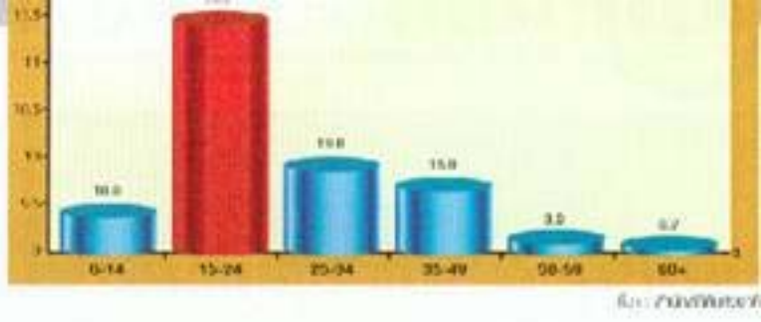

Wireless กับภัยเงียบที่ไม่ธรรมดา

ปัญหาที่เกิดขึ้นควบคู่เป็นเหมือนการจาเงาไปกับความนิยมของระบบแลนไร้สายที่นับวันจะเพิ่มมากขึ้นเรื่อยๆ คือ "ความปลอดภัย" (ซีเคียวริตี้)

อุทัยพัฒน์ รัตนภูผา ผู้จัดการ บริษัท ฟอร์ติเน็ต ประจำประเทศไทยและอินโดจีน ให้ความเห็นกับ eWEEK ว่า ปัญหาใหญ่ของการใช้งานระบบเครือข่ายไร้สาย คือ การไม่มีขีดจำกัด

"การมองไม่เห็นสาย ไม่รู้ว่าขอบเขตอยู่ที่ไหน หากไม่มีระบบรักษาความปลอดภัย บุคคลภายนอก ก็จะสามารถเข้าใช้เครือข่าย ดูข้อมูลได้ ถ้ามีการเปิดแชร์" อุทัยพัฒน์ กล่าว

เขา บอกว่า ระดับความน่ากลัวของการเชื่อมต่อทั้งแบบมีสายและไร้สายเท่ากัน แต่ที่น่าเป็นห่วง คือ ถ้าเป็นแบบไร้สาย แล้วไม่มีระบบรักษาความปลอดภัย เพราะถือเป็นพีซีเดสก์ทอปตัวหนึ่ง เมื่อออกอินเทอร์เน็ตจะไม่สามารถตามรอย และมีระบบแจ้งเตือนเหมือนกับแบบมีสาย

แฮกเกอร์ร้ายกว่าสปายแวร์

ด้าน **ไมค์ โดลน์** ประธานเจ้าหน้าที่บริหารและประธานบริษัท อินเทอร์ลิงค์ เน็ตเวิร์กส์ บอกว่า ต้นตอการคุกคามเครือข่ายไร้สายไม่ได้มาจากสปายแวร์ ซึ่งสามารถกองได้ด้วยไฟร์วอลล์ แต่มาจากผู้ใช้ที่ไม่ได้รับการอนุญาต คือ แฮกเกอร์ ที่สามารถทะลุเข้าสู่เครือข่าย และขโมยข้อมูลสำคัญ จนเป็นเหตุให้เกิดอีกหลายปัญหาตามมา

"สำคัญมากสำหรับองค์กรธุรกิจที่จะต้องตระหนักว่าการไม่มีวิธียืนยันตัวผู้ใช้ ระบบความปลอดภัยเครือข่ายสามารถเจาะโดยแฮกเกอร์ได้เสมอ แม้แต่แฮกเกอร์มือใหม่" โดลน์ กล่าว

ทั้งนี้ ผลการศึกษาล่าสุดของบริษัทดิฟฟิวชันกรุ๊ป ระบุว่า องค์กรธุรกิจส่วนใหญ่ยังนิยมใช้ซอฟต์แวร์ หรือฮาร์ดแวร์ที่เบลออนไฟร์วอลล์ ซึ่งไม่มีการยืนยันตัวผู้ใช้

ป้องกันเท่าไหร่ก็ไม่พอ

คุทัยพัฒน์ กล่าวสรุปว่า การต่อกับเน็ตทั้งแบบมีสายและไร้สาย ต้องโดนไวรัสโจมตีแน่นอน เหมือนคนเป็นหวัด โรคที่ไม่มีทางรักษาให้หายได้ แต่หลีกเลี่ยงได้ ซึ่งจะเจอไวรัสมากหรือน้อยขึ้นอยู่กับพฤติกรรมการใช้งานและเทคโนโลยีที่เข้าไปช่วยป้องกัน

"ลำดับขั้นของการป้องกันการโจมตีมีตั้งแต่กันไวรัส กันคนแฮก กันคนโจมตี ซึ่งต้องใช้เทคโนโลยีแอนติไวรัส ไฟร์วอลล์ และไอดีเอส แต่ในท้ายที่สุด ก็คือ ต้องมีระบบแบ็กอัพ เพราะมีโอกาสติดไวรัส และถูกแฮกได้เสมอ" อุทัยพัฒน์ อธิบาย

สำหรับการป้องกันเครือข่ายเรียงตามระดับดังนี้

1 โคลเอ็นต์ พีซีตัวเดียว ไม่ต่อเน็ตเวิร์ก ใส่ยูสเซอร์เนม พาสเวิร์ด

2 เครือข่าย ประกอบด้วยคอมพิวเตอร์หลายตัว มีคอมเซิร์ฟเวอร์ สร้างยูสเซอร์เนม พาสเวิร์ด และออกนโยบายให้ยูสเซอร์เปลี่ยนพาสเวิร์ด

3 ขึ้นมาระดับแอพพลิเคชัน การป้องกันก็จะเป็นเรื่องของไฟร์วอลล์

ระวังภัยร้ายส่งท้ายช่วงปลายปี

ในส่วนของแนวโน้มการโจมตีของไวรัสในอีก 4 เดือนที่เหลือของปีนี้นั้น อุทัยพัฒน์ แสดงความเห็นว่า น่าจะเกิดขึ้นในช่วงเทศกาลวันหยุด โดยเฉพาะช่วงปลายปี ที่ส่วนใหญ่มักมีแนวโน้มมากกว่าช่วงต้นปี

"เหตุผลหนึ่งที่คนเขียนไวรัสขึ้นมา ก็คือ อยากดัง และจะให้ดังต้องมีวันสำคัญมาผูก เพราะนอกจากจะผูกกับวันสำคัญแล้ว ฝรั่งเมื่อหยุดงาน จะหยุดกันจริงๆ เมื่อเปิดมาทำงานงานเยอะ และพอเจอไวรัสโจมตี งานก็จะละดุด และเดือดร้อนกันทั้งหน้าทันที" อุทัยพัฒน์ อธิบาย

และเสริมว่า แต่ถึงกระนั้น ก็ขึ้นอยู่กับนโยบายการลงทุนซื้อระบบรักษาความปลอดภัยว่าสามารถเข้าไปทดแทน ป้องกันได้เร็วแค่ไหนด้วย

สำหรับการโจมตีรูปแบบใหม่ๆ จะเป็นในเรื่องของฟิชชิง ฟาร์มมิง ซึ่งเป็นคอนเซ็ปต์ล่แบบเมล์ไม่ได้เป็นไวรัส เบากินเลสของมนุษย์มาใช้

โดยฟิชชิง คือ การส่งอีเมล์หลอกให้เข้าไปที่เว็บไซต์ เพื่อกรอกข้อมูลส่วนตัว เลขที่บัตรประกันสังคม รหัสบัตรเครดิต แต่ถ้าเป็นฟาร์มมิง จะดักเว็บไซต์ที่ไปเข้าเว็บไซต์จริง แล้วมีการเก็บข้อมูล ดักออกมา โดยหลอกให้คนกรอกแล้วใช้ข้อมูลเหล่านั้น เพื่อประโยชน์ด้านการเงิน

"ประเด็นการโจมตีแบบฟิชชิง ฟาร์มมิง คือ ถ้าคนมีสติ คิด ก็ไม่ต้องไปห่วงเรื่องพวกนี้ เพราะไม่เหมือนไวรัส ไม่ได้ทำลายข้อมูล แต่ทำลายบุคคลคนนั้นเท่านั้น" อุทัยพัฒน์ กล่าว

และทิ้งท้ายว่า เรื่องของความปลอดภัยบนเครือข่าย ทุกคนสามารถช่วยกันได้ ด้วยการปรับสามัญสำนึก และพฤติกรรมการทำงานการใช้อินเทอร์เน็ต

"เมื่อองค์กรไปเปิดใช้งาน ก็ควรโฟกัสเรื่องงาน เรื่องความปลอดภัย ก็ควรให้คนอื่นจัดการ แต่ก็ต้องรู้การปฏิบัติตัวพื้นฐานด้วย เหมือนกับซื้อรถมาขับก็ควรห่วงเรื่องขับรถ แต่แน่นอนว่าควรจะรู้เรื่องน้ำ เรื่องน้ำมัน เป็นต้น" eWEEK