บทความเรื่อง : เริ่มต้นอย่างไรดี เมื่อต้องการความปลอดภัย?

เรียบเรียงโดย : ศิริวรรณ อภิสิริเดช

คุณคงจะได้ยินเสมอๆเกี่ยวกับความสำคัญของการรักษาความปลอดภัยและโครงสร้างของการรักษาความปลอดภัยว่ามีความสำคัญอย่างไร บางทีก็อาจจะได้รับทราบข้อมูลมากมายเกี่ยวกับเงื่อนไขต่างๆ หรือโฆษณาต่างๆที่อ้างโดยผู้ขายว่าระบบของตัวเองสามารถแก้ไขปัญหาด้านความปลอดภัยให้แก่คุณได้ อย่างไรก็ตาม สิ่งหนึ่งที่คุณก็คงยังไม่แน่ใจคือ จะเริ่มจากตรงไหนดี มีการโฆษณาขายทั้งวิธีแก้ปัญหาภัยคุกคาม (threats) และ ช่องโหว่ของความปลอดภัยที่อันตราย (potential security holes) แต่คำถามหลักก็ยังคงค้างอยู่คือ "ควรจะทำอะไรบ้างขณะนี้เพื่ออย่างน้อยที่สุดจะได้เริ่มต้นรักษาความปลอดภัยให้แก่เครือข่ายเสียที?"

เอกสารฉบับนี้ไม่ได้จัดทำขึ้นเพื่อใช้เป็นหนทางแก้ไขปัญหาของคุณทุกปัญหา แต่มันก็สามารถช่วยให้คุณสามารถเริ่มทำการพิสูจน์และแก้ไขช่องโหว่เด่นๆ (ที่ส่วนใหญ่จะถูก compromise ได้ง่าย) บนเครือข่ายของคุณได้ และศึกษาค้นคว้าเพิ่มเติมในเว็บไซต์ http://www.sans.org/infosecFAQ/index.htm ซึ่งมีรายละเอียดเจาะลึกในแต่ละหัวข้อให้ด้วย

เมื่อต้องการที่จะก้าวเข้ามาปกป้องระบบเครือข่าย คุณก็ควรที่จะเข้าใจว่าจุดมุ่งหมายด้านความปลอดภัยหลักๆมีอยู่ 3 อย่างที่คุณจะต้องคำนึงถึงเสมอ คือ

- ความลับ (Confidentiality) คือ ต้องมั่นใจว่าข้อมูลส่วนตัวหรือข้อมูลที่เป็นความลับไม่ได้ถูกเปิดเผยและยังเป็นความลับอยู่
- ความสมบูรณ์ (Integrity) คือ ต้องมั่นใจว่าข้อมูลและระบบไม่ได้ถูกแก้ไขด้วยวิธีการใดๆที่ไม่ได้รับอนุญาต
- ความพร้อมใช้ (Availability) คือ ต้องมั่นใจว่าระบบและข้อมูลที่มีอยู่สามารถใช้ได้เมื่อต้องการ

หมายเหตุ: The National Institute of Standards and Technology (NIST) ได้เพิ่มจุดมุ่งหมายเข้าไปอีกคือ ความมีเหตุผล (Accountability) (ทุกกิจกรรมจะต้องสามารถติดตามได้) และ ความแน่นอน (Assurance) (ต้องมั่นใจว่าจุดมุ่งหมายหลักอื่นๆทั้งหมดมีอยู่จริง) [1] ขณะที่คุณประเมินการใช้งานเครื่องมือ ระบบ และกระบวนการต่างๆกัน จะต้องใช้หลักทั้งหมดของความปลอดภัยเข้ามาประกอบด้วยเสมอ

ขั้นตอนทั้ง 5 ที่คุณสามารถทำเพื่อให้ระบบเครือข่ายของคุณมีความปลอดภัยขึ้น

1. ปกป้องทรัพย์สินที่มีค่าที่สุดของคุณเป็นสิ่งแรก

เมื่อเริ่มต้นบนถนนสายความปลอดภัยของเครือข่าย คุณควรมุ่งเน้นไปที่ระบบที่คุณรู้สึกสะดวกที่สุดที่จะทำให้ปลอดภัยก่อน คุณอาจจะพร้อมที่จะลง service pack บน NT มากกว่าการปิดพอร์ตของ IP service บนระบบ UNIX ก็ได้ แต่ส่วนแรกที่คุณจะต้องมุ่งเน้นคือการป้องกันระบบที่มีข้อมูลซึ่งเป็นสมบัติมีค่าที่สุดของคุณก่อน

เช่น บริษัทหนึ่งมีเครื่องเซิร์ฟเวอร์ที่เป็น NT มากกว่า 60 เครื่อง อย่างไรก็ตามข้อมูลทางการเงิน ข้อมูลของลูกค้า และข้อมูลของพนักงานอยู่ในเครื่องเซิร์ฟเวอร์ที่เป็น UNIX เพียง 2 เครื่องเท่านั้น ดังนั้นในกรณีนี้จึงเป็นเรื่องที่รู้กันอยู่แล้วว่าควรจะมุ่งเน้นไปที่ระบบเซิร์ฟเวอร์ที่เป็น UNIX ก่อนที่จะจัดการกับระบบ NT

สำหรับการทำให้มีระบบ NT print server ที่ปลอดภัยที่สุดก็เป็นการดี แต่สิ่งแรกที่คุณอาจจะต้องให้ความสำคัญก็คือการหยุดระบบธุรกิจที่สำคัญของเครือข่าย ซึ่งในขั้นนี้คุณควรจะปรึกษาระดับ senior management ก่อนว่าระบบไหนที่สำคัญที่สุดในมุมมองทางธุรกิจ เพราะสิ่งที่คุณคิดอาจจะแตกต่างจากที่พวกเขาคิดก็ได้

2. ปกป้องที่บริเวณรอบๆ

คุณต้องทำอย่างไม่ให้มีข้อผิดพลาดเลย เพราะว่าคุณกำลังถูก probe อยู่ตลอดเวลา คุณสามารถพิสูจน์ด้วยตนเอง โดยการดาวน์โหลด personal firewall เช่น ZoneAlarm (http://www.zonelabs.com) มาติดตั้งที่เครื่องของคุณที่ต่ออยู่กับอินเทอร์เน็ตด้วยการเชื่อมต่อแบบใดก็ตาม แล้วเปิดให้โปรแกรมทำการล็อกไว้ แล้วนั่งดูผลที่จะเกิดขึ้น คุณจะเห็นว่าภายใน 48 ชั่วโมงโอกาสที่คุณจะถูก probe มีมากมายเหลือเกิน และสิ่งเดียวกันนี้เองกำลังเกิดขึ้นกับบริษัทของคุณ ดังนั้นต้องมั่นใจว่าคุณสามารถชี้ชัดได้ว่าจุดไหนเป็นจุดที่เข้าถึงเครือข่ายของคุณแล้วทำการป้องกันจุดเหล่านั้น

Firewalls:

วิธีดั้งเดิมวิธีหนึ่งสำหรับปกป้องบริเวณรอบๆเครือข่ายก็คือการติดตั้งไฟล์วอลล์ที่ถูกตั้งค่าไว้อย่างถูกต้องเหมาะสม (สังเกตว่าไม่ใช่การซื้อไฟล์วอลล์และติดตั้งด้วยค่าที่ถูกตั้งไว้โดย default) ทันทีที่คุณมีไฟล์วอลล์แล้ว ควรกำหนดเส้นทาง (route) ของจุดเชื่อมต่อไปยังเครือข่ายภายนอกที่จะเข้ามายังไฟล์วอลล์ให้มากที่สุดเท่าที่จะเป็นไปได้ คุณสามารถมีไฟล์วอลล์ที่แข็งแรงที่สุดแต่ถ้าแฮกเกอร์ผ่าน dial-up server เข้ามาได้อย่างง่ายๆ (หรือยิ่งเลวร้ายถ้าโมเด็มต่อเข้าโดยตรงกับหนึ่งในระบบของคุณ) ดังนั้นไฟล์วอลล์ของคุณก็ไม่มีประโยชน์เลย เมื่อคุณได้รวบรวมจำนวนการเชื่อมต่อหลายๆการเชื่อมต่อที่ผ่านไฟล์วอลล์แล้ว ให้ตรวจสอบการตั้งค่าอีกครั้งเพื่อความแน่ใจว่าการเชื่อมต่อเหล่านั้นถูกป้องกันอย่างถูกต้องแล้ว

Intrusion Detection Systems:

ส่วนเสริมสำหรับไฟล์วอลล์ก็คือระบบตรวจจับการบุกรุก (Intrusion Detection System) ซึ่งเป็นเครื่องมือสำคัญมากที่สามารถตรวจดูเครือข่ายได้ว่ามีกิจกรรมอะไรที่น่าสงสัยเกิดขึ้นหรือไม่ และจะแจ้งเตือน (alert) คุณเมื่อมีการทำ access compromise เกิดขึ้น ในเอกสารเผยแพร่หัวข้อ Intrusion Detection Systems ของหน่วยงาน NIST ระบุว่าระบบตรวจจับการบุกรุกมีด้วยกัน 3 ชนิดซึ่งแต่ละชนิดมีข้อดีและข้อเสียแตกต่างกัน ระบบทั้ง 3 นั้นได้แก่

- Network-based IDSs
- Host-based IDSs
- Application-based IDS [3]

มีหลายบริษัทที่เสนอขายระบบตรวจจับการบุกรุกซึ่งมีทั้งดีและไม่ดี คุณจึงควรศึกษารายละเอียดและวางแผนให้ดีก่อนที่จะใช้ สำหรับตัวอย่างของระบบตรวจจับการบุกรุกที่เป็น open source network IDS ที่ยอดเยี่ยมคือ snort ซึ่งคุณสามารถดาวน์โหลดได้จาก http://www.snort.org

3. การป้องกันระบบภายในที่สำคัญ

หลังจากที่ทำการป้องกันที่ระบบสำคัญและบริเวณรอบๆเครือข่ายของคุณแล้ว ขั้นตอนต่อไปคือ การป้องกันระบบภายในที่สำคัญ (core/internal systems) ของคุณ หลักสำคัญที่ควรจำไว้คือค่า default ของการติดตั้งระบบใดๆก็ตามนั้นไม่มีความปลอดภัยเลย

Microsoft Windows NT/2000

a. *Service Packs and hotfixes*

คุณควรติดตาม service packs และ hotfixes ใหม่ๆอยู่เสมอ และ Microsoft ได้เผยแพร่เครื่องมือชื่อ Qchain (http://support.microsoft.com/support/kb/articles/Q296/8/61.asp) สำหรับติดตั้ง hotfixes หลายๆตัวโดยไม่ต้อง reboot เครื่องทุกครั้งหลังจากติดตั้งเสร็จแต่ละตัว (แต่คุณก็ยังต้อง reboot อย่างน้อย 1 ครั้งหลังจากลงครบทุกตัวแล้ว)

b. *Hardening your system*

ค่า default ของการติดตั้งไม่มีความปลอดภัยเลย!! ถ้าติดตั้งเซิร์ฟเวอร์ใหม่ ต้องระบุหน้าที่ของเครื่องให้ชัดเจนแล้วปิดหรือยกเลิกการติดตั้งบริการใดๆ หรือพอร์ตใดๆที่ไม่จำเป็นออก Microsoft มี checklists ที่ใช้ประกอบการติดตั้งทั้ง Domain Controllers และ member servers เช่น Checklist for NT 4.0 member servers อยู่ที่: http://www.microsoft.com/technet/security/mbrsrvcl.asp
เพียงแต่ต้องมั่นใจว่าได้ปรับเปลี่ยน checklist ให้ตรงกับความต้องการเฉพาะของคุณด้วย

Microsoft ได้เผยแพร่เครื่องมือออกมาใหม่ชื่อ HFNetChk ซึ่งช่วยให้ผู้ดูแลระบบสามารถตรวจสอบสถานะของ patch ของทุกเครื่องในเครือข่ายจากเครื่องที่เป็นศูนย์กลางได้ ซึ่งตรวจสอบได้ทั้ง NT4.0, Windows2000, IIS, SQL, และ IE5
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/itsolutions/security/tools/hfnetchk.asp

แหล่งอ้างอิงอื่นๆสำหรับการทำ hardening Windows2000 server คือ "Hardening Windows 2000" ของ Philip Cox [4] ซึ่งมีรายละเอียดเกี่ยวกับการติดตั้ง, นโยบายของระบบ, การกำจัดบริการที่ไม่จำเป็น และการจัดการ TCP/IP อย่างเข้มงวด

c. *Auditing*

เพื่อให้มั่นใจว่าไม่มีการกระทำที่ไม่ได้รับอนุญาตใดๆเกิดขึ้นในระบบของคุณ คุณจึงต้องทำการ enable auditing ไม่ว่าจะเป็นการตรวจจับการกระทำที่ไม่ได้รับอนุญาตหรือเป็นเพียงการแจ้งแก่ผู้ใช้ระบบว่า เครื่อข่ายไม่ได้ลบไฟล์ให้ก็ตาม คุณจะต้องทำการ enable auditing สำหรับเหตุการณ์ต่างๆเช่น การสร้าง/ลบไฟล์, การล็อกอินผิด , การพยายามเข้าถึงไดเรกทอรีที่ไม่ได้รับอนุญาต เป็นต้น แต่การ audit จะไม่ให้ผลดีเลยถ้าคุณไม่คอยหมั่นตรวจสอบและพิจารณาดู audit logs อย่างสม่ำเสมอ

d. *Password and account policies*

หนึ่งในวิธีการหลากหลายที่ผู้บุกรุกมักจะใช้เข้าถึงเครือข่ายคือการแอบใช้ชื่อบัญชีและรหัสผ่านของผู้ใช้ของระบบ ดังนั้นคุณควรบังคับให้มีการตั้งรหัสผ่านและมีนโยบายที่รัดกุมเพื่อลดโอกาสของผู้บุกรุกที่จะเข้าถึงเครือข่ายของคุณ วิธีหนึ่งที่จะช่วยลดโอกาสที่จะมีใครขโมยหรือเดารหัสผ่านได้ก็คือการทำ account lockout ซึ่งจะล็อคชื่อบัญชีของผู้ใช้นั้นถ้ามีการเข้ามาด้วยรหัสผ่านที่ผิดด้วยจำนวนครั้งที่กำหนดไว้ โดยวิธีการนี้จะช่วยป้องกันการโจมตีที่เรียกว่า brute-force password attack ได้

คุณสามารถบังคับใช้รหัสผ่านที่แข็งแรงได้โดยใช้เครื่องมือเช่น passfilt และ passprop แต่ต้องทดสอบให้แน่ใจก่อนจะใช้จริง เช่น ถ้าคุณใช้ passfit แล้วระบบที่ใช้ pass-through authentication (เช่น การล็อกอินเข้าเครื่อง Novell และ NT ในเวลาเดียวกัน) จะทำงานได้ไม่สมบูรณ์

คุณสามารถทดสอบความแข็งแรงของรหัสผ่านที่ผู้ใช้ในระบบตั้งไว้ได้โดยใช้เครื่องมือ password-cracking เช่น L0phtcrack ซึ่งเวอร์ชันล่าสุดคือ LC3 (http://www.atstake.com/lc3) สามารถใช้แกะรหัสผ่านของ NT ได้ภายในไม่กี่สัปดาห์ อย่างไรก็ตามผลที่ได้รับจากการใช้เครื่องมือเหล่านี้ก็คือสามารถตรวจสอบได้ว่ารหัสผ่านของบัญชีผู้ใช้มีจุดอ่อนมากน้อยเพียงใด

e. *Vulnerability scanners*

มีเครื่องมือจำนวนมากในท้องตลาดที่ช่วยให้คุณระบุได้ว่าจุดไหนที่มีความอ่อนแอในระบบเครือข่าย scanner เหล่านี้สามารถดูได้ว่าระบบทำการ update แล้วหรือไม่ ระบุได้ว่ามีพอร์ตอะไรบ้างที่เปิดอยู่ซึ่งอาจถูกบุกรุกได้ และข้อมูลอื่นๆขึ้นอยู่กับชนิดของ scanner ที่ใช้

ผลิตภัณฑ์อย่างเช่น Retina (http://www.eeye.com/html/Products/Retina/index.html) และยี่ห้ออื่นๆสามารถระบุและแก้ไขปัญหาความอ่อนแอเหล่านี้ได้ การแก้ปัญหาเหล่านี้สามารทำได้โดยเพียงแค่ติดตั้ง Service Packs, hotfixes ที่ออกมาใหม่อย่างสม่ำเสมอและทำการ disable บริการและพอร์ตที่ไม่จำเป็น

หมายเหตุที่ควรระวัง: คุณต้องได้รับการอนุญาตจากระดับ senior management ของบริษัทก่อนที่จะใช้งานเครื่องมือเหล่านี้ (password crackers และ vulnerability scanners) เพราะเคยมีผู้ดูแลระบบที่มีปัญหากับเรื่องนี้เนื่องจากทำไปโดยยังไม่ได้รับอนุญาตมาแล้ว

UNIX:

ไม่เพียงแต่จะมีครื่องมือสำหรับแกะรหัสผ่านสำหรับระบบ NT เท่านั้น ยังมีเครื่องมือคล้ายๆกันสำหรับระบบ UNIX ด้วยเช่นกัน เครื่องมือ 2 ชนิดที่เป็นที่รู้จักกันดีสำหรับแกะรหัสผ่านในระบบ UNIX คือ Crack และ John the Ripper (หรือเรียกสั้นๆว่า "John") ทำงานโดยการตรวจดูไฟล์รหัสผ่าน (password file) บน UNIX และพยายามเดาอย่างมีหลักการโดยเน้นรหัสผ่านที่มักจะใช้กัน เครื่องมือที่มีขนาดเล็กและใช้ง่ายเหล่านี้สามารถใช้กฎ (rule) ต่างๆมากกว่า 2400 กฎประกอบเข้ากับคำศัพท์ต่างๆใน dicionary เพื่อเดารหัสผ่าน [5] อย่างไรก็ตาม มีหลายวิธีที่คุณสามารถป้องกันระบบ UNIX จากภัยชนิดนี้ เช่น

- บังคับใช้รหัสผ่านที่แข็งแรงโดยการใช้เครื่องมือเช่น passwd+
- รักษากฎหรือนโยบายเกี่ยวกับรหัสผ่านให้เคร่งครัด (เช่น การหมดอายุของรหัสผ่าน เป็นต้น)
- ใช้ไฟล์ shadow ซึ่งเป็นการเก็บรหัสผ่านที่เข้ารหัสไว้ในไฟล์ที่แยกจากไฟล์รหัสผ่านที่เป็น default อยู่แล้ว (/etc/passwd)

ขั้นตอนอื่นๆนอกเหนือจากการทำให้ระบบความปลอดภัยของทั้ง UNIX และ NT มีความแข็งแรงขึ้นแล้วยังมีการกำจัดพอร์ตของ IP service ด้วย ยกตัวอย่างเช่น ถ้าคุณไม่ได้ใช้โปรแกรมใดๆเกี่ยวกับอีเมล์บนระบบ UNIX เลย คุณก็ต้องตรวจสอบให้แน่ใจว่าไม่ได้เปิดพอร์ตหมายเลข 25 ไว้ คุณสามารถตรวจสอบว่าพอร์ตใดบ้างในระบบ (UNIX และ/หรือ NT)ที่ถูกเปิดอยู่โดยใช้ port scanner utility

Desktops:

เมื่อต้องการป้องกันการบุกรุก desktops ของคุณ หลักสำคัญที่จะต้องมุ่งเน้นคือการตั้งค่าให้ระบบปิดการแชร์ไฟล์และเครื่องพิมพ์ (file and print sharing) การทำ disable เหล่านี้ เป็นการป้องกัน desktops ของคุณจากการ broadcast ซึ่งเป็นการเปิดเผยให้ผู้อื่นรู้ว่าระบบของคุณมีตัวตนและใช้งานอยู่ซึ่งอาจทำให้ถูกโจมตีได้ง่าย เช่นเดียวกันกับระบบอื่นๆที่จำเป็นต้องมีการติดตั้งและปรับปรุง service packs, hotfixes, และระบบความปลอดภัยอื่นๆให้ทันสมัยอยู่เสมอ และคุณจะทุ่นเวลาได้มากถ้าหากติดตั้งและคอยดูแลซอฟต์แวร์ป้องกันไวรัสให้ทันสมัยอยู่เสมอ ระบบป้องกันไวรัสในท้องตลาดมีมากมายเช่น Trend - www.trendmicro.com ซึ่งมีสำหรับทั้ง desktops, servers และ ระบบอีเมล์

4. สร้างเครือข่ายที่ง่ายไม่ซับซ้อน

ตามหลักการแล้ว ระบบเครือข่ายที่ไม่มีความซับซ้อนจะสามารถจัดการและทำการรักษาความปลอดภัยได้ง่ายกว่าเครือข่ายที่ยุ่งยากซับซ้อน มีตัวอย่างบริษัทหนึ่งที่เชื่อมต่ออินเทอร์เน็ตโดยผ่านไฟล์วอลล์ที่แตกต่างกันถึง 3 ชนิด (Border Manager, Guantlet, และ PIX) ถึงแม้ว่าจะมีบางคนพยายามอ้างว่าการใช้ไฟล์วอลล์ทั้ง 3 ตัวร่วมกันสามารถทำ

ให้ระบบความปลอดภัยมีความเข้มแข็งขึ้น แต่จริงๆแล้วกลับกลายเป็นการรวมความอ่อนแอของระบบเหล่านี้เข้าด้วยกัน เพราะว่าแฮกเกอร์สามารถทำการโจมตีที่จุดที่อ่อนแอที่สุดหรือที่ไหนก็ตามที่ง่ายต่อการบุกรุกเข้าไป

บางคนคิดว่าการสร้างเครือข่ายให้มีความซับซ้อนจะช่วยให้แฮกเกอร์สับสนยุ่งยากในการบุกเข้ามา หรือบางคนก็อ้างว่าบริษัทของตัวเองไม่ได้ใหญ่โตอะไรคงไม่มีแฮกเกอร์คนไหนสนใจมาเจาะเข้าสู่ระบบอย่างแน่นอน แต่จริงๆแล้วไม่ว่าคุณจะกำลังเชื่อมต่อกับอินเทอร์เน็ตหรือไม่ก็ตาม คุณก็จะถูก probe อยู่ตลอดเวลา Bruce Schneier กล่าวไว้โดยสรุปไว้ว่า " ความซับซ้อนเป็นศัตรูที่ร้ายที่สุดของความปลอดภัย" [6] ดังนั้นยิ่งถ้าเครือข่ายของคุณถูกออกแบบให้ง่ายเท่าไหร่ คุณก็จะเข้าใจ และสามารถจัดการ รวมทั้งป้องกันมันได้ดีเท่านั้น

5. ศึกษาความรู้เรื่องความปลอดภัยอย่างต่อเนื่อง

เรื่องของการรักษาความปลอดภัยเป็นหัวข้อที่ใหญ่และครอบคลุมถึงสาขาอื่นอีกหลายสาขาจึงเป็นไปไม่ได้ที่คนๆเดียวจะรู้ทุกอย่าง อย่างไรก็ตามคุณควรจะศึกษาและทำความเข้าใจในภัยคุกคามต่างๆ ช่องโหว่ต่างๆ และวิธีแก้ไขปัญหาสำหรับระบบความปลอดภัยของเครือข่ายอย่างต่อเนื่อง

สรุป:

ดังนั้นคุณก็สามารถเริ่มต้นการรักษาความปลอดภัยระบบเครือข่ายของคุณได้แล้วด้วยขั้นตอน 5 ขั้นตอนดังนี้

1. ปกป้องทรัพย์สินที่มีค่าที่สุดของคุณเป็นสิ่งแรก
2. ปกป้องที่บริเวณรอบๆ
3. การป้องกันระบบภายในที่สำคัญ
4. สร้างเครือข่ายที่ง่ายไม่ซับซ้อน
5. ศึกษาความรู้เรื่องความปลอดภัยอย่างต่อเนื่อง

ขั้นตอนเหล่านี้สามารถใช้เป็นจุดเริ่มต้นสำหรับการรักษาความปลอดภัยระบบเครือข่ายได้เป็นอย่างดี ขณะที่คุณทำตามขั้นตอนเหล่านี้ซึ่งเน้นที่การปรับปรุงระบบเครือข่าย ก็เป็นการแนะนำให้คุณได้เรียนรู้และเข้าใจเรื่องของความปลอดภัยเพิ่มขึ้นด้วย

ถ้าหากมีผู้เชี่ยวชาญด้านความปลอดภัยอยู่ในองค์กร คุณควรจะปรึกษาผู้เชี่ยวชาญด้วย คุณควรจะแน่ใจว่าบริษัทที่เข้ามาดูแลระบบความปลอดภัยให้แก่บริษัทคุณมีชื่อเสียงที่น่าเชื่อถือได้ด้วย โดยพวกเขาจะต้องใช้เวลาในการทำความเข้าใจภาพรวมขององค์กรของคุณ การตั้งค่าระบบเครือข่าย และกระบวนการต่างๆที่ใช้งานอยู่ก่อนที่พวกเขาจะติดตั้งเครื่องมือใดๆบนเครือข่ายของคุณ

การทำความเข้าใจระบบความปลอดภัยและสร้างโครงสร้างของเครือข่ายที่ปลอดภัยสามารถสร้างความน่าเกรงขามได้ ถ้าคุณใช้เวลาทำความเข้าใจระบบเครือข่ายของคุณ แก้ไขปัญหาของจุดที่สำคัญและระบบหลักของคุณ แล้วเปลี่ยนแปลง

กระบวนการของคุณเพื่อรวมเอาการรักษาความปลอดภัยเข้ามาในทุกๆ phase ของโครงการ ก็จะเป็นการก้าวไปอย่างดีเพื่อสร้างระบบแวดล้อมเครือข่ายที่มีความปลอดภัยและแข็งแกร่งด้วย

Appendix:

Hyperlinks to tools mentioned:

Zone Alarm (personal firewall)– http://www.zonelabs.com

SNORT (IDS) – http://www.snort.org

QChain (Microsoft hotfix installer) –
http://support.microsoft.com/support/kb/articles/Q296/8/61.asp

Windows NT 4.0 Member Server Configuration Checklist -
http://www.microsoft.com/technet/security/mbrsrvcl.asp

HFNetChk (Microsoft security assessment tool)-
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/itsolutions/security/tools/hfnetchk.asp

LC3 (password-cracking tool for NT)- http://www.atstake.com/lc3

Retina (vulnerability scanner)- http://www.eeye.com/html/Products/Retina/index.html

Crack (password-cracking tool for UNIX) –
ftp://ftp.cerias.purdue.edu/pub/tools/unix/pwdutils/crack

John the Ripper (password-cracking tool for UNIX) – http://www.openwall.com/john

Trend (virus protection software) – http://www.trendmicro.com/

Bibliography:

1. "Underlying Technical Models for Information Technology Security". 15 May 2001. URL: http://csrc.nist.gov/publications/drafts/UnderlyingModels-ITSecv0.2.doc (29 June 2001): 4-5
2. Schneier, Bruce. Secrets and Lies. New York: John Wiley and Sons, Inc., 2000. 190
3. Bace, Rebecca and Mell, Peter. "Intrusion Detection Systems". August 2001. URL: http://csrc.nist.gov/publications/nistpubs/800-31/sp800-31.pdf (21 August 2001): 16-20
4. Cox, Philip. "Hardening Windows 2000". 25 May 2001. URL: http://www.securityfocus.com/data/library/hardenW2K12.pdf (27 June 2001): 18
5. Scambray, Joel. Hacking Exposed, Second Edition. Berkeley: McGraw-Hill, 2001: 341
6. Schneier, Bruce. Secrets and Lies. New York: John Wiley and Sons, Inc., 2