ข่าวสารไอที

ปีที่ 18 ฉบับที่ 5 พฤษภาคม 2562

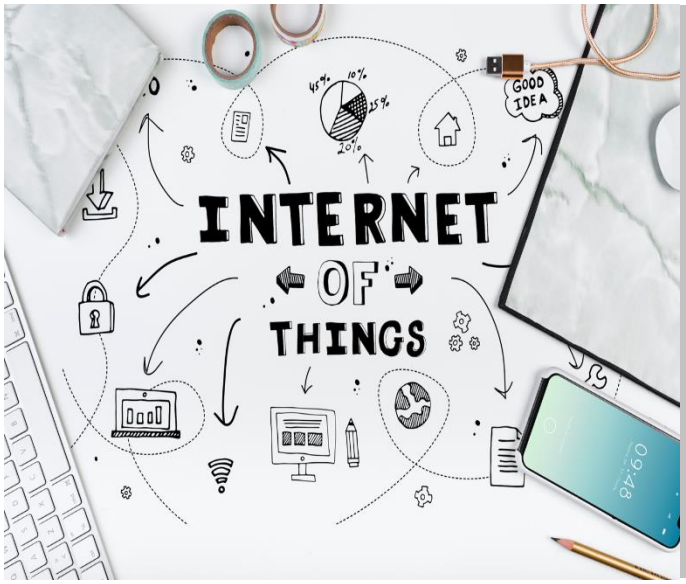
ยกระดับความปลอดภัยให้ Smart Cities ด้วย “ข้อมูล”

หลายๆ เมืองทั่วโลกกำลังก้าวเข้าสู่การเป็น Smart Cities ซึ่งกล่าวได้ว่าเป็นเมืองที่ทุกสิ่งมีการเชื่อมต่อระหว่างกัน ช่วยยกระดับตัวเมืองให้มีประสิทธิภาพมากยิ่งขึ้น รวมไปถึงช่วยเพิ่มความสะดวกสบาย ความมั่นคงปลอดภัย และนำเสนอบริการให้ตรงกับความชื่นชอบของแต่ละคนได้อย่างง่ายๆ เพียงแค่ใช้ปลายนิ้วสัมผัส

ถึงแม้ว่า Smart Cities อาจฟังดูเหมือนเป็นเมืองแห่งอนาคต แต่แผนพัฒนาดังกล่าวอาจกลายเป็นฝันร้ายได้ ถ้าเราเมินเฉยต่อความเสี่ยงที่มาพร้อมกับการนำเทคโนโลยี Internet of Things เข้ามาใช้ ดังที่สิงคโปร์เพิ่งประสบไป เมื่อกลางปีที่ผ่านมา เมื่อ SingHealth เครือหน่วยงานด้านสาธารณสุขที่ใหญ่ที่สุดในประเทศสิงคโปร์ถูกแฮ็ก ข้อมูลผู้ป่วยกว่า 1,500,000 คนซึ่งรวมไปถึงข้อมูลของนาย Lee Hsien Loong ประธานาธิบดีคนปัจจุบันของสิงคโปร์ถูกขโมยออกไป ข้อมูลนี้อาจถูกนำไปขายทอดตลาดมืด นำไปต่อยอดเพื่อเข้าถึงบัญชีธนาคาร หรือนำไปใช้ปลอมแปลงตัวตนเพื่อก่ออาชญากรรมอื่น ๆ ต่อได้

หลุมพรางของ Smart Cities

Melvin Kranzberg นักประวัติศาสตร์ชาวอเมริกันกล่าวไว้ว่า “เทคโนโลยีไม่ใช่ทั้งสิ่งที่ดีหรือเลว และไม่ใช่สิ่งที่เป็นกลางด้วยเช่นกัน” หมายความว่า ผลลัพธ์ที่จะเกิดขึ้นกับ Smart Cities จะขึ้นอยู่กับว่าเทคโนโลยีถูกนำไปใช้อย่างไร การป้องกันการนำเครื่องมือและระบบดิจิทัลไปใช้ในทางที่ผิดจึงกลายเป็นประเด็นที่ต้องให้ความสำคัญ อย่างไรก็ตาม ก่อนจะถึงขั้นนั้น เราต้องเข้าใจก่อนว่า Smart Cities มีช่องโหว่ที่จะถูกโจมตีอย่างไรได้บ้าง ดังนี้



1. IoT เปิดช่องให้ภัยคุกคามไซเบอร์

Frost & Sullivan คาดการณ์ว่า ภูมิภาคเอเชียแปซิฟิกจะลงทุนราว $59,000 ล้าน (ประมาณ 1.9 ล้านล้านบาท) ทางด้าน Internet of Things (IoT) ภายในปี 2020 ซึ่งเพิ่มขึ้นจากปี 2014 เกือบ 6 เท่าตัว ปริมาณการลงทุนที่เพิ่มขึ้นนี้ส่วนใหญ่ถูกผลักดันมาจากแผนพัฒนา Smart Cities อย่างไรก็ตาม อุปกรณ์ IoT เกือบทั้งหมดไม่ได้ถูกพัฒนาให้มีความมั่นคงปลอดภัยเป็นพื้นฐาน รวมไปถึงปัจจุบันยังไม่มีมาตรฐานด้านความมั่นคงปลอดภัย IoT ที่เป็นชิ้นเป็นอัน ทำให้อุปกรณ์ IoT มักตกเป็นช่องทางหลักที่แฮ็กเกอร์ใช้โจมตี

2. มัลแวร์บน IoT มีปริมาณเพิ่มมากขึ้น

เมื่ออุปกรณ์ IoT มีจุดอ่อน แฮ็กเกอร์ย่อมหาหนทางโจมตีจุดอ่อนนั้น ๆ หนึ่งในนั้น คือ มัลแวร์ที่ถูกพัฒนาให้เจาะช่องโหว่ระบบ IoT โดยเฉพาะ รายงานจาก Kaspersky Lab ระบุว่า อุปกรณ์ IoT ถูกโจมตีโดยมัลแวร์มากกว่า 120,000 แบบระหว่างช่วงครึ่งปีแรกของปี 2018 ที่ หนึ่งในนั้นคือ Okiru ซึ่งเป็นสายพันธุ์ย่อยของ Mirai มัลแวร์ดังกล่าวถูกค้นพบเมื่อเดือนมกราคม 2018 โดยพุ่งเป้าที่อุปกรณ์ IoT หลายพันล้านเครื่องที่ใช้หน่วยประมวลผลแบบ ARC แล้วเปลี่ยนอุปกรณ์เหล่านั้นให้กลายเป็นกองทัพ Botnet สำหรับโจมตีแบบ DDoS หรือขโมยข้อมูลจากผู้ใช้

3. ขาดความสามารถในการบริหารจัดการกับข้อมูลปริมาณมหาศาลที่ถาโถมเข้ามา

ผลวิจัยจาก IDC ระบุว่า ภายในปี 2025 จะมีอุปกรณ์ราว 80,000 ล้านเครื่องเชื่อมต่อกับอินเทอร์เน็ต ก่อให้เกิดข้อมูลปริมาณสูงถึง 180 Zettabytes ข้อมูลปริมาณมหาศาลระดับนี้จะกลายเป็นประเด็นท้าทายใหม่สำหรับหน่วยงานรัฐฯ ในการจัดเก็บ วิเคราะห์ และรักษาให้มั่นคงปลอดภัย นอกจากนี้ การเก็บข้อมูลแต่ละประเภทแยกจากกันยิ่งทำให้การวิเคราะห์ข้อมูลในรายละเอียดเชิงลึกทำได้ช้า และการผสานความร่วมมือเพื่อตอบสนองต่อความต้องการของประชาชนก็ทำได้อย่าง

เพิ่มความปลอดภัยให้กับ Smart Cities ตั้งแต่รากฐาน

การทำให้เมืองมีความปลอดภัยสาธารณะเป็นความรับผิดชอบหลักของรัฐบาล การทราบถึงภัยอันตรายที่อาจเกิดขึ้นกับ Smart Cities ช่วยให้รัฐบาลสามารถวางแผนและลงแรงเพื่อปกป้องประชาชนได้ดียิ่งขึ้น Frost & Sullivan คาดการณ์ไว้ว่า การลงทุนทางด้านเทคโนโลยีจากทั่วโลกสำหรับสนับสนุนความปลอดภัยสาธารณะจะเพิ่มขึ้นถึง $85,000 ล้าน (ประมาณ 2.74 ล้านล้านบาท) ภายในปี 2020 โดย 24% จะมาจากประเทศในภูมิภาคเอเชียแปซิฟิก

เนื่องจากข้อมูลเป็นตัวจุดชนวนการเติบโตของ Smart Cities จึงเป็นเรื่องสำคัญที่รัฐบาลจะลงทุนทางด้านแพลตฟอร์ม Data Management, Data Security, Advanced Analytics และ Machine Learning เพื่อตอบโจทย์ความท้าทายดังต่อไปนี้

- เพิ่มประสิทธิภาพในการรวบรวมข้อมูลจากหลายๆ ระบบและหลายๆ องค์กร เพื่อให้แอปพลิเคชันต่างๆ สามารถนำไปทำการวิเคราะห์ต่อได้
- ย่อยข้อมูล จัดเก็บ และนำข้อมูลจากอุปกรณ์ IoT ไปใช้ได้อย่างมีประสิทธิภาพ ในขณะที่มีต้นทุนในการดำเนินงานต่ำ
- ช่วยเพิ่มความสามารถด้าน Data Security, Compliance และ Governance บนทุกข้อมูลที่ถูกจัดเก็บรวบรวมมา
- ผลักดันให้เกิดการวิเคราะห์และประมวลผลข้อมูล IoT แบบเรียลไทม์ ทั้งขณะจัดเก็บหรือรับส่งข้อมูลวิเคราะห์ข้อมูลได้จากทุกที่ ไม่ว่าจะเป็นบน Edge Computing, Cloud, On-premises หรือแบบ Hybridผลักดันให้เกิดการทำ Data Science และสร้างโมเดล Machine Learning

ด้วยความสามารถเหล่านี้ จะช่วยให้รัฐบาลสามารถติดตามความเคลื่อนไหวของข้อมูล รวมไปถึงทำการตัดสินใจอย่างชาญฉลาดและวางแผนบนพื้นฐานของข้อมูลในรายละเอียดเชิงลึกเพื่อพัฒนาความปลอดภัยให้แก่ Smart Cities ได้ดียิ่งขึ้น

ผสานรวมข้อมูลไว้ที่เดียวด้วย Cloudera Enterprise Data Hub

Cloudera Enterprise Data Hub เป็นแพลตฟอร์ม Big Data สำหรับจัดเก็บและรวบรวมข้อมูลที่กระจัดกระจายตามระบบและองค์กรต่าง ๆ ไว้ภายในที่เดียว ช่วยขจัดปัญหาเรื่องแต่ละหน่วยงานต่างฝ่ายต่างจัดเก็บข้อมูลในรูปแบบของตนเอง ทำให้มาตรฐานในการจัดเก็บข้อมูลเป็นแบบเดียวกัน ง่ายต่อการกำกับดูแล และรักษาให้มั่นคงปลอดภัย

Smart Cities เป็นระบบนิเวศขนาดใหญ่ที่ทุกคนควรมีส่วนร่วมในการดูแลให้มั่นคงปลอดภัย นอกจากหน่วยงานรัฐซึ่งเป็นแกนหลักแล้ว องค์กรเอกชนบางแห่งก็ควรเข้ามามีส่วนร่วมในการเพิ่มความปลอดภัยให้แก่ลูกค้าและตัวเมืองด้วยเช่นกัน ยกตัวอย่างเช่น ธนาคาร United Overseas Bank (UOB) ของสิงคโปร์ที่ใช้ Machine Learning ในการตรวจจับและระบุกิจกรรมต้องสงสัยที่อาจเกี่ยวข้องกับการฟอกเงินได้อย่างรวดเร็วและแม่นยำ เหนือกว่าการใช้ระบบป้องกันการฟอกเงินที่ใช้การกำหนดเงื่อนไขแบบเก่า เป็นต้น

อีกหนึ่งตัวอย่างคือ Thorn องค์กรไม่แสวงหาผลกำไรที่ก่อตั้งขึ้นโดยมีจุดประสงค์เพื่อยับยั้งการล่วงละเมิดทางเพศแก่ผู้เยาว์ ด้วยการสนับสนุนจาก Cloudera Enterprise Data Hub ในการจัดเก็บและวิเคราะห์ข้อมูล ทำให้ Thorn สามารถรัน Natural Language Processing และอัลกอริทึมเชิงวิเคราะห์บนข้อมูลที่ตนมีอยู่ได้ ผลลัพธ์คือ Thorn สามารถตรวจเจอการค้ามนุษย์ 4,624 คนและผู้เยาว์อีก 2,025 คน รวมไปถึงสามารถนำผู้กระทำผิดมาลงโทษได้มากกว่า 2,249

ตัวอย่างเหล่านี้แสดงให้เห็นว่า การเพิ่มความปลอดภัยสาธารณะเป็นหนึ่งในตัวขับเคลื่อนสำคัญของสังคมให้ก้าวไปสู่การเป็น Smart Cities แน่นอนว่าไม่มีใครที่ต้องการอยู่ในโลกที่เต็มไปด้วยอาชญากรรมและภัยคุกคาม แม้ว่าจะสะดวกสบายแค่ไหนก็ตาม เพื่อให้บรรลุวัตถุประสงค์นี้ ภาครัฐจำเป็นต้องสร้างรากฐานเพื่อช่วยให้ตนเองสามารถดำเนินการตัดสินใจได้อย่างชาญฉลาด รวมไปถึงร่วมมือกับภาคเอกชนเพื่อให้สามารถรับมือ กับความเสี่ยงที่จะเกิดขึ้นได้อย่างมีประสิทธิภาพ

บทบรรณาธิการ: Mark Micallef, Vice President of Asia Pacific and Japan, Cloudera

เกี่ยวกับ Cloudera

Cloudera ก่อตั้งขึ้นเมื่อปี 2008 เป็นบริษัท Startup ที่มีเป้าหมายเพื่อสร้างแพลตฟอร์ม Big Data Analytics แบบ Open-source ที่ทุก ๆ องค์กรสามารถเข้าถึงและใช้งานได้ง่าย หลังจากที่ Intel ได้เข้ามาลงทุนใน Cloudera ส่งผลให้บริษัทเติบโตขึ้นเรื่อย ๆ จนเข้าสู่ IPO ในเดือนมีนาคม 2017

ปัจจุบันนี้ Cloudera ได้กลายเป็นหนึ่งในผู้ให้บริการแพลตฟอร์ม Big Data Analytics ชั้นนำของโลก ซึ่งเปิดให้บริการโซลูชันทั้งแบบ On-premises และบน Cloud ได้แก่ Data Management Platform, Business Intelligence, NoSQL, Data Science and Engineering และอื่น ๆ
ดูรายละเอียดเกี่ยวกับบริการของ Cloudera ได้ที่ https://www.cloudera.com/

ขอบคุณแหล่งที่มาข่าว

https://www.techtalkthai.com/make-smart-cities-safer-with-data-by-cloudera/

จัดทำโดย นายพร้อมกิติ วรสิษฐ์ดรุณเวทย์
นักศึกษาฝึกงาน มหาวิทยาลัยบูรพา