ข้อสังเกตสำคัญ 10 ประการ ที่ฝ่ายไซเบอร์ซีเคียวริตี้

ข้อสังเกตสำคัญ 10 ประการ ที่ฝ่ายไซเบอร์ซีเคียวริตี้ หรือผู้เชี่ยวชาญด้านความปลอดภัยควรรู้ เมื่อ Internet of Things (IOT) เกิดขึ้นอย่างแพร่หลาย และต่อเนื่องในปัจจุบัน

โดย คุณวัตสัน ถิรภัทรพงศ์ กรรมการผู้จัดการบริษัทซิสโก้ประจำประเทศไทย และภูมิภาคอินโดจีน

เครือข่าย Internet of Everything (IoE) มีวิวัฒนาการอย่างต่อเนื่อง และกำลังจะเข้ามาแทนที่ Internet of Things (IoT) ในปัจจุบัน IoE กำลังสร้างโอกาสสำคัญให้กับองค์กรธุรกิจ ชุมชน และประเทศ เพราะ “สิ่งของบนโลกกำลังเริ่มเชื่อมต่อกับระบบออนไลน์มากขึ้นทุกๆวัน” รวมถึงเชื่อมกับผู้คน กระบวนการ และข้อมูล นอกจาก IoE จะสร้างโอกาส และประโยชน์มหาศาล ยังสร้างความท้าทายเกี่ยวกับ “ความปลอดภัย” อีกด้วย จริงๆแล้วทั้ง IoT และ IoE ไม่ได้ต้องการแค่เพียงการเชื่อมต่อด้านเครือข่ายเท่านั้น (networked connections) แต่ต้องเป็น “การเชื่อมต่อที่ปลอดภัย” (secured networked connections) เพื่อใช้ประโยชน์จากการใช้งานเครือข่ายมูลค่าเป็นล้านล้านบาทในอีกไม่กี่ปีข้างหน้า

การเสริมสร้างประสิทธิภาพด้านความปลอดภัยของเครือข่ายเหล่านี้ ต้องพึ่งพาอาศัยกันในหลายๆ ด้าน เราจำเป็นต้องพัฒนาต่อยอดจากเครือข่ายและระบบรักษาความปลอดภัยที่มีอยู่ พร้อมทั้งนำเสนอมุมมองใหม่ๆ โดยต้องตระหนักว่าทุกแง่มุมของเครือข่ายทำงานอย่างสอดประสานกัน ดังนั้นโซลูชั่นการรักษาความปลอดภัยทางด้านไซเบอร์และกายภาพจะต้องทำงานร่วมกันอย่างกลมกลืนเพื่อรับมือกับภัยคุกคาม สิ่งที่จำเป็นต้องใช้ก็คือ “รูปแบบการรักษาความปลอดภัยที่มุ่งเน้นภัยคุกคามเป็นหลัก” โดยรูปแบบการรักษาความปลอดภัยดังกล่าวจะต้องครอบคลุมช่องทางการโจมตีที่หลากหลาย และรับมือกับการโจมตีในทุกขั้นตอน ทั้งก่อน ระหว่าง และหลังการโจมตี รูปแบบการรักษาความปลอดภัยนี้จะช่วยให้เราสามารถปกป้องระบบคอมพิวเตอร์ เครือข่าย และข้อมูลได้อย่างมีประสิทธิภาพ และสำหรับหลายๆ องค์กรที่เกี่ยวข้องกับการควบคุมภาคอุตสาหกรรมและระบบงานอัตโนมัติ เราจะต้องขยายรูปแบบการรักษาความปลอดภัยเดียวกันนี้ เพื่อปรับปรุงประสิทธิภาพในการปกป้องระบบปฏิบัติงานที่เปรียบเสมือนเลือดหล่อเลี้ยงองค์กรและชีวิตประจำวันของเรา

สำหรับประเทศไทย ปฏิเสธไม่ได้ว่านโยบายดิจิทัลอีโคโนมีจะสร้างโอกาสทางธุรกิจหลายล้านล้านบาทในประเทศ ขณะภัยคุกคามต่อประชาชน ธุรกิจ และประเทศก็เกิดขึ้นพร้อมๆกันเช่นกัน สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ETDA) รายงานว่าประเทศไทยเป็นอันดับ 3 ใน 10 ประเทศในภูมิภาคอาเซียนในแง่ของความเสี่ยงด้านไซเบอร์ (cyber-risk) และการคาดการณ์ว่าปีนี้ภัยคุกคามไซเบอร์หลักๆ จะมาจากเทรนด์ของโมบิลิตี้ และ IoT อย่างไร

ก็ตามรัฐบาลได้วางแผนที่จะตั้ง หน่วยงานด้านความมั่นคงและปลอดภัยทางไซเบอร์ของประเทศ (National Cyber Security Agency) ในอีกไม่กี่ปีข้างหน้าเพื่อช่วยให้ประเทศไทยมีการเชื่อมต่ออย่างปลอดภัย

องค์กรธุรกิจจำเป็นต้องมีนโยบาย และกลยุทธ์ด้านไซเบอร์ซีเคียวริตี้ที่แข็งแกร่งในขณะที่ภัยคุกคามมีความซับซ้อนมากขึ้น เพื่อช่วยให้ผู้เชี่ยวชาญไอทีด้านความปลอดภัยได้รับความเข้าใจที่ถูกต้อง ขณะที่วิวัฒนาการของ IoT ยังคงดำเนินต่อไป ข้อสังเกตที่สำคัญ 10 ประการต่อไปนี้จะช่วยให้บุคลากรไอทีด้านความปลอดภัยสามารถคาดการณ์เหตุการณ์ที่มีความเสี่ยงได้ถูกต้องและแม่นยำมากขึ้น:
1. โลกต่างๆ จะหลอมรวมเข้าด้วยกัน: องค์กรส่วนใหญ่มีเทคโนโลยีและกระบวนการที่แตกต่างหลากหลายในการปกป้องเครือข่ายไอที (Information Technology Networks) และเครือข่ายปฏิบัติการ (Operational Technology Networks) เมื่อเรานำเอาเทคโนโลยีสำหรับผู้บริโภค (Consumer Technology – CT) เช่น สมาร์ทโฟน และแท็บเล็ต มาไว้บนเครือข่ายไอที เราก็จะเห็นว่าเครือข่ายเหล่านี้ผสานรวมเข้าด้วยกันจนกลายเป็นเครือข่าย IoT เราจำเป็นต้องเริ่มต้นปรับใช้โซลูชั่นไซเบอร์ซีเคียวริตี้ เพื่อปกป้องเครือข่ายทั้งหมดอย่างเท่าเทียมกันเพื่อให้รอดพ้นจากการโจมตี โดยสอดรับกับข้อกำหนดและเงื่อนไขที่เฉพาะเจาะจงของแต่ละเครือข่าย

2. “พื้นผิวการโจมตี” จะขยายใหญ่ขึ้น: ปัจจุบันมีอุปกรณ์ใหม่ๆ หลายพันล้านอุปกรณ์ถูกเชื่อมต่อเข้ากับเครือข่าย IoT (เช่น มิเตอร์อัจฉริยะ ฮีตเตอร์ ระบบปรับอากาศ อุปกรณ์ตรวจดูแลสุขภาพ รีโมทเซ็นเซอร์รสำหรับท่อส่งก๊าซและน้ำมัน ฯลฯ) และจะมีอุปกรณ์ใหม่ๆ ถูกเชื่อมต่อเข้าสู่เครือข่ายเพิ่มมากขึ้นในทุกวัน ดังนั้นความสามารถในการตรวจพบ หรือสกัดกั้นการโจมตีเหล่านี้จะยากขึ้นเป็นเงาตามตัว

3. ภัยคุกคามจะมีความหลากหลายมากขึ้น: เนื่องจากวัตถุที่จะตกเป็นเป้าหมายการโจมตีมีความหลากหลายมากขึ้นและส่วนใหญ่อยู่ในตำแหน่งที่ไม่ปลอดภัย ดังนั้นผู้โจมตีจึงสามารถคิดค้นวิธีการใหม่ๆ ที่แวดวงไซเบอร์ซีเคียวริตี้ยังไม่เคยพบเจอมาก่อน และผสานรวมเทคนิคที่ซับซ้อนเข้าด้วยกัน เพื่อทำภารกิจการโจมตีให้สำเร็จ

4. ภัยคุกคามจะมีความก้าวล้ำมากขึ้นอย่างต่อเนื่อง: ทุกวันนี้ภัยคุกคามมีลักษณะล่องหนมากขึ้น สามารถเล็ดลอดการตรวจจับเบื้องต้น และใช้ช่องโหว่ที่แทบจะตรวจไม่พบเพื่อเจาะเข้าสู่เป้าหมาย ระบบไซเบอร์ซีเคียวริตี้ที่พึ่งพาเทคนิคและมาตรการป้องกันเฉพาะจุด ณ ช่วงเวลาหนึ่งๆ จะไม่สามารถรับมือกับการโจมตีใหม่ๆ ได้

5. การแก้ไขปัญหาจะมีลักษณะเร่งด่วนและซับซ้อนมากขึ้น: เมื่อมีการโจมตีเกิดขึ้น องค์กรต่างๆ ไม่สามารถแยกระบบที่มีปัญหาได้เสมอไป เพราะค่าใช้จ่ายและความยุ่งยากซับซ้อนในการปิดระบบอาจสูงกว่ามูลค่าความเสียหายที่เกิดจากภัยคุกคามเสียด้วยซ้ำ โดยองค์กรจะต้องเลือกระหว่างการคุ้มครองความปลอดภัย กับการรักษาความต่อเนื่องในการดำเนินงาน วิธีการแก้ปัญหาจะต้องมุ่งเน้นการตรวจจับ จำกัดขอบเขต และกักกันภัยคุกคามอย่างทันท่วงที และจะต้องล้างระบบ และฟื้นฟูการดำเนินงานให้กลับคืนสู่ภาวะปกติอย่างรวดเร็ว

6. ความเสี่ยงและผลกระทบจะเพิ่มขึ้น: ข้อมูลสำคัญและข้อมูลส่วนตัวจำนวนมากไหลเวียนไปมาระหว่าง

กระบวนการและระบบธุรกิจ รวมไปถึงอุปกรณ์หลายพันล้านอุปกรณ์ทั่วโลกที่เชื่อมต่ออยู่บนเครือข่าย ทั้งในจุดที่ปลอดภัยและไม่ปลอดภัย โดยมากแล้ว อุปกรณ์และโดเมนเหล่านี้อยู่ภายนอกเครือข่าย IT และ OT ที่คุ้มครองด้วยระบบรักษาความปลอดภัย ทั้งนี้ ในเครือข่าย OT ผลกระทบจากการละเมิดระบบรักษาความปลอดภัยอาจมีมากกว่านี้ ตัวอย่างเช่น หากเครือข่ายของโรงพยาบาลหรือศูนย์การแพทย์ถูกโจมตี และระบบที่จำเป็นสำหรับการดูแลรักษาผู้ป่วยหรือการพยุงชีวิตได้รับผลกระทบ ผลลัพธ์ก็อาจรุนแรงมากกว่าระบบคอมพิวเตอร์ที่ติดมัลแวร์ในสภาพแวดล้อม IT เราจึงต้องให้ความสำคัญต่อการปกป้องข้อมูลนี้ในทุกๆ ที่ ไม่ว่าข้อมูลจะถูกใช้งานในลักษณะใดก็ตาม

7. การปฏิบัติตามข้อกำหนดและกฎระเบียบจะมีความจำเป็นมากขึ้น: หน่วยงานกำกับดูแลจะกำหนดให้มีการใช้มาตรการรักษาความปลอดภัยและการควบคุมความเป็นส่วนตัวอย่างเข้มงวดมากขึ้น ซึ่งจะส่งผลกระทบต่ออุตสาหกรรมต่างๆ มากขึ้น หากไม่สามารถปฏิบัติตามข้อกำหนดเหล่านี้ได้อย่างมีประสิทธิภาพ องค์กรก็จะไม่ได้รับประโยชน์อย่างเต็มที่จาก IoE นอกจากนี้ เนื่องจากมีอุปกรณ์ต่างๆ ถูกเชื่อมต่อเข้าสู่เครือข่ายเพิ่มมากขึ้นทุกขณะ ดังนั้นเส้นแบ่งระหว่างความเป็นเจ้าของกับความรับผิดชอบจะค่อยๆ เลือนหายไป และก่อให้เกิดปัญหาท้าทายใหม่ๆ สำหรับการจัดการ การปฏิบัติตามข้อกำหนดและกฎระเบียบ และการดูแลด้านคอมพลายแอนซ์ (compliance)

8. ความสามารถในการตรวจสอบจะเป็นสิ่งจำเป็นอย่างยิ่ง: บุคลากรไอทีด้านความปลอดภัยจะต้องมองเห็นภาพรวมของอุปกรณ์ ข้อมูล และความสัมพันธ์ขององค์ประกอบต่างๆ อย่างถูกต้องในแบบเรียลไทม์ เพื่อให้สามารถใช้ประโยชน์อย่างเต็มที่จากอุปกรณ์หลายพันล้านเครื่อง รวมไปถึงแอพพลิเคชั่น และข้อมูลที่เกี่ยวข้อง โดยจะต้องใช้ “ระบบงานอัตโนมัติ” และ “ระบบวิเคราะห์ข้อมูล” ที่ทำงานได้อย่างรวดเร็วมาเป็นตัวช่วย เพราะมนุษย์เองจะไม่สามารถรับมือกับสภาพแวดล้อมที่ขยายตัวอย่างต่อเนื่องได้

9. การรับรู้ถึงภัยคุกคาม (Threat Awareness) จะกลายเป็นเรื่องที่ต้องได้รับความใส่ใจมากขึ้น: ท่ามกลางสภาพแวดล้อมที่ไม่มีขอบเขตชัดเจน บุคลากรไอทีด้านความปลอดภัยจำเป็นต้องคาดการณ์เกี่ยวกับความเสี่ยง และจะต้องสามารถระบุภัยคุกคามโดยอาศัยความเข้าใจเกี่ยวกับลักษณะการทำงานที่ปกติและผิดปกติ รวมทั้งระบุตัวบ่งชี้เกี่ยวกับความเสี่ยง ดำเนินการตัดสินใจ และโต้ตอบอย่างฉับไว โดยจะต้องรับมือกับสภาพแวดล้อมทางเทคโนโลยีที่ซับซ้อนและแยกกระจัดกระจายได้

10. การดำเนินการต้องเป็นไปอย่างฉับไว: หลังจากที่ระบุภัยคุกคามหรือการทำงานที่ผิดปกติ ฝ่ายไอทีด้านความปลอดภัยจะต้องดำเนินการแก้ไขปัญหาอย่างรวดเร็ว โดยจะต้องอาศัยเทคโนโลยี กระบวนการ และบุคลากรที่เหมาะสม สามารถประสานงานร่วมกันได้อย่างฉับไวและมีประสิทธิภาพ