



บทที่ 8 : การป้องกันไวรัส Part4

สธ412 ความมั่นคงของระบบสารสนเทศ

อาจารย์อภิพงศ์ ปิงยศ

apipong.ping@gmail.com

Outline

- ▶ การป้องกันไวรัส
 - ▶ การป้องกันไวรัสที่ไคลเอนต์
 - ▶ การติดตั้งแอปพลิเคชัน
 - ▶ การป้องกันไวรัสที่เซิร์ฟเวอร์ (Part4)
 - ▶ การป้องกันไวรัสในระดับเครือข่าย (Part4)
 - ▶ การป้องกันทางกายภาพ (Part4)



การป้องกันไวรัสที่เซิร์ฟเวอร์

- ▶ จุดประสงค์หลักคือ**การปกป้องระบบให้สามารถทำงานได้เป็นปกติ**
- ▶ กระบวนการทำให้เซิร์ฟเวอร์มีความปลอดภัยสูงขึ้นจะเรียกว่า Hardening ซึ่งก็จะคล้ายกับการป้องกันไวรัสที่เครื่องไคลเอนต์ ประกอบไปด้วย
 - ▶ ลดช่องทางการถูกโจมตี
 - ▶ อัปเดตแพตช์
 - ▶ ติดตั้งโฮสต์เบสไฟร์วอลล์
 - ▶ สแกนหาช่องโหว่

การป้องกันไวรัสที่เซิร์ฟเวอร์ [2]

ประเด็นที่ควรพิจารณาเมื่อต้องเลือกซอฟต์แวร์ป้องกันไวรัสสำหรับเซิร์ฟเวอร์ ประกอบด้วย

- ▶ **CPU Utilization** ประสิทธิภาพและโหลดของ CPU
- ▶ **Application Reliability** ต้องไม่ส่งผลกระทบต่อการใช้งานบริการ
- ▶ **Management Overhead** ต้องจัดการได้โดยอัตโนมัติ
- ▶ **Application Interoperability** ควรตรวจสอบก่อนว่าซอฟต์แวร์ป้องกันไวรัสสามารถใช้งานร่วมกับโปรแกรมที่ใช้ได้อยู่ได้

การป้องกันไวรัสที่เซิร์ฟเวอร์ [3]

- ▶ **Web Server** เป็นเป้าหมายที่นิยมถูกโจมตี ควรใช้ซอฟต์แวร์เฉพาะทางในการป้องกัน และต้องอาศัยการคอนฟิกเพื่อปิดพอร์ตต่างๆที่อาจเป็นอันตราย ส่วนใหญ่จะใช้ CentOS เป็น Web Server OS
- ▶ **Mail Server** ต้องป้องกัน 2 อย่าง คือปกป้องเซิร์ฟเวอร์จากมัลแวร์และหยุดยั้งไม่ให้มัลแวร์ถูกส่งไปยังเมลบ็อกซ์ของผู้ใช้ ดังนั้นซอฟต์แวร์ป้องกันไวรัสต้องสามารถทำหน้าที่สองอย่างนี้ได้ ในม.แม่โจ้จะใช้ Microsoft Exchange Server เป็น Mail Server



การป้องกันไวรัสที่เซิร์ฟเวอร์ [4]



- ▶ **Database Server** จะต้องปกป้อง 4 ส่วนหลักคือ Host, Database Service, Data Storage, Data Communication ในวงการ Admin ส่วนใหญ่จะใช้ Redhat เป็น DB Server OS
- ▶ **File Server** เป็นเซิร์ฟเวอร์ที่มีจุดอ่อนค่อนข้างมากเพราะผู้ใช้งานมีการถ่ายโอนไฟล์ระหว่างเซิร์ฟเวอร์อยู่ตลอดเวลา ควรมีนโยบายให้ผู้ใช้ทำการสแกนไฟล์ก่อนรับ-ส่งเสมอ ในวงการ Admin ส่วนใหญ่จะใช้ Ubuntu เป็น File Server OS



การป้องกันไวรัสในระดับเครือข่าย

- ▶ เป็นการป้องกันที่ยากเพราะส่วนใหญ่จะมีการประณีประนอมระหว่างความต้องการของผู้ใช้และระดับความเสี่ยงที่องค์กรยอมรับได้ การป้องกันจะต้องทำหลายวิธีควบคู่กันไปประกอบไปด้วย
 - ▶ การติดตั้ง NIDS
 - ▶ การกรองข้อมูลในระดับแอปพลิเคชันโดยไฟร์วอลล์
 - ▶ การบล็อกเว็บไซต์ที่อาจเป็นอันตราย
 - ▶ การสร้างเครือข่ายกักกันโดยเฉพาะ (Quarantine Network)

การป้องกันทางกายภาพ

ส่วนที่สำคัญและจำเป็นต้องมีแผนป้องกัน ประกอบไปด้วย

- ▶ สถานที่
- ▶ บุคคล
- ▶ ควบคุมการเข้าถึงเครือข่าย
- ▶ เครื่องเซิร์ฟเวอร์
- ▶ เครื่องไคลเอนต์
- ▶ คอมพิวเตอร์และอุปกรณ์เคลื่อนที่

อาจมีการใช้วิธีการระบุตัวตนเช่น การสแกนนิ้วมือ หรือ Smart Card



นโยบาย ระเบียบปฏิบัติ และข้อควรระวัง

- ▶ การสแกนไวรัสเป็นประจำ เช่น สัปดาห์ละครั้ง เป็นต้น
- ▶ การอัปเดตไวรัสซิกเนเจอร์เป็นประจำ
- ▶ แอปพลิเคชันและเซอร์วิสที่อนุญาตและไม่อนุญาต
- ▶ การควบคุมการเปลี่ยนแปลงค่าคอนฟิก
- ▶ การมอนิเตอร์เครือข่าย
- ▶ แผนปฏิบัติเมื่อถูกโจมตี

นโยบาย ระเบียบปฏิบัติ และข้อควรระวัง [2]

- ▶ นโยบายการเข้าถึงเครือข่ายจากบ้าน
- ▶ นโยบายเข้าถึงเครือข่ายของผู้มาเยี่ยม
- ▶ นโยบายการใช้งานไวร์เลสแลน
- ▶ นโยบายการอัปเดตแพตช์
- ▶ การแยกกำหนดนโยบายตามการจัดระดับความเสี่ยง
- ▶ การฝึกอบรมและอัปเดตความรู้ใหม่ๆ