BangkokBizNews.com
กรุงเทพธุรกิจ

ปีที่ 30 ฉบับ 10315 วันจันทร์ที่ 19 ธันวาคม พ.ศ. 2559 หน้า 27

ThinkSecure

นักรบ เนียมมามธรรม
กรรมการผู้จัดการ
บริษัท เอ็นฟอร์ซ ซีเคียว จำกัด

'ไอโอที แบล็กดอร์' มาแล้ว

สองสัปดาห์ที่ผ่านมาได้เห็นมัลแวร์ที่ชื่อว่า "มิราย" (Mirai) สร้างความปั่นป่วนด้วยการสร้าง ดีดอส หรือข้อมูลมหาศาลเข้าสู่โจมเป้าหมาย อย่างไรก็ตาม จะเห็นว่าตอนนี้ระบบ ซิเคียวริตี้เริ่มใกล้ตัวมากขึ้น

สมัยก่อน ระบบซิเคียวริตี้แบบกายภาพ และ ไอที เคียวริตี้ แยกออกจากกัน แต่ปัจจุบันทั้งสองรวมเป็นหนึ่ง หรือเรียกว่าการรักษาความปลอดภัยระบบไอทีแบบองค์รวม เดือนต.ค.ที่ผ่านมา บริษัทโซนี่ ออกประกาศว่ากล้องโซนี่ อย่าง 'ไอพี คาเมร่า' จำนวนกว่า 80 รุ่น ถูกพบเจอแบล็ก ดอร์ แอคเคาท์ (Backdoor accounts) หรือการแอบสร้างชื่อผู้ใช้งานเพื่อเข้าสู่ระบบ โดยแบล็กดอร์ แอคเคาท์ที่ถูกพบมีสองแบบ คือ

1.การฝังสิทธิ์การเข้าระบบ หรือเรียกว่า ฮาร์ด โค้ด ครีเดนเชียลส์ ไปยังเว็บอินเตอร์เฟซที่อยู่ในกล้องไอพี คาเมร่าทั้ง 80 รุ่น หลังแฮกเกอร์เข้าควบคุมได้แล้ว จะสามารถส่งคำร้องขอไปเปิดใช้งาน หรือสร้าง เทลเน็ต เซอร์วิส หรือชุดคำสั่งต่างๆ บนกล้องได้ และสามารถส่งข้อมูลมหาศาล เช่น การปิง (Ping)เข้าไปได้

2.การฝังพาสเวิร์ด ที่สามารถควบคุมกล้องผ่านโปรโตคอล ที่เรียกว่าเทลเน็ต ได้เต็มรูปแบบ ไม่นานในบริษัทโซนี่ได้ปล่อยเฟิร์มแวร์ เพื่อแก้ปัญหาเมื่อปลายเดือนพ.ย.โดยบริษัทกำชับให้ลูกค้าอัพเดทเฟิร์มแวร์ใหม่โดยเร็วที่สุด เพราะระบบ ไอพี คาเมร่า เป็นเป้าโจมตีของแฮกเกอร์

ทั้งนี้ แบล็กดอร์ แอคเคาท์ ที่เกิดขึ้นมาจากช่วงทดสอบระบบของพนักงานโซนี่เอง ไม่ใช่จากบุคคลที่สามที่ไม่ได้รับอนุญาตเช่นกรณีอื่นๆ กล้องที่ได้รับผลกระทบ คือ กล้องที่ต่อบนโลคอลเน็ตเวิร์ค หรืออินเทอร์เน็ตที่มีเวบ อินเตอร์เฟซ โดยมีกล้องราว4000 ตัวเชื่อมต่ออินเทอร์เน็ต จำนวนที่มากมายนี้กลายเป็นเป้าล่อเหล่าแฮกเกอร์

หลายองค์กรยังขาดการตรวจสอบระบบไอโอทีต่างๆ เช่น การอัพเดท แพทช์ (Patch) หรือ เฟิร์มแวร์ไม่ทั่วถึง การประเมินความเสี่ยงหรือประเมินช่องโหว่ จำเป็นต้องประเมินแสมออย่างน้อยปีละ 2 ครั้งต่อ 1 ระบบ ไม่ใช่แค่เซิร์ฟเวอร์, เน็ตเวิร์ค , ดาต้า เซ็นเตอร์, ไฟร์วอล หรือระบบปฏิบัติการต่างๆ แต่ต้องรวมถึงระบบซิเคียวริตี้แบบกายภาพ เพราะ เหล่าอุปกรณ์ไอโอทีมักตกเป็นเป้าหมายโจมตีของภัยร้ายต่างๆ

การโจมตีของภัยร้ายต่างๆ ใกล้ตัวมากขึ้น อนาคต มือถือ จะกลายเป็นเป้าหมาย ของแฮกเกอร์ เพราะ 90% ของมือถือเชื่อมต่ออินเทอร์เน็ตมากกว่าอุปกรณ์ ไอโอทีอื่นๆ จึงจำเป็นต้องตรวจสอบ และประเมินความเสี่ยงในทุกระบบที่เชื่อมต่อกับอินเทอร์เน็ตขององค์กรอยู่เสมอ