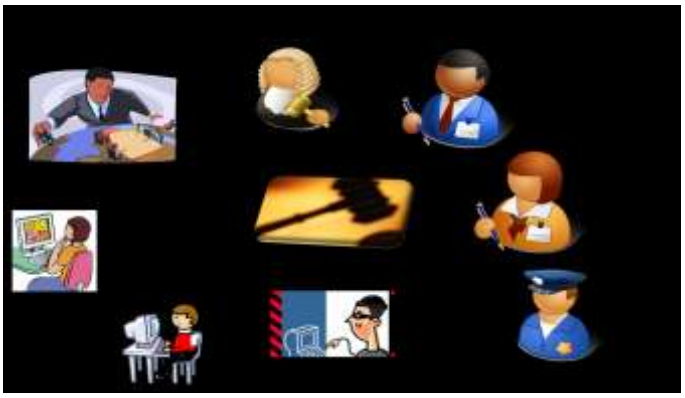
เตรียมความพร้อมในการปฏิบัติตาม พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ที่พึ่งมีผลบังคับใช้เมื่อวันที่ 18 กรกฎาคม 2550 ที่ผ่านมา ถือได้ว่าเป็นกฎหมายที่อยู่ในความสนใจของสาธารณะชนและมีผลกระทบต่อบุคคลทุกกลุ่มอย่างกว้างขวาง ผู้ให้บริการระบบสารสนเทศ (IT) ขององค์กรจะต้องมีความรู้ความเข้าใจ เพื่อที่จะสามารถปกป้ององค์กร สามารถใช้กฎหมายฉบับนี้เอาผิดกับผู้ประสงค์ร้าย รวมไปถึงให้ความร่วมมือกับทางราชการในการตรวจจับผู้กระทำผิดที่อาจจะผ่านมาใช้ระบบเป็นต้น

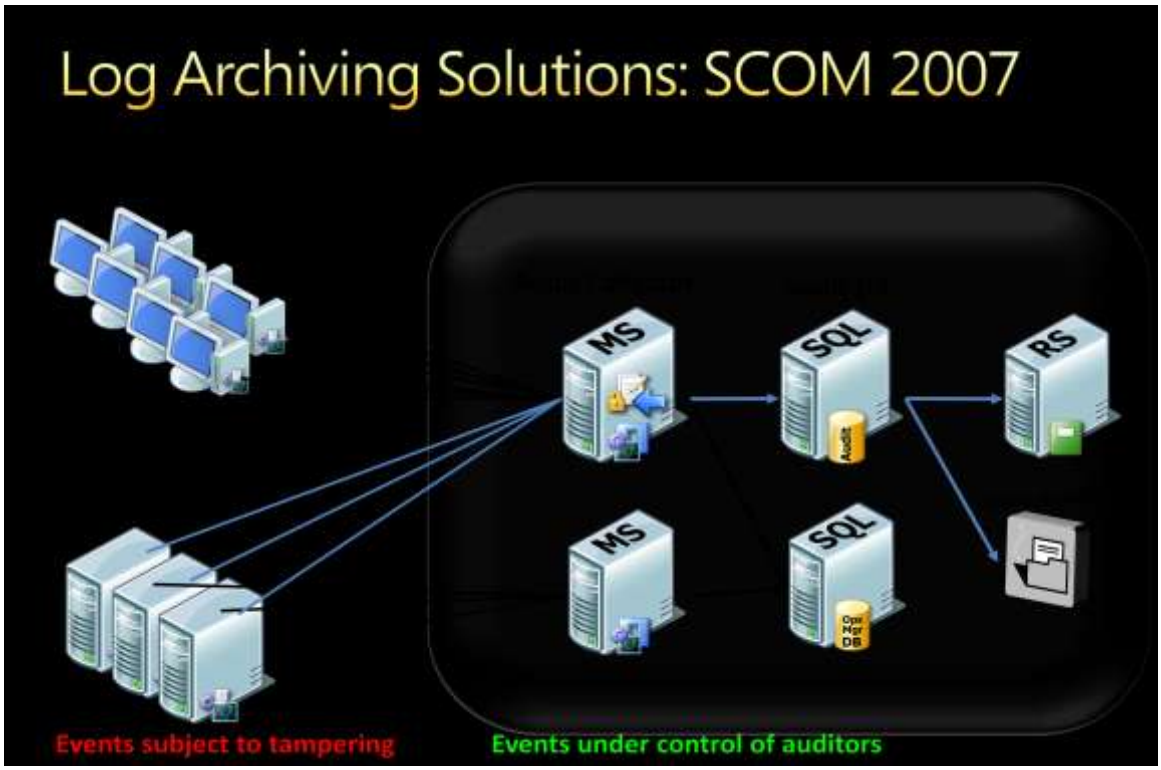


ในลำดับแรก ผู้ดูแลระบบ จำเป็นต้องสำรวจและทำความเข้าใจในโครงสร้างและส่วนประกอบของระบบสารสนเทศ(IT) ในองค์กรของตนเอง ว่าระบบสารสนเทศในองค์กรของท่านมีการให้บริการผู้ใช้งานทั้งภายในและภายนอกองค์กรในการเชื่อมต่อกับเครือข่าย(อินเตอร์เนตและอินทราเนต) และแอปพลิเคชั่นทางเครือข่ายทางใดบ้าง และการให้บริการผ่านเครือข่ายเหล่านั้นมีกลไกการระบุตัวตนผู้ใช้งาน (User Identification)และหมายเลขไอพีแอดเดรส(IP address) ตลอดจนมีข้อมูลจราจร(Log) ที่เก็บข้อมูลผู้ใช้งานและหมายเลขไอพีแอดเดรส, วัน-เวลา ที่ผู้ใช้งานใช้บริการผ่านเครือข่ายเหล่านั้นหรือไม่ ซึ่งบางบริการผ่านเครือข่ายอาจมีกลไกการระบุตัวตนผู้ใช้แต่ไม่ได้ติดตั้งการสร้างข้อมูลจราจรซึ่งผู้ดูแลระบบจะต้องติดตั้ง(Enable) เพิ่มเติม หรือบางบริการเครือข่ายอาจไม่มีกลไกในการระบุตัวตนผู้ใช้งาน ซึ่งผู้ดูแลระบบจะต้องจัดหากลไกการระบุตัวตนผู้ใช้งานที่เหมาะสม เช่น การสร้าง User ID อย่างง่ายโดยการเก็บในไฟล์หรือฐานข้อมูล หรือการนำเอา Directory Service เช่น Microsoft Active Directory มาใช้เพื่อเป็นกลไกในการระบุตัวตนของผู้ใช้งาน หากผู้ดูแลระบบ ไม่สามารถจัดเก็บข้อมูลจรารจโดยละเอียดถึงชื่อผู้ใช้แต่ละราย หมายเลขไอพีแอดเดรส และวันเวลา ที่ใช้งานนั้น จะถือว่ามิได้ปฏิบัติตามพระราชบัญญัติฉบับนี้หากพนักงานเจ้าหน้าที่ขอข้อมูลอาจจะถูกปรับหรือจำคุกได้

หลังจากที่ได้จัดเตรียมการระบุตัวตนของผู้ใช้รวมถึงการเตรียมความพร้อมสำหรับการให้บริการทางเครือข่าย ซึ่งจะเป็นแหล่งข้อมูลที่จะเก็บหลักฐานสำคัญในการสืบสวนเมื่อมีการกระทำความผิดตามพระราชบัญญัติฉบับนี้แล้วนั้น ขั้นตอนต่อมาคือ การเก็บรักษาข้อมูลจราจรที่ได้จากบริการทางเครือข่าย โดยจะต้องเก็บในลักษณะที่ไม่ทำให้เกิดความเสียหายหรือสามารถแก้ไขข้อมูลได้ และจะต้องสามารถนำออกมาใช้เป็นหลักฐานได้เมื่อจำเป็น ซึ่งผู้ดูแลระบบจะต้องศึกษาประกาศหลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550 ซึ่งสามารถดาวน์โหลดได้จากเว็บไซต์ของกระทรวงไอซีที (http://www.mict.go.th) หรือเว็บไซต์คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ (http://www.etcommission.go.th/) นอกจากนี้ ผู้ดูแลระบบจะต้องตั้งเวลาของเครื่องเซอร์เวอร์ทั้งหมดในองค์กรให้มีตรงกับเวลามาตรฐาน

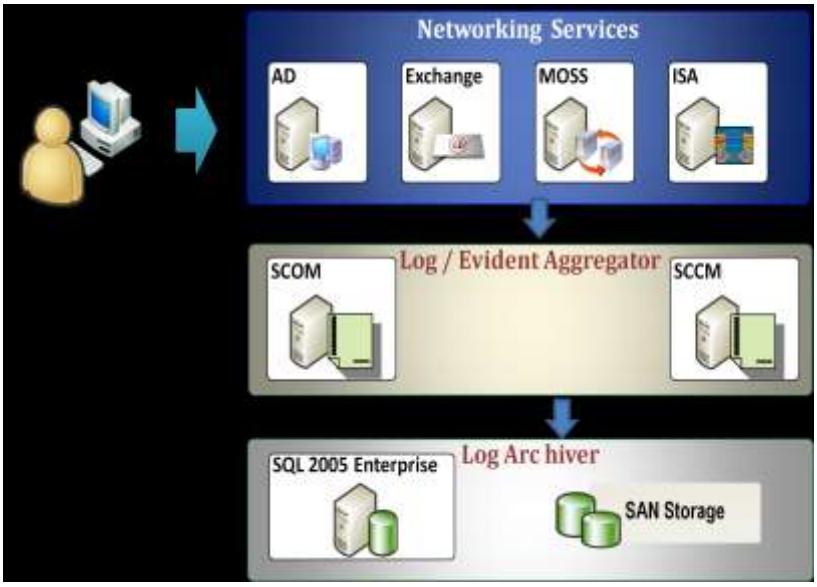
เมื่อผู้ดูแลระบบมีความรู้ความเข้าใจเกี่ยวกับโครงสร้างของระบบสารสนเทศในองค์กรและข้อมูลจราจรที่จำเป็นต้องจัดเก็บแล้ว ขั้นตอนสุดท้ายคือการเลือกเครื่องมือในการจัดเก็บข้อมูลจราจรที่เหมาะสมกับข้อมูลจราจรที่มี รวมไปถึงต้องเลือกเครื่องมือที่เหมาะสมกับลักษณะการให้บริการผ่านเครือข่ายขององค์กรว่ามีความเสี่ยงต่อที่ถูกโจมตีหรืออาจจะถูกใช้เป็นเครื่องมือต่อการกระทำผิดตามที่ระบุไว้ในพระราชบัญญัติฉบับนี้ในระดับใด

สำหรับองค์กรขนาดเล็ก ที่มีเซอร์เวอร์น้อยกว่า 10 เครื่องและ /หรือ ให้บริการผ่านเครือข่ายแก่พนักงาน สำหรับการดำเนินกิจการขององค์กรแบบพื้นฐานเท่านั้น โดยมิได้จัดหาเครื่องมือใดๆ เพิ่มเติม การจัดเก็บข้อมูลจราจร สามารถทำได้โดยการรันชุดคำสั่ง(script) ให้ทำการเก็บรวมรวมข้อมูลจราจร (archive) บนเครื่องเซอร์เวอร์ต่างๆที่มี ไปรวบรวมไว้ในไฟล์เซอร์เวอร์ที่ส่วนกลางอัตโนมัติตามเวลาที่กำหนด ซึ่ง Windows Server 2003 R2 สามารถกำหนด Scheduler ให้สามารถทำคำสั่งอัตโนมัติดังกล่าวได้ตามรอบเวลาที่กำหนด เช่นทุกเที่ยงคืนของทุกวัน เป็นต้น ซึ่งสามารถดูตัวอย่างชุดคำสั่งได้จาก http://msdn.microsoft.com โดยค้นหาคำว่า ‘log archiving script’ และเลือกชุดคำสั่งที่เหมาะสมกับการให้บริการทางเครือข่ายในองค์กรของท่าน



สำหรับองค์กรขนาดกลาง ที่มีเซอร์เวอร์มากกว่า 10 เครื่องแต่น้อยกว่า 30 เครื่อง และ/หรือ ให้บริการผ่านเครือข่ายแก่พนักงานจำนวนมากและให้บริการผ่านเครือข่ายที่หลากหลาย , ผู้ใช้งานสามารถการเชื่อมต่อกับเครื่อข่ายสารสนเทศขององค์กรในหลายรูปแบบ, มีทีมผู้ดูแลระบบหลายท่าน และ/หรือให้บริการข้อมูลแก่บุคคลภายนอกเช่น Web site ซึ่งองค์กรขนาดกลางจะมีระดับความเสี่ยงที่ระบบสารสนเทศขององค์กรจะถูกโจมตีหรือเป็นเครื่องมือต่อการกระทำผิดตามพระราชบัญญัติฉบับนี้ มากขึ้นกว่าองค์กรขนาดเล็กที่ให้บริการแต่พนักงานขององค์กรเท่านั้น สำหรับเครื่องมือที่เหมาะสมกับองค์กรขนาดกลาง จะต้องมีความสามารถในการจัดเก็บข้อมูลจราจรที่มีจำนวนมากขึ้น และมีมาตรการในการปกป้องการจัดเก็บข้อมูลจราจรที่สูงขึ้นและจะต้องนำข้อมูลจราจรที่เก็บไว้กลับออกมา (Restore)ได้เมื่อมีการฟ้องร้องหรือมีการร้องขอจากภาครัฐได้โดยง่าย ซึ่งไมโครซอฟท์มีเครื่องมือที่เหมาะสมกับปริมาณข้อมูลจราจรในองค์กรขนาดกลาง คือ Log Parser ที่สามารถดาวน์โหลดได้ฟรีที่เวบไซด์ของไมโครซอฟท์ Log Parser จะทำหน้าที่คัดเลือกข้อมูลจราจรที่ต้องจัดเก็บและส่งต่อให้ SQL Server 2005 Standard Edition ในการจัดเก็บต่อไป การเก็บข้อมูลลงระบบฐานข้อมูลของ SQL Server 2005 นี้จะมีข้อดีคือสามารถกำหนดสิทธิในการเข้าไปแก้ไขหรือลบได้ นอกจากนี้ยังสามารถออกรายงานต่างๆได้อย่างง่ายดายตามความต้องการอีกด้วย

สำหรับองค์กรขนาดใหญ่ ที่มีเซอร์เวอร์มากกว่า 30 เครื่อง และ/หรือ ให้บริการผ่านเครือข่ายแก่พนักงานจำนวนมากและให้บริการผ่านเครือข่ายที่หลากหลาย, ผู้ใช้งานสามารถการเชื่อมต่อกับเครื่อข่ายสารสนเทศขององค์กรในหลายรูปแบบ , มีทีมผู้ดูแลระบบหลายท่าน หรือ หลายทีม และ/หรือให้บริการข้อมูลและกระดานข้อความแก่บุคคลภายนอกเช่น Web site หรือ Web blog สำหรับองค์กรที่มีเครือข่ายสารสนเทศในลักษณะนี้ จะมีระดับความเสี่ยงที่ระบบสารสนเทศขององค์กรจะถูกโจมตีหรือเป็นเครื่องมือต่อการกระทำผิดตามพระราชบัญญัติฯสูงที่สุด ไม่ว่าจะมาจากพนักงานภายในองค์กรหรือภัยคุกคามที่มาจากทางอินเตอร์เนต ซึ่งองค์กรขนาดใหญ่นี้จำเป็นที่จะต้องจัดหาเครื่องมือในการจัดเก็บข้อมูลจราจรที่สามารถรองรับการเก็บข้อมูลจราจรเป็นจำนวนมาก, รองรับรูปแบบข้อมูลจราจรที่หลากหลาย และสามารถจัดเก็บข้อมูลจราจรได้อย่างปลอดภัยซึ่งผู้บุกรุกจะไม่สามารถเปลี่ยนแปลงข้อมูลจราจรได้โดยง่าย รวมทั้งเครื่องมือในการจัดเก็บข้อมูลจราจร



จะต้องสามารถนำข้อมูลจราจรที่จัดเก็บไว้ออกมา (Restore)ได้เมื่อมีการฟ้องร้องหรือมีการร้องขอจากภาครัฐ ซึ่งไมโครซอฟท์มีเครื่องมือในการจัดเก็บข้อมูลจราจรจำนวนมากและปลอดภัย ได้แก่ System Center Operations Manager 2007 ที่ทำงานร่วมกับ SQL Server 2005 Enterprise Edition ในการจัดเก็บข้อมูลจราจรหลากหลายรูปแบบตามลักษณะการให้บริการทางเครือข่ายต่างๆ พร้อมทั้งมีมาตรการรักษาความปลอดภัยในการส่งข้อมูลจราจรกลับมาที่ศูนย์กลางโดยการเข้ารหัสข้อมูลก่อนส่ง และกำหนดมาตรการการเข้าถึงข้อมูลและสามารถเก็บลงสื่อถาวร /กึ่งถาวร(DVD,CD / Storage) เพื่อป้องกันข้อมูลจราจรถูกทำลายหรือเปลี่ยนแปลง นอกจากนี้ System Center Operations Manager 2007 ยังมีรายงานสถิติ(Statistic Report) ที่เป็นประโยชน์มากมายที่องค์กรสามารถนำไปใช้ในการปรับปรุงระบบสารสนเทศให้มีประสิทธิภาพและความปลอดภัยเพิ่มขึ้น และในกรณีที่ต้องการตรวจเช็คว่าเครื่องคอมพิวเตอร์เครื่องใดในองค์กร มีการเก็บรูปหรือ file ที่ขัดกับกฎหมาย รวมไปถึงมีการใช้งานโปรแกรมบางตัวซึ่งมีความสามารถในการเจาะระบบได้ ก็สามารถตรวจจับได้โดยการติดตั้ง System Center Configuration Manager 2007 เพื่อใช้ในการจัดการดังกล่าว ทั้งนี้ การที่จะเข้าไปสืบค้นหาข้อมูลในเครื่องคอมพิวเตอร์ต่างๆนั้น จะต้องกำหนดเป็นนโยบายให้ชัดเจนจะได้ไม่มีปัญหาเกี่ยวกับความเป็นส่วนตัวของผู้ใช้

สนใจสอบถามข้อมูลเพิ่มเติมติดต่อ Microsoft Call Center โทร 02-263-6888

© 2008 Microsoft Corporation. All rights reserved.

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Microsoft is either a registered trademark or trademark of Microsoft in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

*Microsoft Corporation • One Microsoft Way • Redmond, WA 98052-6399 • USA*0704