี่ยงจากการถูกโจรกรรม

การติดตาม ทบทวน และปรับปรุงกระบวนการจัดการความเสี่ยง (Risk Monitoring, Review and Improvement)

การติดตามความเสี่ยง:

หลังจากจัดทำแผนบริหารความเสี่ยงและมีการดำเนินงานตามแผนแล้ว จะต้องมีการรายงานและติดตามผลเป็นระยะ เพื่อประเมินคุณภาพและความเหมาะสมของวิธีการจัดการความเสี่ยง รวมทั้งติดตามผลการจัดการความเสี่ยงที่ได้มีการดำเนินการไปแล้วว่าบรรลุผลตามวัตถุประสงค์ของการบริหารความเสี่ยงหรือไม่ เพื่อรายงานผลต่อผู้บริหารต่อไป

การติดตามความเสี่ยงสามารถทำได้ใน 2 ลักษณะ คือ

- **การติดตามผลเป็นรายครั้ง (Separate Monitoring):** เป็นการติดตามตามรอบระยะเวลาที่กำหนด เช่น ทุก 3, 6, 9 เดือน หรือทุกสิ้นปี เป็นต้น
- **การติดตามผลในระหว่างการปฏิบัติงาน (Ongoing Monitoring):** เป็นการติดตามที่รวมอยู่ในการดำเนินงานต่าง ๆ ตามปกติของหน่วยงาน

การทบทวนความเสี่ยง:

การทบทวนแผนบริหารความเสี่ยง เป็นการทบทวนประสิทธิภาพของแนวการบริหารความเสี่ยงในทุกขั้นตอน เพื่อการปรับปรุงและพัฒนาแผนงานในการบริหารความเสี่ยงให้ทันสมัยและเหมาะสมกับการปฏิบัติงานจริงเป็นประจำทุกปี

สรุปท้ายบท Chapter 3

แนวทางการวิเคราะห์และการจัดการความเสี่ยง

แนวทางการวิเคราะห์และการจัดการความเสี่ยง ซึ่งเป็นขั้นตอนที่สำคัญในการรักษาความมั่นคงปลอดภัยของสารสนเทศในองค์กร โดยกระบวนการประเมินความเสี่ยงถูกแบ่งออกเป็นสองประเภทหลัก คือ การประเมินเชิงคุณภาพ (Qualitative Risk Assessment) และการประเมินเชิงปริมาณ (Quantitative Risk Assessment) ทั้งสองวิธีนี้ช่วยให้องค์กรสามารถระบุความเสี่ยง ประเมินผลกระทบ และความเป็นไปได้ที่จะเกิดขึ้นได้อย่างเป็นระบบ ในบทนี้ยังได้กล่าวถึงกระบวนการวิเคราะห์ความเสี่ยงที่รวมถึงการระบุสินทรัพย์และภัยคุกคาม การประเมินช่องโหว่ การประเมินความเสี่ยง และการจัดลำดับความเสี่ยง การใช้เมทริกซ์ความเสี่ยง (Risk Matrix) เป็นเครื่องมือสำคัญที่ช่วยให้การประเมินความเสี่ยงมีความแม่นยำและชัดเจนมากขึ้น นอกจากนี้ยังมีแนวคิดการจัดการความเสี่ยงทางสารสนเทศ กระบวนการและวิธีการจัดการความเสี่ยงที่สามารถนำไปใช้ได้จริงในองค์กร

การติดตาม ทบทวน และปรับปรุงกระบวนการจัดการความเสี่ยงเป็นขั้นตอนสุดท้ายที่สำคัญ เพื่อให้มั่นใจว่าการจัดการความเสี่ยงในองค์กรเป็นไปอย่างต่อเนื่องและมีประสิทธิภาพ การสร้างความตระหนักรู้และการฝึกอบรมพนักงานให้เข้าใจถึงความสำคัญของความปลอดภัยสารสนเทศเป็นอีกหนึ่งองค์ประกอบที่ช่วยเสริมสร้างความปลอดภัยขององค์กรในระยะยาว

MODULE 02

การป้องกันสารสนเทศและการสร้างความตระหนักรู้ด้านความปลอดภัยสารสนเทศ

(Information Security Protection and Awareness) #Protect

วัตถุประสงค์

เพื่อให้ผู้เข้ารับการฝึกอบรมมีความรู้ความเข้าใจ เกี่ยวกับหลักการพื้นฐานของการจัดการความมั่นคงปลอดภัยสารสนเทศ แนวคิดและมาตรฐานที่เกี่ยวข้อง ภัยคุกคามและแนวโน้ม กฎหมายและข้อบังคับต่าง ๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศในประเทศไทยและต่างประเทศ โดยสามารถนำความรู้จากบทเรียนไปประยุกต์ใช้ในการออกแบบนโยบายการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

CHAPTER 4

การรักษาความปลอดภัยสารสนเทศ

การจัดการสารสนเทศ (Information Management)

การจัดการสารสนเทศเป็นกระบวนการที่สำคัญในการรักษาความปลอดภัยของข้อมูล โดยครอบคลุมทั้งการจัดเก็บ การป้องกัน การจัดการการเข้าถึง และการบริหารความเสี่ยงข้อมูลสารสนเทศ ดังนี้

การจัดเก็บข้อมูล (Data Storage)

การจัดเก็บข้อมูลเป็นขั้นตอนที่สำคัญในการรักษาความปลอดภัยของสารสนเทศ ต้องมีการจัดการที่ดีเพื่อให้แน่ใจว่าข้อมูลจะไม่สูญหายหรือถูกเข้าถึงโดยไม่ได้รับอนุญาต ซึ่งรวมถึง

การเข้ารหัสข้อมูล (Data Encryption):

การเข้ารหัสเป็นกระบวนการที่แปลงข้อมูลให้อยู่ในรูปแบบที่ไม่สามารถเข้าใจได้โดยผู้ที่ไม่ได้รับอนุญาต ช่วยป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาตในกรณีที่ข้อมูลถูกขโมยหรือหลุดรั่ว

การสำรองข้อมูล (Data Backup):

การสำรองข้อมูลเป็นสิ่งจำเป็นเพื่อป้องกันการสูญหายของข้อมูล การสำรองข้อมูลควรทำอย่างสม่ำเสมอและเก็บสำรองในที่ที่ปลอดภัย

การป้องกันข้อมูล (Data Protection)

การป้องกันข้อมูลเกี่ยวข้องกับการใช้มาตรการต่าง ๆ เพื่อรักษาความปลอดภัยของข้อมูล

การควบคุมการเข้าถึง (Access Control):

การกำหนดสิทธิ์การเข้าถึงข้อมูลให้กับผู้ใช้ตามบทบาทและหน้าที่การงาน (Role-Based Access Control - RBAC) ช่วยป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

การตรวจสอบและการติดตาม (Monitoring and Auditing):

การตรวจสอบและการติดตามการเข้าถึงและการใช้งานข้อมูล เพื่อให้สามารถตรวจพบการกระทำที่น่าสงสัยหรือผิดปกติ

การจัดการการเข้าถึง (Access Management)

การจัดการการเข้าถึงเกี่ยวข้องกับการกำหนดและควบคุมการเข้าถึงข้อมูลสารสนเทศ

การยืนยันตัวตน (Authentication):

การยืนยันตัวตนของผู้ใช้เพื่อให้แน่ใจว่าผู้ใช้เป็นผู้ที่ได้รับอนุญาตให้เข้าถึงข้อมูลจริง ๆ เช่น การใช้รหัสผ่าน การใช้การยืนยันตัวตนสองขั้นตอน (Two-Factor Authentication - 2FA)

การกำหนดสิทธิ์ (Authorization):

การกำหนดสิทธิ์เข้าถึงและการดำเนินการกับข้อมูลตามบทบาทและหน้าที่ของผู้ใช้

การบริหารความเสี่ยง (Risk Management)

การบริหารความเสี่ยงเป็นกระบวนการที่สำคัญในการจัดการสารสนเทศ เพื่อระบุ ประเมิน และลดความเสี่ยงที่เกี่ยวข้องกับข้อมูล

การประเมินความเสี่ยง (Risk Assessment):

การประเมินความเสี่ยงที่เกี่ยวข้องกับข้อมูลเพื่อระบุภัยคุกคามและความเสี่ยงที่อาจเกิดขึ้น

การจัดการความเสี่ยง (Risk Mitigation):

การพัฒนามาตรการและนโยบายเพื่อจัดการและลดความเสี่ยงที่เกี่ยวข้องกับข้อมูลสารสนเทศ

การจัดการสารสนเทศเป็นกระบวนการที่ครอบคลุมและซับซ้อน ซึ่งจำเป็นต้องมีการจัดการและการป้องกันที่ดีเพื่อรักษาความปลอดภัยของข้อมูลสารสนเทศ การจัดเก็บข้อมูลอย่างปลอดภัย การป้องกันข้อมูลจากการเข้าถึงโดยไม่ได้รับอนุญาต การจัดการการเข้าถึงข้อมูล และการบริหารความเสี่ยงที่เกี่ยวข้องกับข้อมูล เป็นสิ่งที่จำเป็นต้องดำเนินการอย่างมีประสิทธิภาพและเป็นระบบ

การจัดการอัตลักษณ์ (Identity Management)

ที่มา https://www.cyfence.com/article/10-worst-behaviors-that-may-make-the-organization-under-cyber-attack/

การจัดการอัตลักษณ์ (Identity Management) เป็นกระบวนการที่สำคัญในการรักษาความปลอดภัยของข้อมูลและระบบสารสนเทศ โดยมุ่งเน้นไปที่การตรวจสอบและควบคุมการเข้าถึงระบบและข้อมูลสำคัญขององค์กร

การระบุอัตลักษณ์ (Identity Identification)

การระบุอัตลักษณ์เป็นขั้นตอนแรกในการจัดการอัตลักษณ์ โดยเป็นการสร้างและเก็บข้อมูลอัตลักษณ์ของผู้ใช้

- **การลงทะเบียนผู้ใช้ (User Registration):** กระบวนการที่ผู้ใช้ลงทะเบียนเพื่อรับข้อมูลอัตลักษณ์ โดยต้องมีการยืนยันตัวตนด้วยข้อมูลส่วนตัวหรือข้อมูลที่องค์กรกำหนด
- **การจัดเก็บข้อมูลอัตลักษณ์ (Identity Data Storage):** การจัดเก็บข้อมูลอัตลักษณ์อย่างปลอดภัย ต้องมีมาตรการรักษาความปลอดภัยที่เข้มงวดในการจัดเก็บและปกป้องข้อมูลนี้
- **ตัวอย่าง:** พนักงานใหม่ในบริษัทต้องกรอกแบบฟอร์มลงทะเบียนโดยใช้บัตรประชาชนและเอกสารที่เกี่ยวข้องเพื่อยืนยันตัวตน ข้อมูลทั้งหมดจะถูกเก็บรักษาในระบบฐานข้อมูลที่มีการเข้ารหัสเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

การยืนยันตัวตน (Authentication)

การยืนยันตัวตนเป็นกระบวนการที่ทำให้ระบบมั่นใจว่าผู้ใช้คือบุคคลที่ได้รับอนุญาตจริง ๆ

- **การยืนยันตัวตนแบบหลายขั้นตอน (Multi-Factor Authentication - MFA):** การใช้ปัจจัยหลายขั้นตอนในการยืนยันตัวตน เช่น รหัสผ่าน โทเค็น และข้อมูลชีวภาพ (biometrics)
- **การจัดการรหัสผ่าน (Password Management):** การกำหนดนโยบายรหัสผ่านที่เข้มงวด การเปลี่ยนรหัสผ่านเป็นระยะ และการใช้รหัสผ่านที่ซับซ้อน
- **ตัวอย่าง:** เมื่อล็อกอินเข้าสู่ระบบภายในบริษัท พนักงานต้องใช้รหัสผ่านของตนเองและรับรหัส OTP ผ่านแอปพลิเคชันบนโทรศัพท์มือถือเพื่อทำการยืนยันตัวตน หากมีการเข้าถึงระบบที่มีความสำคัญสูง จะมีการขอให้ใช้ลายนิ้วมือเพื่อพิสูจน์ตัวตนอีกครั้ง

การควบคุมการเข้าถึง (Access Control)

การควบคุมการเข้าถึงเป็นกระบวนการที่จำกัดการเข้าถึงข้อมูลและระบบให้กับผู้ใช้ที่ได้รับอนุญาตเท่านั้น

- **การกำหนดสิทธิ์ตามบทบาท (Role-Based Access Control - RBAC):** การกำหนดสิทธิ์การเข้าถึงระบบและข้อมูล ตามบทบาทและหน้าที่ของผู้ใช้ในองค์กร
- **การควบคุมการเข้าถึงตามคุณลักษณะ (Attribute-Based Access Control - ABAC):** การใช้คุณลักษณะของผู้ใช้ เช่น ตำแหน่งงาน แผนกหรือสถานะการทำงาน ในการกำหนดสิทธิ์การเข้าถึง
- **ตัวอย่าง:** พนักงานในแผนกบัญชีสามารถเข้าถึงข้อมูลการเงินและบัญชีทั้งหมดได้ ในขณะที่พนักงานในแผนกไอทีจะสามารถเข้าถึงระบบและข้อมูลทางเทคนิคเท่านั้น

การตรวจสอบและการติดตาม (Monitoring and Auditing)

การตรวจสอบและการติดตาม เป็นขั้นตอนที่สำคัญในการจัดการอัตลักษณ์เพื่อให้แน่ใจว่าการเข้าถึงข้อมูลและระบบมีความปลอดภัย

- **การตรวจสอบการเข้าถึง (Access Logging):** การบันทึกและตรวจสอบกิจกรรมการเข้าถึงข้อมูลและระบบของผู้ใช้
- **การวิเคราะห์และการรายงาน (Analysis and Reporting):** การวิเคราะห์ข้อมูลการเข้าถึงเพื่อระบุพฤติกรรมที่น่าสงสัย และการรายงานผลการตรวจสอบ
- **ตัวอย่าง:** ระบบจะบันทึกทุกครั้งที่มีการเข้าถึงข้อมูลสำคัญหรือมีการเปลี่ยนแปลงการตั้งค่าระบบ ผู้ดูแลระบบสามารถตรวจสอบบันทึกเหล่านี้เพื่อตรวจพบการเข้าถึงที่ผิดปกติหรือกิจกรรมที่อาจเป็นภัยคุกคาม

การจัดการอัตลักษณ์เป็นกระบวนการที่ครอบคลุมและสำคัญในการรักษาความปลอดภัยของข้อมูลและระบบสารสนเทศ โดยต้องมีการระบุอัตลักษณ์ ยืนยันตัวตน ควบคุมการเข้าถึง จัดการวงจรชีวิตของอัตลักษณ์ และการตรวจสอบและติดตามอย่างมีประสิทธิภาพตามแนวทางและมาตรฐานที่กำหนด เพื่อให้แน่ใจว่าข้อมูลและระบบขององค์กรจะปลอดภัยจากการเข้าถึงโดยไม่ได้รับอนุญาต

การรักษาความปลอดภัยของแพลตฟอร์ม (Platform Security)

การรักษาความปลอดภัยของแพลตฟอร์ม (Platform Security) เป็นกระบวนการที่สำคัญในการป้องกันภัยคุกคามที่อาจเกิดขึ้นกับระบบและแพลตฟอร์มที่ใช้ในองค์กร โดยมีการจัดการและมาตรการรักษาความปลอดภัยที่ครอบคลุมตั้งแต่ระบบปฏิบัติการ ซอฟต์แวร์ และฮาร์ดแวร์

การรักษาความปลอดภัยระบบปฏิบัติการ (Operating System Security)

การรักษาความปลอดภัยของระบบปฏิบัติการเป็นขั้นตอนที่สำคัญในการป้องกันการโจมตีและการเข้าถึงโดยไม่ได้รับอนุญาต

- **การอัปเดตและแพทช์ระบบ (System Updates and Patches):** การอัปเดตและการติดตั้งแพทช์ระบบปฏิบัติการเพื่อแก้ไขช่องโหว่ที่รู้จัก
- **การกำหนดค่าอย่างปลอดภัย (Secure Configuration):** การกำหนดค่าและการตั้งค่าระบบปฏิบัติการให้ปลอดภัยตามแนวทางที่แนะนำใน NIST SP 800-123 (Guide to General Server Security)
- **ตัวอย่าง:** การใช้เครื่องมือจัดการแพทช์ (Patch Management Tools) เพื่อให้อัปเดตระบบปฏิบัติการและซอฟต์แวร์ที่ใช้งานอยู่เป็นปัจจุบันเสมอ และการตั้งค่าระบบปฏิบัติการให้ปิดการใช้งานบริการที่ไม่จำเป็น

การรักษาความปลอดภัยฮาร์ดแวร์ (Hardware Security)

การรักษาความปลอดภัยของฮาร์ดแวร์เป็นการป้องกันการโจมตีที่มุ่งเป้าไปที่อุปกรณ์ฮาร์ดแวร์

- **การควบคุมการเข้าถึงฮาร์ดแวร์ (Hardware Access Control):** การจำกัดการเข้าถึงอุปกรณ์ฮาร์ดแวร์เฉพาะผู้ที่ได้รับอนุญาต
- **การใช้เทคโนโลยีรักษาความปลอดภัย (Security Technologies):** การใช้เทคโนโลยีรักษาความปลอดภัย เช่น Trusted Platform Module (TPM) และ Secure Boot เพื่อป้องกันการดัดแปลงฮาร์ดแวร์
- **ตัวอย่าง:** การใช้ระบบควบคุมการเข้าถึงทางกายภาพ (Physical Access Control Systems) เพื่อป้องกันการเข้าถึงเซิร์ฟเวอร์หรืออุปกรณ์สำคัญโดยไม่ได้รับอนุญาต และการใช้ TPM เพื่อป้องกันการโจมตีที่มุ่งเป้าไปที่การเปลี่ยนแปลงค่า BIOS หรือเฟิร์มแวร์

การตรวจสอบและการติดตาม (Monitoring and Auditing)

การตรวจสอบและการติดตามแพลตฟอร์มเป็นกระบวนการที่สำคัญในการรักษาความปลอดภัย

- **การบันทึกเหตุการณ์ (Event Logging):** การบันทึกเหตุการณ์ที่เกิดขึ้นในระบบและแพลตฟอร์ม เพื่อวิเคราะห์และตรวจสอบ
- **การตรวจสอบเหตุการณ์ (Event Monitoring):** การตรวจสอบเหตุการณ์และกิจกรรมที่เกิดขึ้นในระบบแบบเรียลไทม์ เพื่อระบุพฤติกรรมที่ผิดปกติ
- **ตัวอย่าง:** การใช้ระบบ SIEM (Security Information and Event Management) ในการรวบรวมและวิเคราะห์ข้อมูลบันทึกเหตุการณ์จากระบบต่าง ๆ เพื่อระบุและตอบสนองต่อเหตุการณ์ความปลอดภัยอย่างรวดเร็ว

การบริหารความเสี่ยง (Risk Management)

การบริหารความเสี่ยงเป็นการประเมินและจัดการความเสี่ยงที่เกี่ยวข้องกับแพลตฟอร์ม

- **การประเมินความเสี่ยง (Risk Assessment):** การประเมินความเสี่ยงที่เกี่ยวข้องกับระบบและแพลตฟอร์มเพื่อระบุช่องโหว่และความเสี่ยงที่อาจเกิดขึ้น
- **การจัดการความเสี่ยง (Risk Mitigation):** การพัฒนามาตรการและนโยบายเพื่อจัดการและลดความเสี่ยงที่เกี่ยวข้องกับแพลตฟอร์ม
- **ตัวอย่าง:** การใช้วิธีการ Threat Modeling เพื่อระบุและประเมินภัยคุกคามที่อาจเกิดขึ้นกับระบบและแพลตฟอร์ม และการพัฒนามาตรการเพื่อลดความเสี่ยงเหล่านี้

สรุปท้ายบท Chapter 4

การรักษาความปลอดภัยสารสนเทศ

การรักษาความปลอดภัยสารสนเทศ โดย มีวัตถุประสงค์เพื่อป้องกันข้อมูลสำคัญขององค์กรจากภัยคุกคามและช่องโหว่ที่อาจเกิดขึ้นครอบคลุมการจัดการนโยบาย กระบวนการ และเครื่องมือที่จำเป็นเพื่อรักษาความลับ (Confidentiality) ความถูกต้อง (Integrity) และความพร้อมใช้งาน (Availability) ของข้อมูล องค์ประกอบสำคัญได้แก่ การจัดการอัตลักษณ์และสิทธิ์การเข้าถึงของผู้ใช้ (Identity Management) การพิสูจน์ตัวตน (Authentication) การควบคุมการเข้าถึง (Access Control) การรักษาความปลอดภัยของแพลตฟอร์ม (Platform Security) และการจัดการโครงสร้างพื้นฐานเทคโนโลยี (Technology Infrastructure Management) ทั้งหมดนี้เพื่อให้มั่นใจว่าข้อมูลขององค์กรมีความปลอดภัย และสามารถใช้งานได้อย่างมีประสิทธิภาพในทุกสถานการณ์

การรักษาความปลอดภัยของแพลตฟอร์ม เป็นกระบวนการที่ครอบคลุมและซับซ้อน ซึ่งจำเป็นต้องมีการจัดการและการป้องกันที่ดี เพื่อรักษาความปลอดภัยของระบบและแพลตฟอร์ม การรักษาความปลอดภัยของระบบปฏิบัติการ ซอฟต์แวร์ และฮาร์ดแวร์ การตรวจสอบและการติดตาม และการบริหารความเสี่ยง เป็นสิ่งที่จำเป็นต้องดำเนินการอย่างมีประสิทธิภาพและเป็นระบบ ตามแนวทางและมาตรฐานที่กำหนด เพื่อให้แน่ใจว่าแพลตฟอร์มขององค์กรจะปลอดภัยจากการเข้าถึงและการโจมตีโดยไม่ได้รับอนุญาต

CHAPTER 5

การสร้างวัฒนธรรมแห่งการตระหนักรู้ด้านความปลอดภัย

พฤติกรรมเสี่ยงที่อาจทำให้เกิดช่องโหว่ด้านความปลอดภัยในองค์กร

- **การใช้ซอฟต์แวร์ที่ล้าสมัย:** ช่องโหว่ในระบบปฏิบัติการ เบราว์เซอร์ และซอฟต์แวร์อื่น ๆ บนพีซีและอุปกรณ์ต่าง ๆ เป็นหนึ่งในวิธีหลักที่อาชญากรไซเบอร์ใช้โจมตี
- **การใช้รหัสผ่านที่อ่อนแอ:** ใช้รหัสผ่านง่าย ๆ หรือใช้รหัสผ่านเดียวกันกับหลายบัญชี ทำให้แฮกเกอร์สามารถเดาและเข้าถึงข้อมูลได้ง่าย ควรเปิดใช้งานการยืนยันตัวตนสองชั้น (2FA) ในบัญชีที่รองรับ
- **การใช้ Wi-Fi สาธารณะ:** Wi-Fi สาธารณะ ที่เปิดให้เราใช้งานอย่างฟรี ๆ ในที่ต่าง ๆ บางทีเราอาจจะกำลังใช้มันร่วมกับเหล่าแฮกเกอร์โดยที่ไม่รู้ตัว และอาจกลายเป็นช่องโหว่ที่จะทำให้ผู้ไม่หวังดีเข้ามาขโมยข้อมูลในเครื่องของเราและต่อเนื่องเข้าสู่ Network ขององค์กรได้อย่างง่ายดาย ดังนั้นคำแนะนำที่ดีที่สุดจึงเป็นการหลีกเลี่ยงการใช้งาน Network สาธารณะ หรือ Network ที่เราไม่รู้จัก หรือหากมีความจำเป็นจะต้องใช้งานจริง ๆ ก็ไม่ควร log in เข้าใช้งานบัญชีที่สำคัญใด ๆ เด็ดขาด

- **การเปิดไฟล์แนบที่ไม่ปลอดภัย:** การดาวน์โหลดซอฟต์แวร์หรือไฟล์จากเว็บไซต์ที่ไม่น่าเชื่อถือ อาจมีมัลแวร์แฝงอยู่ทำให้เสี่ยงต่อภัยคุกคามต่าง ๆ ได้
- **การละเลยการฝึกอบรม:** พนักงานขาดความรู้เกี่ยวกับความปลอดภัย

ผลกระทบที่อาจเกิดขึ้นจากการละเมิดความปลอดภัยสารสนเทศ

การละเมิดความปลอดภัยสารสนเทศสามารถก่อให้เกิดผลกระทบที่รุนแรงต่อองค์กรในหลายด้าน ดังนี้

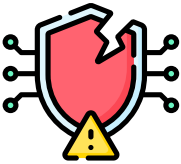
- **ความเสียหายทางการเงิน**
  - **ค่าปรับและบทลงโทษ:** การละเมิดความปลอดภัยของข้อมูลอาจทำให้ต้องจ่ายค่าปรับ และรับบทลงโทษตามกฎหมายและระเบียบข้อบังคับต่าง ๆ เช่น GDPR ในยุโรป หรือ PDPA ในประเทศไทย
  - **ค่าใช้จ่ายในการแก้ไข:** ต้องใช้เงินในการแก้ไขระบบที่ถูกเจาะ ปรับปรุงมาตรการความปลอดภัย และฟื้นฟูข้อมูลที่สูญหาย
  - **การสูญเสียรายได้:** การละเมิดความปลอดภัยอาจทำให้ธุรกิจหยุดชะงัก ส่งผลให้สูญเสียรายได้ในช่วงที่ไม่สามารถให้บริการได้
- **ความเสียหายต่อชื่อเสียง**
  - **การสูญเสียความเชื่อมั่นจากลูกค้า:** การละเมิดความปลอดภัยอาจทำให้ลูกค้าสูญเสียความเชื่อมั่นในองค์กร ส่งผลให้ลูกค้าหันไปใช้บริการของคู่แข่ง
  - **ภาพลักษณ์ขององค์กร:** ชื่อเสียงขององค์กรอาจถูกทำลาย ทำให้ยากต่อการฟื้นฟูภาพลักษณ์และสร้างความเชื่อมั่นใหม่

- **ความเสียหายทางการเงิน**
  - **การหยุดชะงักของธุรกิจ:** การโจมตีทางไซเบอร์อาจทำให้ระบบและการดำเนินงานขององค์กรหยุดชะงัก ส่งผลกระทบต่อประสิทธิภาพและการให้บริการลูกค้า
  - **การสูญเสียข้อมูลสำคัญ:** ข้อมูลสำคัญที่สูญหายหรือถูกทำลายอาจทำให้กระบวนการทางธุรกิจหยุดชะงัก และส่งผลกระทบต่อการตัดสินใจและการวางแผน
- **ผลกระทบทางกฎหมาย**
  - **การถูกฟ้องร้อง:** การละเมิดความปลอดภัยของข้อมูลอาจทำให้ต้องเผชิญกับการฟ้องร้องจากลูกค้า พันธมิตร หรือผู้มีส่วนได้ส่วนเสียที่ได้รับผลกระทบ
  - **การไม่ปฏิบัติตามกฎหมายและมาตรฐาน:** องค์กรที่ไม่สามารถปฏิบัติตามกฎหมายและมาตรฐานความปลอดภัยข้อมูล อาจต้องเผชิญกับบทลงโทษทางกฎหมาย และสูญเสียใบอนุญาตหรือการรับรองต่าง ๆ

กรณีศึกษา: การละเมิดความปลอดภัยสารสนเทศในองค์กรที่มีชื่อเสียง

การถูกโจมตีข้อมูลของ Yahoo ในปี 2013 และ 2014

ในปี 2013 และ 2014 Yahoo ซึ่งเป็นหนึ่งในแพลตฟอร์มอีเมลและข้อมูลที่ใหญ่ที่สุดในโลก ถูกโจมตีข้อมูลในเหตุการณ์ที่ส่งผลกระทบต่อบัญชีผู้ใช้ทั้งหมดกว่า 3 พันล้านบัญชี เหตุการณ์นี้ถือเป็นหนึ่งในเหตุการณ์การละเมิดความปลอดภัยที่ใหญ่ที่สุดในประวัติศาสตร์



ที่มา : https://www.wsj.com/articles/yahoo-hack-are-you-still-at-risk-1489610181

ผลกระทบ:

1. ข้อมูลส่วนตัวของผู้ใช้ เช่น ชื่อ ที่อยู่อีเมล วันเกิด โทรศัพท์ หมายเลข และรหัสผ่านที่เข้ารหัส ถูกขโมยไป
2. ชื่อเสียงของ Yahoo ถูกทำลาย และมูลค่าของบริษัทลดลง
3. การขายกิจการให้กับ Verizon ได้รับผลกระทบ โดยราคาขายลดลงไปถึง 350 ล้านดอลลาร์
4. Yahoo ถูกฟ้องร้อง และต้องเสียค่าปรับและค่าใช้จ่ายในการแก้ไขปัญหามากมาย

กรณีศึกษา: การละเมิดข้อมูลของ Facebook ในปี 2018

ในปี 2018 Facebook ประสบกับเหตุการณ์การละเมิดข้อมูลครั้งใหญ่ที่มีผลกระทบต่อผู้ใช้กว่า 50 ล้านคน เหตุการณ์นี้เกิดจากการที่แฮกเกอร์สามารถเข้าถึงโทเค็นการเข้าถึง (access tokens) ของผู้ใช้ผ่านช่องโหว่ในฟีเจอร์ “View As” ทำให้สามารถเข้าถึงบัญชีผู้ใช้ได้โดยไม่ได้รับอนุญาต

ที่มา: https://securitytoday.com/articles/2018/10/02/facebook-hacked-50-million-users-data-exposed.aspx

ผลกระทบ:

1. ข้อมูลส่วนตัวของผู้ใช้ เช่น ชื่อ อีเมล และหมายเลขโทรศัพท์ถูกเข้าถึงโดยไม่ได้รับอนุญาต
2. ชื่อเสียงของ Facebook ถูกทำลาย และความเชื่อมั่นของผู้ใช้ลดลงอย่างมาก
3. Facebook ถูกตรวจสอบและวิพากษ์วิจารณ์จากหน่วยงานกำกับดูแลด้านความเป็นส่วนตัวทั่วโลก
4. ส่งผลให้มีการฟ้องร้องและต้องเสียค่าปรับและค่าใช้จ่ายในการแก้ไขปัญหามากมาย

การละเมิดความปลอดภัยสารสนเทศในกรณีศึกษา แสดงให้เห็นถึงความสำคัญของการมีระบบการจัดการความปลอดภัยของข้อมูล (ISM) ที่แข็งแกร่ง การป้องกันที่ดีจะช่วยลดความเสี่ยงของการโจมตีและการละเมิดความปลอดภัย ในขณะที่การตอบสนองอย่างรวดเร็วและมีประสิทธิภาพ สามารถช่วยลดความเสียหายและฟื้นฟูความเชื่อมั่นของผู้ใช้ได้

บทบาทและหน้าที่ความรับผิดชอบของบุคลากรในส่วนงานต่าง ๆ ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยสารสนเทศ

การรักษาความมั่นคงปลอดภัยของข้อมูล (Information Security) เป็นหน้าที่ของบุคลากรหลายฝ่ายในองค์กร ซึ่งมีบทบาทและหน้าที่ความรับผิดชอบที่แตกต่างกัน แต่ทำงานร่วมกันเพื่อให้เกิดความปลอดภัยที่ครบวงจร ดังนี้

ที่มา: https://www.pttdigitalconnect.com/product/cyber-security-management

- **ผู้บริหารระดับสูง (Senior Management)**
  - **กำหนดนโยบายและทิศทาง:** ผู้บริหารระดับสูงมีบทบาทสำคัญในการกำหนดนโยบายและทิศทางด้านความมั่นคงปลอดภัยของข้อมูล เพื่อให้แน่ใจว่าองค์กรมีการปฏิบัติตามกฎหมายและมาตรฐานที่เกี่ยวข้อง
  - **จัดสรรทรัพยากร:** จัดสรรทรัพยากรที่จำเป็น ทั้งด้านการเงิน เทคโนโลยี และบุคลากร เพื่อสนับสนุนการดำเนินการด้านความมั่นคงปลอดภัย
  - **ส่งเสริมวัฒนธรรมความมั่นคงปลอดภัย:** สร้างสภาพแวดล้อมและวัฒนธรรมองค์กรที่ให้ความสำคัญกับความมั่นคงปลอดภัยของข้อมูล

- **เจ้าหน้าที่ความมั่นคงปลอดภัยสารสนเทศ (Information Security Officer)**
  - **วางแผนและดำเนินการตามนโยบาย:** เจ้าหน้าที่ความมั่นคงปลอดภัยสารสนเทศมีหน้าที่วางแผนและดำเนินการตามนโยบายที่ผู้บริหารกำหนด รวมถึงการพัฒนายุทธศาสตร์ความมั่นคงปลอดภัย
  - **ติดตั้งและอัปเดตซอฟต์แวร์:** ติดตั้งและอัปเดตซอฟต์แวร์ป้องกันไวรัส แพตช์ความปลอดภัย และการตั้งค่าระบบต่าง ๆ
  - **เฝ้าระวังและตอบสนองต่อเหตุการณ์:** เฝ้าระวังและตอบสนองต่อเหตุการณ์ที่อาจเกิดขึ้น เช่น การโจมตีทางไซเบอร์ การเข้าถึงที่ไม่ได้รับอนุญาต
- **ผู้ใช้งานทั่วไป (End Users):**
  - **การปฏิบัติตามนโยบายและแนวทางปฏิบัติ:** ผู้ใช้งานทั่วไปมีหน้าที่ปฏิบัติตามนโยบายและแนวทางปฏิบัติด้านความมั่นคงปลอดภัยขององค์กร เช่น การใช้รหัสผ่านที่ปลอดภัย การหลีกเลี่ยงการเปิดไฟล์หรือคลิกลิงก์ที่ไม่ปลอดภัย
  - **การรายงานเหตุการณ์ที่ผิดปกติ:** รายงานเหตุการณ์ที่ผิดปกติหรือสงสัยว่าอาจเป็นภัยคุกคามทางไซเบอร์ไปยังเจ้าหน้าที่ความมั่นคงปลอดภัย
  - **การฝึกอบรมและการรับรู้:** มีส่วนร่วมในกิจกรรมฝึกอบรมและการรับรู้เกี่ยวกับความมั่นคงปลอดภัยของข้อมูลที่องค์กรจัดขึ้น

- **ผู้จัดการความเสี่ยง (Risk Manager)**
  - **การระบุและประเมินความเสี่ยง:** ระบุและประเมินความเสี่ยงที่เกี่ยวข้องกับการรักษาความปลอดภัยของข้อมูล
  - **การวางแผนการจัดการความเสี่ยง:** พัฒนาและดำเนินการแผนการจัดการความเสี่ยงเพื่อป้องกันและลดผลกระทบจากเหตุการณ์ความเสี่ยง
  - **การติดตามและรายงาน:** ติดตามและรายงานสถานะของความเสี่ยงและประสิทธิภาพของมาตรการป้องกัน
- **ผู้พัฒนาซอฟต์แวร์ (Software Developer)**
  - **การเขียนโค้ดที่ปลอดภัย:** ผู้พัฒนาซอฟต์แวร์ต้องเขียนโค้ดที่ปลอดภัยและปฏิบัติตามแนวทางการพัฒนาโปรแกรมที่มีความมั่นคงปลอดภัย
  - **การทดสอบและตรวจสอบความปลอดภัย:** ทดสอบและตรวจสอบความปลอดภัยของซอฟต์แวร์เพื่อระบุและแก้ไขช่องโหว่
  - **การอัปเดตและบำรุงรักษา:** อัปเดตและบำรุงรักษาซอฟต์แวร์ให้เป็นไปตามมาตรฐานความปลอดภัยที่กำหนด

การสร้างและส่งเสริมวัฒนธรรมการรักษาความปลอดภัยในองค์กร

ที่มา : https://www.wsj.com/articles/yahoo-hack-are-you-still-at-risk-1489610181

- **การสร้างแรงจูงใจให้พนักงานมีส่วนร่วมในการรักษาความปลอดภัย**
  - **การให้รางวัลและยกย่อง:** มอบรางวัลหรือยกย่องพนักงานที่ปฏิบัติตามนโยบายความปลอดภัยอย่างเคร่งครัด เช่น มอบรางวัลพนักงานดีเด่นด้านความปลอดภัย
  - **การมีส่วนร่วมในการตัดสินใจ:** เปิดโอกาสให้พนักงานมีส่วนร่วมในการกำหนดนโยบายและมาตรการความปลอดภัย ซึ่งจะช่วยเพิ่มความรู้สึกเป็นเจ้าของและความรับผิดชอบ

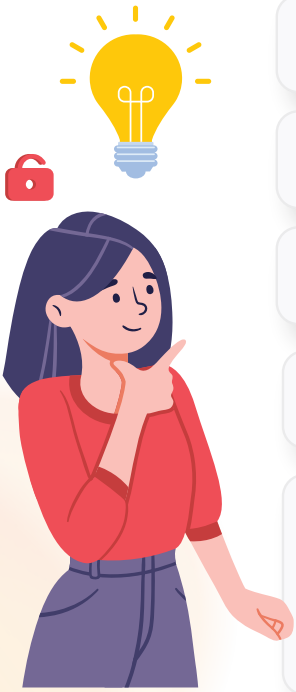
- **การจัดกิจกรรมและโครงการที่ส่งเสริมความตระหนักรู้ด้านความปลอดภัย**
  - **การฝึกอบรมและเวิร์กช็อป:** จัดฝึกอบรมเกี่ยวกับภัยคุกคามไซเบอร์และวิธีการป้องกัน รวมถึงเวิร์กช็อปที่ให้พนักงานได้มีโอกาสเรียนรู้และฝึกฝนทักษะ
  - **การสัมมนาและการบรรยาย:** เชิญผู้เชี่ยวชาญมาบรรยายให้ความรู้เกี่ยวกับเทคโนโลยีและแนวโน้มใหม่ ๆ ในด้านความปลอดภัย
- **การจัดกิจกรรมและเกมเพื่อส่งเสริมความตระหนักรู้ด้านความปลอดภัย**
  - **เกมและกิจกรรมการแข่งขัน:** จัดการแข่งขันเช่น Capture the Flag (CTF) ซึ่งเป็นการแข่งขันเพื่อหาช่องโหว่ในระบบและการแก้ไขปัญหาด้านความปลอดภัย
  - **การใช้สื่ออินเตอร์แอคทีฟ:** สร้างสื่อการเรียนรู้ที่เป็นอินเตอร์แอคทีฟ เช่น วิดีโอ เกม หรือแบบทดสอบ ที่ช่วยให้พนักงานสามารถเรียนรู้เกี่ยวกับความปลอดภัยในรูปแบบที่สนุกและเข้าใจง่าย
- **การประเมินและวัดผลความสำเร็จของโครงการสร้างความตระหนักรู้ด้านความปลอดภัย**
  - **การทำแบบสอบถามและประเมินผล:** ใช้แบบสอบถามเพื่อวัดความรู้และความตระหนักรู้ของพนักงานก่อนและหลังการฝึกอบรมเพื่อดูการเปลี่ยนแปลงและประสิทธิภาพของโครงการ
  - **การวิเคราะห์และรายงานผล:** วิเคราะห์ผลการประเมินและจัดทำรายงานเพื่อนำเสนอผู้บริหาร รวมถึงการปรับปรุงโครงการในอนาคตตามผลการประเมิน

กระบวนการสร้างวัฒนธรรมด้านความปลอดภัยทางไซเบอร์ภายในองค์กร

ประเมินสถานะปัจจุบันในด้านมั่นคงความปลอดภัยทางไซเบอร์ขององค์กร

การรักษาความมั่นคงปลอดภัยทางไซเบอร์มุ่นเน้นไปที่การปกป้องระบบและทรัพย์สินที่สำคัญทางสารสนเทศ การประเมินสถานะความมั่นคงปลอดภัยทางไซเบอร์ ณ ปัจจุบันขององค์กร ช่วยให้องค์กรระบุความเสี่ยงและช่องโหว่ในกระบวนการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ซึ่งสามารถทำให้รับมือกับเหตุภัยคุกคามทางไซเบอร์ได้อย่างรวดเร็วและมีประสิทธิภาพ การวิเคราะห์ความเสี่ยงของมนุษย์ (Human Risk Analysis – HRA) ช่วยให้องค์กรจัดลำดับความสำคัญของความเสี่ยงโดยการนำปัจจัยด้านเวลา ค่าใช้จ่าย และมูลค่าคาดการณ์มาคิดวิเคราะห์

ในระหว่างการดำเนินการประเมินนี้ องค์กรสามารถสร้างวัฒนธรรมด้านความปลอดภัยทางไซเบอร์ได้สำเร็จได้โดย:



- ระบุผู้มีส่วนได้ส่วนเสียของโครงการการสร้างความตระหนักรู้ด้านความปลอดภัยทางไซเบอร์
- กำหนดเป้าหมายการฝึกอบรมด้านความปลอดภัยทางไซเบอร์ของแต่ละกลุ่มเป้าหมายในองค์กร
- เลือกวิธีการเรียนการสอนที่เหมาะสมกับกลุ่มเป้าหมายมากที่สุด เช่น สัมมนา การเรียนออนไลน์ หรือเหตุการณ์จำลอง
- พัฒนาแผนการฝึกอบรมและสร้างการรับรู้ โดยกำหนดผู้ให้การฝึกอบรม และวิธีการสังเกตุดูแล
- จัดตั้ง (Key Performance Indicators – KPI) เพื่อประเมินประสิทธิภาพของการฝึกอบรม ตัวอย่างของ KPI เช่น อัตราการมีส่วนร่วมของผู้ฝึกอบรมในโครงการ ความสำเร็จในการฝึกอบรม และการเปลี่ยนแปลงทัศนคติและพฤติกรรมของผู้ฝึกอบรมเช่นการตั้งรหัสผ่านที่คาดเดาได้ยาก หรือการรายงานอีเมลที่หลอกล่อเอาข้อมูลส่วนบุคคล (Phishing)

การสร้างความรับผิดชอบต่อผู้บริหารระดับสูง ในการสร้างวัฒนธรรมความปลอดภัยทางไซเบอร์ขององค์กร

การสร้างวัฒนธรรมองค์กรต้องเริ่มต้นจากผู้บริหารระดับสูง ซึ่งรวมถึงคณะกรรมการบริษัท ประธานเจ้าหน้าที่บริหารงานด้านสารสนเทศ (Chief Information Officer – CIO) ประธานเจ้าหน้าที่บริหารความมั่นคงปลอดภัยสารสนเทศ (Chief Information Security Officer) และตำแหน่งประธานเจ้าหน้าที่บริหารอื่น ๆ ซึ่งผู้นำเหล่านี้ควรใช้ผลการประเมินสถานะความมั่นคงปลอดภัยทางไซเบอร์ในขั้นตอนก่อนหน้า เพื่อกำหนดจุดประสงค์เชิงกลยุทธ์ เข้าใจคุณค่าของการรักษาความมั่นคงปลอดภัยทางไซเบอร์ภายในองค์กร และให้ความสำคัญกับคุณค่าตรงจุดนี้ นอกจากนี้ ควรตั้งเป้าหมายการสร้างวัฒนธรรมด้านความปลอดภัยทางไซเบอร์ในองค์กรให้เจาะจงและกำหนดระยะการบรรลุเป้าหมายให้สำเร็จอย่างชัดเจน เพื่อช่วยคิดค้นตัวชี้วัดและการติดตามการสร้างวัฒนธรรมด้านความปลอดภัยทางไซเบอร์ในองค์กร สำหรับผู้บริหารระดับสูงที่ไม่ได้เกี่ยวข้องโดยตรงกับไซเบอร์ ต้องมีส่วนร่วมในการขับเคลื่อนให้ความมั่นคงปลอดภัยทางไซเบอร์เป็นคุณค่าหลักในการดำเนินการขององค์กร

การจัดการฝึกอบรมเรื่องความปลอดภัยทางไซเบอร์ให้กับบุคลากร

โครงการการฝึกอบรมช่วยให้ผู้มีส่วนได้ส่วนเสียเข้าใจภัยคุกคามทางไซเบอร์และการโจมตีเครือค่ายของแฮกเกอร์ล่าสุด การฝึกอบรมควรครอบคลุมในเนื้อหาของภัยคุกคามที่ใช้เทคนิคทางวิศวกรรมสังคมอย่างฟิชชิ่ง (Phishing) ที่เกิดขึ้นได้เนื่องจากความผิดพลาดของมนุษย์ที่หลงเชื่อในการหลอกลวง การจัดฝึกอบรมอย่างต่อเนื่องมีความสำคัญอย่างยิ่งเพราะภัยคุกคามสามารถวิวัฒนาการเปลี่ยนแปลงได้ตลอด แผนกทรัพยากรบุคคลและเทคโนโลยีสารสนเทศขององค์กรร่วมกับประธานเจ้าหน้าที่บริหารด้านความมั่นคงปลอดภัยทางสารสนเทศ ควรเป็นผู้จัดและติดตามการดำเนินงานของโครงการฝึกอบรม โดยที่เนื้อหาการฝึกอบรมควรสอดคล้องกับตำแหน่งงานของบุคคลที่เข้ารับการฝึก

การคงไว้ของแคมเปญทางด้านการรักษาความปลอดภัยทางไซเบอร์

การมีส่วนร่วมของบุคลากรเป็นส่วนสำคัญต่อการสร้างวัฒนธรรมองค์กรด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ การเรียนรู้เกี่ยวกับด้านนี้ควรเข้าถึงได้ง่าย ให้ประสบการณ์ผู้เรียนได้ลงมือทำจริง และเนื้อหาการเรียนควรมีความเกี่ยวข้องต่อการทำงานของผู้เรียน รวมถึงสอดคล้องกับสถานการณ์ในปัจจุบัน องค์กรสามารถสนับสนุนให้บุคลากรเข้าร่วมในกระบวนการรักษาสความมั่นคงปลอดภัยทางไซเบอร์และใช้เทคนิคทางการตลาดเพื่อส่งเสริมให้บุคลากรเตรียมตัวกับการทำงานในด้านนี้ รวมถึงจัดแคมเปญเพื่อเสริมสร้างการมีส่วนร่วมของบุคลากร ซึ่งแคมเปญในส่วนนี้ควรปรับให้เหมาะสมกับกลุ่มเป้าหมายต่าง ๆ และจัดทำผ่านสื่ออย่าง วีดีโอและพรีเซ็นเทชัน

การจัดการฝึกซ้อมเพื่อสร้างความตระหนักรู้และรับมือต่อเหตุภัยคุกคามทางไซเบอร์

การฝึกซ้อมรับมือต่อเหตุการณ์ภัยคุกคามทางไซเบอร์เป็นประจำช่วยให้บุคลากรได้รับมุมมองของเหตุการณ์ภัยคุกคามจริงและสามารถปรับตัวกับเหตุการณ์ที่อาจเกิดขึ้นได้ในอนาคต นอกจากนี้การเรียงลำดับความสำคัญของเหตุการณ์ต่อระดับความเสี่ยงทำให้องค์กรสามารถสร้างผลลัพธ์ที่ดีในการฝึกซ้อมได้

การประเมินกิจกรรมการรักษาความมั่นคงปลอดภัยทางไซเบอร์เป็นประจำ

องค์กรควรประเมินกิจกรรมทางไซเบอร์เป็นประจำ เพื่อวัดประสิทธิภาพและความสมบูรณ์ของกิจกรรม การประเมินควรมุ่งเน้นไปที่วัฒนธรรมการรักษาความมั่นคงปลอดภัยทางไซเบอร์ในระดับองค์กรและบุคคล การประเมินอย่างเป็นทางการช่วยให้บุคลากรเข้าใจถึงความสำคัญของการรักษาความมั่นคงปลอดภัยทางไซเบอร์ และรับทราบถึงระดับความเข้าใจขั้นต่ำเรื่องการรักษาความมั่นคงปลอดภัยทางไซเบอร์ที่องค์กรกำหนด

กรณีศึกษาการสร้างวัฒนธรรมความปลอดภัยทางไซเบอร์ภายในองค์กร: Yahoo

บริษัทผู้ให้บริการเบราว์เซอร์ Yahoo สร้างวัฒนธรรมความปลอดภัยไซเบอร์ภายในองค์กรโดยการศึกษาการตอบสนองของบุคลากรต่อการจำลองเหตุการณ์เพื่อทำความเข้าใจวิธีการที่จะทำให้บุคลากรเห็นความสำคัญของการรักษาความมั่นคงปลอดภัยทางไซเบอร์อย่างจริงจัง เพื่อให้สามารถบรรลุเป้าหมายการสร้างวัฒนธรรมด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ได้สำเร็จ บุคลากรที่อยู่ในตำแหน่งผู้จัดการควรปฏิบัติตาม 3 ขั้นตอนนี้:

01 แยกแยะพฤติกรรมที่สำคัญของบุคลากร

02 ผู้จัดการควรประเมินพฤติกรรมของบุคลากรอย่างโปร่งใส

03 ผู้จัดการควรใช้หลักความคิดการตระหนักรู้เพื่ออธิบายเหตุผลว่าทำไมการรักษาความมั่นคงปลอดภัยทางไซเบอร์จึงมีความสำคัญ

หลังจากที่ Yahoo ได้ใช้ขั้นตอนดังกล่าวในการสร้างวัฒนธรรมความปลอดภัยทางไซเบอร์แก่บุคลากร ในช่วงครึ่งหลังของปี 2020 บุคลากรใน Yahoo สามารถรายงานผลการโจมตี Phishing ได้ถูกต้อง เพิ่มขึ้นจากเดิม 2 เท่า นอกจากนี้ ที่สำคัญที่สุด คือ บุคลากรได้นำเครื่องมือการบริหารจัดการรหัสขององค์กรมาใช้มากขึ้นเป็น 3 เท่า

สรุปท้ายบท Chapter 5

การสร้างวัฒนธรรมแห่งการตระหนักรู้ด้านความปลอดภัย

การสร้างวัฒนธรรมแห่งการตระหนักรู้ด้านความปลอดภัยในองค์กร เป็นส่วนสำคัญของการรักษาความปลอดภัยสารสนเทศ บทนี้กล่าวถึงความเสี่ยงที่เกิดจากพฤติกรรมของพนักงาน เช่น การใช้ซอฟต์แวร์ที่ล้าสมัย การใช้รหัสผ่านที่อ่อนแอ และการเชื่อมต่อกับ Wi-Fi สาธารณะ ซึ่งเป็นช่องโหว่ที่มักถูกโจมตีโดยผู้ไม่หวังดี นอกจากนี้ ยังมีการอธิบายถึงจิตวิทยาของการโจมตีทางไซเบอร์ เช่น การฟิชชิ่งและวิศวกรรมสังคม รวมถึงวิธีการป้องกันเพื่อให้พนักงานสามารถรับมือกับภัยคุกคามเหล่านี้ได้อย่างมีประสิทธิภาพ

โดยความสำคัญของการรักษาความลับของข้อมูลส่วนบุคคลและข้อมูลองค์กรด้วยการสร้างวัฒนธรรมแห่งความตระหนักรู้ในองค์กรนั้น ไม่เพียงแต่เกี่ยวข้องกับการให้ความรู้และการฝึกอบรมพนักงานเท่านั้น แต่ยังต้องมีการสร้างสภาพแวดล้อมที่ส่งเสริมและสนับสนุนให้พนักงานทุกคนมีส่วนร่วมในการรักษาความปลอดภัยสารสนเทศ องค์กรควรมีนโยบายและมาตรการที่ชัดเจนในการจัดการกับความเสี่ยง และควรสร้างแรงจูงใจให้พนักงานมีส่วนร่วมในการปฏิบัติตามนโยบายเหล่านี้

MODULE 03

การตรวจจับภัยคุกคามและเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ

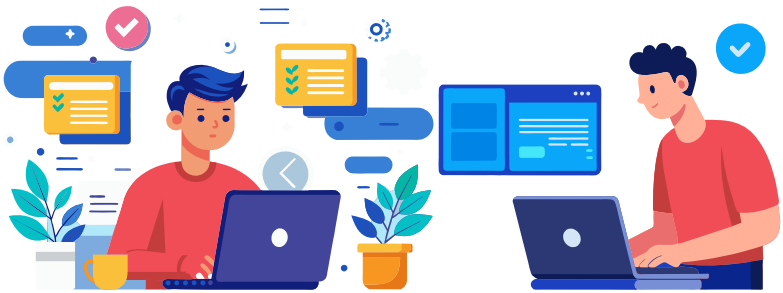
(Information Security Threat and Incident Detection) #Detect

วัตถุประสงค์รายวิชา

เพื่อให้ผู้เข้ารับการฝึกอบรมมีความรู้ความเข้าใจ เกี่ยวกับการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ สามารถระบุและประเมินความเสี่ยง วิเคราะห์และเลือกใช้กลยุทธ์การจัดการความเสี่ยงที่เหมาะสม รวมถึงสามารถนำมาตรการควบคุมต่าง ๆ ไปใช้ในการป้องกันและลดความเสี่ยงได้อย่างมีประสิทธิภาพ

CHAPTER 6

การระบุภัยคุกคามและการประเมินช่องโหว่



ประเภทของภัยคุกคามทางไซเบอร์ (Cyber Threat):

มัลแวร์ (Malware)

มาจาก MALicious และ SoftWARE หมายถึง โปรแกรมประสงค์ร้ายที่ถูกเขียนขึ้นมาเพื่อทำอันตรายกับข้อมูลในระบบ เช่น ทำให้เครื่องคอมพิวเตอร์ทำงานผิดปกติ ขโมยหรือทำลายข้อมูล หรืออาจจะเปิดช่องทางให้ผู้ไม่หวังดีเข้ามาควบคุมเครื่องของเราได้

ที่มา : https://www.ttbbank.com/th/fin-tips/detail/malware

ตัวอย่างของมัลแวร์

1. Virus (ไวรัส): ไวรัสเป็นโปรแกรมคอมพิวเตอร์ที่สามารถทำลายหรือแก้ไขไฟล์ในเครื่องคอมพิวเตอร์ โดยการติดตั้งตัวเองลงในไฟล์อื่น ๆ และทำให้โปรแกรมหรือระบบทำงานผิดปกติ หรือทำลายข้อมูล

2. Worm (เวิร์ม): เวิร์มเป็นโปรแกรมที่สามารถแพร่กระจายตัวเองไปยังเครื่องคอมพิวเตอร์อื่น ๆ ในเครือข่ายโดยอัตโนมัติ โดยไม่ต้องมีการกระทำจากผู้ใช้ สามารถทำให้เครือข่ายหรือเครื่องคอมพิวเตอร์ล้มเหลวได้

3. Trojan (โทรจัน): โทรจันเป็นโปรแกรมคอมพิวเตอร์ที่ปรากฏตัวเป็นโปรแกรมปกติหรือแอปพลิเคชันที่ดูเหมือนไม่มีความเสี่ยง แต่จริง ๆ แล้วมีเป้าหมายที่จะเข้าถึงข้อมูลส่วนตัว หรือควบคุมระบบได้โดยไม่ได้รับอนุญาต

4. Backdoor (แบ็กดอร์): แบ็กดอร์เป็นโปรแกรมหรือโค้ดที่ถูกใส่ไว้ในระบบคอมพิวเตอร์ เพื่อให้ผู้ไม่ประสงค์ดีสามารถเข้าถึง หรือควบคุมเครื่องคอมพิวเตอร์ได้โดยไม่รู้ตัว

5. Spyware (สปายแวร์): สปายแวร์เป็นโปรแกรมที่ถูกติดตั้งในเครื่องคอมพิวเตอร์โดยที่ผู้ใช้ไม่รู้ตัว และมีเป้าหมายเพื่อเก็บข้อมูลส่วนตัวของผู้ใช้ หรือติดตามกิจกรรมที่ทำในเครื่อง

6. Ransomware (แรนซัมแวร์): ภัยคุกคามทางไซเบอร์ที่ทำการเข้ารหัสหรือล็อกไฟล์ ไม่ให้ผู้ใช้สามารถเปิดไฟล์หรือคอมพิวเตอร์ได้ จากนั้นก็จะส่งข้อความหาผู้ใช้หรือองค์กร เพื่อ “เรียกค่าไถ่ (Ransom)” แลกกับการถอดรหัสเพื่อกู้ข้อมูลคืนมา มักพบเจอบ่อยในระดับองค์กรหรือหน่วยงานรัฐบาล

การป้องกันมัลแวร์

1. อัปเดทคอมพิวเตอร์และซอฟต์แวร์ในเครื่องสม่ำเสมอ
2. ติดตั้งโปรแกรมป้องกันมัลแวร์ (Anti-malware) บนคอมพิวเตอร์
3. ระมัดระวังการใช้งานอุปกรณ์เชื่อมต่อทั้งหลาย เช่น แฟลชไดร์ฟ (USB) เป็นต้น ควรทำการสแกนไวรัสทุกครั้งก่อนใช้งาน
4. ไม่คลิกข้อความที่แสดงโฆษณาหรือหน้าต่าง pop-up ปลอม (Adware) บนเว็บไซต์ที่เยี่ยมชม เพราะจะเป็นการเริ่มดาวน์โหลดมัลแวร์ จะต้องเช็คและตรวจสอบก่อนคลิกเสมอ
5. ไม่ดาวน์โหลดโปรแกรมจากแหล่งที่ไม่น่าเชื่อถือหรือเสี่ยงต่อการมีมัลแวร์แฝงอยู่
6. หลีกเลี่ยงการเปิดอีเมล รวมไปถึงไฟล์แนบที่ต้องสงสัยใด ๆ ที่ส่งมาจากอีเมลที่เราไม่รู้จัก และต้องตรวจสอบทุกครั้งก่อนดาวน์โหลดหรือเปิดไฟล์ขึ้นมา

การโจมตีแบบฉวยโอกาส (Zero-day attack)

การโจมตีแบบฉวยโอกาส (Zero-day attack) คือ การโจมตีระบบคอมพิวเตอร์โดยการใช้ช่องโหว่ของซอฟต์แวร์หรือฮาร์ดแวร์ที่ยังไม่มีการแก้ไขหรือเปิดเผยต่อสาธารณะ ซึ่งผู้ผลิตซอฟต์แวร์หรือผู้ดูแลระบบยังไม่ทราบถึงช่องโหว่นี้ จึงยังไม่มีวิธีป้องกันหรือแพตช์ (Patch) ออกมาเพื่อแก้ไขปัญหา

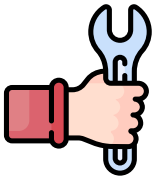
ที่มา : https://www.thirdpartytrust.com/blog/what-is-a-zero-day-exploit/

การโจมตีแบบนี้ถือเป็นภัยคุกคามที่มีความร้ายแรงสูง เนื่องจากผู้โจมตีสามารถใช้ช่องโหว่นี้ในการเข้าถึงระบบหรือข้อมูลที่สำคัญได้ก่อนที่ผู้ดูแลระบบจะมีโอกาสทำการป้องกันหรืออุดช่องโหว่ ทำให้การป้องกันและการตอบสนองต่อการโจมตีแบบฉวยโอกาสมีความท้าทายมากขึ้น

การป้องกันมัลแวร์

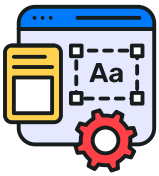
ถอนการติดตั้งปลั๊กอินที่ไม่จำเป็น:

การลดจำนวนซอฟต์แวร์ที่เสี่ยงต่อการโจมตีแบบ Zero-day จะช่วยเพิ่มความปลอดภัยให้กับคอมพิวเตอร์ของคุณ ดังนั้นควรถอนการติดตั้งปลั๊กอินของเบราว์เซอร์ที่คุณไม่ได้ใช้งาน หรือหลีกเลี่ยงการใช้ซอฟต์แวร์ที่ไม่ได้รับความเชื่อถือบนอินเทอร์เน็ต



ติดตั้งโปรแกรมป้องกันไวรัส:

โปรแกรมป้องกันไวรัสมีบทบาทสำคัญในการป้องกันการโจมตีแบบ Zero-day โดยเฉพาะอย่างยิ่งในระบบปฏิบัติการ Windows โปรแกรมป้องกันไวรัสที่มีคุณภาพสามารถวิเคราะห์พฤติกรรมที่น่าสงสัยและบล็อกการโจมตีได้ทันที



อัปเดตซอฟต์แวร์ให้ทันสมัยอยู่เสมอ:

การอัปเดตซอฟต์แวร์เป็นประจำจะช่วยให้คุณได้รับการแก้ไขช่องโหว่ที่อาจถูกโจมตี แม้การอัปเดตจะไม่สามารถป้องกันการโจมตีแบบ Zero-day ได้ร้อยเปอร์เซ็นต์ แต่ก็ช่วยลดความเสี่ยงและป้องกันการสูญเสียได้ การอัปเดตระบบปฏิบัติการและโปรแกรมต่าง ๆ อย่างสม่ำเสมอ จะช่วยให้คุณได้รับแพตช์รักษาความปลอดภัยที่จำเป็น

ตัวอย่างของการโจมตีแบบ Zero-day

ที่มา : https://www.thirdpartytrust.com/blog/what-is-a-zero-day-exploit/

หนึ่งในตัวอย่างที่โด่งดังที่สุดของการโจมตีแบบ Zero-day คือ Stuxnet เวิร์มคอมพิวเตอร์ที่ถูกค้นพบในปี 2010 โดยเจาะจงโจมตีระบบควบคุมของโรงงานนิวเคลียร์ในอิหร่าน เวิร์มนี้ใช้ช่องโหว่ Zero-day หลายช่องโหว่ในระบบปฏิบัติการ Windows และสามารถทำลายเครื่องหมุนเหวี่ยงที่ใช้ในกระบวนการเสริมสมรรถนะยูเรเนียมได้

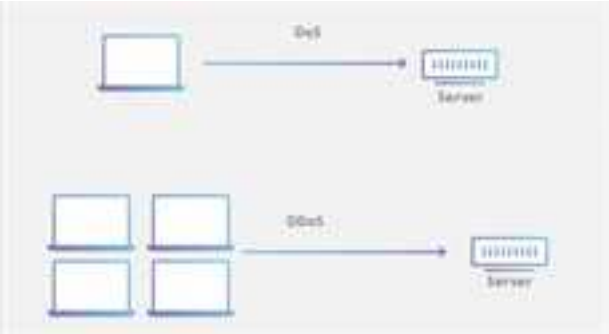
Zoom Zero-day (2020)

https://www.helpnetsecurity.com/2020/07/09/zoom-zero-day-windows/

ในช่วงที่มีการระบาดของ COVID-19 การใช้งานโปรแกรม Zoom เพิ่มขึ้นอย่างมาก ช่องโหว่ Zero-day ใน Zoom บนระบบปฏิบัติการ Windows และ macOS ถูกค้นพบและสามารถใช้ในการควบคุมเครื่องของผู้ใช้ได้ ทำให้เกิดความกังวลเกี่ยวกับความปลอดภัยในการใช้โปรแกรมประชุมทางไกลนี้

การโจมตีแบบปฏิเสธการให้บริการ

Denial-of-Service Attack



ที่มา : https://www.antivirus.in.th/tips/2334.html

DoS Attack หรือ “Denial of Service” เป็นการโจมตีระบบโดยการส่งคำร้อง (Request) จำนวนมากเกินกว่าที่เซิร์ฟเวอร์จะรองรับได้ ส่งผลให้ระบบล่มและไม่สามารถทำงานต่อได้ เมื่อเกิดการโจมตีแบบ DoS ผู้ใช้จะไม่สามารถเข้าถึงเว็บไซต์หรือบริการที่ต้องการได้อีกต่อไป เนื่องจากเซิร์ฟเวอร์ไม่สามารถตอบสนองคำร้องขอใช้งานได้ การโจมตีนี้จึงถูกเรียกว่า “Denial of Service” หรือ “ปฏิเสธการบริการ” ซึ่งสะท้อนถึงผลกระทบที่ทำให้บริการไม่สามารถใช้งานได้

ตัวอย่างการโจมตีแบบ DoS เทคนิค “Buffer Overflow”

ทาง Microsoft ได้อธิบายว่า “Buffer Overflow” เกิดขึ้นเมื่อมีการเขียนข้อมูลในหน่วยความจำที่เกินขีดความสามารถที่หน่วยความจำนั้นรองรับได้ ตัวอย่างเช่น หากโปรแกรมถูกกำหนดให้ประมวลผลข้อมูลขนาด 10 ไบต์ (Bytes) แต่มีข้อมูลขนาด 15 Bytes ถูกส่งเข้ามา จะมีข้อมูลขนาด 5 Bytes ที่เกินออกมา ซึ่งเรียกว่า Buffer Overflow หากเกิดการสะสมจนมีขนาดใหญ่ อาจทำให้โปรแกรมทำงานผิดพลาดหรือแครช เนื่องจาก DoS Attack เป็นการโจมตีจากคอมพิวเตอร์เพียงเครื่องเดียว พลังโจมตีจึงมีสเกลต่ำ แฮกเกอร์จึงมักเลือกโจมตีเว็บไซต์ขนาดเล็กที่มีทรัพยากรจำกัด การป้องกัน DoS Attack นั้นค่อนข้างง่าย หากตรวจพบแหล่งที่มาแล้วก็สามารถปิดกั้น IP address ที่เป็นต้นเหตุได้ เพียงเท่านี้ก็สามารถป้องกันการโจมตีได้

Distributed-Denial-of-Service Attack

DDoS Attack หรือ “Distributed Denial of Service” เป็นการโจมตีที่มีเป้าหมายและรูปแบบคล้ายกับ DoS Attack แต่มีพลังการโจมตีที่มากกว่า โดยความแตกต่างหลักคือ DDoS Attack เป็นการโจมตีเซิร์ฟเวอร์จากอุปกรณ์และอินเทอร์เน็ตจำนวนมากในเวลาเดียวกัน ในขณะที่ DoS Attack มาจากแหล่งที่มาเดียว

DDoS Attack มักใช้ “Botnet” ในการโจมตี โดย Botnet คือเครือข่ายอุปกรณ์จำนวนมากที่ถูกควบคุมโดยแฮกเกอร์ผ่านการแพร่กระจายของมัลแวร์ ซึ่งสามารถแพร่กระจายไปยังคอมพิวเตอร์หรืออุปกรณ์ Internet of Things (IoT) ที่เชื่อมต่อกับอินเทอร์เน็ตได้ เมื่อแฮกเกอร์มีอุปกรณ์ใน Botnet เพียงพอ พวกเขาสามารถใช้ทรัพยากรเหล่านั้นในการทำ DDoS Attack เพื่อโจมตีเซิร์ฟเวอร์เป้าหมายได้

DDoS Attack จะมีการโจมตีอยู่ 2 รูปแบบหลัก ๆ คือ Volume-Based Attacks และ DNS Server Attacks โดย Volume-Based Attacks จะโจมตีไปที่แบนด์วิธของเซิร์ฟเวอร์ ด้วยการระดมส่งคำร้อง (Request) เข้าไปเป็นจำนวนมหาศาล จนระบบไม่สามารถรับมือได้ทัน สุดท้ายก็ล่มไปในที่สุด ส่วน DNS Server Attacks เป็นการโจมตีไปที่ DNS Server โดยตรง ด้วยการปลอมแปลงหมายเลขที่อยู่ไอพี (IP Address) และใช้เลข IP ปลอมในการระดมส่งข้อมูลขยะเข้าไปยังเซิร์ฟเวอร์ของเป้าหมาย

ตัวอย่างการโจมตีแบ DDoS ที่มีชื่อเสียง

Dyn DDoS Attack (2016):

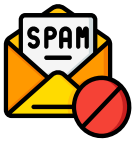
ที่มา : https://mse238blog.stanford.edu/2018/07/clairemw/the-2016-dyn-attack-and-its-lessons-for-iot-security/

ในเดือนตุลาคม 2016 บริษัท Dyn ผู้ให้บริการ DNS ถูกโจมตีด้วยการโจมตี DDoS ขนาดใหญ่ ที่ใช้ Botnet ที่ประกอบด้วยอุปกรณ์ Internet of Things (IoT) การโจมตีนี้ทำให้บริการเว็บไซต์ใหญ่ ๆ เช่น Twitter, Reddit, Netflix, และ Spotify ไม่สามารถใช้งานได้ชั่วคราว

การโจมตีแบบฟิชชิง (Phishing attack)

ฟิชชิง (Phishing) เป็นภัยคุกคามที่ใช้เทคนิคทางวิศวกรรมสังคม (Social engineering) ซึ่งเป็นการหลอกลวงและล่อหลอกผู้อื่น โดยอาศัยหลักการพื้นฐานทางจิตวิทยาเพื่อให้เหยื่อเปิดเผยข้อมูลที่สำคัญและเป็นความลับ

วิธีการทำงานของฟิชชิง



อีเมลหลอกลวง:

ผู้โจมตีจะส่งอีเมลที่ดูน่าเชื่อถือ มักแอบอ้างเป็นองค์กรที่มีชื่อเสียง เช่น ธนาคาร หรือบริษัทเทคโนโลยี อีเมลเหล่านี้มักมีลิงก์ที่นำไปสู่หน้าเพจที่ถูกปลอมแปลงอย่างแนบเนียนให้เหมือนกับหน้าเว็บไซต์จริง ผู้ใช้งานที่ไม่ระวังอาจถูกหลอกให้กรอกข้อมูลบัตรเครดิตหรือข้อมูลสำคัญอื่น ๆ

หน้าเว็บไซต์ปลอม:

หน้าเพจที่ถูกปลอมแปลงมักจะมีรูปลักษณ์และการออกแบบเหมือนกับเว็บไซต์ที่ผู้ใช้คุ้นเคย เพื่อหลอกลวงให้ผู้ใช้กรอกข้อมูลสำคัญ

ไฟล์แนบที่มีมัลแวร์:

ผู้โจมตีอาจแนบไฟล์ที่มีมัลแวร์หรือแรนซัมแวร์ในอีเมล เมื่อผู้ใช้ดาวน์โหลดและเปิดไฟล์นี้ จะติดตั้งมัลแวร์ในคอมพิวเตอร์ของผู้ใช้หรือองค์กร ส่งผลให้เกิดความเสียหายและการโจรกรรมข้อมูล

วิธีการป้องกัน

ตรวจสอบอีเมลและลิงก์:

อย่าคลิกลิงก์หรือดาวน์โหลดไฟล์จากอีเมลที่ไม่แน่ใจหรือไม่รู้จัก ตรวจสอบที่อยู่อีเมลผู้ส่งและลิงก์อย่างละเอียด

ใช้การยืนยันตัวตนสองขั้นตอน (2FA):

เพิ่มความปลอดภัยให้บัญชีออนไลน์โดยใช้การยืนยันตัวตนสองขั้นตอน

ติดตั้งซอฟต์แวร์ป้องกันไวรัสและมัลแวร์:

ใช้ซอฟต์แวร์ป้องกันไวรัสและมัลแวร์ที่มีการอัปเดตล่าสุด

อัปเดตซอฟต์แวร์:

อัปเดตระบบปฏิบัติการและซอฟต์แวร์ให้เป็นเวอร์ชันล่าสุดเพื่อลดช่องโหว่ทางความปลอดภัย

กรณีศึกษา: ตัวอย่างการโจมตีทางไซเบอร์ที่เกิดขึ้นจริงในภาคอุตสาหกรรม

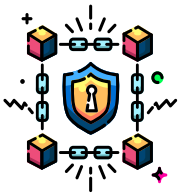
การโจมตีระบบโรงงานผลิต

การโจมตีทางไซเบอร์ในภาคอุตสาหกรรมของไทยเกิดขึ้นอย่างต่อเนื่องและหลากหลาย โดยเป้าหมายที่ถูกโจมตีรวมถึงระบบโรงงานผลิต ระบบธนาคาร และระบบโรงพยาบาล ซึ่งมีตัวอย่างและกรณีศึกษาดังนี้

ตัวอย่างที่สำคัญ ของการโจมตีในภาคโรงงานผลิตในไทยคือ การโจมตีระบบควบคุมการผลิต (Industrial Control Systems - ICS) ที่เกิดขึ้นกับโรงงานผลิตชิ้นส่วนอิเล็กทรอนิกส์ในปี 2018 โดยแฮกเกอร์ใช้มัลแวร์เข้าโจมตีระบบ ทำให้สายการผลิตหยุดชะงักเป็นเวลาหลายชั่วโมง ซึ่งมีผลกระทบต่อการผลิตและการจัดส่งสินค้าไปยังลูกค้า

วิธีการโจมตี:
มัลแวร์เจาะเข้าระบบ ICS ผ่านช่องโหว่ของซอฟต์แวร์ที่ไม่ได้รับการอัปเดต

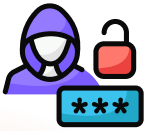
ผลกระทบ:
สายการผลิตหยุดชะงักเป็นเวลาหลายชั่วโมง ส่งผลให้เกิดความล่าช้าในการผลิตและการจัดส่งสินค้า



การตอบสนอง:
การตรวจสอบและปรับปรุงระบบความปลอดภัยทางไซเบอร์ของโรงงาน รวมถึงการอัปเดตซอฟต์แวร์และการฝึกอบรมพนักงาน

การโจมตีระบบธนาคาร

ในปี 2016 ธนาคารพาณิชย์หลายแห่งในไทย ตกเป็นเป้าหมายของการโจมตีด้วยมัลแวร์ที่เรียกว่า “Skimming” ซึ่งแฮกเกอร์ทำการติดตั้งอุปกรณ์ขโมยข้อมูลบนเครื่อง ATM ของธนาคาร ทำให้ข้อมูลบัตรเครดิตและบัตรเดบิตของลูกค้าถูกขโมยและนำไปใช้ในทางที่ผิด ส่งผลให้ธนาคารต้องใช้เวลาหลายเดือนในการฟื้นฟูระบบและชดเชยความเสียหายให้กับลูกค้า



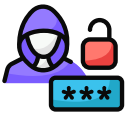
วิธีการโจมตี:
การติดตั้งอุปกรณ์ skimming บนเครื่อง ATM และการใช้มัลแวร์เพื่อดักจับข้อมูลบัตร

ผลกระทบ:
ข้อมูลบัตรเครดิตและบัตรเดบิตของลูกค้าถูกขโมยและใช้ในทางที่ผิด ทำให้เกิดความเสียหายทางการเงิน

การตอบสนอง:
การตรวจสอบและเปลี่ยนแปลงเครื่อง ATM ที่ถูกโจมตี การเพิ่มมาตรการรักษาความปลอดภัย และการให้ความรู้แก่ลูกค้าเกี่ยวกับการป้องกันการถูกขโมยข้อมูล

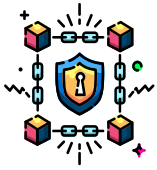
การโจมตีระบบโรงพยาบาล

ในปี 2020 โรงพยาบาลรัฐแห่งหนึ่งในไทยถูกโจมตีด้วย Ransomware ที่เรียกว่า “WannaCry” ซึ่งทำให้ระบบสารสนเทศของโรงพยาบาลทั้งหมดถูกเข้ารหัสและไม่สามารถใช้งานได้ ผู้โจมตีเรียกค่าไถ่เป็นเงินสกุล Bitcoin เพื่อแลกกับการปลดล็อคระบบ เหตุการณ์นี้ทำให้การบริการผู้ป่วยหยุดชะงัก และต้องย้ายผู้ป่วยบางส่วนไปยังโรงพยาบาลอื่น



วิธีการโจมตี:
Ransomware ที่เข้ารหัสข้อมูลระบบสารสนเทศของโรงพยาบาล

ผลกระทบ:
การบริการผู้ป่วยหยุดชะงัก การเข้าถึงข้อมูลผู้ป่วย และการประสานงานทางการแพทย์หยุดชะงัก



การตอบสนอง:
การกู้คืนข้อมูลสำรอง การเสริมสร้างระบบความปลอดภัยทางไซเบอร์ และการฝึกอบรมพนักงานเกี่ยวกับการป้องกันและรับมือกับ Ransomware

การโจมตีทางไซเบอร์ในภาคอุตสาหกรรมในไทยเป็นภัยคุกคามที่เพิ่มขึ้นอย่างต่อเนื่อง ทุกองค์กรควรให้ความสำคัญกับการป้องกันและการตอบสนองต่อการโจมตีเหล่านี้อย่างมีประสิทธิภาพ เพื่อปกป้องข้อมูลและการดำเนินงานของตนเอง

ภัยคุกคามจากภายใน (Insider Threat)

เป็นภัยคุกคามที่เกิดจากบุคลากรขององค์กร ซึ่งอาจจะเกิดจากความตั้งใจ หรือไม่ตั้งใจ ผ่านช่องทางการใช้งานปกติของบุคลากร เช่น เครื่องคอมพิวเตอร์ของบริษัท หรือ สมาร์ตโฟน เป็นต้น ซึ่ง Insider threat เป็นภัยประเภทที่มีความรุนแรงเนื่องจากภายในองค์กร อาจจะมีการป้องกันในระดับต่ำ ทำให้เกิดการโจมตีประเภทนี้ได้ง่าย และผลลัพธ์ของภัยนี้มีความรุนแรง

ประเภทของภัยคุกคามจากภายใน

ภัยคุกคามจากภายในสามารถแบ่งออกเป็นหลายประเภท ได้แก่

การทุจริต: การกระทำที่ผิดกฎหมายหรือไม่เหมาะสมเพื่อผลประโยชน์ส่วนตัว

การก่อวินาศกรรม: การทำลายทรัพย์สินหรือข้อมูลขององค์กร

การขโมยทรัพย์สินทางปัญญา: การนำข้อมูลหรือทรัพย์สินทางปัญญาออกไปจากองค์กร

การเปิดเผยข้อมูล: การเผยแพร่ข้อมูลที่เป็นความลับขององค์กรโดยไม่ได้รับอนุญาต

การใช้ทรัพยากรในกิจกรรมที่ผิดกฎหมาย: การใช้ระบบหรือทรัพยากรขององค์กรในการทำกิจกรรมที่ผิดกฎหมาย

ผลกระทบของภัยคุกคามจากภายใน

ผลกระทบที่เกิดจากภัยคุกคามจากภายในมีมากมาย เช่น ความสูญเสียทางการเงิน การเสื่อมเสียชื่อเสียง การสูญเสียข้อมูลสำคัญ และการถูกลงโทษทางกฎหมาย นอกจากนี้ยังส่งผลกระทบต่อความเชื่อมั่นของลูกค้าและคู่ค้าทางธุรกิจ

การป้องกันและการจัดการภัยคุกคามจากภายใน

การจัดการกับภัยคุกคามจากภายใน ต้องเริ่มจากการตระหนักถึงความเสี่ยงและความสำคัญของการป้องกัน ภายในองค์กรควรมีนโยบายและกระบวนการที่ชัดเจน ในการป้องกันและตรวจสอบการกระทำที่อาจเป็นภัยคุกคาม ตัวอย่างของมาตรการที่สามารถนำมาใช้ได้ ได้แก่

การฝึกอบรมพนักงาน: เพื่อให้พนักงานเข้าใจถึงความสำคัญของการรักษาความปลอดภัยของข้อมูลและวิธีการป้องกันภัยคุกคาม

การตรวจสอบสิทธิ์การเข้าถึงข้อมูล: การกำหนดและตรวจสอบสิทธิ์การเข้าถึงข้อมูล เพื่อให้แน่ใจว่าผู้ที่เข้าถึงข้อมูลมีสิทธิ์และมีความจำเป็นในการเข้าถึง

การติดตามและตรวจสอบ: การใช้เครื่องมือและเทคโนโลยีในการติดตาม และตรวจสอบการเข้าถึงและการใช้ข้อมูล

การประเมินความเสี่ยง: การประเมินความเสี่ยงที่เกี่ยวข้องกับภัยคุกคามจากภายใน และการปรับปรุงกระบวนการป้องกันอย่างต่อเนื่อง

บทบาทของผู้ตรวจสอบภายใน

ผู้ตรวจสอบภายในมีบทบาทสำคัญในการป้องกันและจัดการกับภัยคุกคามจากภายใน พวกเขาควรมีความรู้และความเข้าใจในภัยคุกคาม และสามารถให้คำแนะนำในการปรับปรุงการควบคุมและกระบวนการภายในองค์กรได้

กรณีศึกษา: ตัวอย่างของการเกิดภัยคุกคามจากภายใน

ที่มา: https://www.tba.or.th/

เหตุการณ์การเปิดเผยข้อมูลลูกค้าในธนาคารแห่งหนึ่ง พนักงานธนาคารทำการขายข้อมูลลูกค้าของธนาคารให้กับบุคคลภายนอก ทำให้ลูกค้าถูกละเมิดความเป็นส่วนตัว และธนาคารต้องรับผิดชอบในการปกป้องข้อมูล

ความเสี่ยงด้านความปลอดภัยบนคลาวด์ (Cloud Security)

Cloud Computing คือ การให้บริการทรัพยากรคอมพิวเตอร์ผ่านอินเทอร์เน็ต ซึ่งประกอบด้วยเซิร์ฟเวอร์ที่ถูกจัดเก็บไว้ที่ศูนย์ข้อมูล (data centers) ที่มีการบริหารจัดการโดยผู้ให้บริการคลาวด์ เช่น Amazon Web Services (AWS), Microsoft Azure, และ Google Cloud Platform (GCP) การให้บริการคลาวด์สามารถแบ่งออกเป็นหลายประเภทหลัก ๆ ดังนี้:

Infrastructure as a Service (IaaS): การให้บริการทรัพยากรพื้นฐาน เช่น เซิร์ฟเวอร์เสมือน (virtual servers), เน็ตเวิร์ค และการจัดเก็บข้อมูล ผู้ใช้สามารถจัดการและควบคุมระบบปฏิบัติการและแอปพลิเคชันของตนเอง

Platform as a Service (PaaS): การให้บริการแพลตฟอร์มสำหรับการพัฒนาและทดสอบแอปพลิเคชัน ผู้ใช้สามารถมุ่งเน้นที่การเขียนและทดสอบโค้ดโดยไม่ต้องจัดการทรัพยากรพื้นฐาน

Software as a Service (SaaS): การให้บริการแอปพลิเคชันสำเร็จรูปผ่านอินเทอร์เน็ต เช่น อีเมล การจัดการลูกค้าสัมพันธ์ (CRM) และซอฟต์แวร์การจัดการโปรเจกต์

Cloud Security คืออะไร

Cloud Security คือ การปกป้องข้อมูล แอปพลิเคชัน และโครงสร้างพื้นฐานที่อยู่ในระบบคลาวด์จากภัยคุกคามทางไซเบอร์ ความปลอดภัยบนคลาวด์ครอบคลุมหลายด้าน เช่น การควบคุมการเข้าถึง การเข้ารหัสข้อมูล การสำรองข้อมูล และการตรวจสอบกิจกรรมที่ไม่พึงประสงค์ โดยมีเป้าหมายเพื่อให้การใช้บริการคลาวด์ปลอดภัยและมีความน่าเชื่อถือ

ความเสี่ยงจาก Cloud

การใช้บริการคลาวด์มีความเสี่ยงหลายประการ ซึ่งสามารถแบ่งออกเป็นประเภทต่าง ๆ ได้ดังนี้:

การสูญเสียข้อมูล: ข้อมูลสำคัญอาจสูญหายได้เนื่องจากความผิดพลาดของมนุษย์ ความผิดพลาดของระบบ หรือการโจมตีทางไซเบอร์

การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต: การโจมตีแบบ Brute Force การใช้ข้อมูลประจำตัวที่ถูกขโมย หรือการโจมตีช่องโหว่ของระบบ สามารถทำให้ผู้ไม่หวังดีเข้าถึงข้อมูลได้

การหยุดชะงักของบริการ: การโจมตีแบบ DDoS หรือความล้มเหลวของโครงสร้างพื้นฐาน สามารถทำให้บริการคลาวด์หยุดทำงานชั่วคราวหรือยาวนานได้

กรณีศึกษา:
ตัวอย่างภัยบน Cloud

ที่มา: https://mgronline.com/around/detail/9620000072520

Capital One ถูกโจมตีโดยแฮกเกอร์ที่สามารถเข้าถึงข้อมูลส่วนตัวของลูกค้ากว่า 100 ล้านคน ผ่านช่องโหว่ในการตั้งค่าระบบคลาวด์ AWS ซึ่งแสดงให้เห็นถึงความสำคัญของการตั้งค่าความปลอดภัยที่เหมาะสม

Verizon Data Exposure (2017)

ที่มา: https://9to5mac.com/2022/05/27/verizon-data-base-hacked/

Verizon ทำข้อมูลส่วนตัวของลูกค้ารั่วไหล เนื่องจากการตั้งค่าคลาวด์ AWS ที่ไม่ปลอดภัย ทำให้ข้อมูลลูกค้า 14 ล้านราย ถูกเปิดเผยบนอินเทอร์เน็ต

แนวทางปฏิบัติ

เพื่อป้องกันภัยคุกคามและลดความเสี่ยงจากการใช้บริการคลาวด์ ควรพิจารณาแนวทางปฏิบัติดังนี้:

การเลือกผู้ให้บริการคลาวด์ที่มีความน่าเชื่อถือ: เลือกผู้ให้บริการที่มีชื่อเสียง มีมาตรฐานความปลอดภัยที่ชัดเจน และมีการรับรองจากองค์กรที่เกี่ยวข้อง เช่น ISO 27001

การเข้ารหัสข้อมูล: เข้ารหัสข้อมูลทั้งขณะส่งและขณะเก็บ เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต การใช้การเข้ารหัสที่แข็งแกร่งช่วยลดความเสี่ยงจากการโจมตีได้มาก

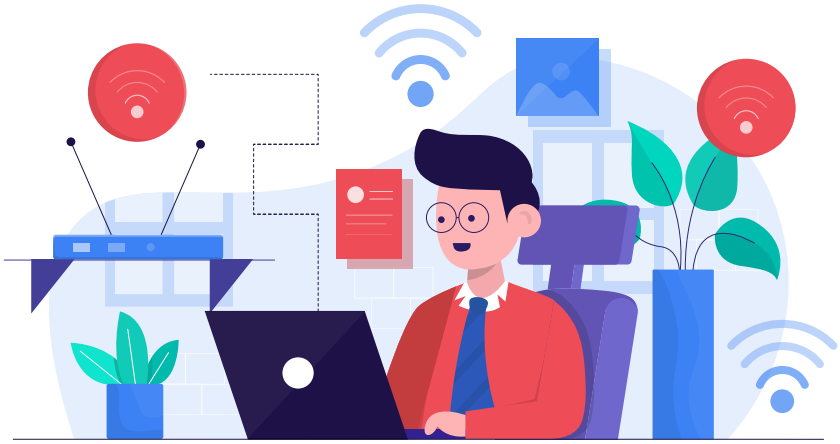
การสำรองข้อมูล: สำรองข้อมูลเป็นประจำ และเก็บสำรองในสถานที่ที่ปลอดภัย เพื่อให้สามารถกู้คืนข้อมูลได้ หากเกิดการสูญหายหรือถูกโจมตี

การจัดการการเข้าถึง: ใช้การยืนยันตัวตนแบบหลายปัจจัย (MFA) และกำหนดสิทธิ์การเข้าถึงที่เหมาะสมให้กับผู้ใช้แต่ละคน เพื่อลดโอกาสการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

การตรวจสอบและติดตาม: ติดตามและตรวจสอบกิจกรรมบนคลาวด์อย่างต่อเนื่อง เพื่อตรวจจับและตอบสนองต่อเหตุการณ์ที่ไม่พึงประสงค์ได้อย่างรวดเร็ว

เทคโนโลยีใหม่ ๆ ที่อาจเป็นช่องโหว่ของระบบ

IoT คืออะไร



IoT (Internet of Things) คือเครือข่ายของอุปกรณ์ที่สามารถเชื่อมต่อและสื่อสารกันผ่านอินเทอร์เน็ตได้ อุปกรณ์เหล่านี้อาจเป็นได้ตั้งแต่เครื่องใช้ไฟฟ้าในบ้าน รถยนต์ อุปกรณ์สวมใส่ ไปจนถึงเซ็นเซอร์ในโรงงานอุตสาหกรรม IoT ช่วยให้การเชื่อมต่อและการแลกเปลี่ยนข้อมูลระหว่างอุปกรณ์เกิดขึ้นได้อย่างราบรื่นและมีประสิทธิภาพ

ความเสี่ยงของ IoT

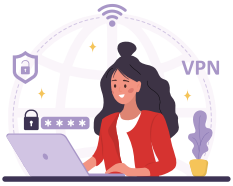
การขาดความปลอดภัยพื้นฐาน: อุปกรณ์ IoT บางรุ่นมักไม่มีการเข้ารหัสข้อมูล หรือมีการรักษาความปลอดภัยที่ไม่เพียงพอ ทำให้ข้อมูลสามารถถูกดักฟังหรือแก้ไขได้ง่าย

การตั้งค่ามาตรฐานที่ไม่ปลอดภัย: อุปกรณ์ IoT มักมาพร้อมกับรหัสผ่านมาตรฐานที่ผู้ใช้ไม่ได้เปลี่ยนแปลง ซึ่งสามารถถูกโจมตีได้ง่าย

การอัปเดตซอฟต์แวร์ไม่สม่ำเสมอ: ผู้ผลิตบางรายไม่สนับสนุนการอัปเดตซอฟต์แวร์อย่างต่อเนื่อง ทำให้อุปกรณ์มีช่องโหว่จากซอฟต์แวร์เวอร์ชันเก่า

การเชื่อมต่อที่ไม่ปลอดภัย: การเชื่อมต่ออินเทอร์เน็ตที่ไม่ปลอดภัย อาจเป็นช่องทางให้ผู้โจมตีเข้าถึงอุปกรณ์ IoT ได้

กรณีศึกษา:
ตัวอย่างของการเกิดภัยคุกคามจาก IoT



ที่มา: https://mgronline.com/around/detail/9620000072520

การโจมตีของ Mirai Botnet ในปี 2016 ซึ่งใช้การโจมตีแบบ Distributed Denial of Service (DDoS) โดยการควบคุมอุปกรณ์ IoT จำนวนมากที่มีการตั้งค่าความปลอดภัยที่ไม่ดี ทำให้เว็บไซต์และบริการหลายแห่งไม่สามารถใช้งานได้

AI คืออะไร

AI (Artificial Intelligence) คือเทคโนโลยีที่ทำให้คอมพิวเตอร์สามารถทำงานที่ต้องการความฉลาดของมนุษย์ได้ เช่น การเรียนรู้วิเคราะห์ แก้ปัญหา และตัดสินใจ AI มีการใช้งานในหลาย ๆ ด้าน เช่น การแพทย์ การเงิน การผลิต และการบริการ

ความเสี่ยงของ IoT

ความผิดพลาดในการเรียนรู้: หากข้อมูลที่ใช้ในการฝึก AI มีความผิดพลาดหรือไม่สมบูรณ์ AI อาจเรียนรู้สิ่งที่ผิดพลาดและให้ผลลัพธ์ที่ไม่ถูกต้อง

การโจมตีด้วยข้อมูล (Data Poisoning): การใส่ข้อมูลที่ผิดพลาดหรือเจตนาทำให้ AI เรียนรู้สิ่งที่ผิด ทำให้ผลลัพธ์ของ AI ไม่ถูกต้อง หรือเป็นไปตามที่ผู้โจมตีต้องการ

ความไม่โปร่งใส (Black Box): กระบวนการทำงานของ AI บางครั้งไม่สามารถอธิบายได้อย่างชัดเจน ทำให้ยากต่อการตรวจสอบและปรับปรุง

การโจมตีทางไซเบอร์: AI อาจถูกโจมตีเพื่อเปลี่ยนแปลงการทำงานของระบบ หรือถูกนำไปใช้ในการโจมตีทางไซเบอร์ เช่น การใช้ AI ในการพัฒนาแฮกเกอร์ต่าง ๆ

กรณีศึกษา:
ตัวอย่างของการเกิดภัยคุกคามจาก AI

ที่มา: https://mgronline.com/around/detail/9620000072520

การใช้ปัญญาประดิษฐ์ (AI) โดยอาชญากรไซเบอร์เพื่อโจมตีองค์กรอย่างมีประสิทธิภาพ โดย AI ถูกใช้ในการเขียนมัลแวร์ที่ซับซ้อนมากขึ้น สร้างสคริปต์ซอฟต์แวร์ประสงค์ร้าย และช่วยในการสอดแนมและหลบเลี่ยงการตรวจจับ ทำให้การโจมตีมีความซับซ้อนและต่อเนื่องมากขึ้น AI ยังถูกนำมาใช้ในขั้นตอนการวิเคราะห์ข้อมูลเพื่อหาช่องโหว่และเจาะระบบได้

วิธีระบุภัยคุกคาม

การระบุภัยคุกคามและเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ เป็นสิ่งสำคัญในการปกป้องข้อมูลและระบบขององค์กร นี่คือขั้นตอนและเครื่องมือที่สามารถนำมาใช้เพื่อระบุและตอบสนองต่อภัยคุกคาม

การตรวจจับภัยคุกคาม

การเฝ้าระวังระบบ (System Monitoring)

1. SIEM (Security Information and Event Management): รวมรวบและวิเคราะห์ข้อมูลความปลอดภัยจากแหล่งต่าง ๆ เพื่อระบุพฤติกรรมที่ผิดปกติ

2. การตรวจสอบล็อกไฟล์ (Log Monitoring): ตรวจสอบบันทึกกิจกรรมของระบบอย่างต่อเนื่องเพื่อหาสัญญาณของการโจมตี

การวิเคราะห์พฤติกรรม (Behavior Analysis)

1. UEBA (User and Entity Behavior Analytics): วิเคราะห์พฤติกรรมของผู้ใช้และระบบ เพื่อระบุพฤติกรรมที่ผิดปกติหรือเป็นภัยคุกคาม

2. Machine Learning: ใช้เทคโนโลยีแมชชีนเลิร์นนิงในการวิเคราะห์และคาดการณ์ภัยคุกคาม

การระบุเหตุการณ์ด้านความมั่นคงปลอดภัย

การตรวจจับเหตุการณ์ (Incident Detection)

1. IDS/IPS (Intrusion Detection/Prevention Systems): ตรวจจับและป้องกันการบุกรุกจากภายนอกและภายในระบบ
2. การตั้งค่าการแจ้งเตือน (Alert Configuration): ตั้งค่าให้ระบบส่งการแจ้งเตือนเมื่อพบกิจกรรมที่น่าสงสัย

การประเมินผลกระทบ (Impact Assessment)

1. Risk Assessment: ประเมินความเสี่ยงและผลกระทบที่เกิดจากเหตุการณ์ต่าง ๆ
2. Prioritization: กำหนดลำดับความสำคัญของเหตุการณ์เพื่อการตอบสนองที่รวดเร็วและมีประสิทธิภาพ

การตอบสนองต่อเหตุการณ์

การจัดการเหตุการณ์ (Incident Response)

1.การจัดตั้งทีมตอบสนอง (Incident Response Team): ทีมที่มีหน้าที่เฉพาะในการจัดการและตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัย
2. แผนการตอบสนอง (Response Plan): วางแผนและเตรียมขั้นตอนการตอบสนองต่อเหตุการณ์ เช่น การกักกัน การกู้คืน และการรายงาน

ตัวอย่างวิธีการป้องกัน และตอบสนอง

การสำรองข้อมูล (Data Backup): สำรองข้อมูลสำคัญอย่างสม่ำเสมอ เพื่อลดความเสี่ยงจากการสูญหายของข้อมูล

การฝึกอบรมพนักงาน (Employee Training): ให้ความรู้และฝึกอบรมพนักงาน เกี่ยวกับการระบุและตอบสนองต่อภัยคุกคาม

การอัปเดตระบบ (System Updates): อัปเดตระบบปฏิบัติการและซอฟต์แวร์อย่างสม่ำเสมอ เพื่อปิดช่องโหว่ด้านความปลอดภัย

วิธีการประเมินช่องโหว่ (Vulnerability Assessment)

การประเมินช่องโหว่คืออะไร

การประเมินช่องโหว่ คือ การตรวจสอบช่องโหว่ของระบบ ตั้งแต่ช่องโหว่ในกระบวนการทำงานของระบบ เซิร์ฟเวอร์ และเครือข่าย ไปจนถึงอุปกรณ์รักษาความปลอดภัย ทำให้ทราบถึงช่องโหว่ภายในองค์กร และนำไปสู่การแก้ไขปรับปรุงได้อย่างถูกจุด อันเป็นการลดความเสี่ยงจากภัยคุกคามที่อาจเกิดขึ้น

การสแกนช่องโหว่ (Vulnerability Scanning)

การสแกนช่องโหว่ หรือที่เรียกกันทั่วไปว่า VA Scan เป็นกระบวนการที่ใช้เครื่องมืออัตโนมัติเพื่อสแกนระบบเป็นระยะ ๆ เพื่อค้นหาจุดอ่อนที่อาจเกิดขึ้นได้ โดยเครื่องมือเหล่านี้ สามารถตั้งโปรแกรมให้สแกนหรือค้นหาเฉพาะองค์ประกอบที่เลือกภายในระบบได้อย่างละเอียดและแม่นยำ เช่น Nessus, OpenVAS, QualysGuard, Nikto เป็นต้น

การทดสอบการเจาะระบบ (Penetration Testing)

การทดสอบการเจาะระบบ หรือที่เรียกกันทั่วไปว่า Pentest เป็นการจำลองการโจมตีระบบคอมพิวเตอร์ เพื่อประเมินความปลอดภัยของระบบ โดยทีมผู้เชี่ยวชาญที่ผ่านการฝึกอบรมจะทำการโจมตีในหลายรูปแบบ หรือใช้เครื่องมือทดสอบการเจาะระบบหลายชนิด โดยพิจารณาจากจุดแข็งและจุดอ่อนของระบบ เพื่อทดสอบความเสี่ยงและความทนทานของระบบต่อการโจมตีจากภัยคุกคาม

การตรวจสอบช่องโหว่ด้วยตนเอง (Manual Vulnerability Assessment)

การตรวจสอบช่องโหว่ด้วยตนเอง คือ กระบวนการที่ผู้เชี่ยวชาญด้านความปลอดภัยทำการตรวจสอบระบบหรือแอปพลิเคชันเพื่อค้นหาช่องโหว่ที่อาจมีอยู่ โดยใช้ความรู้และทักษะทางเทคนิค เพื่อค้นหาข้อบกพร่องที่ไม่สามารถตรวจจับได้ด้วยเครื่องมือสแกนช่องโหว่อัตโนมัติ

การตรวจสอบโค้ด (Code Review)

การตรวจสอบโค้ด เป็นกระบวนการที่มุ่งเน้นที่จะตรวจสอบโค้ดของโปรแกรมหรือแอปพลิเคชัน เพื่อค้นหาข้อผิดพลาดหรือบั๊ก ที่อาจเป็นจุดอ่อนที่สามารถถูกโจมตีได้

การทดสอบการเจาะระบบ (Penetration Testing)

วัตถุประสงค์ของการทดสอบการเจาะระบบ Penetration Testing:

ระบุและประเมินช่องโหว่: ค้นหาและประเมินช่องโหว่ที่อาจมีอยู่ในระบบหรือแอปพลิเคชัน เพื่อทำความเข้าใจถึงจุดอ่อนที่อาจถูกแฮกเกอร์ใช้ประโยชน์

ทดสอบมาตรการป้องกัน: ตรวจสอบความสามารถของมาตรการป้องกันที่มีอยู่ ในการป้องกันการโจมตีและประเมินว่าระบบสามารถทนทานต่อภัยคุกคามได้อย่างไร

ประเมินความเสี่ยง: ประเมินความเสี่ยงที่เกี่ยวข้องกับช่องโหว่ที่พบ และให้ข้อเสนอแนะในการลดความเสี่ยงเหล่านั้น

ตรวจสอบการปฏิบัติตามมาตรฐาน: ตรวจสอบว่าระบบปฏิบัติตามข้อกำหนดและมาตรฐานความปลอดภัยต่าง ๆ เช่น PCI-DSS, HIPAA, ISO/IEC 27001 หรืออื่น ๆ

เพิ่มความมั่นใจในความปลอดภัยของระบบ: เพิ่มความมั่นใจให้กับผู้บริหารและลูกค้า ว่าระบบมีความปลอดภัยและมีการตรวจสอบเป็นประจำ

ปรับปรุงมาตรการรักษาความปลอดภัย: ให้ข้อมูลที่จำเป็นสำหรับการปรับปรุงมาตรการรักษาความปลอดภัยและการบริหารจัดการความเสี่ยงในอนาคต

ทดสอบการตอบสนองต่อเหตุการณ์: ทดสอบและประเมินความพร้อมของทีมในการตอบสนองต่อการโจมตีจริง รวมถึงการจัดการเหตุการณ์และการฟื้นฟูระบบ

ประเภทของการทดสอบการเจาะระบบ:

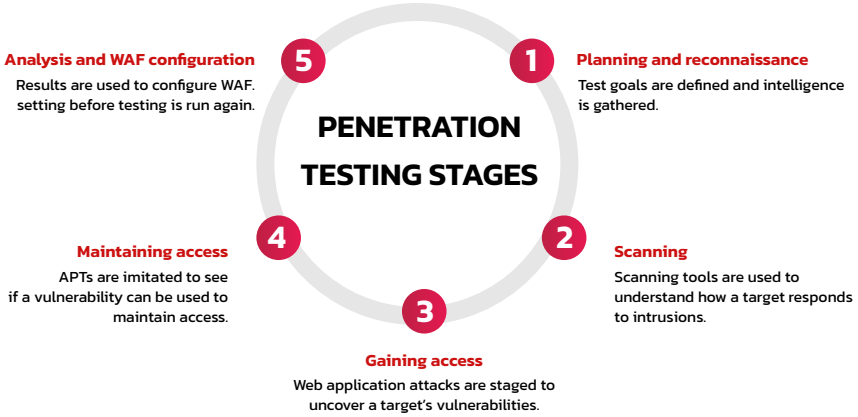
รูปแบบที่รองรับการทำ Pen Test

Black Box Testing: เป็นการเจาะระบบจากภายนอกเครือข่ายขององค์กร โดยมีเป้าหมายเพื่อหาทางเข้าสู่ระบบเครือข่าย และประเมินความเสี่ยงและช่องโหว่ต่าง ๆ ซึ่งรวมถึงความเสี่ยงที่อาจมีผลกระทบต่อธุรกิจ ผู้ทดสอบจะไม่ได้รับข้อมูลใด ๆ เกี่ยวกับระบบล่วงหน้า ทำให้การทดสอบนี้จำลองสถานการณ์การโจมตีจากแฮกเกอร์ภายนอกได้อย่างแท้จริง

Gray Box Testing: เป็นการผสมผสานระหว่าง Black Box และ White Box โดยผู้ทดสอบจะได้รับข้อมูลบางส่วนเกี่ยวกับระบบจากผู้ว่าจ้าง ทำให้สามารถประเมินความเสี่ยงได้ทั้งจากภายในและภายนอกเครือข่ายขององค์กร การทดสอบแบบ Gray Box ช่วยให้สามารถตรวจสอบช่องโหว่ได้อย่างครอบคลุมมากขึ้น เนื่องจากมีข้อมูลเบื้องต้นบางประการที่ช่วยในการค้นหาช่องโหว่ได้รวดเร็วและแม่นยำยิ่งขึ้น

White Box Testing: เป็นการเจาะระบบจากภายในองค์กร ผู้ทดสอบจะได้รับข้อมูลทั้งหมดเกี่ยวกับระบบ รวมถึงซอร์สโค้ดและโครงสร้างเครือข่าย ทำให้สามารถประเมินความเสี่ยงภายในองค์กรได้อย่างละเอียด การทดสอบแบบ White Box ช่วยให้สามารถระบุและแก้ไขช่องโหว่ได้อย่างมีประสิทธิภาพ เนื่องจากมีการเข้าถึงข้อมูลและระบบอย่างครบถ้วน

ขั้นตอนการทดสอบการเจาะระบบ



การวางแผน: การกำหนดขอบเขตและเป้าหมายของการทดสอบ รวมถึงการระบุระบบที่จะถูกทดสอบและวิธีการทดสอบที่จะใช้ มีการรวบรวมข้อมูล เช่น ชื่อเครือข่ายและโดเมน เซิร์ฟเวอร์อีเมล เพื่อทำความเข้าใจวิธีการทำงานของระบบเป้าหมายและจุดอ่อนที่อาจเกิดขึ้นได้อย่างละเอียด

การสแกน: การทำความเข้าใจว่าแอปพลิเคชันเป้าหมายจะตอบสนองต่อความพยายามในการบุกรุกอย่างไร โดยทั่วไปแบ่งการวิเคราะห์ออกเป็นสองประเภท

การวิเคราะห์แบบสถิตย์: ตรวจสอบโค้ดของแอปพลิเคชันเพื่อประเมินลักษณะการทำงานขณะไม่ได้ใช้งาน เครื่องมือเหล่านี้สามารถสแกนโค้ดทั้งหมดได้ในครั้งเดียว

การวิเคราะห์แบบไดนามิก: ตรวจสอบโค้ดของแอปพลิเคชันในขณะกำลังทำงาน ซึ่งเป็นวิธีการที่มีประสิทธิภาพมากกว่า เนื่องจากให้มุมมองแบบเรียลไทม์เกี่ยวกับการทำงานของแอปพลิเคชัน

การเข้าถึง: การโจมตีด้วยเว็บแอปพลิเคชัน เช่น การเขียนสคริปต์ข้ามไซต์ (Cross-site scripting), การฉีด SQL (SQL injection) และ Backdoors เพื่อเปิดเผยช่องโหว่ของระบบ จากนั้นผู้ทดสอบจะพยายามใช้ประโยชน์จากช่องโหว่เหล่านี้ เช่น การเพิ่มสิทธิ์ การขโมยข้อมูล และการสกัดกั้นการรับส่งข้อมูล เพื่อทำความเข้าใจถึงความเสียหายที่อาจเกิดขึ้นได้

การรักษาการเข้าถึง: มีเป้าหมายเพื่อตรวจสอบว่า ช่องโหว่ที่พบสามารถนำมาใช้โจมตีอย่างต่อเนื่อง หรือนานพอที่จะทำให้ผู้ไม่หวังดีเข้าถึงข้อมูลได้ลึกขึ้นหรือไม่ โดยเลียนแบบภัยคุกคามขั้นสูงที่อาจอยู่ในระบบเป็นเวลาหลายเดือน เพื่อขโมยข้อมูลที่ละเอียดอ่อนที่สุดขององค์กร

บทวิเคราะห์: ผลลัพธ์จากการทดสอบจะถูกรวบรวมเป็นรายงานรายละเอียด ซึ่งประกอบด้วย

ช่องโหว่เฉพาะที่ถูกโจมตี

ข้อมูลละเอียดอ่อนที่ถูกเข้าถึงได้

ระยะเวลาที่ผู้ทดสอบสามารถคงอยู่ในระบบโดยไม่ถูกตรวจพบ

ทำความรู้จักข้อมูลเบื้องต้นของระบบสแกนช่องโหว่ (Vulnerability Scanner)

Open Source

OpenVAS

ที่มา: Greenbone Community Forum, New OpenVAS logo

OpenVAS (Open Vulnerability Assessment System) เป็นเครื่องมือสแกนช่องโหว่ที่พัฒนามาจากโปรเจกต์ Nessus เวอร์ชันเก่า เป็นเครื่องมือโอเพ่นซอร์สที่ให้บริการฟรี ประกอบด้วยชุดเครื่องมือสำหรับการสแกน การจัดการ และการรายงานช่องโหว่

จุดเด่น

1. **ชุมชนผู้ใช้และนักพัฒนาที่มีชีวิตชีวา** ซึ่งทำงานปรับปรุงเครื่องมือและอัปเดตข้อมูลภัยคุกคามล่าสุดอย่างต่อเนื่อง
2. **ปลั๊กอินที่หลากหลาย** ช่วยให้สามารถปรับแต่งได้ตามความต้องการเฉพาะของผู้ใช้
3. **ความสามารถในการรายงานโดยละเอียด** ช่วยให้ผู้ใช้เข้าใจจุดอ่อนของระบบ และสร้างกลยุทธ์การบรรเทาผลกระทบที่มีประสิทธิภาพ

Nikto

ที่มา: Bug Zero, Nikto

Nikto เป็นเครื่องมือสแกนช่องโหว่เว็บเซิร์ฟเวอร์โอเพ่นซอร์ส ออกแบบมาเพื่อค้นหาช่องโหว่และการกำหนดค่าที่ไม่ปลอดภัยในเว็บเซิร์ฟเวอร์

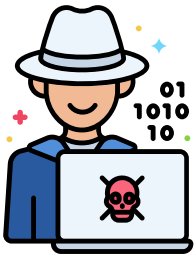
จุดเด่น

1. **ตรวจสอบเว็บเซิร์ฟเวอร์** เพื่อค้นหาช่องโหว่ที่เป็นที่รู้จักและการตั้งค่าที่ไม่ปลอดภัย
2. **ใช้งานฟรีและติดตั้งง่าย**
3. **รองรับการสแกนที่ครอบคลุม** และรายงานผลที่ละเอียด

Kali Linux

ที่มา: The New Stack, Hhjow Kali Linux Can Help Security Test Your Network

Kali Linux เป็นระบบปฏิบัติการที่ออกแบบมาเพื่อการทดสอบการเจาะระบบ (Penetration Testing) และการประเมินความปลอดภัย (Security Assessment) โดยเฉพาะ พัฒนาขึ้นโดย Offensive Security มาพร้อมกับเครื่องมือความปลอดภัยมากมายที่ติดตั้งมาแล้วพร้อมใช้งาน



จุดเด่น

1. **มีเครื่องมือทดสอบการเจาะระบบและประเมินความปลอดภัย** กว่า 600 รายการ
2. **อินเทอร์เฟซที่ใช้งานง่าย เหมาะสำหรับมือใหม่** และสามารถปรับแต่งได้ตามความต้องการ
3. **อัปเดตบ่อยครั้ง** เพื่อให้มั่นใจว่าเครื่องมือทั้งหมดอยู่ในเวอร์ชันล่าสุด
4. **รองรับการใช้งานบนหลายแพลตฟอร์ม** รวมถึงการติดตั้งบนเครื่องเสมือน (Virtual Machine) และ USB

Nmap

ที่มา: NMAP.ORG/images/

Nmap (Network Mapper) เป็นเครื่องมือโอเพ่นซอร์สที่ใช้สำหรับการเก็บข้อมูลบนระบบเครือข่ายด้วย การสแกนเครือข่ายและการค้นหาช่องโหว่ เครื่องมือนี้ถูกใช้กันอย่างแพร่หลายโดยผู้เชี่ยวชาญด้านความปลอดภัย ในการระบุอุปกรณ์ในเครือข่ายและบริการที่เปิดอยู่ รวมถึงระบบปฏิบัติการและลักษณะของแพ็กเก็ต

จุดเด่น

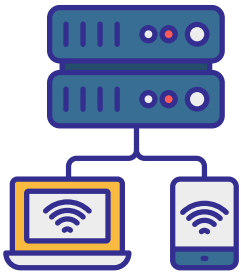
1. **สามารถสแกนพอร์ตเพื่อระบุว่า** พอร์ตใดที่เปิดอยู่และบริการใดที่ทำงานอยู่
2. **ตรวจสอบระบบปฏิบัติการและลักษณะเฉพาะของโฮสต์**
3. **รองรับการสแกนเครือข่ายขนาดใหญ่** และสามารถสร้างแผนที่เครือข่ายได้
4. **อินเทอร์เฟซที่ใช้งานง่าย** และสามารถปรับแต่งสคริปต์เพื่อการสแกนเฉพาะเจาะจงได้

Metasploit

Metasploit

ที่มา: Linkedin, Metasploit Framework Explained

Metasploit เป็นแพลตฟอร์มโอเพ่นซอร์สที่ใช้สำหรับการทดสอบการเจาะระบบ (Penetration Testing) และการวิจัยด้านความปลอดภัยทางไซเบอร์ พัฒนาโดย H.D. Moore ในปี 2003 และปัจจุบันถูกซื้อโดย Rapid7 มีทั้งเวอร์ชันโอเพ่นซอร์สและเชิงพาณิชย์ Metasploit ได้รับการยอมรับอย่างกว้างขวางในชุมชนความปลอดภัยและถูกใช้โดยผู้เชี่ยวชาญด้านความปลอดภัยทางไซเบอร์ทั่วโลก เพื่อทดสอบและประเมินช่องโหว่ของระบบเครือข่ายและซอฟต์แวร์



จุดเด่น

1. **มีฐานข้อมูลเอ็กซ์พลอยต์ (exploits)** ที่ครอบคลุมและอัปเดตอย่างต่อเนื่อง
2. **อินเทอร์เฟซที่ใช้งานง่าย** และรองรับการใช้งานผ่าน CLI และ GUI
3. **สามารถรวมกับเครื่องมืออื่น ๆ** เช่น Nmap เพื่อเพิ่มประสิทธิภาพในการทดสอบการเจาะระบบ
4. **มีฟังก์ชันการสร้างและปรับแต่งเอ็กซ์พลอยต์** เพื่อการทดสอบเฉพาะเจาะจง

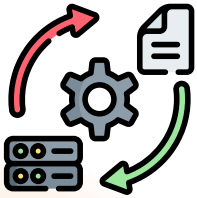
Commercial

Nessus

Nessus
vulnerability scanner

ที่มา: SinFON, Nessus

Nessus เป็นเครื่องมือประเมินช่องโหว่เครือข่ายที่ได้รับความนิยมอย่างสูง มีคุณลักษณะที่ออกแบบมาเพื่อช่วยในการระบุ ประเมิน และแก้ไขจุดอ่อนด้านความปลอดภัย คุณสมบัติของ Nessus ครอบคลุมการสแกนช่องโหว่ การตรวจสอบการกำหนดค่า และการทำโปรไฟล์สินทรัพย์ นอกจากนี้ Nessus ยังมีชื่อเสียงด้านความเร็ว ความแม่นยำ และความครอบคลุมในการสแกนเครือข่ายอีกด้วย



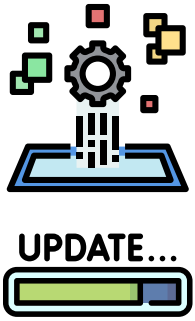
จุดเด่น

1. **ฐานข้อมูลช่องโหว่ที่ครอบคลุมและอัปเดตบ่อยครั้ง**
2. **อินเทอร์เฟซที่ใช้งานง่าย**
3. **สามารถสแกนอุปกรณ์ที่หลากหลาย** รวมถึงอุปกรณ์เครือข่าย ฐานข้อมูล และเว็บเซิร์ฟเวอร์
4. **ความสามารถในการรายงานที่ครอบคลุม** ช่วยให้ผู้ใช้เข้าใจช่องโหว่ในเชิงลึก และวางแผนกลยุทธ์การบรรเทาผลกระทบได้อย่างเหมาะสม

QualysGuard

ที่มา: Wokomedia Commons, Logo-Qualys

QualysGuard เป็นเครื่องมือประเมินช่องโหว่เครือข่ายบนคลาวด์ ที่พัฒนา โดย Qualys มุ่งเน้นการระบุช่องโหว่ในเครือข่าย และให้คำแนะนำสำหรับการแก้ไข



จุดเด่น

1. **ความเร็วในการสแกน** และความสามารถในการปรับขนาด
2. **ความแม่นยำในการสแกนช่องโหว่**
3. **ไม่จำเป็นต้องติดตั้งฮาร์ดแวร์หรือซอฟต์แวร์** เนื่องจากเป็นบริการบนคลาวด์
4. **เหมาะสำหรับธุรกิจทุกขนาด** ตั้งแต่ธุรกิจขนาดเล็กจนถึงองค์กรขนาดใหญ่
5. **การอัปเดตภัยคุกคามแบบเรียลไทม์** ช่วยให้มั่นใจว่าผู้ใช้จะได้รับข้อมูลเกี่ยวกับช่องโหว่ล่าสุดอยู่เสมอ

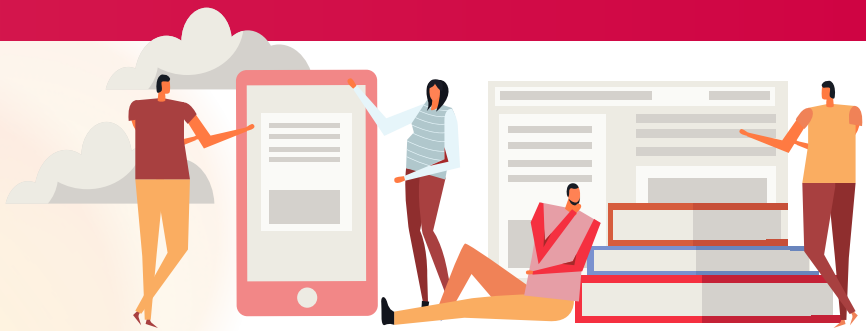
ค่า CVE และ CVSS คืออะไร เกี่ยวข้องกับความปลอดภัยและช่องโหว่อย่างไร

รายงานที่เกี่ยวข้องกับการโจมตีทางไซเบอร์ เมื่อมีการกล่าวถึงช่องโหว่ด้านความปลอดภัย มักจะมีการระบุช่องโหว่เอาไว้เป็นรหัส เช่น CVE-2020-28188, CVE-2019-12725 โดยค่าเหล่านี้ เป็นมาตรฐานที่ใช้ในการระบุและประเมินช่องโหว่และความเสี่ยงในระบบคอมพิวเตอร์และเครือข่าย

CVE (Common Vulnerabilities and Exposures)

CVE (Common Vulnerabilities and Exposures) เป็นโครงการรักษาความปลอดภัย ที่มีเป้าหมายสำคัญในการดูแลซอฟต์แวร์ที่เผยแพร่แบบสาธารณะถูกกำกับดูแลโดยองค์กรไม่แสวงหาผลกำไร MITRE Corporation ซึ่งจะมีการรวบรวมข้อมูลช่องโหว่ความปลอดภัย แล้วจัดตั้งชื่อ ID เฉพาะตัว ให้ช่องโหว่แต่ละรายการที่ถูกค้นพบเพื่อเปิดเผยสู่สาธารณะต่อไป

CVE นั้นมีความสำคัญอย่างยิ่งในหลายด้าน ซึ่งการระบุและจัดหมวดหมู่ช่องโหว่เป็นหนึ่งในหน้าที่สำคัญของ CVE โดยการกำหนดหมายเลข CVE ที่เป็นเอกลักษณ์สำหรับช่องโหว่แต่ละรายการ ช่วยให้การอ้างอิงและสื่อสารข้อมูลเกี่ยวกับช่องโหว่เป็นไปอย่างแม่นยำและชัดเจน ซึ่งมีความสำคัญอย่างยิ่งในการทำให้ผู้ดูแลระบบและนักพัฒนาสามารถรับทราบและแก้ไขปัญหาได้อย่างรวดเร็ว ทำให้ระบบมีความปลอดภัยมากยิ่งขึ้น



การระบุค่า Common Vulnerabilities and Exposures (CVE) ในการตั้งชื่อไอดีของรายการบนฐานข้อมูล Common Vulnerabilities and Exposures (CVE) ทุกรายการจะได้ชื่อที่ไม่ซ้ำกัน โดยมีสูตรในการตั้งชื่อไอดีดังนี้

CVE + ปี + หมายเลขลำดับ
ตัวอย่างเช่น CVE-2021-34527

นอกจากชื่อไอดีเฉพาะตัวแล้ว ทาง MITRE Corporation ยังมีการระบุวันที่ของช่องโหว่ที่ถูกเพิ่มเข้าไปในฐานข้อมูล และคำอธิบายเกี่ยวกับช่องโหว่ ว่ามีลักษณะเป็นอย่างไร และหากช่องโหว่ดังกล่าวได้รับรายงานมาจากแหล่งข้อมูลอื่น ก็จะมีการระบุลิงก์ที่มากลับไปยังผู้ที่รายงานช่องโหว่

นอกจากนี้ หมายเลข CVE สามารถมาจากบริษัทพาณิชย์ที่ได้รับการรับรองอนุญาตให้แต่งตั้งหมายเลข CVE ได้ ซึ่งเรียกว่า CVE Numbering Authorities (CNA) รายชื่อบริษัทเหล่านี้มีมากกว่า 300 รายการ ตัวอย่างเช่น Adobe, Apple, Cisco, Linux, Google, HP, IBM, Microsoft, Mozilla, และ Red Hat เป็นต้น ซึ่งการที่บริษัทเหล่านี้สามารถตั้งหมายเลข CVE ได้ ช่วยให้กระบวนการระบุและจัดการกับช่องโหว่เป็นไปได้อย่างรวดเร็วและมีประสิทธิภาพมากยิ่งขึ้น

การรายงานช่องโหว่เพื่อรับ CVE IDs หากคุณค้นพบช่องโหว่ด้านความปลอดภัยและต้องการรายงานเพื่อให้ข้อมูลนั้นเข้าสู่ฐานข้อมูลของ Common Vulnerabilities and Exposures (CVE) คุณสามารถติดต่อบริษัทที่ได้รับอนุญาตให้กำหนดหมายเลข CVE หรือ CVE Numbering Authorities (CNA) และ MITRE Corporation ซึ่งเป็นองค์กรที่รับผิดชอบหลักสามารถศึกษารายละเอียดเพิ่มเติมได้ที่: CVE Identifiers (https://cve.mitre.org/cve/identifiers/index.html)

อีกหนึ่งช่องทางที่นักพัฒนาหลายคนแนะนำคือ การแจ้งข้อมูลผ่านระบบ Mailing List ที่นิยมใช้ในการแจ้งเตือนเรื่องความปลอดภัย เช่น Bugtraq จากนั้น MITRE Corporation จะตอบรับและเผยแพร่หมายเลข CVE เมื่อผ่านการตรวจสอบแล้ว

อย่างไรก็ตาม ควรทราบว่า แม้ว่าการรายงานช่องโหว่จะมีความสำคัญต่อชุมชนซอฟต์แวร์ และความเร่งด่วนในการเผยแพร่ช่องโหว่ เพื่อให้สาธารณชนเตรียมการป้องกันตนเอง แต่ในความเป็นจริง กระบวนการนี้ไม่ง่าย และอาจใช้เวลาหลายวันหรือหลายเดือน การเผยแพร่รายงาน CVE ในฐานข้อมูลของ MITRE Corporation ต้องผ่านกระบวนการอนุมัติและเซ็นเซอร์ทางการค้า นอกจากนี้ MITRE Corporation เองก็มีทรัพยากรจำกัดในการตอบสนองต่อรายงานช่องโหว่ที่มีเข้ามาเป็นจำนวนมาก

หลังจากที่ข้อมูลช่องโหว่ได้รับการจัดสร้างไอดีเสร็จแล้ว ข้อมูลจะปรากฏอยู่บนฐานข้อมูลของ MITRE ทางเว็บไซต์ หลังจากนั้นทาง National Vulnerability Database (NVD) ซึ่งเป็นฐานข้อมูลช่องโหว่แห่งชาติของรัฐบาลกลางแห่งประเทศสหรัฐอเมริกาก็จะเผยแพร่ข้อมูลช่องโหว่ดังกล่าว พร้อมกับวิเคราะห์ความปลอดภัยที่เกี่ยวข้องเพิ่มเติมเข้าไปด้วย โดยมีฐานข้อมูลจาก Common Vulnerabilities and Exposures (CVE) เป็นองค์ประกอบหลัก


NIST

NVD MENU

Information Technology Laboratory

NATIONAL VULNERABILITY DATABASE

NIST NATIONAL VULNERABILITY DATABASE

CVE-2021-34527 Detail

Description

QUICK INFO

CVE Dictionary Entry:

NVD Published Date:

07/07/2021

NVD Last Modified:

02/02/2024

Source:

Microsoft Corporation

การใช้หมายเลข CVE ในการรายงานและแก้ไขช่องโหว่ยังช่วยสร้างความเชื่อมั่นให้กับผู้ใช้ว่าผลิตภัณฑ์ที่ใช้นั้น ได้รับการตรวจสอบและปรับปรุงความปลอดภัยอย่างต่อเนื่อง นอกจากนี้ หมายเลข CVE ยังมีบทบาทสำคัญในการสนับสนุนกระบวนการวิเคราะห์ความเสี่ยง ทำให้องค์กรสามารถประเมินความเสี่ยงที่อาจเกิดจากช่องโหว่และวางแผนเพื่อลดความเสี่ยงได้อย่างมีประสิทธิภาพ ยิ่งไปกว่านั้น CVE ยังส่งเสริมการแลกเปลี่ยนข้อมูลและความร่วมมือระหว่างองค์กร หน่วยงานรัฐบาล และชุมชนนักพัฒนา ทำให้สามารถรับมือกับภัยคุกคามทางไซเบอร์ได้อย่างรวดเร็วและมีประสิทธิภาพ การมีฐานข้อมูล CVE ช่วยเพิ่มความโปร่งใสและการเข้าถึงข้อมูลเกี่ยวกับช่องโหว่ ซึ่งเป็นปัจจัยสำคัญในการเสริมสร้างความปลอดภัยทางไซเบอร์ให้กับทั้งองค์กรและผู้ใช้ทั่วไป

CVSS คะแนนบอกระดับความอันตรายของช่องโหว่

CVSS (Common Vulnerability Scoring System) คือระบบมาตรฐานในการประเมินและให้คะแนนความรุนแรงของช่องโหว่ในระบบคอมพิวเตอร์ CVSS ถูกออกแบบมาเพื่อให้ผู้ดูแลระบบ ผู้พัฒนา และผู้เชี่ยวชาญด้านความปลอดภัยสามารถเข้าใจและเปรียบเทียบความรุนแรงของช่องโหว่ต่าง ๆ ได้อย่างมีประสิทธิภาพ

องค์ประกอบหลักของ CVSS ในการคิดคะแนน

ที่มา : https://www.ksc.net/th/km.aspx?id=10

1. **Base Score:** คะแนนพื้นฐานที่ประเมินจากคุณสมบัติทั่วไปของช่องโหว่ เช่น ความง่ายในการโจมตี ความสามารถในการเข้าถึง และผลกระทบที่เกิดขึ้นกับระบบ คะแนน Base Score ประกอบด้วย Exploitability Metrics หรือ ความยากง่ายในการเจาะช่องโหว่ และ Impact Metrics หรือ ผลกระทบจากช่องโหว่
2. **Temporal Score:** คะแนนที่ปรับเปลี่ยนตามปัจจัยที่เปลี่ยนแปลงได้ในช่วงเวลา เช่น การมีหรือไม่มีการแก้ไขปัญหา (patch) การมีเครื่องมือโจมตี และความเชื่อถือของข้อมูลเกี่ยวกับช่องโหว่
3. **Environmental Score:** คะแนนที่ปรับเปลี่ยนตามสภาพแวดล้อมเฉพาะขององค์กรหรือระบบ เช่น การกำหนดค่าความสำคัญของสินทรัพย์ที่ได้รับผลกระทบ และการตั้งค่าความปลอดภัยของระบบที่แตกต่างกัน

เกณฑ์คะแนนของ CVSS

Temporal Metric Group

- Maturity
- Remeditation
- Report Confidence

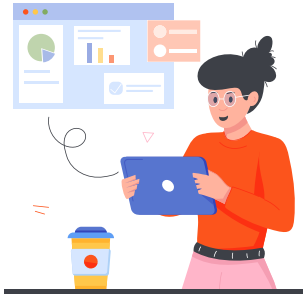
ที่มา : https://cyberint.com/blog/thought-leadership/cvss-4-0-what-you-need-to-know/

คะแนนของ CVSS จะอยู่ในช่วง ตั้งแต่ 0 – 10 คะแนน โดยคะแนนที่มากขึ้นก็จะบ่งบอกถึงความรุนแรงที่มากขึ้น โดยระบบการให้คะแนนของ CVSS จะมีการอัปเดตอยู่เรื่อย ๆ เพื่อให้ครอบคลุมและเท่าทันเทคโนโลยีใหม่ ๆ ที่อาจจะเป็นช่องโหว่ของระบบได้ โดยระบบล่าสุดที่มีการประกาศอัปเดตในเดือนพฤศจิกายน 2023 คือ CVSS 4.0 ที่เพิ่มในส่วนความเรียบง่ายและความชัดเจนเพิ่มขึ้น โดยจะพิจารณาปัจจัยเพิ่มเติม เช่น ความน่าจะเป็นของการโจมตี และผลที่ตามมา ที่อาจเกิดขึ้นจากการโจมตีที่ประสบความสำเร็จ เวอร์ชันนี้เน้นการรวมข้อมูลภัยคุกคามและตัวชี้วัดด้านสิ่งแวดล้อมในการให้คะแนน ส่งผลให้การประเมินความเสี่ยงสมจริงยิ่งขึ้น

กรณีศึกษาเกี่ยวกับ CVE และ CVSS

ที่มา : https://www.netsecurity.com/wannacry-ransomware-explained/

เหตุการณ์ WannaCry ที่เกิดขึ้นในปี 2017 ซึ่งเป็นการโจมตีแบบ Ransomware ที่ใช้ช่องโหว่ EternalBlue (CVE-2017-0143) ในระบบปฏิบัติการ Microsoft Windows ซึ่งมี CVSS score ที่สูงมากถึง 8.1 ด้วยความสามารถในการกระจายตัวผ่านเครือข่ายโดยอัตโนมัติ โดยมีผลกระทบที่รุนแรงต่อระบบที่ไม่ได้อัปเดตแพทช์ความปลอดภัยอย่างทันที มัลแวร์นี้สามารถเข้ารหัสไฟล์บนเครื่องคอมพิวเตอร์ และเรียกเงินจากผู้ใช้ ซึ่งเป็นตัวอย่างที่ชัดเจนเกี่ยวกับผลกระทบที่ร้ายแรงของการไม่รักษาความปลอดภัยอย่างเพียงพอในองค์กร



สรุปท้ายบท Chapter 6

การระบุภัยคุกคามและการประเมินช่องโหว่

ประเภทของภัยคุกคามทางไซเบอร์ต่าง ๆ เช่น มัลแวร์ ฟิชชิง แรนซัมแวร์ และวิศวกรรมสังคม รวมถึงภัยคุกคามจากภายในองค์กรและความเสี่ยงด้านความปลอดภัยบนคลาวด์ นอกจากนี้ ยังมีการอธิบายถึงเทคโนโลยีใหม่ ๆ เช่น IoT และ AI ที่อาจเป็นช่องโหว่ของระบบสารสนเทศ

ในการระบุภัยคุกคาม ให้ใช้ระบบการสแกนช่องโหว่ ที่สามารถแบ่งออกเป็นระบบ Open Source และ Commercial โดยเครื่องมือเหล่านี้ ช่วยในการตรวจสอบและระบุช่องโหว่ที่อาจเป็นเป้าหมายของการโจมตี นอกจากนี้ ยังมีการกล่าวถึงวิธีการประเมินช่องโหว่ต่าง ๆ เช่น การสแกนช่องโหว่ การทดสอบการเจาะระบบ การตรวจสอบช่องโหว่ด้วยตนเอง และการตรวจสอบโค้ด เพื่อประเมินความสามารถของระบบในการต้านการโจมตี

การใช้เครื่องมือและวิธีการที่เหมาะสมในการระบุและประเมินภัยคุกคามและช่องโหว่ โดยการตรวจสอบและประเมินอย่างต่อเนื่อง จะช่วยให้องค์กรสามารถป้องกันและรับมือกับภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ การประเมินเหล่านี้ยังช่วยให้องค์กรสามารถรักษาความปลอดภัยของข้อมูลและระบบได้อย่างยั่งยืน และเตรียมความพร้อมรับมือกับภัยคุกคามที่เปลี่ยนแปลงอยู่ตลอดเวลา รวมถึงการพัฒนาและปรับปรุงกระบวนการรักษาความปลอดภัยอย่างต่อเนื่อง เพื่อให้ทันกับเทคโนโลยีและภัยคุกคาม

CHAPTER
7

การตรวจสอบทรัพย์สินสารสนเทศ

ที่มา: IndiaMART, IS International Audit Services

การตรวจสอบทรัพย์สินสารสนเทศ คืออะไร

การตรวจสอบทรัพย์สินสารสนเทศ คือ กระบวนการที่ใช้ในการระบุ ประเมิน และจัดการทรัพย์สินสารสนเทศ (Information Assets) ขององค์กร ซึ่งรวมถึงฮาร์ดแวร์ ซอฟต์แวร์ ข้อมูล และองค์ประกอบอื่น ๆ ที่มีความสำคัญต่อการดำเนินธุรกิจ การตรวจสอบทรัพย์สินสารสนเทศช่วยให้องค์กรสามารถรับรู้ถึงสถานะของทรัพย์สิน และจัดการความเสี่ยงที่อาจเกิดขึ้นได้อย่างมีประสิทธิภาพ

ความสำคัญของการตรวจสอบทรัพย์สินสารสนเทศ

การบริหารจัดการความเสี่ยงและปกป้องข้อมูลสำคัญ: การตรวจสอบทรัพย์สินสารสนเทศ ช่วยให้องค์กรสามารถระบุจุดอ่อนและความเสี่ยงที่อาจเกิดขึ้นจากการโจมตีทางไซเบอร์ ซึ่งอาจนำไปสู่การรั่วไหลหรือการสูญหายของข้อมูลสำคัญ การประเมินและจัดการความเสี่ยงเหล่านี้ได้อย่างมีประสิทธิภาพ ทำให้องค์กรสามารถดำเนินการป้องกันหรือแก้ไขปัญหาได้ก่อนที่ผู้ไม่ประสงค์ดีจะสามารถโจมตีได้สำเร็จ

การตรวจสอบและปรับปรุงมาตรการป้องกัน: การตรวจสอบทรัพย์สินสารสนเทศอย่างต่อเนื่อง ช่วยให้องค์กรสามารถปรับปรุงมาตรการป้องกันได้อย่างต่อเนื่อง การตรวจสอบช่องโหว่และผลกระทบที่เกิดขึ้น ช่วยให้สามารถวางแผนและดำเนินการแก้ไขปัญหาได้อย่างทันเวลา รวมถึงช่วยในการทดสอบและปรับปรุงมาตรการรักษาความปลอดภัยที่มีอยู่ให้ทันสมัยและเหมาะสมกับภัยคุกคามที่เปลี่ยนแปลงไป

การปฏิบัติตามกฎหมายและข้อบังคับ: การตรวจสอบทรัพย์สินสารสนเทศเป็นส่วนหนึ่งของการปฏิบัติตามกฎหมายและข้อบังคับที่เกี่ยวข้องกับความปลอดภัยของข้อมูล เช่น GDPR หรือ ISO 27001 การมีข้อมูลที่ครบถ้วนและถูกต้อง ช่วยให้องค์กรสามารถปฏิบัติตามข้อกำหนดและกฎหมายได้อย่างมีประสิทธิภาพ

การวางแผนและการจัดการทรัพยากร: การมีข้อมูลที่ถูกต้องและเป็นปัจจุบันเกี่ยวกับทรัพย์สินสารสนเทศ ช่วยให้องค์กรสามารถตัดสินใจเชิงกลยุทธ์ได้อย่างแม่นยำและสามารถใช้ทรัพยากรได้อย่างคุ้มค่าและมีประสิทธิภาพ

วิธีการตรวจสอบทรัพย์สินสารสนเทศอย่างต่อเนื่อง

การตรวจสอบระบบ การตรวจสอบระบบหมายถึง การติดตามและประเมินประสิทธิภาพของระบบสารสนเทศในองค์กร รวมถึงการตรวจสอบสถานะการทำงานของเซิร์ฟเวอร์ อุปกรณ์เครือข่าย แอปพลิเคชัน และบริการต่าง ๆ ที่ใช้งานอยู่ เพื่อให้มั่นใจว่าทำงานได้อย่างถูกต้องและมีความปลอดภัย การตรวจสอบนี้จะช่วยระบุปัญหาที่อาจเกิดขึ้นและช่วยให้ทำการแก้ไขได้ทันท่วงที

เครื่องมือที่ใช้ในการตรวจสอบระบบ

Nagios: เป็นโปรแกรม IT Monitoring ชั้นนำ จากสหรัฐอเมริกา มีจุดเด่นคือ ความเร็วสูง เชื่อถือได้ และปรับแต่งตามความต้องการได้อย่างหลากหลาย มีฟีเจอร์การตรวจสอบแบบเรียลไทม์ การแจ้งเตือน และการรายงาน ที่ช่วยให้ผู้ดูแลระบบสามารถระบุและแก้ไขปัญหาได้ก่อนที่จะส่งผลกระทบต่อธุรกิจ

Nagios

ที่มา: IndiaMART, IS International Audit Services

Zabbix: เป็นเครื่องมือการตรวจสอบที่เป็น Open source และเป็นที่นิยมสำหรับผู้ใช้ เนื่องจากมี Web GUI ที่ใช้งานง่าย และสามารถปรับแต่งค่าการใช้งานได้ทั้งหมด โดยมักนำมาใช้ในการตรวจสอบเซิร์ฟเวอร์และฮาร์ดแวร์เครือข่าย จุดเด่นอย่างหนึ่งของ Zabbix คือ ความสามารถในการคาดการณ์แนวโน้มของทราฟฟิกและพฤติกรรมในอนาคต โดยการวิเคราะห์จากข้อมูลที่ผ่านมา

ZABBIX

ที่มา: Wikimedia Commons, Zabbix logo

การตรวจสอบแอปพลิเคชัน

การตรวจสอบแอปพลิเคชันเป็นกระบวนการสำคัญที่ ช่วยประเมินความปลอดภัยและประสิทธิภาพของซอฟต์แวร์ที่องค์กรใช้งาน การตรวจสอบนี้ ครอบคลุมทั้งการทำงานและความปลอดภัยของแอปพลิเคชัน เพื่อให้มั่นใจว่าแอปพลิเคชันสามารถทำงานได้ตามที่คาดหวัง และไม่มีช่องโหว่ที่อาจเป็นอันตรายต่อระบบ

เครื่องมือที่ใช้ในการตรวจสอบแอปพลิเคชัน

AppDynamics: เป็นเครื่องมือตรวจสอบประสิทธิภาพแอปพลิเคชันขั้นสูง ที่ออกแบบมาเพื่อให้ข้อมูลเชิงลึกแบบเรียลไทม์ เกี่ยวกับประสิทธิภาพของแอปพลิเคชันในสภาพแวดล้อมต่าง ๆ

ที่มา: Icon-Icons, Appdynamics logo

New Relic: ช่วยในการตรวจสอบประสิทธิภาพและความพร้อมใช้งานของแอปพลิเคชัน สามารถวิเคราะห์ข้อมูลเชิงลึก และนำเสนอข้อมูลที่จำเป็นสำหรับการปรับปรุงประสิทธิภาพของแอปพลิเคชัน

ที่มา: Icon-Icons, Appdynamics logo

การตรวจสอบเครือข่าย

การตรวจสอบเครือข่ายเป็นกระบวนการตรวจสอบความพร้อมใช้งาน การทำงาน และความปลอดภัยของเครือข่ายองค์กร ซึ่งครอบคลุมการตรวจสอบการเข้าถึง การใช้ทรัพยากรเครือข่าย และการตรวจจับการบุกรุก การตรวจสอบนี้เกี่ยวข้องกับการติดตามและวิเคราะห์ส่วนประกอบเครือข่ายต่าง ๆ เช่น เราเตอร์ สวิตช์ และไฟร์วอลล์ รวมถึงการเชื่อมต่อระหว่างกัน นอกจากนี้ ยังครอบคลุมการสำรวจชั้นข้อมูล จุดสิ้นสุดของเครือข่าย และลิงก์ต่าง ๆ ด้วย

เครื่องมือที่ใช้ในการตรวจสอบเครือข่าย

SolarWinds Network Performance Monitor: เครื่องมือที่ช่วยในการตรวจสอบประสิทธิภาพของเครือข่าย เฝ้าระวัง และวิเคราะห์ปัญหาที่เกิดขึ้น รวมถึงมีฟีเจอร์สแกนค้นหาอุปกรณ์โดยอัตโนมัติ

ที่มา: FirstLight, SolarWinds

PRTG Network Monitor: ใช้ในการตรวจสอบเครือข่ายแบบเรียลไทม์ รวมถึงการวิเคราะห์ปริมาณการใช้เครือข่ายและการแจ้งเตือนเมื่อเกิดปัญหา เป็นที่รู้จักกันดีในเรื่องความสามารถในการบริหารจัดการ IT infrastructure ขั้นสูง

ที่มา: Wikimedia Commons,
PRTG Network Monitor logo

การตรวจสอบล็อก

ล็อก (Log) คือ ข้อมูลจราจรทางคอมพิวเตอร์ หรือทางเทคนิคเรียกว่า Log File หมายถึงข้อมูลที่เกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งข้อมูลนี้สามารถแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการ หรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น การตรวจสอบล็อกเป็นกระบวนการสำคัญในการติดตามและวิเคราะห์ล็อกไฟล์ที่เกิดจากระบบและแอปพลิเคชันต่าง ๆ เพื่อค้นหาความผิดปกติหรือกิจกรรมที่น่าสงสัย ทำให้สามารถระบุปัญหาและแก้ไขได้ทันท่วงที

เครื่องมือที่ใช้ในการตรวจสอบล็อก

Splunk: เป็นระบบรักษาความปลอดภัยที่หลายองค์กรนำมาใช้ในการเก็บรวบรวม วิเคราะห์ และตรวจสอบข้อมูล มีจุดเด่น คือ การตรวจสอบข้อมูลบนอุปกรณ์ไอทีต่าง ๆ ขององค์กร การ monitor ระบบความปลอดภัย และระบบการแจ้งเตือนที่สามารถแจ้งเตือนทันทีเมื่อพบความผิดปกติเกิดขึ้นกับระบบหรือข้อมูลขององค์กร นอกจากนี้ยังสามารถแสดงผลการ monitor จัดทำรายงานและแดชบอร์ดเพื่อให้ง่ายต่อการวิเคราะห์และการตัดสินใจอีกด้วย

ที่มา: Wikimedia Commons, PRTG Network Monitor logo

Graylog: เป็นเครื่องมือโอเพ่นซอร์สสำหรับการเก็บรวบรวมและวิเคราะห์ล็อกไฟล์ที่มีความสามารถในการค้นหาและวิเคราะห์ข้อมูลแบบเรียลไทม์ รวมถึงการแจ้งเตือนเมื่อพบความผิดปกติหรือกิจกรรมที่น่าสงสัย พร้อมทั้งดีบักแอปพลิเคชันโดยใช้ Elasticsearch สำหรับการจัดเก็บและค้นหาข้อมูล MongoDB สำหรับการจัดการเมตาดาต้า และ Scala สำหรับการพัฒนาซอฟต์แวร์

ที่มา: Icon-Icons, Graylog logo

สรุปท้ายบท Chapter 7

ความรู้พื้นฐานและกฎหมายที่เกี่ยวข้อง กับการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

การตรวจสอบทรัพย์สินทางสารสนเทศ คือกระบวนการสำคัญที่ช่วยให้องค์กรสามารถระบุ ประเมิน และจัดการทรัพย์สินสารสนเทศได้อย่างมีประสิทธิภาพ รวมถึงการใช้เครื่องมือและวิธีการที่เหมาะสมในการตรวจสอบระบบ แอปพลิเคชัน เครือข่าย ล็อก นอกจากนี้ยังเน้นถึงความสำคัญของการตรวจสอบและประเมินอย่างต่อเนื่อง เพื่อให้มั่นใจว่าองค์กรสามารถป้องกันและรับมือกับภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ

การประเมินเหล่านี้ไม่เพียงช่วยรักษาความปลอดภัยของข้อมูลและระบบอย่างยั่งยืน แต่ยังช่วยเตรียมความพร้อมรับมือกับภัยคุกคามที่เปลี่ยนแปลงอยู่ตลอดเวลา รวมถึงการพัฒนาและปรับปรุงกระบวนการรักษาความปลอดภัยอย่างต่อเนื่อง เพื่อตอบสนองต่อเทคโนโลยีและภัยคุกคามใหม่ ๆ ที่เกิดขึ้น

MODULE 04

การตอบสนองต่อเหตุการณ์ภัยคุกคามทางสารสนเทศ

(Information Security Incident Response) #Response

วัตถุประสงค์

เพื่อให้ผู้เข้ารับการฝึกอบรมมีความรู้ความเข้าใจเกี่ยวกับการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ สามารถระบุและประเมินความเสี่ยง วิเคราะห์และเลือกใช้กลยุทธ์การจัดการความเสี่ยงที่เหมาะสม รวมถึงสามารถนำมาตรการควบคุมต่าง ๆ ไปใช้ในการป้องกันและลดความเสี่ยงได้อย่างมีประสิทธิภาพ

CHAPTER 8

การตอบสนองต่อเหตุการณ์

กระบวนการและขั้นตอนการตอบสนองต่อเหตุการณ์ (Incident Response)

ความสำคัญของการมีแผน Incident Response

บริหารจัดการความเสี่ยง: การมีแผนที่ชัดเจนและปฏิบัติต่อเหตุการณ์ที่เกิดขึ้นได้อย่างมีระเบียบ ช่วยในการจัดการความเสี่ยงที่เกี่ยวข้องกับการละเมิดข้อมูลและการโจมตีทางไซเบอร์

ตอบสนองอย่างมีประสิทธิภาพ: การตอบสนองต่อเหตุการณ์ที่เกิดขึ้นอย่างรวดเร็วและมีประสิทธิภาพ ช่วยให้องค์กรกลับสู่สภาวะปกติได้เร็วขึ้น และลดความเสียหายที่อาจเกิดขึ้น

รักษาความต่อเนื่องของการดำเนินงาน: ทำให้ธุรกิจสามารถดำเนินงานต่อไปได้โดยไม่มีการหยุดชะงักในการให้บริการหรือการผลิต แม้จะเผชิญกับเหตุการณ์ที่ไม่คาดคิด

ที่มา: NIST Incident Response Life

ลดผลกระทบต่อข้อมูลและเครือข่าย: การมีแผนรับมือช่วยลดความเสียหายต่อข้อมูลสำคัญและโครงสร้างพื้นฐานทางเทคโนโลยีขององค์กร

สร้างความเชื่อมั่นให้กับลูกค้าและสังคม: การปฏิบัติตามแผน Incident Response อย่างเหมาะสม ช่วยเสริมภาพลักษณ์ขององค์กร และสร้างความเชื่อมั่นให้กับลูกค้าและผู้มีส่วนได้เสีย

ป้องกันการละเมิดกฎหมาย: การที่องค์กรมีการตอบสนองต่อเหตุการณ์ที่เกิดขึ้นได้อย่างมีประสิทธิภาพช่วยลดความเสี่ยงในการละเมิดกฎหมายที่อาจเกิดขึ้นจากผลกระทบของเหตุการณ์ทางไซเบอร์

ขั้นตอน Incident Response: การเตรียมการ การระบุ การกักกัน การตรวจสอบ การกำจัด การกู้คืน บทเรียนที่ได้เรียนรู้

การเตรียมความพร้อม (Preparation)

จัดเตรียมทรัพยากรและเครื่องมือที่จำเป็น เพื่อการรับมือและตอบสนองต่อภัยคุกคาม ซึ่งครอบคลุมดังนี้

1. การสื่อสารและรายงานเหตุการณ์:

- รายชื่อและช่องทางการติดต่อสำหรับผู้รับมือและผู้ตอบสนองต่อเหตุการณ์
- ระบบการรายงานและติดตามสถานะของเหตุการณ์ที่แจ้งเข้ามา

2. โปรแกรมเข้ารหัส (Encryption Software):

- เครื่องมือสำหรับเข้ารหัสข้อมูลเพื่อความปลอดภัยในการสื่อสาร

3. ห้องประชุม (War Room):

- พื้นที่ที่จัดสรรเป็นห้องประชุมสำหรับการประสานงานและตัดสินใจในขณะเกิเหตุการณ์

4. อุปกรณ์และซอฟต์แวร์สำหรับวิเคราะห์เหตุการณ์:

- เครื่องคอมพิวเตอร์หรืออุปกรณ์สำรองข้อมูล (Backup Device)
- เครื่องมือสำหรับตรวจจับและวิเคราะห์ข้อมูลในเครือข่ายคอมพิวเตอร์ เช่น Packet Sniffers และ Protocol Analyzers เพื่อศึกษาพฤติกรรมของ Malware หรือความผิดปกติของเครือข่าย

5. แหล่งข้อมูลเพื่อวิเคราะห์เหตุการณ์ไซเบอร์:

- รายการพอร์ตช่องทางการแลกเปลี่ยนข้อมูลผ่านอินเทอร์เน็ตหรือระบบเครือข่ายคอมพิวเตอร์
- ซอฟต์แวร์สำหรับตรวจจับการบุกรุกและป้องกันไวรัส
- แผนผังเครือข่ายและรายการทรัพย์สินทางสารสนเทศที่มีค่าปกติ (Current Baseline) ของระบบเครือข่ายและแอปพลิเคชัน
- ค่า Hash ของไฟล์ที่สำคัญ เพื่อการตรวจสอบความคงเส้นคงวาของข้อมูล

6. ซอฟต์แวร์สำหรับการบรรเทาเหตุการณ์:

- ไฟล์ Disk Image ของระบบปฏิบัติการ (OS) และแอปพลิเคชัน เพื่อใช้ในการกู้คืนและฟื้นฟูระบบหลังจากเกิดเหตุการณ์

การดำเนินการป้องกันก่อนเกิดเหตุ (Preventing Incidents) ดังต่อไปนี้

1. การประเมินความเสี่ยง (Risk Assessment): องค์กรควรทำการประเมินความเสี่ยง เพื่อพิจารณาว่ามีความเสี่ยงใดบ้างที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์หรือช่องโหว่ด้านความมั่นคงปลอดภัย เพื่อประเมินผลกระทบ และมูลค่าความเสียหายที่แท้จริง และเป็นข้อมูลประกอบการพิจารณาทบทวนหรือปรับปรุงแนวทางในการรับมือและการตอบสนองต่อภัยคุกคามต่อไป

2. การกำหนดแนวทางรักษาความมั่นคงปลอดภัยของระบบแม่ข่าย (Implement Host Security Control): ควรมีการกำหนดสิทธิ์ของผู้ใช้งาน โดยให้สิทธิ์เท่าที่จำเป็นต่อการปฏิบัติงานที่ได้รับอนุญาตเท่านั้น รวมทั้งระบบแม่ข่ายควรบันทึกเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยที่สำคัญของบริษัท และได้รับการติดตามตรวจสอบอย่างสม่ำเสมอ

3. การรักษาความปลอดภัยของเครือข่าย Implement Network Security Control): เป็นการตั้งค่าอุปกรณ์ทางเครือข่ายที่จำเป็น เช่น Router ACL, Firewall, IPDS เป็นต้น ให้ปฏิเสธการเข้าถึงของกิจกรรมทั้งหมดที่ไม่ได้รับอนุญาต รวมทั้งอุปกรณ์เครือข่ายทั้งหมดของบริษัทที่เชื่อมต่อกับเครือข่ายภายนอกเพื่อป้องกันและแจ้งเตือนการบุกรุก

4. การจัดให้มี User Awareness Training: เพื่อให้ทุกคนในองค์กรมีความรู้ความเข้าใจ มีความระมัดระวัง และเข้าใจถึงความผิดปกติที่เกิดขึ้นจากการโจมตีทางไซเบอร์รวมทั้งเข้าใจวิธีการตอบสนองในเบื้องต้น และดำเนินการแจ้งให้หน่วยงานที่ทำหน้าที่ในการรับมือและตอบสนองรับทราบเมื่อมีเหตุการณ์ผิดปกติเกิดขึ้น

การตรวจจับและวิเคราะห์ (Detection & Analysis)

การกำหนดจุดและวิธีการที่จะใช้ในการตรวจจับ Incident: การตรวจจับ Incident จะขึ้นอยู่กับระบบที่ใช้งานอยู่ และรูปแบบของความพยายามในการโจมตี ประกอบกับกลไกต่าง ๆ ที่ทำการปกป้องระบบอยู่ เพราะโดยทั่วไป ระบบการป้องกันจะทำการแจ้งเตือน (Alert) หรือ เก็บบันทึกข้อมูล (Log) เพื่อใช้ในการวิเคราะห์หาความผิดปกติด้วย

การวิเคราะห์เหตุภัยคุกคามหรือความผิดปกติ: เมื่อได้รับแจ้ง การวิเคราะห์เหตุภัยคุกคามหรือความผิดปกติควรมีความถูกต้อง แม่นยำ และมีประสิทธิภาพ เพื่อให้การดำเนินการในขั้นตอนต่อไปสามารถดำเนินการได้เร็วและถูกต้องมากยิ่งขึ้น

การบันทึกข้อมูลเหตุการณ์ภัยคุกคาม: หน่วยงานควรบันทึกข้อมูลเกี่ยวกับเหตุการณ์ที่เกิดขึ้น ตั้งแต่การตรวจพบจนถึงการสิ้นสุดของเหตุการณ์ภัยคุกคาม เพื่อประโยชน์ในการติดตามเหตุการณ์ ขั้นตอนการจัดการ และแก้ไขเหตุภัยคุกคาม เพื่อให้มั่นใจได้ว่าเหตุการณ์ภัยคุกคามที่เกิดขึ้นได้รับการจัดการแก้ไขภายในระยะเวลาที่เหมาะสม

การวิเคราะห์ผลกระทบและการจัดลำดับความสำคัญของ Incident: ช่วยในการตัดสินใจเชิงกลยุทธ์ เพื่อดำเนินการรับมือ และตอบสนองต่อภัยคุกคามที่เกิดขึ้นได้อย่างเหมาะสม ภายใต้ทรัพยากรที่มีอยู่อย่างจำกัดของบริษัท และลดผลกระทบทางธุรกิจให้น้อยลงที่สุด

การติดต่อประสานงานและแจ้งข้อมูลให้กับบุคลากรด้านอื่น ๆ: ควรดำเนินการแจ้งข้อมูลเกี่ยวกับเหตุภัยคุกคามกับผู้ที่เกี่ยวข้อง เพื่อให้ทุกคนสามารถดำเนินการตามหน้าที่ความรับผิดชอบที่ได้กำหนดไว้ ทั้งนี้ องค์กรควรมีข้อกำหนดเกี่ยวกับการแจ้งข้อมูลเหตุภัยคุกคาม โดยอย่างน้อยควรกำหนดบุคคลผู้รับรายงาน ข้อมูลที่ต้องรายงาน และเวลาที่ต้องรายงาน รวมถึงหน่วยงานต่าง ๆ ทั้งภายในและภายนอกที่ต้องได้รับแจ้ง

การควบคุมความเสียหาย การกำจัดสาเหตุของภัยคุกคาม และการกู้คืน (Containment, Eradication & Recovery)

พิจารณาวิธีการในการควบคุมความเสียหาย

การควบคุมความเสียหายมีความจำเป็นอย่างยิ่งที่จะป้องกันไม่ให้ความเสียหายกระจายออกไปเป็นวงกว้าง สร้างผลกระทบต่อทรัพยากรในการดำเนินธุรกิจอื่น ๆ และยังเป็นการเปิดพื้นที่ เพิ่มระยะเวลาให้ทีมที่รับมือ Incident มีเวลาในการคิดหาสาเหตุ และวิธีการแก้ปัญหาได้ ข้อสำคัญของการควบคุมความเสียหาย คือการตัดสินใจเลือกใช้วิธีการที่เหมาะสม โดยวิธีการทั่วไปมีดังต่อไปนี้

1. **ปิดระบบ (Shut Down)**
2. **ตัดการเชื่อมต่อทางเครือข่ายทั้งหมด (Network Disconnection)** ทั้งนี้ อาจมียกเว้นการเชื่อมต่อสำหรับ Endpoint Detection & Response Agent (กระบวนการตรวจสอบและตรวจจับกิจกรรมหรือเหตุการณ์ที่น่าสงสัยใด ๆ ที่เกิดขึ้นที่ปลายทางแบบเรียลไทม์)
3. **หยุดการทำงานของฟังก์ชันที่เกี่ยวข้อง (Disabling Certain Functions)**
4. **Redirect Network Traffic** หรือเบนความสนใจของผู้บุกรุกไปยัง Blackhole/ Sandbox/ Honeypot

การจัดเก็บและดูแลรักษาหลักฐานทางดิจิทัล

วัตถุประสงค์หลักของการจัดเก็บหลักฐาน คือ เพื่อให้การแก้ไข Incident ส่งผลกระทบต่อธุรกิจให้น้อยที่สุด (Minimizing impact to the business)

การกำจัดสาเหตุและการกู้คืนระบบให้กลับมาทำงานปกติ

หากพิจารณาแผนภาพ Incident Response Life Cycle จะพบว่า เมื่อมีการควบคุมความเสียหาย และมีการเก็บหลักฐานข้อมูลเพิ่มเติมเรียบร้อยแล้ว ข้อมูลทั้งหมดจะต้องนำกลับมาวิเคราะห์ตามหลักการที่ได้กล่าวไว้ใน “ขั้นตอนที่ 2 เรื่องการตรวจจับและวิเคราะห์ (Detection & Analysis)” จนกว่าจะสามารถกำจัดสาเหตุที่ทำให้เกิด Incident และช่องทางที่ผู้บุกรุกได้สร้างไว้เพื่อเข้ามาในระบบทั้งหมดได้เรียบร้อย โดยตัวอย่างการกำจัดสาเหตุได้แก่

1. การปิดช่องโหว่ของระบบ
2. การยกเลิก User Account ที่ผู้บุกรุกใช้เข้าสู่ระบบ
3. การแจ้งให้ผู้ใช้งานเปลี่ยนรหัสผ่าน
4. การลบโปรแกรมประเภท Backdoor ออกจากระบบ

การดำเนินการหลังจากการรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์เสร็จสิ้น (Post Incident Activity)

ทีมรับมือและผู้ที่เกี่ยวข้องทั้งหมดควรมีการประชุมหารือ เพื่อแลกเปลี่ยนข้อมูลความคิดเห็น ในการนำไปพัฒนาและปรับปรุงแนวทางในการรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์ รวมทั้งการใช้ข้อมูลจาก Issue Tracking System เพื่อประกอบการพิจารณาปรับปรุงและพัฒนา

กรณีศึกษา: Ransomware โจมตีโรงพยาบาลสระบุรี เรียกค่าไถ่ 200,000 บิทคอยด์ คิดเป็นเงินไทยราว ๆ 63,000 ล้านบาท

ที่มา: Facebook โรงพยาบาลสระบุรี

มัลแวร์เรียกค่าไถ่ (Ransomware) ได้รับการกำหนดโดยกระทรวงยุติธรรมของสหรัฐอเมริกา ในฐานะรูปแบบใหม่ของอาชญากรรมทางไซเบอร์ที่สามารถก่อให้เกิดผลกระทบในระดับโลก สามารถขัดขวางการดำเนินธุรกิจ และนำไปสู่การสูญเสียข้อมูลที่สำคัญได้ ทันทีที่เครื่องเป้าหมายติดมัลแวร์ดังกล่าว คอมพิวเตอร์จะถูกเข้ารหัส หรือบล็อกการเข้าถึงข้อมูลบนดิสก์ แล้วแจ้งหรือยื่นข้อเสนอให้เหยื่อทำการโอนเงินไปยังบัญชีที่ระบุของผู้ไม่ประสงค์ดี เพื่อถอดรหัสไฟล์ที่ถูกเข้ารหัส

โดยปกติแล้วมัลแวร์เรียกค่าไถ่มักจะแพร่กระจายผ่านทางสแปม หรือฟิชชิงอีเมล แต่ยังมีการค้นพบว่า สามารถแพร่กระจายผ่านทางเว็บไซต์ หรือการดาวน์โหลดโดยไดรฟ์ เพื่อติดมัลแวร์ดังกล่าวผ่านอุปกรณ์ปลายทางได้อีกด้วย

วิธีการป้องกัน Ransomware

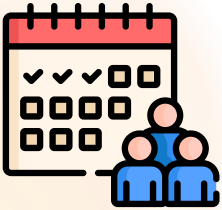
สำหรับผู้ใช้งานทั่วไป (End user)

1. อย่าคลิกเชื่อมโยงจากเว็บไซต์หรืออีเมลที่ไม่น่าเชื่อถือ
2. ติดตั้งและอัปเดตโปรแกรม Antivirus อย่างสม่ำเสมอ
3. สำรองข้อมูลสำคัญอย่างสม่ำเสมอแบบออฟไลน์

ผู้ดูแลระบบที่ต้องดูแลองค์กร (Admin)

1. บล็อก IP จากข้อมูล Threat Intelligence เพื่อป้องกันการเข้าถึงที่ไม่พึงประสงค์
2. จำกัดการเข้าถึงโดยเปิดเฉพาะพอร์ตที่จำเป็น
3. ตั้งค่า Group Policy เพื่อป้องกันการใช้งานไฟล์ที่อาจเป็นอันตราย
4. สำรองข้อมูลแยกออกจากระบบและเข้ารหัสไฟล์ที่สำรอง
5. อบรมเพื่อเพิ่มความรู้และพัฒนาทักษะเกี่ยวกับภัยคุกคามทางอินเทอร์เน็ต

การดำเนินการที่ควรทำทุกเดือน:



1. ตรวจสอบช่องโหว่ของระบบปฏิบัติการ และอัปเดต Patch อย่างสม่ำเสมอ
2. กำหนดสิทธิ์การเข้าถึงไฟล์สำคัญให้เฉพาะ Read-only เท่านั้น
3. ยกเลิกการแชร์ไฟล์ที่ไม่จำเป็นเมื่อไม่มีการใช้งาน

การตรวจจับและรับมือกับภัยคุกคามเชิงรุก

เนื่องจากในปัจจุบัน การโจมตีทางไซเบอร์มีความซับซ้อนและพัฒนาอย่างต่อเนื่อง ทำให้การป้องกันเพียงอย่างเดียวไม่เพียงพออีกต่อไป องค์กรจึงต้องมีการตรวจจับและรับมือกับภัยคุกคามเชิงรุก (Proactive Threat Detection and Response) เพื่อเตรียมพร้อมและตอบสนองต่อเหตุการณ์ที่อาจเกิดขึ้นอย่างมีประสิทธิภาพและรวดเร็ว

การตรวจจับและรับมือกับภัยคุกคามเชิงรุกประกอบด้วยหลายขั้นตอนสำคัญ เช่น การทำ Log Management การใช้ระบบในการตอบสนองและรับมือต่อเหตุการณ์ เช่น SIEM (Security Information and Event Management), SOAR (Security Orchestration, Automation, and Response) และ XDR (Extended Detection and Response) เพื่อช่วยลดความเสี่ยง และเพิ่มความปลอดภัยของระบบและข้อมูลภายในองค์กร

การทำ Log Management

ที่มา: Site24x7 Blog, Top Log Monitoring Tools

Log Management คืออะไร

Log Management คือกระบวนการรวบรวม จัดเก็บ วิเคราะห์ และจัดการข้อมูลบันทึก (Log) จากเซิร์ฟเวอร์ ฐานข้อมูล ระบบเครือข่าย และแอปพลิเคชันต่าง ๆ เป็นเหมือนกลไกที่เก็บรวบรวมเรื่องราวการทำงานและการเข้าถึงของระบบ โดยบันทึกทุกเหตุการณ์ที่เกิดขึ้นในระบบ เช่น errors, warnings, และ events มีประโยชน์มากในการตรวจสอบและวิเคราะห์หาสาเหตุของปัญหา ตรวจสอบความปลอดภัย การเข้าถึงที่ไม่ถูกต้องหรือการเข้าถึงข้อมูลที่มีความลับ และการโจมตีทางไซเบอร์ นอกจากนี้การวิเคราะห์ log ที่รวบรวมไว้ ยังช่วยให้ทราบถึงประสิทธิภาพการทำงานของระบบ และทราบปัญหาที่อาจส่งผลกระทบต่อประสิทธิภาพการทำงาน ทำให้ลดค่าใช้จ่ายในการดูแลระบบและซ่อมบำรุงได้

Log Management มีขั้นตอนอย่างไร

1. กำหนดเป้าหมาย: ระบุวัตถุประสงค์ของการใช้งาน Log Management เพื่อแก้ไขปัญหาที่เกิดขึ้นในระบบหรือฐานข้อมูล วิเคราะห์ประสิทธิภาพของระบบ และกำหนดขอบเขตของการเฝ้าดูระบบ โดยเริ่มจากระบบหรือฐานข้อมูลที่มีความสำคัญเป็นอันดับแรก ๆ

2. เลือกเครื่องมือ: เลือกเครื่องมือ Log Management ที่เหมาะสมกับความต้องการขององค์กร โดยพิจารณางบประมาณและความเชี่ยวชาญของทีม IT

3. รวบรวมข้อมูล: ตั้งค่าระบบเพื่อรวบรวม Log จากแหล่งต่าง ๆ เช่น เซิร์ฟเวอร์ แอปพลิเคชัน ระบบเครือข่าย เป็นต้น

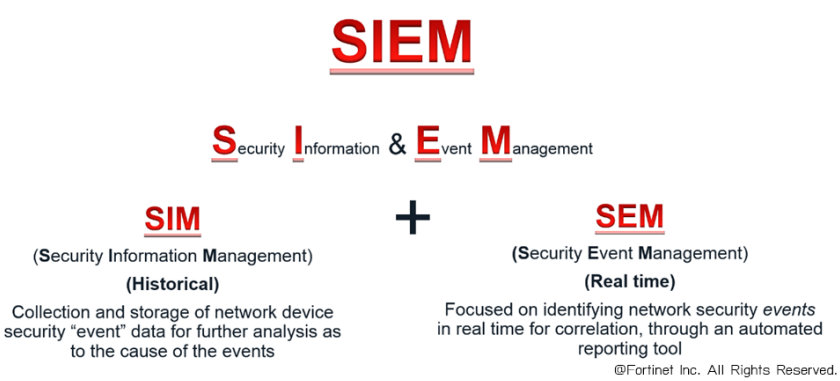
4. จัดเก็บข้อมูล: เลือกวิธีจัดเก็บข้อมูล Log ที่ปลอดภัยและเชื่อถือได้ เช่น ใช้ระบบเก็บข้อมูลที่มีการเข้ารหัสและมีการสำรองข้อมูลอย่างเป็นระบบ

5. วิเคราะห์ข้อมูล: วิเคราะห์ Log โดยใช้เทคนิคการแปลงและตีความข้อมูล เพื่อค้นหาข้อมูลที่สำคัญและการเหตุการณ์ที่มีความหมาย

6. ติดตามผล: ติดตามผลลัพธ์จากการวิเคราะห์ Log เพื่อปรับปรุงและพัฒนาระบบ

การใช้ระบบในการตอบสนองและรับมือต่อเหตุการณ์

ระบบ SIEM กับการตอบสนองและรับมือต่อเหตุการณ์



ที่มา: EZ-GENIUS, ตอนที่ 1 รู้จักระบบ SIEM

ระบบ SIEM คืออะไร

(Security Information and Event Management)

SIEM หมายถึงระบบที่ทำหน้าที่รวบรวมข้อมูลเกี่ยวกับการรักษาความปลอดภัยจากอุปกรณ์ด้านความปลอดภัยของระบบ เช่น Firewall, Active Directory, Endpoint Security หรืออื่น ๆ โดยใช้วิธีการรับข้อมูลจราจรคอมพิวเตอร์ (Log file) จากอุปกรณ์ดังกล่าว และนำมาวิเคราะห์ตรวจหาภัยคุกคามแบบ Real-Time ตามเงื่อนไขที่ผู้ดูแลระบบได้ทำการตั้งค่าไว้ล่วงหน้า SIEM เป็นการผสานการทำงานระหว่างการจัดการข้อมูลการรักษาความปลอดภัย (SIM) และการจัดการเหตุการณ์การรักษาความปลอดภัย (SEM) ให้กลายเป็นระบบการวิเคราะห์ Log บนระบบเครือข่ายและการรักษาความปลอดภัยเพียงระบบเดียว

จุดเด่น

- **ควบคุมและจัดการข้อมูลทั้งหมดได้จากศูนย์กลาง**
- **สามารถรวบรวมข้อมูลจากแหล่งต่าง ๆ ได้อย่างมหาศาล** และสอดคล้องกับกฎหมายที่กำหนดให้เก็บข้อมูลจราจร เป็นเวลา 90 วัน
- **มีระบบช่วยวิเคราะห์ข้อมูลที่รวบรวมมาให้โดยอัตโนมัติ**

ข้อจำกัด

- **ต้องได้รับข้อมูลที่ครบถ้วนจากทุกระบบเพื่อให้สามารถได้อย่างมีประสิทธิภาพ**
- **ต้องมีผู้ดูแลที่มีความเชี่ยวชาญในการทำความเข้าใจข้อมูลจากการสรุปผลและตัดสินใจในการตอบสนองต่อเหตุการณ์ต่าง ๆ** รวมถึงการประสานงานในแต่ละเหตุการณ์
- **การลงทุนในระบบ SIEM มีค่าใช้จ่ายที่ค่อนข้างสูง** เนื่องจากต้องอ้างอิงกับจำนวน Event ที่ระบบต้องรับมาวิเคราะห์

เหมาะกับองค์กรแบบใด

- **มีอุปกรณ์รักษาความปลอดภัยที่ครบครัน:** เช่น Firewall, Endpoint, Proxy เป็นต้น ที่สามารถส่งข้อมูลมาบริหารจัดการจากส่วนกลางได้อย่างมีประสิทธิภาพ
- **มีทีมงานดูแลโดยตรง:** ควรมีบุคลากรที่ถูกมอบหมายให้ดูแลระบบ SIEM โดยเฉพาะ จำนวน 3-5 คน เพื่อทำความเข้าใจและดูแลมาตรการด้านความปลอดภัย รวมถึงการเฝ้าระวังระบบ
- **ต้องการการเก็บข้อมูลเครือข่ายระยะยาว:** เหมาะสำหรับองค์กรที่ต้องเก็บข้อมูลเครือข่ายนานกว่า 90 วัน เพื่อให้สามารถปฏิบัติตามข้อกำหนดและการวิเคราะห์ข้อมูลได้อย่างเต็มประสิทธิภาพ

ระบบ SOAR กับการตอบสนองและรับมือต่อเหตุการณ์

ที่มา: averyittech.com,
Solution Incident Response

ระบบ SOAR คืออะไร

(Security Orchestration, Automation and Response)

ระบบ SOAR เป็นโซลูชันที่ผสานรวมเครื่องมือและกระบวนการรักษาความปลอดภัยต่าง ๆ เข้าด้วยกัน ในรูปแบบของเวิร์กโฟลว์อัตโนมัติ ผู้ดูแลต้องเขียน Playbook หรือ Runbook สำหรับอุปกรณ์ในเครือข่าย ให้สอดคล้องกับภัยคุกคามที่อาจเกิดขึ้น ซึ่งระบบ SOAR จะจัดการตามขั้นตอนที่กำหนดไว้ล่วงหน้าโดยอัตโนมัติ SOAR ช่วยลดภาระงานที่ต้องทำซ้ำ ๆ ด้วยมือ จากงานง่าย ๆ ไปจนถึงงานที่ซับซ้อน นอกจากนี้ยังมอบแพลตฟอร์มสำหรับการจัดการและการตอบสนองต่อเหตุการณ์ โดยรวบรวมและสรุปการแจ้งเตือนจากเครื่องมือรักษาความปลอดภัยต่าง ๆ เช่น ระบบ SIEM ซึ่งช่วยในการตัดสินใจได้อีกด้วย

จุดเด่น

- **ช่วยให้องค์กรสามารถกำหนดและตั้งค่าวิธีการตอบสนองต่อเหตุการณ์ได้** ส่งผลให้มีเวลาและงบประมาณมากขึ้นเพื่อให้ความสำคัญกับโครงการที่มีความสำคัญสูงกว่า
- **ลดปัญหากรณีที่มีบุคลากรดูแลระบบน้อย** หรือมี การเปลี่ยนแปลงบุคลากรที่ดูแลระบบบ่อยครั้ง
- **ลดความเสี่ยงที่เกิดจากความแตกต่างในระดับความรู้และความเข้าใจ** ในการอ่านและตอบสนองต่อภัยคุกคามของผู้ดูแลระบบแต่ละคน

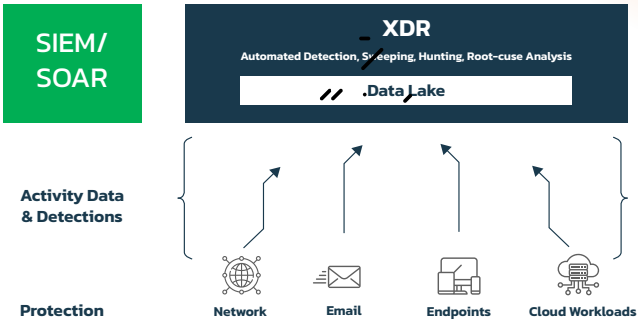
ข้อจำกัด

- **ต้องพึ่งพาและจัดการข้อมูลจากหลายแหล่ง** เช่น SIEM, Firewall และ Endpoint Protection เพื่อสั่งการหรือจัดทำ Playbook
- **ความยากในการจัดการของ Playbook และ Runbook** ต้องอาศัยผู้เชี่ยวชาญในการเข้าบริหารจัดการนโยบาย

เหมาะกับองค์กรแบบใด

- **มีอุปกรณ์รักษาความปลอดภัยครบถ้วน:** เช่น Firewall, Endpoint, Proxy, และ SIEM เพื่อสามารถส่งข้อมูลมาบริหารจัดการความเสี่ยง และกำหนดมาตรการด้านความปลอดภัยให้สอดคล้องกับ Playbook ที่มี
- **มีศูนย์ SOC หรือ CSIRT:** เพื่อการดูแลและบริหารจัดการระบบรักษาความปลอดภัยอย่างมีประสิทธิภาพ
- **องค์กรระดับมหาชน:** มีเครือข่ายสาขามากมายและต้องการเสริมความมั่นคงปลอดภัยทางไซเบอร์ เพื่อเพิ่มความแข็งแกร่งให้กับธุรกิจ

ระบบ XDR กับการตอบสนองและรับมือต่อเหตุการณ์



ที่มา: LinkedIn, Why XDR is Important for Security Operations Modernization?

ระบบ XDR คืออะไร

(Extended Detection and Response)

XDR เป็นโซลูชันที่ใช้ในการตรวจจับและตอบสนองต่อภัยคุกคามทางไซเบอร์อย่างเจาะจง เป็น Software as a Service (SaaS) ที่รวมผลิตภัณฑ์ความปลอดภัยหลายตัวเข้าไว้ในระบบปฏิบัติการเดียว มีการใช้เทคโนโลยี AI และการวิเคราะห์ขั้นสูงเพื่อตรวจสอบโดเมนจำนวนมากในสภาพแวดล้อมทางเทคโนโลยีขององค์กร สามารถเก็บรวบรวมข้อมูลและหาความสัมพันธ์ของข้อมูลจากส่วนต่าง ๆ เช่น เครื่องพีซี อุปกรณ์โมบาย อีเมล์ เครื่องเซิร์ฟเวอร์ Cloud ฯลฯ ทำให้ตรวจจับและระบุภัยคุกคามที่เกิดขึ้นข้าม Security layers และรวมระบบต่าง ๆ ไว้ในภาพรวมเดียวได้ มีการจัดลำดับความสำคัญของเหตุการณ์ที่เกิดขึ้น ช่วยให้ทีมรักษาความปลอดภัยเข้าใจอันตรายที่เกิดขึ้นได้ชัดเจนและตอบสนองได้รวดเร็ว

จุดเด่น

- **บูรณาการเครื่องมือรักษาความปลอดภัยและแหล่งข้อมูลหลายแหล่ง** ทำให้มีมุมมองที่ครอบคลุมมากขึ้นเกี่ยวกับมาตรการรักษาความปลอดภัย
- **ใช้การวิเคราะห์ขั้นสูงและตรวจจับภัยคุกคามที่ซับซ้อนโดยอัตโนมัติ** รับประกันการตอบสนองอย่างรวดเร็วต่อภัยคุกคามที่ระบุ
- **ช่วยให้องค์กรมีความยืดหยุ่นในการดำเนินการตอบสนองต่อการโจมตีได้มากขึ้น** เพิ่มความมั่นใจในระบบความปลอดภัยขององค์กร

ข้อจำกัด

- **XDR มักทำงานได้ดีที่สุดเมื่อใช้ส่วนประกอบทั้งหมดมาจากผู้ขายเดียวกัน** ซึ่งอาจทำให้มีข้อจำกัดในความยืดหยุ่นและทางเลือกสำหรับองค์กร รวมถึงการบูรณาการเครื่องมือของบุคคลที่สามหรือระบบเดิมอาจไม่ราบรื่น
- **การพึ่งพาระบบอัตโนมัติมากเกินไปอาจทำให้เกิดช่องว่างด้านความปลอดภัย** และอาจเกิดความไม่แน่นอนในการตอบสนองต่อภัยคุกคามที่ไม่ได้ระบุล่วงหน้า

เหมาะกับองค์กรแบบใด

- **การปรับปรุงกระบวนการตรวจจับภัยคุกคาม:** องค์กรที่ต้องการเพิ่มประสิทธิภาพในการตรวจจับภัยคุกคามที่ซับซ้อนโดยใช้การวิเคราะห์ขั้นสูงและการเรียนรู้ของเครื่อง เพื่อสามารถตอบสนองต่อการโจมตีได้อย่างมีประสิทธิภาพมากขึ้น
- **การตอบสนองที่เร็วขึ้น:** ตอบสนองต่อภัยคุกคามที่ระบุได้อย่างรวดเร็ว ด้วยการแจ้งเตือนและการรายงานที่ทันท่วงที
- **การเพิ่ม ROI ด้านความปลอดภัย:** XDR ช่วยลดค่าใช้จ่ายในการจัดการความปลอดภัยโดยรวม และเพิ่มผลตอบแทนจากการลงทุนในเทคโนโลยีที่มีประสิทธิภาพในการตอบสนองต่อภัยคุกคาม

ความแตกต่างของระบบ SIEM, SOAR, และ XDR

Functionality	SOAR	SIEM	XDR
Open platform for aggregating telemetry and security-relevant data from diverse sources	✓	Varies	✓
Long-term data retention for compliance and audit	-	✓	Varies
Alert enrichment with threat intelligence to detect & identify advanced threats	✓	-	✓
Uses AI/ML and human intelligence to continuously improve threat detection and identification	✓	-	✓
Helps SecOps respond to and remediate security issues faster and more efficiently with automated actions and proven playbooks	✓	-	✓
A single unified detection and response platform integrated with multiple security tools, vendors, and telemetry types	-	-	✓
Predictable pricing model and reduced tool sprawl to save time and money	-	-	✓

ที่มา: Secureworks, UNDERSTANDING THE DIFFERENCE BETWEEN SOAR VS SIEM VS XDR

SIEM ทำหน้าที่หลักในการเป็นเครื่องมือรวบรวม Log สำหรับข้อมูลเหตุการณ์สำคัญ ซึ่งต้องใช้ความพยายามในการจัดเก็บข้อมูล การรายงานการปฏิบัติตามข้อกำหนด และการวิเคราะห์แบบเรียลไทม์ด้วยมือ

SOAR ช่วยลดความพยายามที่ต้องใช้ด้วยมือ โดยการทำให้กระบวนการสำคัญง่ายขึ้น เช่น การตอบสนองต่อเหตุการณ์ การประสานงาน และการทำงานอัตโนมัติ นอกจากนี้ยังรวมความสามารถหลักของโซลูชัน SIEM เข้ากับเครื่องมือด้านความปลอดภัยที่สำคัญ

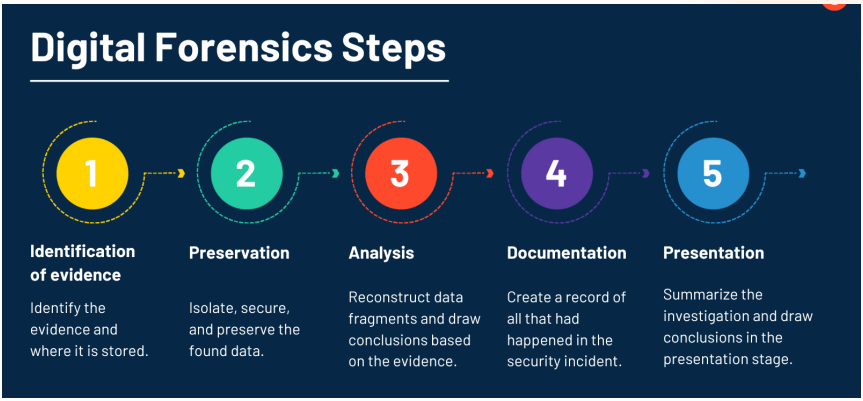
XDR รวบรวมแหล่งข้อมูลการตรวจจับภัยคุกคามที่หลากหลาย ซึ่งก่อนหน้านี้จะถูกส่งไปยัง SIEM พร้อมทั้งเสนอความสามารถแบบ “SOAR-lite” โดยเน้นที่ข้อมูลจาก Endpoint และการปรับแต่งให้เหมาะสม XDR มีความสามารถในการวิเคราะห์ขั้นสูงที่ช่วยให้องค์กรสามารถมุ่งเน้นไปที่เหตุการณ์ที่มีความสำคัญสูงสุดและตอบสนองได้อย่างรวดเร็ว

ความสำคัญของ Digital Forensics ในการสืบสวนเหตุการณ

Digital Forensics คืออะไร และเหตุใดจึงสำคัญในการสืบสวนเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ

Digital Forensics หรือ นิติวิทยาดิจิทัล เป็นการจัดเก็บรวบรวม และวิเคราะห์หลักฐานทางดิจิตอลที่อยู่ในอุปกรณ์คอมพิวเตอร์และอิเล็กทรอนิกส์ เช่น ไฟล์ที่อยู่ในคอมพิวเตอร์ โทรศัพท์มือถือ รวมถึงหลักฐานดิจิทัลที่ถูกสร้างจากระบบคอมพิวเตอร์ เพื่อนำข้อมูลเหล่านั้น มาใช้เป็นหลักฐานประกอบรูปคดี โดยที่หลักฐานดิจิทัลเหล่านี้สามารถช่วยระบุตัวผู้กระทำความผิด หรือผู้ที่มีส่วนเกี่ยวข้องกับการก่อเหตุอาชญากรรมด้านความมั่นคงปลอดภัยสารสนเทศได้ เช่น การจารกรรมข้อมูล ภัยคุกคาม หรือการรั่วไหลของข้อมูล เป็นต้น

ขั้นตอน Digital Forensics:



ที่มา: G2, Digital Forensics

1. การระบุ (Identification)

ขั้นตอนแรกสุดในการสืบสวนทางนิติเวชดิจิทัล คือ การระบุอุปกรณ์และทรัพยากรที่มีข้อมูลที่จะเป็นส่วนหนึ่งของการสืบสวน ซึ่งข้อมูลที่เกี่ยวข้องกับการสืบสวนอาจอยู่ในอุปกรณ์ขององค์กรหรือบนอุปกรณ์ส่วนตัวของผู้ใช้ หลังจากนั้นจะมีการยึดอุปกรณ์เหล่านี้ และแยกออกจากกันเพื่อป้องกันการปลอมแปลงข้อมูล หากข้อมูลตั้งอยู่บนเซิร์ฟเวอร์หรือเครือข่าย หรือเก็บไว้บนคลาวด์ ผู้ตรวจสอบหรือองค์กรจะต้องตรวจสอบให้แน่ใจว่า มีเพียงทีมสืบสวนเท่านั้นที่มีสิทธิ์เข้าถึงข้อมูลได้

2. การเก็บรักษา (Preservation)

หลังจากที่อุปกรณ์ที่เกี่ยวข้องกับการสืบสวนถูกยึด และเก็บรักษาไว้ในสถานที่ที่ปลอดภัยแล้ว นักวิเคราะห์ดิจิทัลหรือนิติเวชดิจิทัลจะใช้เทคนิคทางนิติวิทยาศาสตร์ เพื่อดึงข้อมูลที่เป็นไปได้ที่เกี่ยวข้องกับการสอบสวน และทำการจัดเก็บไว้อย่างปลอดภัย

ขั้นตอนนี้มักเกี่ยวข้องกับการสร้างสำเนาดิจิทัลของข้อมูลที่เกี่ยวข้อง ซึ่งเรียกว่า “ภาพทางนิติวิทยาศาสตร์” จากนั้นสำเนานี้จะถูกนำไปใช้ในการวิเคราะห์และการประเมินผล ในขณะเดียวกัน ข้อมูลและอุปกรณ์ต้นฉบับจะถูกเก็บรักษาไว้ในตู้นิรภัยหรือที่ปลอดภัย เพื่อป้องกันการดัดแปลงข้อมูล

3. การวิเคราะห์ (Analysis)

เมื่อได้ทำการระบุและแยกอุปกรณ์ที่เกี่ยวข้อง และข้อมูลได้รับการทำสำเนาและเก็บไว้อย่างปลอดภัยแล้ว นักวิเคราะห์ดิจิทัลจะใช้เทคนิคที่หลากหลายเพื่อดึงข้อมูลที่เกี่ยวข้อง และทำการตรวจสอบโดยการค้นหาเบาะแสหรือหลักฐานที่ชี้ไปที่การกระทำผิด ซึ่งมักเกี่ยวข้องกับการกู้คืนและตรวจสอบไฟล์ที่ถูกลบ เสียหาย หรือเข้ารหัส โดยใช้เทคนิคต่าง ๆ เช่น:

การดึงข้อมูลที่ซ่อนอยู่ (Reverse Steganography): เทคนิคที่ใช้ในการค้นพบข้อมูลที่ถูกซ่อนอยู่ โดยการตรวจสอบแฮชหรือสตริงอักขระ ที่ซ่อนอยู่ภายในรูปภาพหรือรายการข้อมูลอื่น ๆ

การกู้คืนไฟล์หรือข้อมูลที่ถูกลบ (File Carving): การระบุและกู้คืนไฟล์ที่ถูกลบ โดยการค้นหาแฟรกเมนต์ที่อาจเหลือของไฟล์ที่ถูกลบ

การค้นหาคำหลัก (Keyword Search): การใช้คำหลักเพื่อระบุและวิเคราะห์ข้อมูลที่เกี่ยวข้องกับการสืบสวน รวมถึงข้อมูลที่ถูกลบ

4. การจัดทำเอกสาร (Documentation)

หลังจากการวิเคราะห์ข้อมูลและการค้นพบที่สำคัญในการสืบสวนทางนิติวิทยาศาสตร์ดิจิทัลแล้ว การบันทึกข้อมูลจะถูกทำอย่างเหมาะสมเพื่อให้ง่ายต่อการเข้าใจกระบวนการสืบสวนทั้งหมดและสรุปผลที่ได้ เอกสารที่เหมาะสมจะช่วยในการกำหนดลำดับเวลาของกิจกรรมที่เกี่ยวข้อง เช่น การยักยอกข้อมูล การรั่วไหลของข้อมูล หรือการละเมิดเครือข่าย เป็นต้น

5. การนำเสนอ (Presentation)

หลังจากการสืบสวนทางนิติวิทยาศาสตร์ดิจิทัลเสร็จสิ้นแล้ว ข้อความหลักฐานที่ค้นพบจะถูกนำเสนอให้กับศาลหรือคณะกรรมการ ที่มีหน้าที่ตัดสินคดีหรือการร้องเรียนภายใน ผู้ตรวจสอบนิติเวชดิจิทัลทำหน้าที่เป็นพยานผู้เชี่ยวชาญ โดยสรุปและนำเสนอหลักฐานที่พวกเขาค้นพบ และเปิดเผยข้อความที่ค้นพบ เพื่อให้คณะกรรมการหรือศาลทราบในการตัดสินคดีหรือการร้องเรียนนั้น

เครื่องมือที่ใช้ในการสืบสวน

The Sleuth Kit (+Autopsy)

AUTOPSY
DIGITAL FORENSICS

ที่มา: CyberPunk, Digital Forensics Platform

The Sleuth Kit เป็นเครื่องมือสำหรับตรวจพิสูจน์พยานหลักฐานดิจิทัลที่ เปิดเผยรหัสโปรแกรม (Source Code) ที่สามารถใช้เพื่อวิเคราะห์เชิงลึกกับไฟล์ระบบได้หลากหลายประเภท Autopsy ทำงานเป็น GUI ให้กับ Sleuth Kit ในส่วนที่จำเป็นสำหรับการทำงาน The Sleuth Kit มาพร้อมกับคุณสมบัติพิเศษ เช่น การวิเคราะห์ตามลำดับเวลา (Time Serial) การกรอง Hash การวิเคราะห์ไฟล์ระบบ และความสามารถในการค้นหาข้อมูลด้วยคำสำคัญ และยังสามารถเพิ่มโมดูลอื่น เพื่อให้สามารถใช้งานได้กว้างมากขึ้นได้อีกด้วย

จุดเด่น

1. แสดงเหตุการณ์ที่เกิดขึ้นกับระบบผ่านหน้าจอที่เป็น GUI
2. มีตัวเลือกการวิเคราะห์ Registry, ไฟล์ LNK, และอีเมล
3. สนับสนุนไฟล์หลายรูปแบบ
4. สามารถแยกข้อมูลออกจาก SMS, บันทึกการโทร, บันทึกหมายเลขติดต่อ, โปรแกรม Tango, และคำพูดจากเพื่อนเพื่อวิเคราะห์ได้

FTK Forensic Toolkit

ที่มา: CyberPunk, Digital Forensics Platform

FTK Forensic Toolkit เป็นซอฟต์แวร์สำหรับ Digital Forensics ที่มีความสามารถในการรวบรวมและวิเคราะห์ข้อมูลอย่างเป็นทางการได้ดี สามารถสแกนฮาร์ดไดรฟ์ ค้นหาอีเมลที่ถูกลบ และสแกนดิสก์ เพื่อค้นหาข้อความเพื่อถอดรหัส เป็นการรวบรวมของเครื่องมือฟอร์เรนสิกที่พบบ่อยที่สุดสำหรับนักสืบสอบสวน

จุดเด่น

1. สามารถประมวลผลข้อมูลจำนวนมากได้อย่างรวดเร็ว ช่วยให้สามารถทำการวิเคราะห์ได้ทันที
2. มีประโยชน์สำหรับการสืบสวนทางฟอร์เรนสิกในหลายกรณี เนื่องจากมีการสนับสนุนรูปแบบไฟล์ที่ยืดหยุ่นและชุดคุณสมบัติที่หลากหลาย
3. สนับสนุนฟังก์ชันการทำงานร่วมกัน ทำให้การสืบสวนดำเนินไปได้เร็วขึ้น

EnCase

ที่มา: CyberPunk, Digital Forensics Platform

EnCase เป็นแอปพลิเคชันที่ถูกพัฒนาโดย Guidance Software เป็นเครื่องมือระดับมืออาชีพ ที่ใช้ในการกู้คืนหลักฐานจากฮาร์ดไดรฟ์และอุปกรณ์ต่าง ๆ ทำให้ผู้ใช้สามารถวิเคราะห์ไฟล์อย่างละเอียด เพื่อรวบรวมหลักฐาน เช่น เอกสาร และรูปภาพ เป็นต้น

จุดเด่น

1. สามารถดึงข้อมูลจากอุปกรณ์ได้หลากหลายประเภท
2. ช่วยในการสร้างรายงานที่ครบถ้วน เพื่อรักษาความสมบูรณ์ของหลักฐาน
3. มีความสามารถในการค้นหา ระบุ และจัดลำดับความสำคัญของหลักฐานได้อย่างรวดเร็ว
4. ช่วยในการปลดล็อกหลักฐานที่เข้ารหัสและเตรียมหลักฐานโดยอัตโนมัติ
5. สามารถทำการวิเคราะห์เชิงลึกและการประเมินระดับความรุนแรงและความสำคัญของข้อบกพร่องได้

กรณีศึกษา: การใช้ Digital Forensics ในการสืบสวนการกระทำผิดของพนักงานองค์กร

Digital Forensics ดูเหมือนจะเป็นทางเลือกที่มีราคาค่อนข้างสูง ซึ่งทำให้คิดได้ว่าอาจจะไม่คุ้มค่าในการลงทุน อย่างไรก็ตาม ในระหว่างการสืบสวนข้อมูล บ่อยครั้งที่สามารถตรวจหาหลักฐานสำคัญที่สามารถนำไปดำเนินคดีในศาลได้ และมีหลายคดีที่สามารถนำไปเป็นหลักฐานในการต่อสู้คดี ซึ่งจะช่วยป้องกันความเสียหายทางธุรกิจได้ ดังตัวอย่างต่อไปนี้

เหตุการณ์: พนักงานในองค์กรแห่งหนึ่ง ซึ่งมีหน้าที่รับผิดชอบแบ็กอัปข้อมูลของบริษัทมาเป็นระยะเวลาหลายปี ได้ตัดสินใจลาออกโดยไม่มีการแจ้งให้บริษัททราบล่วงหน้า เมื่อเขาลาออกไป ทางบริษัทพบว่าเขาได้ลบข้อมูลบางส่วนในอีเมลออกไปด้วย

การนำ Digital Forensics มาใช้: เมื่อได้ใช้การตรวจสอบทาง Forensic ที่ฮาร์ดดิสก์คอมพิวเตอร์ของพนักงาน และที่เมลเซิร์ฟเวอร์ของบริษัท พบว่า ก่อนที่เขาจะออกจากบริษัท เขาได้มีการเสียบ USB ไดร์ฟ ที่เครื่องคอมพิวเตอร์และก็อปปี้ข้อมูลที่แบ็กอัปไว้ และเขายังได้เข้าใช้งานอีเมลโดยทำการลบอีเมลสำคัญ เมื่อจำนนต่อหลักฐาน เขาจึงยอมรับสารภาพและไม่สามารถโต้แย้งได้

สรุปท้ายบท Chapter 8

การตอบสนองต่อเหตุการณ์ภัยคุกคามทางสารสนเทศ

กระบวนการและขั้นตอนในการตอบสนองต่อเหตุการณ์ ที่เกี่ยวข้องกับความปลอดภัยทางสารสนเทศ โดยเน้นถึงความสำคัญของการมีแผนการตอบสนองที่ชัดเจนและปฏิบัติได้จริง เพื่อช่วยในการจัดการความเสี่ยงที่เกิดจากการละเมิดข้อมูลและการโจมตีทางไซเบอร์ การตอบสนองที่รวดเร็วและมีประสิทธิภาพ ช่วยให้องค์กรสามารถกลับสู่สภาวะปกติได้เร็วขึ้น และลดความเสียหายที่อาจเกิดขึ้น นอกจากนี้ การทำ Log Management และการใช้ระบบต่าง ๆ เช่น SIEM, SOAR, และ XDR มีประโยชน์ในการตรวจสอบและตอบสนองต่อเหตุการณ์ การฝึกซ้อมแผน Incident Response ช่วยในการบริหารจัดการความเสี่ยงและตอบสนองต่อเหตุการณ์ได้อย่างมีประสิทธิภาพ และการทำ Digital Forensics เพื่อตรวจสอบเหตุการณ์

MODULE 05

การกู้คืนทางสารสนเทศหลังเกิดเหตุการณ์ด้านความมั่นคงปลอดภัย

(Information Security Incident) #Recovery

วัตถุประสงค์

เพื่อให้ผู้เข้ารับการฝึกอบรมมีความรู้ความเข้าใจ เกี่ยวกับการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ สามารถระบุและประเมินความเสี่ยง วิเคราะห์และเลือกใช้กลยุทธ์การจัดการความเสี่ยงที่เหมาะสม รวมถึงสามารถนำมาตรการควบคุมต่าง ๆ ไปใช้ในการป้องกันและลดความเสี่ยงได้อย่างมีประสิทธิภาพ

CHAPTER 9 การกู้คืนทรัพย์สินและการดำเนินงาน

จุดประสงค์และปัจจัยการกู้คืนทรัพย์สินในระบบสารสนเทศ

จุดประสงค์ของการกู้คืนระบบ

Short-Term Recovery Objective: ภายใน 2-3 ชั่วโมงหลังจากเกิดภัยพิบัติ มุ่งเน้นการกู้คืนสิ่งอำนวยความสะดวกและโครงสร้าง

Medium-Term Recovery Objectives: ช่วงสัปดาห์แรกหลังจากเกิดภัยพิบัติ เป้าหมายหลักคือการเรียกคืนงานที่สำคัญที่ส่งผลกระทบต่อการดำเนินงานทางธุรกิจขององค์กร

Long-Term Recovery Projects: จุดประสงค์คือการเรียกคืนระบบให้กลับสู่สภาวะก่อนเกิดภัยพิบัติ และจัดทำแผนงานตรวจสอบการทำงานหลังกู้คืน เพื่อให้แน่ใจว่าสามารถทำงานได้ในระยะยาว

ปัจจัยที่จำเป็นสำหรับกระบวนการกู้คืนระบบ

การกู้คืนระบบหลังจากภัยพิบัติหรือเหตุการณ์ที่ไม่คาดคิด จำเป็นต้องพิจารณาปัจจัยหลายประการเพื่อให้กระบวนการเป็นไปอย่างมีประสิทธิภาพและรวดเร็วที่สุด ดังนี้:

ข้อมูลที่ได้รับ การบำรุงรักษา และค่าใช้จ่ายในการปฏิบัติงาน

1. ข้อมูลที่ได้รับ: ความถูกต้องและความครบถ้วนของข้อมูล ที่รวบรวมมาใช้ในกระบวนการกู้คืนมีความสำคัญสูงสุด ข้อมูลควรได้รับการตรวจสอบและปรับปรุงอยู่เสมอ

2. การบำรุงรักษา: การดูแลรักษาระบบและโครงสร้างพื้นฐาน ให้อยู่ในสภาพดี สามารถลดความเสี่ยงและเวลาในการกู้คืน

3. ค่าใช้จ่ายในการปฏิบัติงาน: การจัดการงบประมาณสำหรับการดำเนินการกู้คืน เช่น ค่าวัสดุอุปกรณ์ ค่าจ้างบุคลากร และค่าใช้จ่ายอื่น ๆ ควรถูกวางแผนและจัดการอย่างเหมาะสม

งบประมาณการกู้คืนระบบขององค์กร

งบประมาณสำหรับกระบวนการกู้คืนระบบควรถูกกำหนดและวางแผนไว้อย่างละเอียด ครอบคลุมทุกด้าน เช่น การจัดหาอุปกรณ์ซ่อมแซม การจ้างผู้เชี่ยวชาญ การฝึกอบรมพนักงาน และการซื้อซอฟต์แวร์หรือโซลูชันเพิ่มเติม งบประมาณที่เพียงพอช่วยให้กระบวนการกู้คืนเป็นไปอย่างราบรื่นและมีประสิทธิภาพ

ระยะเวลาที่ใช้ไปกับการกู้คืนระบบ

การกำหนดเวลาที่ต้องใช้ในการกู้คืนระบบอย่างชัดเจนเป็นสิ่งสำคัญเพื่อลดผลกระทบต่อการดำเนินงานขององค์กรระยะเวลานี้ ขึ้นอยู่กับความรุนแรงของภัยพิบัติและความซับซ้อนของระบบการกำหนดเป้าหมายเวลาที่ใช้ในการกู้คืนในแต่ละระยะจะช่วยในการวางแผน และการจัดการทรัพยากรอย่างมีประสิทธิภาพ

ความพร้อมของบุคลากรเพื่อปฏิบัติงานและการจัดการ

บุคลากรที่มีทักษะและความรู้ความสามารถในการจัดการและกู้คืนระบบเป็นสิ่งจำเป็น การฝึกอบรมและเตรียมความพร้อมให้กับบุคลากร จะช่วยให้กระบวนการกู้คืนเป็นไปอย่างรวดเร็วและมีประสิทธิภาพ นอกจากนี้ การกำหนดบทบาทและความรับผิดชอบของบุคลากรในแต่ละขั้นตอนอย่างชัดเจน จะช่วยลดความสับสนและความล่าช้าในการดำเนินงาน

ความพร้อมและโซลูชันจาก Third Party

โซลูชันและบริการจากผู้ให้บริการภายนอก หรือ Third Party สามารถช่วยเพิ่มประสิทธิภาพในการกู้คืนระบบได้ การเลือกใช้โซลูชันที่เหมาะสม เช่น บริการคลาวด์สำหรับการสำรองข้อมูล โซลูชันการกู้คืนข้อมูลจากภัยพิบัติ การสนับสนุนทางเทคนิค และการให้คำปรึกษาจากผู้เชี่ยวชาญจะช่วยลดความเสี่ยงและเพิ่มความเร็วในการกู้คืน

ระยะของการกู้คืนระบบ (Disaster Recovery Phases)

การกู้คืนระบบที่มีประสิทธิภาพ จำเป็นต้องมีลำดับขั้นตอนที่ชัดเจนและครอบคลุมทุกด้าน เพื่อให้แน่ใจว่าระบบจะกลับมาทำงานได้อย่างสมบูรณ์และปลอดภัย โดยสามารถกำหนดเป็นเฟสของการทำงานดังนี้

1. Activation Phase

ประกาศแจ้งเตือน: แจ้งเตือนแก่ผู้ที่เกี่ยวข้องและผู้ที่มีส่วนได้ส่วนเสียกับกระบวนการกู้คืนระบบ เพื่อให้ทุกคนตระหนักถึงเหตุการณ์ที่เกิดขึ้นและเตรียมพร้อม
ประเมินความเสียหาย: ทำการประเมินความเสียหาย เพื่อกำหนดระดับของความเร่งด่วนในการกู้คืนระบบ รวมถึงการกำหนดทรัพยากรที่จำเป็นต้องใช้ในการกู้คืน
กระตุ้นการกู้คืน: เริ่มกระบวนการกู้คืนระบบ โดยใช้ทรัพยากรและบุคลากรที่เตรียมไว้และกำหนดลำดับขั้นตอนการทำงานอย่างชัดเจน

2. Notification Phase

แจ้งข่าวสาร: แจ้งข่าวสารเกี่ยวกับธรรมชาติของภัยพิบัติและความเสียหายที่อาจเกิดขึ้นให้ทุกคนที่เกี่ยวข้องรับทราบ

รายงานความสูญเสีย: รายงานความสูญเสียชีวิต การบาดเจ็บ และความเสียหายต่อโครงสร้างที่เกิดขึ้น

รายละเอียดการตอบสนองครั้งแรก: ให้ข้อมูลเกี่ยวกับการตอบสนองในครั้งแรกที่เกิดเหตุการณ์ รวมถึงการปฏิบัติงานเบื้องต้น

ประเมินเวลาในการกู้คืน: ประเมินเวลาที่จะใช้ในการกู้คืนระบบ และแจ้งให้ทุกคนรับทราบ

ข้อมูลแผนงานโดยสรุป: ให้ข้อมูลแผนงานโดยสรุปและข้อปฏิบัติต่าง ๆ สำหรับการกู้คืนระบบ

ข่าวสารและข้อแนะนำ: แจ้งข่าวสารและข้อแนะนำ เกี่ยวกับสถานที่พักพิงหรือที่ทำงานชั่วคราว รวมถึงวิธีการเข้าถึงและการใช้สถานที่ดังกล่าว

รายละเอียดการติดต่อ: ให้รายละเอียดการติดต่อบุคคลหรือหน่วยงานที่เกี่ยวข้องในกรณีเกิดเหตุการณ์ เพื่อให้สามารถติดต่อสื่อสารได้อย่างรวดเร็วและมีประสิทธิภาพ

3. Damage Assessment Phase

ระบุสาเหตุและธรรมชาติของภัยพิบัติ: ทำการระบุสาเหตุและธรรมชาติของภัยพิบัติที่เกิดขึ้น เพื่อให้เข้าใจถึงขอบเขตของปัญหา และตรวจสอบว่ามีปัจจัยใดที่เกี่ยวข้อง

ประเมินความเสียหายและผลกระทบ: ประเมินความเสียหาย ขนาดพื้นที่ที่กำลังเกิดปัญหา และผลกระทบต่อระบบและการปฏิบัติงานในยามวิกฤติ เพื่อให้สามารถกำหนดขอบเขตการกู้คืนได้อย่างชัดเจน

ประเมินความเป็นไปได้ของความเสียหายต่อเนื่อง: ประเมินความเป็นไปได้ของความเสียหายที่อาจเกิดขึ้นต่อเนื่อง เพื่อวางแผนการป้องกันและลดผลกระทบ

ประเมินเวลาที่คาดว่าจะใช้ในการกู้คืน: ประเมินเวลาที่จะกู้คืนระบบและการปฏิบัติงานให้กลับมาสู่สภาวะปกติ รวมถึงการกำหนดลำดับความสำคัญของการกู้คืน

ประเมินความสามารถของอุปกรณ์: ประเมินว่าอุปกรณ์ในที่เกิดเหตุจะสามารถทำงานต่อไปได้อีกนานเท่าใด และวางแผนการทดแทนอุปกรณ์ที่เสียหาย

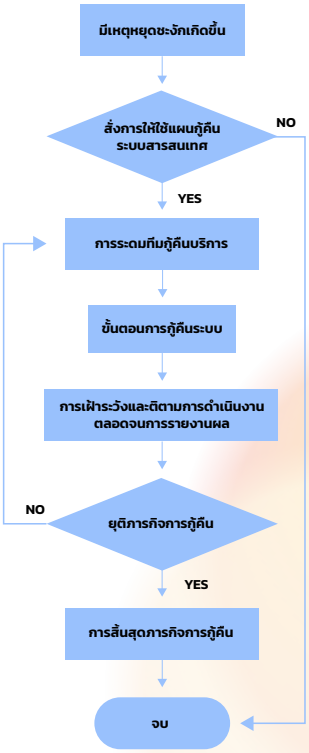
4. Execution Phase

จัดลำดับความสำคัญของกิจกรรมกู้คืนระบบ: จัดลำดับความสำคัญของกิจกรรมต่าง ๆ ในการกู้คืนระบบ เพื่อให้แน่ใจว่าสินทรัพย์ที่มีความสำคัญจะได้รับการกู้คืนก่อน
กระบวนการกู้คืน: กำหนดแนวทางการกู้คืนระบบที่ชัดเจน และมีลำดับขั้นตอนที่เหมาะสมภายใต้สถานการณ์ต่าง ๆ โดยให้ทีมงานตระหนักถึงลำดับการทำงานและปฏิบัติตามอย่างเคร่งครัด

5. Reconstitution Phase

เรียกคืนระบบสู่สภาวะปกติ: ทำการเรียกคืนระบบและปฏิบัติการที่ได้รับผลกระทบกลับสู่สภาวะปกติ โดยระบบที่ไม่สามารถเรียกคืนได้ จะถูกแทนที่ด้วยระบบใหม่
ทดสอบระบบที่กู้คืน: ทดสอบระบบที่กู้คืน เพื่อให้แน่ใจว่าไม่มีความล้มเหลวซ้ำก่อนนำไปติดตั้งที่เดิม
ตรวจสอบและทดสอบการปฏิบัติงานเป็นระยะ ๆ: ทำการตรวจสอบและทดสอบการปฏิบัติงานเป็นระยะ ๆ เพื่อให้แน่ใจว่า ระบบสามารถทำงานได้อย่างมีประสิทธิภาพและปลอดภัย

ที่มา: แผนกู้คืนระบบสารสนเทศ ปี 2564, กองเทคโนโลยีดิจิทัล



แผนฟื้นฟูภัยพิบัติ/แผนการกู้คืนจากภัยคุกคามทางไซเบอร์ (Disaster Recovery Plan – DRP)

ที่มา: https://www.ravepubs.com/make-a-disaster-recovery-plan/

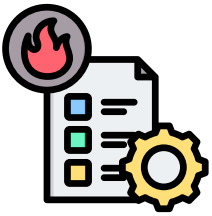
แผนฟื้นฟูภัยพิบัติ (Disaster Recovery Plan - DRP) คือแนวทางปฏิบัติในการระบุสินทรัพย์ที่สำคัญขององค์กร และอธิบายวิธีการจัดการแก้ปัญหาหลังเกิดภัยพิบัติที่ไม่คาดคิด เช่น การโจมตีทางไซเบอร์ ความล้มเหลวของระบบ ไฟฟ้าขัดข้อง ภัยพิบัติทางธรรมชาติฯลฯ เพื่อช่วยในการกู้คืนระบบและทำให้การทำงานขององค์กรกลับคืนสู่สภาวะปกติ ลดผลกระทบความเสียหายต่อระบบข้อมูลขององค์กร และลดโอกาสที่จะเกิดภัยพิบัติประเภทต่าง ๆ ในอนาคต โดย DRP จะระบุตำแหน่งและความรับผิดชอบของพนักงาน ให้คำแนะนำทีละขั้นตอนสำหรับกระบวนการกู้คืน รวมถึงแผนการลดผลกระทบของเหตุการณ์

ขั้นตอนในการวางแผนฟื้นฟูภัยพิบัติ

1. กำหนดทีมกู้คืน:

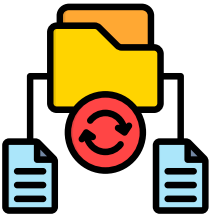
เลือกบุคคลในทีม ซึ่งมีหน้าที่ในการกู้คืนระบบสารสนเทศ และรักษาความต่อเนื่องทางธุรกิจ กำหนดความรับผิดชอบของสมาชิกในทีม โดยที่สมาชิกในทีมไม่ควรมีแต่ผู้เชี่ยวชาญทางด้าน IT เพียงอย่างเดียว แต่ควรรวมถึงบุคคลจากแผนกอื่น ๆ ขององค์กรที่สามารถมีบทบาทในการกู้คืนระบบ เช่น ฝ่ายประชาสัมพันธ์ ซึ่งช่วยให้องค์กรสามารถสื่อสารเรื่องระยะเวลาที่คาดว่าเหตุการณ์จะสงบลงได้ ไปยังผู้มีส่วนได้ส่วนเสีย นอกจากนี้ การแต่งตั้งผู้นำเพื่อควบคุมกระบวนการกู้คืนและทำการตัดสินใจในประเด็นต่าง ๆ เป็นเรื่องที่สำคัญเช่นกัน ตัวอย่างเช่น

Operations Recovery Director



ป้องกันวินาศภัย: ตรวจสอบและอนุมัติแผนงานกู้คืนระบบ
ดูแลกระบวนการ DRP: ควบคุมดูแลและบังคับใช้แผนงาน
ฝึกอบรม: ดำเนินการฝึกอบรมการใช้แผนงาน DRP
ประกาศเหตุการณ์: ประกาศเหตุการณ์วินาศภัยและกำหนดกลยุทธ์กู้คืนระบบ
เฝ้าดูและอัพเดทข้อมูล: ติดตามและอัปเดตสถานะการกู้คืนระบบแก่ฝ่ายบริหารและแผนกต่าง ๆ

ผู้จัดการฝ่ายปฏิบัติการและทีมกู้คืนระบบ



ป้องกันระบบ: พัฒนาและดูแลรักษาระบบ
คัดเลือกทีม: คัดเลือกบุคลากรในทีมและมอบหมายงาน
ฝึกอบรม: อบรมทีมงาน DRP เกี่ยวกับแผนงานและวิธีการปฏิบัติ
อนุมัติกู้คืนระบบ: ประกาศแจ้งและอนุมัติการกู้คืนระบบ
วิเคราะห์และประสานงาน: วิเคราะห์ระดับความรุนแรงของปัญหา และประสานงานกับทีมงาน

Facility Recovery Team

เตรียมสถานที่สำรอง: เตรียมสถานที่และอุปกรณ์สำหรับการสำรองข้อมูล

แผนปฏิบัติการ: จัดทำแผนปฏิบัติการและวิธีการกู้คืนระบบสำหรับ Site งานสำรอง

ซ่อมแซม Site งานหลัก: ดำเนินการซ่อมแซม Site งานหลักให้กลับคืนสู่ปกติ

ทีมงานกู้คืน Platform

ดูแลอุปกรณ์: ดูแลรักษารายการอุปกรณ์ที่เกี่ยวข้องกับกระบวนการกู้คืนระบบ

ติดตั้ง Hardware: ติดตั้งอุปกรณ์ Hardware หลังจากเกิดภัยพิบัติ

เรียกคืนข้อมูล: เรียกคืนข้อมูลและระบบจากสำเนาที่เก็บไว้

2. ประเมินและจัดลำดับความสำคัญของความเสี่ยง

จัดลำดับความสำคัญของระบบและบริการ โดยทำการกู้คืนตามลำดับความสำคัญของสินทรัพย์ เช่น แอปพลิเคชันที่ลูกค้าใช้งานอาจมีสำคัญมากกว่าสภาพแวดล้อมการพัฒนาผลิตภัณฑ์ขององค์กร ดังนั้น องค์กรจึงตัดสินใจทำการกู้คืนแอปพลิเคชันนี้ก่อนสภาพแวดล้อมการพัฒนาผลิตภัณฑ์

3. พัฒนาแผนและขั้นตอนการกู้คืน:

สร้างแผนการกู้คืนที่ระบุวิธีการทางเทคนิคการกู้คืนระบบโดยชัดเจน รวมถึงมาตรการบรรเทาผลกระทบของเหตุการณ์ทางไซเบอร์ที่เกิดขึ้น เช่น หยุดการทำงานบางส่วนของแอปพลิเคชัน เพื่อให้แอปกลับมาทำงานได้ ซึ่งแม้ว่าการทำงานของแอปพลิเคชันจะยังมีข้อจำกัด แต่ก็ช่วยลดผลกระทบจากภัยคุกคามจนสุดท้ายสามารถกู้คืนให้แอปกลับมาทำงานได้เป็นปกติอย่างสมบูรณ์ นอกจากนี้องค์กรควรมีระบบการสื่อสารสำรองในกรณีที่ระบบการสื่อสารปกติไม่สามารถใช้งานได้

4. ออกแบบและดำเนินการสำรองข้อมูล:

ตรวจสอบให้แน่ใจว่าองค์กรมีข้อมูลสำรองสำหรับการกู้คืนระบบ หลังจากนั้น เลือกข้อมูลที่จะทำการกู้คืน และตั้งเป้าหมายต่าง ๆ ในการกู้คืน ซึ่งเป้าหมายในการกู้คืนมีด้วยกัน 2 แบบคือ Recovery Time Objective (RTO) ซึ่งแปลว่าเวลาที่องค์กรสามารถรอได้จนกว่าระบบจะกลับมาทำงานได้เป็นปกติ ตัวอย่าง ถ้าหากองค์กรกำหนด RTO ไว้ 4 ชั่วโมง แล้วเหตุการณ์ภัยพิบัติเกิดขึ้นตอนเที่ยงวัน แปลว่าระบบต้องกู้คืนและสามารถทำงานได้เป็นปกติในเวลา 4 โมงเย็น และ Recovery Point Objective (RPO) คือปริมาณการสูญเสียข้อมูลที่องค์กรยอมรับได้จากภัยพิบัติ หรือความถี่ในการสำรองข้อมูล ตัวอย่าง RPO ของการสำรองข้อมูลธุรกรรมในธุรกิจธนาคารคือ 0 เนื่องจากข้อมูลเหล่านี้ มีความสำคัญมาก ๆ จนต้องมีการสำรองข้อมูลอยู่ตลอดเวลา ไม่มีการหยุด ส่วน RPO ของการสำรองข้อมูลโค้ดสำหรับพัฒนาซอฟต์แวร์คือ 24 ชั่วโมง นั่นหมายความว่าโค้ดต้องมีการสำรองข้อมูลทุก 24 ชั่วโมง ความถี่ในการสำรองนี้ช้ากว่าการสำรองในเรื่องอื่น ๆ เพราะด้วยการเขียนโค้ดใหม่เป็นเรื่องไม่ยาก

5. ทดสอบและปรับแผนการกู้คืน:

ทดสอบแผนการกู้คืน เพื่อให้แน่ใจว่าแผนสามารถนำไปปฏิบัติได้ตามที่วางเอาไว้ นอกจากนี้ การทดสอบช่วยให้ทีมระบุข้อบกพร่องของตัวแผนหรือทางบุคลากรผู้ดำเนินแผน เพื่อที่จะสามารถรับมือกับเหตุการณ์ได้อย่างถูกต้องและทันทีเมื่อเกิดเหตุภัยพิบัติ

การสำรองข้อมูล (Backup)

ประเภทการสำรองข้อมูลกู้คืน:

การสำรองข้อมูลแบบเต็ม (Full Backup)

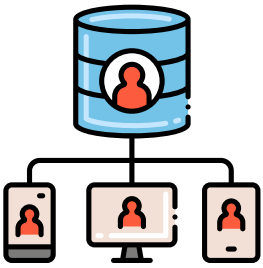
การสำรองไฟล์ข้อมูลทั้งหมดลงในสื่อจัดเก็บข้อมูล ซึ่งช่วยให้การกู้คืนข้อมูลทำได้ง่าย เพียงแค่ถ่ายโอนข้อมูลทั้งหมดที่สำรองไว้ ไปยังอุปกรณ์ที่ต้องการ แต่การทำเช่นนี้ใช้เวลาในการถ่ายโอนข้อมูลค่อนข้างนาน และใช้พื้นที่เก็บข้อมูลในระบบเป็นจำนวนมาก เนื่องจากเป็นการสำรองข้อมูลทั้งหมดในแต่ละครั้งโดยที่มีการทบข้อมูลเก่าซ้ำไปเรื่อย ๆ

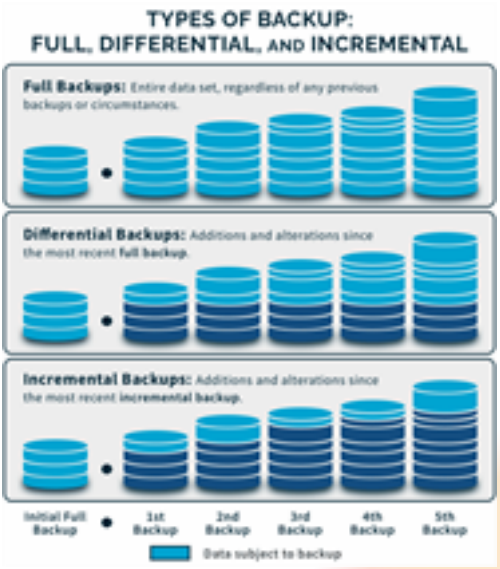
การสำรองข้อมูลส่วนเพิ่ม (Incremental Backup)

การสำรองเฉพาะไฟล์ข้อมูลที่มีการเปลี่ยนแปลงหลังจากทำการสำรองในแต่ละครั้ง เช่น การเพิ่มหรือการแก้ไขของข้อมูล ตัวอย่างเช่น องค์กรทำการสำรองข้อมูลแบบเต็ม (Full Backup) ในวันจันทร์ ส่วนในวันอังคาร องคกร์สำรองข้อมูลเฉพาะในส่วนที่เปลี่ยนแปลงจากวันจันทร์ ต่อมาในวันพุธ องค์กรสำรองข้อมูลเฉพาะส่วนที่เปลี่ยนแปลงจากวันอังคาร และทำเป็นลักษณะเช่นนี้ไปเรื่อย ๆ การสำรองข้อมูลด้วยวิธีนี้ ใช้เวลาไม่นาน และไม่เปลืองพื้นที่จัดเก็บ แต่วิธีการในการกู้คืนข้อมูลทำได้ยาก เนื่องจากในกรณีที่การสำรองข้อมูลส่วนใดส่วนหนึ่งหรือวันใดวันหนึ่งหายไป จำเป็นต้องทำการค้นหาไฟล์ข้อมูลของวันอื่น เพื่อมาทำการทดแทนไฟล์ข้อมูลของวันที่หายไปซึ่งมีกระบวนการที่ซับซ้อน

การสำรองข้อมูลที่แตกต่างกัน (Differential Backup)

การสำรองไฟล์ข้อมูลที่มีการเปลี่ยนแปลงหลังจากการสำรองข้อมูลแบบเต็ม ยกตัวอย่าง ทางองค์กรได้ทำการสำรองข้อมูลแบบเต็มในวันจันทร์ พอถึงวันอังคารทางองค์กรได้สำรองข้อมูลเฉพาะส่วนที่มีการเปลี่ยนแปลงจากวันจันทร์ ถัดไปเป็นวันพุธ ทางองค์กรได้ทำการสำรองข้อมูลในส่วนที่เปลี่ยนแปลงจากวันอังคาร รวมทั้งของวันอังคารด้วยเช่นกัน ต่อมาในวันพฤหัส องค์กรได้สำรองข้อมูลในส่วนที่มีการเปลี่ยนแปลงจากวันพุธ รวมถึงของวันอังคารและพุธด้วย และทำเป็นลักษณะเช่นนี้ไปเรื่อย ๆ การสำรองข้อมูลด้วยวิธีนี้มีความเร็วและการใช้เนื้อที่อยู่ตรงกลางระหว่างการสำรองข้อมูลแบบเต็มและการสำรองข้อมูลส่วนเพิ่ม (Incremental Backup)





ประเภทของการสำรองข้อมูล
หมายเหตุ: จุดที่เป็นสีฟ้าอ่อนคือข้อมูลที่ถูกสำรอง

ที่มา: https://spanning.com/blog/types-of-backup-understanding-full-differential-incremental-backup/

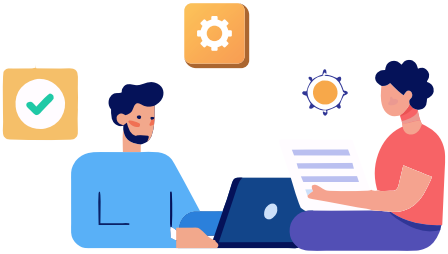
การเลือกประเภทการสำรองข้อมูลที่เหมาะสม

การเลือกใช้รูปแบบการสำรองข้อมูลขึ้นอยู่กับปริมาณของข้อมูลที่ต้องการสำรอง สำหรับองค์กรขนาดเล็กที่ปกติมีการเก็บข้อมูลในปริมาณไม่มากสามารถใช้รูปแบบการสำรองข้อมูลแบบเต็มในทุก ๆ วัน ส่วนองค์กรขนาดใหญ่ที่มีปริมาณข้อมูลเป็นจำนวนมากสามารถเริ่มต้นครั้งแรกด้วยการสำรองข้อมูลแบบเต็ม และหลังจากนั้นสามารถเลือกต่อได้ว่าจะสำรองข้อมูลแบบการสำรองข้อมูลส่วนเพิ่มหรือการสำรองข้อมูลที่แตกต่างกัน (Differential Backup)

กลยุทธ์การสำรองข้อมูล : การปรับใช้ 3-2-1 Backup ในยุคสมัยที่เปลี่ยนไป

3-2-1 เป็นกลยุทธ์การสำรองข้อมูลที่มีเงื่อนไขว่าให้มีข้อมูลทั้งหมด 3 ชุดด้วยกัน ประกอบด้วยชุดข้อมูลไฟล์ต้นฉบับและอีก 2 ชุดข้อมูลสำรอง โดยต้องเก็บในสื่อเก็บข้อมูล 2 แบบที่ไม่เหมือนกัน และมี 1 ชุดข้อมูลที่ต้องเก็บไว้แยกห่างจากแหล่งเก็บชุดข้อมูลอื่น (Off-site backup) ยกตัวอย่างองค์กรทำการเก็บไฟล์ข้อมูลต้นฉบับไว้ในอุปกรณ์คอมพิวเตอร์ขององค์กร ส่วนชุดข้อมูลสำรองอันแรกได้ถูกเก็บไว้ในฮาร์ดดิสก์ซึ่งอยู่คนละประเภทสื่อกับข้อมูลต้นฉบับ และสำหรับชุดข้อมูลสำรองสุดท้าย องค์กรควรเก็บชุดข้อมูลนี้ไว้ในที่ที่ห่างไกลจากชุดข้อมูลอื่นอย่างการเก็บไว้ในพื้นที่จัดเก็บข้อมูลคลาวด์

ถึงแม้ว่ากลยุทธ์การสำรองข้อมูล 3-2-1 Backup จะยังคงเป็นหลักการพื้นฐานของการสำรองข้อมูล แต่การปรับใช้กลยุทธ์นี้ตามยุคสมัยของเทคโนโลยีที่มีการเปลี่ยนแปลงเป็นสิ่งที่สำคัญยิ่ง ซึ่งอุปกรณ์สำรองข้อมูลร่วมสมัยที่รวมซอฟท์แวร์กับฮาร์ดแวร์เข้าด้วยกัน ทำให้การสำรองข้อมูลในครั้งแรก (Initial backups) ทำได้ง่ายขึ้น และสามารถเชื่อมต่อกับข้อมูลที่ถูกเก็บห่างออกไปที่อยู่ในระบบคลาวด์ องค์กรควรใช้วิธีการปกป้องข้อมูลอย่างต่อเนื่อง (Continuous Data Protection – CDP) และ การลดความซ้ำซ้อนของข้อมูล (Deduplication) โดยในขณะเดียวกันใช้บริหารจัดการและกู้คืนข้อมูล (Disaster Recovery as a Service – DRaaS) การใช้วิธีและบริการเหล่านี้ไม่เพียงแต่เป็นการทำให้ข้อมูลได้รับการปกป้องด้วยการสำรอง แต่ยังสามารถทำให้องค์กรรับมือกับการฟื้นฟูจากเหตุการณ์ภัยคุกคามต่าง ๆ

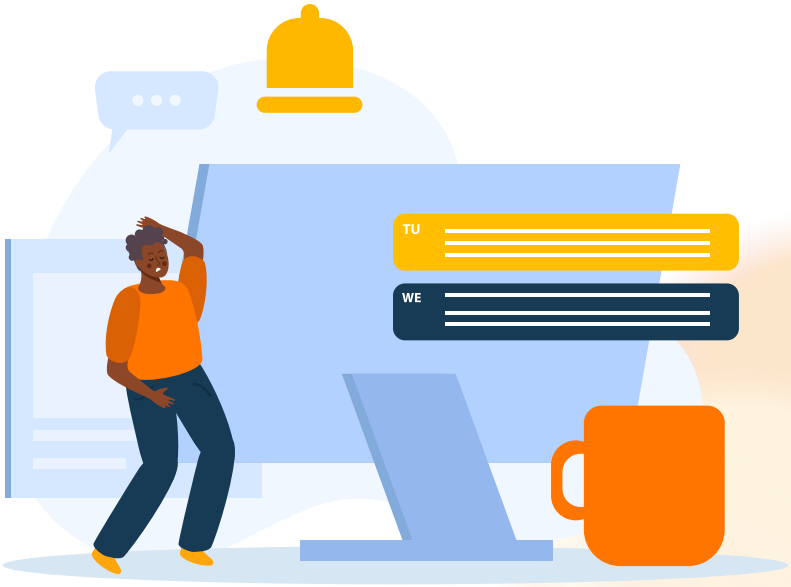


การปกป้องข้อมูลอย่างต่อเนื่อง (Continuous Data Protection – CDP) และการลดความซ้ำซ้อนของข้อมูล (Deduplication)

การปกป้องข้อมูลอย่างต่อเนื่อง เป็นระบบที่บันทึกทุกการเปลี่ยนของข้อมูล และสามารถกู้คืนข้อมูลจากจุดใดก็ได้ที่มีการเปลี่ยนแปลง ทำให้โอกาสการสูญเสียข้อมูลมีน้อยมาก การลดความซ้ำซ้อนของข้อมูล คือการนำข้อมูลที่เหมือนกันออก ซึ่งมีประโยชน์ให้องค์กรลดปริมาณของข้อมูลที่ต้องจัดเก็บและดูแล โดยสามารถลดค่าใช้จ่ายได้ด้วยเช่นกัน นอกจากนี้ยังทำให้การประมวลข้อมูลดีขึ้นและใช้พลังงานน้อยลง

บริการกู้คืนข้อมูล (Disaster Recovery as a Service – DRaaS)

บริการการสำรองและกู้คืนข้อมูลในระบบคลาวด์จากผู้ให้บริการอื่นนอกองค์กร (Third Party) ที่ช่วยให้องค์กรไม่ต้องลงทุนกับทรัพยากรทุกอย่าง และประหยัดค่าใช้จ่าย โดยการจ่ายเพียงเท่าที่ใช้บริการเท่านั้น



แนวทางปฏิบัติการสำรองข้อมูล

องค์กรต้องจัดให้มีนโยบายสำรองข้อมูลที่มีความสำคัญต่อการดำเนินงานขององค์กร รวมถึงระบบปฏิบัติการ (Operating System) แอปพลิเคชันระบบงานคอมพิวเตอร์ (Application System) และชุดคำสั่งที่นำมาใช้ปฏิบัติงานให้ครบถ้วน ที่สามารถพร้อมใช้งานได้อย่างต่อเนื่อง โดยขั้นต่ำ องค์กรควรพิจารณารายละเอียดดังนี้ ในการสำรองข้อมูลภายในองค์กร

1. กำหนดขั้นตอนปฏิบัติในการสำรองข้อมูล โดยอย่างน้อยต้องครอบคลุมรายละเอียดดังต่อไปนี้

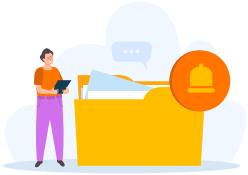
- ข้อมูลที่ต้องสำรอง
- ความถี่ในการสำรอง
- ประเภทสื่อบันทึกข้อมูล
- จำนวนที่ต้องสำรอง
- ขั้นตอนและวิธีการสำรองโดยละเอียด
- สถานที่และวิธีการเก็บรักษาสื่อบันทึกข้อมูล
- กระบวนการกู้คืนข้อมูลในกรณีที่สูญหาย

2. จัดเก็บสื่อบันทึกข้อมูลสำรอง

พร้อมทั้งสำเนาขั้นตอนปฏิบัติต่าง ๆ ไว้นอกสถานที่ เพื่อความปลอดภัยในกรณีที่สถานที่ปฏิบัติงานได้รับความเสียหาย โดยสถานที่ดังกล่าวต้องจัดให้มีระบบควบคุมการเข้าออกและระบบป้องกันความเสียหาย

3. กำหนดเป้าหมายในการกู้คืนข้อมูล

เช่น กำหนดประเภทของข้อมูล และชุดข้อมูลล่าสุดที่สามารถกู้คืนได้ (Recovery Point Objective - RPO)



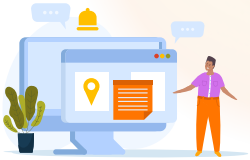
4. จัดให้มีการทดสอบข้อมูลสำรองและกระบวนการกู้คืนข้อมูลอย่างน้อยปีละ 1 ครั้ง

(ระยะเวลาดังกล่าวเปลี่ยนแปลงได้ตามบริบทและการจัดลำดับความสำคัญขององค์กร) เพื่อทดสอบว่า ข้อมูลรวมทั้งโปรแกรมระบบต่าง ๆ ที่ได้สำรองไว้ มีความถูกต้องครบถ้วนและสามารถใช้งานได้

5. ในกรณีองค์กรมีความจำเป็นต้องจัดเก็บข้อมูลเป็นระยะเวลานาน

ต้องคำนึงวิธีการที่จะสามารถนำข้อมูลกลับมาใช้งานได้ ยกตัวอย่าง ให้องค์กรเตรียมอุปกรณ์และโปรแกรมที่ใช้อ่านสื่อบันทึกประเภทนั้นของข้อมูลที่มีการเก็บไว้

แหล่งการกู้คืนจากภัยพิบัติ (Disaster Recovery Sites)



แหล่งการกู้คืนจากภัยพิบัติ (Disaster Recovery Sites) คือสถานที่ที่ทำการกู้คืนระบบหรือแหล่งที่ทดแทนสถานที่เก็บข้อมูลต้นฉบับ (Secondary site) ในระหว่างที่แหล่งเก็บข้อมูลต้นฉบับ (Primary site) ได้รับความเสียหาย โดยแหล่งกู้คืนภัยพิบัติสามารถแบ่งประเภทได้ตามนี้

Hot site

เป็นสถานที่กู้คืนภัยพิบัติที่มีสิ่งอำนวยความสะดวกครบถ้วนไม่ว่าจะเป็น ข้อมูล ฮาร์ดแวร์ ซอฟต์แวร์ การเชื่อมต่อระบบเครือค่าย และบุคลากร ซึ่งมีความเพียบพร้อมใกล้เคียงกับแหล่งเก็บข้อมูลต้นฉบับ โดยที่แหล่งนี้สามารถทำการกู้คืนข้อมูลจากภัยพิบัติได้อย่างรวดเร็วและโดยทันที สถานที่ตั้ง Hot site ควรมีระยะห่างจากพื้นที่เก็บข้อมูลต้นฉบับ เพื่อป้องกันการเกิดเหตุภัยพิบัติเช่นเดียวกันกับแหล่งเก็บข้อมูลต้นฉบับ

Cold site

เป็นสถานที่กู้คืนภัยพิบัติที่มีเพียงสิ่งอำนวยความสะดวกที่จำกัด โดยจะได้รับเทคโนโลยีที่ใช้สำหรับการกู้คืนแบบสมบูรณ์ก็ต่อเมื่อแผนการฟื้นฟูภัยพิบัติได้เริ่มดำเนินการ และได้มีการติดตั้งอุปกรณ์ที่ใช้สำหรับการกู้คืน การมีสิ่งอำนวยความสะดวกที่จำกัด ทำให้ระยะเวลาในการกู้คืนยาวนานมากเมื่อเทียบกับ Hot site

Warm site

มีคุณสมบัติของสถานที่อยู่ตรงกลางระหว่าง Hot site และ Cold site โดยมีสิ่งอำนวยความสะดวกสำหรับการกู้คืนภัยพิบัติในปริมาณหนึ่ง และใช้ระยะเวลาในการกู้คืนเร็วกว่า Cold site แต่ไม่เร็วเท่า Hot site ซึ่งแน่นอนว่า การทำงานของ Warm site ก็ยังไม่สามารถเทียบเท่าการทำงานของแหล่งเก็บข้อมูลต้นฉบับ ดังเช่น Hot site

ปัจจัยที่ส่งผลต่อการเลือกประเภทแหล่งการกู้คืนภัยพิบัติ

เวลา (Time)

องค์กรต้องกำหนดระยะเวลาการกู้คืนที่ยอมรับได้ หรือ Recovery Time Objective (RTO) และปริมาณการสูญหายของข้อมูลที่ยอมรับได้ หรือ Recovery Point Objective (RPO) เพื่อช่วยในการตัดสินว่า จะเลือกแหล่งการกู้คืนข้อมูลประเภทใด โดยพิจารณาจากระยะเวลาและความสามารถในการกู้คืนข้อมูลของแต่ละแหล่ง เช่น

- องค์กรที่ตั้ง RTO กับ RPO ที่สั้น ควรเลือกแหล่งกู้คืนแบบ Hot Site ซึ่งมีความสามารถในการกู้คืนข้อมูลและสถานการณ์ได้เร็ว
- องค์กรที่ตั้ง RTO กับ RPO ที่ยาวเพียงเล็กน้อยสามารถเลือกแหล่งกู้คืนข้อมูลแบบ Warm Site
- RTO กับ RPO ที่ยาวนานสามารถเป็น Cold Site ได้

สิ่งที่สำคัญต่อธุรกิจหรือองค์กร (Business or Organization Priorities)

องค์กรสามารถระบุกระบวนการหรือกิจกรรมที่มีความสำคัญ และประเมินผลกระทบของการที่กระบวนการหรือกิจกรรมเหล่านั้นไม่สามารถดำเนินการได้ เช่น ถ้าหากความเสียหายจากการที่ระบบสารสนเทศขององค์กรล้มเหลวมีอยู่มาก และมีความสำคัญมากต่อการดำเนินงานขององค์กร ตัวอย่างเช่น

- ในด้านของรายได้ที่สูญเสียเป็นจำนวนมาก จากการไม่สามารถขายสินค้าให้กับลูกค้าได้ (ไม่สามารถทำธุรกรรมได้ เนื่องจากระบบเก็บข้อมูลธุรกรรมมีความเสียหาย) ทำให้องค์กรจำเป็นต้องใช้แหล่ง Hot Site ในการกู้คืนระบบและข้อมูล ให้กลับมาทำงานได้ปกติโดยเร็วที่สุด
- กิจกรรมการดำเนินงานที่ไม่สำคัญหรือไม่เร่งด่วนมาก สามารถใช้แหล่ง Cold Site ในการกู้คืนระบบและข้อมูลได้

งบประมาณ (Budget)

องค์กรควรมองว่าตัวองค์กรเองมีงบประมาณเท่าไหร่ เพียงพอต่อการเลือกแหล่งกู้คืนภัยพิบัติประเภทใด โดยที่ Hot Site จะมีราคาในการสร้างพื้นที่แพงที่สุด เนื่องจากต้องสร้างทรัพยากรเป็นจำนวนมากที่มีความเพรียบพร้อมสูง รองลงมาจะเป็น Warm Site จนถึงราคาต่ำที่สุดคือ Cold Site ซึ่งมีการสร้างทรัพยากรน้อยที่สุด นอกจากนี้ องค์กรควรคำนึงว่าค่าใช้จ่ายที่ได้จ่ายไปคุ้มค่ากับคุณค่าที่ได้รับหรือไม่ และตอบสนองต่อความต้องการขององค์กรหรือไม่

ตัวอย่าง ถึงแม้ว่าราคาของการสร้างแหล่งเก็บข้อมูล Cold site จะมีราคาที่ถูกที่สุด แต่หากองค์กรจะได้รับความเสียหายเป็นจำนวนมาก จากความล่าช้าในการกู้คืนระบบและข้อมูล ก็อาจไม่คุ้มค่ากับการที่องค์กรลงทุนเงินจำนวนน้อยในตอนแรกแต่สูญเสียเงินจำนวนมากในภายหลัง

การเลือกสถานที่ตั้งของแหล่งกู้คืนภัยพิบัติ

สถานที่เป็นองค์ประกอบสำคัญของการสร้างแหล่งกู้คืนภัยพิบัติ ซึ่งสถานที่ตั้งจะขึ้นอยู่กับ

- ระดับความสำคัญและความลับของข้อมูล
- งบประมานขององค์กรที่ถูกจัดสรรสำหรับการสร้างแหล่งกู้คืนภัยพิบัติ
- ประเภทของภัยพิบัติที่เกิดขึ้นในแต่ละพื้นที่

ในกรณีขององค์กรที่ตั้ง RTO ไว้สั้นเนื่องจากข้อมูลมีความสำคัญและไม่สามารถรอเวลาในการกู้คืนได้นาน องค์กรควรตั้งแหล่งการเก็บข้อมูลต้นฉบับและแหล่งที่ทดแทนสถานที่เก็บข้อมูลต้นฉบับให้อยู่ในบริเวณใกล้กัน เพื่อความเร็วและความสะดวกในการถ่ายโอนข้อมูล แต่การตั้งสถานที่เก็บข้อมูลต้นฉบับกับสถานที่กู้คืนข้อมูล ให้อยู่ใกล้กันก็มีความเสี่ยงหากมีภัยพิบัติรุนแรงเกิดขึ้นในบริเวณนั้น ทำให้สถานที่กู้คืนข้อมูลได้รับความเสียหายและไม่สามารถกู้คืนข้อมูลได้ในที่สุด นอกจากนี้เป็นกรณีศึกษา การที่องค์กรเลือกตั้งสถานที่กู้คืนข้อมูลห่างออกไปมากเนื่องด้วยราคาการจัดสร้างสถานที่ที่ถูกกว่า แต่หากคิดในอีกมุม การมีระยะห่างตรงนี้ทำให้การถ่ายโอนข้อมูลเพื่อกู้คืนภัยพิบัติใช้เวลานาน ซึ่งอาจส่งผลกระทบถึงการดำเนินงานขององค์กรที่สูญเสียรายได้จำนวนมาก และค่าใช้จ่ายที่เพิ่มขึ้นจากการที่ต้องจ้างพนักงานดูแลสถานที่กู้คืนข้อมูลที่อยู่ห่างไกล จึงทำให้ในที่สุดมูลค่าเงินที่ลงทุนไปเพียงไม่มากตั้งแต่ต้น ไม่คุ้มค่าต่อค่าใช้จ่ายพนักงานและรายได้ที่สูญเสียที่มีมูลค่าเป็นเงินจำนวนมาก

แผนการสื่อสารช่วงการกู้คืนภัยพิบัติ (Disaster Recovery Communication Plan)

แผนการสื่อสารสำหรับการกู้คืนจากภัยพิบัติเป็นสิ่งสำคัญ เพื่อให้ทุกคนได้รับข้อมูลทั้งในช่วงวิกฤตและหลังเกิดวิกฤต แผนนี้ระบุขั้นตอนในการสื่อสารกับพนักงาน เช่นการแนะนำให้หลีกเลี่ยงสถานที่เกิดเหตุหลังจากเกิดเหตุการณ์ และให้คำแนะนำในการทำงานจากระยะไกล แผนนี้ยังรวมถึงการสื่อสารภายนอก เช่น การรายงานข้อมูลแก่สื่อ ลูกค้า และผู้มีส่วนได้ส่วนเสีย และการแจ้งครอบครัวในกรณีที่มีผู้บาดเจ็บหรือเสียชีวิต การมีแผนนี้ ช่วยให้องค์กรสามารถรักษาความต่อเนื่อง และกลับสู่การดำเนินงานตามปกติได้อย่างมีประสิทธิภาพ

ทำการสำรองข้อมูล (Data Backups)

ข้อมูลถือได้ว่าเป็นทรัพย์สินทางสารสนเทศที่สำคัญมากที่สุด เพราะการที่ไม่มีข้อมูลหมายความว่าองค์กรไม่สามารถดำเนินกิจกรรมโดยปกติได้ จึงทำให้การสำรองข้อมูลเป็นประจำ เป็นเรื่องที่มองข้ามไม่ได้ ซึ่งการทำเช่นนี้ทำให้ข้อมูลได้รับการปกป้องจากความเสียหายหลักจากเกิดภัยพิบัติหรือภัยคุกคาม

สร้างทีมการสื่อสาร

การตั้งทีมรับมือภัยคุกคามทางไซเบอร์ล่วงหน้า ช่วยให้องค์กรเตรียมความพร้อมกับการรองรับเหตุการณ์อันไม่พึงประสงค์ทางไซเบอร์ ผู้บริหารระดับสูงและหัวหน้าแผนกเป็นตัวเลือกที่เหมาะสม สำหรับการเป็นสมาชิกในทีมกู้คืนภัยพิบัติ เนื่องจากเป็นบุคคลที่คุ้นเคยกับกระบวนการสำคัญในองค์กร และสามารถวางแผนห่วงโซ่การสื่อสารในกรณีเกิดเหตุภัยพิบัติได้

ห่วงโซ่การสื่อสารคือกระบวนการสื่อสารที่ระบุว่าข้อความจะส่งต่ออย่างไรถึงบุคคลหรือหน่วยงานใด บุคคลในทีมกู้คืนภัยพิบัติควรมอบหมายหน้าที่ การสื่อสารของตนให้กับบุคคลอื่นล่วงหน้า เพื่อในกรณีที่ไม่สามารถปฏิบัติหน้าที่ได้กระทันหัน

การเข้าใจความสำคัญของการรายงานสิ่งจำเป็นต่อผู้มีส่วนได้ส่วนเสีย

ในกรณีขององค์กรภาคธุรกิจ ในช่วงภัยพิบัติ การแจ้งให้ลูกค้าทราบถึงสถานการณ์ปัจจุบันและแผนการฟื้นตัวของธุรกิจเป็นสิ่งสำคัญยิ่ง พวกเขาจำเป็นต้องรู้ว่าธุรกิจจะยังคงให้บริการพวกเขาต่อไป ในขณะที่ตัวธุรกิจทำทุกอย่างเพื่อกลับเข้าสู่เหตุการณ์ปกติ หากธุรกิจไม่สร้างความมั่นใจให้กับลูกค้า ธุรกิจอาจสูญเสียลูกค้าให้กับคู่แข่ง ซึ่งอาจทำให้ความเสียหายของธุรกิจมีมากขึ้นเพิ่มเติมจากภัยพิบัติที่เกิดขึ้น

ผู้มีส่วนได้ส่วนเสียอื่น ๆ เช่น ผู้ขาย ซัพพลายเออร์ และพันธมิตรทางธุรกิจ ควรได้รับการแจ้งเตือนทันทีหากธุรกิจจำเป็นต้องเลื่อนการจัดส่งหรือเลื่อนโครงการอื่น ๆ ในช่วงที่ธุรกิจต้องฟื้นตัวจากภัยพิบัติ บางพันธมิตรอาจสามารถสนับสนุนหรือให้คำแนะนำเพื่อช่วยให้องค์กรฟื้นฟูธุรกิจจากภัยพิบัติได้สำเร็จ

การรักษาการติดต่อกับผู้มีส่วนได้ส่วนเสียภายนอกเป็นสิ่งสำคัญต่อแผนการกู้คืนจากภัยพิบัติ นอกจากนี้ มีหลายธุรกิจที่มีช่องทางสื่อสารสำรอง เช่น อินเทอร์เน็ต ดาวเทียม และบริการความต่อเนื่องทางธุรกิจอื่น ๆ เพื่อให้แน่ใจว่าระบบรองรับการสื่อสารออนไลน์ได้ในทุกสถานการณ์

การคิดค้นกลยุทธ์การสื่อสาร

วิธีสื่อสารข้อมูลเกี่ยวกับภัยพิบัติขึ้นอยู่กับกลุ่มเป้าหมายขององค์กร ซึ่งรวมถึงผู้บริหาร พนักงาน ลูกค้า ผู้จัดหาผู้ควบคุม สื่อ และประชาชนทั่วไป ตัวอย่างเช่น องค์กรสามารถเปิดเผยรายละเอียดเกี่ยวกับความเสียหายของทรัพย์สินและข้อมูลที่เกิดการสูญหายกับพนักงานซึ่งช่วยให้การกู้คืนเหตุการณ์เป็นไปได้ง่ายขึ้นและสำเร็จในที่สุด อย่างไรก็ตาม องค์กรควรแจ้งพนักงานเกี่ยวกับข้อมูลด้านความปลอดภัยของสถานที่ทำงานและข้อมูลที่พวกเขาสามารถเปิดเผยให้กับผู้อื่น

การสื่อสารภายนอก โดยเฉพาะกับสื่อและประชาชนทั่วไปอาจมีความซับซ้อนในกรณีที่เกิดเหตุการณ์อันร้ายแรงที่ไม่คาดคิด แต่การไม่ปิดบังข้อมูลจากสาธารณชนเป็นสิ่งสำคัญ ซึ่งไม่ได้หมายความว่าองค์กรต้องเปิดเผยข้อมูลทุกอย่าง ดังนั้นการมีความโปร่งใสเกี่ยวกับสถานการณ์และแผนการกู้คืนจากภัยพิบัติจะช่วยลดความกังวลของผู้มีส่วนได้ส่วนเสีย และทำให้องค์กรมีภาพลักษณ์ที่ดีในเรื่องของความซื่อสัตย์และความน่าเชื่อถือ

การรวมข้อความสื่อสารเป็นหนึ่งเดียว

ก่อนที่จะแบ่งปันข้อมูลเกี่ยวกับภัยพิบัติให้กับใคร องค์กรควรใช้เวลาประเมินสถานการณ์และพัฒนาข้อความที่เป็นหนึ่งเดียวเกี่ยวกับแผนการกู้คืนขององค์กร ทุกคนในองค์กรต้องสื่อสารไปในทิศทางเดียวกัน นี่ไม่เพียงแต่จะทำให้องค์กรดูมีน่าเชื่อถือและพร้อมรับมือกับความท้าทายต่าง ๆ แต่ยังช่วยหลีกเลี่ยงการส่งสัญญาณที่สับสน โดยเฉพาะในสื่อโซเชียลมีเดีย

เมื่อสร้างข้อความที่เป็นหนึ่งเดียวได้เรียบร้อยแล้ว องค์กรควรพิจารณาสร้าง “ระดับ” บุคคลตามความจำเป็นของบุคคลนั้นในการรับรู้ข้อมูล ตัวอย่างเช่น ผู้บริหารระดับสูงจำเป็นต้องรู้ข้อมูลมากที่สุดเกี่ยวกับสถานการณ์ ตามด้วยพนักงานที่เหลือ และต่อด้วยพันธมิตรทางธุรกิจตามลำดับ ในสถานการณ์ส่วนใหญ่ สื่อควรได้รับรายละเอียดที่จำเป็นเท่านั้น เช่น การปิดทำการหรือความเสียหายที่เกิดขึ้นกับพื้นที่ตั้งขององค์กรโดยผ่านการแถลงข่าวอย่างเป็นทางการ

การทดสอบแผนการสื่อสาร

หลังจากที่องค์กรได้สร้างแผนการสื่อสารสำหรับการกู้คืนจากภัยพิบัติ และจัดตั้งทีมที่พร้อมดำเนินงานตามกลยุทธ์ที่วางเอาไว้ จึงถึงขั้นตอนการทดสอบแผนขององค์กร เพื่อให้องค์กรคุ้นเคยกับกระบวนการในแผนเมื่อมีภัยเกิดขึ้นจริง

การทดสอบแผนการกู้คืนจากภัยพิบัติหรือภัยคุกคามอย่างสม่ำเสมอ ช่วยให้องค์กรสามารถระบุปัญหา และปรับปรุงเพื่อให้มั่นใจว่าแผนมีประสิทธิภาพ ตัวอย่าง องค์กรอาจพบว่าการให้หัวหน้าแผนกติดต่อสมาชิกทีมของพวกเขา มีประสิทธิภาพกว่าการให้บุคคลทั่วไปในทีมติดต่อ เป็นต้น

ขั้นตอนปฏิบัติสำหรับการสื่อสารไปยังผู้ที่เกี่ยวข้อง

การสื่อสารไปยังผู้ที่เกี่ยวข้องในทุกระดับ มีความสำคัญอย่างยิ่งต่อการกู้คืนระบบสารสนเทศ ทั้งนี้ เพื่อให้ผู้ที่เกี่ยวข้องได้รับทราบถึงความคืบหน้าของสถานการณ์ วิธีการสื่อสารที่เป็นพื้นฐานในช่วงที่กู้คืนเหตุการณ์คือ

โทรศัพท์ (ทั้งโทรศัพท์ธรรมดาและโทรศัพท์มือถือ)

อีเมล

แอปพลิเคชัน LINE

SMS

โดยจะเริ่มต้นใช้วิธีการสื่อสารเรียงตามลำดับในข้างต้นจากซ้ายไปขวา กรณีที่ใช้วิธีการในลำดับแรก ๆ ไม่ได้ จะเลื่อนลำดับลงมายังวิธีการในลำดับถัดไป

แนวทางในการสื่อสารที่ ต้องปฏิบัติตามในทุกครั้งที่มีการสื่อสารไปยังผู้ที่เกี่ยวข้อง:

- อยู่ในอาการที่สงบเมื่อทำการสื่อสารไปยังผู้ที่เกี่ยวข้อง
- หลีกเลี่ยงการสนทนาที่ยาวนานโดยไม่จำเป็น
- กรณีที่ติดต่อบุคคลตามที่กำหนดไว้ไม่ได้ ให้ดำเนินการดังนี้
    - กรณีมีผู้รับสายแทน ให้สอบถามว่ามีข้อมูลติดต่ออื่น ของบุคคลตามที่ต้องการหรือไม่
    - ทิ้งข้อความไว้เพื่อให้ติดต่อกลับตามเบอร์โทรศัพท์ที่ให้ไว้
    - กรณีมีผู้รับสายแทน ไม่ควรให้รายละเอียดของเหตุการณ์หยุดชะงักที่เกิดขึ้น

บันทึกข้อมูลที่เกี่ยวข้องกับการติดต่อนั้น ได้แก่ เวลาที่ทำการติดต่อได้รับการตอบกลับหรือไม่ และสิ่งที่ได้ดำเนินการจากการติดต่อนั้น

สรุปท้ายบท Chapter 9

การกู้คืนทรัพย์สินและการดำเนินงาน

กระบวนการสำคัญในการกู้คืนระบบสารสนเทศหลังเกิดภัยพิบัติ โดยมุ่งเน้นที่การฟื้นฟูระบบและข้อมูล ให้กลับมาใช้งานได้ตามปกติอย่างรวดเร็ว เพื่อรักษาความต่อเนื่องในการดำเนินธุรกิจขององค์กร ซึ่งกระบวนการกู้คืนนี้ ประกอบด้วยหลายขั้นตอน เช่น การประเมินความเสียหาย การวางแผนฟื้นฟู และการทดสอบแผนฟื้นฟู นอกจากนี้ยังกล่าวถึงการสำรองข้อมูล (Backup) ที่เป็นส่วนสำคัญในการป้องกันข้อมูลสูญหาย และการจัดเตรียมแหล่งกู้คืนภัยพิบัติ (Disaster Recovery Sites) เพื่อให้สามารถฟื้นฟูระบบได้อย่างรวดเร็วและมีประสิทธิภาพ

แผนฟื้นฟูภัยพิบัติ (Disaster Recovery Plan - DRP) ถูกเน้นถึงความสำคัญในการเตรียมความพร้อม และการฝึกซ้อมอย่างสม่ำเสมอ เพื่อให้แน่ใจว่า เมื่อเกิดเหตุการณ์ไม่คาดฝัน องค์กรจะสามารถดำเนินการตามแผนได้อย่างมีประสิทธิภาพ นอกจากนี้ยังมีการกล่าวถึง การสื่อสารในช่วงกู้คืนภัยพิบัติ (Disaster Recovery Communication Plan) ซึ่งเป็นส่วนสำคัญในการแจ้งเตือนและประสานงานระหว่างทีมงาน เพื่อให้กระบวนการกู้คืนเป็นไปอย่างราบรื่นและไม่เกิดความสับสนในช่วงเวลาวิกฤต

MODULE 06

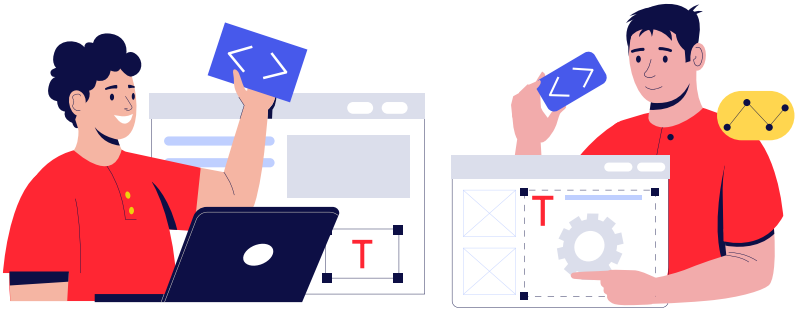
การกำกับดูแล ความมั่นคงปลอดภัยสารสนเทศ

(Information Security Governance) #Govern

วัตถุประสงค์

เพื่อให้ผู้เข้ารับการฝึกอบรมมีความรู้ความเข้าใจเกี่ยวกับการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ สามารถระบุและประเมินความเสี่ยง วิเคราะห์และเลือกใช้กลยุทธ์การจัดการความเสี่ยงที่เหมาะสม รวมถึงสามารถนำมาตรการควบคุมต่าง ๆ ไปใช้ในการป้องกันและลดความเสี่ยงได้อย่างมีประสิทธิภาพ

CHAPTER
10
การนำกลยุทธ์การลดความเสี่ยงไปใช้



กลยุทธ์การลดความเสี่ยง (Risk Mitigation)

การลดความเสี่ยงเป็นกระบวนการที่สำคัญในการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ โดยกลยุทธ์การลดความเสี่ยงคือการนำมาตรการและวิธีการต่าง ๆ มาใช้เพื่อลดความเสี่ยงที่เกิดขึ้นกับองค์กรให้อยู่ในระดับที่ยอมรับได้ โดยมุ่งเน้นที่การลดความน่าจะเป็นของการเกิดเหตุการณ์ที่ไม่พึงประสงค์ หรือการลดผลกระทบที่เกิดจากเหตุการณ์เหล่านั้น

ปัจจัยในการเลือกวิธีการบริหารจัดการความเสี่ยง

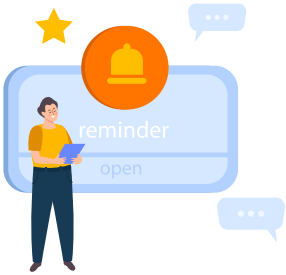
การลดความเสี่ยง สามารถทำได้โดยการจัดให้มีกิจกรรมการควบคุมเพื่อลดความถี่ในการเกิด หรือลดผลกระทบจากความเสี่ยงที่อาจเกิดขึ้น โดยอาจทำได้ใน 2 รูปแบบ คือ แบบที่ 1 กำหนดให้มีการบริหารและจัดการความเสี่ยงอย่างรัดกุม และแบบที่ 2 มีกิจกรรมการควบคุมเพื่อลดโอกาสเกิดหรือผลกระทบจากความเสี่ยงนั้น ๆ นอกจากนี้ยังอาจรวมถึงกิจกรรมอื่น ๆ ในการลดความเสี่ยง เช่น การกำกับดูแลและบริหารจัดการเทคโนโลยีสารสนเทศที่เหมาะสม และการปรับใช้มาตรฐานต่าง ๆ ในการบริหารจัดการทางด้านเทคโนโลยีสารสนเทศ โดยปัจจัยในการเลือกวิธีการบริหารจัดการความเสี่ยงที่เหมาะสม อาจประกอบด้วย

1. **ระดับความสำคัญของโอกาสเกิดและผลกระทบจากความเสี่ยง** ซึ่งแสดงในแผนภาพความเสี่ยง
2. **ประสิทธิผลของการจัดการความเสี่ยง** คือการเปรียบเทียบประโยชน์ที่จะได้รับจากกิจกรรมเพื่อจัดการความเสี่ยงในแบบต่าง ๆ กับต้นทุนที่ต้องใช้เพื่อจัดให้มีกิจกรรมเพื่อจัดการความเสี่ยงนั้น ๆ
3. **ความสามารถของผู้ประกอบธุรกิจ** ในการดำเนินกิจกรรมเพื่อจัดการกับความเสี่ยง อาทิ ผู้ประกอบธุรกิจที่มีความเชี่ยวชาญในการบริหารและจัดการความเสี่ยงย่อมสามารถดำเนินกิจกรรมเพื่อจัดการความเสี่ยงที่ซับซ้อนได้มีประสิทธิภาพกว่าผู้ประกอบธุรกิจที่ยังไม่มีประสบการณ์
4. **ประสิทธิผลของกิจกรรม** หรือการควบคุมเพื่อจัดการความเสี่ยง หรือความสามารถของกิจกรรมหรือการควบคุมในการลดโอกาสเกิดหรือลดผลกระทบจากความเสี่ยงที่อาจเกิดขึ้น

วิธีการวางกลยุทธ์การลดความเสี่ยง

จากเหตุการณ์ความเสี่ยงที่ระบุไว้ ผู้ประกอบธุรกิจควรมีกระบวนการในการประเมินความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ เพื่อประเมินระดับความสำคัญโดยผู้ประกอบธุรกิจควรดำเนินการโดยมีขั้นตอนดังนี้

ประเมินโอกาสเกิดและผลกระทบ



พิจารณาโอกาสและผลกระทบ ทั้งด้านบวกและด้านลบของแต่ละเหตุการณ์ความเสี่ยง ผลการประเมินควรนำเสนอในรูปแบบของแผนภาพความเสี่ยง (Risk Map) ซึ่งแสดงระดับของโอกาสเกิดและผลกระทบ (Risk Scale) ของแต่ละเหตุการณ์ความเสี่ยง

จัดทำทะเบียนความเสี่ยง (Risk Register) ที่ระบุรายละเอียดของความเสี่ยงที่ตรวจพบ

ตัวอย่างทะเบียนความเสี่ยง

ทะเบียนความเสี่ยง	
ส่วนที่ 1 ข้อมูลทั่วไป	
ชื่อความเสี่ยง	
เจ้าของความเสี่ยง	
วันที่ประเมิน	
วันที่ปรับปรุง	
ประเภทของความเสี่ยง	ขาดโอกาสการใช้เทคโนโลยีสารสนเทศให้เกิดประสิทธิภาพ และ ประสิทธิผล / การพัฒนาบริการหรือผลิตภัณฑ์ใหม่ / การปฏิบัติงานประจำวันด้านเทคโนโลยีสารสนเทศ
ระดับความสำคัญ	ต่ำ / ค่อนข้างต่ำ / ค่อนข้างสูง / สูง
ส่วนที่ 2 เหตุการณ์ความเสี่ยง	
ผู้กระทำให้เกิดความเสี่ยง	
ประเภทของความเสี่ยงหรือภัยคุกคาม	
เหตุการณ์ที่อาจเกิดขึ้น	
สินทรัพย์หรือทรัพยากรที่เกี่ยวข้อง	
ช่วงเวลาที่อาจก่อให้เกิด	
ส่วนที่ 3 ผลการวิเคราะห์ความเสี่ยง	
ระดับของโอกาสเกิด	ต่ำ / ค่อนข้างต่ำ / ค่อนข้างสูง / สูง
คำอธิบายโอกาสเกิด	
ระดับของผลกระทบ โดยพิจารณาถึง 1. ผลกระทบกับการดำเนินงาน 2. ต้นทุนการตอบสนองต่อความเสี่ยง 3. ความสามารถในการแข่งขัน 4. การปฏิบัติตามระเบียบข้อบังคับ	ต่ำ / ค่อนข้างต่ำ / ค่อนข้างสูง / สูง
คำอธิบายผลกระทบ	
ส่วนที่ 4 การตอบสนองต่อความเสี่ยง	
การตอบสนองต่อความเสี่ยง	หลีกเลี่ยง / ยอมรับ / ร่วมจัดการ / ลด
รายละเอียดเพื่อประกอบการประเมินการตอบสนอง	1. xxxxx, สถานการณ์การจัดให้มีการควบคุมในปัจจุบัน สถานการณ์ดำเนินงานกิจกรรมการควบคุมเพิ่มเติม 2. xxxxx, สถานการณ์การจัดให้มีการควบคุมในปัจจุบัน สถานการณ์ดำเนินงานกิจกรรมการควบคุมเพิ่มเติม
รายละเอียดวิธีการตอบสนองความเสี่ยง	
สถานะของการดำเนินงานเพื่อการตอบสนองต่อความเสี่ยง	
ปัญหาที่สำคัญในการดำเนินงาน	
ส่วนที่ 5 ตัวชี้วัดความเสี่ยง	
ตัวชี้วัดความเสี่ยง	1. ...

จัดทำโครงร่างของความเสี่ยง (Risk Profile)

รวบรวมข้อมูลความเสี่ยงทั้งหมดและแสดงสถานะปัจจุบันของความเสี่ยง การประเมินควรครอบคลุมทุกปัจจัยที่เกี่ยวข้อง พร้อมกำหนดตัวควบคุม และระบุความเสี่ยงที่ยังเหลืออยู่หลังการควบคุม

เปรียบเทียบความเสี่ยงกับระดับความเสี่ยงที่องค์กรยอมรับได้

ถ้าความเสี่ยงยังเกินระดับที่องค์กรยอมรับได้ ควรมีการกำหนดวิธีการจัดการเพื่อลดความเสี่ยงนั้นให้อยู่ในระดับที่ยอมรับได้

วิเคราะห์ต้นทุนและประโยชน์จากการจัดการความเสี่ยง

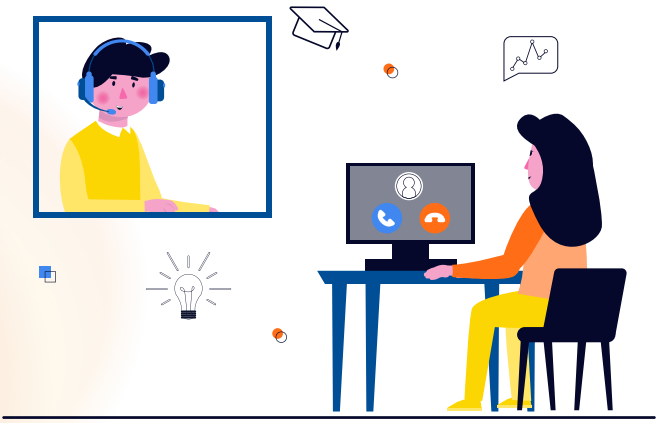
ประเมินต้นทุนและผลประโยชน์ที่จะได้รับจากวิธีการจัดการความเสี่ยงในแต่ละรูปแบบเพื่อเลือกวิธีการที่คุ้มค่าและเหมาะสมที่สุด

ระบุความต้องการของโครงการหรือระบบงาน

ระบุความเสี่ยงและความคาดหวังจากการควบคุมหลักที่ใช้ในการลดความเสี่ยงเพื่อให้สอดคล้องกับความต้องการของโครงการหรือระบบงานนั้น ๆ

ประเมินผลการวิเคราะห์ความเสี่ยงก่อนการตัดสินใจดำเนินการ

ทำการประเมินผลการวิเคราะห์ความเสี่ยงก่อนการตัดสินใจดำเนินการบริหารและจัดการความเสี่ยง เพื่อให้มั่นใจว่า การวิเคราะห์นั้นสอดคล้องกับความต้องการขององค์กรและมีความเหมาะสมและสมเหตุสมผล



การทำประกันภัย (Insurance)

การทำประกันภัย เป็นการถ่ายโอนความเสี่ยงไปยังบริษัทประกันภัยในกรณีที่เกิดเหตุการณ์ไม่คาดฝัน ซึ่งจะช่วยลดผลกระทบทางการเงินต่อองค์กร ประเภทของประกันภัยที่ควรพิจารณา ได้แก่

ประกันภัยทรัพย์สิน (Property Insurance): คุ้มครองทรัพย์สินขององค์กรจากความเสียหายหรือการสูญเสียที่เกิดจากภัยพิบัติ เช่น ไฟไหม้ น้ำท่วม และการโจรกรรม

ประกันภัยความรับผิดชอบ (Liability Insurance): คุ้มครององค์กรจากความรับผิดชอบทางกฎหมายที่อาจเกิดขึ้นจากเหตุการณ์ต่าง ๆ เช่น การรั่วไหลของข้อมูลส่วนบุคคล การถูกฟ้องร้องจากบุคคลที่สาม และความเสียหายต่อชื่อเสียง

ประกันภัยไซเบอร์ (Cyber Insurance): คุ้มครองความเสียหายทางการเงินที่เกิดจากการโจมตีทางไซเบอร์และการรั่วไหลของข้อมูล เช่น ค่าใช้จ่ายในการกู้คืนระบบ ค่าใช้จ่ายทางกฎหมาย และค่าปรับจากหน่วยงานกำกับดูแล

การฝึกอบรมและสร้างความตระหนัก (Training and Awareness)

การฝึกอบรมและสร้างความตระหนักเป็นส่วนสำคัญในการป้องกันและลดความเสี่ยงจากภัยคุกคามทางสารสนเทศ การฝึกอบรมควรครอบคลุมหัวข้อต่าง ๆ ดังนี้

ความรู้พื้นฐานเกี่ยวกับความมั่นคงปลอดภัยสารสนเทศ: การให้ความรู้เกี่ยวกับหลักการและแนวปฏิบัติที่ดีในการป้องกันภัยคุกคามทางสารสนเทศ

การป้องกันการโจมตีทางไซเบอร์: การฝึกอบรมเกี่ยวกับการป้องกันการโจมตีทางไซเบอร์ เช่น ฟิชชิง (Phishing), มัลแวร์ (Malware), และการโจมตีแบบวิศวกรรมสังคม (Social Engineering)

การจัดการข้อมูลส่วนบุคคล: การให้ความรู้เกี่ยวกับการจัดการและปกป้องข้อมูลส่วนบุคคลตามข้อกำหนดของกฎหมายและระเบียบที่เกี่ยวข้อง

การตอบสนองต่อเหตุการณ์ฉุกเฉิน: การฝึกซ้อมสถานการณ์ฉุกเฉินและการตอบสนองต่อเหตุการณ์ไม่คาดฝัน เช่น การรั่วไหลของข้อมูล การโจมตีทางไซเบอร์ และการหยุดชะงักของระบบสารสนเทศ

การควบคุมความเสี่ยง (Risk Control)

การควบคุมความเสี่ยงคือกระบวนการและกิจกรรมที่ใช้เพื่อลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ การควบคุมเหล่านี้ถูกออกแบบมาเพื่อป้องกัน ตรวจจับ และแก้ไขเหตุการณ์ที่อาจก่อให้เกิดความเสี่ยงต่อองค์กร

การควบคุมเชิงป้องกัน (Preventive Controls)

การควบคุมเชิงป้องกัน เป็นการดำเนินการเพื่อป้องกันไม่ให้เกิดเหตุการณ์ที่อาจก่อให้เกิดความเสี่ยง ตัวอย่างของการควบคุมเชิงป้องกัน ได้แก่

การใช้มาตรการควบคุมการเข้าถึง (Access Control):

รหัสผ่านที่ปลอดภัย: การบังคับให้พนักงานใช้รหัสผ่านที่มีความซับซ้อน เช่น ต้องมีตัวอักษรพิมพ์ใหญ่ พิมพ์เล็ก ตัวเลข และสัญลักษณ์

การยืนยันตัวตนแบบหลายขั้นตอน (Multi-factor Authentication): การใช้การยืนยันตัวตนเพิ่มเติม เช่น รหัสผ่านและรหัส OTP ที่ส่งไปยังโทรศัพท์มือถือ

การใช้ซอฟต์แวร์ป้องกันไวรัสและมัลแวร์ (Antivirus/Antimalware Software):

การติดตั้งซอฟต์แวร์ป้องกันไวรัส: การติดตั้งซอฟต์แวร์ป้องกันไวรัสในทุกเครื่องคอมพิวเตอร์และเซิร์ฟเวอร์ขององค์กร

การอัปเดตซอฟต์แวร์ป้องกันไวรัส: การตั้งค่าซอฟต์แวร์ป้องกันไวรัสให้ทำการอัปเดตฐานข้อมูลไวรัสอัตโนมัติ เพื่อป้องกันภัยคุกคามใหม่ ๆ

การควบคุมเชิงตรวจจับ (Detective Controls):

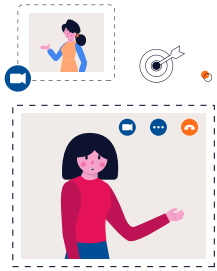
การควบคุมเชิงตรวจจับเป็นการดำเนินการเพื่อตรวจจับเหตุการณ์ที่อาจก่อให้เกิดความเสี่ยง ตัวอย่างของการควบคุมเชิงตรวจจับ ได้แก่

การตรวจสอบระบบ (System Monitoring):

การใช้ระบบ SIEM (Security Information and Event Management): การใช้ระบบ SIEM เพื่อรวบรวมและวิเคราะห์ข้อมูลจากหลากหลายแหล่ง เพื่อตรวจจับกิจกรรมที่น่าสงสัย

การติดตั้งอุปกรณ์ตรวจสอบเครือข่าย: การใช้เครื่องมือ เช่น Wireshark เพื่อตรวจสอบและวิเคราะห์ข้อมูลเครือข่าย

การบันทึกและตรวจสอบเหตุการณ์ (Event Logging and Monitoring)



การเก็บข้อมูลบันทึกการเข้าถึง (Access Logs): การบันทึกข้อมูลการเข้าถึงระบบและแอปพลิเคชันเพื่อใช้ในการตรวจสอบย้อนหลัง

การตรวจสอบเหตุการณ์แบบเรียลไทม์ (Real-time Monitoring): การตั้งค่าการแจ้งเตือนเมื่อเกิดเหตุการณ์ที่ผิดปกติ เช่น การพยายามเข้าสู่ระบบที่ไม่สำเร็จหลายครั้ง

การใช้ระบบตรวจจับการบุกรุก (Intrusion Detection System, IDS):

การติดตั้งระบบ IDS: การติดตั้งระบบ IDS เพื่อสแกนเครือข่ายและระบบคอมพิวเตอร์ เพื่อหากิจกรรมที่น่าสงสัย

การตั้งค่าการแจ้งเตือน (Alert Configuration): การตั้งค่าระบบ IDS ให้แจ้งเตือนเมื่อพบกิจกรรมที่อาจเป็นภัยคุกคาม

การควบคุมเชิงแก้ไข

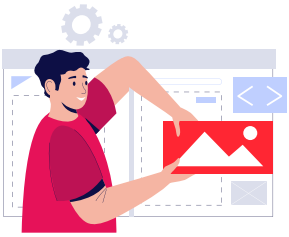
การควบคุมเชิงแก้ไขเป็นการดำเนินการเพื่อแก้ไขปัญหาที่เกิดขึ้นจากเหตุการณ์ที่ก่อให้เกิดความเสี่ยง ตัวอย่างของการควบคุมเชิงแก้ไข ได้แก่

การกู้คืนระบบ (System Recovery)

การสำรองข้อมูล (Backup): การสำรองข้อมูลระบบและข้อมูลสำคัญอย่างสม่ำเสมอ เพื่อให้สามารถกู้คืนข้อมูลได้ หากเกิดเหตุการณ์ที่ทำให้ข้อมูลสูญหาย

การวางแผนการกู้คืนระบบ (Disaster Recovery Plan): การจัดทำแผนการกู้คืนระบบ เพื่อให้สามารถกลับมาดำเนินการได้อย่างรวดเร็วหลังจากเกิดเหตุการณ์ที่ทำให้ระบบล้มเหลว

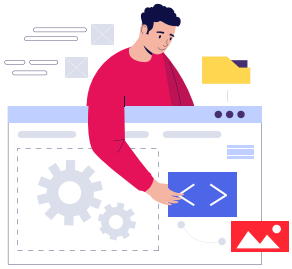
การปรับปรุงมาตรการความปลอดภัย (Security Updates):



การอัปเดตซอฟต์แวร์ (Software Patching): การอัปเดตและแก้ไขช่องโหว่ในซอฟต์แวร์ที่ใช้ในองค์กรอย่างสม่ำเสมอ

การเปลี่ยนแปลงการตั้งค่าระบบ (Configuration Changes): การปรับปรุงการตั้งค่าระบบ เพื่อเพิ่มความปลอดภัยหลังจากพบช่องโหว่

การวิเคราะห์เหตุการณ์ (Incident Analysis):



การตรวจสอบสาเหตุของเหตุการณ์ (Root Cause Analysis): การวิเคราะห์เหตุการณ์ที่เกิดขึ้น เพื่อหาสาเหตุที่แท้จริงและป้องกันไม่ให้เกิดขึ้นอีกในอนาคต

การปรับปรุงกระบวนการ (Process Improvement): การปรับปรุงกระบวนการและมาตรการควบคุมความเสี่ยงหลังจากการวิเคราะห์เหตุการณ์

มาตรการควบคุมด้านเทคนิค (Technical Controls)

มาตรการควบคุมด้านเทคนิคมุ่งเน้นไปที่การใช้เทคโนโลยีเพื่อป้องกัน ตรวจจับ และแก้ไขความเสี่ยงที่เกี่ยวข้องกับระบบและเครือข่าย

ไฟร์วอลล์ (Firewall):

ไฟร์วอลล์คือระบบที่ออกแบบมาเพื่อควบคุมการเข้าถึงเครือข่าย โดยทำหน้าที่ตรวจสอบและกรองข้อมูลที่ส่งผ่านเข้าและออกจากเครือข่าย เพื่อป้องกันการเข้าถึงที่ไม่พึงประสงค์ ตัวอย่างเช่น การตั้งค่าไฟร์วอลล์ให้บล็อกพอร์ตที่ไม่จำเป็น หรือการตั้งกฎการเข้าถึง (Access Control Rules) ที่เฉพาะเจาะจง

ระบบตรวจจับการบุกรุก (Intrusion Detection System, IDS):

IDS เป็นระบบที่ใช้ตรวจจับกิจกรรมที่น่าสงสัยในเครือข่าย โดยการวิเคราะห์ข้อมูลที่ผ่านเข้ามาในระบบ หากพบกิจกรรมที่มีลักษณะเป็นการบุกรุก ระบบจะทำการแจ้งเตือนให้ผู้ดูแลระบบทราบ ตัวอย่างเช่น การติดตั้ง IDS เพื่อสแกนทราฟฟิกในเครือข่ายและตรวจจับการโจมตีแบบ DDoS (Distributed Denial of Service)

ระบบป้องกันไวรัส (Antivirus Systems):

ระบบป้องกันไวรัสทำหน้าที่ตรวจสอบและกำจัดมัลแวร์ (Malware) ที่เข้ามาในระบบ ซึ่งรวมถึงไวรัส (Virus), เวิร์ม (Worm), โทรจัน (Trojan) และสปายแวร์ (Spyware) ตัวอย่างเช่น การติดตั้งซอฟต์แวร์ป้องกันไวรัสในทุกเครื่องคอมพิวเตอร์ในองค์กร และการตั้งค่าให้ซอฟต์แวร์อัปเดตฐานข้อมูลไวรัสอัตโนมัติ

การเข้ารหัส (Encryption)

การเข้ารหัสเป็นกระบวนการที่ใช้แปลงข้อมูลให้อยู่ในรูปแบบที่ไม่สามารถอ่านได้โดยไม่ได้รับอนุญาต เพื่อป้องกันการเข้าถึงข้อมูลที่สำคัญ ตัวอย่างเช่น การใช้การเข้ารหัส SSL/TLS สำหรับการรับส่งข้อมูลบนอินเทอร์เน็ตหรือการเข้ารหัสข้อมูลที่จัดเก็บในฐานข้อมูล

มาตรการควบคุมด้านการบริหารจัดการ (Administrative Controls)

มาตรการควบคุมด้านการบริหารจัดการคือกระบวนการและนโยบายที่ใช้ในการจัดการความเสี่ยง และควบคุมการดำเนินงานขององค์กร เพื่อให้แน่ใจว่าการปฏิบัติงานเป็นไปตามมาตรฐานและข้อกำหนด โดยมาตรการควบคุมด้านการบริหารจัดการมีความสำคัญ เพราะช่วยให้การดำเนินงานขององค์กรเป็นไปอย่างมีประสิทธิภาพและปลอดภัย ช่วยลดความเสี่ยงและเพิ่มความเชื่อมั่นในระบบการทำงาน

นโยบายและขั้นตอน (Policies and Procedures):

ลักษณะของนโยบายและขั้นตอนสำหรับมาตรการควบคุมด้านการบริหารจัดการ (Characteristics of Policies and Procedures): นโยบายและขั้นตอนควรมีความชัดเจน ครอบคลุมทุกด้านของการดำเนินงาน และสามารถปฏิบัติตามได้ง่าย

การพัฒนานโยบายและขั้นตอน (Policy and Procedure Development): การจัดทำและปรับปรุงนโยบายและขั้นตอนอย่างสม่ำเสมอ เพื่อให้สอดคล้องกับความเปลี่ยนแปลงและความเสี่ยงใหม่ ๆ

การฝึกอบรมและสร้างความตระหนัก (Training and Awareness)

การฝึกอบรมและสร้างความตระหนักเป็นกระบวนการที่ให้ความรู้และทักษะด้านความปลอดภัยสารสนเทศแก่พนักงาน เพื่อให้พนักงานมีความรู้ความเข้าใจในความเสี่ยงและวิธีการป้องกัน

การฝึกอบรมด้านความปลอดภัยสารสนเทศ: จัดฝึกอบรมเกี่ยวกับมาตรการความปลอดภัย การใช้ระบบอย่างปลอดภัย และการรับมือกับเหตุการณ์ด้านความปลอดภัย

โปรแกรมสร้างความตระหนัก: การจัดทำโปรแกรมสร้างความตระหนักในรูปแบบต่าง ๆ เช่น การจัดสัมมนา การแจกจ่ายเอกสารข้อมูล การใช้แคมเปญผ่านอีเมล หรือการจัดทำวิดีโอสื่อการเรียนการสอน

การตรวจสอบและประเมิน (Audit and Assessment)

การตรวจสอบและประเมินเป็นกระบวนการที่ใช้ในการตรวจสอบระบบและกระบวนการอย่างสม่ำเสมอ เพื่อให้แน่ใจว่ามาตรการควบคุมความเสี่ยงมีประสิทธิภาพ ตัวอย่างเช่น

การตรวจสอบภายใน (Internal Audit): การตรวจสอบการดำเนินงานภายในองค์กรเพื่อตรวจหาจุดอ่อนและปรับปรุงการควบคุม

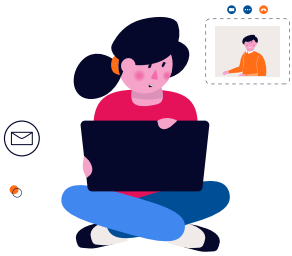
การประเมินความเสี่ยง (Risk Assessment): การประเมินความเสี่ยงเพื่อระบุและจัดลำดับความสำคัญของความเสี่ยงที่ต้องการการจัดการ

มาตรการควบคุมด้านกายภาพ (Physical Controls)

มาตรการควบคุมด้านกายภาพคือการใช้วิธีการต่าง ๆ ในการปกป้องทรัพย์สินทางกายภาพขององค์กรจากการถูกทำลาย ขโมย หรือการเข้าถึงโดยไม่ได้รับอนุญาต มาตรการเหล่านี้มีความสำคัญอย่างยิ่งในการรักษาความปลอดภัยของข้อมูลและระบบสารสนเทศ เนื่องจากสามารถป้องกันความเสี่ยงที่เกิดขึ้นจากการเข้าถึงหรือการทำลายทรัพย์สินทางกายภาพได้ช่วยให้มั่นใจได้ว่า ข้อมูลและทรัพยากรสำคัญต่าง ๆ ขององค์กร จะได้รับการปกป้องอย่างเหมาะสม

ระบบควบคุมการเข้าออก (Access Control Systems)

ระบบควบคุมการเข้าออกเป็นมาตรการที่ใช้ในการควบคุมและจำกัดการเข้าถึงพื้นที่ที่สำคัญขององค์กร เช่น ห้องเซิร์ฟเวอร์ ห้องเก็บข้อมูลสำคัญ เป็นต้น ตัวอย่างของระบบควบคุมการเข้าออกได้แก่



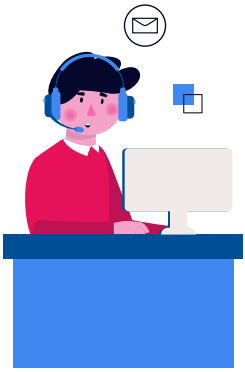
การใช้บัตรผ่าน (Access Cards): การใช้บัตรผ่านในการควบคุมการเข้าถึงพื้นที่ที่ได้รับอนุญาตเท่านั้น

การใช้รหัสผ่าน (PIN): การใช้รหัสผ่านเพื่อควบคุมการเข้าถึง

การใช้ระบบสแกนลายนิ้วมือหรือใบหน้า (Biometric Systems): การใช้เทคโนโลยีสแกนลายนิ้วมือหรือใบหน้าเพื่อยืนยันตัวตนก่อนเข้าถึงพื้นที่

กล้องวงจรปิด (CCTV): การตรวจสอบความปลอดภัย

กล้องวงจรปิดเป็นเครื่องมือที่ใช้ในการตรวจสอบและเฝ้าระวังความปลอดภัยในพื้นที่ต่าง ๆ ขององค์กรช่วยในการตรวจจับกิจกรรมที่น่าสงสัย และเป็นหลักฐานในกรณีที่เกิดเหตุการณ์ความไม่ปลอดภัย ตัวอย่างการใช้งานกล้องวงจรปิดได้แก่



การติดตั้งกล้องวงจรปิดในบริเวณที่มีความเสี่ยงสูง: เช่น ห้องเก็บข้อมูล ห้องเซิร์ฟเวอร์ หรือบริเวณที่มีการเข้าถึงมาก

การตรวจสอบภาพจากกล้องวงจรปิด: การตรวจสอบภาพจากกล้องวงจรปิดอย่างสม่ำเสมอ เพื่อเฝ้าระวังความปลอดภัย

การบันทึกภาพจากกล้องวงจรปิด: การเก็บบันทึกภาพจากกล้องวงจรปิด เพื่อนำมาใช้เป็นหลักฐานในกรณีที่เกิดเหตุการณ์ความไม่ปลอดภัย

ระบบป้องกันอัคคีภัย (Fire Protection Systems)

ระบบป้องกันอัคคีภัยเป็นมาตรการที่ใช้ในการป้องกันและลดความเสี่ยงจากไฟไหม้ที่อาจเกิดขึ้นในพื้นที่สำคัญขององค์กร ตัวอย่างของระบบป้องกันอัคคีภัยได้แก่

การติดตั้งระบบดับเพลิงอัตโนมัติ (Automatic Fire Suppression Systems): การติดตั้งระบบดับเพลิงอัตโนมัติเพื่อดับไฟทันทีที่ตรวจพบการเกิดไฟไหม้

การติดตั้งเครื่องตรวจจับควัน (Smoke Detectors): การติดตั้งเครื่องตรวจจับควันเพื่อแจ้งเตือนเมื่อเกิดไฟไหม้

การติดตั้งระบบพ่นน้ำ (Sprinkler Systems): การติดตั้งระบบพ่นน้ำเพื่อช่วยในการดับไฟ

สรุปท้ายบท Chapter 10

การนำกลยุทธ์การลดความเสี่ยงไปใช้

กระบวนการและกลยุทธ์ต่าง ๆ ที่องค์กรสามารถนำมาใช้ เพื่อลดความเสี่ยงที่เกี่ยวข้องกับความปลอดภัยของสารสนเทศได้อย่างมีประสิทธิภาพ เริ่มต้นจากการระบุและประเมินความเสี่ยง เพื่อตั้งระดับความเสี่ยงที่ยอมรับได้ หลังจากนั้น องค์กรสามารถใช้มาตรการควบคุมต่าง ๆ เช่น มาตรการควบคุมด้านเทคนิค (Technical Controls) มาตรการควบคุมด้านการบริหารจัดการ (Administrative Controls) และมาตรการควบคุมด้านกายภาพ (Physical Controls) เพื่อควบคุมและลดความเสี่ยงที่อาจเกิดขึ้น

การนำกลยุทธ์การลดความเสี่ยงไปใช้นั้น ไม่เพียงแค่ช่วยลดความเสี่ยงในการดำเนินงาน แต่ยังเป็นการสร้างวัฒนธรรมการรักษาความปลอดภัยในองค์กร ที่ทุกคนมีบทบาทและความรับผิดชอบร่วมกันในการปกป้องทรัพย์สินสารสนเทศ การติดตามและประเมินผลของมาตรการควบคุมเหล่านี้อย่างต่อเนื่องเป็นสิ่งสำคัญ เพื่อให้แน่ใจว่ามาตรการที่นำมาใช้นั้น มีประสิทธิภาพและสามารถปรับปรุงได้ตามความเปลี่ยนแปลงของภัยคุกคามและเทคโนโลยีที่เกิดขึ้นใหม่ ๆ

CHAPTER
11

การพัฒนานโยบายความปลอดภัยที่มีประสิทธิภาพ

ที่มา: https://www.skillcast.com/blog/policies-procedures-workplace

นโยบายและขั้นตอนปฏิบัติ (Policies and Procedures) ในการรักษาความมั่นคงปลอดภัยสารสนเทศ

นโยบายการรักษาความมั่นคงปลอดภัยทางสารสนเทศเป็นแนวทางสำหรับผู้ที่มีส่วนเกี่ยวข้องในการปฏิบัติเพื่อบรรลุจุดประสงค์ของการรักษาระบบสารสนเทศให้มีความปลอดภัย ส่วนขั้นตอนการปฏิบัติคือวิธีการที่เป็นขั้นเป็นตอนในการทำตามนโยบายได้สำเร็จ ยกตัวอย่างนโยบายรักษาความมั่นคงปลอดภัยทางไซเบอร์ในด้านการเฝ้าระวังเหตุการณ์ไม่พึงประสงค์จากภายในและภายนอกองค์กร มีขั้นตอนการปฏิบัติ เช่น เริ่มแรกบันทึกข้อมูลเหตุการณ์ไม่พึงประสงค์ที่เจอในระบบขององค์กร ต่อมารวบรวมรายละเอียดเกี่ยวกับเหตุการณ์จากอุปกรณ์ทางสารสนเทศที่เกิดเหตุการณ์

ความสำคัญของนโยบายและขั้นตอนปฏิบัติ

นโยบายและขั้นตอนการปฏิบัติช่วยให้องค์กรจัดการและปกป้องข้อมูลให้มีความปลอดภัย เพื่อป้องกันภัยคุกคามทางไซเบอร์ เช่น การเปิดเผยหรือรั่วไหลของข้อมูล (Data leak) และการเข้าถึงข้อมูลจากบุคคลไม่พึงประสงค์ (Data breach) นอกจากนี้นโยบายและขั้นตอนปฏิบัติกำหนดความคาดหวังที่เกี่ยวข้องกับความปลอดภัยสำหรับพนักงานในองค์กรและเป็นกลไกที่สนับสนุนความรับผิดชอบทางกฎหมายและจริยธรรมขององค์กร

หลักการในการพัฒนานโยบายความปลอดภัยที่มีประสิทธิภาพ

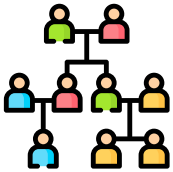
เข้าใจช่องโหว่และความต้องการด้านความปลอดภัยทางสารสนเทศขององค์กร

เริ่มต้นจากการที่องค์กรนั้นๆ ทำความเข้าใจเรื่องความสำคัญในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ภายในส่วนต่าง ๆ องค์กร เช่น ฝ่ายขาย ฝ่ายเทคโนโลยี ฝ่ายบริการ และฝ่ายการตลาด เป็นต้น ซึ่งสำคัญต่อการกำหนดนโยบายโดยรวมขององค์กรในการสร้างความปลอดภัยสารสนเทศ

การประเมินความเสี่ยงของทรัพย์สินทางสารสนเทศ

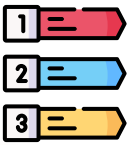
กำหนดและจัดลำดับความสำคัญของทรัพย์สินทางสารสนเทศภายในองค์กรและภัยคุกคามที่อาจเกิดขึ้น พร้อมทั้งประเมินภัยคุกคาม ระดับความเสี่ยง และข้อกังวลหลักเกี่ยวกับความปลอดภัยทางไซเบอร์

1. ระบุทรัพย์สิน: ระบุสินทรัพย์ทั้งหมดที่ต้องการการปกป้อง ซึ่งรวมถึงคอมพิวเตอร์ เซิร์ฟเวอร์ ซอฟต์แวร์ ข้อมูล และทรัพย์สินทางปัญญา และจัดประเภทข้อมูลตามความสำคัญของข้อมูลต่อองค์กร



2. ทำแผนที่ทรัพย์สินขององค์กร: ระบุรายละเอียดตำแหน่งทางกายภาพและตำแหน่งในเครือข่ายของแต่ละทรัพย์สิน บุคคลที่ได้รับการอนุญาตให้เข้าถึง และมาตรการการป้องกันในปัจจุบัน เพื่อเข้าใจช่องโหว่และการส่งต่อของข้อมูลที่ละเอียดอ่อนในองค์กร

3. เข้าใจบริบทภัยคุกคามของอุตสาหกรรมองค์กร: ติดตามแนวโน้มภัยคุกคามไซเบอร์และภัยคุกคามทางไซเบอร์ที่เกิดขึ้นล่าสุดในอุตสาหกรรมขององค์กร และวิเคราะห์ภัยคุกคามทางไซเบอร์ตามอุตสาหกรรมขององค์กรที่มีโอกาสเกิดขึ้นได้



4. จัดลำดับความสำคัญของความเสี่ยง: จัดอันดับความเสี่ยงตามผลกระทบและความเป็นไปได้ในการเกิดความเสี่ยงนั้น เพื่อมุ่งเน้นความพยายามด้านความปลอดภัยทางไซเบอร์ในจุดที่สำคัญที่สุดและมีโอกาสเกิดขึ้นมากที่สุด

5. ดูแลป้องกันจุดที่สามารถโดนโจมตีได้ขององค์กร: ดูแลจุดที่มีความเสี่ยงการโดนโจมตีโดยการรักษาความปลอดภัยที่อุปกรณ์ปลายทางเช่น คอมพิวเตอร์ สมาร์ตโฟน การกำหนดค่าไฟร์วอลล์ (Firewall) อย่างเหมาะสม และจำกัดการเข้าถึงของผู้ใช้ให้เฉพาะแอปพลิเคชันและข้อมูลที่จำเป็น

ตั้งเป้าหมายที่สามารถบรรลุได้และคิดค้นนโยบาย

นำการประเมินความเสี่ยงของทรัพย์สินสารสนเทศ มากำหนดเป้าหมายความปลอดภัยทางไซเบอร์ โดยการทำความเข้าใจความเสี่ยงที่องค์กรยอมรับได้ และตั้งความคาดหวังที่สมเหตุสมผล ซึ่งถ้าเกิดเป้าหมายต่าง ๆ ไม่สามารถบรรลุได้ในครั้งเดียว ต้องมั่นใจให้ได้ว่าสามารถบรรลุเป็นทีละเป้าหมายได้ องค์ประกอบเหล่านี้เป็นสิ่งสำคัญในการพัฒนากลยุทธ์ความปลอดภัยทางไซเบอร์ที่มีประสิทธิภาพ ตัวอย่างของเป้าหมาย เช่น การเสริมความปลอดภัยของเครือข่าย การเพิ่มการปกป้องข้อมูล การปรับปรุงการตอบสนองต่อเหตุการณ์ และการปฏิบัติตามข้อกำหนดทางกฎหมาย

ตรวจสอบนโยบายให้สอดคล้องกับข้อกฎหมาย

องค์กรต้องตรวจสอบให้แน่ใจว่านโยบายที่ตั้งขึ้นมาเป็นไปตามกฎหมายและระเบียบข้อบังคับที่เกี่ยวข้องหรือไม่ ยกตัวอย่าง มาตรฐานความปลอดภัยของ PCI เกี่ยวเนื่องกับการรักษาความปลอดภัยของข้อมูลการชำระเงิน และ Health Insurance Portability and Accountability Act of 1996 (HIPAA) ซึ่งเป็นกฎหมายของประเทศสหรัฐอเมริกาที่คุ้มครองข้อมูลด้านสุขภาพของประชาชน

ทดสอบนโยบาย

ทดสอบนโยบายกับบุคคลในองค์กรที่กำหนดให้ต้องปฏิบัติตามนโยบาย โดยให้บุคคลเหล่านี้ทำการประเมินต่าง ๆ เช่น ทำแบบประเมินความพร้อมการรับมือแรนซัมแวร์ (Ransomware) ทำแบบประเมินการตรวจสุขภาพไซเบอร์ของ NIST และเข้าร่วมการจำลองเหตุการณ์ภัยคุกคามทางไซเบอร์ การทำแบบทดสอบและเข้าร่วมการจำลองเหตุการณ์เหล่านี้อยู่สม่ำเสมอ ช่วยให้องค์กรประเมินความสามารถในการใช้นโยบายรับมือในกรณีเกิดเหตุการณ์จริงเกี่ยวกับภัยคุกคามทางไซเบอร์ และช่วยให้องค์กรนำผลการประเมินมาใช้ปรับปรุงนโยบายให้สอดคล้องกับสถานการณ์ปัจจุบันและรองรับภัยคุกคามต่าง ๆ ที่อาจเกิดขึ้นได้ในอนาคต

การเตรียมตัวเขียนขั้นตอนปฏิบัติ

การเลือกรูปแบบของขั้นตอนปฏิบัติ

เพื่อจัดทำขั้นตอนปฏิบัติ หน่วยงานที่รับผิดชอบในเรื่องนี้ขององค์กร ควรคิดวิธีที่ต้องการนำเสนอหรือรูปแบบของขั้นตอนปฏิบัติ รูปแบบอาจขึ้นอยู่กับรูปแบบองค์กรและประเภทของขั้นตอนปฏิบัติที่เลือกเขียน ตัวอย่างเช่น ขั้นตอนที่ยาวอาจเหมาะสมกับรูปแบบคู่มือการใช้งาน ในขณะที่ขั้นตอนที่สั้นอาจใช้เป็นรูปแบบการเรียงลำดับเป็นข้อ ๆ (Checklist) การใช้สัญลักษณ์ Bullet Points ตัวเลข และช่องทำเครื่องหมาย (Checkmark Boxes) ช่วยให้ขั้นตอนปฏิบัติมีระเบียบ

กระบวนการการเขียนขั้นตอนปฏิบัติ

เลือกหัวข้อที่จะเขียนขั้นตอนปฏิบัติ

หน่วยงานในองค์กรควรพิจารณาว่าจะเริ่มต้นเขียนขั้นตอนปฏิบัติในหัวข้อใด โดยเริ่มต้นจากการเขียนหัวข้อเล็กเรียงไปจนถึงหัวข้อใหญ่เพื่อสะสมประสบการณ์การเขียนให้เขียนได้ดียิ่งขึ้น ยกตัวอย่างเช่น ในบริษัทผู้ผลิต อาจเริ่มต้นด้วยการเขียนขั้นตอนสำหรับเครื่องจักรแต่ละเครื่องก่อนที่จะดำเนินการเขียนขั้นตอนสำหรับทั้งแผนกหรืออาจเริ่มต้นเขียนจากหัวข้อที่มีความสำคัญสูงสุดต่อองค์กร ซึ่งองค์กรหรือแผนกยังไม่เคยเขียนขั้นตอนปฏิบัติในหัวข้อนี้มาก่อน โดยที่สามารถประเมินความสำคัญและคาดการณ์ผลกระทบหลังการบังคับใช้ขั้นตอนปฏิบัติในหัวข้อต่าง ๆ หากมีหัวข้อของขั้นตอนปฏิบัติใดที่มีความสำคัญและสามารถปรับปรุงประสิทธิภาพการทำงานขององค์กรได้ทันที ถือได้ว่าเป็นหัวข้อขั้นตอนปฏิบัติที่ควรเริ่มต้นการเขียนก่อน

ปรึกษากับทีมที่ให้ข้อมูลที่มีประโยชน์ต่อการเขียนขั้นตอนปฏิบัติ

หลังจากเลือกหัวข้อขั้นตอนที่ต้องการเขียนแล้ว ให้ปรึกษากับทางทีมที่ต้องปฏิบัติตามขั้นตอนปฏิบัติ หรือกลุ่มที่ขั้นตอนปฏิบัติมีการบังคับใช้ว่าจะพัฒนาขั้นตอนปฏิบัติอย่างไร ซึ่งบุคคลในทีมดังกล่าวเป็นผู้ที่คุ้นเคยและมีความเชี่ยวชาญเกี่ยวกับหัวข้อขั้นตอนปฏิบัติ คำปรึกษาของทีมมีประโยชน์อย่างมากต่อการพัฒนาขั้นตอนปฏิบัติและสร้างความมีส่วนร่วมให้กับผู้ที่ต้องนำขั้นตอนปฏิบัติไปใช้ ทำให้บุคคลเหล่านี้รู้สึกอยากปฏิบัติตามขั้นตอนที่ตนมีส่วนร่วม

ช่วงเวลาการปรึกษาควรครอบคลุมในประเด็นดังต่อไปนี้

- ระบุวัตถุประสงค์ของขั้นตอนปฏิบัติ
- กำหนดจุดเริ่มต้นและจุดสิ้นสุดที่ชัดเจน
- ระบุผู้ที่เกี่ยวข้อง
- ตกลงในระดับรายละเอียดที่จำเป็น
- หารือเกี่ยวกับขั้นตอนและหลักการพื้นฐานในการเขียนขั้นตอนปฏิบัติ
- ตรวจสอบว่าขั้นตอนควรดำเนินการอย่างไรเพื่อพัฒนาการดำเนินการปัจจุบัน

วิธีการทำงานร่วมกันนี้ จะช่วยให้มั่นใจว่าขั้นตอนมีความถูกต้อง และสามารถนำไปใช้งานได้จริง

เขียนบทนำของขั้นตอนการปฏิบัติ

หลังจากกำหนดกลุ่มเป้าหมายแล้ว หน่วยงานที่เขียนขั้นตอบปฏิบัติสามารถเริ่มเขียนบทนำ ซึ่งโดยปกติจะมีความยาวหนึ่งหรือสองย่อหน้า เริ่มต้นด้วยการเปิดเรื่องที่น่าสนใจ และดึงดูดความสนใจ อธิบายว่าใครควรปฏิบัติตามขั้นตอน เมื่อใดควรปฏิบัติตาม และขั้นตอนนั้นถูกออกแบบมาเพื่อให้บรรลุผลสำเร็จอย่างไร อธิบายความสำคัญของขั้นตอนปฏิบัติงาน หากเป็นไปได้ควรระบุวันที่เผยแพร่ขั้นตอนปฏิบัติเพื่อหลีกเลี่ยงความสับสนเกี่ยวกับเวอร์ชันของขั้นตอนปฏิบัติ

จัดทำรายการทรัพยากรที่จำเป็นและเนื้อหาที่มีประโยชน์

ถัดมาจากบทนำควรเป็นส่วนที่กล่าวถึงรายการทรัพยากรที่จำเป็นและต้องจัดเตรียมในการดำเนินตามขั้นตอนปฏิบัติ ยกตัวอย่าง ในขั้นตอนปฏิบัติสำหรับการพ่นสี รายการทรัพยากรอาจรวมถึงสี พู่กัน ลูกกลิ้ง และอุปกรณ์ป้องกัน

แนะนำให้หน่วยงานที่เขียนขั้นตอนปฏิบัติจัดทำรายการเนื้อหาภายนอกที่เกี่ยวข้องกับขั้นตอนปฏิบัติ เช่น หนังสืออิเล็กทรอนิกส์ (e-books) บทความที่เป็นประโยชน์ หรือการอ้างอิงแหล่งที่มาของข้อมูลที่ใช้เขียนขั้นตอน ไว้ท้ายเอกสารของขั้นตอนปฏิบัติ เพื่อให้ผู้ต้องปฏิบัติตามขั้นตอนสามารถไปศึกษารายละเอียดเพิ่มเติมเกี่ยวกับขั้นตอนการปฏิบัติจากเนื้อหาเหล่านี้ได้ ทำให้ผู้ต้องปฏิบัติตามขั้นตอน เข้าใจขั้นตอนปฏิบัติมากขึ้น และสามารถพัฒนาทักษะของตนด้านการรักษาความปลอดภัยทางสารสนเทศ นอกจากนี้ แนะนำให้ภายในขั้นตอนปฏิบัติมีการแนบลิงก์ที่พาไปสู่ขั้นตอนปฏิบัติอื่น ๆ ขององค์กร ซึ่งช่วยให้การเข้าถึงขั้นตอนปฏิบัติอื่น ๆ ขององค์กรเป็นไปได้ง่ายขึ้น

การลงมือเขียน (การร่าง) ขั้นตอนปฏิบัติ

ใช้รูปแบบของขั้นตอนปฏิบัติที่ได้เลือกไว้ในช่วงการเตรียมตัว ร่วมกับข้อมูลจากการประชุมกับทีมที่เกี่ยวข้อง เพื่อเริ่มลงมือเขียนขั้นตอนปฏิบัติ โดยไม่ต้องกังวลถึงเรื่องรูปภาพ วิดีโอ หรือไฟล์สนับสนุนในขณะนี้ เน้นที่การทำให้ข้อความและขั้นตอนถูกต้อง หลังจากนั้นให้แบ่งขั้นตอนปฏิบัติเป็นรายการขั้นตอน (Task list) ที่มีความชัดเจน เช่น “สำรองข้อมูล” “กำหนดทีมการกู้คืนภัยพิบัติ” “ประกาศรายละเอียดเหตุการณ์ให้ผู้มีส่วนได้ส่วนเสียทราบ” เป็นต้น โดยที่รายละเอียดของรายการขั้นตอน จะปรากฏอยู่ด้านล่างของรายการขั้นตอน ส่วนขั้นตอนปฏิบัติในรูปแบบอิเล็กทรอนิกส์ รายละเอียดจะซ่อนอยู่ภายในแต่ละรายการขั้นตอน ซึ่งรายละเอียดจะปรากฏก็ต่อเมื่อผู้ใช้ได้มีการกดที่รายการขั้นตอนนั้น การทำเช่นนี้เป็นประโยชน์ให้ผู้ที่ต้องปฏิบัติตามขั้นตอนสามารถเข้าใจขั้นตอนปฏิบัติโดยเบื้องต้นได้โดยที่ไม่ต้องเริ่มอ่านรายละเอียด และช่วยให้ผู้อ่านไม่รู้สึกเบื่อจากการที่เห็นแต่ตัวหนังสือของรายละเอียดเป็นจำนวนมาก ซึ่งการเขียนรายละเอียดของรายการขั้นตอนควรมีความกระชับให้ได้มากที่สุดเท่าที่ทำได้

ตัวอย่างรายการขั้นตอนในขั้นตอนปฏิบัติ

ที่มา: https://www.process.st/how-to-write-a-procedure/

การเพิ่มองค์ประกอบภาพ รูปภาพ และสื่อ ในขั้นตอนปฏิบัติ

องค์ประกอบภาพ เช่น กราฟ แผนภูมิ และผังงาน สามารถช่วยอธิบายข้อมูลในขั้นตอนปฏิบัติที่มีความซับซ้อนได้ ตัวอย่างเช่น หน่วยงานอาจใส่รูปภาพที่มีลูกศรกำกับ เพื่อให้สมาชิกในทีมที่ต้องปฏิบัติตามขั้นตอนได้รับข้อมูลเพิ่มเติมเกี่ยวกับขั้นตอน การเพิ่มสื่อประเภทอื่น ๆ ลงในขั้นตอนปฏิบัติ ทำให้ผู้ที่ต้องปฏิบัติตามเกิดความสนใจในการปฏิบัติตามขั้นตอนด้วยความเต็มใจที่จะดำเนินการตามอย่างเคร่งครัด นอกจากนี้ การแสดงขั้นตอนปฏิบัติงานผ่านรูปภาพหรือวิดีโอ ยังมีประสิทธิภาพมากกว่าการพยายามอธิบายงานเหล่านั้นเป็นข้อความยาว ๆ

การทบทวนขั้นตอนการปฏิบัติ

หลังจากร่างขั้นตอนเรียบร้อยแล้ว หน่วยงานภายในองค์กรที่เขียนขั้นตอนปฏิบัติควรทบทวนและแก้ไขงานเขียน พยายามใช้ภาษาในการเขียนให้เรียบง่ายและนำไปใช้ปฏิบัติจริงให้ได้มากที่สุด สามารถใช้คำศัพท์การสั่งการที่ไม่รุนแรง และเขียนขั้นตอนต่าง ๆ เป็นประโยคสั้น ๆ เพื่อช่วยให้ขั้นตอนปฏิบัติมีความชัดเจน นอกจากนี้ การทบทวนและแก้ไขขั้นตอนปฏิบัติให้สอดคล้องกับการทำงานในปัจจุบันของทีมที่ขั้นตอนปฏิบัติจะมีการบังคับใช้ก็เป็นสิ่งสำคัญ เนื่องจากการไม่คำนึงถึงวิธีการทำงานของทีมในปัจจุบัน จะไม่สามารถทำให้ทีมปรับตัวเข้ากับขั้นตอนปฏิบัติได้

การทดสอบขั้นตอนการปฏิบัติ

ทดสอบขั้นตอนปฏิบัติเพื่อให้แน่ใจว่าไม่มีประเด็นใดถูกมองข้ามหรือลืม การทดสอบเหล่านี้ จะแสดงให้เห็นว่า ขั้นตอนปัจจุบันมีประสิทธิภาพ หรือจำเป็นต้องมีการปรับเปลี่ยนหรือไม่ นำผลลัพธ์ของการปฏิบัติตามขั้นตอนอย่างแม่นยำมาวัดประสิทธิภาพของขั้นตอน ปฏิบัติตามวัตถุประสงค์ที่ได้มีการปรึกษากับทีมในกระบวนการช่วงต้น ขึ้นอยู่กับความซับซ้อนของขั้นตอนปฏิบัติ อาจต้องวัดความสำเร็จหรือประสิทธิภาพเพิ่มเติม โดยใช้ดัชนีชี้วัดความสำเร็จ (Key Performance Indicator - KPI)

การปรับปรุงขั้นตอนการปฏิบัติ

ผลการทดสอบในข้างต้นควรบ่งชี้ว่า ขั้นตอนปฏิบัติพร้อมที่จะปรับใช้หรือจำเป็นต้องมีการปรับปรุงหรือไม่ หากจำเป็นต้องมีการปรับปรุงให้ร่างการปรับปรุงทันที เพื่อให้เกิดความต่อเนื่องในกระบวนการพัฒนาขั้นตอนปฏิบัติ ซึ่งผลลัพธ์จากการทดสอบขั้นตอนปฏิบัติอย่างรอบด้าน จะช่วยให้สามารถระบุจุดที่ต้องปรับปรุง และชี้แนววิธีการปรับปรุงเพื่อให้ได้ขั้นตอนปฏิบัติที่มีประสิทธิภาพสูง

หน่วยงานที่เขียนขั้นตอนปฏิบัติควรปรึกษากับทางทีมที่ต้องปฏิบัติตามขั้นตอนอีกครั้ง เพื่อหารือวิธีปรับปรุงขั้นตอนปฏิบัติให้สามารถสร้างผลลัพธ์ที่ดีอย่างก้าวกระโดดตามวัตถุประสงค์ที่ได้วางเอาไว้ แต่ถึงแม้อย่างไร การปรับปรุงขั้นตอนปฏิบัติให้ดีขึ้นเพียงทีละเล็กน้อย อาจทำให้ขั้นตอนปฏิบัติพัฒนาไปมากในอนาคต สำหรับการปรับปรุงขั้นตอนปฏิบัติในแต่ละครั้ง ควรทำการทดสอบซ้ำไปเรื่อย ๆ จนกว่าผลลัพธ์ที่ได้ออกมาจะเป็นที่พึงพอใจ

สรุปท้ายบท Chapter 11

การพัฒนานโยบายความปลอดภัยที่มีประสิทธิภาพ

นโยบายและขั้นตอนปฏิบัติมีความสำคัญเพื่อรักษาความมั่นคงปลอดภัยของสารสนเทศในองค์กร หลักการในการพัฒนานโยบายที่มีประสิทธิภาพ เช่น การยึดตามหลักความลับ (Confidentiality) ความถูกต้อง (Integrity) และความสามารถในการเข้าถึง (Availability) หรือมาตรฐาน ISO 27001 กระบวนการเขียนและพัฒนานโยบาย เริ่มต้นจากการเข้าใจความต้องการในการปกป้องทรัพย์สินทางสารสนเทศขององค์กร ประเมินความเสี่ยงของทรัพย์สิน ไปจนถึงขั้นตอนสุดท้าย การทดสอบนโยบาย ส่วนขั้นตอนการเขียนขั้นตอนปฏิบัติ เริ่มต้นจากการเลือกหัวข้อที่จะเขียนขั้นตอนปฏิบัติ ปรึกษากับทีมที่ต้องปฏิบัติตามขั้นตอนปฏิบัติ ไปจนถึงการปรับปรุงขั้นตอนปฏิบัติ

CHAPTER
12

การบูรณาการนโยบายและขั้นตอนปฏิบัติ

การออกแบบและเชื่อมโยงนโยบายและขั้นตอนปฏิบัติงานตาม NIST Cybersecurity Framework

เป็นการเชื่อมโยงทฤษฎีการออกแบบนโยบายขั้นตอนเข้ากับ NIST Cybersecurity Framework 2.0: มาตรการบริหารจัดการความปลอดภัยทางสารสนเทศ

Govern:
เป็นส่วนเริ่มต้นของการพัฒนานโยบายและขั้นตอนการปฏิบัติ โดยการเข้าใจบริบทและทัศนคติขององค์กรในด้านของกิจกรรมการดำเนินงาน พันธกิจ กลยุทธ์บริหารความเสี่ยง หน้าที่และความรับผิดชอบของบุคลากร เป็นต้น เพื่อสร้างนโยบายและขั้นตอนการปฏิบัติให้สอดคล้องกับบริบทและทัศนคติขององค์กร

Identify:
องค์กรต้องสามารถระบุความเสี่ยงของทรัพย์สินทางสารสนเทศต่อการเกิดภัยอันตรายทางไซเบอร์ ความเสี่ยงของภัยคุกคามทางไซเบอร์ที่ส่งผลกระทบต่อตัวองค์กร ทรัพย์สินต่าง ๆ ในองค์กรและบุคคลต่าง ๆ และแนวทางการปรับปรุงกระบวนการและกิจกรรมในแต่ละฟังก์ชันของกรอบการดำเนินงาน CSF เพื่อสร้างนโยบายที่จัดการกับความเสี่ยงต่าง ๆ เหล่านี้ได้ และสร้างนโยบายที่รักษาความปลอดภัยทางไซเบอร์ได้อย่างรอบด้าน

Protect:

การกำหนดนโยบายและขั้นตอนการปฏิบัติเพื่อปกป้องรักษาความปลอดภัยของข้อมูล เช่น การกำหนดสิทธิ์การเข้าถึงข้อมูล การสร้างเทคโนโลยีสารสนเทศให้มีความแข็งแกร่ง และการจัดอบรมเพิ่มความตระหนักรู้เกี่ยวกับภัยคุกคามไซเบอร์กับพนักงาน

Detect:

การกำหนดนโยบายและขั้นตอนการปฏิบัติที่ทำให้การตรวจจับและวิเคราะห์ความผิดปกติของระบบสารสนเทศ ซึ่งอาจเป็นสัญญานบ่งชี้ถึงภัยคุกคามทางไซเบอร์เป็นได้ไปอย่างมีประสิทธิภาพ

Respond:

การสร้างนโยบายและขั้นตอนการปฏิบัติที่สามารถบริหารจัดการและวิเคราะห์เหตุการณ์ภัยคุกคามทางสารสนเทศ สื่อสารกับผู้มีส่วนได้ส่วนเสียเกี่ยวกับเหตุการณ์ และลดการขยายวงกว้างกับผลกระทบของเหตุการณ์ ได้อย่างมีประสิทธิภาพ

Recover:

การกำหนดนโยบายและขั้นตอนการปฏิบัติตามกระบวนการกู้คืนระบบสารสนเทศที่มีความเหมาะสมจากเหตุการณ์ภัยคุกคามทางไซเบอร์ และกระบวนการสื่อสารที่มีประสิทธิภาพให้ผู้มีส่วนได้ส่วนเสียทราบเกี่ยวกับเหตุการณ์ภัยคุกคามทางไซเบอร์

การนำนโยบายไปใช้จริงในองค์กร

การสื่อสารและเผยแพร่นโยบายและขั้นตอนปฏิบัติให้กับพนักงานทุกคนในองค์กร

การสื่อสารและเผยแพร่นโยบายและขั้นตอนปฏิบัติให้กับพนักงานทุกคนในองค์กรเป็นขั้นตอนที่สำคัญในการนำนโยบายไปใช้จริง ตัวอย่างเช่น:

สื่อสารนโยบายและขั้นตอนปฏิบัติให้พนักงานทุกคนทราบ: การสื่อสารเป็นสิ่งสำคัญเพื่อให้พนักงานทุกคนทราบถึงนโยบายและขั้นตอนปฏิบัติขององค์กร ซึ่งสามารถทำได้ผ่านช่องทางต่าง ๆ เช่น การประชุม อีเมล หรือเว็บไซต์ภายในองค์กร

จัดทำคู่มือหรือเอกสารประกอบ: การจัดทำคู่มือหรือเอกสารประกอบที่ชัดเจนและเข้าใจง่าย จะช่วยให้พนักงานสามารถเรียนรู้และปฏิบัติตามนโยบายได้อย่างถูกต้อง

ใช้ช่องทางการสื่อสารที่หลากหลาย: การใช้ช่องทางการสื่อสารที่หลากหลาย เช่น อีเมล เว็บไซต์ การประชุม หรือการอบรม จะช่วยให้การสื่อสารนโยบายและขั้นตอนปฏิบัติถึงพนักงานได้อย่างทั่วถึงและมีประสิทธิภาพ

การใช้เทคโนโลยีเพื่อช่วยในการบังคับใช้นโยบายและขั้นตอนปฏิบัติ

Firewall: ไฟร์วอลล์ช่วยในการบังคับใช้นโยบายความปลอดภัย โดยกำหนดกฎที่จะอนุญาตหรือไม่อนุญาตให้ใช้งานเซอร์วิสแบบต่าง ๆ ภายในเครือข่าย ทำให้ผู้ดูแลระบบสามารถควบคุมและกำหนดข้อกำหนดในการใช้งานเซอร์วิสต่าง ๆ ได้อย่างเข้มงวดและตรวจสอบได้ง่ายขึ้น

Intrusion Detection System (IDS): IDS ช่วยในการตรวจจับกิจกรรมที่ไม่พึงประสงค์ภายในระบบเครือข่ายหรือจากภายนอก โดยระบุพฤติกรรมที่เป็นไปได้ เช่น การบุกรุกหรือการเข้าถึงข้อมูลที่ไม่ถูกต้อง ซึ่งช่วยในการตอบสนองอย่างรวดเร็วต่อเหตุการณ์ที่เกิดขึ้นตามนโยบายการใช้งานที่ตั้งไว้ เป็นเครื่องมือรักษาความปลอดภัยที่ทุกองค์กรควรจะมีรองจากไฟร์วอลล์

Data Loss Prevention (DLP): DLP ช่วยในการป้องกันการสูญหายของข้อมูลที่สำคัญโดยระบุนโยบายการเข้าถึงและการส่งข้อมูล ซึ่งช่วยลดความเสี่ยงในการรั่วไหลของข้อมูลจากภายในหรือภายนอกองค์กร โดยการตรวจสอบและบล็อกการส่งข้อมูลที่ไม่เหมาะสมหรือไม่ได้รับอนุญาตตามนโยบายที่กำหนดไว้

การจัดฝึกอบรมและสร้างความตระหนักรู้เกี่ยวกับนโยบายและขั้นตอนปฏิบัติ:

การจัดฝึกอบรมและสร้างความตระหนักรู้เกี่ยวกับนโยบายและขั้นตอนปฏิบัติ มีขั้นตอนดังนี้:

การวางแผนและกำหนดเป้าหมายการฝึกอบรม

การจัดฝึกอบรมเริ่มต้นด้วยการระบุความต้องการในการฝึกอบรมและการกำหนดกลุ่มเป้าหมาย โดยอาจจะเป็นพนักงานทั้งหมดหรือเฉพาะกลุ่มที่เกี่ยวข้อง นอกจากนี้ ยังต้องกำหนดเป้าหมายของการฝึกอบรมว่า ต้องการให้พนักงานมีความรู้ความเข้าใจในด้านใด เช่น การระบุความเสี่ยง การป้องกันและการตอบสนองต่อเหตุการณ์ ซึ่งจะช่วยให้การฝึกอบรมมีทิศทางและเน้นไปที่การเพิ่มประสิทธิภาพในการปฏิบัติงานตามแนวทางของ NIST Framework อย่างเต็มที่

การพัฒนาหลักสูตรการฝึกอบรม

การพัฒนาหลักสูตรการฝึกอบรมต้องมีการสร้างเนื้อหาหลักสูตรที่ครอบคลุมแนวทางปฏิบัติตาม NIST Framework ซึ่งประกอบไปด้วยการระบุ (Identify), การป้องกัน (Protect), การตรวจจับ (Detect), การตอบสนอง (Respond), และการฟื้นฟู (Recover) โดยใช้สื่อการสอนที่หลากหลาย เช่น วิดีโอ เอกสาร สไลด์ และแบบฝึกหัด เพื่อให้พนักงานสามารถเรียนรู้และเข้าใจได้อย่างเต็มที่ รวมถึงการอัปเดตเนื้อหาให้ทันสมัยและเหมาะสมกับสถานการณ์ปัจจุบัน

การเลือกวิธีการฝึกอบรม

ควรใช้การฝึกอบรมแบบผสมผสาน (Blended Learning) เช่น การฝึกอบรมออนไลน์และการฝึกอบรมในห้องเรียน เพื่อให้พนักงานสามารถเรียนรู้ได้ทั้งในสถานที่ทำงานและในเวลาที่สะดวก นอกจากนี้ ยังควรจัดสัมมนาและการประชุมเชิงปฏิบัติการเพื่อเพิ่มพูนความรู้และทักษะของพนักงานอย่างต่อเนื่อง

การสร้างความตระหนักรู้

ควรมีการจัดกิจกรรมสร้างความตระหนักรู้เป็นประจำ เช่น การประชุมสั้น ๆ การส่งอีเมลแจ้งเตือน การจัดแข่งขันหรือเกมเพื่อกระตุ้นความสนใจ และการประชาสัมพันธ์ภายในองค์กร เช่น ป้ายประกาศ วารสารองค์กร และอินทราเน็ต เพื่อให้พนักงานเข้าใจและตระหนักถึงความสำคัญของนโยบายและขั้นตอนปฏิบัติงานอยู่เสมอ

การประเมินผลและการติดตาม

การประเมินผลการฝึกอบรมควรใช้แบบสอบถามหรือการทดสอบ เพื่อวัดความรู้และความเข้าใจของพนักงาน และติดตามผลการฝึกอบรมโดยการสังเกตการปฏิบัติงานของพนักงานและการรายงานเหตุการณ์ที่เกี่ยวข้อง ทั้งนี้ ยังต้องมีการปรับปรุงหลักสูตรและวิธีการฝึกอบรม ตามผลการประเมินและข้อเสนอแนะจากพนักงาน เพื่อให้การฝึกอบรมมีประสิทธิภาพมากยิ่งขึ้น

การสนับสนุนและการให้คำปรึกษา

การสนับสนุนและการให้คำปรึกษาหลังการฝึกอบรมเป็นสิ่งสำคัญ โดยควรจัดให้มีการให้คำปรึกษาและการสนับสนุน เช่น การให้ความช่วยเหลือผ่านระบบออนไลน์หรือการสนับสนุนจากทีมผู้เชี่ยวชาญ เพื่อให้พนักงานสามารถปรับตัว และปฏิบัติตามนโยบายและขั้นตอนปฏิบัติงานได้อย่างถูกต้องและมีประสิทธิภาพ

การติดตามและประเมินผลการปฏิบัติตามนโยบายและขั้นตอนปฏิบัติ:

การติดตามและประเมินผลการปฏิบัติตามนโยบายและขั้นตอนปฏิบัติเป็นขั้นตอนสำคัญในการตรวจสอบความถูกต้องและประสิทธิภาพของการปฏิบัติตามนโยบายขององค์กร ตัวอย่าง เช่น

ตรวจสอบการปฏิบัติตามนโยบายและขั้นตอนปฏิบัติอย่างสม่ำเสมอ
การตรวจสอบการปฏิบัติตามนโยบายและขั้นตอนปฏิบัติของพนักงานอย่างสม่ำเสมอ จะช่วยให้องค์กรสามารถระบุปัญหาและปรับปรุงการปฏิบัติตามนโยบายได้ทันที

ใช้เครื่องมือในการตรวจสอบ เช่น Log Analysis, Security Audit
การใช้เครื่องมือในการตรวจสอบ เช่น Log Analysis, Security Audit จะช่วยให้องค์กรสามารถตรวจสอบและประเมินผลการปฏิบัติตามนโยบายได้อย่างมีประสิทธิภาพและแม่นยำ

การปรับปรุงแก้ไขและพัฒนานโยบายและขั้นตอนปฏิบัติอย่างต่อเนื่อง:

การปรับปรุงแก้ไขและพัฒนานโยบายและขั้นตอนปฏิบัติอย่างต่อเนื่องเป็นการประกันว่ากระบวนการและมาตรการต่าง ๆ จะสอดคล้องกับสถานการณ์และเทคโนโลยีที่เปลี่ยนแปลง ตัวอย่างเช่น:

1. ทบทวนและปรับปรุงนโยบายและขั้นตอนปฏิบัติอย่างสม่ำเสมอ
การทบทวนและปรับปรุงนโยบายและขั้นตอนปฏิบัติอย่างสม่ำเสมอ จะช่วยให้นโยบายทันสมัยและเหมาะสมกับความเสี่ยงและเทคโนโลยีใหม่ ๆ

2. รับฟังข้อเสนอแนะจากพนักงานและผู้ที่เกี่ยวข้อง
การรับฟังข้อเสนอแนะจากพนักงานและผู้ที่เกี่ยวข้อง ช่วยให้องค์กรสามารถปรับปรุงและพัฒนานโยบาย และขั้นตอนปฏิบัติได้ตรงความต้องการ และข้อเสนอแนะที่ได้รับ

สรุปท้ายบท Chapter 12

การบูรณาการนโยบายและขั้นตอนปฏิบัติ

การเชื่อม NIST Cybersecurity Framework ให้เข้ากับการออกแบบนโยบายและขั้นตอนการปฏิบัติ ทำให้มั่นใจได้ว่าองค์กรจะมีนโยบายและขั้นตอนปฏิบัติที่รองรับกับแต่ละองค์ประกอบใน NIST Cybersecurity Framework 2.0 เช่น Govern, Identify และ Protect การใช้เทคโนโลยีในการบังคับใช้นโยบาย เช่น การกรองเนื้อหาเว็บ และการควบคุมการเข้าถึง เพื่อให้มั่นใจว่าการบูรณาการนโยบายเป็นไปอย่างมีประสิทธิภาพ

การสื่อสารและเผยแพร่นโยบายและขั้นตอนปฏิบัติให้กับพนักงานทุกคนในองค์กร การจัดฝึกอบรมและสร้างความตระหนักรู้เกี่ยวกับนโยบายและขั้นตอนปฏิบัติ รวมถึงการติดตามและประเมินผลการปฏิบัติตามนโยบายและขั้นตอนปฏิบัติอย่างต่อเนื่อง การดำเนินการเหล่านี้ จะช่วยให้การบูรณาการนโยบายและขั้นตอนปฏิบัติเป็นไปอย่างมีประสิทธิภาพและสามารถปรับปรุงให้ทันสมัยอยู่เสมอ

บรรณานุกรม

กรมวิทยาศาสตร์บริการ. (มปป). นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศกรมวิทยาศาสตร์บริการประจำปี พ.ศ. 2565.
https://www.oic.go.th/FILEWEB/CABINFOCENTER2/DRAWER025/GENERAL/DATA0000/00000116.PDF

กรกนก ศรีมุข. (2022). ทำความรู้จัก PDPA พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.2562.
https://www.arit.rmutt.ac.th/2022/06/08/pdpa/

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม. (2019). พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562.
https://www.mdes.go.th/mission/detail/2481

กุลางกูร พัฒนเมธาดา. (2019). พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562.
https://stri.cmu.ac.th/km_it_detail.php?id=15

ขจร ประเสริฐสม. (2024). การพัฒนา Cybersecurity ในประเทศไทย.
https://www.csu.co.th/2024/09/15/cybersecurity-development/

คณะกรรมการกฤษฎีกา. (2020). ข้อเสนอแนะเกี่ยวกับการปรับปรุงกฎหมายการรักษาความปลอดภัยไซเบอร์.
https://www.legislation.go.th/2020/cybersecurity

ชลธี ตรงจิต. (2023). การจัดการความเสี่ยงในระบบสารสนเทศ.
https://www.chalatech.com/risk- management

ชัยวัฒน์ อรัญญา. (2022). การป้องกันการโจมตีทางไซเบอร์ในองค์กร.
https://www.securitytoday.com/articles/2022/01/cyber-attack-protection.aspx

ทีมข่าวอาชญากรรม. (2023). ตร.ไซเบอร์ จับกุมผู้ต้องหาประกาศขายข้อมูลส่วนบุคคลนับล้านรายชื่อ.
https://mgronline.com/crime/detail/9660000064106

ธวัชชัย รุ่งโรจน์. (2024). การรักษาความมั่นคงปลอดภัยไซเบอร์ในสังคมดิจิทัล.
https://www.cybersecurity.com/thai-security

นครินทร์ สายทอง. (2022). ความสำคัญของข้อมูลในโลกไซเบอร์.
https://www.dataimportance.com/2022/cyber-world

นิวัฒน์ พรรณน้อย. (2023). วิเคราะห์ความเสี่ยงทางไซเบอร์ในธุรกิจ.
https://www.niwatbusiness.com/2023/cyber-risk

บริษัท แอล.พี.เอ็น. ดีเวลลอปเมนท์ จำกัด (มหาชน). (2022). แนวนโยบายและแนวปฏิบัติในการรักษาความ ปลอดภัยระบบสารสนเทศ V2.0.
https://www.lpn.co.th/stocks/wcmpage/o0x0/dg/fv/dgfvnnscm5i/%E0%B9%81%E0%B8%99%E0%B8%A7%E0%B8%99%E0%B9%82%E0%B8

บริษัท บริหารสินทรัพย์ ธนาคารอิสลามแห่งประเทศไทย จำกัด. (มปป). นโยบายความปลอดภัยด้านเทคโนโลยีสารสนเทศ (Information Technology Security Policy).
https://iam-asset.co.t/files/known_iam/operational-policy/%E0%B8%99%E0%B9%82%E0%B8%A2%E0 %B8

บรรจง หะรังษี. (2022). มาตรฐาน ISO/IEC 27001:2022 ฉบับภาษาไทย.
https://www.tnetsecurity.co m/download/%E0%B8%A1%E0%B8%B2%E0%B8%95%E0%B8%A3%E0%B8%9%E0%

บันทึกท้ายพระราชบัญญัติ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562. (27 พฤษภาคม 2562).
ราชกิจจานุเบกษา. เล่มที่ 136 ตอน 69 ก, หน้า 20.

มหาวิทยาลัยสงขลานครินทร์. (2020). กฎหมายทรัพย์สินางปัญญาเบื้องต้น.
https://research.eng.psu.ac.th/images/document/patent/patent_ law.pdf

มหาวิทยาลัยเชียงใหม่. (2023). บทที่ 4 แผนภาพกระแสข้อมูล (Data Flow Diagram).
https://myweb.cmu.ac.th/wijit.a/954243/week3/DFD.pdf

มหาวิทยาลัยราชภัฏอุดรธานี. (มปป).แผนภาพกระแสข้อมูล (Data Flow Diagram : DFD).
https://academic.udru.ac.th/~samawan/content/5SA-DFD.pdf

มนัสธนนท์ เอกโภควัฒน์. (2022). เรื่อง กฎหมาย PDPA ตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล เรื่อง ใกล้ตัวที่ทุกคนควรรู้.
https://www.parliament.go.th/ewtadmin/ewt/elaw_parcy/ewt_dl_ link.php?nid=2975

พรรษกร ฉันทวีโรจน์. (2022). ปกป้องทรัพย์สินทางปัญญา.
https://sciencepark.wu.ac.th/ipservice-e

พระราชบัญญัติ การรักษาความมั่นคงปลอดภัยซเบอร์ พ.ศ. 2562. (24 พฤษภาคม 2562).
ราชกิจจานุเบกษา. เล่มที่ 136 ตอน 69 ก.

ภาพร ภิยโยดิลกชัย. (2010). การตรวจสอบระบบเทคโนโลยีสารสนเทศตามแนวทางของ COBIT.
https://libdoc.dpu.ac.th/thesis/141275.pdf

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ. (2021). เกี่ยวกับ ThaiCERT.
https://www.thaicert.or.th/about-us/

ศิริรัตน์ ตรงวัฒนาวุฒิ. (2023). บทที่ 4 แผนภาพกระแสข้อมูล (Data Flow Diagram).
https://wachum.org/dewey/000/com22.pdf

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.). (2019). เกี่ยวกับ สกมช.
https://www.ncsa.or.th/aboutncsa.html

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์. (2020). พ.ร.บ.ธุรกรรมฯ เดอะซีรีส์.
https://www.etda.or.th/th/Useful-Resource/Knowledge-Sharing/Electronic-Transactions-Act-the-Series_Ep1.aspx

สสวท. (2020). ทรัพย์สินทางปัญญา (Intellectual Property).
https://designtechnology.ipst.ac.th/wpcontent/uploads/sites/83/2020/01/4_05%.pdf

Alphasec. (2024). ISO 27001 คืออะไร? คู่มือฉบับสมบูรณ์ | Alphasec.
https://www.alphasec.co.th/post/iso-27001-%E0 %8C-alphasec

Ben Wolford. (2020). What is GDPR, the EU's new data protection law?.
https://gdpr.eu/what-is-gdpr/

Chad Boutin. (2024). NIST Releases Version 2.0 of Landmark Cybersecurity Framework.
https://www.nist.gov/news-events/news/2024/02/nist-releases-version-20-landmark-cybersecurity-framework

Cyberelite. (2024). รู้จักกับ NIST Cybersecurity Framework 2.0.
https://www.cyberelite.co.th/blog/nist-cybersecurity-framework

Digital Council of Thailand. (2020). สรุปสาระสำคัญพระราชบัญญัติ คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562.
https://www.dct.or.th/upload/downloads/1612025563SummaryPDPA_DigitalCouncilofThailand.pdf

Georgina Guthrie. (2024). Qualitative risk analysis vs quantitative risk analysis: What's the difference?.
https://nulab.com/learn/project-management/qualitative-risk-analysis-vs-quantitative-risk-analysis-whats-difference/

Ingram Micro Thailand. (2019). IT Security VS Cybersecurity — Cybersecurity กับสิ่งที่เราต้องทำ ความเข้าใจสำหรับระบบรักษาความปลอดภัยในอนาคต.
https://medium.com/ingrammicroth/it-security-vs-cybersecurity-cybersecurity-aecbb23a4600

ISO. (2013). Information security, cybersecurity and privacy protection — Information security management systems — Requirements.
https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

ISO. (2022). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection—Information security management systems — Requirements.
https://www.iso.org/standard/27001#lifecycle

Isms.online. (2024). ISO 27001:2022 Annex A Explained.
https://www.isms.online/iso-27001/annex-a/

Itgovernance. (2022). GDPR penalties.
https://www.itgovernance.eu/da-dk/dpa-and-gdpr-penalties-dk

Kyna Kosling. (2024). ISO 27001:2022 Annex A Controls Explained.
https://www.itgovernance.co.uk/blog/iso-27001-the-14-control-sets-of-annex-a-explained

Miro. (2024). ไดอะแกรมการไหลของข้อมูล.
https://miro.com/th/diagramming/what-is-a-data-flow-diagram

NIST. (2024). The NIST Cybersecurity Framework (CSF) 2.0.
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

Niall McCarthy. (2024). The Biggest GDPR Fines of 2023.
https://www.eqs.com/compliance-blog/biggest-gdpr-fines/

Nicharee_m. (2023). ตำรวจไซเบอร์ บุกจับหนุ่มวิศวกร ประกาศขายข้อมูลส่วนบุคคลในเฟซบุ๊ก ให้กลุ่มเว็บพนันออนไลน์ นับล้านรายชื่อ.
https://ch3plus.com/news/crime/weekend/357730

Peak. (2022). เรื่องควรรู้เกี่ยวกับการจัดทำทะเบียนทรัพย์สินของกิจการ.
https://peakaccount.com/blog/business/gen-biz/biz-fixed-asset-register

Peltier, T. R. (2016). Information Security Policies, Procedures, and Standards: guidelines for effective information security management. CRC Press.

Safesiri. (มปป). การประเมินความเสี่ยง risk assessment คืออะไร ขั้นตอนการประเมินความเสี่ยง.
https://www.safesiri.com/risk-assessment/

Silverfort. (2024). ความหมายของการจัดการพื้นผิวการโจมตี?.
https://www.silverfort.com/th/glossary/attack-surface-management/


กรมพัฒนาฝีมือแรงงาน

DSDA
Digital Skill Development Academy

กระทรวงดิจิทัล
เพื่อเศรษฐกิจและสังคม

ETDA