IT Trend 2017 และการรับมือด้านความปลอดภัย

วิชญ์ศุทธ์ เมาะพงษ์
ที่ปรึกษาโครงการสารสนเทศของหน่วยงานภาครัฐ
สังกัดสถาบันวิจัยและให้คำปรึกษา
แห่งมหาวิทยาลัยธรรมศาสตร์

ต่อ จากฉบับที่แล้ว

นอกจากนี้สิ่งที่ควรคำนึงถึงคือเรื่องของความมั่นคงปลอดภัย เนื่องจากในปัจจุบันมีหลายองค์การถูกโจมตีด้วยผู้ไม่ประสงค์ดีผ่านทางการใช้เทคโนโลยีอย่างต่อเนื่อง จำเป็นต้องรู้เท่าทันสถานการณ์ความเสี่ยง และเตรียมพร้อมเพื่อรับมือกับเหตุการณ์ไม่พึงประสงค์ที่เกิดจากการโจมตีดังกล่าว โดยสำหรับปี 2017 Trend Micro ชั้นนำระดับโลกด้านการรักษาความมั่นคงปลอดภัยสารสนเทศได้ออกมากล่าวถึงแนวโน้มด้านความปลอดภัย ดังนี้

1) Ransomware ในปี 2017 จะมีวิธีการและการเลือกเป้าหมายโจมตีที่หวีความหลากหลายมากขึ้น

Ransomware คือชื่อเรียก Software ที่โจมตีไปที่ข้อมูลสำคัญของเป้าหมายด้วยการเจาะระบบ และเข้ายึดครองข้อมูลสำคัญ โดยจะใช้วิธีการเรียกค่าไถ่เพื่อแลกกับการไม่เผยแพร่หรือปล่อยระบบให้สามารถกลับไปให้บริการได้ หลายๆ องค์การโดยโจมตีในลักษณะนี้มาแล้วรวมถึงของผู้เขียนเอง ที่เป็นข่าวไปทั่วโลกเมื่อเร็วๆ นี้ คือกรณีของโรงแรมชั้นนำในยุโรปถูกเจาะระบบ Keycard ทำให้ลูกค้าไม่สามารถเข้าห้องพักได้ ทำให้เราต้องตระหนักถึงรูปแบบและความสามารถของตัว Ransomware ที่ก้าวล่วงไปถึงการเจาะเข้าไปยังอุปกรณ์ต่างๆ ที่มีการเชื่อมต่อเครือข่าย Internet หรืออุปกรณ์ที่เข้าข่ายเทคโนโลยี Internet of thing นั่นเอง

ปี 2017 จะเป็นปีแห่งการรีดไถเงินจากทุกช่องทางด้วยการโจมตีของ Ransomware แบบลูกโซ่ ที่ใช้การผสมผสานวิธีการแพร่เชื้อที่หลากลาย ร่วมกับเทคนิคการเข้ารหัสที่แก้ไขได้ยากมาก และขับเคลื่อนด้วยการสร้างความหวาดกลัวเป็นหลัก ที่เปลี่ยนหน้าต่างข้อความรีดไถแบบเดิมๆ ให้ดูเหมือนมาจากหน่วยงานที่น่าเชื่อถือมากยิ่งขึ้น นอกจากนี้ยังเพิ่มช่องทางทำเงินด้วยการบริการแรนซัมแวร์แบบคลาวด์ หรือ Ransomware-as-a-Service ที่เปิดให้อาชญากรที่อาจไม่รู้เรื่องเกี่ยวกับเทคนิคมาเช่าโครงสร้างพื้นฐานที่วางไว้เป็นอย่างดีแล้ว สำหรับนำไปใช้เพื่อโจมตีผู้อื่นได้ และในปี 2016 ที่ผ่านมานั้น

เหล่าอาชญากรไซเบอร์ได้มีการแบ่งปัน Ransomware code ออกสู่สาธารณะในลักษณะของ Open Source เพื่อเปิดให้ Hacker สามารถนำไปดัดแปลงเป็น Version ของตนเองได้ ทั้งหมดนี้ทำให้จำนวน Ransomware มีอัตราเพิ่มสูงขึ้นอย่างรวดเร็วมากในช่วงที่ผ่านมา โดยอัตราการเติบโตของปี 2017 จะอยู่ที่ 25% และ Ransomware จะกลายเป็นสาเหตุของเหตุการณ์ข้อมูลรั่วไหลมากขึ้น อาชญากรไซเบอร์จะเริ่มจากการขโมยข้อมูลที่เป็นความลับเพื่อนำไปจำหน่ายในตลาดมืด จากนั้นจึงติดตั้ง Ransomware เพื่อยึดเอา Server ที่มีข้อมูลดังกล่าวไว้เป็นประกันยกระดับการทำกำไรให้ได้มากที่สุด

นอกจากนี้ Ransomware บนอุปกรณ์พกพาก็มีแนวโน้มการเติบโตในลักษณะเดียวกัน ทำให้ผู้ใช้อุปกรณ์พกพากลายเป็นเหยื่อของ Ransomware เช่นกัน รวมถึงจะลุกลามไปถึงอุปกรณ์ประมวลผลอื่นๆ เช่น ระบบ Cashier หรือ Point of sale หรือแม้แต่ตู้ ATM ที่อาจตกเป็นเหยื่อรีดค่าไถ่ได้เช่นกัน

องค์การส่วนใหญ่เริ่มตระหนักกันแล้วว่า การโดนโจมตีจาก Ransomware ทำให้เกิดความเสียหายมูลค่ามหาศาล โดยเฉพาะการกระทบความต่อเนื่องทางธุรกิจ Ransomware ที่โจมตีสภาพแวดล้อมการทำงานในระบบอุตสาหกรรม และการโจมตีระบบ Internet of thing อาจทำให้เกิดความเสียหายอย่างมาก ขนาดที่เหล่าอาชญากรไซเบอร์น่าจะพุ่งเป้าเพื่อรีดค่าไถ่แลกกับการนำสายการผลิตทั้งหมดกลับมาออนไลน์อีกครั้ง หรือการนำระบบควบคุมอุณหภูมิที่วิกฤติกลับมาสู่ภาวะที่ปลอดภัยอีกครั้งหนึ่ง เป็นต้น (รู้สึกจะเหมือนในหนังเข้าไปทุกที)

แม้ว่าองค์การต่างๆ ไม่มีแนวทางหรือวิธีการตายตัวที่จะสามารถปกป้องเป้าหมายเสี่ยงจากการโจมตีของ Ransomware ได้อย่าง 100% แต่ก็ควรป้องกันตั้งแต่แหล่งกำเนิดข้อมูลสำคัญด้วยการใช้ Solution ความปลอดภัยกับทุกจุดเสี่ยง ซึ่งเทคโนโลยีการเรียนรู้ด้วยตนเองหรือ Machine-Learning อาจจะกลายเป็นอาวุธสำคัญที่ช่วยสนับสนุนระบบความปลอดภัยให้สามารถตรวจจับ Ransomware ใหม่ๆ หรือที่มีคุณลักษณะจำเพาะได้

2) อุปกรณ์ Internet of thing จะมีบทบาทสำคัญในฐานะส่วนหนึ่งของการโจมตีแบบ DDoS โดยเฉพาะอุปกรณ์ Internet of thing ในวงการอุตสาหกรรม

Webcam จำนวนหลายพันตัวที่ผู้คนไม่เคยนึกถึงเรื่องของระบบความปลอดภัยมาก่อนนั้น ถูกนำมาเป็นกองกำลังสำคัญในการโจมตี Mirai DDoS ที่ยิงเว็บไซต์จำนวนมากร่วงไปแล้ว อุปกรณ์ที่เชื่อมต่อ Internet ทั้งหลาย อาจกลายเป็นอาวุธทำลายล้างที่ทำตามคำสั่งของอาชญากรไซเบอร์ได้ ในปี 2017 จะพบการโจมตีทางไซเบอร์ที่ใช้อุปกรณ์ Internet of Things (Internet of thing) และโครงสร้างพื้นฐานที่เกี่ยวข้องมาเป็นเครื่องมือมากขึ้น ไม่ว่าจะเป็นการเข้าควบคุม Internet router ตามบ้าน และสำนักงานจำนวนมากเพื่อนำมาใช้โจมตีแบบ DDoS หรือการเข้าควบคุมรถยนต์ที่เชื่อมต่อ internet เพื่อนำไปทำอาชญากรรมบางอย่าง เป็นต้น

ข้อเท็จจริงในปัจจุบันก็คือ ผู้จำหน่ายผลิตภัณฑ์ Internet of thing หรืออุปกรณ์เชื่อมต่อส่วนใหญ่ไม่สามารถที่จะออกมาแก้ปัญหาการโจมตีเหล่านี้ได้อย่างทันท่วงที ซึ่งเมื่อการโจมตีของ Mirai botnet ที่อาศัย Webcam เป็นอาวุธในการโจมตีนั้นเกิดขึ้น ผู้จำหน่ายได้มีการเรียก Webcam คืนเพื่อตรวจสอบทันที แต่ก็ไม่ได้ตรวจสอบโค้ดโปรแกรมบนอุปกรณ์เชื่อมต่อตัวอื่นที่ไม่ได้รับผลกระทบในการโจมตีครั้งนั้นไปด้วยพร้อมกัน นั่นหมายความว่า แม้แต่ปัจจุบันก็ยังมีโอกาสที่อาชญากรจะใช้อุปกรณ์ที่เหลือนี้มาเป็นอาวุธโจมตีได้อยู่ Mirai botnet นั้น ไม่จำเป็นต้องอาศัย Domain Name System (DNS) server ในการโจมตีเป้าหมาย แต่ก็สามารถส่งข้อมูลระดมยิงจนระบบปลายทางล่มได้เช่นกัน นั่นคือ Internet of thing botnet ที่มีจำนวนมหาศาลซึ่งสามารถยกระดับความรุนแรงให้การโจมตีแบบ DDoS สามารถสร้างความเสียหายได้อย่างมากมายหลายเท่าตัว

เทคโนโลยี Internet of thing ได้มอบประสิทธิภาพการทำงานที่สูงขึ้นแก่ภาคอุตสาหกรรม โดยเฉพาะด้านงานผลิต และพลังงาน ซึ่งหากนำไปใช้ในทางที่ไม่เหมาะสมก็กลับกลายเป็นแหล่งทรัพยากรสำคัญสำหรับอาชญากรไซเบอร์ได้เช่นกัน ทั้งนี้จากตัวเลขช่องโหว่ที่พบบนระบบควบคุมกระบวนการผลิต และรวบรวมข้อมูลหรือ SCADA มีแนวโน้มพุ่งสูงขึ้น คิดเป็น 30% ของจำนวนช่องโหว่ทั้งหมดที่สังเกตุพบโดย TippingPoint หรือช่องโหว่ขนาดเล็กที่มีนัยสำคัญ ถือว่าการเข้ามาใช้ Internet of thing สำหรับอุตสาหกรรม จะนำมาซึ่งความเสี่ยงและอันตรายที่จะกระทบกับทั้งองค์การเอง และผู้บริโภคอย่างมากในปี 2017

ภัยจากการโจมตีดังกล่าว สามารถป้องกันได้ถ้าผู้จำหน่ายอุปกรณ์ และเครื่องจักรเหล่านี้มีขั้นตอนการพัฒนาผลิตภัณฑ์ที่เน้นด้านความปลอดภัยเป็นหลัก นอกจากนี้ผู้ที่ใช้งานทั้ง Internet of thing ต่างจำเป็นต้องจำลองสถานการณ์การถูกโจมตีเพื่อค้นหาจุดบอดหรือช่องโหว่ที่ร้ายแรงอยู่เสมอ โดยเฉพาะการติดตั้งเทคโนโลยีความปลอดภัยเพื่อปกป้องเครือข่ายของโรงงานถือเป็นความจำเป็นอย่างยิ่ง

อ่านต่อฉบับหน้า