ก้าวสู่ประเทศไทย 4.0 พร้อมความท้าทายของการรักษาความปลอดภัยในระบบควบคุมอุตสาหกรรม (ICS)

โดย มร.เยียว เซียง เทียง ผู้จัดการทั่วไป Kaspersky ภูมิภาคเอเชียตะวันออกเฉียงใต้

จากที่ผมได้สังเกต ภูมิภาคเอเชียตะวันออกเฉียงใต้เป็นพื้นที่ที่ผสมผสานกันระหว่างการพัฒนาและกำลังพัฒนา ถือเป็นแหล่งเศรษฐกิจเกิดใหม่ที่มีความหลากหลายทางด้านภูมิประเทศและการผลิต ซึ่งเปรียบเสมือนสวนที่มีต้นไม้นานาพันธุ์และหลากหลายช่วงวัยของการเจริญเติบโต

ในช่วงปี 2557 สิงคโปร์ มาเลเซียและไทย เป็นผู้นำด้านการผลิต ส่วนเวียดนาม ฟิลิปปินส์และอินโดนิเซียอยู่ในระหว่างการพัฒนา อย่างไรก็ตามจากสถิติต่าง ๆ ที่เคยศึกษามา การผลิตในภูมิภาคนี้มีการเคลื่อนไหวและตอบโตอย่างค่อยเป็นค่อยไป ซึ่งต้องขอบคุณสมาคมประชาชาติแห่งเอเชียตะวันออกเฉียงใต้ (ASEAN) ที่กำหนดวัตถุประสงค์ในการประคองสถานะของอุตสาหกรรมการผลิตในภูมิภาคนี้ และหากภูมิภาคนี้สามารถใช้ประโยชน์จากการปฏิวัติอุตสาหกรรมครั้งที่สี่ อาเซียนจะกลายเป็นเขตเศรษฐกิจที่ใหญ่ที่สุดเป็นอันดับสี่ของโลกภายในปี 2573

ดังนั้นมาดูกันว่าอุตสากรรม 4.0 คืออะไร เป็นแนวโน้มของระบบอัตโนมัติและการแลกเปลี่ยนข้อมูลในเทคโนโลยีการผลิตที่ประกอบด้วยระบบกายภาพทางไซเบอร์ (cyber-physical) การใช้งานอินเทอร์เน็ตกับทุกสิ่ง (IoT) ระบบคลาวด์ (cloud computing) และระบบคอมพิวเตอร์เสมือนมนุษย์ (cognitive computing) ซึ่งจากการศึกษาเพิ่มเติม การปฏิวัติอุตสาหกรรมครั้งที่สี่นี้ สามารถช่วยให้อาเซียนทำกำไรระดับโลกได้สูงสุดถึง 600 พันล้านเหรียญสหรัฐ จากทั้งหมดทั่วโลก 3.7 ล้านล้านเหรียญสหรัฐ ได้จากการอุตสาหกรรม 4.0 ในปี 2568

ประเทศไทย 4.0
ประเทศไทยก็จะขับเคลื่อนอุตสาหากรรม 4.0 เช่นเดียวกับประเทศเพื่อนบ้านอื่น ๆ ด้วยนโยบายการปรับเปลี่ยนเศรษฐกิจเช่นกัน ซึ่งเมื่อปี 2560 รัฐบาลไทยได้เปิดตัวแนวคิด ประเทศไทย 4.0 โดยมีวัตถุประสงค์เพื่อขับเคลื่อนประเทศจากรายได้ระดับกลางไปสู่การพัฒนานวัตกรรมต่าง ๆ เพื่อยกระดับเศรษฐกิจของประเทศ โดยโครงการนี้มุ่งมั่นที่จะพัฒนาและเอาชนะความท้าทายในปัจจัยต่าง ๆ ที่พัฒนามาตั้งแต่อดีต ที่เริ่มจากยุคประเทศไทย 1.0 นั่นคือประเทศไทยยุคเกษตรกรรม จากนั้นก็เป็นยุคอุตสาหกรรมเบาหรือประเทศไทย 2.0 และพัฒนาจนมาถึงยุคปัจจุบันนั่นก็คือประเทศไทย 3.0 คือยุคอุตสาหกรรมหนัก โดยความคิดริเริ่มดังกล่าวถือเป็นแผนแม่บทในการนำประเทศสู่ยุคอุตสาหกรรม 4.0 เพื่อที่จะทำให้ประเทศไทยมีรายได้สูงขึ้นภายใน 5 ปี

การเปลี่ยนผ่านสู่ยุคอุตสาหกรรม 4.0 นั้นหมายถึงการขับเคลื่อนเศรษฐกิจของประเทศจากการที่ต้องอาศัยอุตสาหกรรมการผลิตสินค้าต่าง ๆ ที่มีอยู่ ให้กลายเป็นการสร้างสรรค์และพัฒนาสินค้านวัตกรรมใหม่ ๆ ด้วยการวิจัยและการประดิษฐ์ให้เกิดขึ้น โดยการตั้งเป้าในการพัฒนาเพื่อเพิ่มมูลค่าให้กับเศรษฐกิจ ตัวอย่างเช่น การเปลี่ยนจากการทำเกษตรกรรมแบบดั้งเดิมสู่การทำเป็น Smart Farming ด้วยการนำนวัตกรรมและเทคโนโลยีต่าง ๆ เข้ามาในการทำการเกษตร จากธุรกิจขนาดกลางหรือขนาดเล็ก (SMEs) แบบดั้งเดิม กลายเป็นองค์กรที่ทันสมัยด้วยนวัตกรรมหรือที่เรียกว่า smart enterprise และการเปลี่ยนจากสินค้าหรือบริการแบบดั้งเดิมสู่การพัฒนาสินค้าหรือบริการที่เพิ่มมูลค่าสูงขึ้นมาอีกด้วย โดยยุคประเทศไทย 4.0 นั้นจะให้ความสำคัญกับเทคโนโลยีดิจิทัลต่าง ๆ ประกอบด้วย อินเทอร์เน็ตสำหรับทุกสิ่ง (IoT) คลาวด์ ข้อมูลมหาศาลและการวิเคราะห์ข้อมูล ซึ่งจะทำให้ประเทศพัฒนาได้อย่างชาญฉลาด มั่นคงและเชื่อมต่อกับชุมชน ที่สำคัญต้องคิดวางแผนล่วงหน้า มองการณ์ไกลและควบคู่ไปกับการแข่งขันในตลาด

แผนแม่บทนี้ได้รับการตอบรับและการสนับสนุนจากผู้ประกอบการ องค์กร บริษัทต่าง ๆ ในประเทศไทยมีความพร้อมในการรองรับเทคโนโลยี โดยจากการสำรวจ บริษัทต่าง ๆ ในประเทศไทยถึง 89% พร้อมที่จะก้าวสู่การปฏิบัติการและดำเนินงานด้วยเทคโนโลยีและนวัตกรรมต่าง ๆ ที่ใช้อินเทอร์เน็ต (IoT) ในขณะที่ประเทศมาเลเซีย 86% อินโดนีเซีย 83% ฟิลิปปินส์ 80% และเวียดนาม 79% นอกจากนี้ The Asia IoT Business Platform ยังได้คาดการณ์สถานการณ์การใช้งานอินเทอร์เน็ตกับทุกสิ่งในประเทศไทยจะเพิ่มสูงขึ้นเป็น 1,600% ภายในปี 2563 อีกด้วย

อย่างไรก็ตามการเปลี่ยนผ่านสู่ยุคประเทศไทย 4.0 นั้นยังมีความท้าทายในหลายปัจจัยด้วยกัน หนึ่งในนั้นก็คือด้านความปลอดภัย ซึ่งจริง ๆ แล้วกลยุทธ์ของประเทศไทย 4.0 นั้นให้ความสำคัญกับความปลอดภัยเป็นหนึ่งในสามองค์ประกอบหลัก ที่ควบคู่ไปกับความมั่งคั่งและความยั่งยืน เหตุผลที่ความปลอดภัยนั้นสำคัญในยุคประเทศไทย 4.0 นั้นมีความชัดเจนอย่างมากเพราะระบบกายภาพไซเบอร์ (cyber-physical) แบบไร้สายอัตโนมัติที่อาศัยการสัมผัสของมนุษย์น้อยที่สุดจะให้ประสิทธิภาพที่ดีกว่า แต่ระบบเหล่านี้ยังต้องเผชิญกับการโจมตีทางไซเบอร์อีกด้วย ซึ่งการเชื่อมต่อที่มากขึ้นในยุคประเทศไทย 4.0 จำเป็นจะต้องคำนึงถึงความปลอดภัยเป็นหลัก โดยเฉพาะอย่างยิ่งระบบควบคุมอุตสาหกรรม (ICS)

ความเสี่ยงเหล่านี้ไม่ควรละเลยโดยเฉพาะอย่างยิ่งในเอเชียตะวันออกเฉียงใต้ ซึ่งเป็นภูมิภาคที่ถูกจัดอันดับให้เป็นพื้นที่ที่มีการตรวจจับการติดเชื้อและการโจมตีในระบบควบคุมอุตสาหกรรม (ICS) สูงที่สุด ที่ตรวจจับโดย Kaspersky ในประเทศไทย ทั้งนี้ Kaspersky ได้ตรวจจับการติดเชื้อในอุปกรณ์ของระบบควบคุมอุตสาหกรรม (ICS) คิดเป็น 42.9% โดยอินเทอร์เน็ตยังเป็นแหล่งที่มาหลักของภัยคุกคามต่าง ๆ ในภูมิภาคนี้ โดยได้ตรวจจับภัยคุกคามในเครื่องคอมพิวเตอร์ในระบบ ICS คิดเป็น 39.5% นอกจากนี้ Kaspersky ยังได้ติดตามสังเกตสถานการณ์ซึ่งมีการเพิ่มขึ้นในคอมพิวเตอร์ระบบควบคุมอุตสาหกรรม จากการตรวจจับและบล็อกอีเมลที่มีไฟล์แนบที่เป็นอันตรายอีกด้วย

จากสถิติดังกล่าว แสดงให้เห็นว่ายุคประเทศไทย 4.0 ถือเป็นดาบสองคม นั่นก็คือมีข้อดีมากมาย อาทิ การติดต่อสื่อสารแบบไร้สายที่ทำให้สื่อสารกันได้อย่างรวดเร็ว แต่ก็มีข้อเสียเช่นกัน ได้แก่ ความเสี่ยงในการเสียค่าใช้จ่ายเมื่อมีการโจมตีทางไซเบอร์ เราจะเห็นได้ว่ายิ่งอุตสาหกรรมมีการเชื่อมต่อกันมากเท่าไหร่ ก็ยิ่งมีความเสี่ยงมากขึ้นเช่นกัน เพราะเป็นการเปิดช่องทางให้พวกโจมตีสามารถเข้ามาได้มากขึ้น โดยพวกเขาสามารถกำหนดเป้าหมายการโจมตีไปยังอุปกรณ์ที่สร้างข้อมูล เครือข่ายที่กำลังดำเนินการอยู่ บนเซิร์ฟเวอร์หรือโฮสต์ แม้กระทั่งระบบสารสนเทศที่ใช้อยู่ได้

เมื่อมีภัยคุกคามเข้าสู่ระบบควบคุมกระบวนการผลิต จะทำให้เกิดความเสียหายเป็นอย่างยิ่งต่อการเงินขององค์กร และจะทำให้การปฏิบัติการหยุดชะงักลง จากการที่มี 6 ใน 10 ของอุปกรณ์ในระบบ ICS ในประเทศไทยถูกโจมตีด้วยภัยคุกคามต่าง ๆ ในช่วงครึ่งปีหลังของปีที่แล้ว ทำให้การตระหนักถึงความปลอดภัยเป็นเรื่องสำคัญและต้องคำนึงถึงมากที่สุด

เราในฐานะ Kaspersky ขอแนะนำแนวทางองค์รวมเพื่อความปลอดภัยด้านไซเบอร์ ที่ประกอบด้วย 2 ส่วนหลัก ๆ ส่วนแรกคือการใช้โซลูชั่นความปลอดภัยสำหรับระบบและเครือข่ายที่สำคัญ ส่วนที่สองคือการตระหนักถึงภัยคุกคามให้มากขึ้นด้วยการเพิ่มนิสัยการสังเกตให้เกิดขึ้นกับพนักงานทุกคน เราขอแนะนำให้ใช้มาตรการเทคนิคต่อไปนี้เพื่อลดความเสี่ยงต่อการโจมตีในระบบ ICS

 ควรอัปเดทระบบการปฏิบัติการ ซอฟแวร์ และโซลูชั่นความปลอดภัยอยู่เสมอ
 แก้ไขด้านความปลอดภัยที่จำเป็นและตรวจสอบส่วนประกอบต่าง ๆ ในระบบ ICS บนเครือข่ายอุตสาหกรรมขององค์กรและในขอบเขตที่เกี่ยวข้อง
 จัดการอบรมให้ความรู้กับพนักงาน พันธมิตร ซัพพลายเออร์ ที่เข้าถึงบนเครือข่ายของคุณ
 จำกัดจำนวนการขนส่งหรือการใช้งานบนเครือข่าย ในส่วนของพอร์ตและโปรโตคอลที่ใช้กับเราเตอร์และภายในเครือข่ายระบบเทคโนโลยีการปฏิบัติการขององค์กร
 ใช้โซลูชั่นการตรวจสอบ การวิเคราะห์ การตรวจจับภัยคุกคาม บนเครือข่าย ICS เพื่อป้องกันเป็นอย่างดี จากการภัยคุกคามที่จะโจมตีกระบวนการทางเทคโนโลยีและทรัพย์สินหลักขององค์กร
 หันมาใช้โซลูชั่นด้านความปลอดภัยในเซิร์ฟเวอร์ ฐานปฏิบัติการ และ HMIs อย่าง Kaspersky Industrial CyberSecurity ซึ่งโซลูชั่นนี้ประกอบด้วยการตรวจสอบการขนส่งและการใช้งานบนเครือข่าย วิเคราะห์และตรวจจับเพื่อรักษาความปลอดภัยของเทคโนโลยีการปฏิบัติการ และ โครงสร้างพื้นฐานของอุตสาหกรรมจากการติดเชื่อจากมัลแวร์แบบสุ่ม และการตั้งใจโจมตีจากภัยคุกคามในอุตสาหกรรมต่าง ๆ
 จัดตั้งทีมบุคลากรรักษาความปลอดภัยโดยเฉพาะทั้งส่วนของเทคโนโลยีสารสนเทศ และ เทคโนโลยีการปฏิบัติการ
 เตรียมทีมรักษาความปลอดภัยให้มีความพร้อมอยู่เสมอ ด้วยการจัดการอบรมด้านความปลอดภัยทางไซเบอร์ที่เหมาะสม ควบคู่ไป