โซลูชั่นสำหรับปีใหม่ – ที่ได้รับการพิสูจน์แล้วว่าเหมาะสมสำหรับอนาคต

โดยคุณประคุณ เลาหกิตติกุล, ผู้อำนวยการประจำประเทศไทยของบริษัทอรูบ้าหนึ่งในบริษัทของฮิวเลตต์ แพคการ์ด เอ็นเตอร์ไพรส์

ปัจจุบันภูมิภาคเอเชียแปซิฟิกเป็นภูมิภาคที่มีผู้ใช้อินเตอร์เน็ตมากที่สุดในโลกโดยมีการขยายตัวอย่างรวดเร็วเป็นผลอันเนื่องมาจากการตื่นตัวในการใช้อุปกรณ์พกพาและการเพิ่มขึ้นของคนรุ่นยุคมิลิเนียน ผนวกการริเริ่มนโยบายของรัฐบาลประเทศต่างๆทั่วทั้งเอเชียที่สนับสนุนและผลักดันการเปลี่ยนแปลงเศรษฐกิจสังคมให้เป็นดิจิตอลในระดับกว้างขวาง (mass digitization) – จากนโยบาย Digital India ไปจนถึง Hong Kong Smart City Blueprint ในอนาคต การพัฒนาเศรษฐกิจของภูมิภาคเอเชียตะวันออกเฉียงใต้จะยิ่งขยายตัวมากขึ้น ด้วยการเข้ามาของ(1) ทุนและผลประโยชน์ของจีนจะเข้ามาเป็นตัวกระตุ้นช่วยผลักดันการเติบโตทางเทคโนโลยีของภูมิภาคนี้ต่อไป

สำหรับประเทศไทยรัฐบาลได้ผลักดันตัวแบบนโยบายการพัฒนาเศรษฐกิจที่เรียกว่า Thailand 4.0 ขึ้นมาโดยมุ่งหวังว่าการนำเทคโนโลยีมาใช้มากยิ่งขึ้นจะเป็นตัวผลักดันการเติบโตทางเศรษฐกิจต่อไป บางส่วนของนโยบายนี้ประกอบด้วยการขยายความสามารถทางเทคโนโลยีหลัก ๆ ดังเช่น เทคโนโลยีชีวะภาพ เทคโนโลยีการดูแลสุขภาพ และเทคโนโลยีทางการแพทย์ ยิ่งกว่านั้นตัวแบบนี้ยังเน้นผลักดันให้ทำการปรับปรุงโครงสร้างพื้นฐานในการเชื่อมต่อทั้งหลายของประเทศให้ดีขึ้น และเพิ่มความสามารถให้แก่องค์กรธุรกิจท้องถิ่นด้วยการใช้เทคโนโลยีเข้ามาเพิ่มประสิทธิภาพการดำเนินงานและความสามารถในการผลิตของธุรกิจ
ในขณะเดียวกัน สาธารณะชนคนไทยก็ยอมรับการปรับตัวเป็นดิจิตอลมากขึ้น การมีการเชื่อมต่อและอุปกรณ์พกพาเป็นเรื่องปกติธรรมดาของคนในยุคมิลิเนียมแล้ว ซึ่งคิดเป็น 32 % ของประชากรทั้งประเทศ จากรายงานงานวิจัยของ Frost & Sullivan คาดการณ์ว่าการใช้จ่ายใน IoT ของประเทศไทยจะขยายตัวอย่างรวดเร็วจนถึง 973.3 ล้านดอลลาร์สหรัฐ ฯ (2) (ประมาณ 32,000 ล้านบาทไทยที่อัตราแลกเปลี่ยน 33 บาทต่อดอลลาร์สหรัฐ ฯ) ในปี 2020 (พ.ศ. 2563)
อย่างไรก็ตามการเปลี่ยนเป็นดิจิตอลมักตามมาด้วยการสร้างสภาพแวดล้อมทาง IT ที่ซับซ้อน เมื่อรัฐบาลหรือองค์กรเอกชนนำเทคโนโลยีอย่างเช่น hybrid cloud, the internet of Things (IoT) และปัญญาประดิษฐ์มาใช้ร่วมกัน ยิ่งกว่านั้นเมื่อสภาพแวดล้อมทาง IT มีความซับซ้อนมากขึ้นยอมเพิ่มความอ่อนไหวต่อภัยคุกคามทางไซเบอร์มากขึ้นตามไปด้วย เห็นได้จากการโจมตีโดย ransomware ที่ชื่อ WannaCry และ Petya เมื่อไม่กี่เดือนที่ผ่านมา อาชญากรรมทางไซเบอร์ได้พัฒนาขึ้นไปมากและในปัจจุบันมีอันตรายสูงถึงขั้นทำให้โลกทั้งโลกปั่นป่วนกันไปหมด

ภัยคุกคามเหล่านี้ดูเหมือนว่าจะอยู่ใกล้ตัวเอามาก ๆ เพราะว่าองค์กรต่าง ๆ ในภูมิภาคเอเชียกว่า 80% เห็นว่าตัวเองมีโอกาสถูกโจมตีมากกว่าองค์กรในภูมิภาคอื่น ๆ ของโลก(3) แม้ว่า UN Global Cybersecurity index จะให้ประเทศมาเลเซียและสิงคโปร์จัดอยู่ในประเทศที่มีความปลอดภัยทางไซเบอร์สูงในระดับสามอันดับต้น ๆ ในการในรายงานปี 2017 แต่ประเทศส่วนใหญ่ในเอเชียอย่างเช่น จีน อินเดีย ไต้หวัน และเวียดนามล้วนได้รับความเสียหายค่อนข้างสูงจากการโจมตีของ WannaCry ตามข้อเท็จจริงแล้วครึ่งหนึ่งของระบบคอมพิวเตอร์ที่ถูกโจมตีในสองวันแรกอยู่ในประเทศจีน ตามรายงานของ National Computer network Emergency Response Centre ของจีนเอง

เมื่อองค์กรต่าง ๆ ต้องมุ่งมั่นให้โซลูชั่นที่ดีที่สุดแก่ลูกค้าของตน พวกเขาจะมั่นใจได้อย่างไรว่ายังคงสามารถรักษาระดับการให้บริการที่รวดเร็ว มีความปลอดภัยสูง มีผลกระทบที่ดีและทันต่อความต้องการของลูกค้า ? ต่อไปนี้เป็นโซลูชั่นใหม่ 4 ประการในปีใหม่สำหรับธุรกิจทั้งหลายที่จะต้องมีในรายการ checklist ที่จำเป็นต้องมีของตน

ปีใหม่ เราต้องปรับเปลี่ยนตัวเองใหม่ (New year, new you)

ก่อนที่เราจะพิจารณาแนวโน้มของสภาพแวดล้อมในระดับมหัพภาคเราจำเป็นต้องมองทบทวนและตรวจสอบภายในองค์กรของเราก่อน

ในโลกที่การเปลี่ยนแปลงเกิดขึ้นอย่างรวดเร็วนี้ การทำระบบ IT ให้เป็นอัตโนมัติและนำบริการบนระบบคลาวด์มาใช้งานกลายเป็นปัจจัยสำคัญในการสร้างความสามารถให้ธุรกิจปรับตัวตามทันการเปลี่ยนแปลงที่รวดเร็วมากนี้ การใช้อุปกรณ์พกพาอย่างแพร่หลายได้เปลี่ยนธรรมชาติของการเข้าถึงระบบ IT ให้จำเป็นต้องสามารถรองรับอุปกรณ์หลากหลายที่แต่ละคนมีโดยการเข้าจากสถานที่ใดก็ได้ซึ่งไม่สามารถกำหนดคาดการณ์ได้ล่วงหน้า ต้องรองรับการจราจรของข้อมูลบนระบบเครือข่ายในรูปแบบใหม่ ๆ การเข้าสู่ระบบเครือข่ายของอุปกรณ์ที่ไม่เคยรู้จักมาก่อนและสภาพแวดล้อมทาง IT ที่สลับซับซ้อนแต่อ่อนไหวต่อภัยคุกคามทางไซเบอร์โดยปราศจากขอบเขตด้านการรักษาความปลอดภัย

ตามรายงานของ Frost & Sullivan พบว่ามีเพียง 4.3 % ขององค์กรในภูมิภาคเอเชียที่เชื่อว่าตนเองสามารถยืดหยัดต่อสู้กับภัยคุกคามทางไซเบอร์ได้ ในทำนองกลับกันเท่ากับเป็นการชี้ให้เห็นว่าองค์กรส่วนใหญ่ในภูมิภาคนี้ไม่มีความมั่นใจในความระดับความพร้อมของระบบป้องกันความปลอดภัยทางไซเบอร์ของตน(4) ประเทศไทยเป็นประเทศหนึ่งใน 25 ประเทศระดับต้น ๆ ของโลกที่ติด malware (5) โดยมีมากกว่า 5 ล้านอุปกรณ์ที่ติด malware ข้อมูลจาก Microsoft Digital Crimes Unit สถาปัตยกรรมระบบเครือข่ายแบบดั้งเดิม(legacy) สร้างมาเพื่อรองรับยุค client-server ไม่ได้ออกแบบมาสำหรับรองรับความต้องการในปัจจุบันขององค์กรต่าง ๆ และลูกค้าที่ต้องการให้สามารถรองรับการใช้อุปกรณ์พกพา IoT และทำงานได้บนระบบคลาวด์ทั้งหมดนี้เป็นเหตุผลที่ทำให้จำเป็นต้องเปลี่ยนไปใช้ระบบเครือข่ายแบบใหม่ที่เป็น intelligent core system เพื่อจะสามารถรองรับโอกาสและความท้าทายทางธุรกิจใหม่ ๆ ได้ องค์กรธุรกิจจำเป็นต้องทำระบบเครือข่ายของตนให้ทันสมัย ผนวกระบบมีสายและไร้สายเข้าด้วยกันเป็นระบบเดียว นำเครื่องมือและเทคโนโลยีใหม่ ๆ เข้ามาใช้เพื่อเปลี่ยนที่ทำงานให้เป็นดิจิตอล ในปี 2018 (พ.ศ.2561) องค์กรส่วนมากจะต้องมี intelligent core system ซึ่งค่อนข้างยืดหยุ่น มีระบบปฏิบัติการณ์ที่สามารถ

เขียนโปรแกรมเพิ่มเติมได้เต็มที่ตามต้องการและระบบรักษาความปลอดภัยที่สามารถครอบคลุมทุกระดับการใช้งาน และยังคงเป็นระบบเครือข่ายที่สามารถขยายได้ตามความต้องการและง่ายในการบริหารจัดการอีกด้วย

ทำอย่างอาจได้อย่างอื่นที่คาดไม่ถึง (What goes around might not always come around)

ก้าวเดินเล็ก ๆ ที่ผิดพลาดในวันนี้อาจมีผลร้ายในขนาดที่มโหฬารในอนาคต สะท้อนภาพการรักษาความปลอดภัยบนระบบเครือข่าย ช่องโหว่เล็ก ๆ ช่องหนึ่งหรือการมองข้ามจุดเล็ก ๆ ในบางมาตรการรักษาความปลอดภัยสามารถนำไปสู่การรั่วไหลของข้อมูลอย่างมโหฬารจนเป็นข่าวพาดหัวหนังสือพิมพ์ (headline-grabbing data breach) ดังนั้นจึงจำเป็นต้องสร้างความมั่นใจว่ามีความสามารถในการมองเห็นที่ชัดเจนและโปร่งใสครอบคลุมทุก ๆ ส่วนขององค์กรในการสร้างศักยภาพเพื่อป้องกันการโจมตีใด ๆ ที่คาดว่าจะเกิดขึ้น ขณะที่บริษัทมากกว่าครึ่งในภูมิภาคเอเชียนำเทคโนโลยี IoT เข้ามาใช้งานในปัจจุบัน แต่กลับพบว่ามีถึง 84 % ของบริษัทเหล่านี้เคยประสบกับการโจมตีและการรั่วของระบบรักษาความปลอดภัยที่เกี่ยวข้องกับการใช้อุปกรณ์ IoT(6) ดังนั้นจึงไม่ต้องสงสัยเลยว่า IoT นั้นเองเป็นตัวนำความท้าทายและภัยคุกคามตัวใหม่มาให้องค์กร และทุกองค์กรจะต้องตื่นตัวระมัดระวังต่อภัยคุกคามใด ๆ ที่อาจจะเกิดขึ้นต่อข้อมูลและทรัพยากรทาง IT โดยผ่านอุปกรณ์ IoT

คำถามคือจะนำกลยุทธ์ความปลอดภัยสำหรับ IoT ที่ดีที่สุดมาใช้ได้อย่างไร องค์กรจำเป็นต้องระบุลักษณะเฉพาะของอุปกรณ์ต่าง ๆ ให้ละเอียดมากขึ้นและกำหนดการใช้งานตามบทบาทของผู้ใช้เป็นส่วน ๆ สำหรับการเข้าสู่ระบบเครือข่าย รวมทั้งทบทวนการเปลี่ยนแปลงในการออกแบบโครงสร้างพื้นฐานของเครือข่าย (campus design) ทั้งหมด กลยุทธการรักษาความปลอดภัยขององค์กรสำหรับ IoT ต้องรวมถึงการสร้างโพลิซี่โดยอัตโนมัติที่สามารถระบุว่าอุปกรณ์ไหนสามารถเชื่อมต่อเข้ามาได้ สามารถเข้าถึงข้อมูลและแอพพลิเคชั่นอะไรได้บ้าง และใครมีอำนาจในการบริหารจัดการและดูแลรักษาอุปกรณ์เหล่านี้ นั่นหมายถึงจะต้องมีโซลูชั่นที่สามารถรักษาความปลอดภัยให้แก่ธุรกิจและโครงสร้างพื้นฐานของ IOT ขององค์กรผ่านแนวคิดต้องปิดช่องโหว่บนคลาวด์ให้หมด (closed-loop approach) ดังเช่นการใช้ Aruba 360 Secure Fabric มาช่วยเพิ่มความสามารถในการมองทะลุปรุโปร่งถึงพฤติกรรมการใช้อุปกรณ์ต่าง ๆ ในช่วงเวลาต่าง ๆ อันเป็นกุญแจที่สำคัญมากในการสร้างกลยุทธระบบรักษาความปลอดภัยสำหรับ IoT อย่างครบถ้วนสมบูรณ์

เล่นซ่อนหา (Hide and seek)

เป็นเรื่องง่าย ๆ ที่เราอาจจะพลาดโอกาสดี ๆ ที่ซ่อนอยู่โดยการใช้ระบบดั้งเดิม ๆ ต่อไป แต่ในสภาพบรรยากาศที่การแข่งขันทางธุรกิจสูงขึ้นเรื่อย ๆ การสร้างความผูกพันกับลูกค้า(customer engagement) ได้แบบตอบสนองทันที (real time) และสะดวกกลายเป็นการสร้างความแตกต่างที่มีผลต่อธุรกิจอย่างสูง มีธุรกิจมากขึ้นเรื่อย ๆ ที่มองหาโอกาสใหม่ ๆ โดยใช้ผลิตภัณฑ์บริการอ้างอิงสถานที่ (location-based services) ใช้การวิเคราะห์และการสร้างความผูกพันกับลูกค้าแบบเรียลไทม์

ยิ่งธุรกิจต้องการดำเนินงานอย่างมีประสิทธิภาพสูงสุด สร้างโอกาสในการผูกพันกับผู้ใช้ให้มากขึ้น และลดต้นทุนค่าใช้จ่าย การใช้บริการอ้างอิงสถานที่และการวิเคราะห์ยิ่งจะถูกใช้มากขึ้นเรื่อย ๆ หน่วยงาน IT ในองค์กรธุรกิจค้าปลีก ดูแลสุขภาพ และองค์กรธุรกิจต่าง ๆ ต้องการที่จะมีความสามารถในการระบุรูปแบบการจราจรบนระบบเครือข่าย

การใช้พื้นที่และทรัพยากรทาง IT ที่เกี่ยวข้องกับผู้ใช้ให้ได้ดีขึ้น

ตัวอย่างการใช้ระบบติดตามทรัพย์สิน (asset tracking) ที่ใช้ง่ายและสะดวกสำหรับธุรกิจบริการดูแลสุขภาพ ค้าปลีก และคลังสินค้าเป็นสิ่งที่หลาย ๆ องค์กรต้องใช้ การใช้ Bluetooth Low Energy (BLE) เข้ามาใช้ร่วมกับ access point แบบไร้สายอย่างเช่น Aruba Tags จะช่วยเพิ่มความสามารถที่มีผลโดยตรงต่อธุรกิจและการสร้างความผูกพันกับผู้ใช้โดยไม่จำเป็นต้องสร้างโครงสร้างพื้นฐานระดับที่สองที่ค่อนข้างแพงขึ้นมารองรับ (an expensive secondary infrastructure)

ไปเร็วขึ้นหรือไม่ก็กลับบ้านไปเลย (Go fast or go home)

โมเดลและเทคโนโลยีต่าง ๆ ทางธุรกิจใหม่ ๆ ผ่านมาแล้วก็ผ่านไปแต่ความต้องการของลูกค้าที่เพิ่มขึ้นนั้นเป็นสิ่งที่เป็นจริงเสมอ ธุรกิจต่าง ๆ ต้องการพาร์เนอร์ที่จะมาช่วยเพิ่มเติมและขยายความสามารถในการผูกพันกับลูกค้าผ่านดิจิตอล (digital engagement) ในปี 2018 เราได้สร้างมาตรฐานใหม่ ที่เรียกว่า 802.11ax – เป็นมาตรฐานใหม่ของระบบ LAN ไร้สาย – เป็นเทคโนโลยีหนึ่งที่จะช่วยพัฒนาการผูกพันกับผู้ใช้ที่ปลายทาง (end user engagement) ลองจินตนาการถึงความเร็วที่สูงขึ้น 4 ถึง 10 เท่า – นั้นคือสิ่งที่ 802.11ax สัญญาจะทำให้เป็นจริง ตามรายงานการศึกษาของ The State of Online Retail Performance(7) พบว่าเวลาโหลดเว็บเพจที่ช้าลง 2 วินาทีในเว็บ e-commerce ส่งผลร้ายทำให้อัตราการดูเว็บไซต์เพียงหน้าเดียวแล้วจากไป (bounce rates) สูงขึ้นถึง 103 % มาตรฐาน 802.11ax ไม่เพียงทำให้การเข้าถึงเร็วขึ้นเท่านั้น การเข้าถึงในสถานที่ที่คนเข้ามาใช้มาก ๆ จะไม่สะดุดช้าลง และยังคงรวดเร็วอย่างต่อเนื่องไหลเลื่อน

สิ่งที่ดีที่สุดสำหรับธุรกิจคือความเข้าใจการมีปฏิสัมพันธ์ของผู้ใช้ (users interact) ธุรกิจสามารถลงทุนไปในเครื่องมือที่ก้าวหน้ามาก ๆ แต่มันในสายตาของผู้ใช้ต้องน่าสนใจและใช้ง่าย จำเป็นอย่างยิ่งที่ต้องพึ่งคู่ค้าทางเทคโนโลยีที่สามารถให้สถาปัตยกรรมที่มีบริการที่สามารถตระหนักรู้ถึงบริบท (context aware service) ซึ่งให้ข้อมูลเชิงลึกที่ถูกต้องเกี่ยวกับว่า ผู้ใช้เป็นใคร? ทำอะไร? และอย่างไรในระบบเครือข่าย? และสามารถนำข้อมูลเหล่านั้นมาใช้เสริมสร้างความปลอดภัยของระบบเครือข่ายและคุณภาพการให้บริการของแอพพลิเคชั่นให้ดีขึ้นและยืดหยุ่นสามารถครอบคลุมในทุก ๆ ส่วนของระบบเครือข่าย รวมทั้งบริการจากผู้ผลิตรายอื่น ๆ ได้ด้วย

เทคโนโลยีก้าวหน้าขึ้นด้วยอัตราความเร็วของแสง และในทางเดียวกันต่างต้องยอมรับว่าภัยคุกคามก็เพิ่มความซับซ้อนตามอัตราการเพิ่มของ IoT ในอัตราเดียวกันเช่นกัน ด้วยการวิเคราะห์แนวโน้มและการคาดการณ์ต่าง ๆ ล้วนทำเพียงไม่เกิน 3 เดือนในปัจจุบัน องค์กรต่าง ๆ จำเป็นต้องเตรียมตัวป้องกันภัยคุกคามใกล้ตัวในระบบเครือข่ายที่คาดไม่ถึงและจะต้องเลือกใช้ระบบเครือข่ายที่ถูกทดสอบแล้วว่าพร้อมจะต่อสู้ป้องกันภัยเหล่านี้ในอนาคต การที่ Aruba มีโซลูชั่นที่พร้อมส่งเสริมการใช้อุปกรณ์พกพา (mobility) และความคล่องตัว (agility) ในการปรับเปลี่ยนขององค์กร ขณะเดียวกันมีความก้าวหน้าที่พร้อมจะสู้กับภัยคุกคามที่ซับซ้อนมากขึ้นนี้ด้วย – องค์กรต่าง ๆ จำเป็นต้องทำเพียงก้าวแรกก้าวเดียวคือเลือกเรา

เหนือกว่าอื่นใด ในบรรยากาศที่การแข่งขันสูงขึ้นเรื่อยๆเงินลงทุนทุกบาททุกสตางค์ล้วนมีค่าและไม่มีใครต้องการที่จะปล่อยให้เงินของตนรั่วไหลไปอีกหลายล้านอย่างสูญเปล่าหลังจากอุตส่าห์ลงทุนป้องกันภัยคุกคามไปแล้ว ซึ่งจะส่งผลต่อตัวเลขผลกำไร/ขาดทุนในบรรทัดสุดท้ายของงบการเงิน

——————————————–

(1)Techwire Asia , What tech trends are on the rise in 2018.
(2)IoT Business Platform , IoT Thailand: market to reach US$973.7mil in 2020.
(3)BBC, Asia Companies Have World’s Worst Cybersecurity study says.
(4)Frost & Sullivan: Exploring Cyber Security Maturity in Asia: A study of Enterprise Corporate Executives, IT Executives & IT Practitioners’ Perceptions towards Cyber Security Readiness in Asia-Pacific.
(5)Tech in Asia , Cybersecurity in Thailand, firms lose up to $100m. reports show.
(6) Aruba Networks:The Internet of Things : Today and Tomorrow.
(7) Akamai: The State of Online Retail Performance.