บทที่ 6 : การป้องกันไวรัส Part3

สธ412 ความมั่นคงของระบบสารสนเทศ

อาจารย์อภิพงศ์ ปิงยศ

apipong.ping@gmail.com

Outline

- การป้องกันไวรัสที่เซิร์ฟเวอร์
- การป้องกันไวรัสในระดับเครือข่าย
- การป้องกันทางกายภาพ

การป้องกันไวรัสที่เซิร์ฟเวอร์

- จุดประสงค์หลักคือ***การปกป้องระบบให้สามารถทำงานได้เป็นปกติ***
- กระบวนการทำให้เซิร์ฟเวอร์มีความปลอดภัยสูงขึ้นจะเรียกว่า Hardening ซึ่งก็จะคล้ายกับการป้องกันไวรัสที่เครื่องไคลเอนต์ ประกอบไปด้วย
  - ลดช่องทางการถูกโจมตี
  - อัพเดตแพตช์
  - ติดตั้งโฮสต์เบสไฟร์วอลล์
  - สแกนหาช่องโหว่

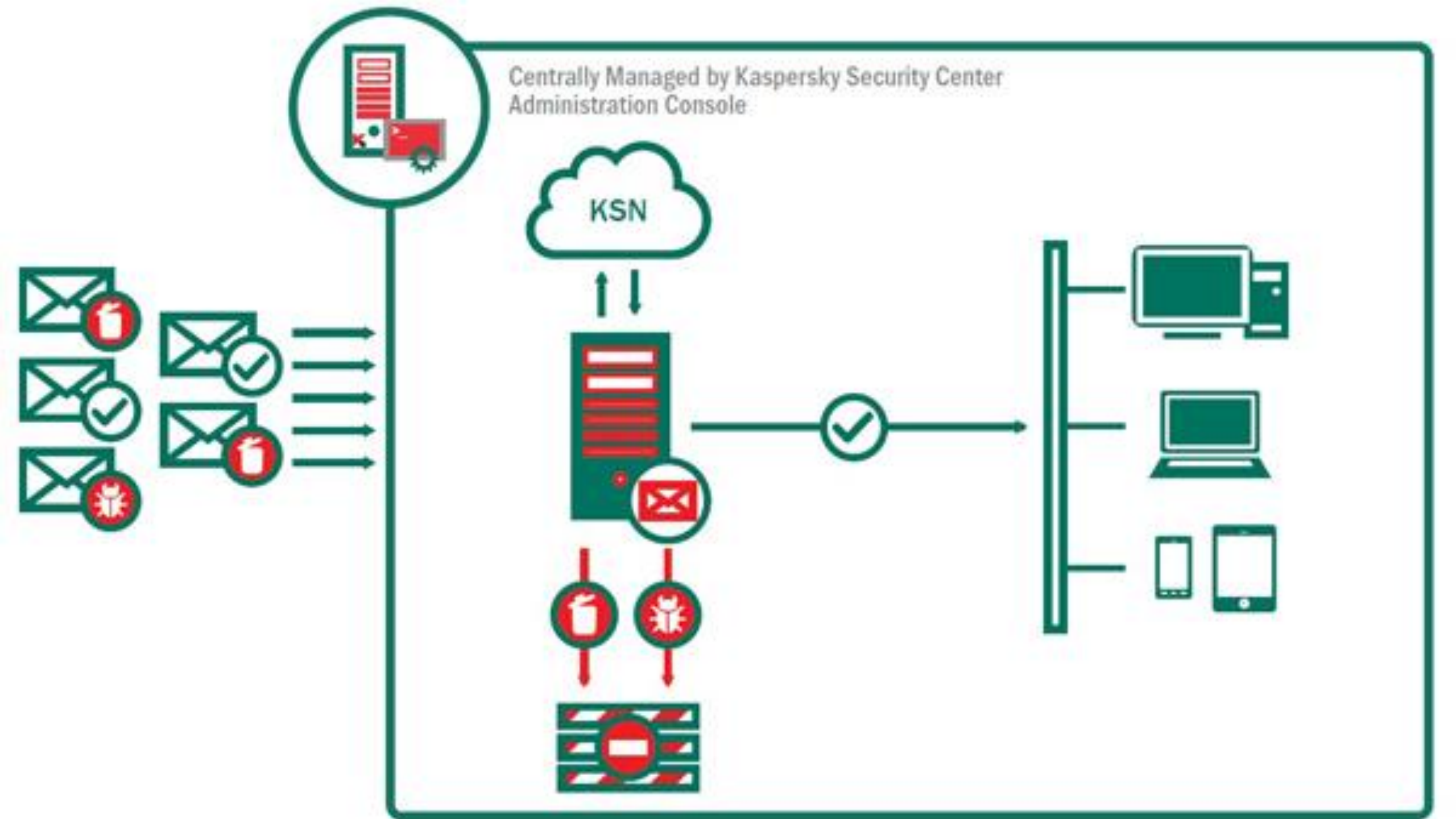
การป้องกันไวรัสที่เซิร์ฟเวอร์ [2]

ประเด็นที่ควรพิจารณาเมื่อต้องเลือกซอฟต์แวร์ป้องกันไวรัสสำหรับเซิร์ฟเวอร์ ประกอบไปด้วย

- CPU Utilization ประสิทธิภาพและโหลดของ CPU
- Application Reliability ต้องไม่ส่งผลต่อการให้บริการ
- Management Overhead ต้องจัดการได้โดยสะดวก
- Application Interoperability ควรตรวจสอบก่อนว่าซอฟต์แวร์ป้องกันไวรัสสามารถใช้งานร่วมกับโปรแกรมที่ใช้อยู่ได้

การป้องกันไวรัสที่เซิร์ฟเวอร์ [3]

- Web Server เป็นเป้าหมายที่นิยมถูกโจมตี ควรใช้ซอฟต์แวร์เฉพาะทางในการป้องกัน และต้องอาศัยการคอนฟิกเพื่อปิดพอร์ตต่างๆที่อาจเป็นอันตราย
- Mail Server ต้องป้องกัน 2 อย่าง คือ 1. ปกป้องเซิร์ฟเวอร์จากมัลแวร์ และ 2. หยุดยั้งไม่ให้มัลแวร์ถูกส่งไปยังเมลบ็อกซ์ของผู้ใช้ได้ ดังนั้นซอฟต์แวร์ป้องกันไวรัสต้องสามารถทำหน้าที่สองอย่างนี้ได้

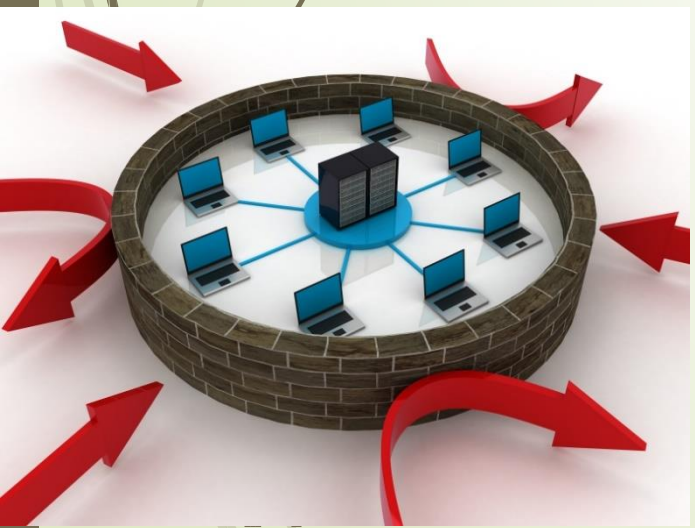

Centrally Managed by Kaspersky Security Center
Administration Console
KSN

การป้องกันไวรัสที่เซิร์ฟเวอร์ [4]

- Database Server จะต้องปกป้อง 4 ส่วนหลักคือ Host, Database Service, Data Storage, Data Communication
- File Server เป็นเซิร์ฟเวอร์ที่มีจุดอ่อนค่อนข้างมากเพราะผู้ใช้มีการถ่ายโอนไฟล์ระหว่างเซิร์ฟเวอร์อยู่ตลอดเวลา ควรมีนโยบายให้ผู้ใช้ทำการสแกนไฟล์ก่อนรับ-ส่งเสมอ

การป้องกันไวรัสในระดับเครือข่าย

- เป็นการป้องกันที่ยากเพราะส่วนใหญ่จะมีการประณีประนอมระหว่างความต้องการของผู้ใช้และระดับความเสี่ยงที่องค์กรยอมรับได้ การป้องกันจะต้องทำหลายวิธีควบคู่กันไป ประกอบไปด้วย
  - การติดตั้ง (Network-based Intrusion Detection System : NIDS)
  - การกรองข้อมูลในระดับแอพพลิเคชั่นโดยไฟร์วอลล์
  - การบล็อกเว็บไซต์ที่อาจเป็นอันตราย
  - การสร้างเครือข่ายกักกันโดยเฉพาะ (Quarantine Network)



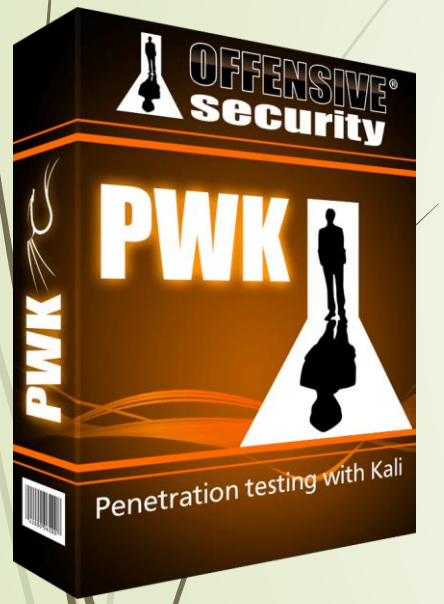
การป้องกันทางกายภาพ

ส่วนที่สำคัญและจำเป็นต้องมีแผนป้องกัน ประกอบไปด้วย

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

อาจมีการใช้วิธีการระบุตัวตนเช่น การสแกนนิ้วมือ หรือ Smart Card

นโยบาย ระเบียบปฏิบัติ และข้อควรระวัง



- การสแกนไวรัสเป็นประจำ เช่น สัปดาห์ละครั้ง เป็นต้น
- การอัพเดตไวรัสซิกเนเจอร์เป็นประจำ
- แอพพลิเคชั่นและเซอร์วิสที่อนุญาตและไม่อนุญาต
- การควบคุมการเปลี่ยนแปลงค่าคอนฟิก
- การมอนิเตอร์เครือข่าย
- แผนปฏิบัติเมื่อถูกโจมตี

นโยบาย ระเบียบปฏิบัติ และข้อควรระวัง [2]

- นโยบายการเข้าถึงเครือข่ายจากบ้าน
- นโยบายเข้าถึงเครือข่ายของแขก
- นโยบายการใช้งานเครือข่ายไร้สาย
- นโยบายการอัพเดตแพตช์
- การกำหนดนโยบายตามการจัดระดับความเสี่ยง
- การฝึกอบรมและอัพเดตความรู้ใหม่ๆ


SECURITY
TRAINING