

## ป้องกันองค์กรให้ปลอดภัยจาก SPAM Mail บนเครือข่ายอินเทอร์เน็ต

นายนรินทร์ พนาवास

(ผู้ช่วยอธิการบดีฝ่ายบริหาร มหาวิทยาลัยศรีปทุม วิทยาเขตชลบุรี)

e-Mail: narin.pa@east.spu.ac.th

สแปมเมลล์ (Spam Mail) คือจดหมายอิเล็กทรอนิกส์ ( e-Mail) ที่ถูกส่งมาให้ผู้รับจำนวนมาก หรือจดหมายขยะที่ไม่พึงประสงค์ (Junk Mail) โดยผู้รับอาจไม่ต้องการรับก็ได้ ในปัจจุบันต้องยอมรับว่าการส่งสแปมเมลล์ได้เพิ่มมากขึ้นทุกวันบนระบบเครือข่ายอินเทอร์เน็ต เช่น จดหมายโฆษณาสินค้าและบริการ โดยเฉพาะอย่างยิ่งจดหมายที่ชักชวนให้เข้าไปยังเว็บไซต์ ลามก เว็บไซต์เล่นการพนัน หรือจดหมายที่ไม่พึงประสงค์ เป็นต้น ส่งผลกระทบต่อเนื้อที่การใช้เมลล์ของผู้ใช้งานอาจเต็ม หรือสร้างความรำคาญในการเปิดอีเมลล์แต่ละครั้งเหตุเพราะได้รับจดหมายเข้ามาเป็นจำนวนมาก

ระบบการจัดส่งอีเมลล์ประกอบด้วย เซิร์ฟเวอร์ที่เป็นตัวหลัก เซิร์ฟเวอร์ทำหน้าที่เป็นตู้จดหมายให้กับผู้ใช้ ผู้ใช้แอดเดรสประจำเซิร์ฟเวอร์ที่ตนเองเป็นสมาชิกอยู่ เซิร์ฟเวอร์ยังทำหน้าที่ที่สำคัญคือ เป็นผู้รับส่งจดหมายระหว่างกันโดยใช้โปรโตคอลที่ชื่อ SMTP(Simple Mail Transfer Protocol) และผู้ใช้งานแต่ละคนจะมี Mail Box ซึ่งเป็นที่เก็บจดหมาย



วิธีการสร้างสแปมเมลล์นั้นอาศัยช่องโหว่ของระบบเมลล์ เช่นการติดต่อผ่านเข้าไปยังพอร์ตเมลล์ ของเซิร์ฟเวอร์แล้วทำการส่งเมลล์ออกไปยังที่อื่นๆ การส่งเมลล์ด้วยวิธีการส่งตรงให้พอร์ตของ Mail Sender จึงไม่จำเป็นต้องมี Mail Box ในเซิร์ฟเวอร์นั้น ดังนั้นจึงสามารถปลอมแปลงแอดเดรสต้นทางได้ ขณะเดียวกันก็ส่งไปยังเป้าหมายปลายทางที่ใดก็ได้ โดยใช้ตัวรับส่งเมลล์ของเซิร์ฟเวอร์เป็นผู้ส่งให้ วิธีการค้นหาคนที่สร้างสแปมเมลล์ ( Spammer) นั้นเป็นเรื่องยาก เพราะพวกเขาเหล่านั้นมีวิธีการอำพรางตัวที่รอดพ้นจากการตรวจสอบและติดตาม

การส่งเมลล์ยังทำได้ด้วยการอาศัยจุดอ่อนของระบบรับ-ส่งเมลล์ ซึ่งองค์กรต่างๆจำนวนไม่น้อยที่ได้ติดตั้งระบบเมลล์เซิร์ฟเวอร์ ( Mail Server) ยังขาดความรู้เกี่ยวกับการดูแลและป้องกัน

ระบบเมลเซิร์ฟเวอร์บนระบบปฏิบัติการ UNIX, LINUX, Windows 2000 และ Windows 2003 ซึ่งมีการสร้างระบบรับ-ส่งเมล โดยรับ-ส่งเมลผ่านทางระบบ POP3 (Post Office Protocol version 3) และ IMAP ทำให้ผู้ใช้ระบบเมลไคลเอนต์สามารถใช้เว็บเบราว์เซอร์ หรือโปรแกรมประเภท Microsoft Outlook เชื่อมต่อเข้ากับเซิร์ฟเวอร์โดยตรง และขอฝากส่งเมลได้โดยไม่ต้องมีเมลบ็อกซ์อยู่บนระบบเมลเซิร์ฟเวอร์

หากองค์กรใดๆ ที่ไม่มีการดูแลและป้องกันระบบเมลเซิร์ฟเวอร์ที่ดี ก็อาจทำให้เป็นแหล่งที่ส่งสแปมเมลไปยังที่ต่างๆ ทั่วโลก ส่งผลให้เกิดผลกระทบกับองค์กรโดยทำให้ขนาด Bandwidth ของระบบเครือข่ายเพิ่มขึ้นโดยไม่ทราบสาเหตุ และหากถึงขั้นร้ายแรงอาจทำให้ระบบเมลขององค์กรโดนบัญชีดำ (Blacklist) จากองค์กรต่างๆ ทั่วโลก ไม่ให้ทำการติดต่อกับระบบเมลองค์กร ที่เป็นแหล่งกำเนิดสแปมเมล ทำให้องค์กรนั้นๆ เสื่อมเสียชื่อเสียง ที่ปล่อยหรือเป็นใจให้มีการส่งสแปมเมลออกไป หากต้องการตรวจสอบว่าระบบเมลเซิร์ฟเวอร์ขององค์กรว่าติด Blacklist หรือไม่ สามารถตรวจสอบหาข้อมูลได้ที่เว็บไซต์ [www.spamcop.net](http://www.spamcop.net)

จากที่กล่าวมาข้างต้น องค์กรต้องมีวิธีการบริหารจัดการ ระบบเมลเซิร์ฟเวอร์อย่างมีประสิทธิภาพ และป้องกันการเข้าใช้บริการจากที่อื่นๆ ไม่ให้สามารถเข้ามารับ-ส่งเมล ภายในองค์กรของเราได้ถ้าไม่ได้เป็นสมาชิก โดยวิธีการทำระบบ Mail Relay ที่เมลเซิร์ฟเวอร์หรือการกำหนด Host และ IP Address ที่สามารถเข้าใช้งานได้เฉพาะสมาชิก ภายในองค์กรเท่านั้น สามารถดูรายละเอียดเพิ่มเติมได้ที่เว็บไซต์ [www.sendmail.org](http://www.sendmail.org) , [www.qmail.org](http://www.qmail.org) , [www.isaserver.org](http://www.isaserver.org) และ [www.microsoft.com](http://www.microsoft.com) เป็นต้น เพื่อไม่ให้ผู้อื่นใช้ประโยชน์จากเมลเซิร์ฟเวอร์ขององค์กรส่งสแปมเมลออกไปภายนอก การเพิ่มประสิทธิภาพระบบการตรวจสอบและป้องกันสแปมเมลที่ผ่านเข้า-ออกบนระบบเครือข่ายอินเทอร์เน็ตขององค์กร สามารถติดตั้งระบบ Mail ANTI-SPAM Gateway เช่น โปรแกรม TREND MICRO, SPAM Fighter เป็นต้น และการติดตั้งโปรแกรม ANTI-SPAM ที่เครื่องคอมพิวเตอร์ของผู้ใช้งาน เพื่อกรองจดหมายแบบละเอียดอีกชั้นหนึ่ง เช่น โปรแกรม MailWasher, โปรแกรม McAfee SpamKiller, โปรแกรม Norton AntiSpam และโปรแกรม Spam Buster เป็นต้น เพราะในปัจจุบันการส่งสแปมเมลนั้นได้เปลี่ยนวิธีการส่งได้หลายรูปแบบ ทำให้บางครั้งระบบโปรแกรมตรวจสอบไม่สามารถป้องกันได้ 100 เปอร์เซ็นต์

ดังนั้นองค์กร ควรให้คำแนะนำ แก่ผู้ใช้งานทุกคน พยายามหมั่นเข้าไปตรวจสอบและลบจดหมายที่ไม่จำเป็นออกจาก Mail Box ของตนเอง เพื่อเป็นการเพิ่มเนื้อที่ ในการรับจดหมายได้ตลอดเวลา และ ไม่ให้ผู้ใช้งานนำ e-Mail ของตนไปลงทะเลเบียนตามเว็บไซต์และ Webboard ต่างๆ เพราะจะทำให้ตกเป็นเหยื่อของ Spammer ทำให้ได้รับจดหมายขยะส่งมาอย่างต่อเนื่อง