ผ่านมาเกือบครึ่งปีแล้ว.. ถึงเวลาที่ต้องเก็บกวาดระบบครั้งใหญ่แล้วหรือยัง

ผ่านมาเกือบครึ่งปีแล้ว.. ถึงเวลาที่ต้องเก็บกวาดระบบครั้งใหญ่แล้วหรือยัง?
คุณวัตสัน ถิรภัทรพงศ์ กรรมการผู้จัดการประจำประเทศไทยและภูมิภาคอินโดจีนของซิสโก้

รายงานด้านความปลอดภัยประจำปีของซิสโก้ (Cisco Annual Security Report – CASR) เน้นย้ำถึงภัยคุกคามที่สำคัญที่สุดต่อธุรกิจ นั่นคือ “การขาดวินัยในการติดตั้งแพตช์” เพื่อแก้ไขช่องโหว่ของระบบ ที่จริงแล้วมีช่องโหว่มากมายในผลิตภัณฑ์และซอฟต์แวร์ต่างๆ ที่ยังไม่ได้รับการแก้ไขโดยทีมงานฝ่ายไอทีภายในองค์กร ทั้งๆ ที่ช่องโหว่เหล่านี้เป็นที่รู้จักอย่างดี ในโลกของธุรกิจ เราจึงขอเชิญชวนให้ท่านหันมาเก็บกวาดระบบไอที เน็ตเวิร์ค และเซิร์ฟเวอร์ของท่านด้วยเช่นกัน

ตัวอย่างเช่น Heartbleed จุดอ่อนด้านการรักษาความปลอดภัย ถูกสร้างขึ้นเพื่อเจาะระบบ OpenSSL โดยมีการรายงานข่าวเกี่ยวกับจุดอ่อนที่ว่านี้อย่างแพร่หลายทั่วโลก แต่ 56 เปอร์เซ็นต์ของ OpenSSL ทุกเวอร์ชั่นมีอายุมากกว่า 56 เดือน จึงเสี่ยงต่อปัญหาช่องโหว่ดังกล่าว จะเห็นว่าช่องโหว่ที่มีการออกข่าวกันอย่างครึกโครมเช่นนี้ยังถูกละเลย แล้วจุดอ่อนหรือภัยคุกคามที่เป็นที่รู้จักน้อยกว่านี้จะเป็นเช่นไร

นอกจากนี้ รายงาน Cisco ASR ยังเน้นย้ำว่า เมื่อปีที่แล้ว 1 เปอร์เซ็นต์ของช่องโหว่ และความเสี่ยงทั่วไปที่เป็นปัญหาเร่งด่วน ถูกใช้ในการเจาะระบบอย่างจริงจัง นั่นหมายความว่าองค์กรต่างๆ ควรจะให้ความสำคัญกับช่องโหว่ 1 เปอร์เซ็นต์ และรีบแก้ไขอย่างเร่งด่วน แต่น่าเสียดายที่ความเป็นจริงแล้ว ปัญหานี้กลับถูกละเลยเพิกเฉย

ที่จริงแล้ว แพตช์สำหรับแก้ไขจุดอ่อนส่วนใหญ่มีอยู่แล้ว ดังนั้นจึงไม่ใช่เรื่องยากที่จะป้องกันภัยคุกคามที่เป็นที่รู้จัก ทั้งนี้ ถ้าหากเราปรับปรุงประสิทธิภาพในการแก้ไขจุดอ่อน.. 99.9% ของภัยคุกคามที่เป็นอันตรายต่อเครือข่ายทั่วโลกก็จะสูญหายไป ขณะที่สื่อมวลชนให้ความสนใจกับช่องโหว่ใหม่ๆ ที่ไม่เคยตรวจพบ (หรือภัยคุกคามที่ไม่รู้จักมาก่อน) แต่ที่จริงแล้ว ช่องโหว่ประเภทนี้มีน้อยมาก และกลุ่มอาชญากรไซเบอร์ก็รู้ดีว่าไม่มีความจำเป็นใดๆ ที่จะต้องค้นหาช่องโหว่ใหม่ๆ เพราะช่องโหว่เดิมๆ ที่มีอยู่ก็ยังคงใช้การได้ดีอยู่แล้ว

ก็เหมือนกับการที่เราสร้างรั้วล้อมฝูงแกะ แต่กลับเปิดประตูรั้วทิ้งไว้ ขณะที่หมาป่ากำลังเดินด้อมๆ มองๆ อยู่นอกรั้ว หมาป่าไม่จำเป็นต้องเสียเวลาปีนข้ามรั้วหรือมองหาช่องโหว่ที่รั้ว แต่มันสามารถเดินผ่านประตูรั้วเข้าไปอย่างง่ายดาย

การใช้วิธีอัพเดตอัตโนมัติมีเพิ่มมากขึ้นอาจเป็นหนทางหนึ่งที่จะช่วยแก้ไขปัญหาซอฟต์แวร์ล้าสมัย ทีมงานฝ่ายวิจัย

ด้านความปลอดภัยของซิสโก้ที่จัดทำรายงาน CASR ได้ตรวจสอบข้อมูลจากอุปกรณ์ที่เชื่อมต่อออนไลน์และใช้เบราว์เซอร์ Chrome และ Internet Explorer ข้อมูลดังกล่าวแสดงให้เห็นว่า 64 เปอร์เซ็นต์ของคำร้องขอจาก Chrome มาจากเบราว์เซอร์รุ่นล่าสุด ส่วน Internet Explorer พบว่ามีเพียง 10 เปอร์เซ็นต์เท่านั้นที่มาจากเบราว์เซอร์รุ่นล่าสุด

ดูเหมือนว่าระบบอัพเดตอัตโนมัติของ Chrome อาจมีประสิทธิภาพมากกว่า จึงช่วยให้ผู้ใช้จำนวนมากมีซอฟต์แวร์รุ่นล่าสุดไว้ใช้งาน ดังนั้นจึงยกระดับการปกป้องได้เหนือกว่า

รายงาน CASR ระบุอย่างชัดเจนว่า “ซอฟต์แวร์ที่ติดตั้งอัพเดตโดยอัตโนมัติมีข้อได้เปรียบในการสร้างกรอบโครงสร้างด้านความปลอดภัยที่ดีกว่า” เพื่อแก้ไขปัญหาความเสี่ยงที่เกิดจากกระบวนการอัพเดตด้วยตนเอง อาจถึงเวลาแล้วที่องค์กรต่างๆ จะต้องยอมรับความเสี่ยงเรื่องระบบหยุดทำงานชั่วคราวและความเข้ากันไม่ได้ ซึ่งเป็นผลมาจากการอัพเดตแบบอัตโนมัติ

“กระบวนการจัดการแพตช์แบบครบวงจร” ควรจะเป็นองค์ประกอบสำคัญในการปกป้องข้อมูล พร้อมใช้งานอยู่เสมอ และป้องกันปัญหาข้อมูลรั่วไหลบนอุปกรณ์ประมวลผล รวมถึงข้อมูลที่ถูกจัดเก็บและถ่ายโอนบนอุปกรณ์ดังกล่าว การจัดการแพตช์ไม่ใช่งานง่าย เพราะองค์กรส่วนใหญ่มีแพลตฟอร์มและอุปกรณ์ที่หลากหลาย ตั้งแต่แบบติดตั้งถาวรไปจนถึงแบบพกพา ทั้งยังมีปัญหาท้าทายอื่นๆ ที่อาจทำให้การติดตั้งแพตช์บนอุปกรณ์เหล่านี้กลายเป็นเรื่องยากมาก

แนวทางที่ดีที่สุดสำหรับกระบวนการจัดการแพตช์ที่ประสบผลสำเร็จก็คือ ก่อนอื่นเราจะต้องค้นหาทรัพยากรทั้งหมดที่อยู่บนเครือข่าย โดยองค์กรจะต้องสร้างและดูแลรักษารายการอุปกรณ์ประมวลผลทั้งหมดสภาพ และจะต้องอัพเดตให้ทันสมัยอยู่เสมอ รายการดังกล่าวจะช่วยให้องค์กรสามารถระบุได้ว่ามีระบบปฏิบัติการ ซอฟต์แวร์ และแพตช์ใดบ้างติดตั้งไว้บนอุปกรณ์ในเครือข่าย ซึ่งจะช่วยให้สามารถพัฒนานโยบายพื้นฐานได้อย่างเหมาะสม ขั้นตอนถัดไปในกระบวนการจัดการแพตช์ก็คือ การระบุว่ามีอุปกรณ์ที่ยังไม่ได้ติดตั้งแพตช์ในสภาพแวดล้อมขององค์กรหรือไม่ และการวิเคราะห์ความเสี่ยงสำหรับแพตช์ที่ขาดหายไป ทั้งนี้มีเครื่องมือมากมายที่วางจำหน่ายในตลาด ซึ่งสามารถช่วยในการสแกนสภาพแวดล้อม เพื่อดำเนินการวิเคราะห์โครงสร้างพื้นฐานอย่างละเอียด

หลังจากที่ดำเนินการตามขั้นตอนทั้งหมดนี้แล้ว เราควรจะทำการแก้ไขเยียวยา เพื่อให้ระบบทั้งหมดมีความทันสมัยด้วยการติดตั้งแพตช์รุ่นใหม่ล่าสุด แต่ก่อนหน้านั้น เราจะต้องสร้างกระบวนการจัดการการเปลี่ยนแปลง เพื่อช่วยในการควบคุมเวอร์ชั่นและการจัดทำเอกสาร หลังจากที่การแก้ไขเสร็จสมบูรณ์ และระบบทั้งหมดใช้ซอฟต์แวร์รุ่นล่าสุดแล้ว องค์กรก็จะมีพื้นฐานสำหรับการเริ่มต้นวงจรการจัดการแพตช์ “นโยบายพื้นฐานพร้อมด้วยแพตช์รุ่นล่าสุด” คือจุดเริ่มต้นที่ดีสำหรับการดำเนินกระบวนการจัดการแพตช์อย่างต่อเนื่อง ราบรื่น และมีประสิทธิภาพ

ตอนนี้ก็ถึงเวลาแล้วที่องค์กรของท่านจะเริ่มต้นเก็บกวาดทำความสะอาดระบบไอที เครือข่าย และเซิร์ฟเวอร์ของท่าน พร้อมทั้งตรวจสอบสถานะการติดตั้งแพตช์ และจัดทำรายการทรัพยากรและอุปกรณ์ต่างๆ ที่ท่านมีอยู่ เพื่อให้

ธุรกิจดำเนินไปอย่างราบรื่น และต่อเนื่องตลอดไป