IT Trend 2017 และการรับมือด้านความปลอดภัย (ตอนจบ)

วิชย์ศุทธ์ เมาระพงษ์
ที่ปรึกษาโครงการสารสนเทศของหน่วยงานภาครัฐ
สังกัดสถาบันวิจัยและให้คำปรึกษา
แห่งมหาวิทยาลัยธรรมศาสตร์

ต่อ จากฉบับที่แล้ว

6) การชวนเชื่อทาง Internet จะเป็นเรื่องที่พบได้อย่างแพร่หลาย

ในปี 2016 ที่ผ่านมานั้น 46.1% ของประชากรโลกสามารถเข้าถึง internet ได้ ผ่านอุปกรณ์ และช่องทางการเชื่อมต่อต่างๆ ซึ่งหมายความว่า มีผู้คนจำนวนมากสามารถเข้าถึงข้อมูลได้อย่างรวดเร็วและง่ายดาย โดยบางรายอาจไม่ได้ตรวจสอบความน่าเชื่อถือของข้อมูลนั้นก่อน ทำให้เป็นการเปิดโอกาสให้บุคคลบางกลุ่มสามารถแสดงความเห็นโน้มน้าว หรือมีอิทธิพลให้ผู้คนเชื่อไปทางใดทางหนึ่งได้ ตัวอย่างเช่น การเลือกตั้งที่เกิดขึ้นในหลายประเทศ ได้สะท้อนให้เห็นถึงพลังของ Social media และแหล่งข้อมูลออนไลน์ทั้งหลายที่มีอิทธิพลอย่างมากต่อการตัดสินใจทางการเมือง โดยเฉพาะกรณีของการเลือกตั้งประธานาธิบดีสหรัฐเมริกา เว็บไซต์ชื่อดัง WikiLeaks ได้ใช้โฆษณาชวนเชื่อด้วยเนื้อหาที่ดูน่าเชื่อถือเป็นอย่างมากมาเผยแพร่บนเว็บไซต์เพียงแค่สัปดาห์เดียวก่อนจะถึงวันเลือกตั้งประธานาธิบดีสหรัฐอเมริกา

นอกจากนี้ยังพบการว่าจ้างนักข่าวสมัครเล่นให้เผยแพร่ข่าวลวงที่เกี่ยวข้องกับการเลือกตั้ง โดยมีค่าจ้างเฉลี่ยอยู่ราวๆ 20 ดอลลาร์สหรัฐฯ ต่อเดือน เพียงแค่คอยโพสต์เนื้อหาที่เกี่ยวข้องกับตัวผู้สมัครลงเลือกตั้ง รวมถึงพบกลุ่มเฉพาะกิจที่ได้รับเงินสนับสนุนให้คอยโพสต์ข่าวชวนเชื่อบน Social media อย่าง Facebook และ LinkedIn ถือเป็นการใช้ประโยชน์จากกลไกการคัดกรองการแสดงเนื้อหาในช่วงเลือกตั้ง

การขาดความถูกต้องแม่นยำของข้อมูล เมื่อผนวกเข้ากับกลุ่มนักกดแชร์ที่ต้องการชักจูงผู้คนให้เปลี่ยนความเชื่อ หรือยกระดับความน่าเชื่อถือของความเชื่อในกลุ่มตนเองนั้น ทำให้การทำข่าวปลอมได้รับความนิยมอย่างมาก ทำให้ผู้ใช้งาน internet บางรายไม่สามารถแยกแยะข่าวจริงกับข่าวลวงได้

แม้จะมีความพยายามจาก Facebook และ Google ที่คอยยกเลิกการโฆษณาบนเว็บไซต์ที่แสดงข่าวปลอม รวมทั้ง Twitter ที่เพิ่มเติมความสามารถในการปิดกั้นการแสดงผล (Mute) เพื่อให้ผู้ใช้เลือกรับข่าวสาร และบทสนทนาได้ตามต้องการแล้ว แต่ก็ยังไม่สามารถลดผลกระทบได้มากเท่าที่ควร

กลุ่มบุคคลที่สามารถชักจูงความเห็นของคนหมู่มากโดยใช้กลยุทธ์ต่างๆ จะสามารถสร้างผลลัพธ์ได้ตามที่ตัวเองต้องการ โดยในปี 2017 เราจะเห็นการใช้ Social media เป็นเครื่องมือหรือใช้เป็นอาวุธในการต่อสู้แข่งขันกันมากขึ้น

7) การบังคับใช้ และปฏิบัติตามกฎหมายเกี่ยวกับการปกป้องข้อมูล จะเป็นการเพิ่มค่าใช้จ่ายในการบริหารจัดการขององค์การขึ้นเป็นอย่างมาก

ในยุโรปกฎหมาย GDPR ซึ่งเป็นการตอบสนองของ EU ต่อปัญหาความเป็นส่วนตัวของข้อมูลนั้น จะไม่ได้กระทบเฉพาะประเทศสมาชิกสหภาพยุโรปเท่านั้น แต่ยังส่งผลกระทบไปทั่วโลกที่มีการใช้งาน ประมวลผลหรือจัดเก็บข้อมูลส่วนตัวของคนใน EU ด้วย จากกำหนดการบังคับใช้ในปี 2018 นั้น จะทำให้องค์การถูกปรับเป็นมูลค่ามากถึง 4% ของรายรับของบริษัททั้งหมดถ้าไม่สามารถทำให้สอดคล้องตามกฎหมายดังกล่าวได้

กฎหมาย GDPR จะบีบให้เกิดการเปลี่ยนแปลงในองค์การที่ได้รับผลกระทบ ทั้งด้านนโยบาย และกระบวนการทางธุรกิจ ซึ่งทำให้เกิดค่าใช้จ่ายในการบริหารงานเพิ่มขึ้น จากกฎ GDPR ทำให้องค์การต้องมีการเปลี่ยนแปลง อันประกอบด้วย

- ต้องมีเจ้าหน้าที่ดูแลความปลอดภัยของข้อมูลหรือ DPO (Data Protection Officer) ซึ่งหมายความว่า ค่าใช้จ่ายขององค์การจะพุ่งสูงขึ้นจากการจัดจ้าง อบรม และรักษาพนักงานระดับอาวุโสเอาไว้
- ผู้ใช้จะต้องได้รับการแจ้งสิทธิที่ได้รับใหม่ตามกฎหมายนี้ และองค์การจะต้องทำให้แน่ใจได้ว่าผู้ใช้สามารถใช้สิทธิดังกล่าวได้ โดยยึดหลักที่ว่าประชาชนของ EU ถือเป็นเจ้าของข้อมูลส่วนตัวของตัวเอง ดังนั้นข้อมูลที่ถูกจัดเก็บจะถือเป็นแค่การ “ยืม” มาใช้ชั่วคราว ซึ่งหลักการนี้จะนำไปสู่การเปลี่ยนแปลงกระบวนการจัดการข้อมูลของธุรกิจเกือบทั้งหมด
- ต้องจัดเก็บข้อมูลน้อยที่สุดเท่าที่จำเป็นต่อบริการนั้นๆ โดยองค์การต่างๆ จะต้องปรับเปลี่ยนวิธีการจัดเก็บข้อมูลให้สอดคล้องกับกฎหมายนี้

การเปลี่ยนแปลงดังกล่าวข้างต้น จะเป็นการบังคับให้องค์การต้องปฏิรูประบบการประมวลผลใหม่ทั้งหมด เพื่อให้แน่ใจว่าสอดคล้องตามข้อกำหนด หรือมีการแยกส่วนของข้อมูลส่วนตัวของคนใน EU ออกจากผู้ที่อยู่ในภูมิภาคอื่นของโลกอย่างชัดเจน ซึ่งเป็นการยากโดยเฉพาะบริษัทข้ามชาติทั้งหลายที่อาจต้องสร้างระบบจัดเก็บข้อมูลใหม่ทั้งหมดเฉพาะสำหรับประชากรในภูมิภาค EU โดยเฉพาะ นอกจากนี้ยังต้องตรวจสอบการปกป้องความเป็นส่วนตัวของข้อมูลบนบริการ Cloud ที่ตกเองใช้อยู่ด้วย องค์การจำเป็นต้องลงทุนในด้านปลอดภัยของข้อมูลที่ครอบคลุม อันรวมไปถึงการฝึกอบรมเจ้าหน้าที่ เพื่อบังคับใช้ให้สอดคล้องกับกฎ GDPR ด้วย

8) ผู้โจมตีเตรียมพัฒนากลยุทธ์การโจมตีแบบใหม่ๆ ที่สามารถหลบเลี่ยงมาตรการ และกลไกความปลอดภัยที่ใช้กันโดยทั่วไปในปัจจุบันได้

การโจมตีที่มีการวางกลยุทธ์ และระบุเป้าหมายจำเพาะนั้นมีการพัฒนามาอย่างต่อเนื่อง ขณะที่โครงสร้างพื้นฐานที่องค์การส่วนใหญ่ใช้งานอยู่ยังคงเดิม แต่สำหรับผู้โจมตีแล้วความสามารถใน

การปรับแต่งเครื่องมือ กลยุทธ์ และวิธีการให้สามารถจัดการเป้าหมายในองค์การที่หลากหลาย ในหลายประเทศพร้อมๆ กันได้ ทำให้เราอาจจะได้เห็นเทคนิคใหม่ๆ ในการโจมตีมากขึ้น ในแบบคาดที่คาดไม่ถึง

ความเร็วในการเรียนรู้การป้องกัน และช่องโหว่ของอาชญากรไซเบอร์ในขณะนี้ จะสามารถพัฒนาวิธีการโจมตีที่หลบเลี่ยงเทคโนโลยีด้านความปลอดภัยที่มีการพัฒนาในช่วงที่ผ่านมาได้อย่างรวดเร็ว จากเดิมที่เหล่าอาชญากรจะเริ่มต้นจากการใช้โค้ดไบนารีก็ย้ายมาโจมตีผ่านไฟล์เอกสารต่างๆ จนในปัจจุบันก็เริ่มหันมาใช้สคริปต์ และไฟล์ Batch แทน การหลบเลี่ยงหรือแม้กระทั่งจัดการกับระบบ Sandbox (ระบบ Program ที่ใช้ตรวจสอบที่มาที่ไป และพฤติกรรมของ file หรือ script ต้องสงสัย) และนอกเหนือจากการหลบเลี่ยงกลไก Sandbox แล้ว เรายังจะได้เห็นการโจมตีที่วิ่งข้าม VM ได้ ซึ่งจะกลายเป็นส่วนหนึ่งของกระบวนการโจมตีแบบลูกโซ่ชั้นสูง โดยจะมีการปรับแต่งการโจมตีที่หลากหลายโดยใช้ช่องโหว่ของ VM บนระบบ Cloud เพื่อเข้าถึงข้อมูลที่ทำงานบนทรัพยากรและสภาพแวดล้อมเสมือนได้

พัฒนาการทางเทคนิคของอาชญากรเหล่านี้ ทำให้องค์การจำเป็นต้องหาเทคโนโลยีด้านความปลอดภัยที่ทำให้ได้การมองเห็นและความสามารถในการควบคุมอย่างสมบูรณ์ ทั้งเครือข่าย และข้อมูล รวมทั้งความสามารถในการระบุตำแหน่งที่ไม่เพียงแค่ตำแหน่งที่โดนโจมตีเท่านั้น แต่ยังต้องระบุตั้งแต่ต้นตอของการโจมตีได้ด้วย การรักษาความปลอดภัยที่ใช้เทคโนโลยีเรียนรู้ด้วยตนเอง หรือ Machine Learning จะสามารถปกป้องจากอันตรายทั้งที่มีการพัฒนาจากตัวที่รู้จักมาก่อน และสามารถใช้กลไกของ Sandbox เพื่อจำกัดบริเวณอันตรายที่ไม่รู้จักให้สามารถจัดการในลำดับต่อไปได้อย่างทันท่วงที แทนที่จะยึดติดกับกลยุทธ์ความปลอดภัยอย่างใดอย่างหนึ่ง องค์การควรใช้เทคโนโลยีที่หลากหลายผสมผสานการทำงานร่วมกันทั้งด้านการตรวจสอบ ตอบสนอง และจัดการรับมือกับการโจมตีที่ระบุเป้าหมายได้ ซึ่งถือเป็นสิ่งสำคัญมากในการรับมือกับการโจมตีที่พัฒนาอย่างรวดเร็วเช่นนี้

จากแนวโน้มของเทคโนโลยี และแนวโน้มความมั่นคงปลอดภัยข้างต้นองค์การต่างๆ จำเป็นต้องเตรียมพร้อมในการป้องกันภัยต่างๆ ที่เหล่าอาชญากรไซเบอร์พัฒนาขึ้น ซึ่งจำเป็นต้องใช้หลายกลยุทธ์ หลายเทคโนโลยีความปลอดภัยมาทำงานผสมผสานกันเป็นระบบป้องกันบนเครือข่ายที่เชื่อมต่อกันอย่างสมบูรณ์ โดยอาจประกอบด้วยเทคโนโลยีต่างๆ อันได้แก่

- Anti-Malware ระดับสูง (ที่เป็นมากกว่าการ black list)
- Anti-spam และระบบป้องกันการหลอกลวง ในทุกระบบที่เกี่ยวข้อง
- ระบบจัดความน่าเชื่อถือเว็บไซต์
- ระบบตรวจจับการรั่วไหลของข้อมูล
- การควบคุม Application (เพื่อจัดทำ white list)
- การคัดกรองเนื้อหาข้อมูล
- การปกป้องช่องโหว่
- การจัดความน่าเชื่อถือ Mobile Application
- ระบบป้องกันการบุกรุก ทั้งบน server และบนเครือข่าย
- ระบบป้องกันด้วย firewall ทั้งบน server และบนเครือข่าย

ภัยต่อความมั่นคงปลอดภัยในปัจจุบันส่วนใหญ่สามารถตรวจจับได้ด้วยการผสานการทำงานร่วมกันของเทคนิคต่างๆ ข้างต้น แต่สำหรับการตรวจจับภัยที่ “ไม่รู้จัก” หรือ bug แบบ Zero-day แล้วองค์การเหล่านั้นจำเป็นต้องใช้ระบบตรวจสอบความถูกต้อง และพฤติกรรมของข้อมูล รวมทั้งระบบ Sandbox ร่วมด้วย

เทคโนโลยี Internet of thing นั้นให้ทั้งความสะดวกสบายและความเสี่ยง ผู้ใช้อุปกรณ์ internet of thing ต่างๆ ควรต้องเรียนรู้วิธีการรักษาความปลอดภัย ก่อนที่อุปกรณ์ของตัวเองจะถูกเข้าควบคุมผ่าน internet นอกจากนี้ยังควรคำนึงถึงความปลอดภัยเป็นหลักเวลาเลือกซื้ออุปกรณ์อีกด้วย อาทิเช่น มีการยืนยันตนหรือเปลี่ยนรหัสผ่าน มีการ update patch firmware มีการเข้ารหัสข้อมูลที่ส่งต่อบนเครือข่าย มีการเปิด/ปิดการใช้งาน port สำหรับเข้าถึงอุปกรณ์ และผู้จำหน่ายได้ออกตัว update patch firmware เป็นประจำ เป็นต้น

นอกจากนี้องค์การต้องให้ความสำคัญต่อการฝึกอบรม ให้ความรู้ สร้างความตระหนักแก่บุคลากร และผู้ที่เกี่ยวข้องให้รับมือกับการโจมตีเชิงจิตวิทยา เรียนรู้รูปแบบการโจมตีใหม่ๆ แนวทางในการป้องกัน และแก้ไข อย่างต่อเนื่องจนกระทั่งกลายเป็นวัฒนธรรมการทำงานขององค์การ ซึ่งจะช่วยเติมเต็มระบบความปลอดภัยโดยรวมขององค์การให้สามารถรับมือกับภัยจากการใช้งานเทคโนโลยีได้อย่างมีประสิทธิภาพสูงสุด TPA news

ข้อมูลอ้างอิง:

www.gartner.com
www.imcinstitute.com
www.trendmicro.com
www.digiday.com
www.techtalkthai.com
www.bangkokbiznews.com