สนค. เตือน “ภัยไซเบอร์–ระบบขัดข้อง” เป็นความเสี่ยงทางเศรษฐกิจยุคดิจิทัล แนะภาคธุรกิจใช้เทคโนโลยีตั้งรับควบคู่การบริหารความเสี่ยง

สนค. ย้ำชัด ภัยคุกคามทางไซเบอร์และความขัดข้องของระบบดิจิทัลเป็นหนึ่งในความเสี่ยงที่ส่งผลต่อการดำเนินธุรกิจและห่วงโซ่อุปทานโลก โดยเทคโนโลยีดิจิทัลและปัญญาประดิษฐ์ (AI) ยังคงเป็นกลไกสำคัญในการเพิ่มประสิทธิภาพและขีดความสามารถในการแข่งขัน แต่ผู้ประกอบการจำเป็นต้องรู้เท่าทันภัยคุกคาม มีมาตรการป้องกัน และเตรียมแผนสำรอง เพื่อรักษาความต่อเนื่องทางธุรกิจและความเชื่อมั่นทางการค้า

นายนันทพงษ์ จิระเลิศพงษ์ ผู้อำนวยการสำนักงานนโยบายและยุทธศาสตร์การค้า (ผอ.สนค.) กระทรวงพาณิชย์ เปิดเผยว่า สถานการณ์ภัยคุกคามทางไซเบอร์ที่เกิดขึ้นในช่วงหลายสัปดาห์ที่ผ่านมา สะท้อนให้เห็นว่า**การโจมตีได้ขยายวงกว้างจากการขโมยข้อมูล ไปสู่การแทรกแซงระบบธุรกรรมทางการเงิน การให้บริการดิจิทัล และระบบควบคุมอุปกรณ์ที่จำเป็นต่อการดำเนินธุรกิจ** ก่อให้เกิดความเสียหายทั้งด้านการเงิน การให้บริการ และสินค้าตลอดห่วงโซ่อุปทาน ตัวอย่างเช่น ในภาคการเงิน ธนาคาร Credit Mutuel Arkea ของฝรั่งเศสถูกโจมตีผ่านแพลตฟอร์มของผู้ให้บริการภายนอก ทำให้เกิดธุรกรรมโอนเงินที่ไม่ได้รับอนุญาตมูลค่าประมาณ 100 ล้านยูโร เช่นเดียวกับธนาคารซิโนแพค (Bank SinoPac) ของไต้หวันที่ตรวจพบธุรกรรมที่ไม่ได้รับอนุญาต 427 รายการ คิดเป็นมูลค่ารวม 41.76 ล้านดอลลาร์ไต้หวัน ขณะที่ภาคค้าปลีก พบการโจมตีระบบควบคุมอุปกรณ์ทำความเย็นของซูเปอร์มาร์เกตหลายแห่งในยุโรป ส่งผลให้อุณหภูมิตู้แช่เย็นและตู้แช่แข็งเพิ่มสูงขึ้นผิดปกติจนสินค้าอาหารได้รับความเสียหาย ส่วนภาคบริการ สวนสนุกฮ่องกงดิสนีย์แลนด์ (Hong Kong Disneyland) ถูกเจาะระบบจำหน่ายบัตรออนไลน์โดยไม่ได้รับอนุญาต ทำให้รหัส QR ของบัตรเข้าชมประมาณ 17,000 รายการถูกขโมย และต้องระงับการให้บริการชั่วคราว

นอกจากการโจมตีทางไซเบอร์แล้ว **ความขัดข้องของระบบจากปัญหาทางเทคนิคก็เป็นอีกความเสี่ยงที่ไม่ควรมองข้าม** เช่น เหตุการณ์ระบบ Microsoft 365 ขัดข้องทั่วโลกเมื่อวันที่ 12–13 พฤศจิกายนที่ผ่านมา ส่งผลให้ผู้ใช้งานในหลายประเทศไม่สามารถเข้าถึงบริการดิจิทัลบางส่วนได้ ซึ่งแม้ไม่ได้เกิดจากการโจมตีทางไซเบอร์ แต่สะท้อนให้เห็นถึงความเสี่ยงจากการพึ่งพาผู้ให้บริการเทคโนโลยีรายใหญ่ ซึ่งหากระบบขัดข้องก็อาจส่งผลกระทบต่อธุรกิจหลายแห่งพร้อมกัน

สำหรับประเทศไทย สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) รายงานว่า ช่วงมกราคม - ตุลาคม 2569 **มีเหตุการณ์ภัยคุกคามทางไซเบอร์เกิดขึ้นรวม 3,520 เหตุการณ์** โดยหน่วยงานด้านการศึกษาถูกโจมตีมากที่สุด 1,208 เหตุการณ์ (สัดส่วนร้อยละ 34.3) รองลงมาคือหน่วยงานของรัฐด้านอื่น ๆ 825 เหตุการณ์ (สัดส่วนร้อยละ 23.4) และผู้ประกอบการพาณิชย์ที่เป็นบริษัทเอกชนสัญชาติไทย 519 เหตุการณ์ (สัดส่วนร้อยละ 14.7) ส่วนภาคการเงินการธนาคารถูกโจมตี 207 เหตุการณ์ (สัดส่วนร้อยละ 5.9) อย่างไรก็ดี ธนาคารแห่งประเทศไทย (ธปท.) รายงานว่า ได้ติดตามเหตุการณ์ระบบเทคโนโลยีสารสนเทศขัดข้องและการโจมตีทางไซเบอร์ที่เกิดขึ้นกับสถาบันการเงินในต่างประเทศและ**ยังไม่พบผลกระทบต่อการให้บริการของสถาบันการเงินในไทย** ขณะที่กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมให้ความสำคัญกับประเด็นดังกล่าวและได้กำชับหน่วยงานกำกับดูแลโครงสร้างพื้นฐานสำคัญ 5 ด้าน ได้แก่ ตลาดเงิน ตลาดทุน สาธารณสุข โครงสร้างพื้นฐาน และพลังงาน ให้ตรวจสอบแผนป้องกันและการรับมือในกรณีเกิดเหตุฉุกเฉินอย่างรัดกุม

แนวโน้มสถานการณ์ที่เกิดขึ้นหลายพื้นที่ทั่วโลก สะท้อนความสำคัญของการตระหนักถึงความมั่นคงทางไซเบอร์และความเสี่ยงดิจิทัล ซึ่งไม่ได้สร้างความเสียหายเฉพาะแก่องค์กรที่ได้รับผลกระทบโดยตรง แต่ยังอาจส่งต่อไปยังผู้บริโภค คู่ค้า และธุรกิจอื่นที่เชื่อมโยงกันในห่วงโซ่อุปทาน สอดคล้องกับมุมมองขององค์การเพื่อความร่วมมือทาง

เศรษฐกิจและการพัฒนา (OECD) ที่ระบุว่า **ความมั่นคงปลอดภัยทางไซเบอร์เป็นความเสี่ยงทางเศรษฐกิจและสังคม และไม่ใช่เพียงประเด็นทางเทคนิค** โดยเฉพาะเมื่อธุรกิจพึ่งพาผู้ให้บริการคลาวด์ ซอฟต์แวร์ และโครงสร้างพื้นฐานดิจิทัลร่วมกัน

ทั้งนี้ ผอ.สนค. กล่าวเพิ่มเติมว่า การรับมือภัยไซเบอร์ไม่ใช่การชะลอการใช้เทคโนโลยี แต่เป็นการบริหารความเสี่ยงเพื่อให้ธุรกิจใช้ประโยชน์จากเทคโนโลยีและ AI ได้อย่างเต็มศักยภาพ โดย**ผู้ประกอบการควรให้ความสำคัญกับ 4 แนวทางปฏิบัติที่ชัดเจน** ได้แก่ **(1) ยกระดับความปลอดภัยของระบบและข้อมูล** เช่น ปรับปรุงซอฟต์แวร์ กำหนดสิทธิ์การเข้าถึง และสำรองข้อมูลอย่างสม่ำเสมอ **(2) ประเมินความเสี่ยงจากผู้ให้บริการภายนอก** ทั้งระบบคลาวด์ ซอฟต์แวร์ และแพลตฟอร์มออนไลน์ พร้อมจัดเตรียมทางเลือกและระบบสำรองกรณีฉุกเฉิน (3) **จัดทำและทดสอบแผนความต่อเนื่องทางธุรกิจ** เพื่อให้สามารถดำเนินงานและให้บริการได้เมื่อเกิดเหตุขัดข้อง และ **(4) เสริมสร้างทักษะและการรู้เท่าทันภัยไซเบอร์**แก่บุคลากรทุกระดับ รวมถึงการใช้ AI และเครื่องมือดิจิทัลอย่างปลอดภัยและสร้างสรรค์

สำหรับผู้ประกอบการ SMEs ที่อาจมีข้อจำกัดด้านบุคลากรที่เชี่ยวชาญทางเทคนิคและงบประมาณ ควรเริ่มจากมาตรการพื้นฐานที่จำเป็น ได้แก่ **การใช้ระบบยืนยันตัวตนหลายขั้นตอน การสำรองข้อมูลสำคัญ และการติดตามข่าวสารหรือการเตือนภัยจากหน่วยงานที่เกี่ยวข้อง** เพื่อเพิ่มความพร้อมในการป้องกันและรับมือเหตุการณ์ไม่คาดคิด

ผอ.สนค. กล่าวทิ้งท้ายว่า ความมั่นคงปลอดภัยทางไซเบอร์เป็นองค์ประกอบสำคัญของการสร้างความเชื่อมั่นในเศรษฐกิจยุคดิจิทัล **ภาคธุรกิจจึงต้องเร่งปรับตัวโดยไม่มองว่าเรื่องนี้เป็นเพียงหน้าที่ของฝ่ายไอที แต่ต้องผนวกแผนรับมือภัยไซเบอร์เข้ากับกลยุทธ์ระดับองค์กร** การส่งเสริมให้ใช้ประโยชน์จากเทคโนโลยีและ AI ควบคู่กับการเตรียมแผนสำรองที่ใช้งานได้จริงและการบริหารความเสี่ยง จะช่วยรักษาความต่อเนื่องของธุรกิจ เสริมความเชื่อมั่นของผู้บริโภคและคู่ค้า และยกระดับความสามารถในการแข่งขันของไทยให้เติบโตได้อย่างยั่งยืนในระยะยาว

สำนักงานนโยบายและยุทธศาสตร์การค้า
กระทรวงพาณิชย์
19 พฤศจิกายน 2569