

เทรนด์ไมโคร เปิดตัวกลยุทธ์สมาร์ท โพรเท็คชั่น พร้อมโซลูชันใหม่ล่าสุด รุกตลาดรักษาความ ปลอดภัยสำหรับกลุ่มลูกค้าเอ็นเตอร์ไพรส์

บริษัท เทรนด์ไมโคร อินคอร์ปอเรท (TYO: 4704; TSE: 4704) พร้อมรุกตลาดรักษาความปลอดภัย ไตรมาส 2 ของปีนี้ ประกาศเปิดตัวกลยุทธ์สมาร์ท โพรเท็คชั่น พร้อมทั้งแนะนำโซลูชันใหม่ล่าสุด ได้แก่ เทคโนโลยีคัสตอม ดีเฟนส์, เซฟซิงค์, เทรนด์ไมโคร ดีพี ซีเคียวริตี้ และเทรนด์ไมโคร ซีเคียวคลาวด์ เพื่อช่วยให้องค์กรสามารถปรับกลยุทธ์ด้านความปลอดภัยเพื่อรับมือกับภัยคุกคามโลกไซเบอร์ที่ซับซ้อนมากยิ่งขึ้นได้



นางอิวา เซน ประธานเจ้าหน้าที่ฝ่ายบริหาร (ซีอีโอ) บริษัท เทรนด์ไมโคร กล่าวว่า “องค์กรต่างๆ ต้องสนับสนุนให้ธุรกิจของตนมีความยืดหยุ่นเพื่อรับมือกับภัยคุกคามที่เกิดการเปลี่ยนแปลงในปัจจุบันให้ได้ เพื่อสร้างโอกาสในการขยายตัวทางธุรกิจภายในภูมิภาคเอเชียแปซิฟิกที่กำลังเติบโต ปัจจุบันอาชญากรรมทางไซเบอร์เริ่มมีความซับซ้อน และคงอยู่ในระบบอย่างต่อเนื่อง เนื่องจากสามารถปรับให้โจมตีไปยังบุคคล ระบบ และช่องโหว่ต่างๆ ภายในองค์กรได้โดยเฉพาะ ซึ่งอีเมลฟิชชิ่งยังเป็นเครื่องมือหลักในการส่งมัลแวร์เข้าสู่ระบบ ขณะที่เทคนิคและเครื่องมือที่หลากหลาย รวมถึงโทรจันสามารถเข้าถึงได้จากระยะไกล และสามารถหลบซ่อนอยู่ภายในเครือข่ายได้อย่างยาวนาน”

จากการสำรวจผู้เชี่ยวชาญและผู้จัดการด้านไอทีกว่า 1,000 คนทั่วทั้งภูมิภาคเอเชียแปซิฟิกครั้งล่าสุด พบว่า ภัยคุกคามด้านไอทีที่ใหญ่ที่สุดคือการละเมิดข้อมูล ซึ่งเกือบครึ่งหนึ่งของผู้ตอบแบบสอบถามระบุว่าปัญหานี้ร้ายแรง และการลงทุนด้านการรักษาความปลอดภัยระดับบนยังคงเป็นการป้องกันไวรัสหรือการป้องกันมัลแวร์ และตามด้วยการป้องกันการรั่วไหลของข้อมูล ส่วน APT หรือการโจมตีแบบมีเป้าหมายถูกมองว่ามีความสำคัญน้อยในมุมมองของผู้ตอบแบบสอบถามในภูมิภาคนี้

นายเจดี เซอร์รี่ ผู้อำนวยการฝ่ายเทคโนโลยีและโซลูชัน บริษัท เทรนด์ไมโคร กล่าวว่า “ผลการสำรวจในครั้งนี้เน้นให้เห็นถึงความจำเป็นที่จะต้องให้ความรู้ในด้านการรักษาความปลอดภัยสำหรับองค์กรในภูมิภาคนี้ องค์กรต่างๆ จำเป็นที่จะต้องมีการป้องกันที่สามารถปรับแต่งได้เอง และเทรนด์ไมโครนับเป็นผู้จำหน่ายระบบรักษาความปลอดภัยรายใหญ่เพียงรายเดียวที่มีความเข้าใจใน APT ทั้งนี้องค์กรจะต้องใช้แนวทางใหม่ที่ไม่เพียงช่วยให้พวกเขาในการตรวจสอบและวิเคราะห์ APT เท่านั้น แต่จะต้องสามารถปรับการควบคุมด้านการรักษาความปลอดภัยและ

ตอบสนองต่อการโจมตีได้อย่างรวดเร็ว ทั้งนี้ Custom Defense Strategy ของเทรนด์ไมโครได้ผสมรวมโซลูชันระบบอัจฉริยะด้านภัยคุกคามส่วนกลาง เครื่องมือและบริการเฉพาะด้านเพื่อนำเสนอโซลูชันที่ครบวงจรสำหรับลูกค้า

APT หรือการโจมตีแบบมีเป้าหมายยังคงทำงานและสามารถหลบหลีกการควบคุมด้านการรักษาความปลอดภัยในรูปแบบเดิมได้ เช่น โปรแกรมป้องกันไวรัส ไฟร์วอลล์รุ่นใหม่ และระบบป้องกันการบุกรุก ซึ่งยืนยันได้จากการโจมตีธนาคารและบริษัทด้านสื่อในเกาหลีใต้เมื่อเร็วๆ นี้ โดยปกติแล้วการโจมตีเหล่านี้มักจะถูกควบคุมจากระยะไกลผ่านทาง การสื่อสารแบบสั่งการและควบคุม (C&C) ระหว่างระบบที่แทรกซึมอยู่กับผู้โจมตี และข้อมูลล่าสุดจากเทรนด์แล็บส์ พบว่ามีไซต์ C&C ที่กำลังทำงานอยู่มากกว่า 1,500 แห่งโดยมีผู้ใช้ที่ตกเป็นเหยื่อต่อไซต์ตั้งแต่ 1 ถึงกว่า 25,000 ราย

จากพฤติกรรมโจมตีดังกล่าว **เทรนด์ไมโครจึงพร้อมนำเสนอกลยุทธ์ Custom Defense Strategy** ด้วยการตรวจสอบที่สามารถกำหนดได้เองและการป้องกันที่กำหนดเส้นทางไปยังอุปกรณ์เครือข่ายเกตเวย์ เซิร์ฟเวอร์ และจุดป้องกันปลายทางต่างๆ ได้โดยอัตโนมัติ ซึ่งจะช่วยเสริมศักยภาพองค์กรในการปรับและรับมือกับการโจมตีได้ทันที ทั้งนี้จากการเปรียบเทียบการเชื่อมโยงของข้อมูลในระบบอัจฉริยะด้านภัยคุกคามบนระบบคลาวด์ที่มีปริมาณมากถึงระดับเทราไบต์ ทำให้เทรนด์ไมโคร สมาร์ท โพรเทคชัน เน็ตเวิร์กสามารถเสริมสร้างศักยภาพให้กับองค์กรด้วยข้อมูลที่จำเป็นในการรับมือกับภัยคุกคามเหล่านี้ได้ โดยลูกค้าของเทรนด์ไมโครในเกาหลีใต้ที่ปรับใช้เทคโนโลยี Custom Defense สามารถตรวจพบและป้องกันได้ก่อนที่จะเกิดความเสียหายขึ้น

การป้องกันผู้ใช้ในยุค BYOD ได้อย่างครอบคลุม

การใช้งานอุปกรณ์ไอทีอย่างแพร่หลายของผู้บริโภคไม่เพียงแต่เพิ่มประสิทธิภาพในการทำงานของพนักงานเท่านั้น แต่ยังก่อให้เกิดปัญหาในด้านการสูญเสียข้อมูลและการละเมิดความปลอดภัยผ่านอุปกรณ์ที่พนักงานเป็นเจ้าของได้เช่นกัน โดยพนักงานที่ใช้บริการคลาวด์ส่วนบุคคลที่ไม่สามารถควบคุมได้ซึ่งตรวจพบว่ามีปัญหาด้านการละเมิดความปลอดภัย เช่น Dropbox, YouSendIt และ iCloud อาจนำไปสู่การรั่วไหลของข้อมูลที่สำคัญได้

บริษัทเทรนด์ไมโครจึงเปิดตัว **โซลูชันเซฟซิงค์ (SafeSync) สำหรับกลุ่มลูกค้าเอ็นเตอร์ไพรส์** ซึ่งเป็นโซลูชันการทำงานร่วมกันและการซิงโครไนซ์ไฟล์ที่ปลอดภัยที่จะผสมรวมอยู่ภายในระบบคลาวด์ส่วนตัวหรือศูนย์ข้อมูลขององค์กร โดยโซลูชันดังกล่าวจะช่วยให้การดำเนินงานและการทำงานร่วมกันของพนักงานแบบเคลื่อนที่ที่ใช้ อุปกรณ์ต่างๆ เช่น สมาร์ทโฟน แท็บเล็ต และพีซี สามารถเป็นไปอย่างราบรื่นโดยไม่กระทบต่อความปลอดภัยของข้อมูลในองค์กร

นอกจากนี้ยังเปิดตัว **เทรนด์ไมโคร เอ็นเตอร์ไพรส์ ซิเคียวริตี้ และดาต้า โพรเทคชัน** ซึ่งเป็นการขยายแพลตฟอร์มการป้องกันมัลแวร์ที่มีอยู่เดิมให้รวมขีดความสามารถด้านการป้องกันข้อมูลรั่วไหล (iDLP) ที่จัดการได้จากส่วนกลาง ติดตั้งได้ง่าย และโซลูชันใหม่นี้ยังเพิ่มความสามารถด้านการป้องกันข้อมูลรั่วไหลได้ทั้งมือถือ อีเมล

เกตเวย์ และอุปกรณ์ปลายทางที่มีอยู่เดิม โดยผู้ใช้จะสามารถเข้าถึงและแลกเปลี่ยนข้อมูลได้อย่างปลอดภัยไม่ว่าจะอยู่ที่ใดหรือผ่านอุปกรณ์และแอปพลิเคชันใดๆ ก็ตาม

ความปลอดภัยสำหรับระบบคลาวด์และศูนย์ข้อมูล

จะเห็นได้ว่าประมาณ 20% ของบริษัทในภูมิภาคเอเชียแปซิฟิกมีเซิร์ฟเวอร์ในจำนวนมากกว่าเครื่องที่เป็นระบบเสมือน และคาดว่าจะเพิ่มขึ้น 37% ภายในสิ้นปี 2556 เมื่อองค์กรต่างๆ ใ้ได้รับใช้ระบบเซิร์ฟเวอร์เสมือนและเริ่มก้าวเข้าสู่ระบบคลาวด์ ศูนย์ข้อมูลจะมีความหลากหลายและซับซ้อนมากขึ้น เมื่อมีการปรับเปลี่ยนรูปแบบศูนย์ข้อมูล องค์กรจึงต้องมีโซลูชันรักษาความปลอดภัยสำหรับเซิร์ฟเวอร์รุ่นใหม่ที่สามารถให้การป้องกันได้อย่างสมบูรณ์ สามารถจัดการผ่านหน้าต่างเดียวได้ และได้รับผลคุ้มค่าจากการลงทุนในระบบเสมือนจริงในระดับสูงสุด ครอบคลุมทั้งระบบจริง ระบบเสมือน และระบบคลาวด์

เทรนด์ไมโคร ดีพ ซิเคียวริตี้ (Trend Micro Deep Security™) แพลตฟอร์มรักษาความปลอดภัยสำหรับเซิร์ฟเวอร์รุ่นใหม่เหมาะอย่างยิ่งสำหรับระบบคลาวด์และระบบเสมือนจริง เนื่องจากได้รับการออกแบบให้สามารถเพิ่มผลตอบแทนจากการลงทุนในระบบเสมือนจริงขององค์กรได้ในระดับสูงสุด อีกทั้งยังช่วยให้ผู้ให้บริการระบบคลาวด์มีโครงสร้างพื้นฐานในรูปแบบบริการ (Infrastructure-as-a-Service: IaaS) โดยแพลตฟอร์มเวอร์ชันล่าสุดได้ขยายการรักษาความปลอดภัยสำหรับศูนย์ข้อมูลให้ครอบคลุมระบบคลาวด์สาธารณะและแบบไฮบริด ซึ่งเป็นการผสมรวมเข้ากับ วิคลาวด์ (vCloud) และอเมซอน เว็บบ เซอร์วิส เอพีไอ (Amazon Web Services API)

นอกจากนี้ยังมี**เทรนด์ไมโคร ซิเคียวคลาวด์ (Trend Micro SecureCloud™)** นำเสนอการเข้ารหัสข้อมูลในระบบคลาวด์ด้วยระบบการจัดการคีย์ โดยการเข้ารหัสลับจะช่วยให้ผู้จัดการฝ่ายไอทีสามารถดูแลระบบเสมือนจริงและการประมวลผลในระบบคลาวด์ได้อย่างปลอดภัยภายใต้การรับรู้ว่าสินทรัพย์ที่มีค่าสูงสุดขององค์กร ซึ่งก็คือข้อมูล จะได้รับการป้องกันจากการโจรกรรม การเปิดเผยโดยไม่ตั้งใจ หรือแม้แต่การโยกย้ายไปยังศูนย์ข้อมูลอื่นโดยไม่ได้รับการอนุมัติ เทรนด์ไมโคร ซิเคียวคลาวด์จะช่วยให้องค์กรธุรกิจสามารถดำเนินการจัดการที่สำคัญได้สอดคล้องตามนโยบายไม่ว่าจะอยู่ในสภาพแวดล้อมใดก็ตาม ซึ่งนั่นจะนำไปสู่การรักษาความปลอดภัยสำหรับข้อมูลได้อย่างสูงสุดและสามารถปฏิบัติตามกฎระเบียบได้อย่างถูกต้อง