องค์กรในไทยพร้อมมองหาแนวทางการรักษาความปลอดภัยรูปแบบอื่น

องค์กรในไทยพร้อมมองหาแนวทางการรักษาความปลอดภัยรูปแบบอื่น
นอกเหนือจากโปรแกรมป้องกันมัลแวร์

กรุงเทพฯ, 20 ตุลาคม, 2558 – บุคลากรฝ่ายรักษาความปลอดภัยเริ่มตระหนักเพิ่มมากขึ้นว่าเพียงแค่การติดตั้งโปรแกรมป้องกันมัลแวร์บนอุปกรณ์ลูกข่ายไม่ใช่มาตรการที่เพียงพอ ทั้งนี้ ผู้ตอบแบบสอบถามในไทยมากถึง 95.5% ระบุว่าตนเองสนใจที่จะใช้มาตรการเพิ่มเติมอื่นๆ เช่น การตรวจจับภัยคุกคามโดยดูจากลักษณะการทำงาน และแซนด์บ็อกซ์ (29.4%) การป้องกันช่องโหว่ (24.5%) การตรวจสอบอุปกรณ์ลูกข่าย (22.9%) และการสร้างรายการแอพพลิเคชั่นที่ปลอดภัย (18.7%) ภายในองค์กร ซึ่งแสดงให้เห็นถึงพัฒนาการของปัญหาด้านความปลอดภัยตลอดช่วงระยะเวลาหลายปีที่ผ่านมา และนำไปสู่การจัดลำดับความสำคัญที่แตกต่างกันภายในองค์กร ขณะเดียวกัน มีผู้ตอบแบบสอบถามเพียง 4.5% เท่านั้นที่ยืนยันว่าจะยังคงใช้เฉพาะซอฟต์แวร์ป้องกันมัลแวร์ที่อ้างอิงฐานข้อมูลที่มีอยู่ต่อไป
การสำรวจความคิดเห็นนี้ดำเนินการโดยเทรนด์ไมโคร ซึ่งเป็นผู้นำระดับโลกด้านการรักษาความปลอดภัยบนระบบคลาวด์ โดยมีผู้ตอบแบบสอบถาม 244 คนจากหลากหลายกลุ่มอุตสาหกรรม เช่น เทคโนโลยี การเงิน และอุตสาหกรรมการผลิต ระหว่างการประชุมด้านความปลอดภัยอินเทอร์เน็ต CLOUDSEC ประจำปี 2558 ที่จัดขึ้นที่กรุงเทพฯ เมื่อไม่นานมานี้

นอกจากนี้ ผลการสำรวจยังระบุว่า แนวโน้มต่างๆ เช่น การเก็บข้อมูลและการประสานงานร่วมกันบนระบบคลาวด์ (22%), โมบิลิตี้ (21.7%) และเซิร์ฟเวอร์เวอร์ช่วลไลเซชั่น (21.4%) ก่อให้เกิดปัญหาท้าทายด้านความปลอดภัยมากที่สุดสำหรับบริษัทต่างๆ ปัญหาความไม่สอดคล้องในองค์กร เช่น พนักงานมีความตระหนักรับรู้ในระดับที่ต่ำ (31.8%), ขาดแคลนบุคลากรที่เชี่ยวชาญ (14.4%) และปัญหาท้าทายด้านการดำเนินงานระหว่างแผนกรักษาความปลอดภัยและแผนกไอที (13.8%) ยังคงเป็นปัญหาที่สร้างความกังวลใจสูงสุด
ด้วยเหตุนี้ จึงมีผู้ตอบแบบสอบถามเพียง 24.4% เท่านั้นที่เชื่อมั่นว่าตนเองเตรียมพร้อมที่จะรับมือกับการโจมตีทางไซเบอร์ โดยส่วนใหญ่ (61.5%) รู้สึกว่าตนเอง “ค่อนข้างจะมีความพร้อม”
“ท่ามกลางสถานการณ์ดิจิตอลในปัจจุบัน มีการใช้งานระบบคลาวด์คอมพิวติ้ง ระบบเวอร์ช่วลไลเซชั่น และระบบโมบิลิตี้สำหรับบุคลากรในองค์กรอย่างกว้างขวาง และมีอุปกรณ์จำนวนมากที่เชื่อมต่อเข้ากับเครือข่ายขององค์กร ด้วยเหตุนี้ องค์กรต่างๆ จึงเสี่ยงที่จะถูกโจมตีผ่านทางช่องโหว่ของอุปกรณ์ลูกข่าย ขณะที่ภัยคุกคามมีความซับซ้อนและ

ปริมาณเพิ่มมากขึ้น ด้วยเหตุนี้ ลำพังเพียงแค่การปกป้องอุปกรณ์ลูกข่ายจึงไม่เพียงพออีกต่อไป ในปัจจุบัน เราจึงจำเป็นที่จะต้องเลือกใช้ยุทธศาสตร์การป้องกันโดยรอบเพื่อปกป้ององค์กรอย่างทั่วถึง” ธันยา ทักการ์ กรรมการผู้จัดการประจำภูมิภาค APAC ของเทรนด์ไมโคร กล่าว

ในยุคที่เกิดกรณีข้อมูลรั่วไหลก่อให้เกิดค่าใช้จ่ายสูงถึง 3.8 ล้านดอลลาร์ ไม่ใช่เรื่องน่าแปลกใจเลยที่ปัญหาเรื่องความปลอดภัยของข้อมูล (54.9%) และความเป็นส่วนตัวของข้อมูล (28.5%) เป็นปัญหาสำคัญที่สุดสำหรับบุคลากรฝ่ายรักษาความปลอดภัย ในส่วนที่เกี่ยวกับการทำงานบนระบบคลาวด์ และจากการสำรวจความคิดเห็น ยังพบอีกว่าการปฏิบัติตามกฎระเบียบ (15.9%) เป็นอีกหนึ่งปัญหาสำคัญสำหรับการทำงานบนระบบคลาวด์

เนื่องจากปัจจุบันการโจมตีทางไซเบอร์มีความรุนแรงและความถี่เพิ่มมากขึ้นอย่างต่อเนื่อง ดังนั้นองค์กรต่างๆ จึงจำเป็นต้องแก้ไขปัญหาที่ระบุข้างต้นอย่างเร่งด่วน กระบวนการปฏิรูปทางดิจิตอล ซึ่งหลายๆ บริษัทกำลังดำเนินการอยู่ในทุกวันนี้ นับเป็นโอกาสที่ดีสำหรับการแก้ไขปัญหาเรื่องความปลอดภัย โดยอาศัยแนวทางที่รอบด้าน และผนวกรวมการรักษาความปลอดภัยเข้าไว้เป็นส่วนหนึ่งในโครงสร้างหลักขององค์กร

เกี่ยวกับเทรนด์ ไมโคร
บริษัท เทรนด์ ไมโคร ผู้นำระดับโลกในด้านซอฟต์แวร์ความปลอดภัย มุ่งมั่นที่จะสร้างโลกที่ปลอดภัยสำหรับการแลกเปลี่ยนข้อมูลดิจิตอล จากประสบการณ์มากกว่า 25 ปีของเรา โซลูชั่นของเราได้ให้บริการทั้งสำหรับผู้ใช้ทั่วไป องค์กรธุรกิจ และหน่วยงานภาครัฐ โดยนำเสนอระบบรักษาความปลอดภัยในการปกป้องข้อมูลแบบแบ่งระดับชั้น [Layered content security] ในอุปกรณ์พกพา อุปกรณ์ลูกข่าย เกตเวย์ เซิร์ฟเวอร์ และระบบคลาวด์ โซลูชั่นทั้งหมดของเราขับเคลื่อนด้วย Trend Micro™ Smart Protection Network™ ซึ่งเป็นเครือข่ายข้อมูลเกี่ยวกับภัยคุกคามทั่วโลกบนระบบคลาวด์ พร้อมการสนับสนุนจากผู้เชี่ยวชาญด้านภัยคุกคามกว่า 1,200 คนทั่วโลก ดูข้อมูลเพิ่มเติมได้ที่ www.trendmicro.co.th
##############################

ติดต่อข้อมูลประชาสัมพันธ์
จารุวรรณ ฤกษ์พิชญโยธิน
บริษัท เทรนด์ไมโคร (ประเทศไทย) จำกัด
+662 646 1968,
jaruwan_r@trendmicro.com

วราวอง จงรักษ์
ดุษฎี เย็นสุดใจ
บริษัท เอฟเอคิว จำกัด: +662 971 3700
Trendmicrothpr@faq.co.th