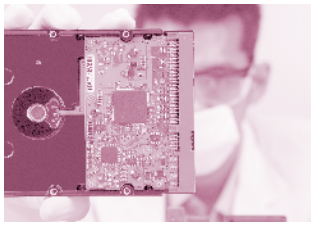

วางแผนรับมือ BYOD โอกาสหรือความเสี่ยง

วิชย์ศุทธ์ เมาระพงษ์
ที่ปรึกษาโครงการสารสนเทศของหน่วยงานภาครัฐ
สังกัดสถาบันวิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์

ต่อ จากฉบับที่แล้ว

ในเรื่องการปกป้องข้อมูลในอุปกรณ์พกพา หรือ MDP เป็นการผสมผสานกันระหว่างการใช้งาน Application ที่รัดกุมกับนโยบายและแนวทางการปฏิบัติงานของผู้ใช้ที่ต้องมีการควบคุมกำกับดูแล รวมถึงความรับผิดชอบต่อทรัพย์สิน หรืออุปกรณ์พกพาที่ตนถือครอง เนื่องจากทุกการเข้าถึงเครือข่ายภายในองค์การและข้อมูลสำคัญเป็นจุดเริ่มต้นของการสร้างความเสี่ยงได้ในทุกกรณี

ดังนั้น การบริหารจัดการที่เหมาะสม คือ การวางแนวทาง หรือนโยบายในการควบคุม BYOD ที่รัดกุมในทุกมิติ ซึ่งหลายองค์การชั้นนำในด้านการรักษาความมั่นคงปลอดภัยสารสนเทศหลายแห่งได้ทำการศึกษาวิจัยเพื่อพัฒนาแนวทางดังกล่าวและนำเสนออย่างเป็นทางการเพื่อให้องค์การต่างๆ นำไปเป็นต้นแบบในการสร้างนโยบาย BYOD ของตน รวมถึงการระบุประเด็นที่ควรคำนึงถึงในการจัดทำนโยบายเพื่อให้แต่ละองค์การสามารถหาแนวทางที่เหมาะสมกับตนได้

ผมขอยกตัวอย่างแนวทางของ Bardford Network ซึ่งเป็นองค์การที่พัฒนา Solution ด้านการรักษาความมั่นคงปลอดภัยเครือข่ายสารสนเทศระดับโลก ได้จัดทำรายงานผลการศึกษาแนวทางการบริหารจัดการด้านความปลอดภัยในการใช้ BYOD ในชื่อ "Ten Steps to Secure BYOD" ซึ่งมีรายละเอียดกล่าวถึงการดำเนินงาน 10 ขั้นตอนหลักในการวางนโยบายเพื่อรักษาความมั่นคงทางสารสนเทศและข้อมูลเมื่อองค์การนำ BYOD มาใช้ ประกอบด้วย

1) พิจารณาว่าอุปกรณ์พกพาใดบ้างที่ควรได้รับอนุญาตให้เชื่อมต่อเครือข่ายองค์การ

ขั้นตอนแรก คือ การกำหนดสิ่งที่อุปกรณ์พกพาควรได้รับการสนับสนุนและถ้าได้รับการสนับสนุนแล้วทำให้อุปกรณ์เหล่านั้นมีความปลอดภัยที่เพียงพอจึงจะได้รับอนุญาตให้เข้าถึงเครือข่ายขององค์การ รูปแบบการดำเนินการ เช่น ผู้ที่มาติดต่อองค์การและนำเอาอุปกรณ์

พกพามาใช้งานทางองค์การอาจให้ใช้สิทธิการเข้าถึงเครือข่ายภายในในระดับ Guest แต่ถ้าเป็นพนักงาน หรือผู้บริหารและมีการลงทะเบียนอุปกรณ์หรือแม้กระทั่งติดตั้ง Application เพื่อบริหารจัดการการเข้าถึงเครือข่ายภายในก็จะได้สิทธิการเข้าถึงที่สูงกว่าสามารถดำเนินกิจกรรมที่เกี่ยวข้องกับระบบงานภายในได้ สิ่งที่สำคัญคือการสร้างความเข้าใจและให้ความรู้พนักงานเกี่ยวกับการรักษาความปลอดภัยการใช้เครือข่ายภายในขององค์การ และที่สำคัญยิ่งกว่าคือให้พนักงานมีส่วนร่วมในการกำหนดนโยบายการเข้าถึงดังกล่าวเพื่อให้เกิดการยอมรับและปฏิบัติตาม

2) การกำหนดรุ่น หรือ Version ของระบบปฏิบัติการ (Mobile Operating System) ที่ได้รับอนุญาตให้เชื่อมต่อเครือข่ายองค์การ

เมื่อตัดสินใจได้ว่าจะกำหนดให้อุปกรณ์พกพาใดได้รับอนุญาตให้เชื่อมต่อเครือข่ายองค์การ ก็จำเป็นต้องมีการตรวจสอบด้วยว่าระบบปฏิบัติการรุ่น หรือ Version ใดที่ติดตั้งบนอุปกรณ์พกพานั้นควรได้รับอนุญาตให้ใช้งานเนื่องจากสามารถสร้างความเสี่ยงในกรณีที่ไม่มีการปรับปรุง (Patch) แก้ไขปัญหาเรื่องช่องโหว่ หรือมีความเสี่ยงที่จะติด Virus Worm Spyware Botnet หรือ Trojan เช่นเดียวกันกับเครื่องคอมพิวเตอร์ที่เราใช้งานกันโดยทั่วไป ในการบริหารจัดการ Patching อาจใช้ Software MDM ติดตั้งลงบนอุปกรณ์พกพาเพื่อจัดการโดยอัตโนมัติเมื่อถึงเวลาที่เหมาะสม

3) กำหนดว่าโปรแกรมประยุกต์ หรือ Application ใดควรที่มีผลบังคับใช้ หรือต้องห้ามใช้สำหรับแต่ละอุปกรณ์

ขั้นตอนต่อไปคือ การกำหนดสิ่งที่พนักงานควรระมัดระวังในการใช้งาน Mobile Application โดยให้ผู้ดูแลระบบกำหนดค่าของ MDM เพื่อจำกัดการเข้าถึงผ่านเครือข่ายองค์การของ Application เฉพาะที่องค์การระบุไว้ ซึ่งเมื่อพนักงานเลิกใช้งานระบบเครือข่ายขององค์การและกลับไปใช้เครือข่ายสาธารณะอื่นๆ เพื่อเชื่อมต่อและใช้งานอุปกรณ์ Application ส่วนตัวอื่นๆ ก็สามารถใช้งานเชื่อมต่อเครือข่ายได้ตามปกติ ทั้งนี้เพื่อป้องกัน มิให้ Application บางตัวที่ต้องการการเชื่อมต่อเครือข่าย มีความอ่อนแอ มีช่องโหว่ที่จะกลายเป็นพาหะ หรือเส้นทางในการเข้าถึงและโจมตีด้วย Software ไม่พึงประสงค์ได้

4) กำหนดกลุ่มของพนักงานที่จะได้รับการอนุญาตให้ใช้อุปกรณ์เหล่านี้

แล้วก็มาถึงขั้นตอนที่จะตัดสินว่าใครควรได้รับอนุญาตให้สามารถใช้อุปกรณ์พกพาส่วนตัวเพื่อเชื่อมต่อเครือข่ายองค์การได้ โดยการอนุมัติจะอาศัยข้อมูลรายละเอียดกลุ่มของพนักงานตามภารกิจหลักและตามที่ได้รับมอบหมายเป็นรายกรณี สิทธิในการใช้งานเครือข่าย ระบบสารสนเทศ รวมถึงการเข้าถึงข้อมูล

5) การเฝ้าจับตาผู้ใช้งานว่าทำอะไรที่ไหนเมื่อเข้าถึงเครือข่ายองค์การ

ในขั้นตอนนี้เป็นการจะเชื่อมโยงตัวพนักงานผู้ใช้งานอุปกรณ์และกลุ่มผู้ใช้งาน เมื่อมีการเชื่อมต่อเครือข่ายองค์การตามนโยบายที่ได้กำหนดไว้ ตัวอย่างเช่น การใช้ BYOD ในโรงพยาบาล ดร.จอห์นสมิธ แพทย์แผนกฉุกเฉินต้องการใช้ iPad ของเขาในการเข้าถึงเวชระเบียน ดังนั้น จำเป็นต้องกำหนดสิ่งที่ระบุตัวตนเฉพาะของอุปกรณ์ (เช่นที่อยู่ MAC Address ของอุปกรณ์) และเชื่อมโยงกับเจ้าของ (ดร.จอห์นสมิธ) ระบุ SSID ที่ iPad ของดร.จอห์นสมิธ เชื่อมต่ออยู่ ซึ่งจะระบุตำแหน่งของเครือข่ายไร้สายภายในโรงพยาบาลว่าใช้งาน ณ ที่ใด เพื่อจะระบุตำแหน่งทางกายภาพของ Access Point (s) โดยเป็นการส่งข้อมูลผ่านระบบเครือข่ายภายในองค์การที่สามารถเข้าถึงได้ ซึ่งเหล่านี้คือหลักการทำงานของ Network Access Control (NAC) ที่ประกอบด้วยปัจจัยหรือ Factor เราสามารถนำมาพูดติดปากเพื่อให้รู้ได้ว่า ใคร / ทำอะไร / ที่ไหน / เมื่อไหร่

User name:	Dr.Iohn Smith
Unique Identifier:	D8:A2:5E:2D:85:AD
SSID/AP:	Patient Info / Emergency-Room (where Patient Info is the SSID and Energency - Room is the access point
Time:	8:00 AM - 5:00 PM (Dr.Smith works the day shift.)

6) การสื่อสารให้พนักงานรับรู้เกี่ยวกับนโยบาย BYOD ขององค์การ

ถึงตอนนี้เราได้สร้างนโยบาย BYOD ขององค์การตามที่ต้องการและเห็นว่าเหมาะสมแล้ว ขั้นตอนต่อไปดำเนินการเพื่อให้แน่ใจว่าพนักงานได้ทำความเข้าใจและเห็นว่ามันสมเหตุสมผล พร้อมทั้งยังเข้าใจด้วยว่านโยบาย BYOD ขององค์การบังคับใช้อย่างไร จากประสบการณ์ของผู้พัฒนาผลิตภัณฑ์ด้านการรักษาความมั่นคงทางเครือข่ายชั้นนำแนะนำว่า การสื่อสารที่มีประสิทธิภาพกับพนักงานเป็นสิ่งจำเป็นสำหรับการประสบความสำเร็จในการวางระบบความปลอดภัยและนโยบายที่เกี่ยวข้อง สำหรับ BYOD ก็เช่นเดียวกัน ปัญหาด้านความปลอดภัยขององค์การโดยส่วนใหญ่จะเกิดจากการที่พนักงานไม่เข้าใจและรับทราบถึงความเสี่ยงและความเสียหายที่จะเกิดขึ้น ส่งผลให้มีการปฏิบัติที่หละหลวมและไม่ตระหนักถึงความสำคัญและจำเป็นเพราะอุปกรณ์ที่ใช้งานอยู่เป็นของส่วนตัว แต่ลืมมองไปว่าทรัพยากรทางสารสนเทศอื่นๆ ที่เข้าถึงและใช้งานอยู่เป็นขององค์การ หรือผ่านเส้นทางการเชื่อมต่อที่องค์การอนุญาตให้เข้าถึง

อ่านต่อฉบับหน้า