

ความปลอดภัยพื้นฐานสำหรับบริการแบบเวอร์ชวลที่ องค์กรควรมี



โดย นายพีระพงศ์ จงวิบูลย์ ผู้จัดการประจำประเทศไทย ฟอर्टิเน็ต อินเทอร์เน็ต เนชั่นแนล อิงค์

เมื่อเร็ว ๆ นี้ ยักษ์ใหญ่ทางด้านธุรกิจเครือข่ายแบบเวอร์ชวล “วีเอ็มแวร์” (VMware) มีปัญหาในการที่จะส่งแพทช์โปรแกรมขนาดเล็กด้านรักษาความปลอดภัยใหม่เพื่อแก้ไขปัญหาคารั่วไหลของซอร์สโค้ดบนเซิร์ฟเวอร์ ESX ไฮเปอร์ไวเซอร์ในเดือนเมษายน และ มีการกล่าวว่าโดนลงตีโดยแฮ็กเกอร์รายหนึ่งจากกลุ่มแฮ็กเกอร์แอกทีฟแอนโนนิมัส ทั้งนี้ แพทช์ใหม่นี้ออกแบบมาให้อุดช่องโหว่ที่สำคัญที่อาจเป็นจุดที่แฮ็กเกอร์ใช้โจมตีส่งรันโค้ดอันตรายจากโฮสต์ที่อยู่ระยะไกล และทำให้สภาพแวดล้อมเวอร์ชวลเสมือนจริงของผู้ใช้ปลายทางเกิดความเสี่ยงต่อการถูกโจมตีทางไซเบอร์ได้



เรื่องนี้จุดประเด็นปัญหาด้านความปลอดภัยของข้อมูลแบบเวอร์ชวล รวมทั้งวิธีการโอนถ่ายข้อมูลบนโครงสร้างแบบเวอร์ชวลที่ย่อมมีผลต่อความปลอดภัยขององค์กรโดยรวม และแน่นอนที่สุด การที่เพิ่มความปลอดภัยอีกชั้นหนึ่งบนสภาพแวดล้อมแบบเวอร์ชวลย่อมอาจมีช่องโหว่ด้านความปลอดภัยถ้าองค์กรไม่รู้ว่าข้อมูลของตนจะอยู่ที่ใดและมีอะไรปกป้องข้อมูลเหล่านั้นของตนบ้าง ทั้งนี้ ข้อมูลขององค์กรจะปลอดภัยมากน้อยแค่ไหนย่อมขึ้นอยู่กับศักยภาพด้านความปลอดภัยขององค์กรนั้นด้วยและรวมทั้งกระบวนการสร้างความปลอดภัยของสภาพแวดล้อมของที่ที่องค์กรหลากหลายประเภทใช้บริการฝากข้อมูลอยู่

มร. เจสัน แบนโดर्फ ผู้เชี่ยวชาญอาวุโสด้านผลิตภัณฑ์แห่งฟอर्टิเน็ตกล่าวว่า “ไม่มีคำตอบที่ถูกต้องเพียงคำตอบเดียวในเรื่องนี้ องค์กรจำเป็นต้องประเมินดูสิ่งแวดล้อม ดูว่าสถานที่เหล่านั้นกำลังทำอะไร ติดตั้งอะไร เหมาะสมหรือไม่” ทั้งนี้ เจสันมีข้อเสนอแนะด้านความปลอดภัยพื้นฐานที่สำคัญสำหรับสิ่งแวดล้อมแบบเวอร์ชวล ดังนี้

ข้อแรก เจสันเห็นว่า ถึงแม้ว่าองค์กรต้องการผันโครงสร้างของตนเองให้เป็นแบบเวอร์ชวลมากที่สุดก็ตาม องค์กรยังคงควรที่จะยังคงสิ่งแวดล้อมแบบไฮบริทไว้และออกแบบความปลอดภัยบนเครือข่ายจริงและเครือข่ายเสมือนจริงเวอร์ชวลให้สมดุลย์เพื่อสร้างเกราะป้องกันที่แข็งแรงให้กับข้อมูล ทั้งนี้ จากการที่เจสันได้สนทนากับการ์ทเนอร์ ได้เห็นแนวโน้มความต้องการทั้งเครือข่ายจริงและเครือข่ายเสมือนจริงสูงมาก “องค์กรจำเป็นต้องสร้างความปลอดภัยทั้งใน

และนอกสิ่งแวดลุ่มนั้น จะเป็นที่ต้องสร้างมีพารามิเตอร์ด้านความปลอดภัยให้กับสิ่งแวดลุ่มเวอร์ชวลที่ไม่ว่าจะเป็น คลาวด์ของสาธารณะหรือของส่วนตัว องค์กรต้องมีพารามิเตอร์ป้องกันอุปกรณ์จริง เช่น เซิร์ฟเวอร์ สตอเรจและการ เชื่อมโยงของอุปกรณ์จริงเหล่านี้ด้วยเช่นกัน”

ข้อที่สอง ดาต้าเซ็นเตอร์ที่มีผู้เช่าใช้บริการที่หลากหลายต้องจัดโซนความปลอดภัยที่แยกออกไปอย่างชัดเจน จำเป็น ต้องลงทุนในอุปกรณ์ความปลอดภัยแบบเวอร์ชวลเพื่อป้องกันมิให้ผู้เข้ามาทางอุปกรณ์จริงข้ามโซนมาดึงข้อมูลจาก โซนเวอร์ชวลไปได้ ตัวอย่างเช่น องค์กร A อาจโฮสต์อยู่ในเว็บเซิร์ฟเวอร์และแอปพลิเคชันเซิร์ฟเวอร์ในอุปกรณ์ เดียวกับองค์กร B ที่ใช้บริการคลาวด์สาธารณะได้ ทั้งนี้ ประโยชน์ของการใช้อุปกรณ์เวอร์ชวลนี้โดยตรงที่จะส่งการ ทำงานจากที่ใดก็ได้ในเครือข่ายคลาวด์ แต่ผู้ให้บริการคลาวด์ต้องแยกผู้เช่าใช้บริการจากกันให้ชัดเจนเพื่อป้องกันการ ข้ามใช้งาน เช่น ในเว็บเซิร์ฟเวอร์หนึ่งอาจบรรจุข้อมูลด้านบัตรเครดิตของลูกค้ามากมาย จึงต้องการความปลอดภัย พิเศษเฉพาะของตนที่แตกต่างไปจากผู้เช่าใช้รายอื่น

ข้อที่สาม ควรจัดให้มีระเบียบปฏิบัติ (Compliance regulations) เพื่อสร้างความปลอดภัยให้ชัดเจน รวมทั้งต้อง ระเบียบปฏิบัติสำหรับการใช้งานแบบเวอร์ชวลเช่นกัน องค์กรต้องปกป้องกราฟฟิคที่อยู่ในอุปกรณ์เสมือนจริงนั้นและ ต้องรองรับเวิร์คโหลตที่แตกต่างกันบนโฮสต์เดียวกันได้ ซึ่งเรามักจะไม่พบปัญหาเวิร์คโหลตนี้ในอุปกรณ์จริง

ข้อที่สี่ จำเป็นอย่างยิ่งที่จะต้องมีการจัดการที่ส่วนกลางที่สามารถตรวจสอบส่วนประกอบและสิ่งแวดลุ่มจริงและ สิ่งแวดลุ่มเสมือนจริงได้ อาจจะเป็นการควบคุมจากหน้าจอเดียวเพื่อลดปัญหาด้านคอขวดและเพื่อเพิ่ม ประสิทธิภาพการทำงานของเครือข่าย

ท้ายสุด เหมือนกันข้อมูลที่อยู่บนอุปกรณ์จริง ข้อมูลที่อยู่บนอุปกรณ์เสมือนก็ย่อมตกในภาวะเสี่ยงถ้าเกิดการรั่ว ไหลไป แต่ไม่เหมือนกันข้อมูลบนอุปกรณ์จริง ตรงที่เวิร์คโหลตจะโอนถ่ายข้อมูลบนอุปกรณ์เสมือนไปยังอีกโฮสต์ หรือเซิร์ฟเวอร์หนึ่งอย่างง่ายดาย ดังนั้น ยิ่งทำให้ องค์กรยิ่งจำเป็นต้องมีนโยบายด้านความปลอดภัยทางด้านนี้อย่าง รัดกุมมากขึ้นด้วย

“ในโลกของเวอร์ชวล องค์กรสามารถเห็นและจัดการด้านโหลตบาลานซ์ได้อย่างเต็มที่ องค์กรสามารถเห็นการ ถ่ายเทเวิร์คโหลตนั้น ดังนั้น องค์กรจำเป็นต้องสร้างความปลอดภัยให้เวิร์คโหลตเหล่านั้น” เจสันกล่าวแนะนำ