Microsoft Business Solutions

คู่มือเสริมสร้างความปลอดภัยให้กับ NAVISION

ตีพิมพ์: ตุลาคม 2004

Microsoft

สารบัญ

คำนำ

MICROSOFT® WINDOWS®
จัดเตรียมคุณลักษณะด้านความปลอดภัยของเครือข่ายที่มีมาตรฐานที่สลับซับซ้อน เมื่อดูในวงกว้างที่สุด ความปลอดภัยเกี่ยวข้องกับการวางแผนการและการพิจารณาชั่งน้ำหนักถึงผลดีผลเสีย ตัวอย่างเช่น
การเลือกล็อกคอมพิวเตอร์ไว้ในห้อง ๆ หนึ่ง
และอนุญาตให้ผู้ดูแลระบบหนึ่งคนเท่านั้นที่เข้ามาใช้คอมพิวเตอร์ได้
คอมพิวเตอร์เครื่องนี้อาจมีความปลอดภัย
แต่ไม่มีประโยชน์มากนักเพราะไม่ได้เชื่อมต่อกับคอมพิวเตอร์เครื่องอื่น
คุณจำเป็นต้องพิจารณาวิธีสร้างความปลอดภัยให้กับเครือข่ายให้มากที่สุดโดยไม่ลดทอนความสามารถในการนำมาใช้งาน

องค์กรส่วนใหญ่วางแผนป้องกันการแอบเข้าระบบจากภายนอก
และสร้างไฟร์วอลล์
แต่บริษัทหลายแห่งไม่ได้พิจารณาวิธีการลดปัญหาการเจาะระบบความปลอดภัยทันทีที่ผู้ใช้ที่มีเจตนาร้ายแอบแฝงเข้ามาภายในไฟร์วอลล์
มาตรการด้านความปลอดภัยสำหรับลูกค้าจะทำงานได้อย่างมีประสิทธิภาพ
หากไม่ได้กำหนดให้ผู้ใช้ดำเนินการหลายกระบวนการและหลายขั้นตอนหากจะทำธุรกิจให้ปลอดภัย
การนำนโยบายความปลอดภัยมาใช้ควรเรียบง่ายที่สุดในสายตาของผู้ใช้
หรือผู้ใช้จะต้องเผชิญกับวิธีการทำสิ่งต่าง ๆ
ที่แทบจะไม่มีความปลอดภัยเลย

เนื่องจากขนาดของการติดตั้ง NAVISION นั้นใหญ่มาก สิ่งสำคัญคือ
การพิจารณาอย่างละเอียดถึงความจำเป็นของลูกค้าแต่ละราย
พร้อมชั่งน้ำหนักถึงประสิทธิภาพของมาตรการป้องกันเมื่อเทียบกับค่าใช้จ่ายที่อาจเกี่ยวข้อง เนื่องจากลูกค้าของคุณเชื่อใจที่ปรึกษา
คุณควรใช้วิจารณญาณที่ดีที่สุด
และแนะนำนโยบายที่สอดคล้องกับความต้องการด้านความปลอดภัยของลูกค้า โดยไม่สร้างภาระที่จะเป็นสาเหตุให้ลูกค้าเลิกใช้นโยบายดังกล่าว

หลักปฏิบัติที่ดีที่สุดในเรื่องความปลอดภัยของ NAVISION

กฎเกณฑ์ทั่วไปต่อไปนี้สามารถช่วยเพิ่มความปลอดภัยให้กับสภาพแวดล้อมของ NAVISION:

- หากคุณต้องการเรียกใช้ Navision Database Server ในฐานะบริการหรือใช้พารามิเตอร์บรรทัดคำสั่ง *installasservice* เมื่อคุณเริ่มใช้เซิร์ฟเวอร์ คุณควรตรวจสอบให้แน่ใจว่า บริการดังกล่าวเปิดใช้ในฐานะบัญชีหนึ่งของ NT Authority\Network Service แล้ว บัญชี NT Authority\Network Service จะมีอยู่เฉพาะในโปรแกรม Windows™ XP และ Windows Server™ 2003 หากคุณกำลังเรียกใช้ Windows 2000 Server คุณควรสร้างบัญชีพร้อมสิทธิ์สำหรับบริการเป็นอย่างน้อย หรือเลือกมอบหมายบริการนั้นให้กับบัญชี Local System แต่อย่างมากที่สุด บัญชีนี้น่าจะมีสิทธิ์พิเศษเหมือนกันกับบัญชีผู้ใช้ปกติ หรือเป็นบัญชีโดเมนที่ไม่ใช่ผู้ดูแลระบบในโดเมนหรือบนคอมพิวเตอร์ท้องถิ่นเครื่องใด

  คุณต้องจดจำที่จะทำให้บัญชี NT Authority\Network Service หรือบัญชีผู้ใช้ที่เซิร์ฟเวอร์ทำงานภายใต้สิทธิ์ในการเขียนและอ่านแฟ้มฐานข้อมูล เพื่อให้แน่ใจว่า ผู้ใช้สามารถเชื่อมต่อกับฐานข้อมูลได้

  หากต้องการทำให้บัญชี NT Authority\Network Service มีสิทธิ์อ่านและเขียนแฟ้มฐานข้อมูลบน Windows XP:

  1. ในโปรแกรม Windows Explorer ให้เลื่อนไปยังโฟลเดอร์ที่มีแฟ้มฐานข้อมูล
  2. เลือกแฟ้มฐานข้อมูล และคลิกขวาที่แฟ้มนั้น และคลิก คุณสมบัติ
  3. ในหน้าต่าง ***คุณสมบัติ*** ให้คลิกแท็บ ***ความปลอดภัย*** และใต้ฟิลด์ **กลุ่มและชื่อผู้ใช้** ให้คลิก เพิ่ม
  4. ในหน้าต่าง ***เลือกผู้ใช้ คอมพิวเตอร์ หรือกลุ่ม*** ให้ระบุ *Network Service* และคลิก ตกลง
  5. NETWORK SERVICE จะถูกเพิ่มลงในฟิลด์ **กลุ่มและชื่อผู้ใช้** ในหน้าต่าง ***คุณสมบัติ***
  6. เลือก NETWORK SERVICE และในฟิลด์ **สิทธิ์** กำหนดสิทธิ์เป็นแบบ *อ่าน* และ *เขียน*

- บริการ Navision Application Server จะทำหน้าที่เป็นบัญชี NT Authority\Network Service ตั้งแต่เริ่มแรก ลักษณะนี้ทำให้บริการดังกล่าวเข้าสู่ Navision Database Server ได้ อย่างไรก็ดี เมื่ออยู่บนเครือข่าย คุณต้องแน่ใจว่า บริการ Navision Application Server ทำงานในฐานะบัญชีโดเมนของ Windows ที่ Navision Database Server รับรู้ หากคุณต้องการให้บัญชีนี้มีสิทธิ์เข้าถึงเซิร์ฟเวอร์ฐานข้อมูล บัญชีนี้ไม่ควรเป็นผู้ดูแลระบบไม่ว่าจะเป็นในโดเมนหรือบนคอมพิวเตอร์ภายใน

- หากคุณเรียกใช้ SQL Server Option for Navision โปรแกรม Microsoft SQL Server™ จะทำงานในฐานะของบริการ ทั้งนี้ ตัวเลือก SQL Server สำหรับ Navision ระบุว่า SQL Server ต้องสามารถค้นหา Active Directory ได้ เพื่อเรียกดูรายชื่อกลุ่มผู้ใช้ Windows เพื่อวัตถุประสงค์ในการพิสูจน์ตัวตนที่แท้จริง ดังนั้น คุณต้องแน่ใจว่า บริการ SQL Server ทำงานในฐานะบัญชีของ NT Authority\Network Service

  หากต้องการให้แน่ใจว่า บริการดังกล่าวทำงานในฐานะ NT Authority\Network Service:

  1. บนคอมพิวเตอร์ SQL Server ให้ค้นหาตำแหน่งของบริการ MSSQLSERVER ก่อนคลิกขวาที่บริการดังกล่าว และคลิก คุณสมบัติ
  2. ในหน้าต่าง ***คุณสมบัติ*** ให้คลิกที่แท็บ ***ล็อกออน***
  3. ในแท็บ ***ล็อกออน*** ใต้คำว่า ล็อกออนในฐานะ ให้คลิก บัญชีนี้ และป้อน *NT Authority|NetworkService* ก่อนคลิก ตกลง

  สำหรับข้อมูลเพิ่มเติมเกี่ยวกับความปลอดภัยของ SQL Server โปรดดูที่:

  http://www.microsoft.com/security/guidance/prodtech/SQLServer.mspx

  และ
  http://www.microsoft.com/technet/security/prodtech/dbsql/default.mspx

- หากคุณใช้ผลิตภัณฑ์ธุรกิจอิเล็กทรอนิกส์ของ Navision เช่น Commerce Gateway คุณควรดูให้แน่ใจว่า ได้ติดตั้ง Commerce Gateway Request Server ได้อย่างถูกต้อง พร้อมทั้งมีการตั้งค่าบัญชีเริ่มต้นสำหรับบริการแล้ว การตั้งค่าบัญชีเริ่มต้นนั้นเรียกว่า *CGRSUser* การตั้งค่านี้อนุญาตให้ Commerce Gateway Server เข้าถึงชุดของบริการอื่น ๆ ที่ต้องการเป็นอย่างน้อย รวมถึง บริการ *MSSQLSERVER* และบริการ *BizTalk Service BizTalk Group : BizTalkServerApplication* ไม่ได้รวมการตั้งค่าบัญชีส่วนรวมใด ๆ เหมือนกับที่บัญชี *Local System* ได้รวมเอาไว้
- ใช้รหัสผ่านที่มีความรัดกุมอยู่เสมอ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับรหัสผ่านที่มีความรัดกุม โปรดดูที่หัวข้อ
- ใช้การล็อกอินสำหรับ Windows Navision เปิดโอกาสให้คุณสร้างการล็อกอินสองแบบ – การล็อกอินสำหรับฐานข้อมูล และการล็อกอินสำหรับ Windows เราขอแนะนำให้คุณใช้การล็อกอินสำหรับ Windows เนื่องจากการล็อกอินนี้ใช้คุณลักษณะการตรวจสอบความถูกต้องของ Windows และอนุญาตให้คุณนำนโยบายรหัสผ่านที่เหมาะสมมาใช้
- ไม่ควรนำรหัสผ่านที่เคยใช้แล้วมาใช้ซ้ำ สิ่งหนึ่งที่เกิดขึ้นเป็นประจำคือ การนำรหัสผ่านมาให้ซ้ำแล้วซ้ำเล่าทั่วทั้งระบบและโดเมน ตัวอย่างเช่น ผู้ดูแลระบบที่รับผิดชอบโดเมน 2 โดเมน อาจสร้างบัญชี ผู้ดูแลระบบโดเมน ในแต่ละโดเมนที่ใช้รหัสผ่านตัวเดียวกัน และอาจทำแม้กระทั่งกำหนดรหัสผ่านสำหรับผู้ดูแลระบบท้องถิ่นบนคอมพิวเตอร์โดเมน โดยรหัสผ่านตัวนี้ใช้กับทั้งโดเมน ในกรณีนี้ หากบัญชีหนึ่งหรือคอมพิวเตอร์เครื่องหนึ่งเสี่ยงต่ออันตรายจากภายนอก ย่อมทำให้โดเมนทั้งเครื่องเสี่ยงต่ออันตรายด้วย
- หลังจากติดตั้งโปรแกรม Navision และสร้างหรือปรับปรุงฐานข้อมูลแล้ว คุณควรสร้างการล็อกอินสำหรับ Windows และกำหนดบทบาท SUPER ให้กับล็อกอินนี้ในโปรแกรม Navision ผู้ใช้ที่มีบทบาท SUPER นี้จะเป็นผู้จัดการเรื่องการดูแลฐานข้อมูล ความปลอดภัยของฐานข้อมูล และอื่น ๆ ป้องกันล็อกอินนี้ด้วยรหัสผ่านที่มีความรัดกุม และควรเก็บรหัสผ่านนี้ไว้เป็นความลับ รหัสผ่านนี้ควรรับประกันถึงการป้องกันในระดับเดียวกันกับที่คุณให้กับรหัสผ่าน SA ใน SQL Server การเข้าใช้ฐานข้อมูลทั้งหมดได้รับการจัดการโดยผู้ที่มีบทบาท SUPER และจำเป็นต้องใช้การป้องกันในระดับสูงสุด บุคคลเดียวที่ควรทราบรหัสผ่านของผู้ใช้ที่มีบทบาท SUPER คือ ผู้ดูแลระบบของคุณ
- ผู้ใช้คนอื่น ๆ ทั้งหมดที่เข้าถึงฐานข้อมูล Navison ควรเรียกใช้ฐานข้อมูลนี้ด้วยสิทธิ์ขั้นต่ำที่สุด ซึ่งหมายถึงการมอบหมายบทบาทใน Navision ให้กับพวกเขา โดยบทบาทดังกล่าวควรระบุถึงเฉพาะการเข้าใช้คุณลักษณะและฟังก์ชันการทำงานที่พวกเขาจำเป็นต้องใช้เพื่อทำงานของตนเองในบริษัท
- สร้างหลักประกันว่า เฉพาะผู้ใช้ที่มีบทบาทภายในบริษัทเท่านั้น ที่สามารถนำเข้าแฟ้ม FOB ออกแบบวัตถุอีกครั้ง รวมทั้งสร้างและกู้คืนข้อมูลสำรองสำหรับฐานข้อมูล
- จัดทำสำรองฐานข้อมูล Navision ของคุณอย่างสม่ำเสมอ และต้องทดสอบการทำสำรองเหล่านั้น เพื่อให้แน่ใจว่า ข้อมูลสำรองได้รับการจัดเก็บไว้แล้ว
- จัดเก็บข้อมูลสำรองไว้ในที่ ๆ ปลอดภัยเพื่อลดผลกระทบจากอันตรายต่าง ๆ อาทิเช่น เพลิงไหม้ ควัน ฝุ่น อุณหภูมิที่สูง ฟ้าแลบ และภัยธรรมชาติ (เช่น แผ่นดินไหว)
- แม้โปรแกรม Navision สามารถทำงานบน Windows ในรุ่นต่าง ๆ มากมาย แต่เราขอแนะนำให้คุณใช้ระบบปฏิบัติการรุ่นใหม่ล่าสุดที่มีคุณลักษณะความปลอดภัยใหม่ล่าสุด ซึ่งก็คือ โปรแกรม Windows XP, Service Pack 2 และ Windows Server 2003
- ใช้บริการ Windows Update ที่รวมอยู่ใน Windows 2000, Windows XP และ Windows Server 2003 เพื่อนำคุณลักษณะ ความปลอดภัย ที่ปรับปรุงล่าสุดมาใช้ ใช้คุณลักษณะ Automatic Update ของโปรแกรม Windows เพื่อทำให้เครื่องคอมพิวเตอร์ไคลเอ็นต์ทุกเครื่องมีโปรแกรมปะแก้ความปลอดภัย ชุดบริการ (Service Pack) และชุดปรับปรุงล่าสุด
- เราขอแะนำให้คุณใช้โปรโตคอล TCPS ที่มีความปลอดภัยเพื่อสื่อสารระหว่างเครื่องไคลเอ็นต์ของ Navision และเซิร์ฟเวอร์ฐานข้อมูลของ Navision TCPS เป็นรุ่นที่ปลอดภัยของ TCP/IP และใช้ Security Support Provider Interface (SSPI) ร่วมกับการเข้ารหัส และการตรวจสอบความถูกต้อง Kerberos TCPS คือ โปรโตคอลเริ่มต้นสำหรับเซิร์ฟเวอร์ฐานข้อมูลของ Navision

- ลูกค้าควรมีแผนกอบกู้หายนะไว้รองรับ เพื่อให้แน่ใจว่า จะสามารถกลับมาให้บริการอีกครั้งได้อย่างรวดเร็วหลังเกิดหายนะ แผนกอบกู้ควรมีเนื้อหาที่เกี่ยวข้องกับ:
  - การเตรียมเครื่องมือใหม่/ชั่วคราวไว้รองรับ
  - การเรียกคืนข้อมูลสำรองไว้บนระบบใหม่
  - การทดสอบประสิทธิภาพของแผนกอบกู้หายนะ

ความปลอดภัยทางกายภาพ

ความปลอดภัยทางกายภาพถือเป็นเรื่องที่จำเป็นเร่งด่วนอย่างแท้จริง เนื่องจากไม่มีวิธีใดที่จะทดแทนได้ในเรื่องความปลอดภัยของซอฟต์แวร์ได้ ตัวอย่างเช่น หากฮาร์ดดิสก์ไดร์ฟถูกขโมย แน่นอนว่า ข้อมูลที่อยู่บนไดร์ฟนั้นก็จะถูกขโมยด้วย หารือในประเด็นต่อไปนี้ที่เกี่ยวกับความปลอดภัยทางกายภาพเมื่อร่างนโยบายร่วมกับลูกค้าของคุณ:

- สำหรับการติดตั้งขนาดใหญ่ในแผนกไอทีที่มีความละเอียดอ่อน ควรแน่ใจว่า ได้ล็อคห้องที่ใช้ตั้งเซิร์ฟเวอร์และที่ ๆ จัดเก็บซอฟต์แวร์แล้ว
- เครื่องคอมพิวเตอร์สำหรับแผนการนี้ รวมถึง:
  - เซิร์ฟเวอร์สำหรับ Microsoft SQL Server 2000
  - เซิร์ฟเวอร์แฟ้มที่ ๆ เก็บแฟ้มปฏิบัติการของ Navision
- ป้องกันไม่ให้ผู้ใช้ที่ไม่ได้รับอนุญาตใช้คอมพิวเตอร์
- ให้แน่ใจว่า ได้ติดตั้งสัญญาณเตือนกันขโมยไม่ว่าข้อมูลจะมีความละเอียดอ่อนมากน้อยเพียงใด
- ให้แน่ใจว่า ข้อมูลสำคัญที่ทำสำรองไว้นั้นอยู่นอกพื้นที่ และจัดเก็บไว้ในที่ ๆ มีคุณสมบัติทนไฟ

พนักงาน

สิ่งที่ดีประการหนึ่งคือ จำกัดสิทธิ์ในการดูแลจัดการผลิตภัณฑ์และคุณลักษณะทั้งหมด โดยตั้งแต่เริ่มแรก ลูกค้าควรให้สิทธิ์พนักงานเฉพาะระดับการอ่านฟังก์ชันของระบบเท่านั้น เว้นแต่ต้องเข้ามาทำงานของตัวเอง จึงควรพิจารณาให้สิทธิ์มากขึ้น ไมโครซอฟท์แนะนำให้ปฏิบัติตามหลักเกณฑ์เรื่องสิทธิ์ขั้นต่ำต่อไปนี้: ให้ผู้ใช้มีเพียงสิทธิ์ขั้นต่ำที่ต้องใช้เพื่อเข้าถึงข้อมูลและฟังก์ชันการทำงาน พนักงานที่ไม่พอใจบริษัทและอดีตพนักงานของบริษัทถือเป็นภัยคุกคามความปลอดภัยของเครือข่าย เมื่อหารือในประเด็นความปลอดภัยร่วมกับลูกค้า ควรแนะนำนโยบายต่อไปนี้ซึ่งเกี่ยวข้องกับพนักงาน:

- ดำเนินการไต่สวนภูมิหลังของพนักงานใหม่
- คาดหวังว่าพนักงานที่ไม่พอใจบริษัทหรืออดีตพนักงานของบริษัทจะทำการ "แก้แค้น"
- ดูให้แน่ใจว่า พนักงานได้ยกเลิกบัญชีและรหัสผ่านที่เกี่ยวข้องทั้งหมดของ Windows เมื่อลาออกจากบริษัท สำหรับวัตถุประสงค์ในการรายงาน ไม่ควรลบผู้ใช้ ห้ามนำบัญชีมาใช้ใหม่
- ฝึกอบรมให้ผู้ใช้มีความตื่นตัวและรายงานให้ทราบถึงกิจกรรมใด ๆ ที่น่าสงสัย
- ห้ามรับรองสิทธิ์พิเศษโดยอัตโนมัติ หากผู้ใช้ไม่มีความจำเป็นต้องใช้คอมพิวเตอร์เฉพาะบางเครื่องเข้าไปในห้องคอมพิวเตอร์ หรือแฟ้มที่เก็บไว้เป็นชุด ให้แน่ใจว่า ผู้ใช้เหล่านั้นไม่ได้ทำเช่นนั้นจริง ๆ

- ฝึกอบรมซุปเปอร์ไวเซอร์เพื่อให้ระบุและตอบสนองต่อปัญหาที่อาจเกิดขึ้นกับพนักงาน
- ให้แน่ใจว่า พนักงานเข้าใจบทบาทของตัวเองในเรื่องการรักษาความปลอดภัยของเครือข่าย
- มอบสำเนานโยบายของบริษัทให้กับพนักงานทุกคน
- ไม่อนุญาตให้ผู้ใช้ติดตั้งซอฟต์แวร์ที่นายจ้างไม่เห็นชอบ

ผู้ดูแลระบบ

เราขอแนะนำให้ผู้ดูแลระบบของลูกค้าของคุณติดตามความเคลื่อนไหวในเรื่องคุณลักษณะความปลอดภัยล่าสุดจากไมโครซอฟท์
บรรดาแฮ็คเกอร์มีความชำนาญเพื่อการพลิกแพลงด้วยการรวมบัคขนาดเล็กจนสามารถรุกล้ำเข้าสู่เครือข่าย สิ่งแรกที่ผู้ดูแลระบบควรทำ คือ
ดูให้แน่ใจว่า
คอมพิวเตอร์แต่ละเครื่องมีความปลอดภัยมากที่สุดเท่าที่จะมากได้
ก่อนเพิ่มโปรแกรมปรับปรุงด้านความปลอดภัยลงไป
และใช้ซอฟต์แวร์ป้องกันไวรัส
รายละเอียดเกี่ยวกับการเชื่อมโยงและแหล่งข้อมูลมีอยู่มากมายในเอกสารชุดนี้ เพื่อช่วยคุณค้นหาข้อมูลที่มีค่าและหลักปฏิบัติที่ดีที่สุด

ความสลับซับซ้อนเป็นอีกเรื่องหนึ่งที่อาจส่งผลกระทบต่อการสร้างความปลอดภัยให้กับเครือข่าย ยิ่งเครือข่ายมีความสลับซับซ้อนมากขึ้น
การทำให้เครือข่ายมีความปลอดภัยหรือการแก้ไขในกรณีที่มีผู้แอบเข้ามาในระบบก็ยิ่งยากขึ้นเท่านั้น
ผู้ดูแลระบบควรจัดทำรายการผังเฉพาะส่วนของเครือข่ายทั้งหมด
โดยมีเป้าหมายเพื่อทำให้เครือข่ายมีความเรียบง่ายที่สุด

ความปลอดภัยเป็นเรื่องแรกที่ฝ่ายบริหารความเสี่ยงให้ความสนใจ
การที่เทคโนโลยีไม่สามารถแก้ไขทุกปัญหา
ย่อมทำให้ความปลอดภัยต้องอาศัยทั้งเทคโนโลยีและนโยบายรวมกัน
กล่าวอีกนัยหนึ่งคือ
ไม่เคยมีผลิตภัณฑ์ใดที่คุณเพียงแค่แกะออกจากกล่องและติดตั้งลงบนเครือข่าย และเครือข่ายนั้นจะมีความปลอดภัยอย่างครบถ้วนในฉับพลับทันที
ความปลอดภัยเป็นผลที่ได้มาจากทั้งเรื่องของเทคโนโลยีและนโยบาย—กล่าวคือ
เทคโนโลยีถูกนำมาใช้เพื่อกำหนดระดับความปลอดภัยของเครือข่าย
ไมโครซอฟท์นำเสนอเทคโนโลยีและคุณลักษณะที่ล้วนแต่ให้ความสำคัญในเรื่องของความปลอดภัย
แต่มีเพียงผู้ดูแลระบบภายใต้คำแนะนำของคุณเท่านั้น
ที่สามารถร่างนโยบายที่ถูกต้องสำหรับแต่ละองค์กร ดังนั้น
ควรแน่ใจว่าได้วางแผนเรื่องความปลอดภัยไว้แต่เนิ่น ๆ
ทั้งในขั้นตอนการใช้และการเผยแพร่ในองค์กร
ทำความเข้าใจถึงสิ่งที่ลูกค้าของคุณต้องการปกป้อง
และสิ่งที่พวกเขาต้องการทำเพื่อปกป้องสิ่งนั้น

ประการสุดท้าย พัฒนาแผนรับมือกรณีฉุกเฉินก่อนจะเกิดเหตุร้าย
ด้วยการรวมแผนการเข้ากับเทคโนโลยีที่มีประสิทธิภาพ
เพื่อให้การป้องกันที่แน่นหนาแก่ลูกค้า

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับรายละเอียดทั่ว ๆ ไปของความปลอดภัย
โปรดดูที่หัวข้อ "กฎสิบประการว่าด้วยเรื่องการจัดการด้านความปลอดภัย"
ที่:
http://www.microsoft.com/technet/archive/community/columns/security/essays/10salaws.mspx

และบทความเรื่องการจัดการด้านความปลอดภัยที่:
http://www.microsoft.com/technet/community/columns/secmgmt/smarch.mspx

การสร้างความปลอดภัยให้กับระบบปฏิบัติการของเซิร์ฟเวอร์

แม้คุณอาจพบว่าลูกค้าขนาดเล็กจำนวนมากไม่มีระบบปฏิบัติการของเซิร์ฟเวอร์ แต่สิ่งสำคัญประการหนึ่งคือ
คุณมีความเข้าใจและสามารถสื่อสารให้ลูกค้าขนาดใหญ่ที่มีสภาพแวดล้อมทางเครือข่ายที่สลับซับซ้อนกว่าทราบถึงหลักปฏิบัติที่ดีที่สุดในเรื่องความปลอดภัย คุณควรตระหนักด้วยว่า
นโยบายและหลักปฏิบัติหลายประการที่อธิบายไว้ในเอกสารชุดนี้
สามารถนำมาประยุกต์ให้เข้ากับลูกค้าเหล่านั้นที่มีเฉพาะระบบปฏิบัติของเครื่องไคลเอนต์ได้อย่างง่ายดาย

เนื้อหาที่อธิบายไว้ในส่วนนี้นำมาใช้ได้กับผลิตภัณฑ์ MICROSOFT WINDOWS 2000 SERVER และ MICROSOFT WINDOWS SERVER 2003
แม้ข้อมูลนี้จะคัดมาจากวิธีใช้แบบออนไลน์สำหรับ WINDOWS SERVER 2003 WINDOWS SERVER 2003
มาพร้อมกับคุณลักษณะด้านความปลอดภัยที่มีประสิทธิภาพชุดหนึ่ง
วิธีใช้แบบออนไลน์ของ WINDOWS SERVER 2003
มีเนื้อหาโดยละเอียดเกี่ยวกับคุณลักษณะด้านความปลอดภัยและขั้นตอนต่าง ๆ ทั้งหมด

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับ WINDOWS 2000 SERVER โปรดเยี่ยมชม WINDOWS 2000 SERVER SECURITY CENTER ได้ที่
http://www.microsoft.com/technet/security/prodtech/win2000/default.mspx

และอ่านคู่มือการเพิ่มความปลอดภัยของ WINDOWS 2000 ได้จาก:
http://www.microsoft.com/technet/security/prodtech/win2000/win2khg/default.mspx

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับ WINDOWS SERVER 2003 โปรดดูที่
แนวทางด้านความปลอดภัยสำหรับ WINDOWS SERVER 2003 จาก
http://www.microsoft.com/technet/security/prodtech/win2003/w2003hg/sgch00.mspx

คุณลักษณะแรกเริ่มของต้นแบบความปลอดภัยสำหรับเซิร์ฟเวอร์ของ WINDOWS คือ การตรวจสอบความถูกต้อง การควบคุมการเข้าใช้ และการลงชื่อเข้าใช้แบบครั้งเดียว:

- การตรวจสอบความถูกต้อง คือ
  ขั้นตอนที่ระบบจะตรวจสอบความมีตัวตนของผู้ใช้ผ่านทางหลักฐานการล็อกออน
  ทั้งยังจะมีการเปรียบเทียบชื่อและรหัสผ่านของผู้ใช้กับรายชื่อผู้มีสิทธิ์อันชอบธรรม
  หากระบบตรวจพบข้อมูลที่ตรงกัน
  การตรวจสอบความถูกต้องจะอนุญาตให้ผู้ใช้เข้าสู่เนื้อหาในขอบข่ายตามที่ระบุไว้ในรายการสิทธิ์สำหรับผู้ใช้รายนั้น
- การควบคุมการเข้าถึงข้อมูลเป็นตัวจำกัดการเข้าถึงแหล่งข้อมูลหรือคอมพิวเตอร์แหล่งอื่นๆ ของผู้ใช้ ด้วยการพิจารณาจากตัวตนของผู้ใช้และการเป็นสมาชิกภาพในกลุ่มต่าง ๆ ที่กำหนดไว้ล่วงหน้าของผู้ใช้ โดยปกติ
  ผู้ดูแลระบบจะเป็นผู้ใช้การควบคุมการเข้าถึงข้อมูลเพื่อควบคุมระดับการเข้าสู่ทรัพยากรเครือข่าย เช่น เซิร์ฟเวอร์ ไดเร็กทอรี และแฟ้ม ที่ผู้ใช้มี
  มาตรการควบคุมนี้นำมาใช้ได้ด้วยการให้สิทธิ์แก่ผู้ใช้หรือกลุ่มผู้ใช้เพื่อเข้าสู่รายการเฉพาะ
- คุณลักษณะ การลงชื่อเข้าใช้แบบครั้งเดียว อนุญาตให้ผู้ใช้ล็อกเข้าสู่โดเมนของ Windows เพียงหนึ่งครั้ง โดยใช้รหัสผ่านหนึ่งตัว
  และมีสิทธิ์เข้าสู่คอมพิวเตอร์เครื่องใดก็ได้ที่อยู่ในโดเมนของ Windows คุณลักษณะการลงชื่อเข้าใช้แบบครั้งเดียว
  ช่วยให้ผู้ดูแลระบบใช้ขั้นตอนการตรวจสอบความถูกต้องด้วยรหัสผ่านได้ทั่วเครือข่าย Windows พร้อม ๆ กับเอื้อให้ผู้ใช้ขั้นสุดท้ายเข้าใช้ระบบได้โดยสะดวก

ดูคำอธิบายโดยละเอียดเกี่ยวกับคุณลักษณะหลักทั้งสามประการนี้ได้จากส่วนต่าง ๆ ต่อไปนี้

การตรวจสอบความถูกต้อง

การตรวจสอบความถูกต้อง คือ
ลักษณะเบื้องต้นของความปลอดภัยของระบบ
และนำมาใช้เพื่อยืนยันถึงตัวตนของผู้ใช้ที่พยายามล็อกเข้าสู่โดเมนหรือเข้าถึงทรัพยากรของเครือข่าย
จุดอ่อนในระบบการตรวจสอบความถูกต้องเกือบทุกระบบ คือ
รหัสผ่านของผู้ใช้

รหัสผ่านคือมาตรการแรกสุดที่ใช้ป้องกันการเข้าสู่โดเมนและคอมพิวเตอร์ภายในโดยไม่ได้รับอนุญาต
แนะนำให้ใช้หลักปฏิบัติเกี่ยวกับรหัสผ่านที่ดีที่สุด ดังต่อไปนี้:

- ใช้รหัสผ่านที่มีความรัดกุมเสมอ
- หากต้องจดรหัสผ่านลงบนแผ่นกระดาษ ควรเก็บกระดาษแผ่นนั้นไว้ในที่ ๆ ปลอดภัย และทำลายทันทีเมื่อไม่จำเป็นต้องใช้อีก
- ห้ามใช้รหัสผ่านร่วมกันคนอื่น
- ใช้รหัสผ่านที่ไม่เหมือนกันสำหรับบัญชีผู้ใช้ทุกบัญชี
- เปลี่ยนรหัสผ่านเป็นระยะ ๆ
- ระมัดระวังเกี่ยวกับตำแหน่งบนคอมพิวเตอร์ที่ใช้จัดเก็บรหัสผ่าน

รหัสผ่านที่มีความรัดกุม

บทบาทของรหัสผ่านในฐานะที่ช่วยสร้างความปลอดภัยให้กับเครือข่ายขององค์กร มักถูกประเมินต่ำเกินไปและถูกมองข้าม เช่นที่กล่าวไว้ข้างต้นว่า รหัสผ่านคือมาตรการแรกสุดที่ใช้ป้องกันการเข้าสู่เครือข่ายของคุณโดยไม่ได้รับอนุญาต ดังนั้น คุณควรดูให้แน่ใจว่า
ลูกค้าของคุณได้แนะนำให้พนักงานของลูกค้าใช้รหัสผ่านที่มีความรัดกุม

อย่างไรก็ดี พัฒนาการของเครื่องมือที่ใช้เจาะรหัสผ่านมีอยู่อย่างต่อเนื่องและคอมพิวเตอร์ที่ใช้ไขปริศนาของรหัสผ่านก็ทรงพลังมากกว่าที่เคยปรากฏ ซึ่งถ้ามีเวลาพอ
เครื่องมือเจาะรหัสผ่านแบบอัตโนมัติก็จะสามารถเจาะรหัสผ่านได้
อย่างไรก็ดี
รหัสผ่านที่มีความรัดกุมย่อมทำให้เจาะได้ยากกว่ารหัสผ่านที่คาดเดาได้ง่าย

สำหรับคำแนะนำในการสร้างรหัสผ่านที่มีความรัดกุมที่ผู้ใช้สามารถจดจำ โปรดดูที่

http://www.microsoft.com/athome/security/privacy/password.mspx

และ

http://www.microsoft.com/ntworkstation/technicalresources/PWDguidelines.asp

การกำหนดนโยบายเกี่ยวกับรหัสผ่าน

เมื่อช่วยลูกค้าร่างนโยบายเกี่ยวกับรหัสผ่าน
จงดูให้แน่ใจว่าได้ร่างนโยบายที่กำหนดให้บัญชีผู้ใช้ทุกบัญชีต้องมีรหัสผ่านที่มีความรัดกุม สำหรับเกือบทุกระบบ
การปฏิบัติตามคำแนะนำที่ปรากฏในแนวทางด้านความปลอดภัยสำหรับ WINDOWS SERVER 2003 ถือว่าเพียงพอ:

- กำหนดนโยบาย **เรียกใช้ประวัติรหัสผ่าน** เพื่อให้มีการจดจำรหัสผ่านที่เคยนำมาใช้
  ด้วยการกำหนดนโยบายเช่นนี้ ผู้ใช้จะไม่สามารถใช้รหัสผ่านตัวเดิมเมื่อรหัสผ่านของผู้ใช้หมดอายุ

  จำนวนรหัสผ่านที่แนะนำ: 24
- กำหนดนโยบาย **อายุสูงสุดของรหัสผ่าน**
  เพื่อให้รหัสผ่านหมดอายุได้บ่อยเท่าที่จำเป็นสำหรับสภาพแวดล้อมของลูกค้า

  ระยะเวลาที่แนะนำ: ระหว่าง 42 (ค่าเริ่มต้น) และ 90
- กำหนดนโยบาย **อายุขั้นต่ำของรหัสผ่าน**
  ซึ่งจะทำให้ไม่สามารถเปลี่ยนรหัสผ่านได้จนกว่าจะใช้รหัสผ่านนั้นนานกว่าจำนวนวันที่ระบุ
  ใช้การกำหนดนโยบายนี้ร่วมกับนโยบาย **เรียกใช้ประวัติรหัสผ่าน**
  หากระบุอายุขั้นต่ำของรหัสผ่าน ผู้ใช้จะไม่สามารถเปลี่ยนรหัสผ่านบ่อย ๆ เพื่อเปิดดูข้อมูลใน **เรียกใช้ประวัติรหัสผ่าน** และใช้รหัสผ่านตัวแรกของผู้ใช้
  ผู้ใช้ต้องรอให้ครบตามจำนวนวันที่ระบุเพื่อเปลี่ยนรหัสผาน

  ระยะเวลาที่แนะนำ: 2

- กำหนดนโยบาย **ความยาวขั้นต่ำของรหัสผ่าน**
  เพื่อทำให้รหัสผ่านประกอบด้วยอักขระในจำนวนที่ระบุเป็นอย่างน้อย รหัสผ่านที่ยาว คือ ประกอบด้วยอักขระตั้งแต่ 7 ตัวขึ้นไป มักมีความรัดกุมมากกว่ารหัสผ่านที่สั้น ด้วยการกำหนดนโยบายเช่นนี้ ผู้ใช้จะไม่สามารถใช้รหัสผ่านเปล่า และต้องสร้างรหัสผ่านที่ประกอบด้วยอักขระในจำนวนที่แน่นอนจำนวนหนึ่งเป็นอย่างน้อย

  จำนวนอักขระที่แนะนำ: 8

- นำนโยบาย **รหัสผ่านต้องตรงกับข้อกำหนดเรื่องความสลับซับซ้อน** มาใช้
  การกำหนดนโยบายในลักษณะนี้จะตรวจสอบรหัสผ่านใหม่ทั้งหมด เพื่อให้แน่ใจว่า รหัสผ่านเหล่านี้ตรงตามข้อกำหนดพื้นฐานเรื่องรหัสผ่านที่มีความรัดกุม
  การกำหนดนโยบายในลักษณะนี้ช่วยรับประกันว่า รหัสผ่านต่าง ๆ จะรวมสัญลักษณ์ใน 3 ลักษณะจากทั้งสิ้น 4 ลักษณะเป็นอย่างน้อย (ตัวพิมพ์ใหญ่ ตัวพิมพ์เล็ก ตัวเลข สัญลักษณ์ที่ไม่ใช่ตัวอักษรและตัวเลข) และไม่มีส่วนใด ๆ ของชื่อผู้ใช้ และชื่อหรือนามสกุลของผู้ใช้

  หมายเหตุ
  รหัสผ่านที่ตรงตามเงื่อนไขเหล่านี้ไม่จำเป็นต้องเป็นรหัสผ่านที่มีความรัดกุมมาก ตัวอย่างเช่น รหัสผ่านที่ใช้คำว่า "Password1" ตรงตามข้อกำหนดเหล่านี้

  รหัสผ่านที่แนะนำให้ใช้: แนะนำ

- สำหรับรายการข้อกำหนดทั้งหมด โปรดดูที่ "รหัสผ่านต้องตรงตามข้อกำหนดเรื่องความสลับซับซ้อน" ในวิธีใช้แบบออนไลน์ของ Windows Server

- จัดเก็บรหัสผ่านโดยใช้เทคนิคการเข้ารหัสที่เปลี่ยนแปลงได้ –
  การเข้ารหัสที่เปลี่ยนแปลงได้ถูกนำมาใช้ในระบบที่แอปพลิเคชันจำเป็นต้องเข้าถึงรหัสผ่าน แต่การเข้ารหัสผ่านชนิดนี้ไม่จำเป็นสำหรับการใช้การเกือบทั้งหมด

  การตั้งค่าที่แนะนำ: ไม่แนะนำ

สำหรับข้อมูลเพิ่มเติม โปรดดูที่แนวทางด้านความปลอดภัยสำหรับ WINDOWS SERVER 2003:

http://www.microsoft.com/technet/security/prodtech/Win2003/W2003HG/SGCH00.mspx

การกำหนดนโยบายล็อกบัญชี

ควรใช้ความระมัดระวังเมื่อร่างนโยบายล็อกบัญชี
ไม่ควรใช้นโยบายล็อกบัญชีในธุรกิจขนาดเล็ก
เนื่องจากมีแนวโน้มค่อนข้างสูงว่า
จะปิดกั้นผู้ใช้ที่ได้รับอนุญาตอันชอบธรรมด้วย
อีกทั้งลูกค้าจะสิ้นเปลืองค่าใช้จ่ายไปกับนโยบายนี้ค่อนข้างสูง

หากลูกค้าตัดสินใจที่จะนำนโยบายล็อกบัญชีมาใช้ ควรกำหนด **กรอบการล็อกบัญชี** ไว้ในจำนวนที่สูงพอที่จะไม่ปิดกั้นผู้ใช้ที่ได้รับอนุญาตอันชอบธรรมเข้ามาใช้บัญชีผู้ใช้ของตนเอง
เพียงเพราะพวกเขาพิมพ์รหัสผ่านของตัวเองผิดหลายครั้ง

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับนโยบายล็อกบัญชี โปรดดูที่ "ภาพรวมนโยบายล็อกบัญชี" ในวิธีใช้แบบออนไลน์ของ WINDOWS SERVER

สำหรับข้อมูลเกี่ยวกับวิธีนำนโยบายล็อกบัญชีมาใช้หรือดัดแปลงนโยบายดังกล่าว โปรดดูที่
"หากต้องการนำนโยบายล็อกบัญชีมาใช้หรือดัดแปลงนโยบายดังกล่าว"
ในวิธีใช้แบบออนไลน์ของ WINDOWS SERVER

การควบคุมการเข้าสู่ระบบ

การรักษาความปลอดภัยให้กับเครือข่ายและทรัพยากรของ WINDOWS (รวมถึง NAVISION) ทำได้ด้วยการพิจารณาสิทธิ์ใดที่ผู้ใช้ กลุ่มผู้ใช้และคอมพิวเตอร์เครื่องอื่น ๆ มีบนเครือข่าย คุณสามารถสร้างความปลอดภัยให้กับคอมพิวเตอร์หนึ่งเครื่องหรือหลาย ๆ เครื่องได้ด้วยการให้ผู้ใช้หรือกลุ่มผู้ใช้มีสิทธิ์เฉพาะ คุณสามารถสร้างความปลอดภัยให้กับวัตถุ เช่น แฟ้มหรือโฟลเดอร์ ได้ด้วยการกำหนดสิทธิ์ที่อนญาตให้ผู้ใช้หรือกลุ่มผู้ใช้ดำเนินการเฉพาะกับวัตถุนั้น แนวคิดหลัก ๆ ที่ประกอบเป็นการควบคุมการเข้าสู่ระบบ รวมถึง:

- สิทธิ์
- การเป็นเจ้าของวัตถุ
- การรับช่วงในสิทธิ์
- สิทธิ์ของผู้ใช้
- การตรวจสอบวัตถุ

สิทธิ์

สิทธิ์เป็นตัวกำหนดชนิดของการเข้าสู่วัตถุหรือคุณสมบัติของวัตถุ เช่น แฟ้ม โฟลเดอร์ วัตถุรีจิสทรีที่มอบให้กับผู้ใช้หรือกลุ่มผู้ใช้ สิทธิ์ถูกนำมาใช้กับวัตถุใด ๆ ที่ต้องการความปลอดภัย เช่น แฟ้ม หรือวัตถุรีจิสทรี และสิทธิ์สามารถนำมามอบให้กับผู้ใช้ กลุ่มผู้ใช้หรือคอมพิวเตอร์ใดก็ได้ และถือเป็นหลักปฏิบัติที่ดีหากมอบหมายสิทธิ์ให้กับกลุ่มผู้ใช้

การเป็นเจ้าของวัตถุ

เจ้าของจะถูกมอบหมายให้กับวัตถุเมื่อวัตถุถูกสร้างขึ้น ตามค่าเริ่มต้นในโปรแกรม WINDOWS 2000 SERVER นั้น เจ้าของก็คือผู้สร้างวัตถุ และรูปการณ์นี้ได้เปลี่ยนแปลงไปใน WINDOWS SERVER 2003 สำหรับวัตถุที่สรางโดยสมาชิกของกลุ่มผู้ดูแลระบบ

เมื่อสมาชิกของกลุ่มผู้ดูแลระบบได้สร้างวัตถุใน WINDOWS SERVER 2003 กลุ่มผู้ดูแลระบบจะกลายเป็นเจ้าของ ไม่ใช่บัญชีรายบุคคลที่สร้างวัตถุ พฤติกรรมในลักษณะนี้สามารถเปลี่ยนแปลงได้ผ่านทางสแน็ป-อินของ LOCAL SECURITY SETTINGS MICROSOFT MANAGEMENT CONSOLE (MMC) โดยใช้การตั้งค่า **วัตถุของระบบ:**
เจ้าของเริ่มต้นสำหรับวัตถุที่สร้างโดยสมาชิกของกลุ่มผู้ดูแลระบบ

ไม่ว่าจะกำหนดสิทธิ์ไว้ที่ระดับใดสำหรับวัตถุ
เจ้าของวัตถุสามารถเปลี่ยนแปลงสิทธิ์บนวัตถุนั้นได้เสมอ

สำหรับข้อมูลเพิ่มเติม โปรดดูที่ "ความเป็นเจ้าของ"
ในวิธีใช้แบบออนไลน์ของ WINDOWS SERVER

การรับช่วงในสิทธิ์

การรับช่วงจะเปิดโอกาสให้ผู้ดูแลระบบมอบหมายและจัดการกับสิทธิ์ได้โดยง่าย คุณลักษณะนี้ทำให้วัตถุที่อยู่ ณ ที่ ๆ
หนึ่งรับช่วงสิทธิ์ทั้งหมดที่รับช่วงได้ของที่ ๆ นั้นโดยอัตโนมัติ ตัวอย่างเช่น
เมื่อคุณสร้างแฟ้มภายในโฟลเดอร์
แฟ้มเหล่านั้นก็จะรับช่วงสิทธิ์ของโฟลเดอร์
โดยสิทธิ์ที่ทำเครื่องหมายรับช่วงได้เท่านั้นที่จะถูกรับช่วง

สิทธิ์ของผู้ใช้

สิทธิ์ของผู้ใช้จะมอบสิทธิ์พิเศษเฉพาะและสิทธิ์ในการล็อกออนให้กับผู้ใช้และกลุ่มผู้ใช้ในสภาพแวดล้อมการใช้คอมพิวเตอร์ของคุณ

สำหรับข้อมูลเกี่ยวกับสิทธิ์ของผู้ใช้ โปรดดูที่ "สิทธิ์ของผู้ใช้"
ในวิธีใช้แบบออนไลน์ของ WINDOWS SERVER

การตรวจสอบวัตถุ

คุณสามารถตรวจสอบการเข้าถึงวัตถุของผู้ใช้ หลังจากนั้นจึงใช้ EVENT VIEWER
ดูเหตุการณ์ที่เกี่ยวข้องกับความปลอดภัยในบันทึกเหตุการณ์ความปลอดภัย

สำหรับข้อมูลเพิ่มเติม โปรดดูที่ "การตรวจสอบ" ในวิธีใช้แบบออนไลน์ของ WINDOWS SERVER

หลักปฏิบัติที่ดีที่สุดสำหรับการควบคุมการเข้าสู่ภายใน

- มอบหมายสิทธิ์ให้กับกลุ่มผู้ใช้แทนที่จะเป็นผู้ใช้
  เนื่องจากการรักษาบัญชีผู้ใช้โดยตรงนั้นไม่มีประสิทธิภาพ
  การมอบหมายสิทธิ์โดยยึดถือผู้ใช้ควรได้รับการยกเว้น
- ใช้ การปฏิเสธสิทธิ์ ในกรณีพิเศษ ตัวอย่างเช่น คุณสามารถใช้ การปฏิเสธสิทธิ์
  เพื่อละเว้นกลุ่มผู้ใช้กลุ่มย่อยที่ได้ การอนุญาตสิทธิ์
- ห้ามปฏิเสธการเข้าสู่วัตถุของกลุ่มประเภท ทุกคน หากคุณปฏิเสธสิทธิ์ของทุกคนในวัตถุ
  การปฏิเสธดังกล่าวจะรวมของผู้ดูแลระบบด้วย แนวทางแก้ปัญหาที่ดีกว่าคือ การย้ายกลุ่มประเภท
  ทุกคน ออกไปก่อนหากคุณยังให้สิทธิ์ในวัตถุนั้นแก่ผู้ใช้ กลุ่มผู้ใช้หรือคอมพิวเตอร์ โปรดจำไว้ว่า
  หากกำหนดเป็นไม่มีสิทธิ์ ย่อมไม่มีการอนุญาตให้เข้าสู่ภายใน

- มอบหมายสิทธิ์ที่สูงเท่าที่จะเป็นไปได้ให้กับวัตถุ ก่อนนำ การรับช่วงมาใช้ เพื่อรวมการตั้งค่าความปลอดภัยเข้าไว้ด้วย คุณสามารถนำการตั้งค่าการควบคุมการเข้าสู่ภายในมาใช้กับวัตถุลูกหรือโครงสร้างย่อยของวัตถุแม่ได้อย่างรวดเร็วและมีประสิทธิภาพ เมื่อดำเนินการเช่นนั้น แสดงว่า คุณได้สร้างสายโซ่ผลกระทบที่ยิ่งใหญ่ที่สุดโดยใช้ความเพียรพยายามน้อยที่สุด การตั้งค่าสิทธิ์ที่คุณกำหนดขึ้นควรเพียงพอสำหรับผู้ใช้ กลุ่มผู้ใช้และคอมพิวเตอร์ส่วนใหญ่
- บางครั้ง สิทธิ์ที่มีความชัดเจนจะถูกนำมาใช้แทนสิทธิ์ที่รับช่วงมา การปฏิเสธสิทธิ์ที่รับช่วงจะไม่ป้องกันการเข้าสู่วัตถุหากวัตถุนั้นมีการอนุญาตสิทธิ์ที่ชัดเจนอยู่ สิทธิ์ที่มีความชัดเจนมีความสำคัญมากกว่าสิทธิ์ที่รับช่วง แม้จะมีการปฏิเสธสิทธิ์ที่รับช่วง
- สำหรับสิทธิ์ของวัตถุ Active Directory® ดูให้แน่ใจว่า คุณเข้าใจหลักปฏิบัติที่ดีสุดสำหรับวัตถุ Active Directory

สำหรับข้อมูลเพิ่มเติม โปรดดูที่
"หลักปฏิบัติที่ดีที่สุดสำหรับการกำหนดสิทธิ์ให้กับวัตถุ ACTIVE DIRECTORY" ในวิธีใช้แบบออนไลน์ของ WINDOWS SERVER 2003

ไฟล์วอลล์ความปลอดภัยภายนอก

ไฟล์วอลล์คือ
ชิ้นงานฮาร์ดแวร์หรือซอฟต์แวร์ที่ป้องกันแพ็คเก็ตข้อมูลไม่ให้ถูกป้อนหรือปล่อยไว้ในเครือข่ายที่ระบุ
หากต้องการควบคุมให้ข้อมูลเคลื่อนที่อย่างต่อเนื่อง
พอร์ตในไพร์วอลล์ต้องเปิดรับหรือปิดรับแพ็คเก็ตข้อมูล
ไฟร์วอลล์จะดูที่ข้อมูลหลาย ๆ ส่วนในแพ็คเก็ตข้อมูลแต่ละแพ็คเก็ต:
โปรโตตอลที่เป็นเส้นทางผ่านของแพ็คเก็ต ปลายทางหรือผู้ส่งแพ็คเก็ต
ชนิดของเนื้อหาที่บรรจุอยู่ในแพ็คเก็ต
และหมายเลขพอร์ตที่ข้อมูลจะส่งไปให้
หากมีการกำหนดค่าให้ไฟร์วอลล์ยอมรับโปรโตคอลที่ระบุผ่านทางพอร์ตเป้าหมาย แพ็คเก็ตข้อมูลก็ย่อมจะได้รับอนุญาตให้ผ่านด้วย MICROSOFT WINDOWS SMALL BUSINESS SERVER 2003 PREMIUM EDITION **ถูกจัดส่งพร้อมกับ** MICROSOFT INTERNET SECURITY AND ACCELERATION (ISA) SERVER 2000 **ในฐานะวิธีแก้ปัญหาของไฟร์วอลล์** SMALL BUSINESS SERVER STANDARD EDITION **ยังมีไฟร์วอลล์รวมอยู่ด้วย**

ISA SERVER 2004

INTERNET SECURITY AND ACCELERATION (ISA) SERVER 2000
ทำให้เส้นทางคำขอและการตอบรับระหว่างอินเทอร์เน็ตและเครื่องคอมพิวเตอร์ไคลเอ็นต์บนเครือข่ายภายในมีความปลอดภัย

ISA SERVER
ทำหน้าที่เหมือนเกตเวย์ที่มีความปลอดภัยสู่อินเทอร์เน็ตสำหรับเครื่องไคลเอ็นต์ที่อยู่บนเครือข่ายท้องถิ่น คอมพิวเตอรบน ISA SERVER
มีความโปร่งใสในสายตาของคู่ดำเนินการอื่น ๆ ในเส้นทางการสื่อสาร ผู้ใช้อินเทอร์เน็ตไม่ควรบอกได้ว่า มีเซิร์ฟเวอร์ของไฟร์วอลล์อยู่

เว้นแต่ผู้ใช้พยายามเข้าสู่บริการ หรือไปที่ไซต์ที่คอมพิวเตอร์ ISA SERVER ปฏิเสธการเข้ามา เซิร์ฟเวอร์อินเทอร์เน็ตที่ถูกเจาะเข้ามา จะตีความคำขอจากคอมพิวเตอร์ ISA SERVER ว่าคำขอนั้นมาจากไคลเอ็นต์แอปพลิเคชัน

เมื่อคุณเลือกตัวกรองการแบ่งส่วนของ INTERNET PROTOCOL (IP) แสดงว่าคุณได้เรียกใช้การทำงานของบริการเว็บพร็อกซีและไฟร์วอลล์เพื่อทำหน้าที่กรองการแบ่งส่วนแพ็คเก็ต เมื่อใช้ตัวกรองการแบ่งส่วนแพ็คเก็ต แพ็คเก็ต IP ทั้งหมดที่ถูกแบ่งส่วนจะถูกปล่อย "การจู่โจม" ที่รู้จักกันดี รวมถึง การส่งแพ็คเก็ตที่ถูกแบ่งส่วนก่อนประกอบกลับแพ็คเก็ตเหล่านั้นในแบบที่อาจเป็นอันตรายต่อระบบ

ISA SERVER มีกลไกการตรวจหาการรุกล้ำสู่ระบบ กลไกนี้เป็นตัวกำหนดเวลาที่มีความพยายามเข้าเจาะเครือข่ายพร้อมดำเนินการกำหนดค่าชุดหนึ่ง (หรือเตือนให้ทราบ) ในกรณีที่มีการจู่โจม

หากติดตั้ง INTERNET INFORMATION SERVICES (IIS) บนคอมพิวเตอร์ ISA SERVER คุณต้องกำหนดค่าโปรแกรมนี้เพื่อไม่ให้ใช้พอร์ตที่ ISA SERVER ใช้รองรับคำขอเว็บออก (ตามค่าเริ่มต้นคือ พอร์ต 8080) และคำขอเว็บเข้า (ตามค่าเริ่มต้นคือ พอร์ต 80) ตัวอย่างเช่น คุณสามารถเปลี่ยน IIS เพื่อควบคุมพอร์ต 81 ก่อนกำหนดค่าคอมพิวเตอร์ ISA SERVER เพื่อระบุให้คำขอเว็บเข้าไปที่พอร์ต 81 บนคอมพิวเตอร์ภายในที่เรียกใช้ IIS

หากมีความขัดแย้งระหว่างพอร์ตต่าง ๆ ที่ ISA SERVER และ IIS ใช้ โปรแกรมการติดตั้งจะหยุดให้บริการประกาศ IIS หลังจากนั้น คุณสามารถเปลี่ยน IIS เพื่อควบคุมพอร์ตอื่น และเริ่มบริการประกาศ IIS อีกครั้ง

นโยบายของ ISA SERVER

คุณสามารถกำหนดนโยบาย ISA SERVER ที่ชี้ถึงการเข้าสู่ระบบทั้งในแบบขาเข้าและขาออก กฎเกี่ยวกับไซต์และเนื้อหาเป็นตัวระบุว่า ไซต์และเนื้อหาใดที่สามารถเข้ามาใช้ได้ กฎเกี่ยวกับโปรโตคอลเป็นตัวระบุว่า โปรโตคอลเฉพาะเปิดรับการสื่อสารเข้าและออกหรือไม่

คุณสามารถสร้างกฎเกี่ยวกับไซต์และเนื้อหา กฎสำหรับโปรโตคอล กฎการประกาศเว็บ และตัวกรองแพ็คเก็ต IP กฎเหล่านั้นเป็นตัวกำหนดวิธีที่เครื่องคอมพิวเตอร์ไคลเอ็นต์ของ ISA SERVER จะใช้สื่อสารกับอินเทอร์เน็ตและการสื่อสารใดที่ได้รับอนุญาต

การป้องกันไวรัส

ไวรัสคอมพิวเตอร์คือ แฟ้มปฏิบัติการที่ถูกออกแบบขึ้นมาให้จำลองตัวเอง ลบหรือทำให้แฟ้มและโปรแกรมเสียหาย และหลบเลี่ยงการตรวจจับ ตามข้อเท็จจริงนั้น ไวรัสมักถูกเขียนซ้ำไปซ้ำมา และถูกปรับแต่งเพื่อไม่ให้สามารถตรวจจับได้ นอกจากนี้ ไวรัสยังถูกส่งเป็นสิ่งที่แนบกับอีเมล จึงจำเป็นต้องปรับปรุงโปรแกรมป้องกันไวรัสอยู่เสมอเพื่อค้นหาไวรัสใหม่ ๆ และที่มีการปรับเปลี่ยน ไวรัสถือเป็นวิธีการอันดับหนึ่งที่ทำลายคอมพิวเตอร์

ซอฟต์แวร์ป้องกันไวรัสถูกออกแบบมาเป็นพิเศษเพื่อทำหน้าที่ตรวจจับและป้องกันโปรแกรมไวรัส และเนื่องจากโปรแกรมไวรัสใหม่ ๆ ได้รับการสร้างขึ้นอยู่ตลอดเวลา ผู้ผลิตผลิตภัณฑ์ป้องกันไวรัสหลายรายจึงได้เสนอโปรแกรมปรับปรุงซอฟต์แวร์ของตนเองให้กับลูกค้าเป็นระยะ ๆ ไมโครซอฟท์ขอแนะนำให้นำซอฟต์แวร์ป้องกันไวรัสมาใช้ในสภาพแวดล้อมของลูกค้าของคุณ

โดยทั่วไป มักติดตั้งซอฟต์แวร์ไวรัสไว้ในแต่ละจุดจากสามจุดเหล่านี้: เวิร์คสเตชันของผู้ใช้ เซิร์ฟเวอร์ และเครือข่ายที่ ๆ รับอีเมลเข้าสู่องค์กร (และออกไปจากองค์กร)

ไวรัสประเภทต่าง ๆ

ไวรัสที่แพร่ระบาดในระบบคอมพิวเตอร์แบ่งออกเป็น 3 ประเภทใหญ่ ๆ คือ: ไวรัสในส่วนของการบูตระบบ ไวรัสที่แพร่ระบาดในแฟ้ม และโปรแกรม TROJAN

ไวรัสในส่วนของการบูตระบบ

เมื่อเปิดเครื่องคอมพิวเตอร์ คอมพิวเตอร์จะสแกนส่วนของการบูตระบบในฮาร์ดดิสก์ก่อนโหลดระบบปฏิบัติการหรือแฟ้มเริ่มต้นแฟ้มอื่น ๆ ไวรัสในส่วนของการบูตระบบถูกออกแบบขึ้นมาเพื่อนำรหัสของไวรัสมาแทนที่ข้อมูลที่อยู่ในส่วนการบูตระบบของฮาร์ดดิสก์ เมื่อคอมพิวเตอร์ติดไวรัสในส่วนของการบูตระบบ รหัสไวรัสจะถูกอ่านเข้าสู่หน่วยความจำก่อนสิ่งอื่น หลังจากไวรัสเข้าไปอยู่ในหน่วยความจำแล้ว ไวรัสจะจำลองตัวเองเข้าไปในดิสก์อื่น ๆ ที่ถูกเรียกใช้ในคอมพิวเตอร์ที่ติดไวรัส

ไวรัสที่แพร่ระบาดในแฟ้ม

ไวรัสที่แพร่ระบาดในแฟ้ม ถือเป็นไวรัสที่พบเห็นบ่อยที่สุด
ไวรัสนี้จะแนบตัวเองเข้ากับแฟ้มปฏิบัติการของโปรแกรมด้วยการเพิ่มรหัสของไวรัสลงในแฟ้มปฏิบัติการ
รหัสไวรัสมักถูกเพิ่มเข้ามาในลักษณะนี้ทำให้เล็ดรอดจากการถูกตรวจพบ
เมื่อเรียกใช้แฟ้มที่ติดไวรัส
ไวรัสก็จะสามารถแนบตัวเองลงในแฟ้มปฏิบัติการอื่น
แฟ้มที่ติดไวรัสประเภทนี้มักมีส่วนขยายของชื่อแฟ้มเป็น .COM, .EXE, หรือ .SYS

ไวรัสบางตัวที่แพร่ระบาดผ่านแฟ้มถูกออกแบบมาสำหรับโปรแกรมเฉพาะชนิดของโปรแกรมที่มักเป็นเป้าหมายคือ แฟ้มโอเวอร์เลย์ (.OVL) และแฟ้มไดนามิก-ลิงค์ ไลบรารี (.DLL) แม้จะไม่ได้เรียกใช้แฟ้มเหล่านี้ แต่แฟ้มปฏิบัติการก็จะร้องขอแฟ้มดังกล่าวอยู่ดี
และไวรัสก็จะแพร่ระบาดในระหว่างขั้นตอนดังกล่าว

ข้อมูลจะเกิดความเสียหายเมื่อไวรัสถูกกระตุ้นให้ทำงาน
ไวรัสถูกกระตุ้นได้เมื่อแฟ้มที่ติดไวรัสทำงานหรือเมื่อสภาพแวดล้อมเฉพาะตรงตามที่กำหนดไว้ (เช่นวันที่ที่ระบุของระบบ)

โปรแกรม TROJAN HORSE

จริง ๆ แล้ว โปรแกรม TROJAN HORSE ไม่ใช่ไวรัส
ข้อแตกต่างที่เห็นได้อย่างชัดเจนระหว่างไวรัสและโปรแกรม TROJAN HORSE คือ โปรแกรม TROJAN HORSE ไม่จำลองตัวเอง
โปรแกรมจะทำลายข้อมูลที่อยู่บนฮาร์ดดิสก์เพียงอย่างเดียว โปรแกรม TROJAN HORSE พรางตัวเองให้อยู่ในรูปของโปรแกรมที่ถูกต้อง เช่น เกมส์หรืออรรถประโยชน์ ซึ่งเมื่อเรียกใช้โปรแกรมนั้น
โปรแกรมจะทำลายข้อมูลหรือทำให้ข้อมูลยุ่งเหยิง

หลักปฏิบัติที่ดีที่สุดของการป้องกันไวรัส

การแพร่ระบาดของแมโครไวรัสเป็นเรื่องที่ป้องกันได้
เคล็ดลับบางข้อต่อไปนี้เกี่ยวกับการหลีกเลี่ยงการติดไวรัสที่คุณควรถ่ายทอดให้กับลูกค้า:

- ติดตั้งโซลูชันการป้องกันไวรัสที่จะสแกนไวรัสในข้อความเข้าจากอินเทอร์เน็ตก่อนผ่านข้อความนั้นไปที่เราเตอร์ ซึ่งจะรับประกันว่า มีการสแกนไวรัสที่เป็นที่รู้จักในอีเมลต่าง ๆ
- ทราบแหล่งที่มาของเอกสารที่ได้รับ
  ไม่ควรเปิดเอกสารหากเอกสารนั้นไม่ได้มาจากบุคคลที่ลูกค้ารู้สึกว่าน่าเชื่อถือ
- พูดคุยกับบุคคลที่สร้างเอกสาร หากผู้ใช้ไม่แน่ใจเลยว่าเอกสารนั้นปลอดภัยหรือไม่
  ผู้ใช้ควรติดต่อบุคคลที่สร้างเอกสารนั้น

- ใช้คุณลักษณะ การป้องกันแมโครไวรัสของ Microsoft Office ใน Office แอปพลิเคชันจะเตือนให้ผู้ใช้ทราบหากเอกสารนั้นมีแมโคร คุณลักษณะนี้อนุญาตให้ผู้ใช้เลือกเปิดหรือปิดการทำงานของแมโครในขณะที่เปิดเอกสาร
- ใช้ซอฟต์แวร์สแกนไวรัสเพื่อตรวจจับและขจัดแมโครไวรัส ทั้งนี้ ซอฟต์แวร์สแกนไวรัสสามารถตรวจหาแมโครไวรัส ก่อนลบออกจากเอกสาร ไมโครซอฟท์ขอแนะนำให้ใช้ซอฟต์แวร์ป้องกันไวรัสที่ได้รับการรับรองโดย International Computer Security Association (ICSA)

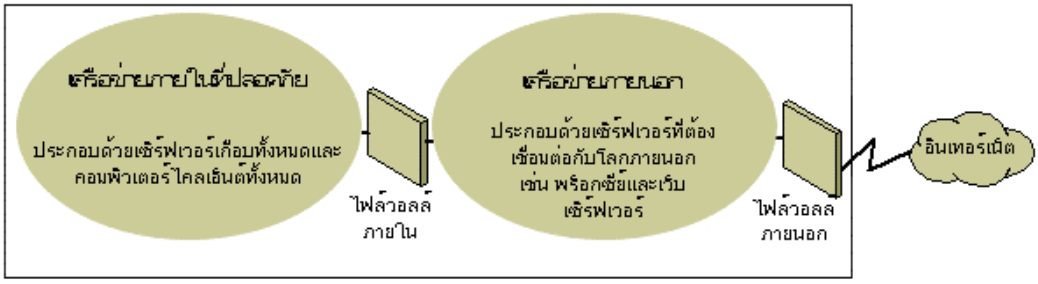
สำหรับข้อมูลเพิ่มเติมเกี่ยวกับไวรัสและความปลอดภัยโดยทั่ว ๆ ไปของคอมพิวเตอร์ โปรดดูที่เว็บไซต์ ความปลอดภัยของไมโครซอฟท์ ต่อไปนี้:

- ความปลอดภัยของไมโครซอฟท์ที่ http://www.microsoft.com/security/default.asp
- เอกสารเรื่องความปลอดภัยสำหรับ Microsoft TechNet http://www.microsoft.com/technet/security/Default.mspx

กลยุทธ์ด้านความปลอดภัยของเครือข่าย

เนื่องจากการออกแบบและการใช้สภาพแวดล้อมของเครือข่ายระหว่าง IP ต้องอาศัยสมดุลความสนใจในเรื่องเครือข่ายของภาคเอกชนและภาครัฐ ไฟร์วอลล์จึงกลายเป็นส่วนประกอบหลักในการสร้างบูรณาการให้กับเครือข่ายที่มีความปลอดภัย ไฟร์วอลล์ไม่ใช่องค์ประกอบเดี่ยว ๆ NATIONAL COMPUTER SECURITY ASSOCIATION (NCSA) ได้นิยามคำว่า ไฟร์วอลล์ ว่าคือ "ระบบหรือการรวมกันของระบบต่าง ๆ ที่ใช้พรมแดนระหว่างเครือข่ายสองหรือหลายเครือข่าย" แม้มีการเลือกใช้คำที่แตกต่างกัน แต่พรมแดนที่ว่านี้มักรู้จักกันในชื่อเครือข่ายภายนอก (PERIMETER NETWORK) เครือข่ายภายนอกทำหน้าที่ปกป้องอินทราเน็ตหรือเครือข่ายในพื้นที่ (LAN) ของบริษัทจากการลักลอบเข้ามาใช้ด้วยการควบคุมการเข้าสู่ภายในจากอินเทอร์เน็ตหรือเครือข่ายขนาดใหญ่อื่น ๆ

ไดอะแกรมต่อไปนี้แสดงภาพเครือข่ายภายนอกที่โอบล้อมด้วยไฟร์วอลล์ และวางอยู่ระหว่างเครือข่ายส่วนตัวและอินเทอร์เน็ต เพื่อรักษาความปลอดภัยของเครือข่ายส่วนตัว:



เครือข่ายภายนอกเบื้องต้น

องค์กรทั้งหลายใช้มาตรการต่าง ๆ เพื่อใช้ไฟร์วอลล์เป็นมาตรการป้องกัน
ตัวกรองแพ็คเก็ต IP ให้การปกป้องที่ยังมีจุดด้อย
และยากที่จะบริหารจัดการ อีกทั้งยังง่ายที่จะถูกจู่โจม
เกตเวย์ของแอปพลิเคชันมีความปลอดภัยมากกว่าตัวกรองแพ็คเก็ต
และบริหารจัดการได้ง่ายกว่าเนื่องจากเกตเวย์ดังกล่าวนี้เสี่ยงกับแอปพลิเค
ชันเฉพาะบางแอปพลิเคชันเท่านั้น เช่น ระบบอีเมลเฉพาะ
เกตเวย์ของวงจรถือเป็นวิธีที่มีประสิทธิภาพมากที่สุดเมื่อผู้ใช้แอปพลิเคชันเ
ครือข่าย
เป็นปัจจัยที่ต้องให้ความสำคัญมากกว่าข้อมูลที่แอปพลิเคชันนั้นส่งผ่าน
พร็อกซีย์เซิร์ฟเวอร์ถือเป็นเครื่องมือที่ให้ความปลอดภัยที่ครอบคลุม
ประกอบด้วยเกตเวย์แอปพลิเคชัน
สิทธิ์ในการเข้าใช้อย่างปลอดภัยสำหรับผู้ใช้ที่ไม่ประสงค์ออกนาม
และบริการอื่น ๆ ต่อไปนี้คือรายละเอียดบางประการเกี่ยวกับตัวเลือกต่าง ๆ
เหล่านี้:

- **ตัวกรองแพ็คเก็ต IP**
  ตัวกรองแพ็คเก็ต IP คือ ปฏิบัติการแรกสุดของเทคโนโลยีไฟร์วอลล์
  ส่วนหัวของแพ็คเก็ตจะถูกตรวจสอบหาที่อยู่ต้นทางและปลายทาง Transmission Control Protocol (TCP) และหมายเลขพอร์ตของ User Datagram Protocol (UDP) และข้อมูลอื่น ๆ
  ตัวกรองแพ็คเก็ตเป็นเทคโนโลยีที่มีข้อจำกัด
  และจะทำงานได้ดีที่สุดในสภาพแวดล้อมที่มีความปลอดภัยอย่างเห็นได้ชัด ยกตัวอย่างเช่น
  ที่ซึ่งทุกอย่างที่อยู่ด้านนอกเครือข่ายภายนอกจะไม่มีความน่าเชื่อถือ
  ส่วนทุกอย่างที่อยู่ภายในเครือข่ายดังกล่าวนี้จะมีความน่าเชื่อถือ ในช่วงไม่กี่ปีที่ผ่านมา
  ผู้ขายหลายรายได้ปรับปรุงวิธีการกรองแพ็คเก็ต
  ด้วยการเพิ่มคุณลักษณะการตัดสินใจที่ชาญฉลาดให้แก่ส่วนสำคัญของตัวกรองแพ็คเก็ต
  ทำให้เกิดรูปแบบใหม่ของตัวกรองแพ็คเก็ตที่เรียกว่า *การตรวจสอบโปรโตคอลเต็มสภาพ (stateful protocol inspection)* คุณสามารถกำหนดค่าตัวกรองแพ็คเก็ตให้ยอมรับแพ็คเก็ตเฉพาะประเภท
  ในขณะที่ปฏิเสธประเภทอื่น ๆ ทั้งหมด หรือปฏิเสธแพ็คเก็ตเฉพาะประเภทและยอมรับประเภทอื่น ๆ ทั้งหมด
- **เกตเวย์ของแอปพลิเคชัน**
  เกตเวย์ของแอปพลิเคชันจะถูกนำมาใช้
  เมื่อเนื้อหาที่แท้จริงของแอปพลิเคชันเป็นประเด็นที่น่าเป็นห่วงมากที่สุด
  ซึ่งจะเกี่ยวข้องทั้งในเรื่องจุดแข็งและข้อจำกัดของเกตเวย์ของแอปพลิเคชัน
  เนื่องจากเกตเวย์ของแอปพลิเคชันไม่ยอมปรับตัวเข้ากับเทคโนโลยีที่มีการเปลี่ยนแปลงได้ง่าย ๆ
- **เกตเวย์ของวงจร**
  เกตเวย์ของวงจร คือ
  อุโมงค์ที่สร้างขึ้นผ่านไฟร์วอลล์สำหรับเชื่อมต่อกระบวนการหรือระบบเฉพาะที่อยู่ด้านหนึ่งเข้ากับกระบวนการ หรือระบบเฉพาะที่อยู่อีกด้านหนึ่ง
  เกตเวย์ของวงจรนำมาใช้ได้ดีที่สุดในสถานการณ์ที่บุคคลที่กำลังใช้แอปพลิเคชัน
  มีความเป็นไปได้ว่าจะมีความเสี่ยงมากกว่าข้อมูลที่แอปพลิเคชันจัดการ
  เกตเวย์ของวงจรต่างจากตัวกรองแพ็คเก็ตในเรื่องความสามารถในการเชื่อมต่อกับแบบแผนแอปพลิเคชันนอกช่วงคลื่น ที่สามารถเพิ่มข้อมูลได้
- **พร็อกซีย์เซิร์ฟเวอร์**
  พร็อกซีย์เซิร์ฟเวอร์เป็นเครื่องมือด้านความปลอดภัยที่สมบูรณ์แบบ
  ซึ่งครอบคลุมถึงไฟร์วอลล์และฟังก์ชันการทำงานของเกยเวต์ของแอปพลิเคชัน
  ที่จัดการการจราจรของอินเทอร์เน็ตทั้งไปและจาก LAN
  พร็อกซีย์เซิร์ฟเวอร์ยังมีส่วนของการแคชชิ่งข้อมูลและการควบคุมการเข้าถึงอีกด้วย
  พร็อกซีย์เซิร์ฟเวอร์สามารถปรับปรุงผลการทำงาน ด้วยการแคชชิ่งและป้อนข้อมูลที่ร้องขอบ่อย ๆ โดยตรง เช่น เว็บเพจยอดนิยม
  พร็อกซีย์เซิร์ฟเวอร์ยังสามารถกรองและยกเลิกการร้องขอที่เจ้าของพิจารณาว่าไม่เหมาะสม เช่น
  การขอเข้าสู่แฟ้มกรรมสิทธิ์โดยไม่ได้รับอนุญาต

ต้องแน่ใจว่า
ลูกค้าได้ใช้ประโยชน์จากคุณลักษณะเรื่องความปลอดภัยของไฟร์วอลล์ที่สามารถช่วยเหลือพวกเขาได้
วางตำแหน่งเครือข่ายพารามิเตอร์ในโทโพโลจีของเครือขายตรงตำแหน่งที่การจราจรทั้งหมดจากภายนอกเครือข่ายบริษัทต้องผ่านทะลุเครือข่ายภายนอกที่ได้รับการดูแลโดยไฟร์วอลล์ภายนอก
คุณสามารถปรับเปลี่ยนการควบคุมการเข้าถึงสำหรับไฟร์วอลล์เพื่อตอบสนองความต้องการของลูกค้า
และสามารถกำหนดค่าไฟร์วอลล์ให้รายงานกรณีมีความพยายามเข้าระบบโดยไม่ได้รับอนุญาต

หากต้องการลดจำนวนพอร์ตที่คุณจำเป็นต้องเปิดบนไฟร์วอลล์ด้านในให้เหลือน้อยที่สุด คุณสามารถใช้แอปพลิเคชัน เลเยอร์ ไฟร์วอลล์ เช่น ISA SERVER 2000

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับ TCP/IP โปรดดูที่ "การออกแบบเครือข่าย TCP/IP " ที่
http://www.microsoft.com/resources/documentation/WindowsServ/2003/all/deployguide/en-us/dnsbb_tcp_overview.asp

เครือข่ายไร้สาย

ตามค่าเริ่มต้นนั้น
เครือข่ายไร้สายมักถูกกำหนดค่าในลักษณะที่จะปล่อยให้มีการลอบฟังบนสัญญาณไร้สาย
เครือข่ายไร้สายอาจเอื้อประโยชน์ให้กับการเจาะเข้าระบบของบุคคลภายนอกที่ประสงค์ร้าย
เนื่องจากการตั้งค่าเริ่มต้นสำหรับฮาร์ดแวร์ไร้สายบางรายการ
ความสามารถในการเข้าถึงที่เครือข่ายไร้สายเสนอและการแสดงวิธีการเข้ารหัส
มีตัวเลือกการกำหนดค่าและเครื่องมือชุดหนึ่งซึ่งสามารถป้องกันการลอบฟัง
แต่จำไว้ว่าทั้งการกำหนดค่าและเครื่องมือจะไม่ช่วยในเรื่องการป้องกันเครื่องคอมพิวเตอร์จากแฮ็คเกอร์
และไวรัสซึ่งเข้าสู่ระบบผ่านทางการเชื่อมต่ออินเทอร์เน็ต ดังนั้น
มีความสำคัญอย่างยิ่งยวดที่จะรวมไฟร์วอลล์เข้าไว้ด้วย
เพื่อป้องกันเครื่องคอมพิวเตอร์จากผู้บุกรุกที่ไม่พึงประสงค์บนอินเทอร์เน็ต

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการป้องกันเครือข่ายไร้สาย โปรดดูที่
"วิธีทำให้เครือข่ายบ้านแบบไร้สาย 802.11B มีความปลอดภัยยิ่งขึ้น"
ได้จาก http://support.microsoft.com/default.aspx?scid=kb;en-us;309369

เหตุการณ์จำลองเกี่ยวกับความปลอดภัยของเครือข่าย

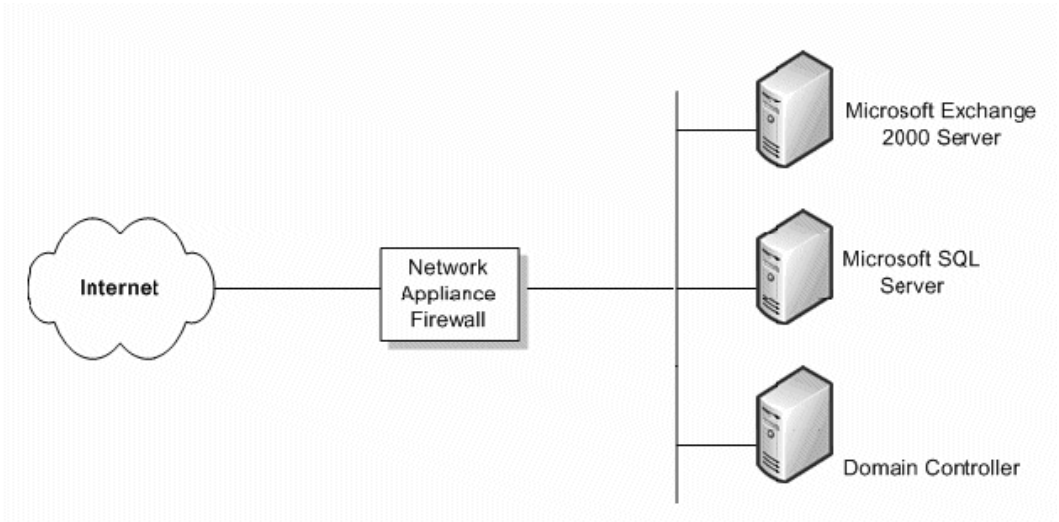
ระดับความปลอดภัยของเครือข่ายที่องค์กรของลูกค้าต้องการขึ้นอยู่กับหลายปัจจัย
บ่อยครั้งจะนำไปสู่การชั่งน้ำหนักระหว่างเรื่องของงบประมาณและความจำเป็นในการทำให้ข้อมูลของบริษัทมีความปลอดภัยอยู่เสมอ
มีความเป็นไปได้ที่ธุรกิจขนาดเล็กจะมีโครงสร้างความปลอดภัยที่สลับซับซ้อนมาก ๆ
อันจะช่วยให้เครือข่ายมีความปลอดภัยในระดับสูงสุดเท่าที่จะเป็นไปได้
แต่ธุรกิจขนาดเล็กอาจจะไม่สามารถลงทุนเพื่อให้ได้ความปลอดภัยในระดับนั้น สำหรับเนื้อหาส่วนนี้ เราจะดูที่เหตุการณ์จำลองรวม 4 เหตุการณ์
พร้อมให้คำแนะนำสำหรับแต่ละเหตุการณ์ที่นำเสนอความปลอดภัยในระดับที่แตกต่างกัน

ไม่มีไฟร์วอลล์

ถ้าลูกค้าของคุณใช้อินเทอร์เน็ตแต่ไม่มีไฟร์วอลล์
มาตรการด้านความปลอดภัยของเครือข่ายบางมาตรการจำเป็นต้องได้รับการปฏิบัติ มีเครื่องมือไฟร์วอลล์ระดับเครือข่ายแบบง่าย ๆ
ที่ให้ความปลอดภัยเพียงพอที่จะป้องปรามบุคคลที่มีแนวโน้มว่าจะกลายเป็นแฮ็คเกอร์

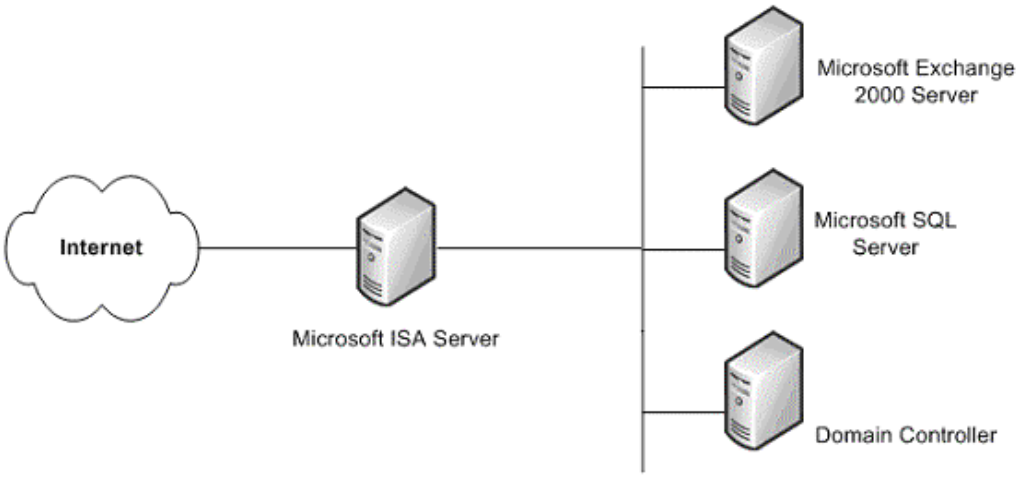
ไฟร์วอลล์ธรรมดาหนึ่งอัน

ความปลอดภัยขั้นต่ำที่สุดที่แนะนำ คือ
ไฟร์วอลล์ธรรมดาหนึ่งอันระหว่างอินเตอร์เน็ตและข้อมูลของลูกค้าของคุณ
ไฟร์วอลล์ในลักษณะนี้อาจจะไม่ให้ความปลอดภัยขั้นก้าวหน้าไม่ว่าจะเป็นระดับใด ๆ ก็ตาม และไม่น่าจะเข้าข่ายว่ามีความปลอดภัยสูง
แต่ก็ยังดีกว่าไม่มีอะไรเลย



ไฟร์วอลล์ธรรมดา

ได้แต่หวังว่า
งบประมาณลูกค้าจะเปิดโอกาสให้ลูกค้าใช้แนวทางแก้ปัญหาที่มีความปลอดภัยสูงขึ้น ซึ่งจะช่วยป้องกันข้อมูลบริษัทของพวกเขา
แนวทางแก้ปัญหาในลักษณะนี้ก็คือ ISA SERVER
ต้นทุนที่เพิ่มขึ้นของเซิร์ฟเวอร์เสริมนี้
ได้สร้างความปลอดภัยในระดับสูงกว่าการใช้ไฟร์วอลล์ของคุณโดยเฉลี่ยค่อนข้างมาก เนื่องจากมีเฉพาะส่วนของการแปลที่อยู่เครือข่าย (NAT) และตัวกรองแพ็คเก็ต



ไฟร์วอลล์ ISA SERVER

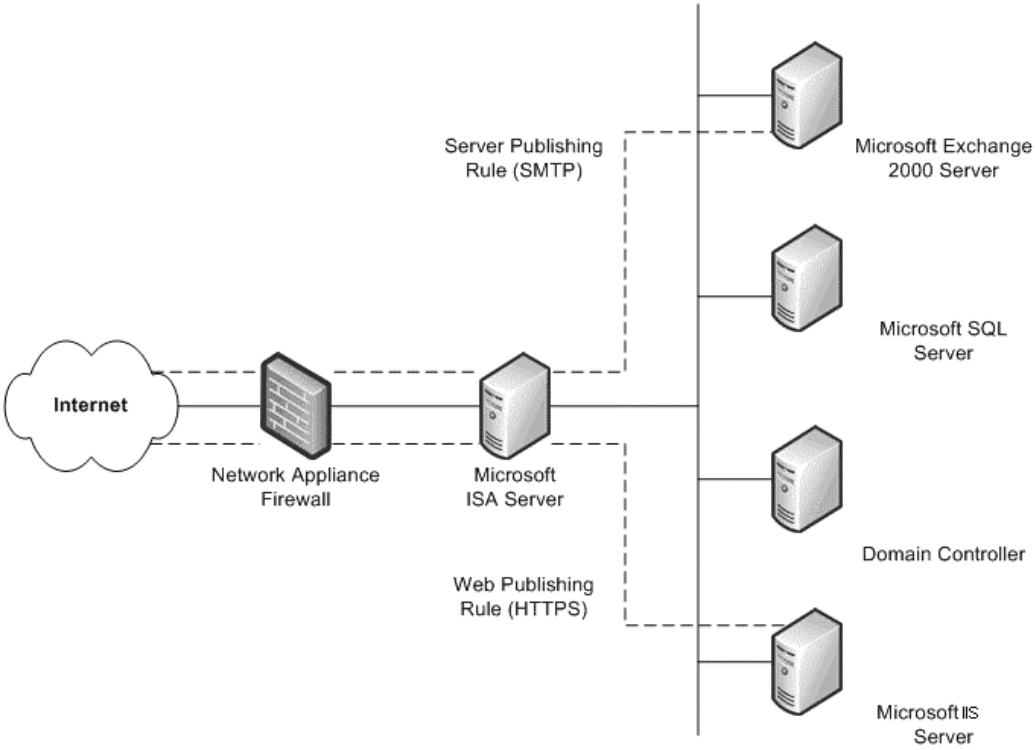
แนวทางแก้ปัญหาโดยใช้ไฟร์วอลล์เดี่ยวนี้ให้ความปลอดภัยได้มากกว่าเครื่องมือไฟร์วอลล์ในระดับการป้อนข้อมูล
ทั้งยังให้บริการด้านความปลอดภัยเฉพาะของโปรแกรม WINDOWS

ไฟร์วอลล์ที่มีอยู่แล้วหนึ่งอัน

ถ้าลูกค้ามีไฟร์วอลล์อยู่แล้ว
โดยไฟร์วอลล์นี้แยกอินทราเน็ตออกจากอินเทอร์เน็ต
คุณอาจจะต้องพิจารณาใช้ไฟล์วอลล์เสริมที่คุณสามารถใช้หลาย ๆ วิธีเพื่อกำหนดค่ารีซอร์สภายในให้กับอินเทอร์เน็ต

หนึ่งในวิธีการนั้น คือ การประกาศเว็บ การประกาศเว็บจะนำมาใช้เมื่อติดตั้ง ISA SERVER ไว้ด้านหน้าเว็บเบราว์เซอร์ขององค์กร
และใช้เว็บเบราว์เซอร์นี้เพื่อเข้าถึงผู้ใช้อินเทอร์เน็ต ด้วยคำขอเว็บที่เข้ามา ISA SERVER จะสามารถแสดงตัวเป็นเว็บเซิร์ฟเวอร์สำหรับโลกภายนอก
ตอบสนองความต้องการเนื้อหาเว็บของลูกค้าโดยดึงออกมาจากแคชของเซิร์ฟเวอร์ ISA SERVER
ส่งต่อคำขอไปยังเว็บเซิร์ฟเวอร์ก็ต่อเมื่อแคชของเซิร์ฟเวอร์ไม่สามารถให้บริการคำขอนั้นได้เท่านั้น

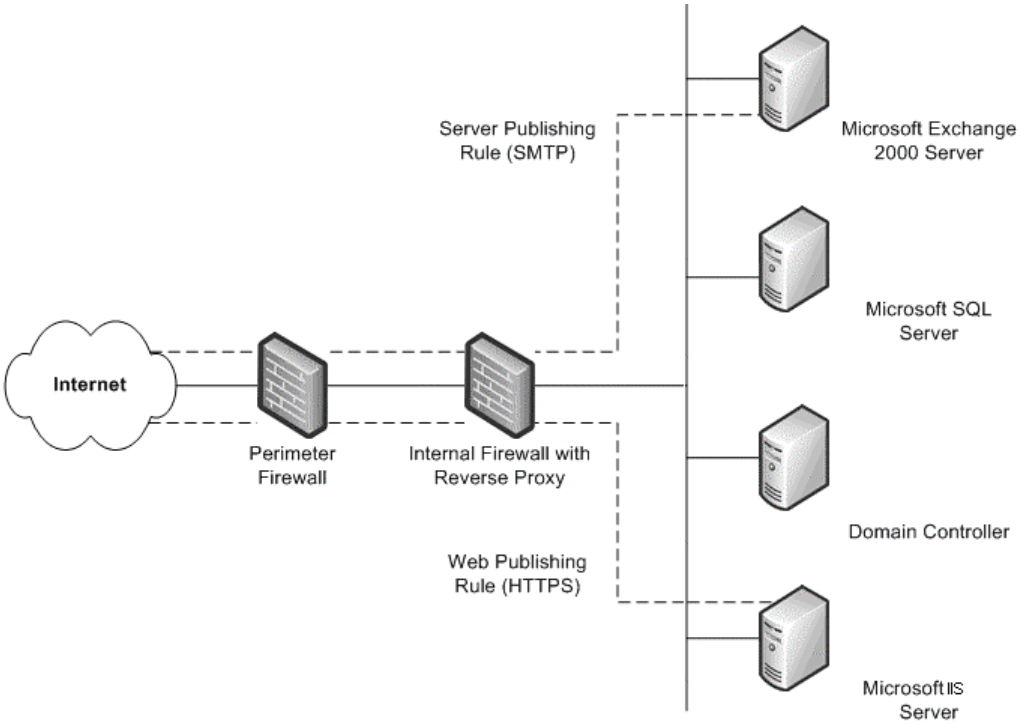
อีกวิธีการหนึ่ง คือ การประกาศเซิร์ฟเวอร์ ISA SERVER
ปล่อยให้มีการประกาศเซิร์ฟเวอร์ภายในไปยังอินเทอร์เน็ตโดยไม่ลดระดับความปลอดภัยของเครือข่ายภายใน
คุณสามารถกำหนดค่าการประกาศเว็บและกฎการประกาศเซิร์ฟเวอร์ซึ่งเป็นตัวกำหนดว่า ควรส่งคำขอใดไปที่เซิร์ฟเวอร์บนเครือข่ายท้องถิ่น
และยังให้ชั้นความปลอดภัยเพิ่มขึ้นสำหรับเซิร์ฟเวอร์ภายใน



ไฟร์วอลล์ที่มีอยู่พร้อม ISA SERVER เพิ่ม

ไฟร์วอลล์ที่มีอยู่แล้วสองอัน

เหตุการณ์จำลองลำดับที่สี่ คือ องค์กรมีไฟร์วอลล์สองอัน
ทั้งยังมีเครือข่ายภายนอกที่ถูกสร้างขึ้นเรียบร้อยแล้ว (DMZ)
เซิร์ฟเวอร์หนึ่งเซิร์ฟเวอร์หรือมากกว่านั้นกำลังให้บริการพร็อกซีย์ย้อนกลับ
ซึ่งจะทำให้ลูกค้าอินเทอร์เน็ตไม่สามารถเข้าถึงเซิร์ฟเวอร์บนอินทราเน็ตได้โดยตรง และในเวลาเดียวกันนี้ ไฟร์วอลล์อีกอันหนึ่ง
ซึ่งสมมุติให้เป็นไฟร์วอลล์ภายใน
กำลังยับยั้งคำขอสำหรับเซิร์ฟเวอร์ภายใน ตรวจสอบแพ็คเก็ตเหล่านั้น
และส่งต่อแพ็คเก็ตแทนแม่ข่ายอินเทอร์เน็ต



ไฟร์วอลล์ที่มีอยู่สองอัน

เหตุการณ์จำลองนี้เหมือนกับสถานการณ์ก่อนหน้านี้หลังจากเพิ่มไฟร์วอลล์อันที่สอง
ข้อแตกต่างเพียงอย่างเดียวก็คือไฟร์วอลล์ภายในซึ่งสนับสนุนพร็อกซีย์ย้อนกลับไม่ใช่ ISA SERVER ในสถานการณ์นี้
คุณควรจะทำงานอย่างใกล้ชิดกับผู้จัดการไฟร์วอลล์แต่ละอัน
เพื่อร่างกฎการประกาศเซิร์ฟเวอร์
โดยคำนึงถึงนโยบายด้านความปลอดภัยเป็นสำคัญ

การบริหารจัดการโปรแกรมปะแก้ความปลอดภัย

ระบบปฏิบัติการและแอปพลิเคชันมีความสลับซับซ้อนมาก
และสามารถประกอบด้วยรหัสนับล้านบรรทัดที่โปรแกรมเมอร์จากทั่วทุกมุมโลกเขียนขึ้น สิ่งสำคัญประการหนึ่งคือ
ซอฟต์แวร์ต้องทำงานได้อย่างน่าเชื่อถือ
และไม่ลดทอนความสำคัญเรื่องความปลอดภัยหรือเสถียรภาพของสภาพแวดล้อมไอที หากต้องการขจัดปัญหาต่าง ๆ ให้เหลือน้อยที่สุด
ควรจะมีการทดสอบทั้งโปรแกรมก่อนนำออกวางจำหน่าย อย่างไรก็ตาม
แฮ็คเกอร์ก็ยังคงเพียรพยายามค้นหาจุดอ่อนในซอฟต์แวร์ ดังนั้น
การคาดหวังว่าจะมีการแอบเจาะเข้าระบบบอีกในอนาคตจึงไม่ใช่ว่าจะเป็นไปไม่ได้

สำหรับองค์กรจำนวนมากแล้ว การบริหารจัดการโปรแกรมปะแก้ (PATCH) ถือเป็นส่วนหนึ่งของการเปลี่ยนแปลงโดยองค์รวม และกลยุทธ์การบริหารจัดการการกำหนดค่า อย่างไรก็ตาม ไม่ว่าลักษณะและขนาดขององค์กรจะเป็นเช่นไร สิ่งที่สำคัญอย่างยิ่งยวดก็คือ จะต้องมีกลยุทธ์การบริหารจัดการโปรแกรมปะแก้ (PATCH) ที่ดี ถึงแม้ว่าในขณะนั้น องค์กรยังไม่มีการบริหารจัดการการเปลี่ยนแปลงและการกำหนดค่าที่มีประสิทธิภาพก็ตามที ความสำเร็จจากการโจมตีระบบคอมพิวเตอร์ส่วนใหญ่เกิดขึ้นกับระบบของคอมพิวเตอร์ ที่ยังไม่ได้ติดตั้งโปรแกรมปะแก้ความปลอดภัย

โปรแกรมปะแก้ความปลอดภัยแสดงให้เห็นถึงความท้าทายเฉพาะต่อองค์กรส่วนมาก เมื่อจุดอ่อนปรากฏให้เห็นในซอฟต์แวร์ ผู้โจมตีจะกระจายข้อมูลเกี่ยวกับเรื่องนี้ให้กับแฮ็คเกอร์คนอื่น ๆ อย่างรวดเร็ว เมื่อจุดออนปรากฏขึ้นในตัวซอฟต์แวร์ ไมโครซอฟต์จะเข้ามาแก้ไขด้วยการปล่อยโปรแกรมปะแก้ความปลอดภัยโดยเร็วที่สุดเท่าที่จะทำได้ ความปลอดภัยที่ลูกค้าต้องอาศัยและคาดหวังอาจจะน้อยมากจนกว่าจะนำโปรแกรมปะแก้มาใช้

ในสภาพแวดล้อมของ NAVISION คุณต้องแน่ใจว่าลูกค้าได้รับการติดตั้งโปรแกรมปะแก้ความปลอดภัยล่าสุดทั่วทั้งระบบ ต้องแน่ใจว่าลูกค้าได้ใช้เทคโนโลยีอันหนึ่งอันใดของไมโครซอฟท์ เทคโนโลยีดังกล่าวรวมถึง:

- **บริการแจ้งให้ทราบเรื่องความปลอดภัยของไมโครซอฟท์**
  บริการแจ้งให้ทราบเรื่องความปลอดภัย คือ รายการอีเมลที่จะแจกจ่ายประกาศทุกครั้งที่มีโปรแกรมปรับปรุง การแจ้งให้ทราบเหล่านี้ถือเป็นองค์ประกอบที่มีคุณค่าสำหรับกลยุทธ์ความปลอดภัยเชิงสนับสนุน หรือจะเปิดดูคำประกาศเหล่านี้ได้จากเว็บไซต์ TechNet Product Security Notification: http://www.microsoft.com/technet/security/bulletin/notify.mspx
- **โปรแกรมปรับปรุงอัตโนมัติของไมโครซอฟท์**
  Windows สามารถนำโปรแกรมปรับปรุงด้านความปลอดภัยมาใช้กับคอมพิวเตอร์ของคุณได้โดยอัตโนมัติ
- **เครื่องมือค้นหากระดานข่าวความปลอดภัยของไมโครซอฟท์**
  คุณสามารถใช้เครื่องมือค้นหา กระดานข่าวความปลอดภัย ได้จากเว็บไซต์ Security Bulletin Service ที่: http://www.microsoft.com/technet/security/current.aspx ลูกค้าสามารถระบุได้ว่า โปรแกรมปรับปรุงใดที่ลูกค้าต้องการโดยพิจารณาจากระบบปฏิบัติการ แอปพลิเคชัน และชุดบริการ (Service Pack) ที่พวกเขาใช้

- **ตัววิเคราะห์ความปลอดภัยเบื้องต้นของไมโครซอฟท์ (MBSA)**
  เลือกใช้เครื่องมือกราฟิคนี้ได้จากเว็บไซต์ Microsoft Baseline Security Analyzer ที่:
  http://www.microsoft.com/technet/security/tools/mbsahome.mspx
  เครื่องมือนี้ทำงานโดยการเปรียบเทียบสถานะปัจจุบันของคอมพิวเตอร์กับรายชื่อโปรแกรมปรับปรุงที่ไมโครซอฟท์ดูแลอยู่ MBSA
  ยังช่วยตรวจสอบความปลอดภัยเบื้องต้นเกี่ยวกับความรัดกุมของรหัสผ่านและการกำหนดระยะเวลาหมดอายุของรหัสผ่าน นโยบายบัญชีของผู้เข้ามาเยี่ยมระบบ และส่วนอื่น ๆ MBSA
  ยังค้นหาจุดเสี่ยงในบริการข้อมูลอินเทอร์เน็ตของไมโครซอฟท์ (IIS), SQL Server™ 2000, Exchange 5.5, Exchange 2000, และ Exchange Server 2003
- **บริการปรับปรุงซอฟต์แวร์ของไมโครซอฟท์ (SUS)**
  เครื่องมือดังกล่าวนี้ที่เคยรู้จักกันในชื่อ Windows Update Corporate Edition
  จะช่วยให้ภาคธุรกิจทำหน้าที่เป็นแม่ข่ายบนคอมพิวเตอร์ภายในให้กับการปรับปรุงที่สำคัญทั้งหมดและแพ็คเก็จความปลอดภัย (SRPs) ที่อยู่บนไซต์ Windows Update ซึ่งเป็นไซต์สาธารณะ
  เครื่องมือนี้ทำงานรวมกับเครื่องไคลเอนต์การปรับปรุงอัตโนมัติ (AU)
  รุ่นใหม่เพื่อวางรูปแบบพื้นฐานสำหรับการดาวน์โหลดอัตโนมัติ และติดตั้งกลยุทธ์ เครื่องไคลเอนต์ AU ชุดใหม่ยังรวมถึงเครื่องไคลเอนต์สำหรับระบบปฏิบัติการของ Windows 2000 และ Windows Server 2003 และมีความสามารถในการติดตั้งโปรแกรมปรับปรุงที่ดาวน์โหลดมาได้โดยอัตโนมัติ
  สำหรับข้อมูลเพิ่มเติมเกี่ยวกับ Microsoft SUS โปรดดูที่
  http://www.microsoft.com/windows2000/windowsupdate/sus/default.asp
- **ชุดบริการปรับปรุงซอฟต์แวร์ Microsoft Systems Management Server (SMS)**
  SMS Software Update Services Feature Pack
  ประกอบด้วยเครื่องมือชุดหนึ่งที่มุ่งจะทำให้กระบวนการนำเสนอโปรแกรมปรับปรุงซอฟต์แวร์ในองค์กรเป็นไปอย่างราบรื่น เครื่องมือนี้รวมไปถึง เครื่องมือจัดระบบการปรับปรุงความปลอดภัย
  เครื่องมือจัดระบบการปรับปรุงของ Microsoft Office
  ตัวช่วยสร้างการแจกจ่ายโปรแกรมปรับปรุงซอฟต์แวร์ และเครื่องมือการรายงาน SMS Web พร้อมด้วย Add-in ของรายงานเว็บสำหรับการปรับปรุงซอฟต์แวร์
  สำหรับข้อมูลเพิ่มเติมเกี่ยวกับเครื่องมือแต่ละอย่าง โปรดดูที่
  http://www.microsoft.com/smserver/downloads/20/featurepacks/suspack/

พูดคุยกับลูกค้าของคุณเกี่ยวกับเครื่องมือแต่ละชนิดและส่งเสริมให้พวกเขาใช้เครื่องมือเหล่านั้น เป็นสิ่งสำคัญว่าประเด็นปัญหาความปลอดภัยจะต้องถูกหยิบยกขึ้นมาพิจารณาโดยเร็วที่สุดควบคู่กับการรักษาเสถียรภาพของสภาพแวดล้อม

การตั้งค่าความปลอดภัยสำหรับ SQL SERVER 2000

เนื่องจาก NAVISION ยังสามารถทำงานบน SQL SERVER 2000 สิ่งสำคัญ คือคุณต้องใช้มาตรการต่าง ๆ เพื่อเพิ่มความปลอดภัยให้กับกระบวนการติดตั้ง SQL SERVER 2000 ของลูกค้า
ขั้นตอนต่อไปนี้จะช่วยคุณเพิ่มความปลอดภัยให้กับ SQL SERVER:

- ต้องแน่ใจว่า ได้ติดตั้งระบบปฏิบัติการรุ่นล่าสุดและชุดบริการ SQL Server 2000 และโปรแกรมปรับปรุงแล้ว สำหรับข้อมูลล่าสุด
  โปรดดูที่เว็บไซต์ความปลอดภัยของไมโครซอฟท์ที่
  http://www.microsoft.com/security/default.asp
- สำหรับความปลอดภัยในระดับระบบแฟ้ม ต้องแน่ใจว่า
  ได้ติดตั้งแฟ้มข้อมูลและแฟ้มระบบทั้งหมดของ SQL Server 2000 ไว้บนพาร์ติชันของ NTFS แล้ว
  คุณควรกำหนดให้เฉพาะผู้ดูแลระบบหรือผู้ใช้ในระดับระบบเท่านั้นที่สามารถเข้าถึงแฟ้มเหล่านี้ได้ผ่านสิทธิ์ NTFS สิ่งนี้จะเป็นมาตรการป้องกันไม่ให้ผู้ใช้เข้าสู่แฟ้มเหล่านั้นเมื่อไม่ได้เรียกใช้บริการ MSSQLSERVER

- ใช้บัญชีโดเมนที่มีสิทธิพิเศษในระดับต่ำ เช่น NT Authority\Network Service หรือบัญชี LocalSystem (แนะนำ) สำหรับบริการ SQL Server 2000 (MSSQLSERVER) บัญชีนี้ควรจะมีสิทธิขั้นต่ำในโดเมนและสามารถช่วยปิดล้อม (แต่ไม่ใช่หยุด) การโจมตีเซิร์ฟเวอร์ในกรณีที่อาจมีความเสี่ยง กล่าวอีกนัยหนึ่ง คือ บัญชีนี้ควรมีแค่สิทธิ์ในโดเมนในระดับผู้ใช้ภายในเท่านั้น ถ้า SQL Server 2000 ใช้บัญชีผู้ดูแลระบบสำหรับโดเมนเพื่อเรียกใช้บริการ ภาวะเสี่ยงของเซิร์ฟเวอร์อาจจะก่อให้เกิดอันตรายต่อทั้งโดเมน หากต้องการเปลี่ยนแปลงการตั้งค่านี้ ให้ใช้ SQL Server Enterprise Manager ทำการเปลี่ยนแปลง รายชื่อการควบคุมการเข้าถึง (ACLs) บนแฟ้ม รีจิสตรี และสิทธิผู้ใช้ก็จะเปลี่ยนแปลงด้วยโดยอัตโนมัติ
- SQL Server 2000 เกือบทุกรุ่นจะถูกติดตั้งพร้อมกับฐานข้อมูลเริ่มต้นสองฐานข้อมูล อันได้แก่ ฐานข้อมูล **Northwind** และ **pubs** ฐานข้อมูลทั้งสองนี้ คือ ฐานข้อมูลตัวอย่างที่ถูกนำมาใช้สำหรับการทดสอบ การฝึกฝน และใช้เป็นตัวอย่างทั่วไป จึงไม่ควรถูกสลับสับเปลี่ยนภายในระบบการผลิต การรู้ว่ามีฐานข้อมูลเหล่านี้อยู่สามารถกระตุ้นให้แฮ็คเกอร์มีความพยายามตักตวงผลประโยชน์จากฐานข้อมูลดังกล่าว ที่รวมไปถึงการตั้งค่าเริ่มต้นและการกำหนดค่าเริ่มต้น ดังนั้นถ้ายังมีฐานข้อมูล **Northwind** และ **pubs** อยู่บนคอมพิวเตอร์ SQL Server 2000 สำหรับการผลิต ควรลบฐานข้อมูลทั้งสองนี้เสีย
- มีการปิดการทำงานของฟังก์ชันการตรวจสอบระบบ SQL Server 2000 ตั้งแต่เริ่มต้น จึงไม่จำเป็นต้องตรวจสอบเงื่อนไขใด ลักษณะนี้ทำให้การตรวจหาการบุกรุกทำได้ยากและช่วยเหลือแฮ็คเกอร์ปิดบังร่องรอยของตนเอง อย่างน้อยที่สุด คุณควรเปิดใช้งานการตรวจสอบการล็อกอินที่ไม่สำเร็จ

สำหรับข้อมูลปรับปรุงล่าสุดเกี่ยวกับความปลอดภัยของ SQL SERVER 2000 โปรดดูที่ http://www.microsoft.com/sql/techinfo/administration/2000/security/default.asp

เกี่ยวกับ MICROSOFT BUSINESS SOLUTIONS

MICROSOFT BUSINESS SOLUTIONS แผนกหนึ่งของบริษัทไมโครซอฟท์ นำเสนอแอปพลิเคชันและบริการแบบรวม สำหรับผู้ใช้ขั้นสุดท้ายอันหลากหลายเอาไว้ให้ โดยทั้งแอปพลิเคชันและบริการได้รับการออกแบบขึ้นมาเพื่อช่วยธุรกิจขนาดเล็ก ขนาดกลางและธุรกิจของบริษัทต่าง ๆ ให้สามารถติดต่อสื่อสารกับลูกค้า พนักงาน คู่ค้าและซัพพลายเออร์ได้อย่างใกล้ชิดมากขึ้น แอปพลิเคชันของ MICROSOFT BUSINESS SOLUTIONS ใช้ประโยชน์จากกระบวนการทางธุรกิจเชิงกลยุทธ์ทั้งในด้านการบริหารทางการเงิน การวิเคราะห์ การจัดการทรัพยากรบุคคล การบริหารโครงการ การบริหารลูกค้าสัมพันธ์ การบริหารการให้บริการในพื้นที่ การบริหารด้านซัพพลาย ธุรกิจพาณิชย์อิเล็กทรอนิกส์ การผลิตและการจัดการการค้าปลีก แอปพลิเคชันต่าง ๆ ได้รับการออกแบบขึ้นมาเพื่อให้มุมมองเชิงลึก ซึ่งจะช่วยให้ลูกค้าประสบความสำเร็จทางธุรกิจ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับ MICROSOFT BUSINESS SOLUTIONS โปรดดูที่ http://www.microsoft.com/BusinessSolutions/