การป้องกันไวรัสสำหรับระบบเครือข่าย

กำหนดมาตรการป้องกันไวรัสที่มีประสิทธิภาพสำหรับเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่ายที่เชื่อมต่อกับระบบเครือข่ายทุกเครื่อง เช่น การติดตั้งซอฟต์แวร์ป้องกันไวรัส เป็นต้น การปกป้องระบบเครือข่าย สิ่งที่สำคัญอย่างยิ่ง คือ ผู้ใช้งานในระบบจะต้องคอยดูแล และป้องกันไม่ให้ตนเองเป็นช่องทางผ่านของ Hacker ผู้ดูแลระบบจะต้องคอยติดตามและหาวิธีการป้องกัน และแก้ไขจุดบกพร่องของซอฟต์แวร์ที่ใช้งาน เพราะไม่มีระบบเครือข่ายใดที่ปลอดภัยสมบูรณ์แบบ ดังนั้นจึงต้องมีระบบป้องกันที่ดีโดยมีวิธีการ ดังนี้

- ติดตั้งโปรแกรมป้องกันไวรัสและอัพเดตข้อมูลไวรัสอยู่เสมอ
    - ติดตั้งโปรแกรมป้องกันไวรัสที่เหมาะสม
    - สร้างแผ่น Emergency Disk เพื่อใช้ในการกู้ระบบ
    - อัพเดตข้อมูลไวรัสของโปรแกรมทุกครั้งที่เครื่องเตือนให้อัพเดต
    - เปิดใช้งาน Auto Protect
    - ตรวจสอบหาไวรัสทุกครั้งก่อนเปิดไฟล์จากแผ่นหรือบันทึกข้อมูลต่างๆ
    - ใช้โปรแกรมเพื่อทำการตรวจหาไวรัสอย่างน้อยสัปดาห์ละ ๑ ครั้ง
- การป้องกันจากการเปิดไฟล์จากสื่อบันทึกข้อมูล (Media) ต่างๆ - การป้องกันจากการดาวน์โหลดจาก Internet
    - แผ่น CD , เทปต่างๆ • ไม่ควรเปิดไฟล์ที่แนบมากับโปรแกรมสนทนาต่างๆ เช่น MSN
    - สแกนหาไวรัสจากสื่อบันทึกข้อมูลก่อนใช้งานทุกครั้ง • ไม่ควรเข้า Website ที่มากับ E-Mail
    - ไม่ควรเปิดไฟล์ที่มีนามสกุลแปลกๆ ที่น่าสงสัย เช่น .pif เป็นต้น • ไม่ดาวน์โหลดไฟล์จาก Website ที่ไม่มั่นใจหรือไม่น่าเชื่อถือ
    - ไม่ใช้สื่อบันทึกที่ไม่ทราบแหล่งที่มา • ติดตามข้อมูลการแจ้งเตือนจากแหล่งข้อมูลด้านความปลอดภัยเสมอ
    - หลีกเลี่ยงการแชร์ไฟล์โดยไม่จำเป็น
- การป้องกันจากการเปิด E-Mail • หลีกเลี่ยงการแชร์ไฟล์ประเภท Peer to Peer เนื่องจากมีโอกาสติดไวรัสสูง
    - อย่าเปิดไฟล์ E-Mail จากผู้ส่งที่ไม่รู้จัก และไม่ทราบที่มา
    - อย่าเปิดอ่าน E-Mail ที่มีหัวเรื่องเป็นข้อความไม่ปกติ
    - ลบ E-Mail ที่ไม่ทราบแหล่งที่มาทิ้งทันที
    - อัพเดตโปรแกรม E-Mail สม่ำเสมอ

ความเสี่ยงด้านระบบเครือข่าย

หมายถึง ความเสี่ยงหรือภัยต่างๆที่เกิดขึ้นกับระบบเครือข่ายของ องค์กร ทั้งระบบอินทราเน็ต (Intranet) และอินเทอร์เน็ต (Internet) ซึ่งรวมถึงภัยที่มีสาเหตุมาจากปัญหาพื้นฐานของโพรโตคอล (Protocol) TCP/IP ด้วย เช่น ความเสี่ยงด้านกายภาพ ความเสี่ยงด้านระบบปฏิบัติการความเสี่ยงระบบแม่ข่าย ความเสี่ยงจากการบุกรุกระบบเครือข่าย และความเสี่ยงจากภัยคุกคามต่างๆ

การบริหารจัดการความเสี่ยงด้านระบบเครือข่าย มีประเด็นหลัก ดังนี้

๑. ความเสียหายที่เกิดจากระบบเครือข่าย การเฝ้าระวังและตรวจสอบระบบเครือข่าย และการจัดทำระบบการกำหนดสิทธิในการเข้าถึงระบบเครือข่ายได้การดำเนินการควรจัดให้มีระบบการติดตามและเฝ้าดูการใช้เครือข่ายภายในและการเข้าออก Internet ทุกวัน รวมทั้งการสร้าง Firewall เพื่อป้องกันการเข้าถึงและการโจมตีจากภายนอกให้ทุกเครื่องคอมพิวเตอร์ลูกข่าย (Client) ในเครือข่ายระบบฐานข้อมูล ,ระบบ Web Server เป็นต้น

๒. พัฒนาระบบงานด้านเครือข่าย โดยการพัฒนา บริหาร ควบคุม กำกับดูแล และบำรุงรักษาระบบคอมพิวเตอร์ และเครือข่ายสารสนเทศพื้นฐาน พัฒนาระบบการให้บริการเครือข่ายร่วมกับหน่วยงานอื่นๆ ที่เกี่ยวข้อง การเพิ่มการรักษาและคุ้มครองความปลอดภัยข้อมูลผ่านระบบเครือข่าย

๓. เพิ่มประสิทธิภาพในการให้บริการระบบเครือข่ายคอมพิวเตอร์ ให้มีความเสถียรและมีประสิทธิภาพรองรับกับปริมาณฐานข้อมูล และการเคลื่อนไหวของฐานข้อมูล

๔. หน่วยงานภายในกองพิสูจน์หลักฐานกลาง และผู้มีความรู้ต้องร่วมวิเคราะห์ ออกแบบ วางแผน การจัดการระบบโครงข่ายร่วมกันอย่างบูรณาการ และมีการให้คำปรึกษา แนะนำและแก้ไขปัญหาในการพัฒนาเครือข่าย

๕. มีแผนการรักษาความปลอดภัยของระบบเครือข่าย (Network Security) มีวัตถุประสงค์เพื่อควบคุมบุคคลที่ไม่เกี่ยวข้องไม่ให้เข้าถึง ล่วงรู้(access risk) หรือแก้ไขเปลี่ยนแปลง (integrity risk) ข้อมูล หรือ การท างานของระบบเครือข่ายที่จะมีผลถึงระบบคอมพิวเตอร์ในส่วนที่มิได้มีอำนาจหน้าที่เกี่ยวข้อง การป้องกันการบุกรุกผ่านระบบเครือข่าย มีวัตถุประสงค์เพื่อป้องกันบุคคล ไวรัส มิให้เข้าถึงหรือสร้างความเสียหาย (availability risk) แก่ข้อมูลหรือการท างานของระบบคอมพิวเตอร์ โดยมีเนื้อหารายละเอียดเกี่ยวกับแนว ทางในการรักษาความปลอดภัยข้อมูล ระบบคอมพิวเตอร์ เครื่องแม่ข่ายและระบบเครือข่าย

(๑) การบริหารจัดการข้อมูลบนเครือข่าย

- กำหนดชั้นความสำคัญในการเข้าถึงข้อมูลแต่ละประเภท ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงการเข้าถึงข้อมูลผ่านระบบเครือข่าย
- ในการรับส่งข้อมูลผ่านเครือข่ายสาธารณะต้องได้รับการเข้ารหัสที่เป็นมาตรฐานสากล
- กำหนดมาตรการรักษาความปลอดภัยข้อมูล เช่น กรณีนำเครื่องคอมพิวเตอร์ส่งซ่อม

(๒) การควบคุมการกำหนดสิทธิให้แก่ผู้ใช้งาน (user privilege)

- กำหนดสิทธิการเข้าถึงข้อมูลและระบบคอมพิวเตอร์ เช่น สิทธิการใช้โปรแกรมระบบงานคอมพิวเตอร์ (application system)ให้แก่ผู้ใช้งานให้เหมาะสมกับหน้าที่และความรับผิดชอบ

- กำหนดระยะเวลาการใช้งานของ user พร้อม password และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

- กำหนดให้มีการเปลี่ยนรหัสผ่านอย่างรอบคอบ และมีชั้นความลับ

- ในกรณีที่มีความจำเป็นต้องให้สิทธิบุคคลอื่นให้มีสิทธิใช้งานระบบคอมพิวเตอร์ เช่น การทดสอบระบบของเจ้าหน้าที่ภายนอกต่างๆ ต้องมีการขออนุมัติจากผู้มีอำนาจ หน้าที่ทุกครั้ง โดยบันทึกเหตุผลและความจำเป็นรวมถึงกำหนดระยะเวลาในการใช้งาน

(๓) ควบคุมการใช้งานบัญชีรายชื่อผู้ใช้งาน (user account) และรหัสผ่าน (password)

- กำหนดให้รหัสผ่านมีความยาวตามมาตรฐานสากลโดยทั่วไปไม่ต่ำกว่า ๖ ตัวอักษร

- ควรใช้อักขระพิเศษประกอบ เช่น @ ; < > เป็นต้น

- สำหรับผู้ใช้งานทั่วไปจะมีการเปลี่ยนรหัสผ่านอย่างน้อยทุกๆ ๖ เดือน ส่วนผู้ดูแลระบบควรเปลี่ยนรหัสผ่านอย่างน้อยทุกๆ ๓ เดือน

- ในการเปลี่ยนรหัสผ่านแต่ละครั้งไม่ควรกำหนดรหัสผ่านใหม่ให้ซ้ำของเดิมครั้งสุดท้าย

- กำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิดได้ไม่เกิน ๓ ครั้ง

- ผู้ใช้งานจะต้องเก็บรหัสผ่านไว้เป็นความลับ ทั้งนี้ในกรณีที่มีการล่วงรู้รหัสผ่าน โดยบุคคลอื่นผู้ใช้งานจะต้องเปลี่ยนรหัสผ่านใหม่โดยทันที

๖. การบริหารจัดการและการตรวจสอบระบบเครือข่าย (Network)

(๑) กำหนดแบ่งแยกระบบเครือข่ายให้เป็นสัดส่วนตามการใช้งาน เช่น ส่วนเครือข่ายภายในกองพิสูจน์หลักฐานกลางและ หน่วยในสังกัดกองพิสูจน์หลักฐานกลาง

(๒) ติดตั้งระบบป้องกันการบุกรุก เช่น Firewall ระหว่างเครือข่ายภายในกับเครือข่ายภายนอกโดยการติดตั้งผ่านอุปกรณ์คอมพิวเตอร์ ติดตั้งระบบป้องกันการบุกรุกในระบบเครือข่ายด้วยซอฟต์แวร์และฮาร์ดแวร์ให้แก่ ระบบ Firewall ซึ่งเป็นซอฟต์แวร์ทำหน้าที่เสมือนกับกำแพงกันไฟไม่ให้ลุกลามขยายตัวหากมีไฟไหม้เกิดขึ้น Firewall จะอาศัยคอมพิวเตอร์เครื่องหนึ่งเป็นด่านเข้าออกเครือข่ายและเป็นเสมือนกำแพงกันไฟ และมีซอฟต์แวร์ที่ผู้ดูแลระบบจะติดตั้งและกำหนดรูปแบบการอนุญาตให้เข้าใช้เครือข่ายอินเทอร์เน็ต

(๓) จัดทำแผนผังระบบเครือข่าย / แผนผังการเชื่อมโยงระบบเครือข่าย (network diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายทั้งภายในและภายนอกรวมทั้ง อุปกรณ์เครื่อข่ายอื่น ๆ ให้เป็นปัจจุบันอยู่เสมอ

(๔) ตรวจสอบความปลอดภัยของอุปกรณ์คอมพิวเตอร์ก่อนเชื่อมต่อกับระบบเครือข่าย เช่นตรวจสอบไวรัส เป็นต้น

(๕) กำหนดบุคคลผู้รับผิดชอบในการกำหนดแก้ไขหรือเปลี่ยนแปลงค่า parameter ต่างๆของอุปกรณ์เครือข่าย

(๖) ข้อควรปฏิบัติในการใช้ระบบ LAN ไร้สายให้ปลอดภัยจากแฮกเกอร์

๑. วาง Access Point (AP) ในตำแหน่งที่เหมาะสมไม่ควรวาง AP ไว้ในระบบ LAN ภายในควรวาง AP บริเวณหน้า Firewall จะปลอดภัยกว่า แต่ถ้าจำเป็นจริงๆ ต้องวางภายใน LAN ที่เป็น Internal Network ก็ควรจะมีการเพิ่มการ Authentication, Encryption เข้าไปช่วยในการควบคุมด้วย

๒. กำหนดรายการ MAC Address ที่สามารถเข้าใช้ AP ได้เฉพาะที่เราอนุญาตเท่านั้น การ Lock ด้วยวิธีกำหนดค่า MAC Address นั้น แม้ว่าจะไม่ใช้วิธีที่กัน Hacker ได้ ๑๐๐% ก็ตาม เพราะ Hacker สามารถ Spoof ปลอม MAC Address ได้ แต่ก็ยังดีกว่าไม่มีการกำหนดเสียเลย เหมือนกับว่าเราควรมีการป้องกันหลายๆ วิธี การกำหนด MAC Address ให้เฉพาะเครื่องที่เราอนุญาตก็เป็นการกันในชั้นหนึ่ง เพื่อให้ Hacker เกิดความยากล าบากในการ Hack เข้าสู่ระบบ Wireless LAN ของเรา

๓. จัดการกับ SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่า Default มาจากโรงงานผลิตค่า SSID จะถูกกำหนดเป็นค่า Default มาจาก Vendor เช่น Cisco Aironet กำหนดเป็นชื่อ tsunami เป็นต้น เราควรทำการเปลี่ยนค่า SSID ที่เป็นค่า Default ทันทีที่เรานำ AP มาใช้งาน และ ควรปิดคุณสมบัติการ Auto Broadcast SSID ของตัว AP ด้วย

๔. ใช้ WEP (Wired Equivalent Privacy) security protocol ในการเข้ารหัสข้อมูลระหว่าง IEEE ๘๐๒.๑๑b Wireless LAN Client และ Access Point (AP) มาตรฐาน WEP เป็นมาตรฐานหลักที่มีใน AP ทุกตัว แต่โดยปกติแล้วจะไม่ได้เปิดใช้ ทำให้แฮกเกอร์สามารถใช้โปรแกรม Packet Sniffer เช่น Ethereal (www.ethereal.com) ดักจับ Packet และสามารถอ่านข้อมูลที่เป็น Plain text ได้เพราะ AP มีลักษณะการท างานแบบ HUB ไม่ใช่ Switching เหมือนที่เราใช้กันใน LAN ทุกวันนี้ เราจึงควรมีการเข้ารหัส Packet ของเราในระดับ Layer ๒ เพื่อให้ยากต่อการจับด้วยโปรแกรมประเภทนี้ ถ้าเราเพิ่มการ generate WEP Key เป็นแบบ Dynamic จะช่วยให้ปลอดภัยมากยิ่งขึ้น รวมถึงการใช้งานแบบ Session-Based และ User-Based WEP Key ก็ช่วยได้เช่นกัน

๕. อย่าหวังพึ่ง WEP อย่างเดียว เพราะ WEP สามารถที่จะถูก Crack ได้ การเพิ่ม WEP เข้ามาในการใช้งาน Wireless LAN เป็นสิ่งที่ควรทำแต่ WEP ก็ไม่สามารถกันพวกแฮกเกอร์ได้ ๑๐๐% เพราะมีโปรแกรมที่สามารถถอดรหัส WEP ได้ ถ้าได้ IP Packet จำนวนมากพอ เช่น โปรแกรม AirSnort จากhttp://www.shmoo.com เป็นต้น เพราะ ฉะนั้นเราควรเพิ่มการป้องกันใน Layer อื่นๆ เข้าไปด้วย

๖. ใช้VPN ร่วมกับการใช้งาน Wireless LAN การใช้VPN ระหว่าง Wireless LAN Client กับ AP ต่อเชื่อมไปยัง VPN Server เป็นวิธีที่ปลอดภัยมากกว่าการใช้ WEP และ การ Lock MAC Address การใช้ VPN ถือได้ว่าเป็นการป้องกันที่ลึกอีกขั้นหนึ่ง และ เป็นการรักษาความปลอดภัยในลักษณะ end to end อีกด้วย

๗. เพิ่มการ Authentication โดยใช้ RADIUS หรือ TACACS Server ถ้าองค์กรมี RADIUS Server หรือ CISCO Secure ACS (TACACS) Server อยู่แล้ว สามารถนำมาใช้ร่วมกับ AP ที่มีความสามารถในการตรวจสอบ Username และ Password ก่อนที่ผู้ใช้จะเข้าสู่ระบบ (Authentication Process) และ ทำให้ผู้ใช้ไม่ต้องจำหลาย Username หลาย Password ผู้ใช้สามารถใช้ Username และ Password เดียวกับที่ใช้ในระบบ Internal LAN ได้เลย ทำให้สะดวกในการบริหารจัดการ Account ภายใน และ IT Auditor ควร ตรวจสอบการเข้าระบบ Wired และ Wireless LAN จาก Log ของระบบด้วย

๘. การใช้ Single Sign On (SSO) ดังที่กล่าวมาแล้วในข้อ ๗ ควรกำหนดเป็น Security Policy ให้กับองค์กรสำหรับระบบ Wired และ Wireless LAN เพื่อที่เราสามารถที่จะกำหนดคุณสมบัติ AAA ได้แก่ Authentication, Authorization และ Accounting ได้ การใช้งานควรกำหนด Security Policy ทั้งระบบ Wired และ Wireless LAN ไปพร้อมๆ กัน และ แจ้งให้ผู้ใช้ได้ทราบปฏิบัติตาม Security Policy และสามารถตรวจสอบได้

๙. อุปกรณ์ Wireless LAN จากแต่ละผู้ผลิตอาจมีคุณสมบัติแตกต่างจากมาตรฐานและมีปัญหาในการท างานร่วมกันแม้ว่าผู้ผลิตอุปกรณ์จะผลิตตามมาตรฐาน IEEE ๘๐๒.๑๑b ผู้ผลิตบางรายมักจะเพิ่มคุณสมบัติบางอย่างเฉพาะผู้ผลิตรายนั้นๆ เช่น เพิ่มคุณสมบัติทางด้าน security ของอุปกรณ์เป็นต้น เราควรตรวจสอบให้ดีก่อนที่จะตัดสินใจซื้อมาใช้งานจริงว่าอุปกรณ์ไม่มีปัญหาในการท างานร่วมกัน

๑๐. ระวัง Rouge AP แม้ว่าจะไม่ได้ใช้ระบบ Wireless LAN เลยก็ตาม การ Hack จากภายในองค์กรในสมัยนี้ทำได้ง่าย แม้องค์กรจะไม่ได้ใช้ระบบ Wireless LAN เลย วิธีการก็คือ มีผู้ไม่หวังดีทำการแอบติดตั้ง AP ที่ไม่ได้รับอนุญาตเข้ากับระบบ Internal LAN เรียกว่า Rouge AP จากนั้นผู้ไม่หวังดีก็สามารถ Access Internal LAN ผ่านทาง Rouge AP ที่ทำการแอบติดตั้งไว้ ซึ่งเขาสามารถเข้าถึงระบบภายในได้ จากภายนอกอาคาร หรือ จากที่จอดรถของหน่วยงานก็ได้ ถ้าระยะห่างไม่เกิน ๑๐๐ เมตร จาก AP ที่แอบติดตั้งไว้ เราควรมีการตรวจสอบ Rouge AP เป็นระยะๆ โดยใช้โปรแกรม Networkstumbler (http://www.netstumbler.com) เพื่อหาตำแหน่งของ Rouge AP

หรือ เราควรติดตั้ง IDS (Intrusion Detection System) เช่น SNORT (http://www.snort.org) เพื่อคอยตรวจสอบพฤติกรรมแปลกๆ ในระบบ Internal LAN ภายในของเรา เป็นระยะๆ จะทำให้ระบบของเรามีความปลอดภัยมากขึ้น และ มีการเตือนภัยในลักษณะ Proactive ด้วย