การประเมินระดับความเสี่ยงด้านไซเบอร์และการบริหารความเสี่ยงด้านไซเบอร์ภายในองค์กร

ปัจจุบันเทคโนโลยีและระบบสารสนเทศ เป็นเครื่องมือสำคัญต่อการขับเคลื่อนธุรกิจและองค์กรให้มีความก้าวหน้าและรวดเร็ว รวมทั้งการเปลี่ยนแปลงธุรกิจให้เข้าสู่สังคมดิจิทัล (Transformation) ทำให้ธุรกิจและองค์กรเหล่านั้นต้องเผชิญกับความเสี่ยงจากภัยคุกคามทางไซเบอร์ (Cyber Threats) ที่มากขึ้น การรักษาความมั่นคงปลอดภัยต่อภัยคุกคามทางไซเบอร์ จึงมีบทบาทที่สำคัญต่อธุรกิจและองค์กรเป็นอย่างมาก การมีความมั่นคงปลอดภัยจากภัยคุกคามทางไซเบอร์ที่มีความรัดกุมต่อระดับความเสี่ยง เพื่อเตรียมความพร้อมในการรับมือกับภัยคุกคาม ทางไซเบอร์รวมถึงการบริหารความเสี่ยงทั้งด้านบุคลากร กระบวนการ และเครื่องมือเทคโนโลยีสารสนเทศ เพื่อช่วยเพิ่มความมั่นใจและมั่นคงต่อผู้ใช้บริการทั้งภาครัฐและภาคประชาชน โดยหลักเกณฑ์กำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศ ประกอบด้วย ๒ ส่วนสำคัญ ได้แก่

๑. การรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศขั้นต้นที่จำเป็น (Cyber Hygiene) ซึ่งเป็นมาตรการขั้นต้นเพื่อยกระดับความมั่นคงปลอดภัยในการป้องกันและรับมือภัยคุกคามทางไซเบอร์ที่สำคัญทั้งภายในและภายนอก

๒. การบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ (IT risk management) ซึ่งมุ่งเน้นให้มีคุณสมบัติตามหลักเกณฑ์การบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศที่เหมาะสม มีโครงสร้างองค์กร องค์ประกอบและการกำหนดบทบาทหน้าที่ของผู้ดูแล เพื่อกำหนดนโยบายในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ครอบคลุมตลอดจนกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศให้สอดคล้องกับลักษณะการให้บริการหรือดำเนินธุรกิจในการกำกับดูแลการดำเนินงานและการบริหารความเสี่ยงด้านไซเบอร์สอดคล้องตามหลัก 3-Lines of Defense ซึ่งเป็นเครื่องมือมาตรฐานสากลมาตรการตรวจสอบ

จุดประสงค์สำคัญของ “Lines of Defense Model” คือหลักการควบคุมดูแลแบบเป็นลำดับขั้นให้เป็นไปตามกฎระเบียบขั้นตอน โดย 3 Lines of Defense ประกอบไปด้วยส่วนที่เป็น 1st Line of Defense , 2nd Line of Defense และ 3rd Line of Defense ซึ่งกระบวนการในแต่ละระดับ (Line) โดยก่อให้เกิดกระบวนการกำกับดูแลที่ดีมีประสิทธิภาพและเป็นส่วนหนึ่งของการบริหารตามกรอบการบริหารจัดการความเสี่ยงในภาพรวมขององค์กร (enterprise wide risk) รวมถึงมีบุคลากรที่มีความรู้และความเชี่ยวชาญเพียงพอในการปฏิบัติงานและบุคลากรทุกระดับมีความตระหนักถึงการรักษาความมั่นคงปลอดภัยไซเบอร์โดยคณะกรรมการสถาบันการเงินมีบทบาทและหน้าที่ความรับผิดชอบในการดูแลให้มีกลยุทธ์และนโยบายรวมทั้งดูแลให้มีกลไกในการกำกับดูแลและติดตามให้มีการรักษาความมั่นคงปลอดภัยไซเบอร์

๑. ความเสี่ยงทางไซเบอร์คืออะไร

ความเสี่ยงทางไซเบอร์คือแนวโน้มที่จะได้รับผลกระทบจากการหยุดชะงักต่อข้อมูลที่ละเอียดอ่อน การเงิน หรือการดำเนินธุรกิจออนไลน์ รวมถึงการให้บริการบางอย่างที่มีความเกี่ยวข้องต่อการดำเนินธุรกิจและการให้บริการประชาชน โดยทั่วไปความเสี่ยงทางไซเบอร์มีความเกี่ยวข้องกับเหตุการณ์ที่อาจส่งผลให้เกิดการละเมิดข้อมูล การขโมยข้อมูล หรือการทำลายข้อมูลเพื่อให้ไม่สามารถให้บริการได้ ความเสี่ยงทางไซเบอร์นั้นเป็นภัยคุกคามด้านความปลอดภัยต่อการดำเนินงานของธุรกิจและองค์กร ตัวอย่างของความเสี่ยงทางไซเบอร์ ได้แก่

๑.๑ Ransomware (แรนซัมแวร์) ซึ่งเป็นหนึ่งในมัลแวร์ที่มีวัตถุประสงค์ที่มุ่งเน้นในการโจมตีข้อมูล ไฟล์ และเอกสารภายในระบบสารสนเทศของเป้าหมายโดยวิธีการเข้ารหัสข้อมูลด้วยวิธีการต่าง ๆ เช่น การเข้ารหัสด้วย Advanced Encryption Standard (AES) ซึ่งเป็นหนึ่งในมาตรฐานการเข้ารหัสที่ได้รับความเชื่อถือในอุตสาหกรรมและองค์กรต่าง ๆ ที่ต้องการสร้างความมั่นใจและความปลอดภัยของข้อมูลเพื่อไม่ให้ผู้อื่นสามารถล่วงรู้ความลับของข้อมูลได้ ด้วยเหตุนี้จึงทำให้ผู้ไม่หวังดีได้มีการพัฒนามัลแวร์ได้มีการเอาประโยชน์ของการเข้ารหัสนี้มาใช้ประโยชน์ด้วยการเข้ารหัสข้อมูลของเป้าหมายทำให้ไม่สามารถเข้าใช้ข้อมูลได้จนกว่าจะจ่ายค่าไถ่ข้อมูลให้กับผู้พัฒนา Ransomware

๑.๒ Data leaks (ข้อมูลรั่วไหล) ข้อมูลรั่วไหลเกิดขึ้นเมื่อมีข้อมูลที่ละเอียดอ่อนหรือข้อมูลที่เป็นความลับถูกเปิดเผยโดยไม่ได้ตั้งใจบนอินเทอร์เน็ตหรือรูปแบบอื่นใด การนำข้อมูลออกโดยอาจบันทึกผ่าน Flash drive External Hard disk หรือผ่านเครื่องคอมพิวเตอร์พกพาและเกิดการสูญหายซึ่งอาจเกิดความเสี่ยงที่ผู้ไม่หวังดีสามารถเข้าถึงข้อมูลที่ละเอียดอ่อน

๑.๓ Phishing (ฟิชชิง) คือการโจมตีรูปแบบหนึ่งที่หลอกให้เป้าหมายกรอกข้อมูลส่วนบุคคล ข้อมูลที่เป็นความลับ ข้อมูลทางการเงิน ข้อมูลบัตรประชาชน ด้วยวิธีการต่าง ๆ เพื่อให้เป้าหมายส่งข้อมูลนั้นให้กับผู้ไม่หวังดี เช่นการส่งอีเมลหลอกเป้าหมาย “คุณมีการถอนเงินเป็นจำนวนหนึ่ง หากไม่ใช่กรุณาคลิกลิงก์ด้านล่างนี้เพื่อ ยกเลิกการทำรายการ” หรือ “คุณเป็นผู้โชคดีได้รับ iPhone ฟรีเพียงแค่กรอกข้อมูลในนี้” และเมื่อเป้าหมายส่งข้อมูลให้กับผู้ไม่หวังดีถูกนำข้อมูลไปดำเนินการเข้าถึงข้อมูลส่วนอื่น ๆ ของเป้าหมาย เช่นข้อมูลการเงิน ข้อมูลรหัสระบบต่าง ๆ ที่เป็นข้อมูลส่วนบุคคล

๑.๔ Malware (มัลแวร์) หรือ Malicious Software (ซอฟต์แวร์อันตราย) คือซอฟต์แวร์ที่พัฒนาโดยผู้ไม่หวังดีเพื่อขโมยข้อมูลและสร้างความเสียหายให้กับระบบคอมพิวเตอร์ โดยมัลแวร์นั้นได้แบ่งออกเป็นหลายประเภท เช่น

(๑) Virus (ไวรัส) เป็นซอฟต์แวร์ที่เป็นอันตรายต่อระบบสารสนเทศเป็นอย่างซึ่งโดยมุ่งเน้นในการโจมตี ขัดขวางเพื่อไม่ให้ระบบสามารถใช้งานได้

(๒) Worms (เวิร์ม) เป็นซอฟต์แวร์ที่เป็นอันตรายต่อระบบสารเทศที่มีการเชื่อมต่อผ่านระบบเครือข่ายทั้งภายในและภายนอกโดยซอฟต์แวร์ชนิดนี้มุ่งเน้นเพื่อการโจมตี ขัดขวางการทำงานและขยายตัวส่งต่อภายในระบบเครือข่ายจนทำให้ไม่สามารถใช้งานระบบสารสนเทศได้

(๓) Trojan (โทรจัน) เป็นซอฟต์แวร์ที่มีเป้าหมายการดักจับเปลี่ยนแปลงแก้ไขข้อมูลซึ่งอาจส่งผลต่อความถูกต้องของข้อมูลภายในระบบสารสนเทศหรืออาจเกิดความเสียหายภายในระบบสารสนเทศได้

(๔) Spyware (สปายแวร์) ซอฟต์แวร์ประสงค์ร้ายที่ทำงานอย่างลับๆ บนคอมพิวเตอร์และรายงานกลับไปยังผู้ใช้ระยะไกล โดยสปายแวร์มุ่งเน้นเพื่อขโมยข้อมูลทางการเงินหรือข้อมูลส่วนบุคคล

(๕) Adware (แอดแวร์) คือซอฟต์แวร์ที่รวบรวมข้อมูลการใช้งานระบบคอมพิวเตอร์และจัดเตรียมโฆษณาให้กับเป้าหมาย ถึงแม้ว่าแอดแวร์อาจไม่เป็นอันตราย แต่ในบางกรณีแอดแวร์อาจทำให้เกิดปัญหากับระบบสารสนเทศ ซึ่งแอดแวร์สามารถเปลี่ยนแปลงเส้นทางการเข้าถึงเว็บไซต์ไปสู่เว็บไซต์ที่ไม่ปลอดภัย

(๖) Ransomware (แรนซัมแวร์) คือซอฟต์แวร์ที่มีวัตถุประสงค์ที่มุ่งเน้นในการโจมตีข้อมูล ไฟล์ และเอกสารภายในระบบสารสนเทศของเป้าหมายโดยวิธีการเข้ารหัสข้อมูล ไฟล์และเอกสารเพื่อไม่ให้เป้าหมายสามารถใช้งาน

(๗) Insider threats (ภัยคุกคามจากภายใน) คือภัยคุกคามจากภายในอาจเกิดขึ้นได้กับคนใกล้ชิดภายในองค์กรที่ได้รับอนุญาตในการเข้าถึงข้อมูลที่เป็นความลับซึ่งการเข้าถึงอาจส่งผลเสียต่อข้อมูลหรือระบบที่สำคัญขององค์กร โดยภัยคุกคามชนิดนี้อาจจะเป็นพนักงาน ผู้ขาย ผู้รับเหมา หุ้นส่วนหรือบุคคลที่มีความใกล้ชิด โดยความเสี่ยงและช่องโหว่ทางไซเบอร์นั้นมีวิธีการในการทำงานที่แตกต่างกัน โดยช่องโหว่ถือเป็นจุดอ่อนที่ส่งผลให้เกิดการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาตจากผู้ไม่หวังดีที่อาจก่อให้เกิดความเสี่ยงทางไซเบอร์ภายในระบบสารสนเทศของธุรกิจและองค์กร

การประเมินความเสี่ยงด้านความปลอดภัยทางไซเบอร์ การประเมินความเสี่ยงด้านความปลอดภัยทางไซเบอร์ช่วยให้ธุรกิจและองค์กรเข้าใจ ควบคุม และลดความเสี่ยงทางไซเบอร์ทุกรูปแบบ ที่เป็นองค์ประกอบสำคัญของการบริหารความเสี่ยงและลดความเสี่ยง หากไม่มีการประเมินความเสี่ยงการรักษาความปลอดภัยทางไซเบอร์ อาจส่งผลกระทบต่อข้อมูลและทรัพยากรสำคัญใน การดำเนินการอยู่ของธุรกิจและองค์กรได้ การใช้มาตรการรักษาความปลอดภัยทางไซเบอร์ มีวิธีการคำนวณตาม OWASP Risk Assessment โดยมีขั้นตอนการประเมินความเสี่ยงดังนี้

๑. ระบุความเสี่ยง คือการระบุถึงความเสี่ยงที่จะเกิดขึ้นกับระบบสารสนเทศ

๒. ปัจจัยในการประมาณความน่าจะเป็น คือปัจจัยที่สามารถช่วยกำหนดความน่าจะเป็นได้ ซึ่งมีความเกี่ยวข้องกับภัยคุกคาม

๓. ปัจจัยในการประเมินผลกระทบ คือปัจจัยที่ส่งผลกระทบการทำงานของระบบสารสนเทศ

๔. การกำหนดความรุนแรงของความเสี่ยง คือความรุนแรงที่อาจส่งผลกระทบต่อระบบสารสนเทศ

๕. ตัดสินใจว่าจะแก้ไขในอนาคตหรือไม่ คือมีแนวโน้มที่จะแก้ไขช่องโหว่ที่เกิดขึ้นนี้ในอนาคตหรือไม่

๖. การจำลองการประเมินความเสี่ยง คือการมีกรอบการจัดลำดับความเสี่ยงที่ปรับแต่งได้สำหรับธุรกิจเป็นสิ่งสำคัญสำหรับการนำไปใช้

๒. ความรุนแรง

เมื่อเข้าสู่ขั้นตอนการประเมินความเสี่ยงต่อภัยคุกคามทางไซเบอร์ โดยคำนึงถึงจุดอ่อนที่มีระดับความเสี่ยงต่ำหมายถึงจุดอ่อนมีความรุนแรงต่ำ จุดอ่อนที่มีความเสี่ยงสูงหมายถึงจุดอ่อนที่อาจก่อให้เกิดความเสียหายต่อระบบสารสนเทศสูงหรือมีระดับความรุนแรงสูง และง่ายต่อการโจมตี โดยใช้หลักการวิเคราะห์ความรุนแรงของช่องโหว่และการประเมินความเสี่ยง ดังนี้

๒.๑ ความเสี่ยงมาก ช่องโหว่สามารถขัดขวาง หรือยุติการให้บริการ หรือทำให้ข้อมูลเสียหายได้

๒.๒ ความเสี่ยงปานกลาง ช่องโหว่ไม่สามารถทำให้ระบบหยุดการให้บริการได้ หรือจำเป็นจะต้องอาศัยช่องโหว่อื่น ๆ ช่วยในการทำให้ระบบยุติการให้บริการ

๒.๓ ความเสี่ยงต่ำ ช่องโหว่ไม่สามารถยุติการให้บริการได้ แต่ทำให้ได้ข้อมูลพื้นฐานเกี่ยวกับการให้บริการ

ซึ่งการประเมินความเสี่ยงทางไซเบอร์ถูกกำหนดโดยสถาบันมาตรฐานและเทคโนโลยีแห่งชาติ (NIST) เป็นการประเมินความเสี่ยงที่ใช้ในการระบุ การประมาณการและการจัดลำดับความสำคัญของความเสี่ยง ต่อการดำเนินงานของธุรกิจและองค์กร สินทรัพย์ของธุรกิจและองค์กร บุคคล ธุรกิจและองค์กรอื่นๆ และประเทศ ซึ่งเป็นผลมาจากการดำเนินงานและการใช้ระบบสารสนเทศ วัตถุประสงค์หลักของการประเมินความเสี่ยงทางไซเบอร์คือ การแจ้งให้ผู้มีส่วนได้ส่วนเสียทราบและสนับสนุนการตอบสนองที่เหมาะสมต่อความเสี่ยงที่เกิดขึ้น พร้อมสามารถสรุปข้อมูลสำคัญสำหรับผู้บริหาร เพื่อช่วยผู้บริหารและกรรมการในการตัดสินใจเกี่ยวกับการรักษาความปลอดภัย

๓. กรอบการบริหารความเสี่ยงทางไซเบอร์โดยสถาบันมาตรฐานและเทคโนโลยีแห่งชาติ (NIST)

NIST Cyber Security Framework Functions ช่วยให้สามารถสร้างกลยุทธ์การป้องกันความเสี่ยงทาง ไซเบอร์และลดความเสี่ยงทางไซเบอร์พร้อมทั้งการบริหารความเสี่ยงทางไซเบอร์ซึ่งมีองค์ประกอบดังนี้

๓.๑ Identify ฟังก์ชันการระบุช่วยในการพัฒนาความเข้าใจในธุรกิจและองค์กรเกี่ยวกับการจัดการความเสี่ยงต่อระบบ บุคคล สินทรัพย์ ข้อมูล และความสามารถ วัตถุประสงค์หลักเพื่อระบุบุคคล กระบวนการ หรือระบบทั้งหมดที่อาจเสี่ยงต่อภัยคุกคามประเภทนี้

๓.๒ Protect ฟังก์ชันป้องกันสนับสนุนความสามารถในการจำกัดหรือควบคุมผลกระทบของภัยคุกคาม วัตถุประสงค์หลักเพื่อจำกัดการคุกคามของการโจมตีได้อย่างไรโดยการลบหรือบล็อกช่องโหว่

๓.๓ Detect ฟังก์ชันตรวจจับกำหนดกิจกรรมเพื่อระบุเหตุการณ์ที่เกิดขึ้นในเวลาที่เหมาะสม วัตถุประสงค์หลักเพื่อหากไม่สามารถหยุดการคุกคามได้ (เช่น ขั้นตอนการป้องกัน) จะรู้ได้อย่างไรว่าสิ่งที่กำลังเกิดขึ้น และธุรกิจและองค์กรกำลังประสบกับอันตรายทางภัยคุกคามทางไซเบอร์

๓.๔ Respond ฟังก์ชันตอบสนองรวมถึงกิจกรรมที่เหมาะสมเกี่ยวกับภัยคุกคามทางไซเบอร์เพื่อลดผลกระทบ วัตถุประสงค์หลักเพื่อตระหนักถึงภัยคุกคาม ป้องกันความเสียหายที่เกิดขึ้นเพิ่มเติม ความเสียหายต่อชื่อเสียง หรือการละเมิดความเป็นส่วนตัว

๓.๕ Recover ฟังก์ชันการกู้คืนประกอบด้วยการระบุกิจกรรมที่เหมาะสมเพื่อรักษาแผนสำหรับความยืดหยุ่นและเพื่อกู้คืนบริการที่บกพร่องระหว่างเหตุการณ์ด้านความปลอดภัยทางไซเบอร์ที่เกิดขึ้น วัตถุประสงค์หลักเพื่อให้สิ่งที่เกิดขึ้นกลับสู่ในสภาพที่เท่าเทียมหรือดีกว่าก่อนเกิดเหตุ

๔. สรุป

การบริหารความเสี่ยงด้านความปลอดภัยทางไซเบอร์คือ แนวปฏิบัติในการจัดลำดับความสำคัญของ มาตรการป้องกันความปลอดภัยทางไซเบอร์ โดยพิจารณาจากผลกระทบที่อาจเกิดขึ้นจากภัยคุกคามที่ออกแบบ มาเพื่อใช้ในการโจมตีเป้าหมาย การสร้างแนวทางการบริหารความเสี่ยง เพื่อการสร้างความมั่นคงด้านความปลอดภัยทางไซเบอร์ ซึ่งธุรกิจและองค์กรที่เกิดขึ้นใหม่ อาจไม่สามารถกำจัดช่องโหว่ของระบบทั้งหมดหรือบล็อกการโจมตี ทางไซเบอร์ได้ทั้งหมด ผ่านการจัดการความเสี่ยงด้านความปลอดภัยทางไซเบอร์ ธุรกิจและองค์กรควรให้ความสำคัญกับข้อบกพร่องของระบบ แนวโน้มภัยคุกคาม และการโจมตีที่สำคัญที่สุดต่อธุรกิจก่อน โดยการจัดทำกรอบการบริหารความเสี่ยงทางไซเบอร์ซึ่งเป็นกรอบงานความปลอดภัยทางไซเบอร์ของสถาบันมาตรฐานและเทคโนโลยีแห่งชาติ (NIST) เป็นหนึ่งในกรอบการจัดการความเสี่ยงด้านความปลอดภัยทางไซเบอร์ ที่ได้รับความนิยมมากที่สุดในอุตสาหกรรม NIST จัดทำแผนที่แบบ end-to-end ของกิจกรรมและผลลัพธ์ที่เกี่ยวข้อง ๕ ฟังก์ชันของการจัดการความเสี่ยงด้านความปลอดภัยทางไซเบอร์คือ ระบุ **ปกป้อง ตรวจจับ ตอบสนอง และกู้คืน** ซึ่งเป็นส่วนสำคัญต่อการดำเนินงานของธุรกิจและองค์กรในยุคดิจิทัล ๔.๐