Industrial IoT เทคโนโลยีที่มาพร้อมกับภัยคุกคามทางไซเบอร์

การปฏิวัติอุตสาหกรรมครั้งที่ 4 หรือ Industry 4.0 ได้นำมาซึ่งการเปลี่ยนแปลงอย่างมีนัยสำคัญในภาคการผลิตทั่วโลก โดย Industrial Internet of Things (Industrial IoT) เป็นหนึ่งในเทคโนโลยีที่เป็นรากฐานสำคัญของการปฏิวัติอุตสาหกรรมและการพัฒนาโรงงานอัจฉริยะ (Smart Factory) ซึ่งเป็นระบบการผลิตที่สามารถปรับเปลี่ยนและตอบสนองต่อความต้องการของลูกค้าและตลาดที่เปลี่ยนแปลงได้อย่างรวดเร็ว บทบาทสำคัญของ Industrial IoT ใน Industry 4.0 คือการสนับสนุนการวิเคราะห์ข้อมูลขั้นสูง (Advanced Analytics) และปัญญาประดิษฐ์ (AI) โดย Industrial IoT เป็นแหล่งที่มาของข้อมูลมหาศาล (Big Data) จากกระบวนการผลิต ซึ่งเมื่อผ่านการวิเคราะห์ด้วยอัลกอริทึมการเรียนรู้ของเครื่อง (Machine Learning) จะนำไปสู่การหยั่งรู้เชิงลึก (Insights) ที่มีคุณค่าสำหรับการตัดสินใจเชิงกลยุทธ์และการปรับปรุงกระบวนการอย่างต่อเนื่อง

ด้วยการเชื่อมต่อที่ไร้รอยต่อระหว่างเครื่องจักร ระบบการผลิต และห่วงโซ่อุปทาน Industrial IoT สามารถช่วยยกระดับอุตสาหกรรมการผลิตให้มีระบบการผลิตที่ยืดหยุ่น (Flexible) ปรับเปลี่ยนได้ (Adaptive) และตอบสนองได้อย่างรวดเร็ว (Responsive) สามารถปรับเปลี่ยนสายการผลิตเพื่อรองรับผลิตภัณฑ์ที่หลากหลายได้อย่างฉับไว ทำให้สามารถรองรับการผลิตแบบเฉพาะเจาะจงสำหรับลูกค้าแต่ละราย (Mass Customization) ได้อย่างมีประสิทธิภาพ ความก้าวหน้าของ Industrial IoT ทำให้กระบวนการผลิตมีข้อมูลแบบเรียลไทม์จากเซ็นเซอร์และแหล่งข้อมูลต่าง ๆ ช่วยให้อุปกรณ์และเครื่องจักรทางอุตสาหกรรมตัดสินใจได้ด้วยตนเอง สามารถผลิตแบบอัตโนมัติเต็มรูปแบบ (Fully Automated Production) และจัดการทรัพยากรอย่างมีประสิทธิภาพสูงสุด ซึ่งเป็นการพลิกโฉมอุตสาหกรรมไปอย่างสิ้นเชิง

แม้ความก้าวหน้าของ Industrial IoT (Industrial IoT) จะช่วยยกระดับประสิทธิภาพการผลิตและเพิ่มขีดความสามารถทางการแข่งขัน ทว่าในขณะเดียวกัน ภัยคุกคามทางไซเบอร์ที่ภาคการผลิตต้องเผชิญกลับทวีความรุนแรงอย่างต่อเนื่อง ยิ่งมีการใช้ Industrial IoT มากขึ้น ความเสี่ยงก็ยิ่งเพิ่มขึ้นเป็นเงาตามตัว อุปกรณ์อัจฉริยะและระบบอัตโนมัติที่ช่วยเพิ่มประสิทธิภาพการผลิต อาจกลายเป็นจุดอ่อนที่ถูกใช้เป็นช่องทางโจมตีในการแทรกซึมระบบควบคุมเครื่องจักร ขโมยข้อมูลสำคัญ ดัดแปลงกระบวนการผลิต หรือแม้แต่ทำให้ทั้งโรงงานต้องหยุดชะงัก ผลกระทบที่ได้รับอาจรุนแรงถึงขั้นสูญเสียรายได้มหาศาล เสียความน่าเชื่อถือ และต้องเผชิญกับความเสียหายที่ไม่อาจประเมินได้หากไม่มีมาตรการรักษาความปลอดภัยที่เพียงพอ

ศักยภาพของเทคโนโลยี Industrial IoT

เทคโนโลยี Industrial IoT เป็นการประยุกต์ใช้เทคโนโลยี Internet of Things (IoT) ในบริบทของภาคอุตสาหกรรมการผลิต โดย Industrial IoT เป็นระบบเครือข่ายของอุปกรณ์อัจฉริยะ เซ็นเซอร์ และระบบควบคุมอัตโนมัติต่าง ๆ ที่เชื่อมต่อกันผ่านเครือข่ายอินเทอร์เน็ตหรือเครือข่ายภายในองค์กร เพื่อเก็บรวบรวม แลกเปลี่ยน และวิเคราะห์ข้อมูลแบบเรียลไทม์ มุ่งเน้นไปที่การสื่อสารระหว่างเครื่องจักร (Machine-to-machine Communication) รวมถึง Big Data และ Machine Learning ซึ่งช่วยให้อุตสาหกรรมและองค์กรสามารถดำเนินงานได้อย่างไร้รอยต่อและมีประสิทธิภาพเพิ่มขึ้น องค์ประกอบหลักของ Industrial IoT ประกอบด้วย

- **อุปกรณ์และเซ็นเซอร์** เปรียบเสมือนประสาทสัมผัสของระบบ Industrial IoT ทำหน้าที่รับรู้และเก็บข้อมูลจากสภาพแวดล้อมทางกายภาพ เช่น เซ็นเซอร์อุณหภูมิสำหรับตรวจวัดความร้อนในกระบวนการผลิต เซ็นเซอร์

การสั่นสะเทือนสำหรับตรวจจับการสั่นผิดปกติที่อาจบ่งชี้ว่าเครื่องจักรกำลังจะเสีย เป็นต้น เซ็นเซอร์เหล่านี้ถูกออกแบบให้ทนทานต่อสภาวะอุตสาหกรรมที่รุนแรง เช่น อุณหภูมิ ความชื้น การสั่นสะเทือน หรือสารเคมีกัดกร่อน และสามารถทำงานอย่างต่อเนื่องหลายปีโดยไม่ต้องบำรุงรักษาบ่อย

- **ระบบเครือข่ายการสื่อสาร** เปรียบเสมือนเส้นประสาทที่นำข้อมูลจากส่วนต่าง ๆ ของร่างกายไปยังสมอง เป็นโครงสร้างพื้นฐานที่ช่วยให้อุปกรณ์และระบบสามารถสื่อสารกันได้ มีทั้งแบบมีสายและไร้สาย เช่น Ethernet, Wi-Fi, Bluetooth, Zigbee, 5G, LoRaWAN, NB-IoT และโปรโตคอลอุตสาหกรรม
- **การประมวลผล** มี 2 รูปแบบ ได้แก่ Edge Computing เปรียบเสมือนไขสันหลังของมนุษย์ที่สามารถประมวลผลข้อมูลและตอบสนองได้โดยไม่ต้องส่งข้อมูลทั้งหมดไปยังสมอง ทำให้การตอบสนองรวดเร็วและลดภาระการส่งข้อมูล ในขณะที่ Cloud Computing เปรียบเสมือนสมองที่ทำการวิเคราะห์ขั้นสูง จัดเก็บความทรงจำระยะยาว และประสานงานส่วนต่าง ๆ ของระบบเข้าด้วยกัน ทำให้สามารถจัดการข้อมูลจำนวนมหาศาลและทำการวิเคราะห์ที่ซับซ้อนได้
- **แพลตฟอร์ม Industrial IoT** เปรียบเสมือนระบบประสาทส่วนกลางที่ประสานงานระหว่างส่วนต่าง ๆ เป็นซอฟต์แวร์ที่ช่วยเชื่อมต่อ จัดการ และวิเคราะห์อุปกรณ์และข้อมูล Industrial IoT เช่น PTC ThingWorx, Siemens MindSphere, GE Predix, AWS IoT, Microsoft Azure IoT

ถึงแม้ Industrial IoT และ IoT จะมีหลักการบางประการที่เหมือนกัน แต่ทั้งสองเทคโนโลยีมีความแตกต่างกันอย่างมีนัยสำคัญ โดย IoT เน้นการใช้งานสำหรับผู้บริโภคในชีวิตประจำวัน ขณะที่ Industrial IoT เน้นสำหรับการเพิ่มผลิตภาพภายใต้สภาพแวดล้อมของอุตสาหกรรม เช่น โรงงาน ระบบการผลิต โครงสร้างพื้นฐานสาธารณูปโภค และการขนส่ง โดยมีความต้องการด้านความน่าเชื่อถือ ความปลอดภัย และความทนทานที่สูงกว่า เนื่องจากมีผลกระทบโดยตรงต่อกระบวนการทางธุรกิจที่สำคัญและความปลอดภัยของบุคลากร โดยจุดแตกต่างที่สำคัญระหว่าง Industrial IoT และ IoT ได้แก่

ตารางที่ 1 ความแตกต่างระหว่าง IoT และ Industrial IoT

	IoT	Industrial IoT
ขอบเขต	ใช้ในชีวิตประจำวัน สำหรับผู้บริโภคที่ใช้งานทั่วไป	ใช้ในภาคอุตสาหกรรม และกระบวนการทางอุตสาหกรรมที่ซับซ้อน
สภาพแวดล้อม	การค้าปลีก, บ้าน, สำนักงาน	โรงงานอุตสาหกรรม, คลังสินค้า, และโรงงาน
การใช้งาน	บ้านอัจฉริยะ, เมืองอัจฉริยะ, Connected Vehicles, Wearable Health Devices	การบำรุงรักษาเชิงคาดการณ์, การอัตโนมัติและการปรับปรุงการผลิต, การจัดการพลังงานและกริดอัจฉริยะ, การจัดการห่วงโซ่อุปทานและโลจิสติกส์
ความซับซ้อน	งานที่ไม่ซับซ้อน เช่น การติดตามกิจกรรม การออกกำลังกายหรือปรับอุณหภูมิห้อง	งานที่ซับซ้อนและต้องการความแม่นยำสูง

	IoT	Industrial IoT
การเชื่อมต่อ	ใช้โปรโตคอลการสื่อสารทั่วไป เช่น Wi-Fi, Zigbee, Bluetooth, Broadband	ใช้โปรโตคอลการสื่อสารสำหรับอุตสาหกรรมโดยเฉพาะ เช่น Modbus, OPC-UA, Profinet
ปริมาณข้อมูล	ปานกลางถึงสูง	สูง
โปรโตคอลความปลอดภัย	ไม่จำเป็นต้องเข้มงวดมาก	ต้องมีการใช้โปรโตคอลความปลอดภัยขั้นสูงอย่างเข้มงวด
การเขียนโปรแกรม	ใช้ฟังก์ชันที่ตั้งโปรแกรมไว้แล้ว	สามารถเขียนโปรแกรมและปรับแต่งได้สูงตามความต้องการเฉพาะของผู้ใช้งาน
ความสามารถในการทำงานร่วมกัน	ทำงานได้โดยอิสระจากกัน	สามารถรวมเข้ากับระบบปฏิบัติการเก่าที่มีอยู่

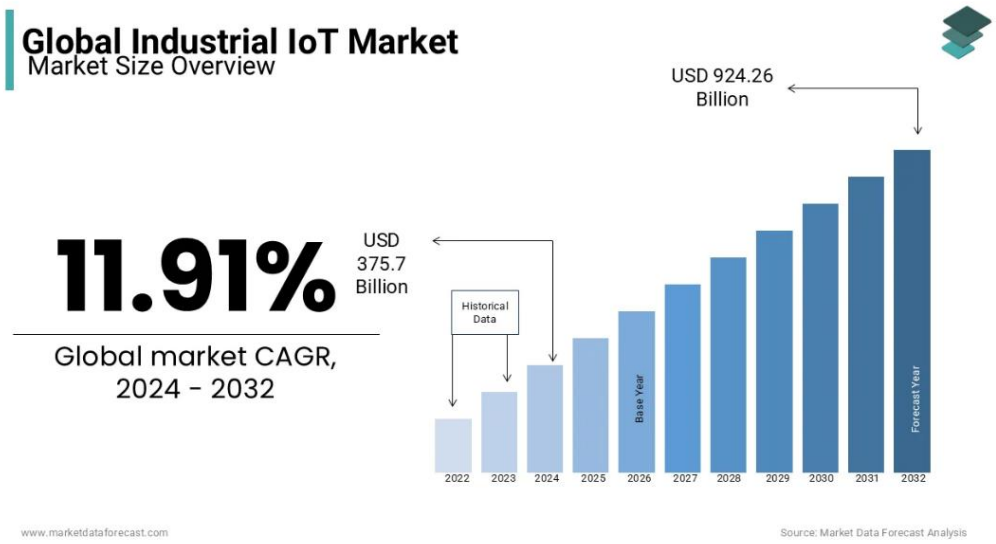
ที่มา: Imaginovation, 2024

Industrial IoT มีบทบาทสำคัญในการเปลี่ยนแปลงภาคการผลิตในหลายด้าน การนำ IIoT มาประยุกต์ใช้อย่างมีประสิทธิภาพจะนำไปสู่การลดต้นทุน เพิ่มผลิตภาพ ยกระดับคุณภาพ และสร้างความได้เปรียบทางการแข่งขันอย่างยั่งยืนในยุคอุตสาหกรรม 4.0 โดยศักยภาพที่สำคัญของ Industrial IoT ในการปฏิวัติกระบวนการผลิตและเพิ่มความสามารถในการแข่งขันของโรงงานอุตสาหกรรมในยุคดิจิทัล มีดังนี้

- **การเพิ่มประสิทธิภาพการผลิต** ถือเป็นศักยภาพหลักของ Industrial IoT โดยเทคโนโลยีเซ็นเซอร์อัจฉริยะที่ติดตั้งในกระบวนการผลิตสามารถเก็บข้อมูลแบบเรียลไทม์ ทำให้ผู้ประกอบการสามารถระบุและแก้ไขจุดที่เป็นปัญหาในสายการผลิตได้อย่างทันท่วงที อีกทั้งยังสามารถปรับเปลี่ยนกำลังการผลิตให้สอดคล้องกับความต้องการของตลาดได้อย่างแม่นยำ ส่งผลให้สามารถลดต้นทุนการผลิตและเพิ่มอัตราการผลิตได้อย่างมีประสิทธิภาพ
- **การบำรุงรักษาเชิงพยากรณ์** ระบบตรวจสอบสภาพเครื่องจักรแบบต่อเนื่องสามารถวิเคราะห์รูปแบบการทำงานและคาดการณ์ความผิดปกติก่อนที่จะเกิดความเสียหาย ทำให้สามารถช่วยในการวางแผนการซ่อมบำรุงได้อย่างมีประสิทธิภาพ ลดการหยุดชะงักของกระบวนการผลิตโดยไม่คาดคิด และยืดอายุการใช้งานของอุปกรณ์ ส่งผลให้อัตราการใช้งานสินทรัพย์สูงขึ้นและลดต้นทุนการบำรุงรักษาในระยะยาว
- **การควบคุมคุณภาพอัตโนมัติ** ระบบตรวจสอบด้วยภาพและเซ็นเซอร์อัจฉริยะสามารถตรวจจับข้อบกพร่องของผลิตภัณฑ์ได้อย่างแม่นยำและรวดเร็วกว่ามนุษย์ ทำให้สามารถคัดแยกสินค้าที่ไม่ได้มาตรฐานออกจากสายการผลิตได้ทันที และยังสามารถวิเคราะห์สาเหตุของปัญหาเพื่อป้องกันการเกิดซ้ำ ส่งผลให้อัตราการผลิตสินค้าที่มีคุณภาพสูงขึ้นและลดอัตราการเกิดของเสีย
- **การบูรณาการห่วงโซ่อุปทาน** การเชื่อมโยงข้อมูลระหว่างผู้ผลิต ซัพพลายเออร์ และลูกค้าทำให้เกิดความโปร่งใสและการตอบสนองที่รวดเร็ว การคาดการณ์ความต้องการที่แม่นยำช่วยให้การจัดการสินค้าคงคลังมีประสิทธิภาพมากขึ้น ลดความจำเป็นในการสำรองวัตถุดิบและสินค้าสำเร็จรูปในปริมาณมาก อีกทั้งยังสามารถติดตามสถานะการจัดส่งและคุณภาพของวัตถุดิบได้แบบเรียลไทม์

ทุกวันนี้อุตสาหกรรมทั่วโลกมีการนำ Industrial IoT มาประยุกต์ใช้อย่างแพร่หลายและกลายเป็นหัวใจสำคัญของการปฏิรูปกระบวนการผลิต Juniper Research คาดการณ์ว่า ในปี 2568 จำนวน Industrial IoT ทั่วโลกจะเพิ่มขึ้นเป็น 36.8 พันล้านเครื่อง เติบโตขึ้น 107% จากปี 2563 ซึ่งมีจำนวน Industrial IoT เพียง 17.7 พันล้านเครื่องเท่านั้น โดยการขยายตัวของ Industrial IoT ได้รับแรงหนุนจากเทคโนโลยีเครือข่ายที่พัฒนาไปสู่ 5G และ Low Power Wide Area (LPWA) Networks ซึ่งช่วยให้การรับส่งข้อมูลมีความรวดเร็วและเสถียรมากขึ้น ทำให้อุตสาหกรรมสามารถใช้ข้อมูลเรียลไทม์ในการปรับปรุงกระบวนการผลิตและบริหารจัดการซัพพลายเชนได้อย่างมีประสิทธิภาพ ซึ่ง Market Data Forecast Analysis คาดการณ์ว่า ตลาด Industrial IoT ทั่วโลกจะยังคงเติบโตขึ้นอย่างต่อเนื่องจากปี 2567 ที่มีมูลค่าตลาดประมาณ 375.7 พันล้านดอลลาร์สหรัฐ จะเพิ่มขึ้นเป็น 924.26 พันล้านดอลลาร์สหรัฐ ในปี 2575 โดยมีอัตราการเติบโตเฉลี่ยต่อปี (CAGR) อยู่ที่ 11.91% ระหว่างปี 2567 - 2575

ภาพที่ 1 แนวโน้มขนาดตลาด Industrial IoT ระหว่างปี 2565 - 2575



ที่มา: Market Data Forecast, 2024

การบูรณาการ Industrial IoT เข้ากับเทคโนโลยีขั้นสูงอื่น ๆ เช่น เทคโนโลยี AI, Machine Learning และการวิเคราะห์ Big Data ยิ่งเพิ่มศักยภาพในการสร้างมูลค่าให้กับภาคการผลิต ระบบการวิเคราะห์ขั้นสูงสามารถประมวลผลข้อมูลจำนวนมหาศาลที่รวบรวมจากอุปกรณ์ Industrial IoT เพื่อค้นหารูปแบบที่ซ่อนอยู่ คาดการณ์แนวโน้มในอนาคต และให้คำแนะนำสำหรับการตัดสินใจที่สำคัญ นอกจากนี้ Industrial IoT ยังมีบทบาทสำคัญในการส่งเสริมความยั่งยืนในภาคการผลิต ด้วยการติดตามและวิเคราะห์การใช้พลังงาน น้ำ และทรัพยากรอื่น ๆ แบบเรียลไทม์ช่วยให้องค์กรสามารถระบุโอกาสในการลดการใช้ทรัพยากรและลดผลกระทบต่อสิ่งแวดล้อม

ในอนาคตอันใกล้ ด้วยการพัฒนาของเทคโนโลยีเครือข่าย จะทำให้ Industrial IoT ไม่เพียงเป็นรากฐานสำคัญของ Industry 4.0 เท่านั้น แต่กลายเป็นตัวขับเคลื่อนหลักของการเปลี่ยนแปลงในภาคการผลิตทั่วโลก ด้วยความสามารถของ Industrial IoT ซึ่งช่วยให้ภาคการผลิตสามารถเปลี่ยนผ่านไปสู่การผลิตอัจฉริยะที่มีความยืดหยุ่น ตอบสนองได้อย่างรวดเร็วและยั่งยืนมากขึ้น องค์กรที่สามารถนำ Industrial IoT มาใช้อย่างมีประสิทธิภาพ

และรับมือกับความท้าทายที่เกี่ยวข้องจะอยู่ในตำแหน่งที่ได้เปรียบในการแข่งขันและพร้อมสำหรับอนาคตของการผลิตในยุคดิจิทัล ดังนั้น การนำ Industrial IoT มาใช้ไม่ใช่ทางเลือกแต่เป็นความจำเป็นสำหรับองค์กรที่ต้องการรักษาความสามารถในการแข่งขันในยุคดิจิทัล บริษัทที่ล้าหลังในการนำเทคโนโลยีนี้มาใช้อาจเสี่ยงต่อการสูญเสียส่วนแบ่งตลาดให้กับคู่แข่งที่มีความคล่องตัวและนวัตกรรมมากกว่า

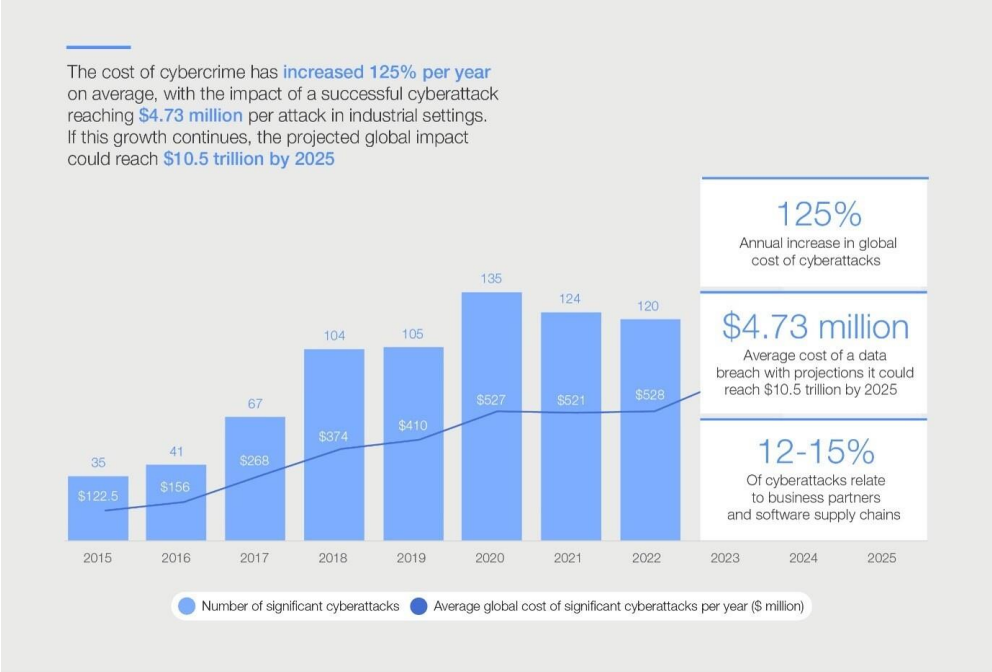
อย่างไรก็ตาม แม้ว่า Industrial IoT จะมอบประโยชน์อย่างมหาศาลให้กับภาคการผลิต แต่ก็มาพร้อมกับความท้าทายที่สำคัญ โดยเฉพาะในด้านความปลอดภัยทางไซเบอร์ การเชื่อมต่ออุปกรณ์และระบบจำนวนมากเข้ากับเครือข่ายทำให้เกิดความเสี่ยงด้านความปลอดภัยทางไซเบอร์ที่มีความซับซ้อนและความท้าทายอย่างไม่เคยปรากฏมาก่อน การละเมิดความปลอดภัยในระบบการผลิตที่เชื่อมต่อกันไม่เพียงแต่สร้างความเสี่ยงต่อการสูญเสียข้อมูลที่เป็นความลับเท่านั้น แต่ยังอาจส่งผลให้เกิดการหยุดชะงักของการผลิต ความเสียหายต่อเครื่องจักร หรือแม้กระทั่งอันตรายต่อความปลอดภัยของพนักงาน

ภัยคุกคามทางไซเบอร์ใน Industrial IoT

ในปีที่ผ่านมา รายงาน IBM X-Force Threat Intelligence Report ได้จัดให้อุตสาหกรรมการผลิตเป็นเป้าหมายลำดับหนึ่งของอาชญากรไซเบอร์ต่อเนื่องเป็นปีที่ 3 โดยคิดเป็น 25.7% ของการโจมตีทางไซเบอร์ในภาคอุตสาหกรรมทั้งหมด ภัยคุกคามหลักได้แก่ การโจมตีด้วยมัลแวร์ โดยเฉพาะแรนซัมแวร์ ซึ่งมีสัดส่วนสูงถึง 71% ของการโจมตีทั้งหมด แสดงให้เห็นว่า อุตสาหกรรมการผลิตทั่วโลกกำลังตกอยู่ในความอันตรายทางไซเบอร์ที่รุนแรงขึ้นเรื่อย ๆ และกำลังเผชิญกับความเสี่ยงที่อาจทำให้ระบบการผลิตพังทลาย และอุตสาหกรรมต้องหยุดชะงักโดยสิ้นเชิง

World Economic Forum ระบุสาเหตุสำคัญที่ทำให้อุตสาหกรรมการผลิตกลายเป็นเป้าหมายหลักในการโจมตี นั่นคือ การที่ภาคการผลิตไม่สามารถปล่อยให้เครื่องจักรหยุดการทำงาน (Downtime) ได้นาน เนื่องจากส่งผลต่อรายได้และต้นทุนโดยตรง รวมถึงยังส่งผลกระทบต่อห่วงโซ่อุปทานทั้งระบบ ประกอบกับการที่ภาคการผลิตมีระดับวุฒิภาวะทางไซเบอร์ (Cyber Maturity) ต่ำ และการมีรอบการผลิตที่ยาวนานและต้องใช้เงินลงทุนสูงในการปรับปรุงสายการผลิตจึงมักลงทุนด้านการรับมือกับภัยคุกคามทางไซเบอร์ (Cyber Resilience) น้อยกว่าภาคธุรกิจอื่น ๆ ทำให้อุตสาหกรรมการผลิตกลายเป็นเป้าหมายของอาชญากรไซเบอร์ที่ต้องการใช้แรงกดดันเพื่อเรียกค่าไถ่หรือแสวงหาผลประโยชน์ทางการเงินแบบต่าง ๆ ส่งผลให้ภาคการผลิตมีมูลค่าความเสียหายจากการโจมตีทางไซเบอร์เพิ่มขึ้นถึง 125% ต่อปี โดยผลกระทบจากการโจมตีทางไซเบอร์ที่ประสบความสำเร็จในภาคอุตสาหกรรมนั้นทำให้เกิดความสูญเสียเฉลี่ย 4.73 ล้านดอลลาร์สหรัฐต่อการโจมตี 1 ครั้ง และคาดการณ์ว่า ในปี 2568 อาจเกิดความสูญเสียเฉลี่ยสูงถึง 10.5 ล้านล้านดอลลาร์สหรัฐต่อการโจมตี 1 ครั้ง ทำให้ความเสี่ยงไซเบอร์ถูกจัดให้เป็นความเสี่ยงภายนอกลำดับ 3 ที่สำคัญที่สุดของอุตสาหกรรมภาคการผลิต โดย 12-15% ของการโจมตีทางไซเบอร์เกี่ยวข้องกับคู่ค้าทางธุรกิจและ Software Supply Chain (กระบวนการทั้งหมดที่เกี่ยวข้องกับการพัฒนา จัดหา และส่งมอบซอฟต์แวร์)

ภาพที่ 2 มูลค่าความเสียหายจากการโจมตีทางไซเบอร์ในภาคอุตสาหกรรม



ที่มา: World Economic Forum, 2024

รูปแบบการโจมตีทางไซเบอร์ที่พบใน Industrial IoT

รูปแบบการโจมตีทางไซเบอร์ที่พบใน Industrial IoT มีหลายรูปแบบ โดยส่วนใหญ่มักมุ่งเป้าหมายไปที่โครงสร้างพื้นฐานและอุปกรณ์เชื่อมต่อในอุตสาหกรรมการผลิต โรงงานอัจฉริยะ และระบบอัตโนมัติ โดยรูปแบบการโจมตีที่พบได้บ่อยที่สุด มีดังนี้

1. มัลแวร์ (Malware)

เป็นซอฟต์แวร์ที่ถูกออกแบบมาโดยเฉพาะเพื่อวัตถุประสงค์ที่เป็นอันตราย อุปกรณ์ Industrial IoT มีความเสี่ยงต่อมัลแวร์เป็นพิเศษ เนื่องจาก Industrial IoT มักมีหน่วยประมวลผลที่มีประสิทธิภาพต่ำ หน่วยความจำจำกัด และแบนด์วิดธ์น้อย ทำให้ไม่สามารถรองรับซอฟต์แวร์ป้องกันที่ซับซ้อนได้ ในขณะเดียวกัน อุปกรณ์ Industrial IoT ถูกออกแบบให้สามารถทำงานเป็นเวลานานโดยไม่ต้องมีการอัปเกรด ส่งผลให้ยังคงใช้ซอฟต์แวร์ที่ล้าสมัยและมีช่องโหว่ ทั้งนี้ มัลแวร์ที่พบในระบบ Industrial IoT มีหลายรูปแบบ แต่ละแบบมีวัตถุประสงค์และกลไกการทำงานที่แตกต่างกัน ได้แก่

1.1 มัลแวร์เฉพาะทางอุตสาหกรรม (Industrial-Specific Malware) เป็นมัลแวร์ที่ถูกออกแบบมาเพื่อโจมตีระบบควบคุมอุตสาหกรรมและโครงสร้างพื้นฐานที่สำคัญโดยเฉพาะ ลักษณะพิเศษของมัลแวร์ชนิดนี้คือ ผู้พัฒนามัลแวร์มีความรู้เฉพาะทางและมีความเข้าใจอย่างลึกซึ้งในโปรโตคอลและระบบอุตสาหกรรม จึงสามารถแทรกแซงกระบวนการทำงานของระบบอุตสาหกรรมได้อย่างแม่นยำ ตัวอย่างมัลแวร์เฉพาะทางอุตสาหกรรมที่มีชื่อเสียง เช่น

- **Stuxnet** ถูกสร้างขึ้นเพื่อโจมตีระบบควบคุมอุตสาหกรรม ด้วยการทำลายระบบ SCADA โดยเฉพาะ PLCs ในปี 2553 Stuxnet ได้โจมตีโรงงานเสริมสมรรถนะยูเรเนียมของอิหร่าน ด้วยการแทรกแซง

ความเร็วของเครื่องหมุนเหวี่ยง (Centrifuges) ซึ่งใช้แยกไอโซโทปยูเรเนียมเพื่อผลิตเชื้อเพลิงนิวเคลียร์ ซึ่งส่งผลให้เครื่องหมุนเหวี่ยงกว่า 1,000 เครื่องได้รับความเสียหาย และเสี่ยงต่อการเกิดระเบิดร้ายแรงภายในโรงงาน ซึ่งจะสร้างความเสียหายมหาศาลและคร่าชีวิตพนักงานจำนวนมาก Stuxnet ถือเป็นอาวุธไซเบอร์แรกของโลกที่สร้างความเสียหายในโลกจริงและเป็นจุดเริ่มต้นที่แสดงให้เห็นว่า ภัยคุกคามทางไซเบอร์สามารถทำลายระบบอุตสาหกรรมได้

- **Industroyer / CrashOverride** เป็นมัลแวร์อุตสาหกรรมที่ถูกใช้โจมตีโครงข่ายไฟฟ้าโดยเฉพาะ SCADA และ ICS (Industrial Control System) ซึ่งควบคุมโครงสร้างพื้นฐานด้านพลังงาน ในปี 2559 Industroyer ถูกใช้โจมตีโรงไฟฟ้าในยูเครน ด้วยการปิดสวิตช์จ่ายไฟในสถานีไฟฟ้าย่อยและขัดขวางการทำงานของระบบควบคุมระยะไกล ทำให้วิศวกรไม่สามารถกู้คืนระบบได้ทันที ส่งผลให้ไฟฟ้าดับทั่วกรุงเคียฟ ระบบขนส่ง โรงพยาบาล และอุตสาหกรรมทั้งหมดต้องหยุดชะงักเป็นเวลาหลายชั่วโมง กระทบชีวิตประชาชนหลายแสนคน

- **Triton / TRISIS** เป็นมัลแวร์ที่มุ่งเป้าหมายไปที่ระบบความปลอดภัยเครื่องมือ (Safety Instrumented Systems) ซึ่งเป็นระบบที่ใช้ปกป้องโรงงานจากอุบัติเหตุร้ายแรง โดยทำหน้าที่ตรวจจับสภาวะที่เป็นอันตรายและหยุดการทำงานของโรงงานอย่างปลอดภัย ในปี 2560 Triton ได้โจมตีโรงงานปิโตรเคมีในซาอุดีอาระเบีย โดยพยายามปิดการทำงานของระบบ Triconex SIS ซึ่งทำหน้าที่ควบคุมกระบวนการผลิต ส่งผลให้โรงงานต้องหยุดการผลิตฉุกเฉิน ซึ่งหาก Triton สำเร็จ อาจนำไปสู่การระเบิดครั้งใหญ่ที่ทำให้พนักงานเสียชีวิตและโรงงานถูกทำลาย Triton ถือเป็นหนึ่งในมัลแวร์เฉพาะทางอุตสาหกรรมที่อันตรายที่สุด เพราะไม่ได้มุ่งเน้นการทำลายข้อมูลหรือเรียกค่าไถ่ แต่พุ่งเป้าไปที่การทำลายชีวิตและโครงสร้างโรงงานโดยตรง

1.2 บอทเน็ต Industrial IoT (Industrial IoT Botnet) เป็นเครือข่ายของอุปกรณ์ Industrial IoT ที่ถูกควบคุมโดยไม่ได้รับอนุญาตผ่านมัลแวร์หรือซอฟต์แวร์ที่เป็นอันตราย โดยอุปกรณ์เหล่านี้จะถูกเรียกว่า "บอท" (Bot) หรือ "ซอมบี้" (Zombie) ซึ่งสามารถรับคำสั่งผ่านเซิร์ฟเวอร์ควบคุมและบัญชาการ (Command and Control) เพื่อทำการโจมตีเป้าหมายพร้อมกัน บอทเน็ต Industrial IoT มีลักษณะแตกต่างจากบอทเน็ตทั่วไป โดยบอทเน็ตทั่วไปมักประกอบด้วยคอมพิวเตอร์ส่วนบุคคลหรืออุปกรณ์ IoT ทั่วไป เช่น กล้องวงจรปิด เราเตอร์ หรืออุปกรณ์สมาร์ทโฮม ในขณะที่บอทเน็ต Industrial IoT มุ่งเน้นไปที่อุปกรณ์ในภาคอุตสาหกรรม เช่น เซ็นเซอร์อุตสาหกรรม, SCADA, PLCs, HMI และอุปกรณ์ Industrial IoT อื่น ๆ ที่เชื่อมต่อกับเครือข่าย เป็นต้น บอทเน็ต Industrial IoT มักแพร่กระจายผ่านช่องโหว่ด้านความปลอดภัยในอุปกรณ์ Industrial IoT เช่น อุปกรณ์ที่ใช้รหัสผ่านเริ่มต้นจากโรงงานโดยไม่ได้ถูกเปลี่ยนหลังการติดตั้ง หรือซอฟต์แวร์หรือเฟิร์มแวร์ที่ไม่ได้รับการอัปเดต ซึ่งอาจมีช่องโหว่ที่ผู้โจมตีสามารถใช้ประโยชน์ได้ ตัวอย่างบอทเน็ต Industrial IoT ที่สำคัญ เช่น

- **VPNFilter** เป็นมัลแวร์แบบโมดูลาร์ที่มีเป้าหมายโจมตีเราเตอร์และอุปกรณ์เครือข่าย Industrial IoT ในอุตสาหกรรมและโครงสร้างพื้นฐานสำคัญ รวมถึง Linksys, MikroTik, NETGEAR และ TP-Link โดยมีความสามารถในการเจาะระบบเราเตอร์และอุปกรณ์เครือข่ายผ่านช่องโหว่ของเราเตอร์และ NAS (Network-Attached Storage) และติดตั้งตัวเองหลังการรีบูตอุปกรณ์เครือข่าย ทำหน้าที่ดักจับและวิเคราะห์ข้อมูล เช่น รหัสผ่านหรือความลับทางการค้าต่าง ๆ ที่ส่งผ่านไปยังระบบควบคุมอุตสาหกรรม แก้ไขข้อมูลที่ส่งระหว่างกัน และขัดขวางการทำงานด้วยการลบเฟิร์มแวร์หรือทำให้อุปกรณ์ใช้งานไม่ได้ และที่สำคัญคือใช้อุปกรณ์ที่ติดเชื้อเป็นบอท

เน็ตเพื่อโจมตีเครือข่ายและองค์กรขนาดใหญ่ โดยในปี 2561 FBI ได้แจ้งเตือนว่า VPNFilter ได้ถูกติดตั้งในอุปกรณ์กว่า 500,000 เครื่องใน 54 ประเทศ รวมถึงอุปกรณ์ในระบบโครงสร้างพื้นฐานสำคัญหลายแห่ง

- **Mirai Industrial IoT Variant** เป็นเวอร์ชันพัฒนาต่อจาก Mirai Botnet ซึ่งเป็นมัลแวร์ชื่อดัง โดยถูกออกแบบมาเพื่อโจมตีอุปกรณ์ Industrial IoT และ ICS โดยเฉพาะ ด้วยการเจาะระบบอุปกรณ์ด้วย Brute Force Attack เพื่อเดารหัสผ่านของอุปกรณ์ที่ไม่ได้เปลี่ยนค่าเริ่มต้นจากโรงงาน และทำการโจมตีระบบอุตสาหกรรม เช่น SCADA, PLCs รวมถึงอุปกรณ์ Industrial IoT ในโรงงาน ให้ขัดขวางการผลิตและการทำงานของโครงสร้างพื้นฐานสำคัญ เช่น ทำให้เกิดไฟฟ้าดับ เครื่องจักรขัดข้อง หรือการผลิตหยุดชะงัก รวมถึงขโมยข้อมูลอุตสาหกรรมส่งต่อให้กลุ่มแฮ็กเกอร์หรือคู่แข่ง นอกจากนี้ Mirai Industrial IoT Variant ยังสามารถใช้ในการควบคุมอุปกรณ์ที่ถูกเจาะให้กลายเป็นส่วนหนึ่งของเครือข่ายกองทัพบ็อตในการโจมตีแบบ DDoS (Distributed Denial-of-Service) ซึ่งส่งผลให้ระบบโรงงานและเครือข่ายอุตสาหกรรมล่มได้ โดยในปี 2562 มีการพบ Mirai ทำการโจมตี Industrial IoT โดยเฉพาะ และในปี 2565 ยังถูกใช้ในการโจมตีโรงงานและโครงข่ายพลังงานในหลายประเทศ

1.3 แรนซัมแวร์ (Ransomware) แรนซัมแวร์เป็นประเภทของมัลแวร์ที่เข้ารหัสข้อมูลหรือล็อคระบบของเหยื่อ แล้วเรียกค่าไถ่เพื่อคืนการเข้าถึง สำหรับ Industrial IoT แรนซัมแวร์มีความอันตรายเป็นพิเศษ เนื่องจากผลกระทบต่อการดำเนินงานและความปลอดภัยทางกายภาพ ลักษณะเฉพาะของแรนซัมแวร์ในบริบท Industrial IoT คือ มักมุ่งเป้าหมายไปที่ระบบควบคุมและการมองเห็น เช่น SCADA หรือ HMI มากกว่าตัวอุปกรณ์เอง ซึ่งเป็นยุทธศาสตร์ที่ชาญฉลาด เนื่องจากการรบกวนการควบคุมสามารถหยุดการดำเนินงานได้โดยไม่ต้องเข้ารหัสระบบที่มีความซับซ้อน และค่าไถ่ที่ผู้โจมตีเรียกร้องมักสูงกว่าการโจมตีอุปกรณ์ IT ทั่วไป เนื่องจากต้นทุนของการหยุดชะงักของเครื่องจักรหรืออุปกรณ์ในอุตสาหกรรมการผลิตมีมูลค่าสูงมาก สร้างแรงกดดันมหาศาลให้องค์กรต้องแก้ไขปัญหาโดยเร็วและนำไปสู่การตัดสินใจจ่ายค่าไถ่ ตัวอย่างที่สำคัญของแรนซัมแวร์ใน Industrial IoT มีดังนี้

- **EKANS** หรือที่รู้จักในชื่อ Snake เป็นแรนซัมแวร์ที่ได้รับการค้นพบในปี 2563 ถูกออกแบบมาเฉพาะเพื่อมุ่งเป้าหมายไปที่ระบบ ICS โดย EKANS มีลักษณะเด่นคือมี "Kill List" ที่จำเพาะเจาะจงกับกระบวนการที่เกี่ยวข้องกับ ICS เช่น GE Proficy, Honeywell HMIWeb และ ThingWorx หลังจากเข้าถึงระบบเป้าหมาย EKANS จะยุติกระบวนการทำงานของซอฟต์แวร์และเข้ารหัสข้อมูลสำคัญ ทำให้ Industrial IoT ไม่สามารถทำงานได้จนกว่าจะมีการจ่ายค่าไถ่ ในปี 2563 EKANS ได้ทำการโจมตีบริษัท Honda จนส่งผลกระทบต่อเครือข่ายคอมพิวเตอร์ของ Honda ทั่วโลก ทำให้บริษัทต้องหยุดการผลิตชั่วคราวในหลายประเทศ รวมถึงสหรัฐอเมริกา ตุรกี อินเดีย และบราซิล
- **DarkSide** ได้สร้างความเสียหายอย่างมหาศาลในการโจมตีระบบ Industrial IoT ของบริษัท Colonial Pipeline ในปี 2564 ซึ่งเป็นผู้ให้บริการท่อส่งน้ำมันรายใหญ่ที่สุดในสหรัฐอเมริกาที่ดูแลท่อส่งน้ำมันกว่า 8,850 กิโลเมตรจากเท็กซัสไปถึงชายฝั่งตะวันออกของประเทศ การโจมตีส่งผลกระทบต่อระบบเครือข่ายที่เชื่อมโยงกับอุปกรณ์ Industrial IoT ทำให้บริษัทไม่สามารถเข้าถึงข้อมูลการตรวจสอบและควบคุมระบบได้ จนต้องหยุดการดำเนินงานของระบบท่อส่งน้ำมันทั้งหมดเป็นเวลาหลายวัน ส่งผลให้เกิดวิกฤตพลังงานชั่วคราวในภูมิภาคตะวันออกของสหรัฐฯ ก่อให้เกิดความเสียหายเป็นมูลค่ามากถึง 4 พันล้านดอลลาร์สหรัฐ
- **BlackMatter** เป็นแรนซัมแวร์ที่นักวิเคราะห์ความปลอดภัยทางไซเบอร์เชื่อว่ามีความเชื่อมโยงอย่างมากกับ DarkSide โดยมุ่งเป้าหมายไปที่บริษัทในภาคการเกษตรและการผลิตอาหารที่ใช้ระบบ

Industrial IoT ในกระบวนการผลิต การโจมตีที่มีชื่อเสียงมากที่สุดของ BlackMatter คือการโจมตีบริษัท NEW Cooperative ในสหรัฐอเมริกาในปี 2564 ซึ่งส่งผลกระทบต่อระบบอัตโนมัติในไซโลเก็บธัญพืช และระบบจัดส่งอาหารสัตว์ โดยมีการเรียกค่าไถ่ 5.9 ล้านดอลลาร์สหรัฐ เพื่อแลกกับกุญแจถอดรหัสและคำสัญญาที่จะไม่เผยแพร่ข้อมูลที่ขโมยมา ถึงแม้ BlackMatter ได้ประกาศยุติการดำเนินงานหลังจากปฏิบัติการเพียง 4 เดือน แต่ได้สร้างความเสียหายอย่างมากต่อองค์กรหลายแห่งทั่วโลก

- **LockBit 2.0** เป็นแรนซัมแวร์ที่มีการพัฒนาให้สามารถแพร่กระจายตัวเองโดยอัตโนมัติในเครือข่าย Industrial IoT ได้ ด้วยการเข้ารหัสไฟล์และปิดกั้นการเข้าถึงข้อมูล โดยสามารถปิดการทำงานของ Windows Defender และ Antivirus รวมถึงสามารถหลีกเลี่ยงการตรวจจับจากระบบ SIEM (Security Information and Event Management) ซึ่งมีหน้าที่รวบรวม ตรวจสอบหาจุดเสี่ยง วิเคราะห์ และระบุตำแหน่งของภัยคุกคาม LockBit 2.0 เป็นแรนซัมแวร์ที่มีความอันตรายเป็นอย่างมาก เนื่องจากมีการเปิดให้แฮ็กเกอร์เช่าหรือซื้อไปใช้ในรูปแบบ Ransomware-as-a-Service (RaaS) เพื่อโจมตีองค์กรต่าง ๆ ทั่วโลก โดยเฉพาะในอุตสาหกรรมการผลิต พลังงาน และโครงสร้างพื้นฐานที่สำคัญ จำนวนองค์กรที่เคยถูก LockBit 2.0 โจมตีมีจำนวนมากถึง 1,700 แห่งทั่วโลก

2. การโจมตีแบบ Man-in-the-Middle (MitM)

เป็นหนึ่งในการคุกคามที่พบบ่อยที่สุดในระบบ Industrial IoT โดยผู้โจมตีจะวางตัวเองอยู่ระหว่างผู้ส่งและผู้รับข้อมูล ทำให้สามารถดักฟัง ดักจับ และแม้กระทั่งเปลี่ยนแปลงข้อมูลที่ส่งระหว่างกันได้อย่างแยบยล ลักษณะสำคัญของการโจมตีนี้คือ ทั้งผู้ส่งและผู้รับไม่สามารถรับรู้ได้ว่ามีผู้โจมตีแทรกอยู่ในการสื่อสาร ทำให้ทั้งสองฝ่ายเชื่อว่ากำลังสื่อสารโดยตรงกับอีกฝ่ายอย่างปลอดภัย การโจมตีแบบนี้มีความซับซ้อนและอันตรายเป็นพิเศษในบริบทของ Industrial IoT เนื่องจากระบบ Industrial IoT มักประกอบด้วยอุปกรณ์จำนวนมากที่สื่อสารกันผ่านโปรโตคอลที่หลากหลาย ซึ่งบางส่วนอาจไม่ได้ถูกออกแบบมาโดยคำนึงถึงความปลอดภัยเป็นหลัก การโจมตีแบบ MitM สามารถเกิดขึ้นได้หลายรูปแบบ เช่น

- **การโจมตี ARP Spoofing** ผู้โจมตีส่งข้อความ ARP (Address Resolution Protocol) ปลอมเพื่อเชื่อมโยง MAC Address ของผู้โจมตีกับ IP Address ของอุปกรณ์เป้าหมายหรือเกตเวย์ ทำให้ข้อมูลทั้งหมดถูกส่งผ่านไปยังผู้โจมตีก่อนที่จะถูกส่งต่อไปยังปลายทางที่แท้จริง
- **การโจมตี DNS Spoofing** ผู้โจมตีปลอมแปลงคำตอบของ DNS (Domain Name System) เพื่อทำให้ Industrial IoT ให้เชื่อมต่อกับเซิร์ฟเวอร์ที่ควบคุมโดยผู้โจมตี แทนที่จะเชื่อมต่อกับเซิร์ฟเวอร์ที่ถูกต้อง
- **การโจมตี SSL/TLS Stripping** ผู้โจมตีลดระดับการเชื่อมต่อ HTTPS ให้เป็น HTTP ทำให้การสื่อสารไม่มีการเข้ารหัส และง่ายต่อการดักจับข้อมูล
- **การปลอมแปลงจุดเชื่อมต่อ Wi-Fi** ผู้โจมตีสร้างจุดเชื่อมต่อ Wi-Fi ปลอมที่มีชื่อเหมือนกับเครือข่ายที่อุปกรณ์ Industrial IoT เชื่อมต่ออยู่ เพื่อให้อุปกรณ์เชื่อมต่อกับจุดเชื่อมต่อปลอมแทน
- **การโจมตีโปรโตคอลอุตสาหกรรม** หลายโปรโตคอลที่ใช้ใน Industrial IoT เช่น Modbus, MQTT, OPC UA อาจมีช่องโหว่ที่ผู้โจมตีสามารถใช้ประโยชน์เพื่อแทรกตัวเข้าไปในการสื่อสาร

การโจมตีแบบ Man-in-the-Middle สามารถสร้างความเสียหายอย่างร้ายแรงต่อภาคอุตสาหกรรมการผลิต เนื่องจากแฮกเกอร์สามารถดักจับหรือแก้ไขข้อมูลที่ถูกส่งระหว่างระบบและอุปกรณ์ ทำให้ข้อมูลสำคัญ เช่น คำสั่งการผลิตหรือข้อมูลลูกค้า ถูกขโมยหรือถูกปลอมแปลงได้ ซึ่งอาจนำไปสู่ความผิดพลาดในการดำเนินงานและกระบวนการผลิตที่ผิดเพี้ยน หากการโจมตีส่งผลให้เกิดข้อบกพร่องในผลิตภัณฑ์อาจจำเป็นต้องมีการเรียกคืนสินค้า ซึ่งสร้างต้นทุนทางการเงินที่สูงและกระทบต่อความเชื่อมั่นของลูกค้า นอกจากนี้ การโจมตียังอาจทำให้ระบบขัดข้อง ส่งผลให้กระบวนการผลิตหยุดชะงักและเกิดความสูญเสียทางเศรษฐกิจ ทั้งหมดนี้เป็นการทำลายชื่อเสียงขององค์กรและอาจทำให้สูญเสียโอกาสทางธุรกิจในระยะยาว ตัวอย่างที่เคยเกิดขึ้น เช่น

- ผู้โจมตีได้แทรกตัวในเครือข่าย Industrial IoT โรงงานผลิตชิ้นส่วนยานยนต์ในญี่ปุ่น ในปี 2561 ด้วยวิธี ARP Spoofing และดักจับข้อมูลการสื่อสารระหว่างเครื่องจักร CNC กับระบบควบคุมกลางให้พารามิเตอร์การผลิตถูกเปลี่ยนแปลงเล็กน้อย ทำให้ชิ้นส่วนที่ผลิตออกมามีขนาดคลาดเคลื่อนจากมาตรฐาน ส่งผลให้ต้องเรียกคืนชิ้นส่วนกว่า 100,000 ชิ้น เกิดความเสียหายต่อชื่อเสียงและค่าใช้จ่ายในการแก้ไขมากกว่า 10 ล้านดอลลาร์สหรัฐ
- ผู้โจมตีใช้เทคนิค DNS Spoofing โจมตีโรงงานอาหารในสหรัฐอเมริกา ในปี 2562 หลอกให้อุปกรณ์ Industrial IoT ในระบบแปรรูปอาหารเชื่อมต่อกับเซิร์ฟเวอร์ปลอม ส่งผลให้ระบบควบคุมอุณหภูมิในกระบวนการแปรรูปอาหารถูกปรับเปลี่ยน ทำให้การฆ่าเชื้อไม่สมบูรณ์ เกิดการปนเปื้อนในผลิตภัณฑ์บางส่วน นำไปสู่การเรียกคืนสินค้า ความเสียหายทางการเงินประมาณ 15 ล้านดอลลาร์สหรัฐ และมีผู้ป่วยจากการบริโภคอาหารที่ปนเปื้อนกว่า 50 ราย
- ผู้โจมตีได้ทำการโจมตีช่องโหว่ในโปรโตคอล OPC UA ที่ใช้ในการสื่อสารระหว่างเครื่องจักรในโรงงานผลิตชิปเซมิคอนดักเตอร์ในไต้หวัน ในปี 2564 จนทำให้เกิดความผิดพลาดในกระบวนการผลิตชิป ทำให้ Yield Rate ลดลงอย่างมีนัยสำคัญ จาก 92% เหลือเพียง 68% โดยที่ระบบตรวจสอบคุณภาพไม่พบความผิดปกติเนื่องจากข้อมูลถูกปลอมแปลง ส่งผลให้เกิดความล่าช้าในการผลิตและเสียหายทางการเงินกว่า 50 ล้านดอลลาร์สหรัฐ

3. การโจมตีแบบ Distributed Denial of Service (DDoS)

เป็นการโจมตีที่มุ่งเป้าหมายไปที่ความพร้อมใช้งานของระบบ Industrial IoT โดยพยายามครอบงำทรัพยากรของระบบและทำให้ไม่สามารถให้บริการผู้ใช้ที่ถูกต้องได้ เช่น ระบบเครือข่ายล่ม ล่าช้า หรือใช้งานไม่ได้ การโจมตี DDoS มักมีความซับซ้อนเพราะคำร้องขอที่ส่งมาจะเลียนแบบพฤติกรรมของผู้ใช้จริง ทำให้ยากต่อการตรวจจับและป้องกัน โดยมักเกี่ยวข้องกับการใช้เครือข่ายของอุปกรณ์ที่ถูกบุกรุกจำนวนมาก (Botnet) เพื่อสร้างปริมาณการรับส่งข้อมูลมหาศาลที่มุ่งไปยังเป้าหมาย ระบบ Industrial IoT มีความเสี่ยงเป็นพิเศษต่อการโจมตี DDoS เนื่องจากอุปกรณ์ Industrial IoT จำนวนมากมีทรัพยากรการประมวลผล หน่วยความจำ และแบนด์วิดธ์ที่จำกัด ทำให้ง่ายต่อการครอบงำ การโจมตี DDoS ใน Industrial IoT มีหลายรูปแบบ ตัวอย่างเช่น

- **การโจมตีระดับเครือข่าย (Network Layer Attacks)** การสร้างการรับส่งข้อมูลปริมาณมหาศาลเพื่อครอบงำแบนด์วิดธ์เครือข่าย เช่น การโจมตีแบบ SYN Flood (การส่งคำขอเชื่อมต่อจำนวนมหาศาลไปยังเซิร์ฟเวอร์ แต่ไม่ตอบกลับ ทำให้เซิร์ฟเวอร์ทำงานหนักจนล่ม) หรือ UDP Flood (การส่งหน่วยข้อมูลจำนวนมากผ่านโปรโตคอล UDP ไปยังเป้าหมายเพื่อให้ระบบเครือข่ายรับภาระเกินขีดจำกัด จนเกิดความล่าช้าหรือใช้งานไม่ได้)

- **การโจมตีระดับแอปพลิเคชัน (Application Layer Attacks)** การโจมตีมุ่งเป้าหมายไปที่แอปพลิเคชันหรือซอฟต์แวร์ที่ใช้ในระบบ Industrial IoT เช่น SCADA , HMI หรือซอฟต์แวร์ควบคุมกระบวนการผลิต โดยผู้โจมตีจะส่งคำร้องขอจำนวนมากไปยังเซิร์ฟเวอร์หรือแอปพลิเคชันเพื่อให้ใช้ทรัพยากรเกินขีดจำกัด จนไม่สามารถให้บริการแก่ผู้ใช้ตามปกติได้

- **การโจมตีแบบใช้โปรโตคอล (Protocol-Based Attacks)** เป็นการโจมตีที่มุ่งเป้าหมายไปที่ช่องโหว่ของโปรโตคอลเครือข่าย เช่น TCP, UDP, ICMP และ DNS เพื่อทำให้ระบบเครือข่ายของเป้าหมายใช้ทรัพยากรเกินขีดจำกัดจนไม่สามารถให้บริการได้ โดยตัวอย่างการโจมตีที่พบบ่อย ได้แก่ TCP SYN Flood ซึ่งเป็นการส่งคำขอเชื่อมต่อจำนวนมากแต่ไม่ตอบกลับ ทำให้เซิร์ฟเวอร์รอการเชื่อมต่อจนทรัพยากรถูกใช้หมด

- **การโจมตีที่กระจายต่อเนื่อง (Low-rate DoS)** การรบกวนการทำงานของโปรโตคอลหรือแอปพลิเคชัน โดยเน้นที่การส่งข้อมูลเป็นช่วง ๆ ในปริมาณทราฟฟิกที่ต่ำ เพื่อหลีกเลี่ยงการตรวจจับจากระบบป้องกัน จึงไม่ทำให้ระบบเครือข่ายหรือเซิร์ฟเวอร์ล่มในทันที แต่ส่งผลกระทบต่อประสิทธิภาพของระบบในระยะยาว

- **การโจมตีแบบปฏิเสธการให้บริการถาวร (Permanent Denial-of-Service)** เป็นรูปแบบที่ร้ายแรงที่สุดสำหรับอุปกรณ์ IIoT เนื่องจากมีเป้าหมายที่จะทำลายอุปกรณ์อย่างถาวร โดยโจมตีเพื่อให้เกิดความเสียหายต่อเฟิร์มแวร์หรือฮาร์ดแวร์ ทำให้อุปกรณ์ไม่สามารถทำงานได้อย่างถาวร

การโจมตีแบบ DDoS ไม่เพียงแต่สร้างความเสียหายทางการเงินโดยตรงจากการหยุดชะงักของระบบ แต่ยังส่งผลกระทบในวงกว้างต่อกระบวนการผลิตและการดำเนินงานขององค์กร โดยเฉพาะในภาคอุตสาหกรรมที่ต้องพึ่งพาเครือข่ายและระบบดิจิทัลอย่างต่อเนื่อง หากระบบ Industrial IoT ถูกโจมตีจนไม่สามารถทำงานได้ อุปกรณ์อัตโนมัติและห่วงโซ่อุปทานอาจหยุดชะงัก จะส่งผลให้กระบวนการผลิตล่าช้าและอาจเกิดข้อผิดพลาดที่กระทบต่อคุณภาพของสินค้า นอกจากนี้ ความน่าเชื่อถือของบริษัทอาจลดลงในสายตาของลูกค้าและคู่ค้า ยิ่งไปกว่านั้น การส่งมอบสินค้าที่ล่าช้าหรือผิดพลาดเนื่องจากระบบล่ม อาจนำไปสู่การผิดสัญญาทางธุรกิจและความเสียหายต่อชื่อเสียงในระยะยาว ตัวอย่างการโจมตีแบบ DDoS ที่เกิดขึ้นในภาคอุตสาหกรรมการผลิต เช่น

- การโจมตี DDoS แบบ UDP Flood โรงงานอิเล็กทรอนิกส์ในเกาหลีใต้ ในปี 2563 เป็นการโจมตีแบบมุ่งเป้าหมายไปที่เกตเวย์ Industrial IoT หลักที่ควบคุมระบบการผลิตชิ้นส่วนอิเล็กทรอนิกส์ จนระบบ SCADA ไม่สามารถสื่อสารกับอุปกรณ์ในสายการผลิตได้ ทำให้เกิดความล่าช้าในการผลิตและระบบควบคุมคุณภาพทำงานผิดพลาด สินค้าบางส่วนถูกผลิตโดยไม่ผ่านการตรวจสอบคุณภาพที่เหมาะสม ต้องเรียกคืนชิ้นส่วนอิเล็กทรอนิกส์มากกว่า 50,000 ชิ้น และเกิดความเสียหายราว 7 ล้านดอลลาร์สหรัฐ

- การโจมตี DDoS แบบระดับแอปพลิเคชันของโรงงานผลิตอุปกรณ์การแพทย์ในสหรัฐอเมริกา ในปี 2566 เป็นการโจมตีที่มุ่งเป้าหมายไปยังเซิร์ฟเวอร์ด้านการจัดการคุณภาพที่เชื่อมโยงกับระบบการผลิต ให้ไม่สามารถตรวจสอบคุณภาพและบันทึกข้อมูลการติดตามที่จำเป็นตามข้อกำหนดของ FDA ทำให้บริษัทต้องเรียกคืนอุปกรณ์การแพทย์ที่ผลิตในช่วงการโจมตี เนื่องจากไม่สามารถยืนยันได้ว่าผ่านการตรวจสอบคุณภาพอย่างเหมาะสม ส่งผลให้เกิดความสูญเสียทางการเงินกว่า 10 ล้านดอลลาร์สหรัฐ

4. การแสวงหาประโยชน์จากช่องโหว่ซอฟต์แวร์ (Software Vulnerability Exploitation)

ช่องโหว่ซอฟต์แวร์ในบริบทของ Industrial IoT หมายถึง ข้อบกพร่องในโค้ดหรือการออกแบบของซอฟต์แวร์ที่ใช้ในระบบควบคุมอุตสาหกรรม เซ็นเซอร์ อุปกรณ์ตรวจวัด หรือองค์ประกอบอื่น ๆ ในระบบ Industrial IoT ซึ่งผู้ไม่ประสงค์ดีสามารถใช้ประโยชน์เพื่อเข้าถึงระบบโดยไม่ได้รับอนุญาต การหาประโยชน์จากช่องโหว่นี้เกิดขึ้นเมื่อผู้โจมตีสามารถระบุช่องโหว่และใช้วิธีการเฉพาะหลบหลีกกลไกความปลอดภัยของระบบ โดยกระบวนการโจมตีมักเริ่มต้นด้วยการค้นหาช่องโหว่ผ่านการสแกนเครือข่ายหรือการวิเคราะห์ซอฟต์แวร์ย้อนกลับ จากนั้นจึงพัฒนาและใช้เครื่องมือเฉพาะเพื่อหาประโยชน์จากช่องโหว่ที่พบ ประเภทของช่องโหว่ซอฟต์แวร์ที่พบบ่อยใน Industrial IoT มีดังนี้

- **ช่องโหว่การบริหารจัดการรหัสผ่าน** อุปกรณ์ Industrial IoT จำนวนมากใช้รหัสผ่านเริ่มต้นที่ตั้งโดยผู้ผลิต ซึ่งมักไม่ได้รับการเปลี่ยนแปลง หรือการตั้งค่าการยืนยันตัวตนที่ไม่ปลอดภัย
- **ช่องโหว่ Buffer Overflow** เกิดขึ้นเมื่อโปรแกรมพยายามเก็บข้อมูลมากเกินไปในพื้นที่หน่วยความจำชั่วคราว ทำให้ผู้โจมตีสามารถแทรกและดำเนินการโค้ดที่เป็นอันตรายได้
- **ช่องโหว่ในโปรโตคอลการสื่อสาร** โปรโตคอลอุตสาหกรรมดั้งเดิมหลายตัว เช่น Modbus, DNP3 หรือ Profinet มักไม่มีการเข้ารหัสหรือการตรวจสอบตัวตนที่แข็งแกร่ง
- **ช่องโหว่การอัปเดต** ซอฟต์แวร์และเฟิร์มแวร์ที่ล้าสมัยในอุปกรณ์ Industrial IoT ทำให้ระบบมีความเสี่ยงต่อช่องโหว่ที่ได้รับการแก้ไขแล้วในเวอร์ชันใหม่กว่า
- **ข้อผิดพลาดในตรรกะความปลอดภัย** เมื่อการออกแบบเชิงตรรกะของซอฟต์แวร์มีข้อบกพร่อง ทำให้ผู้โจมตีสามารถข้ามขั้นตอนสำคัญหรือแก้ไขลำดับการดำเนินการได้

การแสวงหาประโยชน์จากช่องโหว่ซอฟต์แวร์มีผลกระทบอย่างมากทั้งในด้านความปลอดภัยและประสิทธิภาพการดำเนินงาน เนื่องจากสามารถทำให้ข้อมูลสำคัญขององค์กรถูกขโมย หรือระบบการผลิตหยุดชะงักได้ ส่งผลให้เกิดความเสียหายทั้งในด้านการเงินและชื่อเสียงขององค์กร อีกทั้งยังทำให้เกิดการสูญเสียความเชื่อมั่นจากลูกค้าและคู่ค้า ซึ่งอาจมีผลต่อความสามารถในการแข่งขันในตลาดโลก การถูกโจมตีช่องโหว่ซอฟต์แวร์ในระบบอัตโนมัติหรือเครื่องจักรที่ใช้ในกระบวนการผลิตจะทำให้ประสิทธิภาพการผลิตลดลงและมีความเสี่ยงในการเกิดอันตรายกับพนักงาน นอกจากนี้ องค์กรยังต้องเผชิญกับค่าใช้จ่ายเพิ่มเติมในการฟื้นฟูระบบและดำเนินการแก้ไขปัญหาทางด้านความปลอดภัย ซึ่งอาจส่งผลต่อการเติบโตและการขยายตัวของธุรกิจในระยะยาว ตัวอย่างการโจมตีแบบการแสวงหาประโยชน์จากช่องโหว่ซอฟต์แวร์ที่เกิดขึ้นจริงในระบบ Industrial IoT ภาคการผลิต เช่น

- การโจมตีช่องโหว่ในเฟิร์มแวร์ของ PLCs ที่ใช้ควบคุมสายการผลิตอัตโนมัติของบริษัทผลิตชิ้นส่วนยานยนต์ในสหรัฐอเมริกา ในปี 2560 ด้วยการใช้ประโยชน์จากช่องโหว่การตรวจสอบสิทธิ์ในอุปกรณ์ PLCs ที่เชื่อมต่อกับเครือข่าย ด้วยการทำให้สามารถอัปโหลดโค้ดที่ได้รับการแก้ไขโดยไม่ต้องผ่านการยืนยันตัวตน จนพารามิเตอร์การผลิตถูกเปลี่ยนแปลงแบบแนบเนียน ส่งผลให้ชิ้นส่วนที่ผลิตมีคุณภาพต่ำกว่ามาตรฐาน แต่ไม่มีเครื่องหมายบ่งชี้ถึงความผิดปกติ ต้องเรียกคืนผลิตภัณฑ์กว่า 500,000 ชิ้น คิดเป็นมูลค่าความเสียหายประมาณ 25 ล้านดอลลาร์สหรัฐ
- ผู้โจมตีใช้ช่องโหว่ในการอัปเดตเฟิร์มแวร์ของระบบจัดการแบตเตอรี่ (Battery Management System) โรงงานผลิตแบตเตอรี่ในเกาหลีใต้ ในปี 2565 ซึ่งไม่มีการตรวจสอบลายเซ็นดิจิทัลอย่างเหมาะสม และทำ

การแก้ไขระบบควบคุมการชาร์จ ทำให้เกิดการชาร์จเกินในแบตเตอรี่บางส่วน จนเกิดเหตุไฟไหม้เล็กน้อยในโรงงาน สายการผลิตต้องหยุดชะงักเป็นเวลา 3 วัน เกิดความเสียหายทางการเงินประมาณ 15 ล้านดอลลาร์สหรัฐ

- ผู้โจมตีใช้ช่องโหว่ในระบบจัดเก็บข้อมูลเพื่อเข้าถึงและปรับเปลี่ยนไฟล์แบบ CAD สำหรับการผลิตชิ้นส่วน โรงงานผลิตเครื่องใช้ไฟฟ้าในญี่ปุ่น ในปี 2566 ทำให้แบบ CAD สำหรับส่วนประกอบสำคัญของเครื่องใช้ไฟฟ้าถูกเปลี่ยนแปลง ส่งผลให้ผลิตภัณฑ์เกิดความเสียหายเมื่อใช้งานไประยะหนึ่ง ต้องเรียกคืนสินค้ากว่า 200,000 ชิ้น มูลค่าความเสียหายรวมประมาณ 70 ล้านดอลลาร์สหรัฐ

5. การโจมตีผ่านห่วงโซ่อุปทาน (Supply Chain Attacks)

การโจมตีผ่านห่วงโซ่อุปทานถือเป็นรูปแบบการคุกคามที่ละเอียดอ่อนเป็นพิเศษสำหรับระบบ Industrial IoT โดยแทนที่จะโจมตีระบบเป้าหมายโดยตรง แต่กลับโจมตีไปที่ช่องโหว่ในกระบวนการจัดหา พัฒนา หรือจัดส่งผลิตภัณฑ์และบริการที่ใช้ในระบบ Industrial IoT ด้วยการแทรกแซงผู้ให้บริการหรือผู้จัดจำหน่ายที่องค์กรเป้าหมายไว้วางใจ การโจมตีนี้มีความซับซ้อนและอันตรายเป็นพิเศษในบริบทของ Industrial IoT เนื่องจากระบบ Industrial IoT มักประกอบด้วยอุปกรณ์ ซอฟต์แวร์ และบริการจากผู้ผลิตหลากหลายราย รูปแบบของ Supply Chain Attacks ใน Industrial IoT มีดังนี้

- **การดัดแปลงซอฟต์แวร์ (Software Tampering)** ผู้โจมตีแทรกโค้ดที่เป็นอันตรายเข้าไปในซอฟต์แวร์หรือเฟิร์มแวร์ที่ใช้ในระบบ Industrial IoT ก่อนที่จะถูกส่งถึงผู้ใช้ปลายทาง โดยอาจแทรกแซงระหว่างกระบวนการพัฒนา การสร้าง หรือการจัดจำหน่าย ตัวอย่างเช่น การดัดแปลงการอัปเดตเฟิร์มแวร์ของเซ็นเซอร์อุตสาหกรรม หรือการแทรกแบ็คดอร์ในซอฟต์แวร์ SCADA
- **การปลอมแปลงฮาร์ดแวร์ (Hardware Counterfeiting)** ผู้โจมตีทำการแทรกซึมอุปกรณ์ปลอมหรือที่ถูกดัดแปลงเข้าสู่ห่วงโซ่อุปทาน โดยอาจมีการติดตั้งชิปสอดแนมหรืออุปกรณ์ที่ถูกดัดแปลงให้มีช่องโหว่ที่สามารถใช้ประโยชน์ได้ในภายหลัง เช่น PLCs ปลอมที่มีการฝังมัลแวร์หรือแบ็คดอร์ไว้ล่วงหน้า
- **การโจมตีผ่านบุคคลที่สาม (Third-party Compromise)** ผู้โจมตีเจาะระบบของบริษัทที่เป็นผู้ให้บริการหรือผู้จัดหาให้กับองค์กรเป้าหมาย เพื่อใช้เป็นช่องทางในการเข้าถึงระบบ Industrial IoT ขององค์กรนั้น เช่น การเจาะระบบของผู้ให้บริการบำรุงรักษาระยะไกล (Remote Maintenance Provider) เพื่อใช้สิทธิ์ในการโจมตีระบบการผลิต
- **การสวมรอยเป็นผู้จัดจำหน่ายที่ถูกต้อง (Vendor Spoofing)** ผู้โจมตีปลอมตัวเป็นผู้จัดจำหน่ายหรือผู้ให้บริการที่ไว้วางใจได้ เพื่อหลอกให้องค์กรเป้าหมายติดตั้งอุปกรณ์หรือซอฟต์แวร์ที่มีมัลแวร์ เช่น การส่งอีเมลหลอกลวงเกี่ยวกับการอัปเดตความปลอดภัยสำคัญสำหรับระบบควบคุมอุตสาหกรรม

การโจมตีผ่านห่วงโซ่อุปทานส่งผลกระทบต่อภาคอุตสาหกรรมการผลิตในหลายด้าน โดยเฉพาะในด้านความปลอดภัยและความต่อเนื่องในการดำเนินงาน เนื่องจากการโจมตีในขั้นตอนใดขั้นตอนหนึ่งของห่วงโซ่อุปทานสามารถแพร่กระจายไปยังส่วนอื่น ๆ ของระบบผลิตภัณฑ์และบริการได้ง่าย ทำให้เกิดความเสียหายจากข้อมูลที่ถูกขโมยหรือถูกทำลาย การหยุดชะงักของกระบวนการผลิตที่เกิดจากการโจมตีสามารถทำให้การผลิตล่าช้า หรือไม่สามารถดำเนินการได้ตามปกติ ส่งผลต่อการส่งมอบสินค้าตามกำหนดเวลา และอาจทำให้บริษัทสูญเสียลูกค้าหรือความเชื่อมั่น

จากผู้ร่วมธุรกิจ นอกจากนี้ ยังทำให้เกิดค่าใช้จ่ายเพิ่มเติมในการฟื้นฟูระบบและตรวจสอบความปลอดภัยที่เพิ่มขึ้น รวมถึงการต้องปรับปรุงกระบวนการและมาตรการป้องกันใหม่เพื่อป้องกันการโจมตีในอนาคต ซึ่งทั้งหมดนี้สามารถส่งผลกระทบต่อภาพรวมของธุรกิจในระยะยาว ทั้งในแง่ของการเงินและชื่อเสียง กรณีศึกษาที่เกิดขึ้นจริงในภาคการผลิต มีดังนี้

- ผู้โจมตีทำการดัดแปลงซอฟต์แวร์อัปเดตสำหรับ PLCs ยี่ห้อ WAGO ซึ่งใช้ในสายการผลิตอัตโนมัติในโรงงานผลิตชิ้นส่วนยานยนต์ในยุโรป ในปี 2560 เมื่อวิศวกรโรงงานดาวน์โหลดการอัปเดตจากเว็บไซต์ที่ดูเหมือนเป็นทางการ ระบบควบคุมถูกดัดแปลงทำให้สายการผลิตทำงานผิดพลาด ส่งผลให้ชิ้นส่วนที่ผลิตมีขนาดคลาดเคลื่อนเล็กน้อย แต่เพียงพอที่จะทำให้เกิดปัญหาในการประกอบขั้นสุดท้าย ความเสียหายรวมกว่า 3 ล้านยูโร
- ผู้โจมตีสามารถเข้าถึงระบบที่ใช้ในการพัฒนาเฟิร์มแวร์อุปกรณ์ Industrial IoT บริษัทผลิตเซ็นเซอร์อุตสาหกรรมในไต้หวัน ในปี 2563 ทำให้เฟิร์มแวร์ของเซ็นเซอร์ที่ใช้ในอุตสาหกรรมการผลิตอิเล็กทรอนิกส์ถูกแทรกแซงด้วยโค้ดอันตราย ส่งผลให้เซ็นเซอร์ส่งข้อมูลที่ไม่ถูกต้องเกี่ยวกับอุณหภูมิและความชื้นในสภาพแวดล้อมการผลิต ทำให้เกิดความเสียหายต่อกระบวนการผลิตที่ต้องควบคุมสภาพแวดล้อมอย่างเข้มงวด
- ผู้โจมตีทำการเจาะระบบของผู้ให้บริการบำรุงรักษาระบบ Industrial IoT ในสหรัฐอเมริกาเมื่อปี 2564 โดยผู้โจมตีใช้ช่องทางการเข้าถึงระยะไกลของบริษัทนี้เพื่อเข้าสู่ระบบ Industrial IoT ของโรงงานผลิตอาหารหลายแห่ง ทำให้สามารถปรับเปลี่ยนพารามิเตอร์ในกระบวนการแปรรูปอาหาร ส่งผลให้ผลิตภัณฑ์บางส่วนมีการปนเปื้อนแบคทีเรีย ทำให้ต้องเรียกคืนสินค้าและสูญเสียรายได้กว่า 15 ล้านดอลลาร์สหรัฐ

จะเห็นได้ว่า ทุกวินาทีที่อุปกรณ์และระบบ Industrial IoT ทำงาน องค์กรกำลังเผชิญกับความเสี่ยงจากมัลแวร์ แรนซัมแวร์ และการโจมตีอื่น ๆ ที่ซับซ้อนขึ้นเรื่อย ๆ หากมาตรการด้านความปลอดภัยไม่มีประสิทธิภาพเพียงพอ องค์กรอาจไม่เพียงจะสูญเสียข้อมูลสำคัญเท่านั้น แต่ยังส่งผลกระทบต่อรายได้ ความเชื่อมั่นของลูกค้า และชัพพลายเชนอย่างมหาศาล ดังนั้น ภัยคุกคามทางไซเบอร์จึงไม่ใช่เพียงความเสี่ยงธรรมดา แต่คือวิกฤตที่องค์กรในอุตสาหกรรมการผลิตต้องเผชิญหน้าและหาแนวทางป้องกันอย่างเร่งด่วน หากองค์กรไม่เตรียมพร้อมรับมือกับภัยไซเบอร์ที่คืบคลานเข้ามา อนาคตของการผลิตอัจฉริยะอาจไม่ใช่ความก้าวหน้าขององค์กร แต่เป็นจุดเปราะบางที่นำไปสู่ความเสียหายครั้งใหญ่แทน

แนวคิดสำคัญในการป้องกันภัยคุกคาม Industrial IoT

ในยุคที่ Industrial IoT (Industrial IoT) กลายเป็นหัวใจสำคัญของภาคการผลิต ความก้าวหน้าทางเทคโนโลยีได้นำมาซึ่งความเชื่อมโยงอัจฉริยะระหว่างเครื่องจักร อุปกรณ์ และระบบวิเคราะห์ข้อมูล ซึ่งช่วยเพิ่มประสิทธิภาพการทำงาน ลดต้นทุน และเร่งกระบวนการตัดสินใจ อย่างไรก็ตาม การพึ่งพาการเชื่อมต่อเครือข่ายและอุปกรณ์ที่หลากหลายทำให้ Industrial IoT กลายเป็นเป้าหมายหลักของภัยคุกคามทางไซเบอร์ แนวทางการป้องกันภัยคุกคาม Industrial IoT จึงเป็นสิ่งจำเป็นที่องค์กรต้องให้ความสำคัญ ตั้งแต่ขั้นตอนการออกแบบ ไปจนถึงการบริหารจัดการและดูแลความปลอดภัยในระยะยาว เพื่อให้มั่นใจว่าระบบสามารถรับมือกับความเสี่ยงได้อย่างมีประสิทธิภาพ โดยแนวคิดที่สำคัญในการรักษาความปลอดภัยของระบบ Industrial IoT ประกอบด้วย

1. การออกแบบความปลอดภัยของ Industrial IoT ตั้งแต่ต้น (Security by Design)

Security by Design เป็นแนวคิดที่ให้ความสำคัญกับการผนวกความปลอดภัยเข้าเป็นส่วนหนึ่งของระบบ Industrial IoT ตั้งแต่ขั้นตอนการออกแบบ ไม่ใช่เพิ่มเติมภายหลัง โดยตั้งอยู่บนหลักการว่าการป้องกันปัญหาตั้งแต่ต้นมีประสิทธิภาพและคุ้มค่ามากกว่าการแก้ไขในภายหลัง เพราะการแก้ไขปัญหาความปลอดภัยในภายหลังมักมีค่าใช้จ่ายสูงกว่าการป้องกันตั้งแต่ต้น โดยเฉพาะในโลกของ Industrial IoT ที่อุปกรณ์อาจถูกใช้งานยาวนานหลายปีโดยไม่มีการอัปเดต ความปลอดภัยตั้งแต่ต้นจึงมีความสำคัญมากเป็นพิเศษ

ในทางปฏิบัติ Security by Design เป็นการเลือกใช้อุปกรณ์ที่ได้มาตรฐานความปลอดภัยตั้งแต่แรก การเข้ารหัสข้อมูลระหว่างอุปกรณ์ (End-to-End Encryption) ในทุกขั้นตอนการสื่อสาร การตรวจสอบรหัสซอฟต์แวร์เพื่อหาช่องโหว่ การตรวจสอบความถูกต้องของซอฟต์แวร์ทุกส่วนก่อนที่จะทำงาน ตลอดจนการตรวจสอบซัพพลายเชน เพื่อให้ได้ระบบที่มีความทนทานต่อภัยคุกคามมากขึ้น ลดความเสี่ยงของการละเมิดความปลอดภัย และมีต้นทุนโดยรวมที่ต่ำกว่าในระยะยาว

2. การป้องกันภัยคุกคามจากเครือข่าย (Network Security)

Network Security ในบริบทของ Industrial IoT เน้นการปกป้องการสื่อสารและข้อมูลที่ส่งผ่านเครือข่ายระหว่างอุปกรณ์ Industrial IoT ระบบควบคุม และระบบบริหารจัดการข้อมูล แนวคิดนี้ครอบคลุมทั้งการป้องกัน การตรวจจับ และการตอบสนองต่อภัยคุกคามที่อาจเกิดขึ้นในเครือข่าย มาตรการหลักของ Network Security ประกอบด้วยการแบ่งแยกเครือข่ายออกเป็นโซน (Network Segmentation) โดยแยกระบบ OT (Operational Technology) ออกจากระบบ IT (Information Technology) การใช้ไฟร์วอลล์อุตสาหกรรม (Industrial Firewall) ที่เข้าใจโปรโตคอลเฉพาะทางอุตสาหกรรม และการติดตั้งระบบตรวจจับและป้องกันการบุกรุก (IDS/IPS) ที่ทำงานแบบเรียลไทม์

ในระบบ Industrial IoT ที่ซับซ้อน การมองเห็นเครือข่าย (Network Visibility) เป็นสิ่งสำคัญ องค์กรต้องสามารถตรวจสอบและเข้าใจการไหลของข้อมูลทั้งหมดในเครือข่าย Industrial IoT เพื่อสามารถตรวจจับพฤติกรรมที่ผิดปกติได้อย่างรวดเร็ว ทั้งนี้ การเข้ารหัสข้อมูลระหว่างการส่งผ่านและการใช้ VPN สำหรับการเข้าถึงระยะไกลยังเป็นองค์ประกอบสำคัญของ Network Security ในยุค Industrial IoT

3. การบริหารจัดการอุปกรณ์ Industrial IoT อย่างมีประสิทธิภาพ (Device Management)

Device Management คือการบริหารจัดการวงจรชีวิตทั้งหมดของอุปกรณ์ Industrial IoT ตั้งแต่การนำเข้าสู่ระบบไปจนถึงการปลดระวาง แนวคิดนี้มุ่งเน้นที่การบำรุงรักษา อัปเดต และควบคุมการเข้าถึงอุปกรณ์ให้มีความปลอดภัยและทำงานได้อย่างมีประสิทธิภาพตลอดการใช้งาน องค์ประกอบสำคัญของ Device Management ได้แก่ การอัปเดตเฟิร์มแวร์และแพตช์ความปลอดภัยอย่างสม่ำเสมอและมีการตรวจสอบความถูกต้อง การใช้แนวคิด Zero Trust ที่ทุกการเข้าถึงระบบต้องผ่านการยืนยันตัวตน ตรวจสอบสิทธิ์ และมีการติดตามพฤติกรรมตลอดเวลา เพื่อป้องกันภัยคุกคามที่อาจแฝงตัวอยู่ในระบบ (Never Trust, Always Verify)

นอกจากนี้ Device Management ยังรวมถึงการทำ Asset Inventory คือการจัดทำบัญชีและติดตามอุปกรณ์ Industrial IoT ทั้งหมดในองค์กร การจัดการการตั้งค่าที่ปลอดภัย (Secure Configuration Management)

และการตรวจสอบสถานะความปลอดภัยของอุปกรณ์อย่างต่อเนื่อง ระบบ Device Management ที่ดีจะช่วยให้องค์กรสามารถตอบสนองต่อภัยคุกคามได้อย่างรวดเร็ว เช่น การแยกอุปกรณ์ที่น่าสงสัยออกจากเครือข่าย หรือการแก้ไขช่องโหว่บนอุปกรณ์จำนวนมากพร้อมกัน

ทั้งสามแนวคิดนี้ไม่ได้ทำงานแยกกัน แต่เสริมซึ่งกันและกันเพื่อสร้างระบบรักษาความปลอดภัย Industrial IoT ที่ครบวงจร Security by Design สร้างพื้นฐานความปลอดภัยตั้งแต่เริ่มต้น Network Security ปกป้องการสื่อสารระหว่างองค์ประกอบต่าง ๆ ในระบบ และ Device Management ดูแลรักษาความปลอดภัยตลอดอายุการใช้งานของอุปกรณ์ ในการนำไปใช้งานจริง องค์กรควรพัฒนากลยุทธ์ที่ผสมผสานทั้งสามแนวคิดนี้เข้าด้วยกัน โดยเริ่มต้นจากการออกแบบระบบที่ปลอดภัย (Security by Design) สร้างเครือข่ายที่มีการป้องกันแข็งแกร่ง (Network Security) และมีกระบวนการบริหารจัดการอุปกรณ์ที่มีประสิทธิภาพ (Device Management) เพื่อรับมือกับภัยคุกคามที่มีความซับซ้อนเพิ่มขึ้นเรื่อย ๆ ในยุคของ Industry 4.0

แนวทางการป้องกันภัยคุกคาม Industrial IoT

เทคโนโลยีและภัยคุกคามยังคงพัฒนาไปอย่างต่อเนื่อง การรักษาความปลอดภัย Industrial IoT จึงไม่ใช่เป้าหมายที่มีจุดสิ้นสุด แต่เป็นกระบวนการต่อเนื่องที่ต้องได้รับการปรับปรุงและปรับตัวอยู่เสมอ องค์กรที่วางแผนและดำเนินมาตรการรักษาความปลอดภัย Industrial IoT อย่างรอบคอบและเป็นระบบ จะสามารถปกป้องธุรกิจของตนได้อย่างมีประสิทธิภาพ พร้อมทั้งใช้ประโยชน์จากโอกาสที่เทคโนโลยีนี้มอบให้ โดยไม่ต้องเผชิญกับความเสี่ยงหรือผลกระทบร้ายแรงจากภัยคุกคามทางไซเบอร์

การป้องกันภัยคุกคาม Industrial IoT ในภาคการผลิตถือเป็นความท้าทายที่ซับซ้อนและต้องการแนวทางแบบองค์รวมที่รวมเทคโนโลยี กระบวนการ และบุคลากรเข้าด้วยกัน ดังนั้น จึงไม่มีวิธีการแก้ปัญหาเพียงวิธีเดียวที่สามารถรับประกันความปลอดภัยได้อย่างสมบูรณ์ แต่การนำแนวทางหลายชั้นที่ประกอบด้วยการรักษาความปลอดภัยทางกายภาพ การรักษาความปลอดภัยเครือข่าย การจัดการอุปกรณ์ การเฝ้าระวัง และการฝึกอบรมพนักงานมาใช้สามารถช่วยลดความเสี่ยงได้อย่างมีประสิทธิภาพ โดยแนวทางหลักที่องค์กรควรใช้ในการป้องกันภัยคุกคาม Industrial IoT ประกอบด้วย

1. ความเข้าใจภูมิทัศน์ภัยคุกคาม Industrial IoT ในภาคการผลิต

ก่อนกำหนดแนวทางการป้องกัน องค์กรจำเป็นต้องเข้าใจภัยคุกคามสำหรับระบบ Industrial IoT ในภาคการผลิต ซึ่งมีลักษณะพิเศษเนื่องจากสภาพแวดล้อมการผลิตมักประกอบด้วยเทคโนโลยีปฏิบัติการ (OT) ที่มีอายุการใช้งานยาวนาน ซึ่งไม่ได้ออกแบบมาโดยคำนึงถึงการเชื่อมต่อกับอินเทอร์เน็ตหรือความปลอดภัยทางไซเบอร์เป็นหลัก โดยต้องทำความเข้าใจภัยคุกคามหลักที่องค์กรภาคการผลิตต้องเผชิญ รวมถึงการโจมตีในรูปแบบต่าง ๆ ที่ล้วนแต่สามารถสร้างความเสียหายในระยะยาว

2. การสร้างกรอบการรักษาความปลอดภัยแบบหลายชั้น

การป้องกันภัยคุกคาม Industrial IoT ที่มีประสิทธิภาพจำเป็นต้องใช้แนวทางแบบหลายชั้น (Defense-in-Depth) ที่ไม่พึ่งพามาตรการรักษาความปลอดภัยเพียงชั้นเดียว แนวทางนี้เริ่มต้นจากการกำหนดนโยบายและแนวทางปฏิบัติด้านความปลอดภัยที่ชัดเจน การประเมินความเสี่ยงอย่างครอบคลุม และการสร้างวัฒนธรรมความตระหนักด้านความปลอดภัยทั่วทั้งองค์กร

ชั้นแรกของการป้องกัน ได้แก่ การรักษาความปลอดภัยทางกายภาพ โรงงานผลิตต้องมีการควบคุมการเข้าถึงพื้นที่ที่มีอุปกรณ์ Industrial IoT สำคัญตั้งอยู่ และมีมาตรการป้องกันทางกายภาพสำหรับพอร์ตและอินเทอร์เฟซที่ใช้ในการตั้งค่าหรือควบคุมอุปกรณ์เหล่านี้ ชั้นที่ 2 คือการรักษาความปลอดภัยเครือข่าย ซึ่งรวมถึงการแบ่งแยกเครือข่าย (Network Segmentation) ที่แยกระบบ OT ออกจากระบบ IT และอินเทอร์เน็ต การใช้ไฟร์วอลล์อุตสาหกรรมที่เข้าใจโปรโตคอลเฉพาะทางในการผลิต และการเฝ้าระวังเครือข่ายแบบเรียลไทม์เพื่อตรวจจับกิจกรรมที่ผิดปกติ ชั้นที่ 3 เกี่ยวข้องกับการรักษาความปลอดภัยของอุปกรณ์และระบบ Industrial IoT เอง ได้แก่ การตรวจสอบและอัปเดตเฟิร์มแวร์อย่างสม่ำเสมอ การตั้งค่าความปลอดภัยที่เหมาะสม การเข้ารหัสข้อมูลที่สื่อสารระหว่างอุปกรณ์ และการใช้การยืนยันตัวตนแบบหลายปัจจัยสำหรับการเข้าถึงระบบควบคุม ชั้นสุดท้ายคือการรักษาความปลอดภัยของข้อมูล ซึ่งรวมถึงการจัดหมวดหมู่ข้อมูลตามความสำคัญและความอ่อนไหว การเข้ารหัสข้อมูลที่สำคัญ และการตรวจสอบการเข้าถึงและการเปลี่ยนแปลงข้อมูล

3. การบูรณาการความปลอดภัยตั้งแต่การออกแบบ

หลักการ Security by Design มีความสำคัญอย่างยิ่งในการป้องกันภัยคุกคาม Industrial IoT ในภาคการผลิต แทนที่จะเพิ่มมาตรการรักษาความปลอดภัยหลังจากที่ระบบถูกติดตั้งและใช้งานแล้ว องค์กรควรรวมการพิจารณาด้านความปลอดภัยเข้าไปในทุกขั้นตอนของการพัฒนาและการติดตั้งระบบ Industrial IoT นอกจากนี้ องค์กรควรพิจารณาใช้เทคโนโลยีที่ช่วยเสริมความปลอดภัยตั้งแต่ต้น เช่น ระบบการจัดการตัวตนและการเข้าถึง (Identity and Access Management) ที่ควบคุมว่าใครสามารถเข้าถึงอุปกรณ์และข้อมูล Industrial IoT ได้ การใช้ Public Key Infrastructure (PKI) เพื่อรับรองความถูกต้องของอุปกรณ์และการสื่อสาร และการใช้เทคโนโลยี Trusted Execution Environment ที่แยกการทำงานด้านความปลอดภัยออกจากระบบปฏิบัติการหลัก

4. การจัดการอุปกรณ์และการประเมินความเสี่ยงอย่างต่อเนื่อง

การจัดการอุปกรณ์ Industrial IoT อย่างมีประสิทธิภาพเป็นองค์ประกอบสำคัญของกลยุทธ์การรักษาความปลอดภัยในภาคการผลิต เริ่มต้นจากการสร้างและรักษาบัญชีทรัพย์สิน (Asset Inventory) ที่ครบถ้วนของทุกอุปกรณ์ที่เชื่อมต่อในสภาพแวดล้อมการผลิต รวมถึงข้อมูลเกี่ยวกับเฟิร์มแวร์ การตั้งค่า และช่องโหว่ที่ทราบ โดยองค์กรควรมีกระบวนการประเมินและจัดการช่องโหว่อย่างเป็นระบบ ด้วยการสแกนหาช่องโหว่ในระบบ Industrial IoT อย่างสม่ำเสมอ จัดลำดับความสำคัญของช่องโหว่ตามระดับความเสี่ยง และวางแผนการแก้ไขที่พิจารณาถึงผลกระทบต่อการผลิต โดยควรมีการปรับให้เหมาะกับสภาพแวดล้อมการผลิตที่มีความอ่อนไหวต่อการหยุดชะงัก ซึ่งอาจจำเป็นต้องมีการวางแผนการอัปเดตในช่วงการบำรุงรักษาตามกำหนดหรือในช่วงที่มีการผลิตน้อย นอกจากนี้ ควรมีการ

ดำเนินการประเมินความเสี่ยงเป็นประจำ เพื่อระบุภัยคุกคามใหม่ ๆ รวมถึงประเมินประสิทธิภาพของมาตรการรักษาความปลอดภัยที่มีอยู่ และปรับกลยุทธ์การป้องกันให้สอดคล้องกับภูมิทัศน์ภัยคุกคามที่เปลี่ยนแปลงไป

5. การเฝ้าระวังและการตอบสนองต่อเหตุการณ์

การเฝ้าระวังอย่างต่อเนื่องเป็นสิ่งสำคัญในการตรวจจับและตอบสนองต่อการโจมตีที่อาจเกิดขึ้นกับระบบ Industrial IoT ในภาคการผลิต องค์กรควรใช้ระบบตรวจจับการบุกรุก (Intrusion Detection Systems) ที่ออกแบบมาเฉพาะสำหรับสภาพแวดล้อมอุตสาหกรรม ซึ่งสามารถตรวจจับพฤติกรรมที่ผิดปกติในโปรโตคอลอุตสาหกรรมและการสื่อสารระหว่างอุปกรณ์ รวมถึงการรวบรวมและวิเคราะห์บันทึกเหตุการณ์ (Logs) จากอุปกรณ์และระบบ Industrial IoT ซึ่งเป็นองค์ประกอบสำคัญของการเฝ้าระวัง ข้อมูลเหล่านี้ควรถูกส่งไปยังระบบจัดการข้อมูลและเหตุการณ์ด้านความปลอดภัย (Security Information and Event Management) ที่สามารถรวบรวมและวิเคราะห์ข้อมูลจากหลายแหล่งเพื่อระบุรูปแบบที่น่าสงสัย

นอกจากการเฝ้าระวังแล้ว องค์กรยังต้องมีแผนการตอบสนองต่อเหตุการณ์ (Incident Response Plan) ที่ชัดเจนและได้รับการทดสอบสำหรับเหตุการณ์ด้านความปลอดภัย Industrial IoT โดยในแผนควรมีการกำหนดบทบาทและความรับผิดชอบ ขั้นตอนการสื่อสาร และกระบวนการตัดสินใจในระหว่างเกิดเหตุ รวมถึงแนวทางการแยกส่วนที่ได้รับผลกระทบออกจากส่วนอื่นของระบบการผลิตเพื่อจำกัดความเสียหาย

6. การสร้างความร่วมมือระหว่างทีม IT และ OT

หนึ่งในความท้าทายสำคัญในการรักษาความปลอดภัย Industrial IoT ในภาคการผลิตคือช่องว่างระหว่างทีมเทคโนโลยีสารสนเทศ (IT) และทีมเทคโนโลยีปฏิบัติการ (OT) ทั้งสองทีมมักมีวัฒนธรรม เป้าหมาย และมุมมองที่แตกต่างกัน โดยทีม IT ให้ความสำคัญกับความปลอดภัยและการปกป้องข้อมูล ในขณะที่ทีม OT มุ่งเน้นที่ความพร้อมใช้งานและประสิทธิภาพของระบบการผลิต การสร้างความร่วมมือที่แข็งแกร่งระหว่างทั้งสองทีมเป็นสิ่งสำคัญสำหรับกลยุทธ์การรักษาความปลอดภัย Industrial IoT ที่มีประสิทธิภาพ องค์กรควรส่งเสริมการสื่อสารและความเข้าใจร่วมกันระหว่างทีม เช่น การจัดประชุมร่วมเป็นประจำ การแลกเปลี่ยนความรู้และทักษะ และการพัฒนาภาษาและเป้าหมายร่วมกัน บางองค์กรอาจพิจารณาจัดตั้งทีมความปลอดภัยทางไซเบอร์อุตสาหกรรมที่มีผู้เชี่ยวชาญจากทั้งสองด้าน หรือสร้างบทบาทเชื่อมโยงที่ทำหน้าที่เป็นสะพานระหว่างทั้งสองโลก การบูรณาการนี้ไม่เพียงแต่ช่วยปรับปรุงความปลอดภัย แต่ยังช่วยให้มั่นใจว่ามาตรการรักษาความปลอดภัยจะไม่ส่งผลกระทบต่อประสิทธิภาพการผลิตหรือความพร้อมใช้งานของระบบ

7. การฝึกอบรมและการสร้างวัฒนธรรมความปลอดภัย

การรักษาความปลอดภัย Industrial IoT ไม่ใช่เพียงเรื่องของเทคโนโลยีและกระบวนการ แต่ยังเกี่ยวข้องกับพนักงาน พนักงานที่มีความตระหนักด้านความปลอดภัยและได้รับการฝึกอบรมอย่างเหมาะสมเป็นแนวป้องกันที่สำคัญเป็นอย่างมากต่อภัยคุกคามทางไซเบอร์ องค์กรควรจัดหลักสูตรฝึกอบรมด้านความปลอดภัยทางไซเบอร์ที่ปรับให้เหมาะกับบทบาทต่าง ๆ ในโรงงานผลิต ตั้งแต่ผู้ปฏิบัติงานในพื้นที่ไปจนถึงวิศวกรและผู้จัดการ ซึ่งการฝึกอบรมควรครอบคลุมหัวข้อที่เกี่ยวข้องกับภัยคุกคาม Industrial IoT โดยเฉพาะ เช่น วิธีการระบุอีเมลฟิชชิ่งที่มุ่งเป้าหมายไปที่

พนักงานด้านการผลิต ความสำคัญของการใช้รหัสผ่านที่แข็งแกร่งสำหรับอุปกรณ์ Industrial IoT และขั้นตอนการรายงานเหตุการณ์ด้านความปลอดภัยที่น่าสงสัย

นอกจากการฝึกอบรมอย่างเป็นทางการแล้ว องค์กรควรส่งเสริมวัฒนธรรมความตระหนักด้านความปลอดภัยผ่านการสื่อสารอย่างสม่ำเสมอ การประชุมเรื่องความปลอดภัย และการฝึกซ้อมรับมือกับเหตุการณ์ในแต่ละรูปแบบ การสร้างสภาพแวดล้อมที่พนักงานรู้สึกสบายใจในการรายงานปัญหาหรือข้อกังวลเกี่ยวกับความปลอดภัยโดยไม่ต้องกลัวการถูกลงโทษเป็นสิ่งสำคัญในการตรวจจับและจัดการกับภัยคุกคามในระยะเริ่มต้น

สำหรับ SMEs ซึ่งมีความท้าทายสำคัญคือ การใช้เทคโนโลยีให้เกิดประโยชน์สูงสุด โดยต้องรักษาความปลอดภัยทางไซเบอร์ให้รัดกุม ขณะเดียวกันก็มีข้อจำกัดด้านงบประมาณ ทรัพยากร และบุคลากรผู้เชี่ยวชาญ ทำให้หลายองค์กรลังเลที่จะลงทุนด้านความปลอดภัย เพราะมองว่าเป็นภาระที่เกินความจำเป็น อย่างไรก็ตาม การละเลยความปลอดภัยอาจทำให้ธุรกิจต้องเผชิญกับความเสียหายที่สูงกว่าต้นทุนการป้องกันหลายเท่า ดังนั้น SMEs จึงต้องหาวิธีสร้างเหมาะสมระหว่างการนำ Industrial IoT มาใช้กับการป้องกันความเสี่ยง เพื่อให้ธุรกิจสามารถเติบโตได้อย่างมั่นคงและปลอดภัย ซึ่งแนวทางการป้องกันภัยคุกคาม Industrial IoT ที่เหมาะสมสำหรับ SMEs จะมีความแตกต่างจากองค์กรขนาดใหญ่ โดย SMEs ควรมีการดำเนินการดังนี้

1. การประเมินความเสี่ยงและจัดลำดับความสำคัญ

จุดเริ่มต้นที่สำคัญสำหรับ SMEs คือการทำความเข้าใจสถานะปัจจุบันและความเสี่ยงเฉพาะของระบบ Industrial IoT ในองค์กร ด้วยทรัพยากรที่จำกัด SMEs จำเป็นต้องจัดลำดับความสำคัญของการลงทุนด้านความปลอดภัยให้ตรงกับความเสี่ยงที่มีนัยสำคัญที่สุด กระบวนการประเมินควรเริ่มต้นด้วยการสำรวจและจัดทำบัญชีทรัพย์สินด้านเทคโนโลยีให้ครบถ้วน ทั้งอุปกรณ์ Industrial IoT เครื่องมือควบคุมอุตสาหกรรม และระบบที่เชื่อมต่อกับเครือข่าย ขั้นตอนต่อมาคือการระบุและประเมินมูลค่าของข้อมูลและกระบวนการสำคัญในการผลิต โดยการตั้งคำถามว่า "อะไรคือสิ่งที่สำคัญที่สุดต่อการดำเนินธุรกิจ?" และ "อะไรคือผลกระทบหากระบบหรือข้อมูลเหล่านี้ถูกละเมิด?" คำตอบจะช่วยให้สามารถจัดลำดับความสำคัญของทรัพยากรที่ต้องได้รับการปกป้องมากที่สุด การลงทุนในการประเมินความเสี่ยงที่ครอบคลุมในขั้นตอนแรกจะช่วยกำหนดทิศทางการลงทุนด้านความปลอดภัยที่มีประสิทธิภาพในระยะยาว

2. การสร้างความปลอดภัยพื้นฐาน

แม้ว่า SMEs อาจไม่สามารถลงทุนในเทคโนโลยีรักษาความปลอดภัยที่ซับซ้อนและราคาแพงได้ แต่สามารถสร้างรากฐานความปลอดภัยที่แข็งแกร่งได้ด้วยมาตรการพื้นฐานที่มีประสิทธิภาพและคุ้มค่า มาตรการเหล่านี้รวมถึงการเปลี่ยนรหัสผ่านเริ่มต้น (Default Password) ของอุปกรณ์ Industrial IoT ทั้งหมด การใช้นโยบายรหัสผ่านที่เข้มงวด และการบังคับใช้การยืนยันตัวตนแบบหลายปัจจัย (Multi-factor Authentication) สำหรับการเข้าถึงระบบที่สำคัญ รวมถึงการอัปเดตซอฟต์แวร์และเฟิร์มแวร์เป็นประจำ ซึ่ง SMEs ควรสร้างกระบวนการที่เป็นระบบในการติดตามการอัปเดตความปลอดภัยจากผู้ผลิตและดำเนินการติดตั้งในเวลาที่เหมาะสม นอกจากนี้ การสำรองข้อมูลอย่างสม่ำเสมอและการทดสอบการกู้คืนเป็นอีกหนึ่งสิ่งจำเป็นโดยเฉพาะสำหรับ SMEs ที่อาจไม่มีทรัพยากรเพียงพอในการ

ฟื้นตัวจากการโจมตีที่ร้ายแรง โดยควรใช้กฎ 3-2-1 สำหรับการสำรองข้อมูล (เก็บสำเนา 3 ชุด บน 2 ประเภทสื่อที่แตกต่างกัน โดยมีอย่างน้อย 1 ชุดเก็บไว้นอกสถานที่หรือบนคลาวด์ที่ปลอดภัย) ซึ่งจะช่วยเพิ่มความปลอดภัยและลดความเสี่ยงจากการสูญหายของข้อมูลจากการโจมตีทางไซเบอร์

3. การแบ่งแยกเครือข่ายอย่างเหมาะสม

การแบ่งแยกเครือข่าย (Network Segmentation) เป็นกลยุทธ์ที่มีประสิทธิภาพในการจำกัดการแพร่กระจายของการโจมตีในระบบ Industrial IoT โดยไม่จำเป็นต้องใช้อุปกรณ์เครือข่ายราคาแพง แม้แต่ SMEs ที่มีงบประมาณจำกัดก็สามารถนำแนวคิดนี้มาปรับใช้ได้ โดยเริ่มต้นด้วยการแบ่งแยกระบบเทคโนโลยีปฏิบัติการ (OT) ออกจากระบบเทคโนโลยีสารสนเทศ (IT) ปกติ โดยใช้ไฟร์วอลล์พื้นฐานหรือ Virtual LAN (VLAN) ที่มีการกำหนดค่าอย่างเหมาะสม นอกจากนี้ ควรพิจารณาการสร้างเครือข่ายแยกสำหรับอุปกรณ์ที่มีความสำคัญแตกต่างกัน เช่น แยกระบบ ICS ออกจากเครือข่ายสำนักงาน หรือแยกอุปกรณ์ IoT ออกจากเครือข่ายหลัก เพื่อลดโอกาสที่มัลแวร์หรือผู้โจมตีจะสามารถเข้าถึงระบบที่สำคัญได้ง่าย นอกจากนี้ยังช่วยควบคุมและตรวจสอบการรับส่งข้อมูล ทำให้สามารถตรวจจับและตอบสนองต่อภัยคุกคามได้อย่างมีประสิทธิภาพมากขึ้น

4. การใช้บริการคลาวด์และโซลูชันความปลอดภัย

SMEs สามารถใช้ประโยชน์จากบริการคลาวด์และโซลูชันความปลอดภัย (Security-as-a-Service) เพื่อเข้าถึงความสามารถด้านความปลอดภัยระดับองค์กรโดยไม่ต้องลงทุนในโครงสร้างพื้นฐานที่มีราคาแพง โซลูชันเหล่านี้มักมีรูปแบบการชำระเงินตามการใช้งาน (Pay-as-you-go) ซึ่งเหมาะกับงบประมาณของ SMEs บริการคลาวด์สำหรับการจัดการข้อมูล Industrial IoT มักมาพร้อมกับคุณสมบัติด้านความปลอดภัยในตัว เช่น การเข้ารหัสข้อมูล การตรวจสอบตัวตน และการตรวจจับความผิดปกติ โดยควรเลือกผู้ให้บริการที่มีประวัติด้านความปลอดภัยที่ดีและมีคุณสมบัติด้านความเป็นส่วนตัวและการปฏิบัติตามข้อกำหนดที่เกี่ยวข้องกับอุตสาหกรรม นอกจากนี้ ยังมีผู้ให้บริการด้านความปลอดภัยที่มุ่งเน้น SMEs โดยเฉพาะ ซึ่งให้บริการเช่น การเฝ้าระวังเครือข่ายตลอด 24 ชั่วโมง การตรวจจับภัยคุกคาม และการจัดการช่องโหว่ การใช้บริการเหล่านี้ช่วยให้ SMEs สามารถเข้าถึงผู้เชี่ยวชาญด้านความปลอดภัยโดยไม่ต้องจ้างพนักงานเต็มเวลา ซึ่งอาจมีค่าใช้จ่ายสูงและหายาก

5. การร่วมมือกับพันธมิตรและการสร้างเครือข่าย

SMEs ไม่จำเป็นต้องเผชิญกับความท้าทายด้านความปลอดภัย Industrial IoT เพียงลำพัง การร่วมมือกับธุรกิจอื่นในอุตสาหกรรมเดียวกันหรือในพื้นที่เดียวกันสามารถเป็นกลยุทธ์ที่มีประสิทธิภาพในการเพิ่มความสามารถด้านความปลอดภัย การสร้างกลุ่มแลกเปลี่ยนเรียนรู้ (CoP) ระหว่างผู้ปฏิบัติงานด้านความปลอดภัยของ Industrial IoT ช่วยให้ SMEs สามารถแบ่งปันข้อมูลเกี่ยวกับภัยคุกคาม แนวทางปฏิบัติที่ดีที่สุด และบทเรียนที่ได้รับจากเหตุการณ์ด้านความปลอดภัย

6. การสร้างวัฒนธรรมความปลอดภัยและการฝึกอบรมพนักงาน

แม้ว่า SMEs อาจมีพนักงานจำนวนไม่มากนัก แต่ก็เป็นโอกาสในการสร้างวัฒนธรรมความปลอดภัยที่แข็งแกร่งทั่วทั้งองค์กร ความตระหนักด้านความปลอดภัยไม่ควรเป็นความรับผิดชอบของแผนก IT หรือผู้จัดการเพียงคนเดียว แต่ควรฝังอยู่ในวิธีการทำงานของทุกคนในองค์กร โดยควรจัดฝึกอบรมด้านความปลอดภัยทางไซเบอร์ให้กับพนักงานทุกคนที่มีส่วนเกี่ยวข้องกับระบบ Industrial IoT การฝึกอบรมควรเน้นความเสี่ยงเฉพาะในสภาพแวดล้อมการผลิต และวิธีปฏิบัติที่ดีในการลดความเสี่ยง เช่น การจัดการรหัสผ่าน การระมัดระวังการพยายามหลอกลวง และการรายงานกิจกรรมที่น่าสงสัย นอกจากนี้ ผู้นำขององค์กรควรแสดงให้เห็นถึงความมุ่งมั่นในการรักษาความปลอดภัย Industrial IoT โดยการจัดสรรทรัพยากรที่เหมาะสม การเข้าร่วมการฝึกอบรม และการรวมความปลอดภัยเข้าเป็นส่วนหนึ่งของการตัดสินใจทางธุรกิจ วัฒนธรรมที่ส่งเสริมการสื่อสารเปิดเกี่ยวกับปัญหาด้านความปลอดภัยโดยไม่มีการกล่าวโทษจะช่วยให้สามารถระบุและแก้ไขช่องโหว่ได้อย่างรวดเร็ว

7. การวางแผนตอบสนองต่อเหตุการณ์และความต่อเนื่องทางธุรกิจ

สำหรับ SMEs การโจมตีทางไซเบอร์ที่ประสบความสำเร็จอาจส่งผลกระทบอย่างร้ายแรงต่อความอยู่รอดของธุรกิจ ดังนั้นการมีแผนตอบสนองต่อเหตุการณ์ (Incident Response Plan) และแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan) ที่มีประสิทธิภาพจึงมีความสำคัญอย่างยิ่ง โดยแผนตอบสนองต่อเหตุการณ์ควรระบุขั้นตอนชัดเจนที่ต้องดำเนินการเมื่อเกิดการละเมิดความปลอดภัย รวมถึงผู้ที่ต้องติดต่อ วิธีการจำกัดความเสียหาย และวิธีกู้คืนการดำเนินงาน แผนตอบสนองต่อเหตุการณ์ไม่จำเป็นต้องซับซ้อน แต่ควรครอบคลุมและเข้าใจได้โดยทุกคนที่เกี่ยวข้อง ในขณะที่แผนความต่อเนื่องทางธุรกิจควรระบุวิธีการรักษาฟังก์ชันธุรกิจที่สำคัญในกรณีที่ระบบ Industrial IoT ไม่สามารถใช้งานได้เนื่องจากการโจมตีหรือความล้มเหลวอื่น ๆ สำหรับ SMEs ที่มีทรัพยากรจำกัดควรให้ความสำคัญกับการกู้คืนกระบวนการที่สำคัญที่สุดก่อน ซึ่งทั้งสองแผนควรได้รับการทดสอบเป็นระยะด้วยการฝึกซ้อมและการจำลองสถานการณ์อย่างง่าย เพื่อให้แน่ใจว่าทุกคนเข้าใจบทบาทของตนและแผนสามารถนำไปปฏิบัติได้จริง การทดสอบยังช่วยระบุช่องว่างหรือปัญหาในแผนที่ต้องได้รับการแก้ไข

8. การเลือกพันธมิตรทางเทคโนโลยีที่น่าเชื่อถือ

การเลือกซัพพลายเออร์และผู้ให้บริการ Industrial IoT อย่างรอบคอบเป็นองค์ประกอบสำคัญของกลยุทธ์ความปลอดภัยสำหรับ SMEs แทนที่จะเลือกโซลูชันที่มีราคาถูกที่สุด ควรพิจารณาผู้ให้บริการที่มีประวัติด้านความปลอดภัยที่ดีและมุ่งมั่นในการรักษาความปลอดภัยของผลิตภัณฑ์ตลอดวงจรชีวิต โดยก่อนทำสัญญาหรือซื้อผลิตภัณฑ์ควรตรวจสอบนโยบายการอัปเดตความปลอดภัยของผู้ให้บริการ ระยะเวลาที่จะสนับสนุนผลิตภัณฑ์ และวิธีการจัดการกับช่องโหว่ที่พบ ผู้ให้บริการที่ดีควรมีกระบวนการที่ชัดเจนในการแจ้งเตือนลูกค้าเกี่ยวกับปัญหาด้านความปลอดภัยและการออกแพตช์อย่างทันท่วงที นอกจากนี้ ควรพิจารณาประเด็นด้านความเป็นส่วนตัวและการเป็นเจ้าของข้อมูล โดยทำความเข้าใจว่าข้อมูลใดที่ผู้ให้บริการรวบรวม วิธีการใช้ข้อมูลนั้น และวิธีการปกป้องข้อมูล ความชัดเจนในข้อตกลงระดับการให้บริการ (SLAs) เกี่ยวกับความปลอดภัยและความเป็นส่วนตัวเป็นสิ่งสำคัญ โดยเฉพาะอย่างยิ่งสำหรับ SMEs ที่อาจไม่มีทีมกฎหมายขนาดใหญ่ในการตรวจสอบสัญญา

ในยุค Industry 4.0 เทคโนโลยี Industrial IoT ได้กลายเป็นเครื่องมือสำคัญในการยกระดับประสิทธิภาพการผลิต การบำรุงรักษาเชิงคาดการณ์ และการวิเคราะห์ข้อมูลเชิงลึก ถึงแม้การนำ Industrial IoT มาใช้จะช่วยให้ภาคการผลิตทำงานได้อย่างมีประสิทธิภาพมากขึ้น ช่วยลดต้นทุนในระยะยาว และตอบสนองต่อความต้องการของตลาดได้อย่างแม่นยำ แต่ก็มาพร้อมกับภัยคุกคามทางไซเบอร์ที่อาจสร้างความเสียหายอย่างใหญ่หลวง การโจมตีทางไซเบอร์ที่ประสบความสำเร็จไม่เพียงแค่ทำให้ข้อมูลรั่วไหล แต่ยังสามารถควบคุมเครื่องจักรและกระบวนการทางกายภาพ ส่งผลให้เกิดอันตรายต่อมนุษย์และสิ่งแวดล้อมได้ ดังนั้น การรักษาความปลอดภัยของ Industrial IoT จึงไม่ใช่เพียงเรื่องของเทคโนโลยี แต่เป็นเรื่องของการตัดสินใจทางธุรกิจที่ชาญฉลาด เพราะการรักษาความปลอดภัยทางไซเบอร์ไม่ได้เป็นแค่ทางเลือก แต่เป็นสิ่งที่ขาดไม่ได้สำหรับทุกองค์กรในยุคปัจจุบัน การเพิกเฉยต่อความปลอดภัยทางไซเบอร์อาจส่งผลให้เกิดวิกฤตการณ์ครั้งใหญ่กว่าที่เคยมีมาและกระทบต่อความอยู่รอดของธุรกิจ การเข้าใจความเสี่ยงและการลงทุนในความปลอดภัยอย่างเหมาะสมจะช่วยให้องค์กรสามารถใช้ประโยชน์จากนวัตกรรมอย่างเต็มที่ โดยยังคงรักษาความปลอดภัยของระบบ ข้อมูล พนักงาน และสิ่งแวดล้อมไว้ได้

Reference

1. IBM. (2024). *X-Force Threat Intelligence Index 2024*. https://www.ibm.com/reports/threat-intelligence
2. Imaginovation. (2024, 9 May). *IIoT Explained: Benefits, Use Cases, and Implementation Challenges*. https://imaginovation.net/blog/iiot-explained/
3. Market Data Forecast. (2024, June). *Industrial IoT Market*. https://www.marketdataforecast.com/market-reports/industrial-ioT-market
4. National Technology. (2020, 2 November). *Industrial IoT connections to reach 37bn by 2025*. https://nationaltechnology.co.uk/Juniper_Research_Industrial_IoT_Connections_Prediction_Smart_Factory.php?utm_source=jsrecent
5. World Economic Forum. (2024, 7 June). *3 Ways Manufacturers Can Build a Culture of Cyber Resilience*. https://www.weforum.org/stories/2024/06/manufacturers-face-cyber-threats-cyber-resilience-culture/