ไซเบอร์ซีเคียวริตี้สำคัญอย่างยิ่งต่อความสำเร็จของ ”Thailand 4.0”

ไซเบอร์ซีเคียวริตี้สำคัญอย่างยิ่งต่อความสำเร็จของ ”Thailand 4.0”

โดย: คุณวัตสัน ถิรภัทรพงศ์ กรรมการผู้จัดการประจำประเทศไทยและภูมิภาคอินโดจีนของซิสโก้

ประเทศไทยมุ่งมั่นที่จะเดินหน้าสู่ยุคดิจิตอลด้วยการปรับใช้เทคโนโลยีที่ทันสมัยเพื่อพัฒนาศักยภาพทางด้านเศรษฐกิจของประเทศ ภายใต้โมเดล ‘Thailand 4.0’ ซึ่งมุ่งเน้นการสร้างสรรค์นวัตกรรมทางด้านเทคโนโลยีและการพัฒนาระบบดิจิตอล เพื่อปรับปรุงคุณภาพชีวิต กำลังการผลิต และประสิทธิภาพการทำงาน

รัฐบาลมีจุดมุ่งหมายที่จะพัฒนาเศรษฐกิจโดยการเพิ่มมูลค่า ด้วยการเปลี่ยนจากวิถีการทำเกษตรแบบเดิมไปสู่แนวทางเกษตรอัจฉริยะ (Smart Farming) พร้อมทั้งพัฒนาธุรกิจเอสเอ็มอีแบบเดิมให้กลายเป็นองค์กรอัจฉริยะ (Smart Enterprise) และเปลี่ยนจากการบริการทั่วไปสู่การบริการที่มีมูลค่าทางธุรกิจที่สูงกว่า โดยมีการปรับใช้เทคโนโลยีดิจิตอลที่หลากหลาย เช่น Internet of Things (IoT), เทคโนโลยีคลาวด์ (Cloud), บิ๊กดาต้า (Big Data) และระบบวิเคราะห์ข้อมูลขั้นสูง (Analytics) เพื่อบ่มเพาะชุมชนให้ชาญฉลาด ปลอดภัย มีการเชื่อมต่อถึงกัน สามารถสร้างสรรค์นวัตกรรมใหม่ๆ มีวิสัยทัศน์กว้างไกล และเปี่ยมด้วยศักยภาพที่จะก้าวล้ำนำหน้าคู่แข่ง

หัวใจสำคัญของการพัฒนาสู่ ‘Thailand 4.0’ ขึ้นอยู่กับผู้บริโภคและไลฟ์สไตล์แบบดิจิตอลที่ขยายตัวอย่างต่อเนื่อง สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.) เปิดเผยว่า คนไทยใช้เวลากับอินเทอร์เน็ตเพิ่มมากขึ้น โดยปัจจุบันอยู่ที่ 6.2 ชั่วโมงต่อวัน และการใช้งานสมาร์ทโฟนในประเทศไทยเพิ่มขึ้นอย่างมากจนแตะระดับที่ 85.5 เปอร์เซ็นต์ ทุกวันนี้องค์กรต่างๆ เปิดตัวโมเดลธุรกิจใหม่ๆ กันอย่างต่อเนื่อง เพื่อตอบสนองความต้องการที่เพิ่มมากขึ้นของผู้บริโภคชาวไทยสำหรับดิจิตอลคอนเทนต์ ผลิตภัณฑ์ และบริการต่างๆ ด้วยเหตุนี้ “ระบบรักษาความปลอดภัย” จึงถือเป็นรากฐานสำคัญที่จะช่วยส่งเสริมการสร้างสรรค์นวัตกรรมและการเติบโต ของโมเดลธุรกิจใหม่ๆ ที่ต้องอาศัยความน่าเชื่อถือ และจะได้รับการใช้งานอย่างกว้างขวางก็ต่อเมื่อผู้บริโภคเชื่อมั่นในความสามารถขององค์กรนั้นๆ ในการปกป้องข้อมูลส่วนตัวและข้อมูลด้านการเงิน

การโจมตีทางไซเบอร์ที่ซับซ้อนมีการขยายตัวเพิ่มมากขึ้น
องค์กรที่ขาดกลยุทธ์ด้านการรักษาความปลอดภัยที่มีประสิทธิภาพมีแนวโน้มที่จะปรับใช้เทคโนโลยีดิจิตอลได้ช้ากว่าและได้รับประโยชน์น้อยกว่า ทั้งนี้ สพธอ. เปิดเผยว่า ประเทศไทยตกเป็นเป้าหมายการโจมตีทางไซเบอร์มากกว่า 4,300 ครั้งเมื่อปีที่แล้ว เพิ่มขึ้นจาก 3,000 ครั้งในปี 2557 ขณะที่มาสเตอร์การ์ด (MasterCard) ระบุว่าความ

ปลอดภัยของระบบชำระเงินเป็นประเด็นหลักที่สร้างความกังวลให้แก่ผู้ใช้ระบบออนไลน์ส่วนใหญ่ ทั้งยังเป็นสาเหตุสำคัญที่ทำให้ตัวเลขการซื้อสินค้า/บริการทางออนไลน์ในประเทศไทยอยู่ในระดับต่ำ กล่าวคือ กว่าครึ่งหนึ่งของประชากรในประเทศไทยไม่ได้ซื้อสินค้าทางออนไลน์ นอกจากนี้ เมื่อต้นเดือนสิงหาคมที่ผ่านมา ธนาคารแห่งหนึ่งของไทยต้องปิดเครื่องเอทีเอ็มราวครึ่งหนึ่งของจำนวนที่ติดตั้งไว้ทั่วประเทศ หลังจากที่แฮ็กเกอร์เจาะเข้าสู่ระบบเซิร์ฟเวอร์และโจรกรรมเงินไปได้ราว 12 ล้านบาท กลุ่มอาชญากรทางไซเบอร์ได้โหลดมัลแวร์เข้าสู่เครื่องเอทีเอ็มและสั่งให้เครื่องจ่ายเงินสดออกมา

มัลแวร์เรียกค่าไถ่ (Ransomware) ได้กลายเป็นมัลแวร์ประเภทที่สร้างกำไรให้แก่คนร้ายมากที่สุดในประวัติศาสตร์ และถึงเวลาแล้วที่บริษัทต่างๆ จะต้องกำหนดกลยุทธ์ด้านการรักษาความปลอดภัยที่มีประสิทธิภาพ เพื่อรองรับเป้าหมายในการปฏิรูปธุรกิจ รายงานความปลอดภัยทางไซเบอร์ประจำกลางปี 2559 ของซิสโก้ (Cisco 2016 Midyear Cybersecurity Report) ระบุว่าองค์กรต่างๆ ไม่มีความพร้อมสำหรับการรับมือกับปัญหาในอนาคตที่เกิดจากมัลแวร์เรียกค่าไถ่ (Ransomware) ซึ่งมีความซับซ้อนมากขึ้น โครงสร้างพื้นฐานที่เปราะบาง เครือข่ายที่มีสิ่งแปลกปลอม และการตรวจจับที่ล่าช้าเปิดโอกาสให้คนร้ายมีเวลาอย่างเหลือเฟือในการแทรกซึมเข้าสู่เครือข่ายขององค์กร ความพยายามในการจำกัดพื้นที่ดำเนินการของผู้โจมตีถือเป็น ‘ความท้าทายที่สำคัญที่สุด’ ซึ่งองค์กรธุรกิจต้องเผชิญ ทั้งยังคุกคามต่อพื้นฐานที่จำเป็นสำหรับการปฏิรูประบบดิจิตอล

องค์ธุรกิจสามารถสร้างระบบการรักษาความปลอดภัยอย่างชาญฉลาด
เพื่อปกป้องธุรกิจ องค์กรต่างๆ สามารถดำเนินการตามขั้นตอนง่ายๆ เพื่อปรับปรุงการรักษาความปลอดภัยดังนี้:

• ปรับปรุงความเป็นระเบียบเรียบร้อยของเครือข่ายด้วยการตรวจสอบดูแลเครือข่าย การติดตั้งแพตช์และการอัพเกรดตามกำหนดเวลา การแบ่งเครือข่ายเป็นส่วนๆ การปรับใช้ระบบป้องกันที่ส่วนรอบนอกของเครือข่าย รวมถึงการปกป้องอีเมลและเว็บ ไฟร์วอลล์รุ่นอนาคต (Next-Generation Firewall) และระบบป้องกันการบุกรุกรุ่นอนาคต (Next-Generation IPS)

• ผนวกรวมระบบป้องกันเข้าด้วยกันโดยใช้แนวทางเชิงสถาปัตยกรรมสำหรับการรักษาความปลอดภัย แทนที่จะติดตั้งเฉพาะจุด

• ตรวจวัดเวลาในการตรวจจับโดยเฉพาะอย่างยิ่งเวลาที่เร็วที่สุดในการตรวจพบภัยคุกคาม แล้วแก้ไขปัญหาอย่างทันท่วงที ทำให้การตรวจวัดเวลาในการตรวจจับ กลายเป็นส่วนหนึ่งของนโยบายการรักษาความปลอดภัยขององค์กรอย่างต่อเนื่อง

• ปกป้องผู้ใช้ของคุณทุกที่ทุกเวลาไม่ว่าผู้ใช้จะอยู่หรือทำงานที่ใดก็ตาม ไม่ใช่ปกป้องเพียงแค่ระบบที่ผู้ใช้ใช้งานหรือขณะที่ผู้ใช้ใช้งานอยู่บนเครือข่ายของบริษัทเท่านั้น

• แบ็คอัพข้อมูลสำคัญและทดสอบประสิทธิภาพอย่างสม่ำเสมอ พร้อมทั้งตรวจสอบว่าข้อมูลแบ็คอัพไม่มีความเสี่ยงที่

จะได้รับความเสียหาย

ในช่วงปี 2558 สพธอ. ได้ดำเนินการสำรวจความคิดเห็นทางด้านไซเบอร์ซีเคียวริตี้ และพบว่า 87 เปอร์เซ็นต์ของบริษัทที่ตอบแบบสอบถามเคยประสบปัญหาข้อมูลสูญหายและความสูญเสียด้านการเงินอันเนื่องมาจากการโจมตีทางไซเบอร์ แน่นอนว่าการโจมตีทางไซเบอร์ย่อมสร้างความอ่อนแอให้กับธุรกิจ ไม่ว่าขนาดเล็กหรือขนาดใหญ่ และอาจสร้างความกังวลใจและค่าใช้จ่ายจำนวนมากต่อผู้บริโภค เพื่อให้บรรลุเป้าหมายของการพัฒนา ‘Thailand 4.0’ จำเป็นที่จะต้องสร้างระบบรักษาความปลอดภัยที่แข็งแกร่งสำหรับใช้เป็นรากฐานที่สำคัญ และในการปิดกั้นโอกาสสำหรับการโจมตีทางไซเบอร์ องค์กรต่างๆ จะต้องปรับใช้แนวทางการรักษาความปลอดภัยแบบหลายเลเยอร์ และผนวกรวมระบบไซเบอร์ซีเคียวริตี้เข้าไว้ในกระบวนการปฏิรูปทางด้านดิจิตอล โดยถือเป็นองค์ประกอบพื้นฐานที่สำคัญ แทนที่จะใช้วิธีติดตั้งโซลูชั่นการรักษาความปลอดภัยในลักษณะ ‘วัวหายล้อมคอก’ หลังจากที่มีปัญหาเกิดขึ้น