หัวข้อการบรรยาย ความมั่งคงปลอดภัยทางดิจิทัลสำหรับผู้บริหารภาครัฐ

(Digital Security for Government Executives)

วันที่ 22 สิงหาคม 2566

เวลา 10.30 – 12.00 น.

ห้องประชุม ❍ Grand Ballroom

⊘ ห้องประชุม 1 ❍ ห้องประชุม 2 ❍ ห้องประชุม 3

โดย ดร. มัชฌิกา อ่องแตง

อาจารย์ประจำ คณะวิศวกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

ตั้งแต่อดีตจนถึงปัจจุบันมีการโจมตี cyber attack ตลอดเวลา ทั่วโลก โดยเฉพาะอย่างยิ่งมีการดาวน์โหลดและส่งผ่านข้อมูลทาง network จะถูกโจมตีจาก hackers เป้าหมายของระบบความมั่งคงปลอดภัย (Security Goals) ประกอบด้วย การปกปิด รักษาความลับ (Confidentiality) การรักษาการคงสภาพ/ป้องกันการแอบเขียน (Integrity) พร้อมใช้งาน (Availability) เป็นต้นตนอย่างถ่องแท้/ห้ามปลอม (Authenticity) และป้องกันการปฏิเสธการทำธุรกรรม (Non-repudiation) ต้องรู้ว่ามีช่องโหว่อะไร (Vulnerability) มีช่องทางการนำมาใช้ประโยชน์ (exploit) และมีแนวทางการโจมตี (Threat) จะเกิดความเสี่ยงที่จะมีการละเมิด Security goals และเมื่อมีการโจมตี (attack) ระบบสำเร็จ จะทำให้ระบบทำงานไม่สมบูรณ์ (system compromised) กระทบ Assets (ทรัพย์สิน ข้อมูล เวลา ความน่าเชื่อถือ)

ความเสี่ยงเป็นแนวโน้มที่จะเข้ามากระทบ assets ว่ามีมูลค่าขนาดไหน ผ่านช่องโหว่ (ควบคุมได้) และการโจมตี (ควบคุมไม่ได้) จึงจำเป็นต้องมี 1) การบริหารจัดการความเสี่ยง (Risk management) เริ่มจากประเมินความเสี่ยง (risk assessment) 2) กำหนดแนวทางการจัดการ (risk treatment) โดยการลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ หลีกเลี่ยงความเสี่ยง ปิดช่องทางการใช้งานที่ไม่ได้ใช้ ยอมรับความเสี่ยง (risk acceptance) โอนถ่ายไปให้คนอื่นดูแล/ซื้อประกันภัยไซเบอร์ และ 3) ดำเนินการตอบโต้ (response)

ISO 27001 Information Security Management System (ISMS) Requirement เป็นกรอบในการบริการจัดการความเสี่ยง มีระบบในการบริหารจัดการความมั่นคงปลอดภัยตามเกณฑ์มาตรฐาน ประกอบด้วยกระบวนการที่ช่วยในการประเมินความเสี่ยง พัฒนาแผนบำบัดความเสี่ยง และมีกลไกควบคุมด้านความปลอดภัยที่

จะช่วยควบคุมบำบัดความเสี่ยง เริ่มจากประเมินความเสี่ยง ทำ risk treatment plan สุดท้ายดูความเสี่ยงคงเหลือหลังบำบัดความเสี่ยงว่าอยู่ในระดับที่ยอมรับได้หรือไหม ผ่านกระบวนการ Plan Do Check Act

กระบวนการวางแผน ต้องเข้าใจบริบทขององค์กร พิจารณาความเสี่ยง ISMS ตามที่จะ verified ประเมินความเสี่ยง บันทึกเกี่ยวกับกระบวนการ และบำบัดความเสี่ยง (risk treatment process) ได้แผนงาน ทั้งนี้การประเมินความเสี่ยง ต้องจัดทำหลักเกณฑ์ ระบุความเสี่ยงและหน่วยงานไหนเป็นคนดูแล ประเมินระดับความเสี่ยง จัดลำดับความสำคัญ เมื่อได้ risk treatment plan แล้ว ต้องเลือก controls ในภาคผนวกท้ายเล่ม มีข้อไหนบ้างสามารถประยุกต์ใช้กับองค์กร (Statement of applicability) วาง risk treatment plan และรับการอนุมัติจาก risk owners

กรอบการทำงานด้านความมั่นคงปลอดภัยไซเบอร์ (NIST) เป็นกรอบการออกแบบและวางกลยุทธ์ให้ระบบรักษาความปลอดภัยทางไซเบอร์ ประกอบด้วย 1) Identify (ID) ระบุและเข้าใจถึงบริบทต่างๆ 2) Protect (PR) วางมาตรฐานควบคุม เพื่อปกป้องระบบ 3) Detect (DE) กำหนดขั้นตอนและกระบวนการต่างๆ เพื่อตรวจจับสถานการณ์ผิดปกติ 4) Respond (RS) กำหนดขั้นตอนและต่างๆ เพื่อรับมือกับสถานการณ์ผิดปกติที่เกิดขึ้น และ 5) Recover (RC) กำหนดขั้นตอนและกระบวนการต่างๆ เพื่อให้ธุรกิจสามารถดำเนินได้อย่างต่อเนื่อง ใน พ.ร.บ. ไซเบอร์ดำเนินการตาม NIST มาใช้อ้างอิง

Data Leak Protection ใช้ในการป้องกันการรั่วไหลข้อมูล มีการตั้งเป็นกฎในการควบคุมข้อมูล DLP จะแสกนข้อมูลที่ไม่เป็นไปตามกฎ แจ้งเตือนไปยังผู้ดูแลข้อมูล และผู้ดูแลข้อมูลประเมินอนุญาตหรือไม่อนุญาต

ดังนั้นผู้บริหารองค์กรต้องเข้าใจและให้ความสำคัญต่อการระบบการ ระบบในการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ ทั้งการประเมินความเสี่ยง กำหนดแนวทางการจัดการ และดำเนินการตอบโต้ โดยมีแผนในการจัดการความเสี่ยง ผ่านกระบวนการ PDCA

ชื่อ-สกุล นางสาวนาฎอนงค์ เจริญสันติสุข
นายนายธิติพันธ์ นำก้าวหน้า
บันทึกการประชุม