ก้าวทันภัยคุกคามด้านไอที

แม้เทคโนโลยีการรักษาความปลอดภัยด้านไอทีจะก้าวหน้าไปอย่างมาก แต่ภัยคุกคามและกลุ่มอาชญากรในโลกไซเบอร์นั้นก็มีนำเทคโนโลยีที่ทันสมัยและเทคนิคการหลบหลีกรูปแบบใหม่ๆ มาใช้อย่างต่อเนื่อง ทำให้ในช่วงที่ผ่านมาเราอาจจะได้ยินข่าวองค์กรโดนท้าทายมาตรการรักษาความปลอดภัยในรูปแบบต่างๆ และกลายเป็นภาระอันหนักอึ้งที่ฝ่ายไอที ผู้บริหารและพนักงงานผู้มีส่วนเกี่ยวข้องต้องรับมือ

ท่ามกลางสถานการณ์ภัยคุกคามทั่วโลกในปัจจุบัน องค์กรธุรกิจและหน่วยงานราชการจำเป็นที่จะต้องมีความตื่นตัวมากขึ้น และจะต้องปรับปรุงนโยบายด้านความปลอดภัยให้ทันสมัย ขณะที่ประเทศไทยกำลังพัฒนาไปสู่เศรษฐกิจดิจิตอล ผู้บริหารฝ่ายรักษาความปลอดภัยจำเป็นที่จะต้องมีบทบาทในคณะกรรมการบริหารขององค์กร เพราะปัญหาข้อมูลรั่วไหลอาจสร้างความเสียหายอย่างมากมายมหาศาลต่อธุรกิจ ประเทศไทยครองอันดับ 3 ของโลกในแง่ภัยคุกคามทางไซเบอร์ (ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย – ThaiCERT, มิถุนายน 2558)

รายงานจาก ThaiCERT ระบุว่า ในปี 2558 อาชญากรรมออนไลน์ราว 34.5% เกี่ยวข้องกับโค้ดอันตราย ขณะที่ 26.3 % และ 23.3% เกี่ยวข้องกับการฉ้อโกงและการบุกรุกระบบตามลำดับ เป็นเรื่องที่น่าเศร้าที่พบว่าองค์กรที่ถูกโจมตีมากที่สุดคือ หน่วยงานของรัฐ และสถาบันการศึกษา ที่จริงแล้ว ทุกๆ องค์กรล้วนมีความเสี่ยง และถือ

เป็นภารกิจระดับชาติในการสร้างระบบเศรษฐกิจที่มีความมั่นคงปลอดภัย ขณะที่ประเทศไทยกำลังพัฒนาสู่การเป็นประเทศดิจิตอลที่มีการเชื่อมต่อถึงกันอย่างทั่วถึง”

โดยรายงานภัยคุกคามด้านไอทีที่น่าสนใจมีดังนี้

- การโจมตีทางไซเบอร์ก่อให้เกิดค่าใช้จ่ายเพิ่มมากขึ้นและรับมือได้ยากกว่าเดิม ในช่วงปีที่ผ่านมา ค่าใช้จ่ายโดยเฉลี่ยของการละเมิดด้านความปลอดภัยเพิ่มเป็น 5.9 ล้านดอลลาร์ หรือ 213 ล้านบาท แต่ที่สำคัญกว่านั้นก็คือ เวลาเฉลี่ยที่ใช้ในการแก้ปัญหาการโจมตีทางไซเบอร์ในปัจจุบันอยู่ที่ 45 วัน ซึ่งเพิ่มขึ้นเกือบ 50% เมื่อเทียบกับหนึ่งปีที่แล้ว
- องค์กรไม่สามารถตรวจพบการละเมิดได้อย่างทันท่วงที อาจใช้เวลากว่า 2 ปีสำหรับบางองค์กรกว่าที่จะสามารถตรวจพบการละเมิด ขณะที่บริษัทกว่าครึ่งหนึ่งไม่สามารถระบุจุดที่มีการบุกรุกได้อย่างแน่ชัด
- เว็บ เครือข่าย และอีเมล คือ 3 ช่องทางหลักที่โดนโจมตีมากที่สุด ทั้ง 3 ช่องทางนี้ได้รับการใช้งานอย่างแพร่หลายในปัจจุบัน โดยเฉพาะอย่างยิ่งในเอเชียแปซิฟิก ซึ่งอัตราการใช้งานอินเทอร์เน็ตและโทรศัพท์เคลื่อนที่อยู่ในระดับที่สูง
- การแฮ็กระบบเป็นสาเหตุหลักของการเกิดช่องโหว่ ตามมาติดๆ ด้วยมัลแวร์และโซเชียลมีเดีย โดยนักวิเคราะห์ระบุว่าโซเชียลมีเดียเป็นปัจจัยสำคัญที่ก่อให้เกิดการหยุดชะงักในโลกปัจจุบันที่มีการเชื่อมต่อถึงกันอย่างใกล้ชิด
- เมื่อปีที่แล้ว ธุรกิจค้าปลีกถูกโจมตีหนักที่สุดความเสียหายสูงถึง 245 ล้านดอลลาร์ รองลงมาได้แก่ ธุรกิจบริการด้านการเงิน (80 ล้านดอลลาร์) และการแพทย์ (4.5 ล้านดอลลาร์)
- โมบายล์มัลแวร์คือช่องทางใหม่สำหรับผู้โจมตี ขณะเดียวกัน 99% ของซอฟต์แวร์อันตรายเหล่านี้พุ่งเป้าไปที่ระบบปฏิบัติการ Android ในปี 2556
- Flash กลับมาอีกครั้ง การโจมตีช่องโหว่ของ Adobe Flash ซึ่งรวมอยู่ในชุดเครื่องมือสำหรับการโจมตี Angler และ Nuclear มีแนวโน้มเพิ่มสูงขึ้น
- วิวัฒนาการของมัลแวร์เรียกค่าไถ่ มัลแวร์เรียกค่าไถ่ (Ransomware) ยังคงสร้างรายได้เป็นกอบเป็นกำให้แก่แฮกเกอร์ และมีการเผยแพร่มัลแวร์ชนิดนี้รุ่นใหม่ๆ ออกมาอย่างต่อเนื่อง
- Dridex: การโจมตีที่ปรับเปลี่ยนอย่างต่อเนื่อง ผู้สร้างแคมเปญการโจมตีที่กลายพันธุ์อย่างรวดเร็วนี้มีความเข้าใจอย่างลึกซึ้งเกี่ยวกับการหลบเลี่ยงมาตรการรักษาความปลอดภัย

เตรียมพร้อมรับมือกับการต่อสู้

จะเห็นได้ว่า ภัยคุกคามด้านไอทีสามารถสร้างความเสียหายทางธุรกิจได้อย่างน่าตกใจ ผู้ผลิตเทคโนโลยีด้านความปลอดภัยต้องทำงานอย่างหนักเพื่อพัฒนานวัตกรรมใหม่ๆ มาปกป้องลูกค้าผู้ใช้บริการ ขณะที่ผู้ใช้และองค์กรตกอยู่ในความเสี่ยงที่เพิ่มสูงขึ้น และจำเป็นที่จะต้องมีความตื่นตัวมากขึ้นในการมองหาโซลูชั่นการรักษาความปลอดภัยแบบครบวงจรที่จะช่วยให้องค์กรต่างๆ สามารถดำเนินการป้องกันเชิงรุก รวมทั้งปรับเปลี่ยนบุคลากร กระบวนการ เทคโนโลยีให้สอดคล้องกัน

บทความจาก CAT club เดือน พฤศจิกายน 2558