นโยบายที่แข็งแกร่ง – สิ่งจะเป็นเมื่อองค์กรให้พนักงานใช้อุปกรณ์ไอทีของตนเองในงาน (BYOD)

โดย พีระพงศ์ จงวิบูลย์

ผู้จัดการ ประจำประเทศไทย ฟอร์ติเน็ต อิงค์

ในปัจจุบันนี้ ไม่มีใครปฏิเสธได้ว่า ไม่เคยเห็นพนักงานได้นำอุปกรณ์ของตนเอง อาทิแทปเล็ต ไอแพด โน้ตบุ๊ค มือถือแอนรอยด์มาใช้ในการงาน หรือที่เรียกกันย่อๆ ทั่วไปว่า BYOD (Bring Your Own Device) อาจเป็นการนำงานมาทำต่อที่บ้าน หรือใช้อุปกรณ์ของตนเองเมื่ออยู่นอกบ้าน แต่ก็ต้องเชื่อมต่อข้อมูลเข้ามาเก็บไว้ที่เครื่องของตนเอง ด้วยเหตุนี้ องค์กรต่างๆ จึงต้องพัฒนาระบบองค์กรให้เป็นระบบเปิดมากขึ้นเพื่อรองรับกับการใช้งานของอุปกรณ์ส่วนตัวของพนักงานนอกสถานที่

องค์กรเองก็ได้ประโยชน์ด้วยเช่นกัน โดยที่พนักงานเองมักมีและใช้อุปกรณ์ที่ทันสมัยใหม่อยู่เสมอ จึงทำให้การใช้งานมีประสิทธิภาพและรวดเร็ว พนักงานสามารถโต้ตอบอีเมล โหลดไฟล์ข้อมูลต่างๆ ขณะที่อยู่บนรถไฟฟ้า ขณะเดินทาง และจากการสำรวจ พบว่าพนักงานเองมีความพอใจที่ใช้อุปกรณ์และใช้แอปพลิเคชั่นที่ตนได้เลือกเองในการทำงาน

อย่างไรก็ตาม ย่อมมีเรื่องที่องค์กรควรระวัง จากผลการวิจัยของฟอร์ติเน็ต อิงค์เมื่อปีที่แล้วกับองค์กรขนาดกลางถึงขนาดใหญ่ในเอเชียจำนวน 350 แห่งพบว่า 85% ของผู้บริหารระดับสูงด้านไอทีตอบว่า มีความกังวลเรื่องความปลอดภัยของข้อมูลองค์กรที่ใช้ในสิ่งแวดล้อมใหม่นี้ และองค์กรส่วนใหญ่ยังไม่มีกระบวนการหรือยังไม่มั่นใจในกระบวนการด้านความปลอดภัยของตนที่มีอยู่ในการปกป้องข้อมูลที่ใช้ในอุปกรณ์ส่วนตัวของพนักงานนั้น โดยที่ 67% กล่าวว่ายังคงกำหนดสิทธิ์ใช้งานให้แก่พนักงานที่ใช้อุปกรณ์ที่องค์กรจัดหาให้เท่านั้น และ 26% ยังพึ่งพาให้พนักงานจัดหาด้านความปลอดภัยสำหรับอุปกรณ์และข้อมูลเอาเอง ซึ่งเป็นเรื่องที่อันตรายมาก

อุปกรณ์ส่วนตัวของพนักงานเองยังขาดวิธีด้านความปลอดภัยพื้นฐานเหมือนที่พวกเรามีใช้บนพีซีทั่วไป ไม่ว่าจะเป็นแอนตี้ไวรัส และการใช้พาสเวิร์ด ในขณะที่การใช้อุปกรณ์ส่วนบุคคลหมายถึงความคล่องตัวสามารถใช้แอปพลิเคชันทางธุรกิจที่สำคัญได้และเข้าถึงได้จากเครือข่ายใด ๆ ในสถานที่ใดได้ จึงทำให้ข้อมูลทางธุรกิจมีความเสี่ยงสูง

ทั้งนี้ พีระพงศ์ จงวิบูลย์ ผู้จัดการ ประจำประเทศไทย ฟอร์ติเน็ต อิงค์ เปิดเผยว่า “ฟอร์ติเน็ตมองเรื่องการสร้างความปลอดภัยว่ามี 2 ส่วน คือ ตัวผู้ใช้งานที่เมื่อเอาซอฟท์แวร์หรือแอปพลิเคชั่นไปลงแล้ว ต้องรับผิดชอบใน

พฤติกรรมของตนไม่ให้นำข้อมูลออกมาเปิดเผย หรือต้องระวังการล้วงความลับต่างๆ เช่น เมื่อมีใครเข้ามาแอบสอบถามขอข้อมูลส่วนตัว (Fishing) ก็ให้ระวัง มิให้ความร่วมมือ และกรณีที่ 2 คือ ผู้ให้บริการหรือองค์กรต้องมีระบบป้องกันภัยในการใช้งานโมบิลิตี้ของพนักงานด้วยเช่นกัน”

อย่างไรก็ตาม ฟอร์ติเน็ตสรุปมาตรการสำคัญ 3 ข้อเพื่อช่วยเป็นแนวทางให้องค์กรได้พิจารณา

จัดทำนโยบายด้านการใช้งานโมบายที่แข็งแรง (Implement A Relevant Mobile Policy): เป็นกฎเหล็กข้อแรกเลยที่เดียว โดยองค์กรต้องพิจารณาถึงภัยที่อาจคุกคามเข้ามาและผลที่จะเกิดขึ้น อาทิ เว็ปไซท์แปลกปลอม ประสิทธิภาพการทำงานตกต่ำลง การใช้แบนวิธมากเกินจำเป็น และรวมทั้งให้ลองตอบคำถามดังต่อไปนี้

- พนักงานต้องการใช้แอปพลิเคชั่นใดบ้าง ห้ามมิให้ใช้แอปพลิเคชั่นใดบ้าง
- อนุญาตให้พนักงานกลุ่มใดใช้อุปกรณ์ใด บริการใดได้บ้าง
- กระบวนการอนุมัติให้เข้าใช้ ขึ้นอยู่กับใคร อะไร ที่ไหน เมื่อไหร่

ใช้ซอฟท์แวร์ในการจัดการจากระยะทางไกล (Remote Management Software): เป็นสิ่งจำเป็นอย่างยิ่งที่องค์กรต้องมีซอฟท์แวร์แอนตี้ไวรัสหรือซอฟต์แวร์การจัดการระยะไกลที่มีความสามารถในการอัปเดทแพทช์ล่าสุดโดยอัตโนมัติเพื่อป้องกันช่องโหว่ที่มีอยู่ในอุปกรณ์ต่างๆ ให้พ้นจากการโจมตีที่เข้ามาทางโทรศัพท์มือถือ นอกจากนี้องค์กรควรมีวิธีจัการจากส่วนกลางในการค้นหาติดตาม ล็อค เช็ค สำรองและติดตั้งทูลส์ใหม่ได้จากระยะไกลเพื่อให้ทีมไอทีสามารถปกป้องและเรียกคืนข้อมูลขององค์กรที่ติดไปกับในกับโทรศัพท์มือถือที่สูญหายหรือถูกขโมยได้

บล็อคอุปกรณ์ที่มิทำตามกฎให้เข้าใช้งาน (Blocking Non-Compliant Devices): องค์กรควรยินยอมให้พนักงานใช้อุปกรณ์ส่วนตัวในเรื่องงานก็ต่อเมื่อพนักงานยินยอมตามข้อกำนดเท่านั้น เช่น ยินยอมที่จะติดตั้งแอปพลิเคชั่นบางประเภทที่องค์กรใช้ทางด้านความปลอดภัย มิเช่นนั้นแล้วพนักงานจำเป็นต้องใช้อุปกรณ์ที่องค์กรจัดหามาให้เท่านั้น อีกทางหนึ่งคือ องค์กรอาจต้องพิจารณาใช้โทรศัพท์ที่แบ่งการใช้งานได้เป็น 2 ส่วนอย่างชัดเจน (2 logical partitions) ที่แบ่งเป็นเรื่องส่วนตัว และเรื่องงาน ซึ่งองค์กรมีสิทธิ์ที่จะจัดการด้านความปลอดภัยในส่วนที่ใช้ในเรื่องงานอย่างเต็มที่

พีระพงศ์กล่าวเสริมว่า “อุปกรณ์โมบายยังมีศักยภาพด้านคอมพิวติ้งพาวเวอร์จำกัดอยู่ คงจะลงโอเอสหลากหลายประเภทไม่ได้ ดังนั้น ในการใช้งานโมบิลิตี้ของพนักงาน จำเป็นต้องมีระบบที่แข็งแกร่งด้านความปลอดภัยของข้อมูลที่จัดการโดยองค์กร มิใช่หวังแต่พนักงานเท่านั้น” นอกจากนี้ ที่สำนักงานขององค์กรเองควรมีกระบวนการด้านความปลอดภัยเน็กซ์เจเนอเรชั่นที่ครบถ้วน เพื่อดักตรวจและควบคุมแอปพลิเคชั่นได้ สามารถวิเคราะห์ประเภทของแอปพลิเคชั่นได้ วิเคราะห์พฤติกรรมของผู้ใช้งานได้ เชื่อมโยงกับผู้ใช้งานได้ สามารถตรวจสอบทราฟฟิคแอปพลิเคชั่นที่เข้ารหัสมาได้โดยไม่ว่าทราฟฟิคนั้นจะเข้ามาทางพอร์ตใดหรือโปรโตคอลใดก็ตาม