การใช้อุปกรณ์ส่วนตัว (BYOD) มีส่วนสร้างระบบความปลอดภัยไอทีขององค์กร

การใช้อุปกรณ์ส่วนตัว (BYOD**) มีส่วนสร้างระบบความปลอดภัยไอทีขององค์กร**

ผลการสำรวจในเอเชียของฟอร์ติเน็ตพบว่าพนักงานเกือบครึ่งหนึ่งไม่พอใจนโยบายขององค์กรด้านไอที

กรุงเทพฯ 5 กรกฎาคม 2555 — Fortinet ® (NASDAQ : FTNT) — ฟอร์ติเน็ตผู้นำโลกด้านโซลูชั่นประสิทธิภาพสูงสำหรับความปลอดภัยเครือข่ายประกาศผลจากการสำรวจทั่วโลกที่เผยให้เห็นว่าผู้ที่ใช้อุปกรณ์ของตนเองในที่ทำงาน หรือเพื่อการทำงานนำมาซึ่งประเด็นท้าทายของระบบไอทีองค์กร โดยที่พนักงานให้ความสำคัญด้านความปลอดภัยของข้อมูลองค์กรต่ำ แต่ยังคาดหวังที่จะใช้อุปกรณ์มือถือของตัวเองในงานต่อไป และพบว่าเกือบหนึ่งในพนักงานชาวเอเชียมีความรู้สึกขัดขืนกับนโยบายการรักษาความปลอดภัยของบริษัท ที่ห้ามพวกเขาใช้อุปกรณ์ส่วนบุคคลของพวกเขาในที่ทำงาน หรือเพื่อการทำงาน จึงเห็นถึงความจำเป็นเร่งด่วนที่องค์กรควรจะพัฒนากลยุทธ์การรักษาความปลอดภัยเพื่อรองรับการใช้อุปกรณ์ของตนเองในที่ทำงาน หรือเพื่อการทำงานของพนักงาน

การสำรวจภูมิภาค 15 เขตทั่วโลก (อินเดีย, เกาหลี, จีน, ไต้หวัน, ฮ่องกง, สิงคโปร์, ญี่ปุ่น, สหรัฐอเมริกา, สหราชอาณาจักร, ฝรั่งเศส, เยอรมนี, อิตาลี, สเปน, โปแลนด์และยูเออี) ในช่วงพฤษภาคม- มิถุนายน พ.ศ. 2555 นี้ได้ถามพนักงานที่ใช้อุปกรณ์ของตนเองเพื่อทำงานมากกว่า 3,800 คน (โดยมี 1,443 เป็นผู้ตอบในเอเชีย) อายุระหว่าง 21-31 ถึงมุมมองของพวกเขาในด้าน BYOD และผลกระทบต่อสภาพแวดล้อมการทำงานของพวกเขาและวิธีการรักษาความปลอดภัยด้านไอทีส่วนบุคคลของตันเอง รวมทั้งทัศนคติด้านไอทีขององค์กร

ยืนยันในสิทธิส่วนบุคคล จึงยังต้องมี BYOD อยู่

ในกลุ่มประชากรสำรวจแสดงให้เห็นว่า BYOD จะเป็นที่นิยมต่อไป กว่าสามในสี่ (85%) ของผู้ตอบแบบสอบถามในเอเชียตอบว่าใช้เป็นประจำอยู่แล้ว ที่สำคัญ มากกว่าครึ่งหนึ่ง (55%) ของผู้ตอบแบบสอบถามในเอเชียเห็นว่าการอุปกรณ์ของพวกเขาที่ทำงานเป็น ‘ถูกต้อง’ มากกว่า ‘สิทธิ’

จากผู้มองของผู้ใช้งาน เห็นว่า BYOD เป็นที่นิยมเนื่องจากผู้ใช้งานสามารถเข้าถึงโปรแกรมที่ตนเองชินและชอบได้โดยเฉพาะอย่างยิ่งโปรแกรมโซเชี่ยลมีเดียต่างๆ การสื่อสารเฉพาะกลุ่ม (Personal communications) ทั้งนี้ กับ

59% ของผู้ตอบแบบสอบถามในเอเชียยอมรับว่าการสื่อสารส่วนบุคคลที่มีอิทธิพลมาก ไม่มีวันไหนที่พวกเขาไม่มีการเข้าถึงเครือข่ายทางสังคมและ 67% จะหยุดส่ง SMS ได้ไม่ถึง 1 วัน และเมื่อเปรียบเทียบกับค่าเฉลี่ยทั่วโลกแล้ว จะเห็นว่าพนักงานในเอเชียให้ความสำคัญกับอุปกรณ์มือถือของพวกเขาอย่างมีนัยสำคัญสูงกว่าถึง 35% และให้ความสำคัญกับเครือข่ายทางสังคมและ SMS สูงกว่าถึง 47%

ความเข้าใจที่หละหลวมด้านความเสี่ยงทางธุกิจอาจเกิดความขัดขืนต่อนโยบายองค์กรได้

จากกลุ่มคนใช้งาน BYOD รุ่นแรกๆ ในโลกนั้นเข้าใจว่าการนำอุปกรณ์ส่วนตัวของเขามาใช้เพื่อทำงานอาจจะนำพาซึ่งความเสี่ยงให้กับองค์กรของพวกเขา ทั้งนี้ ร้อยละสี่สิบสองของกลุ่มตัวอย่างการสำรวจในเอเชียเชื่อว่าสามารถก่อให้เกิดปัญหาข้อมูลสูญหายและความเสี่ยงต่อภัยคุกคามไอทีที่เป็นอันตรายได้จริง แต่ถึงแม้ว่าจะเห็นความเสี่ยงและนโยบายขององค์กรด้านไอทีอยู่ก็ไม่สามารถหยุดการนำอุปกรณ์ไอทีส่วนตัวมาใช้ได้ ยิ่งไปกว่านั้น เกือบครึ่งหนึ่งของผู้ตอบแบบสอบถามในเอเชีย (47%) ยอมรับว่าพวกเขาได้ขัดขืนหรือจะขัดขืนต่อนโยบายของบริษัทที่ห้ามการใช้อุปกรณ์ส่วนตัวเพื่อการทำงานด้วยซ้ำ

ต่อคำถามเกี่ยวกับนโยบายห้ามการใช้อุปกรณ์ที่ไม่ได้รับการอนุมัตินั้น ตัวเลขยังคงอยู่ประมาณเดียวกันที่ 39% ของผู้ตอบแบบสอบถามในเอเชียที่ยอมรับว่าพวกเขาได้ขัดขืนหรือจะขัดขืนนโยบายนี้อย่างแน่นอน ดังนั้น องค์กรจึงมีความเสี่ยงสูงจากการที่พนักงานใช้อุปกรณ์ที่ไม่ได้รับการอนุมัติ อันที่จริง กว่าสามในสี่ (81%) ของผู้ตอบแบบสอบถามในเอเชียยืนยันว่าพวกเขามีความสนใจในการ Bring Your Own Application – BYOA หรือ จะสร้างโปรแกรมแอปพลิเคชั่นขึ้นเองในที่ทำงานอีกต่อไป

ผลการสำรวจยังชี้อย่างเป็นนัยให้เห็นว่าองค์กรอาจเผชิญการต่อต้านหากดำเนินการรักษาความปลอดภัยบนอุปกรณ์ของพนักงาน ทั้งนี้ ส่วนใหญ่ (54%) ของผู้ตอบแบบสอบถามในเอเชียเห็นว่าตนเองจะเป็นผู้รับผิดชอบในการรักษาความปลอดภัยของอุปกรณ์ส่วนบุคคลที่พวกเขาใช้เพื่อการทำงาน (มิใช่บริษัท) และมี 35% เห็นว่าในที่สุดแล้ว ความรับผิดชอบก็ยังอยู่ที่องค์กรอยู่ดี

“การสำรวจนี้แสดงให้เห็นอย่างชัดเจนความท้าทายที่ยิ่งใหญ่ที่องค์กรเผชิญอยู่เพื่อรักษาปลอดภัยและจัดการกับ BYOD” แพททริค เปร์ซ รองประธานอาวุโสฝ่ายขายต่างประเทศและสนับสนุนแห่งฟอร์ติเน็ตกล่าวว่า “ในขณะที่ผู้ใช้อุปกรณ์ยังต้องการและคาดว่าจะใช้อุปกรณ์ของตัวเองสำหรับการทำงานต่อไป ส่วนใหญ่เพื่อความสะดวกส่วนบุคคล แต่ไม่ต้องการให้องค์กรมาก้าวก่ายรับผิดชอบในการรักษาความปลอดภัยบนอุปกรณ์ของตัวเอง ทำให้ในสถานการณ์นี้ องค์กรจะต้องเร่งปรับกระบวนการควบคุมโครงสร้างพื้นฐานด้านไอทีของพวกเขา โดยต้องสร้างเกราะการรักษาความปลอดภัยที่แข็งแกร่งสำหรับการเข้าถึงของผู้ใช้งานทั้งขาเข้าและขาออกที่เครือข่ายขององค์กร ไม่ใช่

เพียงแค่องค์กรจะจัดการระบบความปลอดภัยสำหรับอุปกรณ์เคลื่อนที่หรือ “Mobile device management – MDM“ เท่านั้น นอกจากนี้ องค์กรไม่สามารถพึ่งพาเทคโนโลยีเดียวในการรับมือกับความท้าทายด้านความปลอดภัยของ BYOD เครือข่าย โดยเห็นว่ากลยุทธ์ด้านรักษาความปลอดภัยเครือข่ายที่มีประสิทธิภาพมากที่สุดคือการที่สามารถควบคุมด้านผู้ใช้งานและแอปพลิเคชั่นมีใช่แค่ตัวอุปกรณ์”