@Post

ฉบับที่ 06/2561 ประจำเดือน มิถุนายน พ.ศ. 2561 Free Copy

รู้เท่าทัน Internet of Things : IoT กับภัยคุกคามไซเบอร์

https://www.enterpriseitpro.net/

เนื่องจากภัยคุกคามบนอินเทอร์เน็ตในปัจจุบันนั้นถูกพบเห็นเป็นข่าวบ่อยขึ้นเรื่อย ๆ ดังนั้นอุปกรณ์ที่มีการเชื่อมต่ออินเทอร์เน็ต (IoT) จึงมีความน่าจะเป็นที่จะถูกแฮกโดยผู้ไม่หวังดีได้มากขึ้นตามไปด้วย ดังตัวอย่างเช่น การสั่งเปิด-ปิด อุปกรณ์เครื่องใช้ไฟฟ้า รถยนต์ โทรศัพท์มือถือ เครื่องมือสื่อสาร เครื่องใช้สำนักงาน เครื่องมือทางการเกษตร เครื่องจักรในโรงงานอุตสาหกรรม อาคาร บ้านเรือน เครื่องใช้ในชีวิตประจำวันต่าง ๆ ผ่านเครือข่ายอินเทอร์เน็ต เป็นต้น โดยเทคโนโลยีนี้จะเป็นทั้งประโยชน์อย่างมหาศาลและความเสี่ยงไปพร้อม ๆ กัน เพราะหากระบบรักษาความปลอดภัยของอุปกรณ์และเครือข่ายอินเทอร์เน็ตไม่ดีพอจะทำให้ผู้ไม่ประสงค์ดีเข้ามากระทำการที่ไม่พึงประสงค์ต่ออุปกรณ์ ข้อมูลสารสนเทศ หรือความเป็นส่วนตัวของบุคคลได้ ทำให้เห็นได้ว่า IoT นั้นนอกจากจะนำมาซึ่งความสะดวกสบายในชีวิตประจำวันของท่านแล้วยังนำมาซึ่งภัยคุกคามด้วยเช่นกัน

ขอบคุณภาพจาก : www.inman.com/2014/12/12/10-smart-home-products-to-keep-an-eye-on

อุปกรณ์ IoT ที่มีการเชื่อมต่ออินเทอร์เน็ตจะต้องพร้อมที่จะรับกับความเสี่ยงที่จะโดนแฮกข้อมูล หรือครอบครองโดยผู้ไม่หวังดี เพราะไม่ว่าคุณจะมีการป้องกันด้วยอุปกรณ์ security ที่ดีเลิศที่สุดในโลก หรือคุณจะมีการเข้ารหัสข้อมูลหรือมีการป้องกันใด ๆ ก็ตามที่เรียกได้ว่าดีที่สุด แข็งแรงที่สุด แต่ทันทีที่มันมีการเชื่อมต่อกับอินเทอร์เน็ตความเสี่ยงบังเกิดขึ้นทันที ซึ่งอุปกรณ์ IoT ก็ไม่สามารถปฏิเสธความเสี่ยงนี้ได้ แต่สิ่งที่น่ากลัวกว่าก็คืออุปกรณ์ IoT ในปัจจุบันนั้นก็เหมือนกับอุปกรณ์คอมพิวเตอร์หรือสมาร์ทโฟนรุ่นแรก ๆ ที่เริ่มมีการเชื่อมต่ออินเทอร์เน็ตที่มีช่องโหว่มากมายให้ผู้บุกรุกสามารถเลือกสรรใช้ในการโจมตีอย่างสบาย ๆ ดังนั้นการตั้งอยู่ในความไม่ประมาทด้วยการพิจารณาอุปกรณ์ IoT ที่ท่านเลือกใช้ว่ามีมาตรการอย่างไรในการรักษาความปลอดภัยให้กับท่านได้ก่อนที่จะซื้อมาใช้งานก็จะช่วยให้ท่านมีความเสี่ยงลดลง

โดยที่ในอดีตนั้นเราจะคิดว่าแฮกเกอร์นั้นมุ่งหวังที่จะโจมตีเฉพาะองค์กร เพราะผลลัพธ์ที่ได้นั้นคุ้มค่าการลงทุนลงแรงมากกว่าการโจมตีไปที่ตัวบุคคล (ยกเว้นบุคคลสำคัญ) แต่ในปัจจุบันนั้นแฮกเกอร์เริ่มมุ่งเป้าไปที่อุปกรณ์ IoT ที่มีความง่ายในการโจมตีมากกว่า และผู้ใช้ส่วนใหญ่ยังขาดความระมัดระวังตัวด้วย ให้ลองคิดง่าย ๆ ว่าถ้าคุณมีสมาร์ทโฟนที่เชื่อมต่อกับกล้องวงจรปิดและระบบป้องกันขโมยผ่านระบบคลาวด์ หากมีใครขโมยสมาร์ทโฟนของคุณไปก็สามารถที่จะควบคุมทุกอย่างในบ้านของคุณได้อย่างสบาย หรือแม้แต่ถ้าผู้บุกรุกสามารถแฮกระบบคลาวด์ได้ก็สามารถควบคุมทุกอย่างในบ้านของคุณได้เช่นกัน

วิธีการแก้ไขและป้องกันความเสี่ยง

1. การออกแบบโดยคำนึงถึงความปลอดภัย

ผู้ผลิตก็จะต้องคำนึงถึงความเสี่ยงที่มีโอกาสจะเกิดขึ้นกับผลิตภัณฑ์ที่ต้องการจะผลิตตั้งแต่ตอนออกแบบทดสอบว่าการป้องกันที่ออกแบบไว้นั้นเพียงพอจะป้องกันความเสี่ยงที่ได้คิดเอาไว้หรือไม่ ก่อนที่จะนำออกมาจำหน่ายและควรตั้งค่า default ของผลิตภัณฑ์ให้เป็นค่าที่ปลอดภัยเสมอ

2. การใช้งานอย่างปลอดภัย

เมื่อผู้ขายทำให้ผลิตภัณฑ์มีความปลอดภัยแล้ว คนใช้ก็ควรจะทำความเข้าใจกับมาตรฐานความปลอดภัย (Security standard) ที่ผู้ผลิตแนะนำและใช้งานผลิตภัณฑ์นั้นอย่างปลอดภัย เช่น การเปลี่ยน default password, เลือกเข้ารหัสข้อมูลที่สำคัญและอัปเดตแพทช์อยู่ตลอด

3. การจัดการเมื่อเกิดเหตุผิดปกติ

ในฐานะผู้ใช้ไม่ว่าจะเพื่อการใช้งานส่วนตัวหรือใช้สำหรับองค์กร เมื่อเกิดเหตุผิดปกติขึ้นนั้น ผู้ใช้จะเป็นคนแรก ๆ ที่รับรู้ถึงความผิดปกติที่เกิดขึ้น ดังนั้นผู้ใช้ควรจะทราบว่าเมื่อเกิดเหตุผิดปกติขึ้นจะต้องแจ้งเหตุกับใครหรือต้องทำอย่างไรบ้าง (รวมถึงวิธีการติดต่อกับผู้ผลิต)

4. การเข้าใจสิทธิของผู้ใช้

ผู้ผลิตส่วนใหญ่ชอบให้ผู้ใช้ติ๊ก Agreed ให้ผู้ผลิตสามารถเข้าถึงข้อมูลของผู้ใช้ก่อนจึงจะสามารถใช้งานซอฟต์แวร์หรืออุปกรณ์ IoT ได้ หากบรรดาข้อมูลที่เก็บจากอุปกรณ์อัจฉริยะเหล่านี้อยู่ในมือของคนอื่น แล้วคุณจะแน่ใจได้อย่างไรว่าตัวคุณนั้นปลอดภัย เช่น ถ้าคนร้ายสามารถแฮกบริษัทผู้ผลิตอุปกรณ์ IoT ที่คุณใช้งานอยู่จนสามารถรู้ที่อยู่ของคุณแล้วตามมาทำร้ายคุณ เป็นต้น

ที่มา : - นิตยสาร Enterprise ITPro
- https://www.enterpriseitpro.net/%E0%B8%9A%E0%B8%97%E0%B8%84%E0%B8%A7%E0%B8%B2%E0%B8%A1-internet-of-threats-%E0%B9%80%E0%B8%A1%E0%B8%B7%E0%B9%88%E0%B8%AD-iot-%E0%B9%80%E0%B8%95%E0%B8%B4%E0%B8%9A%E0%B9%82%E0%B8%95%E0%B8%84/