สรุปความรู้ที่ได้จากการพัฒนาความรู้ผ่านระบบ (e-Learning)
การสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์ cyber security awareness

โดยคุณพลากร ลาภอลงกรณ์
จากสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
Thailand Digital Government Academy

Cyber Security คือ ความมั่นคงปลอดภัยทางไซเบอร์ ที่ต้องการป้องกันและการรักษาความปลอดภัยของระบบคอมพิวเตอร์ ระบบเครือข่าย และข้อมูลที่เกี่ยวข้อง โดยประกอบไปด้วย ระบบสารสนเทศ (Information System) โปรแกรมประยุกต์ (Application) ข้อมูล (Data) ระบบคอมพิวเตอร์หรือเครื่องมือที่ใช้ในการเข้าระบบเครือข่าย (Mobile Phone, Tablet, TV, IoT) หน่วยบันทึกข้อมูลและอุปกรณ์เครือข่าย (Storage, Network Device) ศูนย์ข้อมูล (Data Center) รวมถึงกระบวนการบริหารจัดการด้านความมั่นคงปลอดภัยที่เกี่ยวข้องกับความปลอดภัยของระบบคอมพิวเตอร์โดยเฉพาะระบบเครือข่ายอินเตอร์เน็ต ซึ่งมีจุดประสงค์ คือ เพื่อป้องกันการเข้าถึง การแก้ไข การเปลี่ยนแปลง หรือการทำลายข้อมูลจากบุคคลที่ไม่ได้รับอนุญาต หรือบุคคลที่ต้องการเข้าถึงข้อมูลเพื่อวัตถุประสงค์ที่ไม่เหมาะสม ดังนั้นหลายๆองค์กรจึงให้ความสำคัญเรื่องระบบรักษาความปลอดภัยของข้อมูลไม่แพ้กัน เพราะหากลูกค้าหรือผู้ใช้บริการโดนโจรกรรมข้อมูลทางอิเล็กทรอนิกส์ไป อาจทำให้องค์กรเสียหายหรือเสียชื่อเสียงได้

ความสำคัญของ Cyber Security

๑. ความสุ่มเสี่ยงต่อการถูกโจรกรรมทางไซเบอร์จากการศึกษาของ University of Maryland พบว่าระบบคอมพิวเตอร์ทั่วโลกมีแฮกเกอร์พยายามเข้าถึงและโจมตีระบบในระยะเวลาเพียง ๓๙ วินาทีโดยประมาณหรือประมาณ ๒,๒๔๔ ครั้งต่อวัน ดังนั้นองค์กรจะต้องให้ความสำคัญกับการเก็บข้อมูล โดยเฉพาะข้อมูลส่วนบุคคลของลูกค้า ข้อมูลทางการเงิน ทรัพย์สินทางปัญญา และข้อมูลสำคัญระดับประเทศ เป็นต้น หากไม่มีระบบการป้องกันทางไซเบอร์ที่เข้มงวด แฮกเกอร์อาจสามารถเข้าถึงและนำข้อมูลไปใช้งานได้อย่างง่ายดาย

๒. การรั่วไหลของข้อมูลหากองค์กรไม่มีระบบการป้องกันและรักษาความปลอดภัยของข้อมูลที่มีประสิทธิภาพเพียงพอ อาจทำให้เกิดการรั่วไหลของข้อมูลสำคัญ โดยเฉพาะข้อมูลส่วนบุคคล (Personal Data) และข้อมูลส่วนบุคคลที่มีความอ่อนไหว (Sensitive Personal Data) อาจถูกเปิดเผยหรือนำไปใช้งานอย่างไม่เหมาะสมที่อาจก่อให้เกิดความเสียหายมหาศาลตามมาได้

๓. องค์กรเสียชื่อเสียงเมื่อเกิดเหตุการณ์ที่องค์กรไม่สามารถรักษาความปลอดภัยของข้อมูลได้ จนทำให้บุคคลภายนอกสามารถเข้าถึงหรือเปิดเผยข้อมูล อาจส่งผลกระทบร้ายแรงต่อองค์กร เช่น สูญเสียค่าใช้จ่ายมหาศาลในการแก้ไขสถานการณ์เฉพาะหน้าและซื้อข้อมูลที่ถูกขโมยไปกลับมา หรือแม้กระทั่ง ชื่อเสียงเกี่ยวกับความปลอดภัยขององค์กรก็จะเสื่อมถอยลง ทำให้เกิดภาพลักษณ์ไม่ดีต่อองค์กรและยากที่จะกู้คืนความเชื่อมั่นของผู้ใช้บริการให้กลับมาเชื่อมั่นในองค์กรเหมือนเดิม

Cyber Security มี ๕ ประเภท

๑. Critical Infrastructure Security เป็นการรักษาความปลอดภัยของระบบโครงสร้างพื้นฐานที่สำคัญ การสร้างระบบความปลอดภัยที่เหมาะสมเป็นสิ่งจำเป็น เนื่องจากหากไม่มีการป้องกันอย่างเหมาะสม อาจเกิดความเสี่ยงที่จะถูกโจมตีมากกว่ารูปแบบอื่น โดยเฉพาะระบบรักษาความปลอดภัยของธนาคาร ตลาดหลักทรัพย์ รัฐบาล ที่มีข้อมูลส่วนบุคคลอยู่เป็นจำนวนมาก หรือแม้กระทั่งข้อมูลทางการเงินก็นับว่าเป็นข้อมูลละเอียดอ่อน ที่การรักษาความปลอดภัย Critical Infrastructure Security จะต้องทำโครงสร้างออกมาให้แข็งแรง เพื่อป้องกันข้อมูลได้ดียิ่งขึ้น

๒. Network Security คือการรักษาความปลอดภัยของระบบเครือข่ายอินเทอร์เน็ต ซึ่งเป็นการป้องกันการคุกคามจากบุคคลภายนอกที่พยายามเข้าถึงและใช้งานระบบเครือข่ายอินเทอร์เน็ตโดยไม่ได้รับอนุญาต ร่วมกับการนำเทคโนโลยีและระบบปัญญาประดิษฐ์มาช่วยเพื่อตรวจจับและแจ้งเตือนเกี่ยวกับความผิดปกติที่เกิดขึ้นในส่วนนี้

๓. Cloud Security หากองค์กรตัดสินใจเก็บข้อมูลต่าง ๆ ในเซิร์ฟเวอร์ภายในบริษัท จะมีความเสี่ยงที่ข้อมูลอาจถูกโจมตีได้ การโอนย้ายข้อมูลเพื่อจัดเก็บบน Cloud Security เป็นตัวช่วยที่สามารถเพิ่มความปลอดภัยและประหยัดค่าใช้จ่ายได้มากขึ้น อีกทั้งในปัจจุบันระบบความปลอดภัยของคลาวด์ก็มีการพัฒนาและปรับปรุงอย่างต่อเนื่อง ทำให้เหมาะสมกับความต้องการและเป็นทางเลือกที่ดีในการใช้งาน

๔. Application Security ในกระบวนการพัฒนาหรือติดตั้งแอปพลิเคชัน อาจเกิดการโจมตีหรือการแฝงตัวเข้ามาได้ ดังนั้นการเลือกใช้ตัวช่วยในการรักษาความปลอดภัยผ่านแอปพลิเคชันเป็นทางเลือกที่ดีเพื่อเพิ่มระดับความปลอดภัยให้กับกระบวนการพัฒนาระบบได้อีกวิธีหนึ่ง

๕. Internet of Things Security การรักษาความปลอดภัยบนอุปกรณ์ Internet of Things (IoT) ที่มีการใช้งานตลอดเวลาเป็นเรื่องสำคัญ เนื่องจากระบบ IoT มีการส่งรับข้อมูลผ่านเครือข่ายอินเทอร์เน็ต ดังนั้นจำเป็นต้องมีการกำหนดมาตรการที่เหมาะสมเพื่อรักษาความปลอดภัยบนอุปกรณ์เหล่านี้ให้มีประสิทธิภาพและป้องกันการเข้าถึงที่ไม่ได้รับอนุญาต

๕ เหตุผลที่องค์กรต้องทำระบบ Cyber Security

ซึ่งแม้จะไม่ได้เห็นผลลัพธ์เป็นมูลค่า แต่ก็นับว่าเป็นการลงทุนที่สำคัญและคุ้มค่ามากที่สุด เพื่อป้องกันก่อนที่จะเกิดความเสียหายทั้งในด้านข้อมูลส่วนบุคคล ข้อมูลธุรกิจ สูญเสียค่าใช้จ่ายมหาศาลจากการโจมตี รวมถึงความเสียหายทางด้านภาพลักษณ์ขององค์กร

๑. เพื่อปกป้องข้อมูลขององค์กรและข้อมูลส่วนบุคคลไม่ให้ถูกนำไปใช้ในทางทุจริต การสร้างระบบ Cybersecurity ที่รัดกุมและครอบคลุมตั้งแต่การป้องกัน ไปจนถึงการวางแผนระยะยาว คือส่วนสำคัญที่จะช่วยให้องค์กรสามารถสกัดกั้นการโจมตีจากแฮกเกอร์ก่อนที่จะเข้ามาขโมยข้อมูลและนำไปใช้ในทางทุจริต ไม่ว่าจะเป็นการเข้าระบบเพื่อโจมตีให้ข้อมูลเสียหาย การขโมยข้อมูลลูกค้าไปขายหรือใช้ในการหลอกลวงเพื่อสร้างความเสียหายต่อบุคคล การนำข้อมูลไปใช้ปลอมแปลงเพื่อการทำธุรกรรม รวมทั้งการโจรกรรมข้อมูลเพื่อเรียกค่าไถ่ (Ransomware) เป็นต้น ซึ่งองค์กรควรมีการวางแนวทางและเตรียมความพร้อมทั้งในด้านเทคโนโลยี นโยบายขององค์กร และพนักงานในองค์กร เพื่อให้ระบบ Cybersecurity ทำงานได้อย่างมีประสิทธิภาพสูงสุด

๒. เพื่อป้องกันไม่ให้เกิดความเสียหาย ทั้งในด้านค่าใช้จ่ายและชื่อเสียงขององค์กร หากองค์กรถูกโจมตีทางไซเบอร์ แน่นอนว่าสิ่งที่ตามมานั้น คือความเสียหายทางด้านค่าใช้จ่ายที่อาจมีมูลค่ามหาศาล อย่างเช่น การโจรกรรมข้อมูลเพื่อเรียกค่าไถ่ด้วยวิธีการแอบลักลอบขนข้อมูลออกไปและติดตั้งมัลแวร์เพื่อเข้ารหัสข้อมูลไม่ให้เจ้าของข้อมูลสามารถใช้งานได้หากไม่ยอมจ่ายเงิน ที่เรียกว่า Ransomware หรืออาจเกิดค่าใช้จ่ายในการกู้คืนข้อมูลที่สูญหายไป รวมไปถึงความเสียหายในด้านชื่อเสียงขององค์กร ที่ประเมินค่าเป็นตัวเลขชัดเจนไม่ได้ แต่เรียกได้ว่าเป็นความเสียหายที่รุนแรงไม่แพ้กัน ซึ่งส่งผลให้องค์กรถูกมองในทางลบทั้งต่อผู้ลงทุน ลูกค้า รวมถึงพนักงานในองค์กรเอง การทำระบบ Cybersecurity จึงเป็นแนวทางสำคัญที่จะสามารถป้องกันไม่ให้เกิดความเสียหายเหล่านี้ได้

๓. เพื่ออุดช่องโห่วการป้องกันด้วยระบบสารสนเทศขั้นพื้นฐานรูปแบบเดิม ๆ ที่ไม่เพียงพอในการป้องกันภัยไซเบอร์สมัยใหม่ มาตรการทางสารสนเทศ (IT Policy) คือมาตรฐานในการป้องกันภัยคุกคามทางไซเบอร์ ซึ่งถือเป็นเกราะป้องกันภัยขององค์กรที่มีประสิทธิภาพและประสบความสำเร็จมาโดยตลอด แต่ปัจจุบันภัยคุกคามทางไซเบอร์มีการพัฒนารูปแบบการโจมตีที่มีความหลากหลายและซับซ้อนมากขึ้น ทำให้การป้องกันเพียงระบบสารสนเทศขั้นพื้นฐาน (Infrastructure Protection) เช่น การติดตั้ง Firewall, การแยก Zone ของระบบเครือข่าย อาจดีไม่เพียงพอสำหรับโลกในยุคปัจจุบันและเป็นช่องโหว่ให้เกิดการโจมตีได้ ซึ่งองค์กรควรวางระบบป้องกันที่ครอบคลุมมากขึ้น ตั้งแต่ระบบตรวจจับมัลแวร์หรือไวรัสที่ครอบคลุมทั้งระบบขององค์กร เช่น Antivirus, EDR (Endpoint Detection and Response) ระบบรวบรวมข้อมูลบันทึกและแจ้งเตือนจากอุปกรณ์ในองค์กรเพื่อการป้องกันและแจ้งเตือนที่ดียิ่งขึ้น เช่น SIEM (Security incident and event management)

๔. เพื่อสร้างความเชื่อมั่นให้กับลูกค้าและพันธมิตรที่ร่วมงานกับองค์กรสถิติการเกิดภัยคุกคามทางไซเบอร์ที่ค่อนข้างสูงทั้งในประเทศไทยและทั่วโลก ทำให้องค์กร หน่วยงาน รวมถึงประชาชนเองต่างเกิดความกังวลและเกิดคำถามว่าข้อมูลที่หมุนเวียนอยู่ในโลกดิจิทัลนั้นถูกปกป้องอย่างดีแล้วหรือยัง ดังนั้นองค์กรและธุรกิจจึงต้องเร่งสร้างความเชื่อมั่นด้านความปลอดภัยในข้อมูลให้ได้มากที่สุด ผ่านการวางระบบ Cybersecurity ที่ชัดเจนและได้ประสิทธิภาพ เพื่อเป็นการสร้างความมั่นใจให้กับพันธมิตรทางธุรกิจและลูกค้าผู้ใช้บริการที่ร่วมเดินทางไปพร้อมกับองค์กร

๕. ปฏิบัติตามพรบ. คุ้มครองข้อมูลส่วนบุคคล (PDPA) พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๒ หรือ PDPA คือข้อสำคัญที่ทำให้องค์กรต้องวางระบบความปลอดภัยในข้อมูลเพื่อดูแลและปกป้องข้อมูลของลูกค้า ข้อมูลผู้ใช้งาน หรือข้อมูลพนักงานในองค์กรให้ได้ประสิทธิภาพและปลอดภัยที่สุด เพราะถ้าหากองค์กรหรือหน่วยงานใดไม่ปฏิบัติตามจะทำให้เกิดบทลงโทษกฎหมาย ซึ่งมีทั้งโทษทางแพ่ง โทษทางอาญา และโทษทางปกครอง จึงเป็นเหตุผลให้องค์กรทั้งภาครัฐและเอกชน ต้องตระหนักและเพิ่มมาตรการการรักษาข้อมูล เพื่อป้องกันความเสียหายทั้งต่อบุคคล องค์กร และความเสียหายทางด้านโทษทางกฎหมาย

ประเภทของการโจมตีด้วยการแฮ็กข้อมูล

มีการโจมตีทางไซเบอร์ประเภทที่เป็นทั้งแบบเปิดเผยและแบบแอบแฝง ซึ่งพบบ่อยที่สุดมีอยู่ ๕ ประเภท

๑. มัลแวร์ (Malware) เป็นช่องโหว่ที่สามารถทะลุการปกป้องเครือข่ายของคุณเช่น สปายแวร์ (spyware) ไวรัสเรียกค่าไถ่ (ransomware) และไวรัสคอมพิวเตอร์ (viruses)

๒. ฟิชชิ่ง (Phishing) ข้อความเหล่านี้เป็นข้อความที่เป็นอันตราย (โดยส่วนมากที่พบคืออีเมล) ที่มีลิงก์ที่เป็นอันตราย ซึ่งเมื่อได้คลิกเข้าไปแล้ว จะทำการหลอกล่อให้คุณส่งข้อมูลที่ละเอียดอ่อนไปยังเป้าหมาย

๓. การปฏิเสธการให้บริการ (Denial of Service (DoS)) แฮกเกอร์มักทำการโจมตีเพื่อทำให้เครือข่าย หรือระบบของคุณ ที่มีข้อมูลส่วนเกิน จนล้นเครือข่าย และบังคับให้ระบบหยุดทำงาน

๔. เทคนิคคนกลาง (Man in the middle (MitM)) อาชญากรไซเบอร์ที่เข้ามาอยู่ระหว่างการเชื่อมต่อของคุณ ซึ่งมักจะกระทำผ่านเครือข่าย Wi-Fi สาธารณะที่ไม่ปลอดภัย และขโมยข้อมูลที่ละเอียดอ่อนของคุณไป

๕. การโจมตีแบบซีโร่เดย์ (Zero-day attack) พบได้น้อย แต่มากขึ้นเรื่อย ๆ การโจมตีทั่วไปที่เกิดขึ้นระหว่างรอการประกาศการอัปเดตความปลอดภัย หรือโปรแกรมแก้ไข และการติดตั้งดังกล่าว การโจมตีทางไซเบอร์เหล่านี้อาจส่งผลกระทบต่อธุรกิจจำนวนมาก เช่น คาเฟ่ที่มีเครือข่าย Wi-Fi ที่ไม่ปลอดภัย หรือร้านค้าออนไลน์ที่เสี่ยงต่อการถูกโจมตีแบบ Zero-day เป็นต้น

ความเข้าใจที่ผิด ต่อ Cyber Security

๑. เข้าใจผิดว่าเป็นเรื่องของฝ่ายไอทีเท่านั้น ไม่เกี่ยวกับฝ่ายอื่น

๒. เข้าใจผิดว่าภาครัฐจัดการให้ทั้งหมด

๓. เข้าใจผิดว่าเป็นเรื่องของความปลอดภัยของระบบเครือข่าย (Network) อย่างเดียว โดยไม่เกี่ยวข้องกับแอปพลิเคชั่นของผู้ใช้งาน (User Application)

๔. เข้าใจผิดว่ามีพาสเวิร์ดสำหรับการล็อกอินก็ปลอดภัยพอแล้ว

๕. เข้าใจผิดว่าเป็นเรื่องของการถูกโจมตีจากแฮ็คเกอร์ภายนอกเท่านั้น

๖. เข้าใจผิดว่าเป็นเรื่องไกลตัว ยังไม่ต้องรีบ

๗. เข้าใจผิดว่าเป็นการทำโครงการครั้งเดียวแล้วเลิก ไม่ต้องหมั่นซ้อม ไม่พัฒนาต่อเนื่อง

การบริหารจัดการด้านความมั่นคงปลอดภัยไซเบอร์ คือความสามารถในการเตรียมความพร้อมสำหรับการป้องกันความเสี่ยงทางไซเบอร์ทั้งจากการดำเนินการเอง และจากภัยคุกความทางไซเบอร์ประกอบไปด้วย

๑. การระบุเหตุการณ์ความเสี่ยงได้ครอบคลุม

๒. การกำหนดมาตรการป้องกันล่วงหน้า

๓. การตรวจจับข้อผิดพลาดหรือการตรวจจับการบุกรุกทางไซเบอร์

๔. การรับมือกับสถานการณ์ข้อผิดพลาด

๕. การคืนสภาพจากการความเสียหายที่เกิดขึ้นได้อย่างรวดเร็ว

ประโยชน์ที่ได้รับ

ประโยชน์ที่ได้รับและนำมาปรับใช้ในการปฏิบัติงาน คือ ทำให้ทราบถึงภัยคุกคามทางไซเบอร์ที่สำคัญ เพื่อที่จะได้ป้องกันไม่หลงเชื่อส่งข้อมูลส่วนตัวไปยังเป้าหมาย และยังช่วยเตือนผู้มารับบริการทั้งภายในและภายนอกหน่วยงานไม่ให้หลงเชื่อส่งข้อมูลส่วนตัวหลังได้รับอีเมลหรือข้อความ

นางสาวจิราพร วงษ์พาดกลาง
ตำแหน่ง นักทรัพยากรบุคคลปฏิบัติการ
กลุ่มทะเบียนประวัติและบำเหน็จความชอบ