# ผลวิจัยแคสเปอร์สกี้เผย ธุรกิจส่วนใหญ่ในอาเซียนตั้งเป้าปรับปรุงความปลอดภัยไอทีเตรียมไว้ก่อนจะสาย

น่าหวั่นใจ มากกว่า 1 ใน 10 ใช้ฟรีซอฟต์แวร์ และเกือบ 2 ใน 10 ใช้ซอฟต์แวร์ที่ใช้ตามบ้านมาป้องกันระบบไอทีขององค์กร

จากการทะลวงล้วงเอาข้อมูลจากเอ็นเตอร์ไพรซ์ระดับชั้นนำแถวหน้าของภูมิภาคเอเชียตะวันออกเฉียงใต้ (SEA) ที่ผ่านมา ได้เป็นตัวกระตุ้นความเต็มใจจากเหล่าบรรดาเจ้าของธุรกิจให้หันมาลงทุนอย่างจริงจังมากขึ้นกับระบบความปลอดภัยทางไซเบอร์ ยืนยันจากผลการสำรวจล่าสุดจัดทำโดยแคสเปอร์สกี้ การวิจัยประจำปีนี้เผยข้อมูลว่า 79% ของผู้เข้าร่วมการสำรวจจากภูมิภาคได้ยืนยันหนักแน่นว่ามีแผนการที่จะยกระดับความเข้มข้นของระบบความปลอดภัยของตน ไม่เกี่ยงเรื่องผลตอบแทนจากการลงทุน โดยให้เหตุผลว่าปลอดภัยไว้ก่อนดีกว่ามาเสียใจภายหลัง

หลังการสัมภาษณ์ผู้บริหารงานไอทีระดับผู้ตัดสินใจทั่วโลก รวมทั้งอีกเกือบ 300 รายในเอเชียตะวันออกเฉียงใต้ พบว่าส่วนใหญ่ (96%) ของเวิร์กสเตชั่นที่ติดตั้งอยู่ในภูมิภาคนี้นั้นจะลง endpoint security solutions เอาไว้ เป็นตัวเลขที่สูงกว่าเกณฑ์เฉลี่ยของเอเชียแปซิฟิกนิดหน่อยที่ 92% และ 87% ทั่วโลก

เป็นที่น่าสนใจว่า มากกว่า 1-ใน-10 ของโซลูชั่นเพื่อความปลอดภัยที่ใช้งานกันอยู่ตามธุรกิจระดับ SMBs และเอ็นเตอร์ไพรซ์ในภูมิภาคนั้นเป็นซอฟต์แวร์แบบให้เปล่าไม่มีค่าใช้จ่าย อีก 19.5% ของผู้เข้าร่วมการสำรวจยอมรับว่า

ได้ลงโซลูชั่นที่มีไลเซ่นส์ถูกต้อง แต่เป็นแบบสำหรับใช้ในบ้านเท่านั้น

นายโยว เชียง เทียง ผู้จัดการทั่วไป บริษัท แคสเปอร์สกี้ ประจำภูมิภาคเอเชียตะวันออกเฉียงใต้ กล่าวว่า “เป็นเรื่องที่น่าชื่นชมที่ได้รู้ว่ามีธุรกิจมากขึ้นในภูมิภาคที่เห็นคุณค่าของการเสริมความแข็งแกร่งให้กับศักยภาพของการป้องกันตัวเองให้พ้นภัยไซเบอร์ ความเต็มใจที่จะเพิ่มอัตราการลงทุนก็เป็นเรื่องสำคัญอย่างไม่น่าสงสัยเลย อย่างไรก็ตาม ก็ยังเป็นเรื่องน่าตระหนกที่ยังมีธุรกิจจำนวนไม่น้อย ที่ยังละเลยใช้เอ็นด์พอยต์ซีเคียวริตี้แบบให้ฟรี หรือใช้โซลูชั่นที่ควรจะสำหรับการใช้งานรายบุคคลตามบ้านเท่านั้น”

“เอ็นด์พอยต์โซลูชั่นแบบแจกฟรีไม่มีค่าใช้จ่ายนั้นอาจจะให้การป้องกันจากไวรัสทั่วไป แต่การกระทำแบบนี้ทำให้ระบบขององค์กรเปิดรับโอกาสที่จะเกิดความเสียหายจากสิ่งที่เราไม่รู้ และภัยไซเบอร์ที่มีความซับซ้อนได้มากกว่าเดิมด้วยซ้ำ เน็ตเวิร์กขององค์กรธุรกิจมีความซับซ้อนกว่าระบบอินเตอร์เน็ตที่เราใช้งานตามบ้าน และเมื่อพิจารณาถึงข้อมูลที่มีความอ่อนไหวของธุรกิจ ที่ใช้ทำงานกันอยู่ตามจุปฏิบัติงานไม่ว่าจะเป็นระดับ SMBs และองค์กรขนาดใหญ่ ก็ตาม การใช้ซอฟต์แวร์ฟรีหรือซอฟต์แวร์รายบุคคล สามรถกลายมาเป็นจุดอ่อนดึงระบบธุรกิจและที่เกี่ยวข้องทั้งหมดให้อยู่ในความเสี่ยงได้เลย” นายโยวอธิบายเพิ่มเติม

สำหรับในส่วนการสำรวจเกี่ยวกับบุคลากรด้านไอที เกือบ 4-ใน-10 (39.8%) ของธุรกิจในเอเชียตะวันออกเฉียงใต้จะมีพนักงานสองในเก้าคนที่ดูแลงานด้านระบบความปลอดภัยไอที ประมาณ 6.7% ใช้พนักงานจำนวนหนึ่งคนเท่านั้นบริหารจัดการสภาพแวดล้อมความปลอดภัยไซเบอร์ของทั้งองค์กร

สำหรับการสำรวจข้อมูลเมื่อปลายปีที่ผ่านมา พบว่าส่วนใหญ่ (78.3%) ของพนักงานที่ทำด้านไอทีซีเคียวริตี้จะเป็นเจ้าหน้าที่ผู้เชี่ยวชาญอินเตอร์เน็ต ขณะที่ 21.4% จะเป็นคนที่มาจากบริษัทภายนอก (เอ้าท์ซอร์ส) และอีก 11.7% เป็นเจ้าหน้าที่ทั่วไปขององค์กรนั่นเอง

ยิ่งไปกว่านั้น การวิจัยดำเนินการโดยองค์กรเน้นด้านความปลอดภัยไซเบอร์ระดับโลก ยังเปิดเผยข้อมูลอีกด้วยว่าเกือบกึ่งหนึ่ง (42%) ของธุรกิจในเอเชียตะวันออกเฉียงใต้มีความไม่มั่นใจในนโยบายที่จะต่อกรรับมือภัยคุกคามที่มีความซับซ้อน

“ยอมรับเถอะว่า การล่วงละเมิดข้อมูล (data breaches) เกิดกับใครก็ได้ โดยเฉพาะอย่างยิ่งในยุคนี้ที่บรรดาธุรกิจต่างก็ถูกบีบให้เปลี่ยนตัวเองสู่รูปแบบดิจิทัลกันอย่างรวดเร็ว ซึ่งจริงๆ แล้วก็ไม่ใช่เรื่องไม่ดี แต่เป็นความท้าทายที่ต้องหาทางจัดการให้ได้ เอ็นด์พอยต์โซลูชั่นจะทำหน้าที่เป็นพื้นฐานของโครงสร้างระบบความปลอดภัยขององค์กร การผนวกประสานทูลที่มีประสิทธิภาพเข้ากับข้อมูลวิเคราะห์เจาะลึกภัยไซเบอร์จะสามารถสนับสนุนการสร้างเน็ตเวิร์กระบบไอทีที่ปลอดภัยสำหรับการใช้งานได้มากกว่าสำหรับองค์กรทุกๆ ประเภท” นายโยวกล่าวเสริม

ผู้เชี่ยวชาญจากแคสเปอร์สกี้ก็มีคำแนะนำสำหรับองค์กรธุรกิจในการติดตั้งระบบป้องกันไอทีให้องค์กร ดังนี้:
 จัดเทรนนิ่งและพูดคุยกับพนักงานให้เข้าใจถึงไซเบอร์ซีเคียวริตี้ ทุกคนต้องเข้าใจกฎระเบียบและความคาดหวังใน

การปฏิบัติตนเกี่ยวกับทุกๆ จุด ตั้งแต่พาสเวิร์ดไปจนถึงความเป็นส่วนตัวของข้อมูลของลูกค้า ตั้งแต่เทคโนโลยีการป้องกันไปจนกระทั่งการจัดลำดับความสำคัญข้อมูล

 ประเมินความเสี่ยงไซเบอร์ซีเคียวริตี้ขององค์กรเวลาที่จัดทำงบประมาณ พิจารณาค่าใช้จ่ายและความน่าจะเป็น

 พึ่งพาผู้เชี่ยวชาญ การตัดสินใจเกี่ยวกับการจัดซื้อไซเบอร์ซีเคียวริตี้ทูล หรือบริการนั้นไม่เป็นการตัดสินใจของคนเดียว ก่อนจะมาถึงขั้นตอนนี้ ควรจะต้องมีกระบวนการวิเคราะห์โดยผู้เชี่ยวชาญเพื่อนำเสนอตัวเลือกในราคาที่เหมาะสมที่สุด

 ติดตั้งซอฟต์แวร์เพื่อความปลอดภัยที่ครบถ้วนในทุกจุด – เซิร์ฟเวอร์ เครื่องคอมพิวเตอร์ใช้งาน ดีไวซ์ต่างๆ ที่มาต่อเชื่อม เช่น Kaspersky Endpoint Security for Business ซึ่งประกอบขึ้นด้วยฟีเจอร์แบบมัลติเลเยอร์ในหนึ่งโซลูชั่น สำหรับการลงทุนซื้อในครั้งเดียว และยังป้องกัน exploits และการโจมตีแบบ file-less และเซ็ตฟีเจอร์แอนตี้แรนซั่มแวร์ที่สมบูรณ์ที่สุดในโลก

 ตั้งค่าเอ็นด์พอยต์โซลูชั่นของคุณให้ทันสมัยอยู่เสมอ และต่ออายุให้ตรงเวลา

การวิจัยเรื่อง Kaspersky Global Corporate IT Security Risks Survey (ITSRS) เป็นการสำรวจผู้มีอำนาจตัดสินใจด้านไอทีขององค์กรต่างๆ ทั่วโลก ซึ่งได้จัดทำต่อเนื่องกันเป็นปีที่ 9 แล้ว แคสเปอร์สกี้ได้สัมภาษณ์ผู้มีอำนาจตัดสินใจด้านไอทีทั้งสิ้น 4,958 ราย จาก 23 ประเทศ ในภูมิภาคละตินอเมริกา ยุโรป อเมริกาเหนือ เอเชียแปซิฟิก รวมถึงจีน ญี่ปุ่น รัสเซีย และตะวันออกกลาง รวมตุรกีและแอฟริกา ผู้เข้าร่วมการสำรวจจะถูกสอบถามเกี่ยวกับสถานะความปลอดภัยไอทีภายในองค์กร ประเภทของภัยคุกคามที่ประสบ และค่าเสียหายในการจัดการฟื้นฟูจากการถูกโจมตี