วารสารวิชาชีพบัญชี

มุมไอที

มนวิกา พดุงสิทธิ์*

2008 Annual Google Communications Intelligence Report

มุม IT สำหรับนักบัญชีฉบับนี้ ผู้เขียนจะสรุปเนื้อหาของ Annual Google Communications Intelligence Report ซึ่งเป็นรายงานประจำปี ค.ศ. 2008 ของกูเกิลมาเล่าสู่กันฟัง เพื่อ Update เรื่องราวด้านการรักษาความปลอดภัยของระบบคอมพิวเตอร์และการสื่อสาร แต่ก่อนที่จะเล่าถึงเนื้อหาของรายงาน ผู้เขียนขอเล่าถึงที่มาของรายงานฉบับนี้ก่อน

เมื่อเดือนกรกฎาคมปีที่แล้ว กูเกิลได้ซื้อบริษัทรักษาความปลอดภัยระบบเมล์ที่ชื่อว่า Postini ซึ่งบริษัทดังกล่าวจัดว่าเป็นผู้นำทางด้านโปรแกรมรักษาความปลอดภัยและป้องกันสแปม กูเกิลเข้าซื้อ Postini โดยมีวัตถุประสงค์หลักสองประการคือ ประการแรกเป็นการแสดงให้เห็นว่ากูเกิลมีความจริงจังที่จะนำระบบแอปพลิเคชั่นของกูเกิลเข้าสู่ตลาด และประการที่สองการซื้อ Postini ทำให้กูเกิลเข้าถึงข้อมูลที่สำคัญ เนื่องจาก Postini มีฐานลูกค้าที่เป็นหน่วยธุรกิจมากกว่า 35,000 ธุรกิจและฐานลูกค้าที่เป็นผู้ใช้ระบบมากกว่า 10 ล้านคนทั่วโลก และเมื่อเป็นเจ้าของ Postini แล้ว กูเกิลได้มุ่งเป้าหมายการทำตลาดด้านบริการรักษาความปลอดภัยสำหรับการป้องกันสแปม การป้องกันไวรัส และการเก็บรักษาข้อมูลจดหมายอิเล็กทรอนิกส์ไปยังธุรกิจขนาดกลางและขนาดย่อมที่ต้องการบริการดังกล่าวในราคาที่ไม่แพง

* Ph.D (Accounting) ผู้ช่วยศาสตราจารย์ประจำ ภาควิชาการบัญชี ผู้อำนวยการโครงการปริญญาโททางการบัญชี คณะพาณิชยศาสตร์และการบัญชี มหาวิทยาลัยธรรมศาสตร์
คณะกรรมการวิชาชีพด้านการศึกษาและเทคโนโลยีการบัญชี สภาวิชาชีพบัญชีฯ

ปีที่ 4 ฉบับที่ 9
เมษายน 2551
หน้า 16-19

การซื้อ Postini ทำให้กูเกิลก้าวเข้าสู่ธุรกิจด้านการรักษาความปลอดภัย และเช่นเดียวกับธุรกิจอื่นๆ ในอุตสาหกรรมนี้ที่จะต้องมีการจัดทำรายงานและพยากรณ์ทิศทางเกี่ยวกับสถานการณ์ด้านการรักษาความปลอดภัยของระบบคอมพิวเตอร์ กูเกิลได้ทำงานวิจัยประกอบกับข้อมูลที่ได้จาก Postini เพื่อแสดงให้เห็นถึงอันตรายของโลกออนไลน์ในปัจจุบัน และนี่จึงเป็นที่มาของรายงานที่มีชื่อว่า 2008 Annual Google Communications Intelligence Report

ในงานวิจัยดังกล่าว กูเกิลได้จัดทำแบบสอบถามทางออนไลน์ขึ้นเมื่อสิ้นปี ค.ศ. 2007 สำหรับกลุ่มตัวอย่างซึ่งเป็นผู้ที่มีอาชีพเกี่ยวข้องกับระบบการสื่อสาร รวมทั้งการสัมภาษณ์เก็บข้อมูลจาก CEO (Chief Executive Officer) CIO (Chief Information Officer) และ CTO (Chief Technical Officer หรือ Chief Technology Officer) จากองค์กรทั้งขนาดเล็กและขนาดใหญ่ เพื่อให้ทราบถึงการสื่อสารที่นิยมใช้กันในอดีต รวมถึงแนวโน้มที่สำคัญของการสื่อสารทางธุรกิจในอนาคต

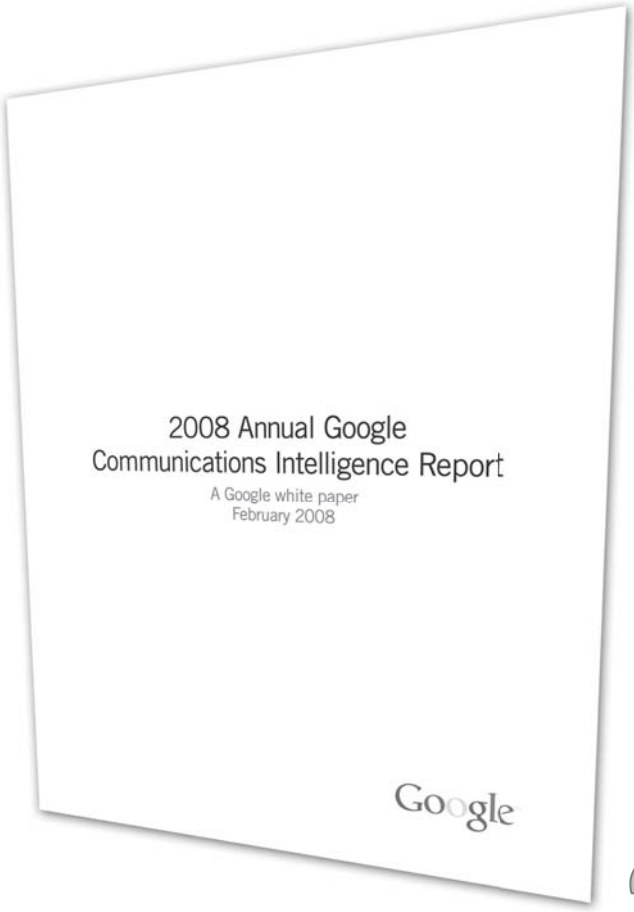
กูเกิลได้คาดการณ์ว่า แม้ว่าปริมาณภัยคุกคามต่อระบบจะไม่เพิ่มขึ้นในปี ค.ศ. 2008 ในสัดส่วนเดียวกันกับอัตราการเพิ่มในปี ค.ศ. 2007 แต่ความซับซ้อนของภัยคุกคามเหล่านี้จะเพิ่มขึ้น ธุรกิจจะต้องเผชิญกับมัลแวร์หรือโปรแกรมประสงค์ร้าย (Malicious Application; Malware) ประเภทต่างๆ ที่หลากหลายมากขึ้น รวมทั้งจะต้องป้องกันข้อมูลที่เป็นความลับที่อาจจะรั่วไหลจากวิธีการ Social Engineering ซึ่งเป็นเทคนิคที่ผู้ไม่หวังดีใช้ในการหลอกล่อพนักงานขององค์กรให้เปิดเผยข้อมูลที่เป็นความลับ กูเกิลจึงคาดว่าองค์กรต่างๆ จะเพิ่มความสนใจไปที่นโยบายการตรวจสอบการส่งข้อความและการเข้ารหัสข้อมูลมากขึ้น

นอกจากนี้ จากข้อมูลของ Postini ซึ่งแสดงให้เห็นว่าปีที่ผ่านมาระบบเครือข่ายถูกคุกคามด้วยสแปมและไวรัสมากที่สุดเป็นประวัติการณ์ กูเกิลจึงคาดว่า สแปมยังคงเป็นภัยคุกคามอันดับหนึ่งสำหรับองค์กรส่วนใหญ่ ดังนั้นจึงขอเสริมเรื่องสแปมในส่วนนี้เพื่อให้ผู้อ่านได้รู้จักกับสแปมมากขึ้น

สแปมเป็นการใช้ระบบการสื่อสารทางอิเล็กทรอนิกส์ในทางที่ไม่ถูกต้องโดยมีวัตถุประสงค์เพื่อส่งข้อความออกไปให้กับผู้รับเป็นจำนวนมาก โดยที่ผู้รับข้อความนั้นไม่ได้ขอให้มีการส่งข้อความดังกล่าวมาให้ และผู้ส่งก็ไม่จำเป็นต้องรู้จักกับผู้รับมาก่อน สแปมที่เราพบเห็นกันบ่อยก็คือ สแปมเมล์ หรือที่บางคนเรียกว่าอีเมล์ขยะ (Junk Mail) ซึ่งผู้ส่งมักจะใช้โปรแกรมเป็นเครื่องมือในการหว่านแหส่งอีเมล์ไปให้ได้มากที่สุด โดยมีวัตถุประสงค์ส่วนใหญ่เพื่อโฆษณาสินค้าหรือบริการ หรือสแปมโดยการส่ง SMS ทางโทรศัพท์มือถือ หรือสแปมโดยการส่งข้อความผ่าน Instant Messaging Service เป็นต้น

สแปมเกิดขึ้นครั้งแรกในปี ค.ศ.1978[1] โดย Gary Thuerk นักการตลาดของบริษัท Digital Equipment Corporation (DEC) ที่ต้องการส่งข่าวเกี่ยวกับสินค้าตัวใหม่ของบริษัท ซึ่งก็คือระบบคอมพิวเตอร์ที่พัฒนาขึ้นมาใหม่ Thuerk ใช้ระบบเครือข่ายคอมพิวเตอร์ของรัฐบาลและมหาวิทยาลัยที่เรียกว่าอาร์พาเน็ต (Arpanet) ในการส่งอีเมล์เพียงฉบับเดียวให้กับผู้รับทั้งหมดพร้อมๆ กัน ทำให้เขาไม่ต้องเสียเวลาโทรศัพท์หรือส่งข้อความให้กับผู้รับทีละคน แม้ว่าปฏิกิริยาที่ได้รับจากการส่งอีเมล์ในครั้งนั้นเป็นไปในทางลบ เนื่องจากเป็นการใช้เครือข่ายอาร์พาเน็ตที่ผิดวัตถุประสงค์ แต่ DEC ก็สามารถขายระบบคอมพิวเตอร์ได้มากกว่า 20 ระบบ ในราคาเฉลี่ยระบบละ 1 ล้านเหรียญสหรัฐ Thuerk ถูกตำหนิอย่างรุนแรง แต่เขาก็ยังเห็นว่าการกระทำของเขาไม่ได้ก่อให้เกิดอันตรายใดๆ ตรงกันข้ามเขา (และคนอีกจำนวนมาก) กลับเห็นว่า เครือข่ายเป็นสัญลักษณ์ใหม่ของความเป็นอิสระทางปัญญา

1 Spinner, M. (2007), "Damn Spam: The losing war on junk e-mail", *The New Yorker;* March 17.



จริงๆ แล้วจะกล่าวว่าสแปมไม่ได้ก่อให้เกิดอันตรายก็คงไม่ถูกต้องนัก เนื่องจากผู้ที่ไม่หวังดีสามารถใช้สแปมในการส่งต่อไวรัสคอมพิวเตอร์ หรือมัลแวร์อื่นๆ เพื่อใช้ในการขโมยข้อมูลส่วนตัว หรือเพื่อล่อลวงให้ผู้หลงเชื่อทำตามที่ตนต้องการโดยใช้เทคนิคที่เรียกว่า Phishing สภานิติบัญญัติของรัฐแคลิฟอร์เนียเปิดเผยว่า เฉพาะปี ค.ศ. 2007 ธุรกิจของสหรัฐอเมริกามีค่าใช้จ่ายเกี่ยวกับสแปมมากกว่า 13,000 ล้านเหรียญสหรัฐ ซึ่งต้นทุนดังกล่าวรวมถึงความสามารถในการผลิตหรือการให้บริการที่ลดลง ต้นทุนในการจัดหาอุปกรณ์ ซอฟต์แวร์และกำลังคนเพื่อจัดการกับสแปม

ในปี ค.ศ. 2007 ในขณะที่ปริมาณอีเมล์ต่อผู้ใช้เพิ่มขึ้นจากปีที่ผ่านมาร้อยละ 47 แต่ปริมาณสแปมเพิ่มขึ้นถึงร้อยละ 57 ในช่วงเวลาเดียวกัน Postini ได้ป้องกันสแปม (Block) สแปมมากกว่าในปีที่ผ่านมาถึงร้อยละ 160 ซึ่งปริมาณสแปมที่เพิ่มขึ้นมากส่วนหนึ่งเป็นผลมาจากบอตเน็ต (BOTNET) นั่นคือการที่คอมพิวเตอร์จำนวนมากที่ถูกควบคุมโดยแฮกเกอร์ ถูกสั่งการให้ส่งข้อความหรือไวรัสผ่านเครือข่ายโดยที่เจ้าของเครื่องคอมพิวเตอร์ไม่รู้ตัว ในช่วงแรกของปี ค.ศ. 2007 สแปมจะอยู่ในรูปของไฟล์รูปภาพที่แนบมากับอีเมล์ แต่ในช่วงครึ่งหลังของปีได้เปลี่ยนรูปแบบเป็นไฟล์เอกสาร ไฟล์ PDF ไฟล์กระดาษทำการ รวมทั้งไฟล์ MP3

ในปี ค.ศ. 2008 กูเกิลคาดว่าสแปมยังคงเป็นเรื่องใหญ่ที่สุดที่ธุรกิจจะต้องให้ความสนใจ แต่ปริมาณของสแปมจะคงที่หรืออาจจะค่อยๆ ลดลง เนื่องจากการโจมตีด้วยสแปมจะมุ่งความสนใจไปที่เป้าหมายมากขึ้น นอกจากนี้ ปัญหาที่น่าเป็นห่วงมากกว่าปริมาณของสแปมก็คือ เราไม่สามารถคาดการณ์ได้ว่าสแปมจะเกิดขึ้นในช่วงใด Postini ได้ยกตัวอย่างให้เห็นว่า ในเดือนสิงหาคมของปีที่ผ่านมาจำนวนสแปมได้เพิ่มขึ้นถึงร้อยละ 100 ภายในช่วงเวลาเพียง 7 วัน ซึ่งองค์กรจะต้องจัดเตรียมทรัพยากรเผื่อไว้ทั้งด้านอุปกรณ์ ซอฟต์แวร์และกำลังคนให้เพียงพอต่อการโจมตีที่อาจจะเกิดขึ้นมากในช่วงใดช่วงหนึ่ง ทำให้ต้นทุนในการกำจัดสแปมเพิ่มสูงขึ้น

นอกจากนี้ ภัยคุกคามสแปมยังมีการโจมตีร่วมกับไวรัส โดยมีวัตถุประสงค์หลักเพื่อขโมยข้อมูลที่แสดงความเป็นตัวตน (Identity) มีการใช้เทคนิค Social Engineering ที่เกี่ยวข้องกับเหตุการณ์ในปัจจุบันเป็นตัวล่อลวงให้เหยื่อหลงเชื่อ เช่น เกม กีฬาต่างๆ หรือภัยพิบัติทางธรรมชาติที่อาจจะเกิดขึ้น การขโมยข้อมูลจะมาจากเว็บไซต์ที่ให้ผู้ใช้กำหนดเนื้อหา (Content) ด้วยตนเอง เช่น Blogs หรือเว็บที่ใช้ในการประมูลราคาสินค้าเป็นต้น นอกจากนี้ การโจมตีด้วยไวรัสยังมีเป้าหมายที่มุ่งขโมยข้อมูลของผู้บริหารที่แฮกเกอร์สามารถนำไปขายได้ในตลาดมืด ซึ่งการโจมตีเหล่านี้จะทำให้ดูเหมือนว่ามาจากหน่วยงานที่ถูกต้องตามกฎหมาย เช่น กรมสรรพากร หรือตลาดหลักทรัพย์ กูเกิลคาดว่าจะมีการโจมตีในรูปแบบ

ดังกล่าวมากขึ้น ส่งผลให้องค์กรธุรกิจและหน่วยงานรัฐบาลอาจถูกละเมิดข้อมูลที่สำคัญ ซึ่งการที่ข้อมูลสำคัญถูกล่วงละเมิดก็จะเป็นแรงกดดันให้หน่วยงานมีการปรับแนวทางปฏิบัติเกี่ยวกับอีเมล์ เช่น ลบลิงค์หรือ URL ที่จะใช้ดาวน์โหลดไฟล์ออกจากอีเมล์ที่ส่งให้กับลูกค้า

ในงานวิจัยนี้ นอกจากจะแสดงให้เห็นว่าการกำจัดสแปมและมัลแวร์เป็นเรื่องสำคัญอันดับหนึ่งแล้ว ผู้ตอบแบบสอบถามยังเห็นว่าเรื่องสำคัญรองลงมาคือ องค์กรธุรกิจเฉพาะ เช่น ธุรกิจด้านบริการวิชาชีพ ด้านการเงิน ด้านกฎหมาย ด้านบริการสุขภาพ เป็นต้น ควรจะทำให้เกิดความมั่นใจได้ว่าการสื่อสารขององค์กรธุรกิจเหล่านี้เป็นไปตามกฎระเบียบของหน่วยงานกำกับดูแล เนื่องจากอุตสาหกรรมเหล่านี้ต้องปฏิบัติตามกฎระเบียบอย่างมาก จึงเปรียบเสมือนกับตัวเปรียบเทียบที่ทำให้เห็นว่ากฎระเบียบจะส่งผลกระทบต่ออุตสาหกรรมอื่นอย่างไร ส่วนบริษัทในตลาดหลักทรัพย์ก็จะต้องมีการบันทึกข้อมูลอย่างโปร่งใสตาม Sarbanes-Oxley Act อีกเรื่องหนึ่งที่ผู้ตอบแบบสอบถามเห็นว่ามีความสำคัญคือ ความปลอดภัยของการเข้าใช้เว็บ เนื่องจากธุรกิจมีปฏิสัมพันธ์กับลูกค้าโดยใช้เว็บไซต์มากขึ้น ซึ่งอาจเป็นช่องให้มีการคุกคามจากมัลแวร์

งานวิจัยนี้ยังคาดว่าในปี ค.ศ. 2008 หน่วยงานธุรกิจและองค์กรต่างๆ จะหันมาใช้นโยบายการตรวจสอบเนื้อหาของอีเมล์ที่ส่งออกไปมากขึ้น มีการใช้ระบบเพื่อตรวจสอบและบังคับใช้นโยบายดังกล่าวเพื่อป้องกันการรั่วไหลของข้อมูลที่สำคัญ องค์กรจะมีความต้องการจัดการและเก็บรักษาข้อมูลส่วนตัวของลูกค้ามากขึ้น ซึ่งจะทำให้การเข้ารหัสข้อมูลและการเก็บรักษาข้อมูลมีความสำคัญมากขึ้น

สุดท้าย กูเกิลมีข้อเสนอแนะเพื่อให้องค์กรเตรียมรับมือกับภัยคุกคามต่างๆ ข้างต้น ดังนี้คือ องค์กรควรจะป้องกันตนเองด้วยการใช้โซลูชั่นป้องกันสแปมและมัลแวร์ (ซึ่งก็ไม่เป็นเรื่องที่น่าแปลกใจ เพราะกูเกิลกำลังก้าวเข้ามาสู่ตลาดนี้) รวมทั้ง update โซลูชั่นและแอปพลิเคชั่นต่างๆ ที่ใช้งานอยู่เสมอ เช่น เว็บเบราเซอร์ เพื่อให้มีระดับความปลอดภัยสูงขึ้น กำหนดนโยบายการใช้อีเมล์ ตรวจสอบเนื้อหา (content) ของอีเมล์ที่รับเข้าและส่งออก มีการเข้ารหัสข้อมูลในอีเมล์ที่มีข้อมูลที่เป็นความลับ รวมทั้งกำหนดนโยบายและตรวจสอบการใช้เว็บไซต์ในที่ทำงาน ที่สำคัญคือองค์กรควรให้ความรู้ผู้ใช้ระบบเกี่ยวกับภัยคุกคามต่างๆ เพื่อให้ผู้ใช้มีความระมัดระวังในการใช้ระบบมากขึ้น

JAP