รายงานระดับช่องโหว่ไซเบอร์ทั่วโลก กระตุ้นองค์กรเพิ่มนวัตกรรมรับมือการรักษาความปลอดภัย

การจัดอันดับข้อมูล “ไซเบอร์ ซีเคียวริตี้” ขององค์กรครั้งล่าสุด เผยให้เห็นถึงภาคอุตสาหกรรมที่ถูกพุ่งเป้าโจมตีมากที่สุด พร้อมแนวทางการรับมือภัยคุกคามที่มีการพัฒนาอยู่ตลอดเวลาได้อย่างมีประสิทธิภาพ

ไดเมนชั่น ดาต้า บริษัทผู้จัดจำหน่ายและให้บริการแบบครบวงจรด้านเทคโนโลยีสารสนเทศระดับโลก ทั้งการออกแบบ ติดตั้ง การให้คำปรึกษา และให้บริการด้านการจัดการระบบแบบไฮบริดไอที ที่ในปัจจุบันมีธุรกิจทั่วโลกมูลค่ากว่า 8 พันล้านเหรียญสหรัฐฯ เปิดเผยการค้นพบที่น่าสนใจจากรายงานภัยคุกคามข้อมูลทั่วโลก ปี 2562 (Global Threat Intelligence Report 2019 : GTIR) ของ NTT Security ซึ่งเกี่ยวข้องกับการกำหนดมาตรการด้านการรักษาความปลอดภัยทางไซเบอร์ในองค์กร รวมถึงภาคส่วนต่างๆ

จากผลสำรวจทั่วโลก ระดับความมั่นคงทางการรักษาความปลอดภัยบนไซเบอร์ (cybersecurity) โดยเฉลี่ยอยู่ที่ระดับ 1.45 จาก 5 ระดับ โดยระดับคะแนนจะถูกวัดโดยวิธีการที่กำหนดแบบองค์รวมจากกระบวนการรักษาความปลอดภัยทางไซเบอร์ขององค์กร รวมถึงกระบวนการ ตัวชี้วัดต่างๆ และกลยุทธ์การป้องกันในภาพรวม โดยสิ่งที่เกิดขึ้นพบว่าในช่วงระยะเวลาหนึ่งมีช่องโหว่จากการถูกโจมตีพุ่งสูงขึ้นเป็นประวัติการณ์ (เพิ่มขึ้นถึงร้อยละ 12.5 จากปี 2560)

โดยอันดับสูงสุด ได้แก่ ภาคการเงิน (1.71) และกลุ่มเทคโนโลยี (1.66) ซึ่งยังคงเพิ่มระดับความแข็งแกร่งบนระบบรักษาความปลอดภัยอย่างต่อเนื่อง ซึ่งเป็นไปได้ว่ากลุ่มอุตสาหกรรมดังกล่าวได้รับการแจ้งเตือนถึงสถานะที่จะถูกพุ่งเป้าโจมตีมากที่สุด โดยคิดเป็นร้อยละ 17 ของการโจมตีทั้งหมดที่บันทึกไว้ในปี 2561

ในงานวิจัยที่ได้จากการบันทึกข้อมูลกว่าล้านล้านครั้ง และการโจมตีกว่าพันล้านครั้ง เปิดเผยถึงประเภทการโจมตีด้วยวิธีการโจมตีเว็บ หรือ web attack ซึ่งเป็นภัยคุกคามที่แพร่หลายมากที่สุด มีความถี่เพิ่มขึ้นเป็นสองเท่าตั้งแต่ปี 2560 คิดเป็นร้อยละ 32 ของการโจมตีทั้งหมดจากการตรวจพบเมื่อปีที่แล้ว โดยการโจมตีมาในรูปแบบสอดแนมเพื่อหาช่องโหว่เจาะเข้าระบบ หรือ Reconnaissance (ร้อยละ 16) ซึ่งเป็นรูปแบบที่พบมากที่สุด รองลงมาคือการมุ่งโจมตีในบริการเฉพาะด้าน หรือ service-specific attacks (ร้อยละ 13) และการโจมตีแบบสุ่มรหัสผ่าน หรือ brute-force (ร้อยละ 12)

นายเนวิลล์ เบอร์ดาน ผู้อำนวยการด้านการรักษาความปลอดภัยทางไซเบอร์ ของ Dimension Data Asia Pacific

กล่าวว่า ในองค์กรทุกภาคส่วนหันมาให้ความสำคัญและมีการดำเนินงานที่ชัดเจนเพื่อสร้างระบบรักษาความปลอดภัยที่แข็งแกร่งยิ่งขึ้น อย่างไรก็ตามเรามั่นใจว่าจะเห็นผู้นำ ในฐานะผู้บริหารระดับสูงหลายท่านได้ตระหนักถึงความสำคัญของการลงทุนเชิงกลยุทธ์เพื่อปรับปรุงการป้องกันความปลอดภัยทางไซเบอร์ในองค์กรของพวกเขาอย่างเต็มศักยภาพ

“มีการเปลี่ยนแปลงเพื่อพัฒนาที่น่าสนใจในส่วนของข้อมูลการคาดการณ์พื้นที่ภัยคุกคาม ด้วยระดับใหม่ของการร่วมมือ และห่วงโซ่ของระบบรักษาความปลอดภัยทางไซเบอร์ ที่มากไปกว่านั้นคือในอุตสาหกรรมที่มีการกำหนดเป้าหมายที่ชัดเจนมากที่สุด มีแนวโน้มที่จะขอคำปรึกษาเพื่อปรับกลยุทธ์และสร้างโปรแกรมการรักษาความปลอดภัยให้สอดรับกับความต้องการขององค์กรให้มีประสิทธิภาพมากยิ่งขึ้น ซึ่งเป็นแนวโน้มที่ดีสำหรับองค์กรที่ต้องการเข้าถึงสถานะความปลอดภัยทางไซเบอร์อย่างแท้จริง” นายเบอร์ดาน กล่าวสรุป

สิ่งที่น่าสนใจจากผลการวิจัยในภาพรวม

• จากทั่วโลก คิดเป็นร้อยละ 35 ของการโจมตีที่เกิดจาก IP addresses ในสหรัฐอเมริกา และจีน ตามด้วย ทวีปยุโรปตะวันออกกลาง แอฟริกา และเอเชียแปซิฟิก

• การลักลอบใช้ทรัพยากรคอมพิวเตอร์ (Cryptojacking) แสดงถึงกิจกรรมหรือการใช้งานที่ซุ่มเสี่ยงต่อการถูกโจมตีอยู่เป็นจำนวนมาก ในบางครั้งการตรวจจับแต่ละ accounting มีมากกว่าการตรวจจับมัลแวร์ทั้งหมดรวมกัน ทั้งนี้ในภาคเทคโนโลยีและการศึกษานั้นทำได้ยากที่สุด

• การโจรกรรมข้อมูลส่วนตัวขึ้นอยู่กับผู้โจมตีกำหนดกลุ่มเป้าหมายที่มีข้อมูลรับรองบนคลาวด์ โดยในกลุ่มเทคโนโลยี คิดเป็นร้อยละ 36, กลุ่มโทรคมนาคม (ร้อยละ 18) และกลุ่มธุรกิจและบริการด้านวิชาชีพ (ร้อยละ 14) ที่จะได้รับผลกระทบอย่างเห็นได้ชัด

Click here เพื่อดาวน์โหลด Dimension Data Executive Guide รายงานความปลอดภัยข้อมูลทั่วโลกของ NTT Security 2019