9 ใน 10 ของการรั่วไหลของข้อมูลในคลาวด์เกิดจากฝีมือคน

รายงานใหม่ล่าสุด ‘Understanding security of the cloud: from adoption benefits to threats and concerns’ จาก Kaspersky Lab ระบุว่าเหตุที่มีข้อมูลรั่วไหลที่เกิดขึ้นในโครงสร้างพื้นฐานคลาวด์สาธารณะ ส่วนใหญ่เกิดจากพนักงานของลูกค้ามากกว่าการกระทำที่เกิดจากผู้ให้บริการคลาวด์ องค์กรต่าง ๆ คาดหวังให้ผู้บริการคลาวด์เป็นผู้รับผิดชอบกับความปลอดภัยของข้อมูลที่เก็บไว้บนแพลตฟอร์มคลาวด์ อย่างไรก็ตาม 90% (องค์กรธุรกิจขนาดเล็กและขนาดกลาง 88% และองค์กรธุรกิจขนาดใหญ่ 91%) ของการรั่วไหลของข้อมูลในคลาวด์เกิดขึ้นเพราะการสร้างเทคนิคต่าง ๆ โดยลูกค้า พนักงาน ไม่ได้เกิดจากผู้ให้บริการคลาวด์

การใช้งานคลาวด์ทำให้องค์กรมีกระบวนการในการทำธุรกิจที่คล่องตัวขึ้น ลด CAPEX และจัดการด้านไอทีได้เร็วขึ้น อย่างไรก็ตามพวกเขาก็ยังคงกังวลถึงโครงสร้างพื้นฐานของคลาวด์และความปลอดภัยของข้อมูล อย่างน้อย 1 ใน 3 ขององค์กรธุรกิจ (องค์กรธุรกิจขนาดเล็กและขนาดกลาง 88% และองค์กรธุรกิจขนาดใหญ่ 91%) คำนึงถึงอุบัติการณ์ที่จะเกิดกับโครงสร้างพื้นฐานที่โฮสต์โดยบุคคลที่สาม ผลที่ตามมาของอุบัติการณ์อาจทำให้เกิดขึ้นซ้ำ และจะเกิดความเสียหายต่อการค้าและเสี่ยงต่อภาพลักษณ์เสียหายได้อีกด้วย

ถึงแม้ว่าองค์กรต่าง ๆ จะกังวลถึงความสมบูรณ์ของแพลตฟอร์มคลาวด์ภายนอก แต่พวกเขามีแนวโน้มที่จะได้รับผลกระทบจากจุดอ่อนแอภายใน ซึ่ง 33% ของเหตุการณ์ข้อมูลรั่วไหลในคลาวด์เป็นเพราะเทคนิคของวิศวกรรมทางสังคมที่มีผลต่อพฤติกรรมของพนักงาน ในขณะที่มีเพียง 11% เท่านั้นที่เกิดจากผู้ให้บริการคลาวด์

ผลสำรวจชี้ว่ายังมีส่วนที่สามารถปรับปรุงได้อีกเพื่อให้มั่นใจได้ว่าความปลอดภัยทางอินเทอร์เน็ตมีเสถียรภาพเมื่อทำงานกับบุคคลที่สาม โดย 39% ขององค์กรธุรกิจขนาดเล็กและขนาดกลาง และ 47% ขององค์กรธุรกิจขนาดใหญ่ที่ใช้ระบบคลาวด์ที่ได้รับการปรับแต่งด้านการป้องกันความปลอดภัย ซึ่งอาจเป็นผลมาจากองค์กรส่วนใหญ่เชื่อมั่นในความปลอดภัยในโครงสร้างพื้นฐานจากผู้ให้บริการคลาวด์นั่นเอง หรือไม่ก็พวกเขามีความเข้าใจที่ผิดว่ามาตรฐานของการรักษาความปลอดภัยปลายทางทำงานได้อย่างราบรื่น ภายใต้สภาพแวดล้อม โดยมิได้ทำให้ประสิทธิภาพของคลาวด์ลดลง

“สิ่งที่องค์กรควรคำนึงถึงอันดับแรกก่อนที่จะย้ายข้อมูลไปยังแพลตฟอร์มคลาวด์สาธารณะ ต้องทราบว่าใครเป็นผู้รับผิดชอบต่อข้อมูลขององค์กร ส่วนใหญ่แล้วผู้ให้บริการจะเป็นผู้รับผิดชอบในการรักษาความปลอดภัยในแพลตฟอร์มคลาวด์ของลูกค้า แต่เมื่อมีภัยคุกคามเกิดขึ้นจากฝั่งของลูกค้า จะไม่ใช่ความรับผิดชอบของผู้ให้บริการคลาวด์อีกต่อ

ไป การวิจัยของเราแสดงให้เห็นว่าองค์กรควรให้ความสำคัญกับสุขอนามัยด้านความปลอดภัยออนไลน์ของพนักงาน และมีมาตรการที่จะต้องรักษาความปลอดต่อสภาพแวดล้อมของคลาวด์จากภายในอีกด้วย” แม็กซิม ฟรอลอฟ รองประธานฝ่ายขายโกลบอล Kaspersky Lab กล่าว

มาตรการและข้อแนะนำจาก Kaspersky Lab เพื่อให้มั่นใจได้ว่าข้อมูลที่อยู่ในคลาวด์ปลอดภัย

• ชี้แจงให้พนักงานทราบว่าพวกเขาสามารถกลายเป็นเหยื่อของอาชญากรออนไลน์ได้ พวกเขาไม่ควรเข้าไปคลิกลิงก์หรือเปิดไฟล์ที่แนบมาจากผู้ส่งที่ไม่รู้จัก ตอกย้ำการตระหนักด้วยการจัดอบรม เช่น Kaspersky Security Awareness สามารถช่วยได้

• ลดความเสี่ยงในการใช้แพลตฟอร์มคลาวน์ที่ไม่ได้รับการอนุญาต ให้ความรู้ในด้านผลเสียที่จะเกิดขึ้น และติดตั้งกระบวนการสั่งซื้อและการใช้โครงสร้างพื้นฐานของคลาวด์ในแต่ละแผนก

• ใช้โซลูชั่นการรักษาความปลอดภัยปลายทาง เพื่อป้องกันการสร้างพาหะที่ใช้โจมตี ซึ่งควรจะรวมถึงการป้องกันเซิร์ฟเวอร์ของอีเมล อีเมลของลูกค้า และบราวเซอร์ด้วย

• ใช้การป้องกันสำหรับโครงสร้างพื้นฐานคลาวน์ของคุณทันทีหลังจากโยกย้าย เลือกระบบรักษาความปลอดภัยบนคลาวน์โดยเฉพาะ ด้วยการจัดการแบบรวมศูนย์เพื่อรักษาความปลอดภัยบนแพลตฟอร์มคลาวน์ทั้งหมด และสนับสนุนการตรวจจับโฮสต์คลาวน์โดยอัตโนมัติ รวมทั้งปรับขนาดการป้องกันในแต่ละส่วนอย่างอัตโนมัติเช่นกัน

• Kaspersky Hybrid Cloud Security ให้การรักษาความปลอดภัยต่อธุรกิจแบบหลายชั้น สำหรับสภาพแวดล้อมของคลาวด์ในหลายระบบ ความปลอดภัยทางออนไลน์แบบรวมศูนย์และการเชื่อมต่อที่ราบรื่น โซลูชั่นนี้ตรวจจับทั้งภัยคุกคามทั่วไปและภัยคุกคามที่ซับซ้อนรวมทั้งป้องกันทั้งโครงสร้างพื้นฐานของคลาวด์ด้วย ตั้งแต่แบบสภาพแวดล้อมเสมือนจริงไปจนถึงแพลตฟอร์มสาธารณะ เช่น AWS และ Microsoft Azure

รายงานฉบับเต็ม ‘Understanding security of the cloud: from adoption benefits to threats and concerns’ สามารถดูเพิ่มเติมได้ ที่นี่

เกี่ยวกับ Kaspersky Lab

Kaspersky Lab เป็นบริษัทด้านความปลอดภัยบนอินเทอร์เน็ตระดับโลก ที่ดำเนินธุรกิจมากว่า 21 ปี ด้วยความเชี่ยวชาญด้านความปลอดภัยที่ได้พัฒนามาอย่างต่อเนื่อง จนปัจจุบันเปลี่ยนเป็นโซลูชั่นความปลอดภัยยุคใหม่ ที่ให้บริการในการป้องกันสำหรับธุรกิจ โครงสร้างพื้นฐาน รัฐบาลและลูกค้าทั่วโลก การให้บริการของบริษัทประกอบด้วยการป้องกันปลายทาง โซลูชั่นการป้องกันความปลอดภัยแบบพิเศษจำนวนมาก และบริการเพื่อป้องกันภัยคุกคามดิจิทัล ซึ่ง Kaspersky Lab ได้ป้องกันความปลอดภัยให้แก่ผู้ใช้กว่า 400 ล้านคน และอีกกว่า 270,000 องค์กร ที่ป้องกันความปลอดภัยให้กับทุกส่วนที่สำคัญสำหรับลูกค้า ศึกษาข้อมูลเพิ่มเติมได้ที่ www.kaspersky.com