@Post

ฉบับที่ 1/2561 ประจำเดือน มกราคม พ.ศ. 2561 Free Copy

ภัยคุกคามไซเบอร์ Cybersecurity Trends ที่ต้องพึงระวังในปี 2018

เมื่อโลกเข้าสู่ยุคระบบเศรษฐกิจและสังคมดิจิทัล เทคโนโลยีดิจิทัลเข้ามาเป็นส่วนหนึ่งในชีวิตประจำวัน ทั้งในการปฏิบัติงานและส่วนตัว เมื่อมีประโยชน์อนันต์ก็อย่าลืมว่ามีโทษมหันต์เช่นกัน โดยเฉพาะอย่างยิ่งข้อมูลที่อยู่บนเครือข่ายอินเทอร์เน็ตหรือไซเบอร์ (Cyber) ที่ต้องพึงระวังให้ความตระหนักเพื่อไม่ให้ตกเป็นเป้าของการโจมตีจากภัยคุกคามอันจะนำมาซึ่งความเสียหายและเสื่อมเสียต่อไป

https://depositphotos.com

1 Machine Learning ศึกใหญ่ระหว่างฝั่งโจมตีกับฝั่งป้องกัน

เทคนิค Machine Learning ถูกนำมาใช้เพื่อประมวลผลข้อมูลบนระบบเครือข่ายและอุปกรณ์ปลายทางเพื่อค้นหาช่องโหว่ พฤติกรรมต้องสงสัย หรือการโจมตีแบบ Zero-day อย่างไรก็ตาม ฝั่งแฮกเกอร์เองก็สามารถนำ Machine Learning มาใช้เพื่อสนับสนุนการโจมตีของตนเช่นเดียวกัน ไม่ว่าจะเป็นการเรียนรู้จากการป้องกันของอีกฝ่าย สร้างโมเดลในการขัดขวางการตรวจจับการโจมตี หรือเจาะช่องโหว่ใหม่ที่เพิ่งค้นพบให้เร็วกว่าที่แพตช์จะถูกอัปเดต เป็นต้น ก่อให้เกิดเป็นการปะทะกันระหว่างเทคนิค Machine Learning ของฝั่งโจมตีและฝั่งป้องกัน จึงควรเลือกใช้เทคนิค Machine Learning ที่มีประสิทธิภาพ เข้าใจถึงรูปแบบการโจมตีของแฮกเกอร์และสามารถดำเนินการตัดสินใจเพื่อรับมือกับการโจมตีได้อย่างรวดเร็ว

2 เตรียมพบ Ransomware รูปแบบใหม่ ที่เทคโนโลยี เป้าหมาย และค่าไถ่ต่างไปจากเดิม

การเรียกค่าไถ่จากแคมเปญ Ransomware แบบเดิมๆ จะเริ่มลดลง เนื่องจากโซลูชันสำหรับป้องกัน Ransomware มีให้เลือกมากขึ้น ผู้ใช้มีความตระหนัก และหลายองค์กรเริ่มวางกลยุทธ์สำหรับรับมือกับการโจมตี ส่งผลให้แฮกเกอร์เริ่มปรับเปลี่ยนเป้าหมายไปยังกลุ่มอื่น เช่น ผู้ใช้ทั่วไปที่มีฐานะและอุปกรณ์ Internet of Things แทน นอกจากนี้ Ransomware กลับมีเทคนิคในการโจมตีเพื่อเรียกค่าไถ่มากขึ้น แทนที่จะเข้ารหัสหรือบล็อกการเข้าไฟล์เพียงอย่างเดียว ยังมีการเพิ่มการทำลายข้อมูลและการขัดขวางธุรกิจเข้าไปด้วย เพื่อกดดันให้เหยื่อต้องจ่ายค่าไถ่


https://www.csiac.org

3 แอปพลิเคชัน Serverless เริ่มแพร่หลาย สร้างช่องทางโจมตีใหม่แก่แฮกเกอร์

แอปพลิเคชันประเภทที่ไม่จำเป็นต้องมีเซิฟเวอร์อยู่ตลอดเวลา หรือ Serverless เริ่มเป็นที่นิยมมากขึ้น เนื่องจากช่วยลดเวลาและค่าใช้จ่ายในการพัฒนาแอปพลิเคชัน แต่แอปพลิเคชัน Serverless ยังเปราะบางต่อการโจมตีที่อาศัยการทำ Privilege Escalation (การยกระดับสิทธิ์) และ Application Dependencies (การโจมตีแอปพลิเคชันที่เกี่ยวข้องเพื่อให้ส่งผลกระทบต่อแอปพลิเคชันหลัก) รวมไปถึงการโจมตีข้อมูลที่ส่งผ่านไปมาข้ามระบบเครือข่ายและการโจมตีแบบ Denial of Service เพื่อป้องกันปัญหาดังกล่าว กระบวนการพัฒนาและวางระบบของแอปพลิเคชัน Serverless ควรมีการพิจารณาถึงประเด็นด้านความมั่นคงปลอดภัย การรองรับการขยายระบบในอนาคต และการใช้ VPN หรือการเข้ารหัสข้อมูลในการปกป้องทราฟฟิคที่รับส่งบนระบบเครือข่าย

https://blogs.perficient.com

4 ข้อมูลจากครัวเรือนอัจฉริยะถูกแอบเก็บไปใช้ประโยชน์โดยไม่สนความเป็นส่วนบุคคล

บ้านเรือนในปัจจุบันเริ่มนำเอาอุปกรณ์อัจฉริยะเข้ามาใช้งานเพิ่มขึ้นเรื่อยๆ ส่งผลให้ผู้ผลิตหรือผู้ให้บริการอุปกรณ์เหล่านี้เริ่มต้องการเก็บข้อมูลพฤติกรรมการใช้งานเพื่อนำไปใช้ประโยชน์ทางการตลาด ที่สำคัญคือลูกค้าส่วนใหญ่ไม่ให้ความสำคัญเกี่ยวกับข้อตกลงเรื่องความเป็นส่วนบุคคล ทำให้ผู้ผลิตเหล่านั้นแอบเปลี่ยนเงื่อนไขและข้อตกลงภายหลังเพื่อเก็บข้อมูลโดยไม่ผิดกฎหมาย หรือต่อให้ถูกจับได้ทางผู้ผลิตก็ได้คำนวณค่าปรับเข้าไปในการดำเนินธุรกิจเพื่อป้องกันการขาดทุนด้วยเช่นกัน

https://stores.org

5 ข้อมูลออนไลน์ของผู้เยาว์จะถูกนำไปใช้อ้างถึงตัวตนในอนาคต

โลกกำลังถูกขับเคลื่อนด้วยเทคโนโลยี มนุษย์ทุกเพศทุกวัยต่างหันมาใช้งานเทคโนโลยีเพิ่มมากขึ้น โดยเฉพาะอย่างยิ่งกลุ่ม Gen Z หรือกลุ่มวัยเด็กที่เรียกได้ว่าเติบโตมาพร้อมกับเทคโนโลยีอย่างแท้จริง ข้อมูลดิจิทัลต่างๆ ที่คนกลุ่มนี้สร้างขึ้นบนโลกออนไลน์จะถูกรวบรวมและถูกนำใช้อ้างอิงถึงตัวตนในอนาคต ซึ่งอาจส่งผลในแง่ร้ายได้ เช่น สถานศึกษาตัดสิทธิ์ผู้เข้าสมัคร เนื่องจากพบโพสต์วิดีโอไม่เหมาะสมบน YouTube สมัยยังเป็นเด็ก เป็นต้น ดังนั้นผู้ปกครองควรศึกษารูปแบบของสื่อและข้อมูลออนไลน์ต่างๆ ไปพร้อมกับเด็กยุคใหม่ เพื่อที่จะได้ให้คำแนะนำว่า สิ่งใดควรออกสื่อ สิ่งใดไม่ควรโพสต์ออกไป และสิ่งใดควรระวัง เพื่อปกป้องเด็กเหล่านั้นจากการถูกนำข้อมูลออนไลน์ไปใช้ในทางที่มิชอบ

ที่มา : https://www.catcyfence.com
https://securingtomorrow.mcafee.com