พยากรณ์ภัยคุกคามและความมั่นคงปลอดภัยปี 2017 โดย Forcepoint

Forcepoint (Raytheon + Websense + Stonesoft) ผู้ให้บริการโซลูชันด้าน Cyber Security แบบครบวงจร ออกรายงานการพยากรณ์ภัยคุกคามและแนวโน้มด้านความมั่นคงปลอดภัยในปี 2017 โดยอาศัยการวิเคราะห์จาก Forcepoint Security Labs และ Raytheon ที่คอยเฝ้าระวังและเก็บข้อมูลภัยคุกคามจากทั่วทุกมุมโลก

พยากรณ์ภัยคุกคามและความมั่นคงปลอดภัย 10 ข้อในปี 2017 มีดังนี้

1. สงครามไซเบอร์จะกลายเป็นสงครามเย็น (หรือสงครามโลก?) ครั้งใหม่

NATO ระบุไว้ในเอกสาร **“Enhanced NATO Policy on Cyber Defense”** ว่าการโจมตีไซเบอร์มีผลเทียบเท่ากับการโจมตีทางการทหารด้านอื่นๆ ซึ่งประเทศในสังกัด NATO ความเตรียมความพร้อมและพัฒนาการป้องกันภัยคุกคามในโลกไซเบอร์ด้วยเช่นกัน นอกจากนี้ ประเทศจีนและรัสเซียเองก็มีการก่อตั้งหน่วยงานด้านการทหารไซเบอร์มานานหลายปีแล้วเช่นกัน

จากการวิเคราะห์ของ Forcepoint ชนวนของภัยสงครามไซเบอร์อาจเกิดได้จาก

- แฮ็คเกอร์มือที่สามสร้างสถานการณ์ปั่นป่วน
- แต่ละประเทศทั่วโลกมีศักยภาพในการโจมตีไซเบอร์เพื่อจุดประสงค์ทางการเมืองมากขึ้น
- ความเชื่อที่แตกต่างกัน เช่น การโจมตีไซเบอร์ของกลุ่ม ISIS ซึ่งอาจมีหน่วยงานรัฐบาลหนุนหลัง

- การเพิ่มจำนวนของกลุ่มผู้ก่อการร้ายไซเบอร์ ที่พุ่งเป้าทางการทหาร

2. กลุ่ม Gen Y เพิ่มความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

Gen Y เป็นกลุ่มที่เติบโตมาพร้อมกับอินเทอร์เน็ตและเทคโนโลยี ทำให้เปิดใจและเชื่อมั่นในการใช้เทคโนโลยีต่างๆ ส่งผลให้สามารถนำเทคโนโลยีเหล่านั้นมาสนับสนุนการทำงานได้อย่างมีประสิทธิภาพ แต่การที่ใกล้ชิดกับการใช้เทคโนโลยีมากเกินไปทำให้ขาดความตระหนักถึงความมั่นคงปลอดภัยและความเป็นส่วนบุคคล เช่น นำอุปกรณ์ส่วนตัวเข้ามาใช้ทำงาน หรือแชร์ข้อมูลที่ทำงานสู่สาธารณะ เป็นต้น เหล่านี้ก่อให้เกิดช่องโหว่ที่แฮ็คเกอร์สามารถนำไปใช้ประโยชน์ได้

Forcepoint แนะนำว่า องค์กรไม่ควรปฏิเสธการนำเทคโนโลยีเข้ามาใช้ แต่ควรวางมาตรการควบคุมและสร้างความตระหนักทางด้านความมั่นคงปลอดภัยให้แก่กลุ่ม Gen Y เหล่านี้

3. การปกป้องข้อมูลกลายเป็นกฎระเบียบข้อบังคับ

สหภาพยุโรป (EU) เตรียมออกข้อบังคับทั่วไปว่าด้วยการปกป้องข้อมูล (General Data Protection Regulation: GDPR) ซึ่งพร้อมบังคับใช้ในเดือนพฤษภาคมปี 2018 ส่งผลให้ในปี 2017 บริษัทและโซเชียลมีเดียต่างๆ ต้องเตรียมวางมาตรการควบคุมสำหรับปกป้องข้อมูลส่วนบุคคล (Personally Identifiable Information: PII) รวมไปถึงแต่ละองค์กรจำเป็นต้องประเมินความเสี่ยงกันใหม่ โดยให้ความสำคัญกับการเกิด Data Breach มากขึ้น

นอกจากนี้ ผลลัพธ์ที่ตามมาอีกอย่างคือ MSSP อาจมีค่าบริการสูงขึ้น เนื่องจากจำเป็นต้องแยกข้อมูลของลูกค้ามาดูแล และทำให้มั่นใจได้ว่าข้อมูลเหล่านั้นถูกปกป้องเป็นอย่างดี

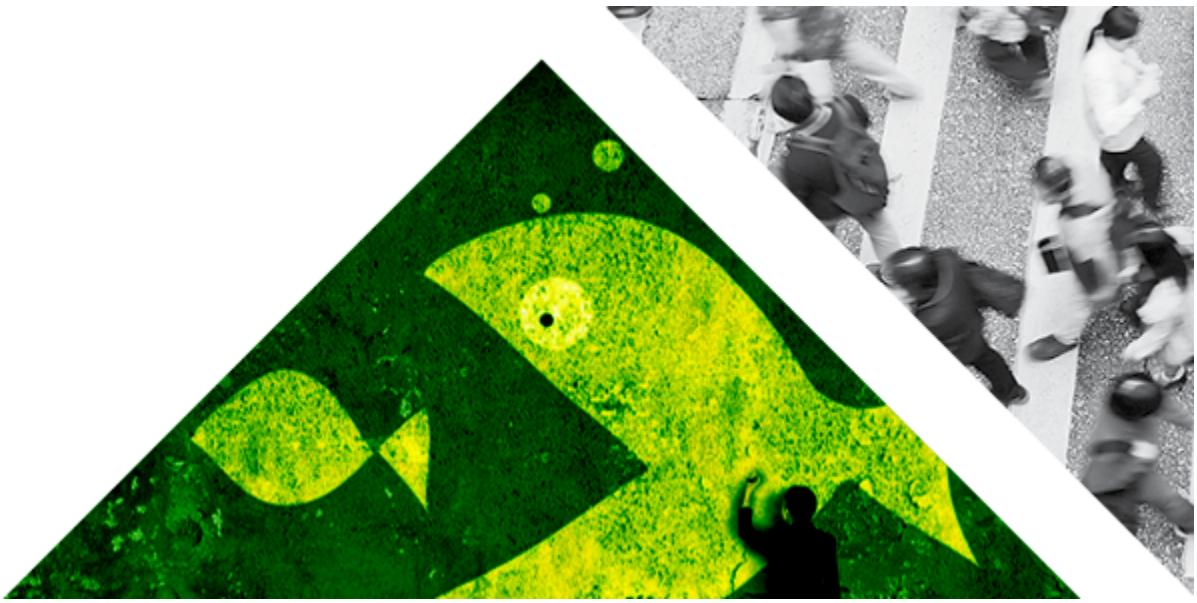
4. พนักงานภายในองค์กรกลายเป็นโจรเสียเอง

จากการสำรวจของ Forcepoint ระบุว่า พนักงานภายในองค์กรมีแนวโน้มที่จะนำข้อมูลส่วนบุคคล (PII) ของลูกค้าไปใช้เพื่อแลกกับค่าตอบแทนมหาศาล เนื่องจากสามารถเข้าถึงข้อมูลของลูกค้าได้ง่าย และไม่มีกฎระเบียบข้อบังคับที่เข้มงวดเพียงพอ ยกตัวอย่างเคสเมื่อเร็วๆ นี้ พนักงานของธนาคารขนาดใหญ่แห่งหนึ่งกว่า 5,300 คน พร้อมใจกันใช้ข้อมูลลูกค้าในการเปิดบัญชีปลอมมากกว่า 2,000,000 บัญชี แลกกับการสร้างยอดหลายล้านดอลลาร์สหรัฐฯ

Forcepoint แนะนำว่า ควรมีการออกมาตรการป้องกันที่พร้อมบังคับใช้ในระดับประเทศหรือระดับนานาชาติ เพื่อจำกัดและควบคุมการเข้าถึงข้อมูลส่วนบุคคล เช่นเดียวกับ GDPR

5. Vendor รายใหญ่ควบรวมกิจการรายย่อยมากขึ้น

ปี 2017 จะเป็นปีเห็นการบูรณาการเทคโนโลยี เรียกได้ว่าเป็นยุค **Security Consolidation 4.0** ซึ่งจะเห็นบริษัทด้านความมั่นคงปลอดภัยขนาดใหญ่เข้าซื้อกิจการของบริษัทขนาดเล็กมากขึ้น หลายบริษัทที่ไม่ถูกควบรวมหรือไม่มีนักลงทุนสนับสนุนอาจต้องปิดตัวลง ก่อให้เกิดสิ่งที่เรียกว่า Abandonware หรือก็คือเทคโนโลยีที่ถูกทิ้งให้ไม่มีการซัพพอร์ตหรือการอัปเกรดอีกต่อไป ซึ่งเป็นช่องโหว่สำคัญที่แฮ็คเกอร์นำมาใช้เจาะระบบขององค์กร



6. ภัยคุกคามเตรียมพุ่งเป้าระบบ Cloud

ปัจจุบันหลายองค์กรเริ่มหันไปใช้ระบบ Cloud มากขึ้น ทำให้แฮ็คเกอร์เริ่มค้นหาวิธีในการโจมตีระบบ Cloud โดยเฉพาะอย่างยิ่งการโจมตีในระดับ Hypervisor ของ Virtual Machine ซึ่งเป็นรากฐานของโครงข่าย Cloud Computing ถ้าแฮ็คเกอร์โจมตีได้สำเร็จ ย่อมเข้าควบคุมระบบทั้งหมดที่รันอยู่บน Cloud ได้ทันที ที่สำคัญคือ Cloud Provider อาจเสี่ยงตกเป็นเป้าหมายของการโจมตีแบบ DDoS มากขึ้น ถึงแม้ว่าแฮ็คเกอร์จะมีเป้าหมายที่ระบบอื่น แต่ระบบขององค์กรอาจเสี่ยงได้รับกระทบจากการโจมตีด้วยเช่นกัน

7. AI สั่งการด้วยเสียงกลายเป็นส่วนหนึ่งในชีวิตของมนุษย์

การมาถึง AI สั่งการด้วยเสียง เช่น SIRI, Cortana และ Amazon Echo ก่อให้เกิดการเปลี่ยนแปลงในการเข้าถึงเว็บ ข้อมูล และแอพพลิเคชัน เช่น

- มอบประสบการณ์ใหม่ในการใช้เว็บให้แก่ผู้ใช้ เนื่องจาก AI มีการเก็บข้อมูลผู้ใช้ตลอดเวลา ทำให้สามารถเรียนรู้และเลือกสรรสิ่งที่เหมาะสมให้แก่ผู้ใช้ โดยที่ไม่ต้องทำอะไรมาก
- ก่อให้เกิดการแข่งขันระหว่างบริษัทขนาดใหญ่ เพื่อให้ลูกค้าเกิดความคุ้นเคยกับระบบ AI ของตน
- ผู้พัฒนา AI กลายเป็นผู้มีอิทธิพลเชิงธุรกิจ เนื่องจากสามารถควบคุมได้ว่าให้ AI นำเสนอข้อมูลจากแหล่งใดแก่ผู้ใช้
- แอพพลิเคชันที่มีระบบ AI สั่งการด้วยเสียงจะเป็นที่นิยมในปี 2017 ซึ่งอาจกลายเป็นช่องทางใหม่ให้แฮ็คเกอร์ขโมยข้อมูล เนื่องจาก AI มักเก็บข้อมูลส่วนบุคคลเป็นจำนวนมาก

8. เครื่องจักรสำหรับแฮ็คมาแรงในปี 2017

เช่นเดียวกับที่หลายบริษัทนำระบบ AI เข้ามาสนับสนุนธุรกิจของตน แฮ็คเกอร์ก็นำระบบ AI เข้ามาสนับสนุนการแฮ็คด้วยเช่นกัน โดยการออกแบบเครื่องจักรที่สามารถค้นหาจุดอ่อนหรือช่องโหว่บนระบบเครือข่ายได้โดยอัตโนมัติ ซึ่งในปี 2017 นี้ ความสามารถในการค้นหาและเจาะระบบของเครื่องจักรอาจก้าวข้ามความสามารถในการปฏิบัติงานด้านความมั่นคงปลอดภัยของมนุษย์ไปแล้วก็ได้

9. Ransomware ยังเป็นที่นิยม

จากความสำเร็จของ Ransomware ในปี 2015 และ 2016 ทำให้เราคาดการณ์ได้ว่าในปี 2017 Ransomware จะยังคงเป็นที่นิยมในหมู่แฮ็คเกอร์ จากการตรวจสอบของ Forcepoint พบว่าในช่วงครึ่งแรกของปี 2016 แฮ็คเกอร์สามารถทำรายได้จาก Ransowmare รวมแล้วไม่ต่ำกว่า 4,300 ล้านบาท องค์กรส่วนใหญ่ยังคงไม่มีมาตรการรับมือกับ Ransomware ที่ดีเพียงพอ และโดยเฉลี่ยแล้ว 37% ของเหยื่อมักยอมจ่ายค่าไถ่เพื่อแลกกับการเข้าถึงข้อมูล

นอกจากนี้ แฮ็คเกอร์ยังมีการพัฒนา Ransomware เพื่อให้สามารถจารกรรมข้อมูลของเป้าหมายได้อีกด้วย เพื่อนำข้อมูลเหล่านั้นไปขายให้บริษัทคู่แข่ง เป็นการทำกำไรสองต่อนอกจากการเรียกค่าไถ่เพียงอย่างเดียว

10. Abandonware: ของหมดอายุนำมาซึ่งช่องโหว่

จากการสำรวจของ Forcepoint พบว่ามีผู้ใช้ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไม่ต่ำกว่า 75,000 คนที่ยังคงใช้ซอฟต์แวร์ที่หมดอายุ หรือไม่มีการอัปเดตภายในองค์กรของตน เสี่ยงถูกแฮ็คเกอร์ใช้ช่องโหว่ของซอฟต์แวร์เหล่านั้นในการเจาะระบบเพื่อขโมยข้อมูล นอกจากนี้ ผู้ใช้หลายล้านคนพึงพอใจเพียงการอัปเดตแพทช์ด้านความมั่นคงปลอดภัยอัตโนมัติ จนไม่มีการวางมาตรการควบคุมอื่นๆ ส่งผลให้ระบบรักษาความมั่นคงปลอดภัยของตนไม่แข็งแกร่งเพียงพอที่จะรับมือกับการโจมตีรูปแบบอื่นๆ ที่มีความซับซ้อน

“ภัยคุกคามไซเบอร์ทวีความรุนแรงขึ้นเรื่อยๆ ในปัจจุบัน นอกจากองค์กรควรสรรหาเทคโนโลยีใหม่ๆ มารับมือกับการโจมตีของแฮ็คเกอร์แล้ว องค์กรควรมีการกำกับดูแล และวางมาตรการควบคุม เช่น การนำมาตรฐาน ISO 27001 เข้ามาใช้ เพื่อเพิ่มความมั่นคงปลอดภัยขององค์กรให้เป็นไปตามมาตรฐานสากล นอกจากนี้ ต้องไม่ลืมสร้างความตระหนัก และให้ความรู้ด้านภัยคุกคามและผลกระทบต่อธุรกิจกับพนักงานภายในองค์กรอีกด้วย” — คุณฉัตรกุล โสภณางกูร ผู้จัดการฝ่ายขายของ Forcepoint ประเทศไทย

ดาวน์โหลดรายงานฉบับเต็มได้ที่: https://www.forcepoint.com/2017predictions