IT Trend 2017 และการรับมือด้านความปลอดภัย

วิชญ์ศุทธ์ เมาระพงษ์
ที่ปรึกษาโครงการสารสนเทศของหน่วยงานภาครัฐ
สังกัดสถาบันวิจัยและให้คำปรึกษา
แห่งมหาวิทยาลัยธรรมศาสตร์

ต่อ จากฉบับที่แล้ว

3. การโจมตีด้วยเมล์หลอกลวงจะเพิ่มขึ้นอย่างมากในปี 2017

ด้วยการเจาะกลุ่มเหยื่อที่เป็นสถาบัน และหน่วยงานทางการเงินทั่วโลก ทำให้การโจมตีด้วยเมล์หลอกลวงเชิงธุรกิจหรือ Business Email Compromise (BEC) อยู่ในรูปของการเจาะบัญชีอีเมล์หรือหลอกลวงพนักงานเพื่อให้โอนเงินมายังบัญชีของอาชญากร แม้จะไม่มีการใช้เทคโนโลยีที่ซับซ้อนเป็นพิเศษสำหรับการโจมตีในลักษณะนี้ แต่ความพยายามที่จะบรรจงซอกแซกข้อมูลภายในองค์การเพื่อให้สามารถแต่งอีเมล์ให้น่าเชื่อถือมากขึ้นเรื่อยๆ ก็ถือว่าเป็นแนวโน้มที่ค่อนข้างน่ากลัว โดยเฉพาะองค์การที่สามารถค้นข้อมูลภายในบางอย่างได้ผ่าน Search engine

จากความง่ายในการโจมตีแบบ BEC โดยเฉพาะการปลอมเป็นเมล์จากผู้บริหารองค์การได้รับความนิยมจากอาชญากรไซเบอร์มากขึ้น เนื่องจากไม่ต้องลงทุนมาก ทำได้ง่าย ไม่ต้องพึ่งพาเทคโนโลยีที่ซับซ้อน แต่กลับได้ผลตอบแทนสูง ตัวเลขความเสียหายที่ประมาณการณ์ไว้จากการโจมตีแบบ BEC ในช่วงสองปีที่ผ่านมาอยู่ที่ 3 พันล้านดอลลาร์สหรัฐฯ ขณะที่ถ้าเปรียบเทียบกับการโจมตีด้วย Ransomware ที่ได้ผลตอบแทนเฉลี่ยต่อครั้งอยู่ที่ 722 ดอลลาร์สหรัฐฯ หรืออาจจะมากถึง 30,000 ดอลลาร์สหรัฐฯ ได้ถ้ายึดได้ทั่วทั้งเครือข่ายขององค์การ

นอกจากนี้ ความเร็วในการจ่ายเงินของเหยื่อยังเป็นสิ่งดึงดูดอาชญากรให้เลือกวิธีนี้มาก รวมทั้งความล่าช้าในการดำเนินคดีโดยเฉพาะเมื่อเป็นคดีที่เกิดขึ้นระหว่างประเทศ ยิ่งทำให้อาชญากรชื่นชอบวิธีการนี้มากขึ้นตามไปด้วย

BEC ถือว่ายากต่อการตรวจจับ เนื่องจากอีเมล์เหล่านี้ไม่ได้มีข้อมูลหรือโค้ดอันตรายที่ระบบปกติคัดกรองได้ แต่องค์การก็ควรคัดกรองอันตรายเหล่านี้ที่แหล่งกำเนิด ด้วยกลไกความปลอดภัยบนระบบเครือข่ายองค์การ และ server ระบบอีเมล์ ด้วยเทคโนโลยีความปลอดภัยลักษณะนี้จะช่วยระบุความผิดปกติ และพฤติกรรมของไฟล์หรือองค์ประกอบอื่นๆ ที่ดูเป็นอันตรายได้ แต่อย่างไรก็ดี การป้องกัน BEC ก็ยังยุ่งยากในมิติของบุคคล เพราะถ้าเกิดเหยื่อยังคงยอมโอนเงินให้แก่อาชญากรอย่างต่อเนื่อง องค์การควรมีนโยบายที่แข็งแกร่งสำหรับการโอนจำนวนมาก เป็นต้น

4. การเจาะระบบกระบวนการทางธุรกิจจะพุ่งเป้าไปที่เหยื่อที่เป็นหน่วยงานทางการเงินเป็นหลัก

จากกรณีการจารกรรมเงินของธนาคารในบังคลาเทศ ที่สร้างความเสียหายมากถึง 81 ล้านดอลลาร์สหรัฐฯ ถือว่าแตกต่างจากการโจมตีแบบ BEC ที่อาศัยจิตวิทยาเป็นหลัก การเจาะระบบเชิงธุรกิจนี้เป็นวิธีที่ต้องทำเข้าความใจอย่างลึกซึ้งเกี่ยวกับขั้นตอนการทำธุรกรรมทางการเงินของสถาบันการเงินขนาดใหญ่ จึงเรียกการโจมตีนี้ว่า Business Process Compromise หรือ BPC

BPC จะเกิดขึ้น และขยายวงกว้างออกจากฝ่ายการเงิน แม้ว่าขั้นตอนสุดท้ายยังคงต้องอาศัยการโอนเงินของเหยื่อ กรณีที่เป็นไปได้มีตั้งแต่การเจาะเข้าระบบสั่งซื้อเพื่อให้อาชญากรไซเบอร์สามารถรับเงินค่าสินค้าจากผู้จำหน่ายที่มีตัวตนจริงได้ การเจาะเข้าสู่ระบบชำระเงินก็สามารถชักนำให้เกิดการโอนเงินที่ไม่ถูกต้องได้ด้วยเช่นกัน หรืออาชญากรอาจจะเจาะระบบเข้าศูนย์บริหารการจัดส่งสินค้า แล้วเปลี่ยนที่อยู่จัดส่งสินค้าที่มีมูลค่าสูง เหตุการณ์ดังกล่าวเคยเกิดขึ้นแล้วเมื่อปี 2556 เมื่อบริษัทชิปปิ้งอย่าง Antwerp Seaport ถูกเจาะระบบเพื่อใช้ประโยชน์ในการขนส่งยาเสพติด

อาชญากรไซเบอร์ที่ทำการโจมตีแบบ BPC ยังมีแนวโน้มที่จะทำเพื่อหาเงินมากกว่าเพื่อแรงจูงใจทางการเมืองหรือเพื่อล้วงข้อมูล แต่ว่าวิธีการ และกลยุทธ์ที่ใช้ในการโจมตียังคงมีลักษณะคล้ายกัน ซึ่งถ้าเปรียบเทียบผลตอบแทนระหว่างการโจมตีด้วย Ransomware (ประมาณ 20,000 ดอลลาร์สหรัฐฯ) กับการโจมตีแบบ BEC (140,000 ดอลลาร์สหรัฐฯ) และ BPC (81 ดอลลาร์สหรัฐฯ) จากเหตุการณ์ข้างต้นแล้ว จะเห็นได้ชัดถึงเหตุผลที่เหล่าอาชญากรไซเบอร์จะเลือกวิธีการโจมตีแบบ BPC แทน

องค์การมักมีความสามารถในการมองเห็นความเสี่ยงที่เกี่ยวข้องกับการโจมตีกระบวนการทางธุรกิจดังกล่าวค่อนข้างต่ำ ระบบความปลอดภัยทั่วไปมักจำกัดอยู่ที่การป้องกันไม่ให้อุปกรณ์ถูกเจาะระบบ ซึ่งอาชญากรไซเบอร์ต่างใช้ประโยชน์จากการตื่นตัวกับความเสี่ยงที่ล่าช้าขององค์การ แต่ยังมีเทคโนโลยีความปลอดภัยอย่างเช่น การควบคุม application ที่สามารถปิดกั้นการเข้าถึงอุปกรณ์ปลายทางที่สำคัญทางธุรกิจได้ ซึ่งก็ควรใช้ร่วมกับการปกป้องอุปกรณ์ปลายทางในรูปแบบอื่นๆ เพื่อตรวจจับความเคลื่อนไหวที่ผิดปกติ ระบบความปลอดภัยเหล่านี้ควรใช้ควบคู่กับนโยบายและแนวทางปฏิบัติที่เหมาะสมเกี่ยวกับการรับมือการโจมตีทางจิตวิทยา ซึ่งควรจะต้องทำให้กลายเป็นพื้นฐานของวัฒนธรรมองค์การ

5. Adobe และ Apple อาจกลายเป็น Platform ที่พบช่องโหว่จำนวนมากกว่า Microsoft

ในปี 2016 Adobe พบช่องโหว่ที่ถูกเปิดเผยทั้งหมดแบบ Zero-Day ถึง 135 ช่องโหว่ ขณะที่ผลิตภัณฑ์ของ Microsoft มี 76 ช่องโหว่ นอกจากนี้ผลิตภัณฑ์ของ Apple พบช่องโหว่สูงมากขึ้นเป็นประวัติการณ์ในปี 2016 ด้วยตัวเลขช่องโหว่ที่พบถึง 50 ช่องโหว่ เมื่อเทียบกับปี 2015 ที่พบ 25 ช่องโหว่

การค้นพบช่องโหว่ในผลิตภัณฑ์ของ Adobe จำนวนมาก ย่อมหลีกเลี่ยงไม่ได้ที่จะนำไปสู่การพัฒนาชุดโจมตีสำเร็จรูป ซึ่งอาชญากรอาจสามารถใช้ประโยชน์จากชุดโจมตีสำเร็จรูปดังกล่าวในการแพร่กระจาย Ransomware ต่อไปได้ software ของ Apple ก็ตกอยู่ในชะตากรรมเดียวกัน เนื่องจากมีผู้ใช้งานเครื่อง Mac มากขึ้นเรื่อยๆ ดังนั้น เมื่อพิจารณาร่วมกับการยกระดับด้านความปลอดภัยของ Microsoft แล้ว ย่อมทำให้เหล่าอาชญากรไซเบอร์เบนเข็มมาโจมตี Platform อื่นนอกเหนือจากของ Microsoft มากขึ้น อีกทั้งจากการที่ Apple ได้หยุดการ Support iPhone 4S แล้ว ทำให้อาจจะได้เห็นการใช้ช่องโหว่ที่มีการ patch ไปแล้วในโทรศัพท์รุ่นใหม่กว่ามาโจมตีโทรศัพท์รุ่นที่ไม่มี Patch ออกมาให้ update มากขึ้นตามไปด้วย

การป้องกัน และอุดช่องโหว่ถือเป็นวิธีเดียวที่จะปกป้องได้อย่างมีประสิทธิภาพ และยั่งยืนเพียงพอ จากช่องโหว่ต่างๆ ที่ยังไม่ได้รับการ patch และช่องโหว่แบบ Zero-day ยิ่งพบช่องโหว่จำนวนมากในองค์การส่วนใหญ่ โดยเฉพาะองค์การที่ยังใช้ Software เก่าที่ถูกยกเลิกการ Support ไปแล้ว ยิ่งทำให้การปกป้องช่องโหว่มีความสำคัญเป็นอย่างยิ่ง โดยเฉพาะเมื่อ Software ที่ได้รับความนิยมระดับสูง และมีการใช้งานอย่างแพร่หลายอย่างผลิตภัณฑ์ของ Apple และ Adobe เริ่มตกเป็นเหยื่อมากขึ้นอย่างชัดเจน ผู้ใช้ผลิตภัณฑ์ของทั้ง Apple และ Adobe ควรปกป้องเครื่อง และอุปกรณ์พกพาจาก Malware ที่ใช้ประโยชน์จากช่องโหว่ของผลิตภัณฑ์ดังกล่าวด้วย

อ่านต่อฉบับหน้า