MarSec Focus
Maritime Security Focus
สำนักงานสภาความมั่นคงแห่งชาติ
Office of the National Security Council
เอกสารวิชาการวิเคราะห์สถานการณ์ความมั่นคงฯ | ฉบับที่ ๓/๒๕๖๕ | วันที่ ๑ มิถุนายน ๒๕๖๕

Maritime Cyber Security ความท้าทายใหม่ของโลกยุคดิจิทัล (ตอนที่ ๑)

Maritime Cyber Security หรือความมั่นคงด้านไซเบอร์ทางทะเล กำลังเป็นสิ่งที่ท้าทายต่อความมั่นคงในยุคปัจจุบันที่ระบบอิเล็กทรอนิกส์ได้เข้ามาเป็นส่วนหนึ่งของการดำรงชีวิตประจำวัน ไม่ว่าจะเป็นการทำงาน การเรียน ตลอดจนการทำธุรกรรมใด ๆ ซึ่งล้วนแต่กระทำผ่านระบบอิเล็กทรอนิกส์ทั้งสิ้น ยิ่งในช่วงการแพร่ระบาดของเชื้อไวรัสโควิด - ๑๙ การใช้ระบบอิเล็กทรอนิกส์ก็แทบจะกลายเป็นปัจจัยหลักที่คนส่วนใหญ่ใช้ในการดำรงชีวิตท่ามกลางสถานการณ์วิกฤตินี้

ที่มาของเหตุการณ์

เมื่อเดือนมิถุนายน ๒๕๖๐ สายการเดินเรือสายใหญ่ที่สุดของโลกอย่าง Maersk หรือ A.P. Moller Maersk บริษัทขนส่งสัญชาติเดนมาร์ก ถูกโจมตีทางไซเบอร์ครั้งใหญ่จากมัลแวร์ NotPetya (NotPetya Ransomware) ส่งผลให้ธุรกิจขนส่งและโลจิสติกส์หยุดชะงัก การทำงานภายในท่าเรือ ๗๖ แห่งทั่วโลกต้องหยุดการทำงานและปิดระบบเครือข่ายภายในองค์กรหลายวัน โดยการโจมตีดังกล่าวสร้างปัญหาใหญ่ให้กับบริษัท Maersk ซึ่งขนส่งสินค้าด้วยตู้คอนเทนเนอร์ประมาณร้อยละ ๑๕ ของการค้าโลก และแม้จะสามารถฟื้นตัวจากปัญหาได้อย่างรวดเร็ว แต่ก็ส่งผลให้ Maersk ต้องสูญเสียมูลค่าทางการเงินสูงถึง ๓๐๐ ล้านดอลลาร์สหรัฐ ทั้งรายได้ ค่าใช้จ่ายในการกู้คืนไอที และค่าใช้จ่ายพิเศษที่เกี่ยวข้องกับการดำเนินงาน

จุดเริ่มต้นของเหตุการณ์ทั้งหมดเกิดขึ้นเมื่อพนักงานในยูเครนตอบกลับอีเมลที่มีมัลแวร์ NotPetya ทำให้มัลแวร์ดังกล่าวเข้าไปฝังตัวอยู่ในระบบปฏิบัติการ ส่งผลให้การปฏิบัติงานและการดำเนินกิจกรรมด้านขนส่งต้องหยุดชะงัก โดยระบบจะถูกระงับไว้จนกว่าจะสามารถกู้คืนได้ ส่งผลกระทบต่อระบบโลจิสติกส์ และห่วงโซ่อุปทาน (Supply Chain) ของการขนส่งทั้งระบบ ซึ่งมีความละเอียด ยุ่งยาก และซับซ้อน เนื่องจาก ระบบการทำงานของ Maersk เป็นระบบปฏิบัติการดิจิทัล และที่สำคัญคือก่อนหน้านั้นบริษัท Maersk ได้ประกาศมาตรการป้องกันสำหรับเหตุการณ์ในลักษณะดังกล่าวในรายงานประจำปี ๒๕๕๙ เพื่อทำให้ธุรกิจสายการเดินเรือเป็นธุรกิจดิจิทัลมากขึ้น โดยการพึ่งพาระบบไอทีที่ทำงานได้ดี และลดความเสี่ยงต่าง ๆ รวมถึงมุ่งเน้นการจัดการความต่อเนื่องทางธุรกิจ ในกรณีที่ระบบไอทีล่มหรือถูกโจมตี

ทั้งนี้ ภายหลังจากการถูกโจมตีทางไซเบอร์ Maersk มีการใช้แนวทางใหม่ในการรักษาความปลอดภัยในโลกไซเบอร์ เพื่อปรับปรุงความยืดหยุ่นทางไซเบอร์ให้ดียิ่งขึ้น และวางแผนเพื่อรักษาความปลอดภัยต่อธุรกิจดิจิทัล เสริมความแข็งแกร่งให้กับแพลตฟอร์มโครงสร้างพื้นฐานด้านไอที ปรับปรุงความต่อเนื่องของบริการด้านไอทีและการกู้คืนข้อมูล ตลอดจนเสริมสร้างแผนความต่อเนื่องทางธุรกิจ นอกจากนี้ยังมีการซื้อประกันทางไซเบอร์เพื่อลดผลกระทบทางการเงินที่อาจเกิดขึ้นจากการถูกโจมตีทางไซเบอร์อีกในอนาคต

ข้อพิจารณา

ในอนาคตยังมีความเป็นไปได้สูงที่องค์กรหรือภาคส่วนต่าง ๆ จะต้องเผชิญหน้ากับภัยคุกคามทางไซเบอร์ ดังนั้นแต่ละองค์กรจึงควรเตรียมความพร้อมรับมือ ขณะเดียวกัน คำแนะนำและการตัดสินใจ รวมถึงการจัดการสื่อสารของผู้บริหารระดับสูงถือเป็นสิ่งสำคัญในภาวะวิกฤติ เนื่องจาก เป็นผู้มีอำนาจในการสั่งการและชี้นำการดำเนินการต่าง ๆ เพื่อนำไปสู่การแก้ไขปัญหาและป้องกันไม่ให้กระทบต่อการดำเนินงานขององค์กร นอกจากนี้ พนักงานทุกระดับควรตระหนักถึงภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นได้ตลอดเวลา และเตรียมแผนรับมือเพื่อลดความเสียหาย รวมทั้งการทดสอบและปรับปรุงพัฒนาแผนการรับมือขององค์กรอย่างสม่ำเสมอ เพื่อสามารถตอบสนองได้อย่างเท่าทันต่อภัยคุกคามที่อาจเกิดขึ้นใหม่

ดังนั้น การลงทุนเพื่อปกป้องเครือข่ายไอทีขององค์กรและสร้างความตระหนักถึงภัยคุกคามทางไซเบอร์ของพนักงาน จึงมีความคุ้มค่ามากกว่าการสูญเสียทางด้านต่าง ๆ ที่จะตามมาอันเนื่องมาจากการถูกโจมตีทางไซเบอร์

ผลกระทบ

จากข้อมูลข้างต้นสามารถสรุปผลกระทบที่เกิดขึ้นได้ดังนี้ การถูกโจมตีทางไซเบอร์โดยมัลแวร์ NotPetya ทำให้ Maersk สูญเสียมูลค่าทางการเงินมากถึง ๓๐๐ ล้านดอลลาร์สหรัฐ และทำให้การปฏิบัติงานต้องหยุดชะงักเป็นเวลา ๒ สัปดาห์ สำหรับมัลแวร์ NotPetya พบอย่างแพร่หลายในยูเครน ซึ่งแม้ดูเหมือนเป็นเพียงแรนซัมแวร์บนหน้าจอคอมพิวเตอร์ แต่หน้าที่ของมัลแวร์ตัวนี้มีจุดประสงค์ที่จะมุ่งทำลายฐานข้อมูลทั้งหมด โดยบริษัท Maersk เป็นเพียงหนึ่งในบริษัทประมาณ ๗,๐๐๐ แห่งจากทั่วโลกที่ถูกโจมตี ทั้งนี้ Earl Perkins นักวิเคราะห์การวิจัยของ Gartner Inc. ได้ให้ข้อสังเกตว่าบริษัทที่ประสบการโจมตีทางไซเบอร์โดยมัลแวร์ NotPetya ส่วนใหญ่มักเป็นบริษัทอุตสาหกรรม สาธารณูปโภคและก๊าซ และเป็นองค์กรที่มีความลับทางธุรกิจเป็นจำนวนมาก

ข้อเสนอแนะ

แม้ว่ามาตรการการรักษาความปลอดภัยทางไซเบอร์จะมีการเปลี่ยนแปลงอยู่ตลอดเวลา แต่ผู้นำองค์กรทั้งหน่วยงานภาครัฐและเอกชนควรมีความตระหนักและเตรียมพร้อมรับมืออยู่ตลอดเวลา รวมถึงหามาตรการในการป้องกันภัยคุกคามทางไซเบอร์อย่างต่อเนื่องเพื่อป้องกัน และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ไม่ให้เกิดผลกระทบต่อความมั่นคงของรัฐ และความสงบเรียบร้อยภายในประเทศ พร้อมทั้งการเสริมสร้างการตระหนักรู้ให้กับบุคลากรในองค์กรให้รู้เท่าทันและมีความระมัดระวังในการใช้อุปกรณ์อิเล็กทรอนิกส์มากขึ้น รวมถึงพิจารณาชั้นของข้อมูลที่ส่งออกและนำเข้าซึ่งเป็นมาตรการป้องกันพื้นฐานของผู้ใช้ระบบคอมพิวเตอร์

★อ้างอิง

- https://www.intelligentcio.com/
- https://www.gartner.com/
- https://www.latimes.com/business/la-fi-maersk-cyberattack-20170817-story.html
- https://www.springnews.co.th/spring-life/822207

วิเคราะห์โดย... ว่าที่ ร.ต. อเนชา เผ่าพานิชย์ เจ้าหน้าที่วิเคราะห์นโยบายและแผน