ฟอร์ซพ้อยต์ เผยแนวภัยคุกคามความปลอดภัย ปี 2018 ทำนายจุดเริ่มต้น “สงครามชิงความเป็นส่วนตัว”

ความเสี่ยงมาจาก ผู้รวบรวมข้อมูล ระบบเงินดิจิทัล และมัลแวร์เรียกค่าไถ่
ทุกอย่างจะผ่านไปได้ หากมุ่งเน้นรักษาความปลอดภัยโดยใส่ใจที่พฤติกรรมเป็นหลัก

ฟอร์ซพ้อยต์ Forcepoint ผู้นำระดับโลกด้านการรักษาความปลอดภัยไซเบอร์ เผย รายงานเกี่ยวกับการคาดการณ์ความปลอดภัยสำหรับปี 2018 (2018 Security Predictions Report) พร้อมแนวทางจากผู้เชี่ยวชาญด้านการรักษาความปลอดภัย ในการรับมือกับภัยคุกคามที่องค์กรธุรกิจต้องเผชิญในอีกไม่กี่เดือนที่จะถึงนี้
สิ่งที่เพิ่มขึ้นมาจากสภาพแวดล้อมที่มีการเปลี่ยนแปลงอยู่ตลอดเวลา และเป็นสิ่งที่มืออาชีพด้านการรักษาความปลอดภัยต้องเผชิญ นั่นคือ พายุลูกใหญ่ที่พัดนำไปสู่การโต้แย้งด้านความเป็นส่วนตัว นี่คือ เมกะเทรนด์ ที่จะเปลี่ยนแปลงภาพรวมในเรื่องความเป็นส่วนตัว และส่งผลถึงการรวบรวมและบริหารจัดการข้อมูลภายในองค์กร ฟอร์ซพ้อยต์ เชื่อว่าที่ผ่านมาอุตสาหกรรมด้านการรักษาความปลอดภัย กำลังมุ่งเน้นผิดประเด็น มาตรการด้านการรักษาความปลอดภัยแบบเดิมเริ่มไม่ได้ผล หรือล้าสมัยนั่นเอง ดังนั้น แทนที่จะมุ่งเน้นที่การสร้างกำแพงป้องกันที่ใหญ่ขึ้น อุตสาหกรรมควรมีความสามารถในการมองเห็นสิ่งต่างๆ ได้ชัดเจนยิ่งขึ้น ซึ่งการเข้าใจถึงเหตุและผล วิธีการ รวมถึงช่วงเวลาที่คนมีการปฏิสัมพันธ์หรือโต้ตอบโดยใช้ข้อมูลสำคัญทางธุรกิจไม่ว่าข้อมูลนั้นจะอยู่ที่ไหนก็ตามนับเป็นเรื่องสำคัญ ทั้งนี้ ข้อมูลสำคัญยังคงถูกย้ายไปไว้บนคลาวด์อย่างต่อเนื่อง ส่วนมัลแวร์ก็ยังคงพัฒนาไปเรื่อยๆ และแม้ว่าจะมีการลงทุนด้านเทคโนโลยีเพื่อการป้องกันมากยิ่งขึ้น แต่ระบบควบคุมความปลอดภัยรูปแบบเดิมๆ ก็พิสูจน์ให้เห็นแล้วว่าไม่มีประสิทธิภาพ

“หัวใจหลักของการคาดการณ์ของเรา คือ ต้องการเข้าใจในเวลาที่คนใช้ข้อมูลสำคัญ รวมถึงทรัพย์สินทางปัญญา” ดร. ริชาร์ด ฟอร์ด หัวหน้านักวิทยาศาสตร์ ฟอร์ซพ้อยต์ กล่าว “การรักษาความปลอดภัย โดยดูเรื่องของเจตนา และพฤติกรรมการใช้งานบนไซเบอร์เป็นหลัก ก็จะช่วยให้อุตสาหกรรมมีโอกาสต่อสู้ เพื่อก้าวให้ทันต่อการเปลี่ยนแปลงที่เกิดขึ้นกับสภาพแวดล้อมภัยคุกคามอย่างหนักหน่วงได้”

“เรารู้ว่าการรั่วไหลของข้อมูลและมัลแวร์เรียกค่าไถ่ (ransomeware) ยังคงเป็นเรื่องที่ต้องเน้นป้องกันและแก้ไขอยู่ แต่ความเสี่ยงที่เกิดจากพฤติกรรมการใช้งาน ก็เป็นสิ่งที่อยู่เบื้องหลังเหตุการณ์คุกคามความปลอดภัยมากมายหลาย

เหตุการณ์” ฟอร์ด กล่าวเสริม “ไม่ควรกำหนดว่าพฤติกรรมของคนเป็นการต่อต้านการรักษาความปลอดภัย เพราะทั้งสองอย่างไม่ได้แยกจากกันอย่างชัดเจน เป็นไปได้ว่าผู้ใช้อาจทำให้ระบบของตัวเองเกิดความไม่ปลอดภัยโดยไม่ได้เจตนาในเวลาเพียงแค่นาทีเดียว และต่อมาอาจกลายเป็นแหล่งที่มาของนวัตกรรม แต่ที่เราสามารถทำได้คือการเพิ่มอำนาจให้กับผู้ใช้ ขอเพียงเข้าใจอย่างถ่องแท้ถึงวิธีการที่ผู้คนใช้ในการปฏิสัมพันธ์ หรือสื่อสารโต้ตอบด้วยข้อมูลสำคัญทางธุรกิจ”

8 แนวโน้ม สำหรับปี 2018
ในปีนี้ ฟอร์ซพ้อยต์ ได้คาดการณ์ไว้ 8 แนวโน้มด้วยกัน การคาดการณ์บางส่วนมีดังต่อไปนี้

ความเป็นส่วนตัวต่อสู้เพื่อแย่งชิงพื้นที่
ในช่วงไม่กี่ปีที่ผ่านมานี้ ผู้ใช้มีแนวความคิดเรื่องความเป็นส่วนตัวเปลี่ยนไป เส้นแบ่งระหว่าง “ความเป็นส่วนตัว” และ “ส่วนรวม” เริ่มเลือนหายไปเรื่อยๆ ทำให้เกิดความตึงเครียดในภาพรวม ระหว่างเรื่องของสิทธิส่วนบุคคลและการรักษาความปลอดภัย โดยมีปัจจัยขับเคลื่อนคือความเห็นต่างในเรื่องของการเมือง สังคม เทคโนโลยี และกฎหมาย ประเด็นเหล่านี้เมื่อรวมๆ กันแล้วอาจเป็นจุดเริ่มต้นของสิ่งที่ฟอร์ซพ้อยต์เรียกว่า “สงครามชิงความเป็นส่วนตัว” ที่เป็นความเห็นต่างระหว่างนักเทคโนโลยี และคนธรรมดาทั่วไป ทำให้เกิดความเห็นแตกแยกทั้งในหน่วยงานรัฐบาล ที่ทำงาน และที่บ้าน

การคาดการณ์ : ปี 2018 จะจุดประกายให้เกิดการโต้แย้งกันแบบแบ่งฝักแบ่งฝ่ายในวงกว้าง ไม่ใช่แค่ระหว่างรัฐบาลแต่ระหว่างประชาชนทั่วไป

ผู้รวบรวมข้อมูล – เหมืองทองที่รอการขุด
ช่องโหว่ Equifax เขย่าวงการรักษาความปลอดภัย และยังสร้างผลกระทบอยู่อย่างไม่จบไม่สิ้น ฟอร์ซพ้อยต์เชื่อว่าEquifax เป็นช่องโหว่แรก และจะเกิดอีกหลายช่องโหว่ตามมาจากการใช้แอปพลิเคชันธุรกิจซึ่งมีข้อมูลเกี่ยวกับการขาย ข้อมูลลูกค้า และลูกค้ามุ่งหวัง หรือข้อมูลในการบริหารจัดการแคมเปญการตลาดอยู่ในแอปฯ ดังกล่าว โดยผู้โจมตีจะมองหาเส้นทางที่มีระบบป้องกันน้อยที่สุด และถ้าหาจุดอ่อนในระบบที่เก็บสินทรัพย์ที่มีค่า อย่างข้อมูลส่วนตัวเจอเมื่อไหร่ ก็จะโจมตีเพื่อนำข้อมูลเหล่านี้มาแสวงประโยชน์

การคาดการณ์ – ผู้รวบรวมข้อมูล จะโดนเจาะช่องโหว่ ในปี 2018 โดยใช้วิธีโจมตีซึ่งเป็นที่รู้จักกันดี

ขาขึ้นของการแฮกเงินดิจิทัล
เนื่องจากเงินดิจิทัล หรือ Cryptocurrencies เริ่มมีบทบาทสำคัญมากขึ้น อีกทั้งยังเป็นวิธีการที่ผู้โจมตีใช้ดึงรายได้จากการก่ออาชญากรรมไซเบอร์ ทั้งนี้ฟอร์ซพ้อยต์ คาดการณ์ว่าระบบต่างๆ ที่เกี่ยวข้องกับเงินดิจิทัลจะโดนโจมตีมากขึ้น เราคาดว่าจะได้เห็นมัลแวร์จำนวนมากขึ้นพุ่งเป้าไปที่ข้อมูลส่วนตัวของผู้ใช้ ที่ใช้ยืนยันตัวตนในการแลกเปลี่ยนเงินดิจิทัล และการก่ออาชญากรรมดังกล่าวจะมุ่งความสนใจที่ช่องโหว่ในระบบที่มีการนำเทคโนโลยีสำหรับ

บล็อกเชน (blockchain) มาใช้

การคาดการณ์ – ผู้โจมตีจะมุ่งเป้าที่ช่องโหว่ในระบบที่มีการติดตั้งบล็อกเชน

การพลิกโฉมครั้งสำคัญของสรรพสิ่ง กำลังจะเกิดขึ้น
การนำอุปกรณ์ IoT มาใช้ในวงกว้าง ทั้งในสภาพแวดล้อมการใช้งานเพื่อธุรกิจและเพื่อผู้บริโภคเองก็ดี อุปกรณ์เหล่านี้ส่วนใหญ่จะเข้าถึงได้ง่าย และมักไม่ค่อยมีการตรวจสอบ จึงทำให้กลายเป็นเป้าหมายที่ดึงดูดสำหรับอาชญากรไซเบอร์ ที่อยากยึดเพื่อเรียกค่าไถ่หรือพยายามแฝงตัวอยู่ในเครือข่ายไปเรื่อยๆ ในระยะยาว แม้จะมีความเป็นไปได้ว่าอาจมีมัลแวร์เรียกค่าไถ่ (ransomware) สำหรับสรรพสิ่งที่เชื่อมต่อ (connected things) แต่ยังไม่น่าจะเกิดในปี 2018 อย่างไรก็ตาม ภัยคุกคามแบบใหม่ที่จะเกิดขึ้นในปี 2018 ก็คือการพลิกโฉมครั้งสำคัญของสรรพสิ่ง หรืออุปกรณ์ต่างๆ เนื่องจาก IoT สร้างความเป็นไปได้มากมายในการปฏิรูปการดำเนินงานและช่วยให้เข้าถึงข้อมูลสำคัญมากมายมหาศาล ซึ่งเราอาจจะได้เห็นการโจมตีในส่วนนี้ และอาจเห็นการผสมผสานวิธีการโจมตีแบบแทรกกลางการสื่อสาร (MITM – Man-in-the-middle) อีกด้วย

การคาดการณ์ – IoT จะไม่ได้ถูกนำมาใช้เรียกค่าไถ่ แต่จะกลายเป็นเป้าหมายสำหรับการเปลี่ยนแปลงครั้งสำคัญในวงกว้าง

อ่านเพิ่มเติมเกี่ยวกับการคาดการณ์ทั้งหมด
• Download the Forcepoint 2018 Security Predictions Report to read more about these and four other predictions:
• ดาวน์โหลด รายงานการคาดการณ์การรักษาความปลอดภัยปี 2018 (2018 Security Predictions Report) ของฟอร์ซพ้อยต์ โดยอ่านเพิ่มเติมเกี่ยวกับการคาดการณ์ประเด็นที่เหลือได้
o GDPR (ร่างกฎหมายคุ้มครองข้อมูลส่วนบุคคล) – ผัดผ่อนในตอนนี้ กังวลในภายหลัง
o การรักษาความปลอดภัยบนคลาวด์ – ผู้ดูแลคลาวด์ คือผู้ดูแลโดเมนใหม่
o เข้ารหัสความปลอดภัยให้เป็นค่ามาตรฐาน – เรื่องสำคัญสำหรับทุกคน
o UEBA (User and Entity Behavioral Analytics) – การก้าวกระโดดครั้งใหญ่ ครั้งถัดไปของอุตสาหกรรม