ความปลอดภัยพื้นฐานสำหรับบริการแบบเวอร์ชั่วล์ที่องค์กรควรมี

โดย นายพีระพงศ์ จงวิบูลย์ ผู้จัดการประจำประเทศไทย ฟอร์ติเน็ต อินเตอร์เนชั่นแนล อิงค์

เมื่อเร็ว ๆ นี้ ยักษ์ใหญ่ทางด้านธุรกิจเครือข่ายแบบเวอร์ชั่วล์ “วีเอ็มแวร์” (VMware) มีปัญหาในการที่จะส่งแพทช์โปรแกรมขนาดเล็กด้านรักษาความปลอดภัยใหม่เพื่อแก้ไขปัญหาการรั่วไหลของซอร์สโค้ดบนเซิร์ฟเวอร์ ESX ไฮเปอร์ไวเซอร์ในเดือนเมษายน และ มีการกล่าวว่าโดนลองดีโดยแฮ็กเกอร์รายหนึ่งจากกลุ่มแฮกเกอร์แอคทีฟแอนโนนิมัส ทั้งนี้ แพทช์ใหม่นี้ออกแบบมาให้อุดช่องโหว่ที่สำคัญที่อาจเป็นจุดที่แฮกเกอร์ใช้โจมตีสั่งรันโค้ดอันตรายจากโฮสต์ที่อยู่ระยะไกล และทำให้สภาพแวดล้อมเวอร์ชั่วล์เสมือนจริงของผู้ใช้ปลายทางเกิดความเสี่ยงต่อการถูกโจมตีทางไซเบอร์ได้

เรื่องนี้จุดประเด็นปัญหาด้านความปลอดภัยของข้อมูลแบบเวอร์ชั่วล์ รวมทั้งวิธีการโอนถ่ายข้อมูลบนโครงข่ายแบบเวอร์ชั่วล์ที่ย่อมมีผลต่อความปลอดภัยขององค์กรโดยรวม และแน่นอนที่สุด การที่เพิ่มความปลอดภัยอีกชั้นหนึ่งบนสภาพแวดล้อมแบบเวอร์ชั่วล์ย่อมอาจมีช่องโหว่ด้านความปลอดภัยถ้าองค์กรไม่รู้ว่าข้อมูลของตนจะอยู่ที่ใดและมีอะไรปกป้องข้อมูลเหล่านั้นของตนบ้าง ทั้งนี้ ข้อมูลขององค์กรจะปลอดภัยมากน้อยแค่ไหนย่อมขึ้นอยู่กับศักยภาพด้านความปลอดภัยขององค์กรนั้นด้วยและรวมทั้งกระบวนการสร้างความปลอดภัยของสภาพแวดล้อมของที่ที่องค์กรหลากหลายประเภทใช้บริการฝากข้อมูลอยู่

มร. เจสัน แบนโดฟร์ ผู้เชี่ยวชาญอาวุโสด้านผลิตภัณฑ์แห่งฟอร์ติเน็ตกล่าวว่า “ไม่มีคำตอบที่ถูกต้องเพียงคำตอบเดียวในเรื่องนี้ องค์กรจำเป็นต้องประเมินดูสิ่งแวดล้อม ดูว่าสถานที่เหล่านั้นกำลังทำอะไร ติดตั้งอะไร เหมาะสมหรือไม่” ทั้งนี้ เจสันมีข้อแนะนำด้านความปลอดภัยพื้นฐานที่สำคัญสำหรับสิ่งแวดล้อมแบบเวอร์ชั่วล์ ดังนี้

ข้อแรก เจสันเห็นว่า ถึงแม้ว่าองค์กรต้องการผันโครงข่ายของตนเองให้เป็นแบบเวอร์ชั่วล์มากที่สุดก็ตาม องค์กรยังควรจะยังคงสิ่งแวดล้อมแบบไฮบริทไว้และออกแบบความปลอดภัยบนเครือข่ายจริงและเครือข่ายเสมือนจริงเวอร์ชั่วล์ให้สมดุลย์เพื่อสร้างเกราะป้องกันที่แข็งแรงให้กับข้อมูล ทั้งนี้ จากการที่เจสันได้สนทนากับการ์ทเนอร์ ได้เห็นแนวโน้มความต้องการทั้งเครือข่ายจริงและเครือข่ายเสมือนจริงสูงมาก “องค์กรจำเป็นต้องสร้างความปลอดภัยทั้งใน

และนอกสิ่งแวดล้อมนั้น จะเป็นต้องสร้างมีพารามิเตอร์ด้านความปลอดภัยให้กับสิ่งแวดล้อมเวอร์ชั่วล์ที่ไม่ว่าจะเป็นคลาวด์ของสาธารณะหรือของส่วนตัว องค์กรต้องมีพารามิเตอร์ป้องกันอุปกรณ์จริง เช่น เซิร์ฟเวอร์ สตอเรจและการเชื่อมโยงของอุปกรณ์จริงเหล่านี้ด้วยเช่นกัน”

ข้อที่สอง ดาต้าเซ็นเตอร์ที่มีผู้เช่าใช้บริการที่หลากหลายต้องจัดโซนความปลอดภัยที่แยกออกไปอย่างชัดเจน จำเป็นต้องลงทุนในอุปกรณ์ความปลอดภัยแบบเวอร์ชั่วล์เพื่อป้องกันมิให้ผู้ที่เข้ามาทางอุปกรณ์จริงข้ามโซนมาดึงข้อมูลจากโซนเวอร์ชั่วล์ไปได้ ตัวอย่างเช่น องค์กร A อาจโฮสต์อยู่ในเว็ปเซิร์ฟเวอร์และแอปพลิเคชั่นเซิร์ฟเวอร์ในอุปกรณ์เดียวกับองค์กร B ที่ใช้บริการคลาวด์สาธารณะได้ ทั้งนี้ ประโยชน์ของการใช้อุปกรณ์เวอร์ชั่วล์นี้ดีตรงที่จะสั่งการทำงานจากที่ใดก็ได้ในเครือข่ายคลาวด์ แต่ผู้ให้บริการคลาวด์ต้องแยกผู้เช่าใช้บริการจากกันให้ชัดเจนเพื่อป้องกันการข้ามใช้งาน เช่น ในเว็บเซิร์ฟเวอร์หนึ่งอาจบรรจุข้อมูลด้านบัตรเครดิตของลูกค้ามากมาย จึงต้องการความปลอดภัยพิเศษเฉพาะของตนที่แตกต่างไปจากผู้เช่าใช้รายอื่น

ข้อที่สาม ควรจัดให้มีระเบียบปฏิบัติ (Compliance regulations) เพื่อสร้างความปลอดภัยให้ชัดเจน รวมทั้งต้องระเบียบปฏิบัติสำหรับการใช้งานแบบเวอร์ชั่วล์เช่นกัน องค์กรต้องปกป้องทราฟฟิคที่อยู่ในอุปกรณ์เสมือนจริงนั้นและต้องรองรับเวิร์คโหลดที่แตกต่างกันบนโฮสต์เดียวกันได้ ซึ่งเรามักจะไม่พบปัญหาเวิร์คโหลดนี้ในอุปกรณ์จริง

ข้อที่สี่ จำเป็นอย่างยิ่งที่จะต้องมีระบบจัดการที่ส่วนกลางที่สามารถตรวจสอบส่วนประกอบและสิ่งแวดล้อมจริงและสิ่งแวดล้อมเสมือนจริงได้ อาจจะเป็นการควบคุมจากหน้าจอเดียวเพื่อลดปัญหาด้านคอขวดและเพื่อเพิ่มประสิทธิภาพการทำงานของเครือข่าย

ท้ายสุด เหมือนกันข้อมูลที่วิ่งอยู่บนอุปกรณ์จริง ข้อมูลที่อยู่บนอุปกรณ์เสมือนก็ย่อมตกในภาวะเสี่ยงถ้าเกิดการรั่วไหลไป แต่ไม่เหมือนกันข้อมูลบนอุปกรณ์จริง ตรงที่เวิร์คโหลดจะโอนถ่ายข้อมูลบนอุปกรณ์เสมือนไปยังอีกโฮสต์หรือเซิร์ฟเวอร์หนึ่งอย่างง่ายดาย ดังนั้น ยิ่งทำให้ องค์กรยิ่งจำเป็นต้องมีนโยบายด้านความปลอดภัยทางด้านนี้อย่างรัดกุมมากขึ้นด้วย

“ในโลกของเวอร์ชั่วล์ องค์กรสามารถเซ็ทและจัดการด้านโหลดบาลานซิ่งได้อย่างเต็มที่ องค์กรสามารถเห็นการถ่ายเทเวิร์คโหลดนั้น ดังนั้น องค์กรจำเป็นต้องสร้างความปลอดภัยให้เวิร์คโหลดเหล่านั้น” เจสันกล่าวแนะนำ