เดลินิวส์

ฉบับที่ 24,960 วันอังคารที่ 13 กุมภาพันธ์ พ.ศ. 2561 หน้า 23

แนะ 3 มาตรการป้องกันภัยในไอโอที

ฟอร์ติเน็ต เผยอุปกรณ์ไอโอที 70% เสี่ยงถูกโจมตีโดยภัยไซเบอร์ พร้อมแนะ 3 มาตรการป้องกันภัยในไอโอที

"เกวิน เชา" นักกลยุทธ์ด้านความปลอดภัยและเครือข่ายแห่งฟอร์ติเน็ต กล่าวว่า อุปกรณ์ไอโอทีจำนวนมาก ไม่เคยถูกออกแบบมาโดยคำนึงถึงความปลอดภัยและเมื่อมีการใช้อุปกรณ์ไอโอทีนับพันล้านชิ้น จึงเกิดผลกระทบด้านความปลอดภัยของสังคมที่มีการเชื่อมต่อกันมากขึ้นเป็นทวีคูณ และเริ่มจะขาดการควบคุม ซึ่งอุปกรณ์เหล่านี้มักเป็นอุปกรณ์ประเภท "Headless" ที่มีศักยภาพในการทำงานและความสามารถในการประมวลผลที่ต่ำ ไม่สามารถติดตั้งโปรแกรมรักษาความปลอดภัย อัพเดทหรือแก้ไขช่องโหว่ได้ ซึ่งมีการวิจัยเมื่อเร็ว ๆ นี้ พบว่าอุปกรณ์ไอโอทีประมาณ 70% ของจำนวนทั้งหมดมีความเสี่ยงในการถูกโจมตีโดยภัยไซเบอร์

ทั้งนี้การรักษาความปลอดภัยให้ไอโอทีต้องมีความเข้าใจในเชิงลึกว่าอุปกรณ์ใดบ้างที่สามารถเชื่อถือได้และจัดการได้ ฟอร์ติเน็ต ได้แนะนำแนวทางในการพัฒนาและปรับใช้ "ซีเคียวริตี้แฟบริค" สถาปัตยกรรมความปลอดภัยแบบไซเบอร์แบบอัจฉริยะระดับโลก โดยมี 3 ขั้นตอนสำคัญ คือ 1. เรียนรู้ (Learn) องค์กรต้องเข้าใจถึงขีดความสามารถและข้อจำกัดของแต่ละอุปกรณ์และระบบนิเวศของเครือข่ายที่พวกเขาผูกไว้ด้วยกัน โซลูชั่นด้านความปลอดภัยที่ใช้ต้องมีศักยภาพในการมองเห็นที่ครอบคลุมในการตรวจสอบความถูกต้องของเครือข่ายและแยกแยะอุปกรณ์ไอโอทีทั้งหมดแบบเรียลไทม์

2. จัดกลุ่ม (Segment) ซึ่งมีการกำหนดมาตรการป้องกันโดยแบ่งกลุ่มอุปกรณ์และจัดสร้างโซลูชั่นการสื่อสารสำหรับกลุ่มต่าง ๆ นั้นแบบอัจฉริยะและอัตโนมัติ เครือข่ายสามารถให้สิทธิและบังคับใช้สิทธิพื้นฐานสำหรับแต่ละโปรไฟล์ความเสี่ยงของอุปกรณ์ไอโอทีโดยอัตโนมัติ และ 3. การปกป้อง (Protect) ซึ่งองค์กรสามารถตรวจสอบและบังคับใช้นโยบายอุปกรณ์ได้หลายระดับ โดยอิงจากกิจกรรมทุกกิจกรรมที่เกิดในเครือข่ายขององค์กร

อย่างไรก็ตาม การแบ่งส่วนอย่างเดียวอาจยังมีปัญหาการมองเห็นที่เป็นส่วน ๆ อยู่ ดังนั้นองค์กรจึงควรเชื่อมโยงแต่ละกลุ่มและกลุ่มเครือข่ายเข้าด้วยกันด้วยกรอบความปลอดภัยแบบองค์รวม ที่เรียกว่า "ซีเคียวริตี้แฟบริค" ซึ่งการเชื่อมโยงแบบบูรณาการนี้จะช่วยเชื่อมโยงข้อมูลด้านภัยคุกคาม (Threat intelligence) ระหว่างเครือข่ายต่าง ๆ และอุปกรณ์รักษาความปลอดภัยต่าง ๆ และส่วนต่าง ๆ อีกทั้งยังบังคับใช้ฟังก์ชันการรักษาความปลอดภัยขั้นสูงให้กับอุปกรณ์ไอโอที และให้กับทราฟฟิคที่อยู่ทุกแห่งทั่วเครือข่ายโดยอัตโนมัติ.