
สำนักงานเศรษฐกิจการเกษตร
ศัพท์เฉพาะที่น่าสนใจเกี่ยวกับ
การรักษาความมั่นคงปลอดภัย
Cybersecurity
การให้คำปรึกษา กลุ่มตรวจสอบภายใน
www.audit.oae.go.th

สามารถแบ่งได้ออกเป็นหลายส่วน ดังนี้

- **Network Security** การตรวจจับและรักษาความมั่นคงปลอดภัย จากภัยคุกคามที่โจมตีผ่านระบบเครือข่าย
- **Endpoint Security** การตรวจจับและรักษาความมั่นคงปลอดภัย จากภัยคุกคามที่มุ่งเป้าโจมตีไปยังอุปกรณ์ของผู้ใช้งาน เช่น PC, Notebook, Smartphone และ Tablet
- **Data Center & Cloud Security** การตรวจจับและรักษาความมั่นคงปลอดภัย จากภัยคุกคามที่โจมตีไปยังศูนย์ข้อมูลหรือบริการ Cloud
- **Application Security** การตรวจจับและรักษาความมั่นคงปลอดภัย จากภัยคุกคามที่มุ่งเป้าโจมตีระบบ Application
- **Identity Management & Authentication** การบริหารจัดการบัญชีผู้ใช้งาน และการยืนยันตัวตนขององค์กร
- **Vulnerability & Patch Management** การตรวจสอบและบริหารจัดการ อุดช่องโหว่ในระบบต่าง ๆ ที่มีการใช้งานภายในองค์กร
- **Penetration Testing** การทดสอบเจาะระบบเพื่อหาช่องโหว่ภายใน ระบบ Application และระบบ IT ขององค์กร เพื่อทำการแก้ไขช่องโหว่ หรือจุดอ่อนด้านความมั่นคงปลอดภัยก่อนที่ผู้ประสงค์ร้ายจะทำการโจมตี

- **Secure Coding & DevSecOps** การพัฒนาซอฟต์แวร์และการจัดเตรียมกระบวนการและระบบเพื่อการพัฒนาซอฟต์แวร์อย่างมั่นคงปลอดภัย

- **Incident & Response** การเฝ้าระวัง ตรวจสอบ และตอบสนองต่อเหตุการณ์ภัยคุกคามที่เกิดขึ้นในธุรกิจองค์กรด้วยกระบวนการที่เป็นมาตรฐานและเหมาะสม พร้อมมีเครื่องมือและข้อมูลที่จำเป็นต่อการตอบสนองได้อย่างทันท่วงที

- **และอื่น ๆ อีกมากมาย** จะเห็นได้ว่าแนวทางในการรักษาความมั่นคงปลอดภัยนี้มีด้วยกันหลากหลายวิธีการ ซึ่งแต่ละธุรกิจองค์กรและระบบย่อยแต่ละส่วนในองค์กรนั้นก็ต้องการการรักษาความมั่นคงปลอดภัยด้วยวิธีการที่แตกต่างกันไป

ดังนั้นขั้นตอนที่สำคัญในการเตรียมตัวในส่วนนี้จึงเป็นการที่ธุรกิจองค์กรนั้นต้องทำการสำรวจและจำแนกว่าระบบ IT ใดที่ใช้งานอยู่นั้นมีการจัดเก็บข้อมูลส่วนบุคคลใดบ้างอยู่ และมีความสำคัญต่อธุรกิจมากน้อยเพียงใด รวมถึงมีการใช้เทคโนโลยีเบื้องหลังและเปิดให้มีการเชื่อมต่อใช้งานในช่องทางใดบ้าง เพื่อให้การจัดลำดับความสำคัญในการปกป้องระบบสามารถเป็นไปได้อย่างแม่นยำ และเลือกใช้งานแนวทางการปกป้องระบบได้อย่างเหมาะสม

ในขณะเดียวกัน ประเด็นด้านการเฝ้าระวังและดูแลรักษาความมั่นคงปลอดภัย โดยบุคลากรมืออาชีพผู้เชี่ยวชาญเองก็มีความสำคัญเช่นกัน ซึ่งธุรกิจองค์กรก็สามารถเลือกได้ทั้งการจัดตั้งทีมงานภายในเอง และการเลือกใช้บริการทีมงานภายนอกอย่างเช่นบริการด้าน Penetration Testing, Managed Security Services หรือการเลือกใช้บริการ Cyber Security Operation Center (SOC) as a Service ก็จะช่วยให้องค์กรสามารถรับมือกับการขาดแคลนบุคลากรด้าน Cybersecurity ที่ทั่วโลกกำลังเผชิญอยู่ในเวลานี้ได้

อย่างไรก็ดี การวางแผนและจัดการด้าน Cybersecurity นี้ก็เป็นกิจกรรมที่ต้องมีการตรวจสอบทบทวนและปรับปรุงอยู่เสมอเช่นกัน เพื่อให้การปกป้องรักษาระบบและข้อมูลสำคัญขององค์กรนั้นทันกับภัยคุกคามที่มีวิวัฒนาการอยู่ตลอดเวลาและมีการใช้เทคนิคใหม่ ๆ ในการโจมตีอยู่เสมอ

เครดิต ITAuditThailand