บทที่ 7 : การป้องกันไวรัส Part3

สธ412 ความมั่นคงของระบบสารสนเทศ

อาจารย์อภิพงศ์ ปิงยศ

apipong.ping@gmail.com

Outline

- มัลแวร์ในปัจจุบัน
- การป้องกันไวรัส
  - การป้องกันไวรัสที่ไคลเอนต์
  - การติดตั้งแอพพลิเคชั่น
  - การป้องกันไวรัสที่เซิร์ฟเวอร์ (Part4)
  - การป้องกันไวรัสในระดับเครือข่าย (Part4)
  - การป้องกันทางกายภาพ (Part4)

มัลแวร์ในปัจจุบัน

ชื่อมัลแวร์	การแพร่กระจาย	การโจมตี
SQLSlammer	อาศัยช่องโหว่ของ Microsoft SQL Server	DOS จนทำให้เซิร์ฟเวอร์ล่ม และใช้แบนด์วิดธ์จนเต็ม
Sasser	เครื่องเป้าหมายที่มีการเปิดพอร์ต 445 (พอร์ตสำหรับแชร์ไฟล์บน Windows)	พยายามชัตดาวน์ระบบทุกๆ 30 วินาที
Mydoom	อีเมล ภายในเมลจะมี Executable File อยู่	สร้าง Backdoor และป้องกันไม่ให้รันสองโปรเซสพร้อมกัน

มัลแวร์ในปัจจุบัน [2]

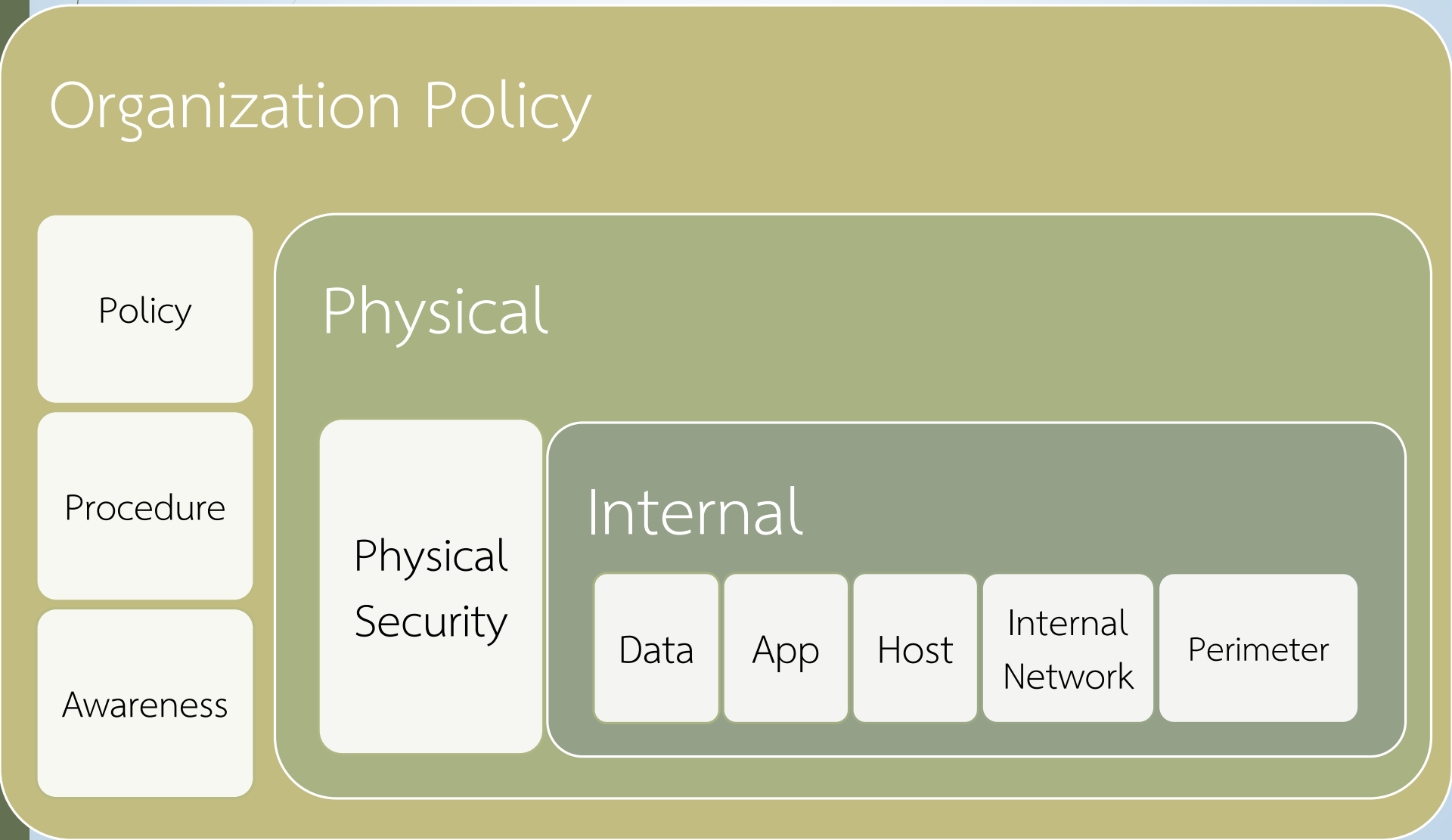
ชื่อมัลแวร์	การแพร่กระจาย	การโจมตี
Netsky	อีเมล	ส่งอีเมลที่ติดเวิร์มชนิดนี้ไปเรื่อยๆ และสแกนหาช่องโหว่ของเครื่องที่ติดเวิร์ม
Blackmal	อีเมล	ส่งอีเมลออกไปเป็นจำนวนมาก และพยายามทำลายซอฟต์แวร์ป้องกันไวรัสของโฮสต์

การป้องกันไวรัส

: พาหะที่ใช้สำหรับการแพร่ระบาด

- **เครือข่ายภายนอก** เช่น อินเทอร์เน็ต ซึ่งอยู่นอกเหนือการควบคุมขององค์กร
- **คอมพิวเตอร์ของแขกที่มาเยือน** อาจติดต่อมาจากภายนอก
- **เอ็กซีคิวต์ไฟล์** เช่น .exe, .dll, .sys เป็นต้น
- **ไฟล์เอกสาร** สามารถติดต่อได้โดยมาโครใน MS Office
- **อีเมล** ปกติจะติดมากับไฟล์แนบ
- **มีเดียเก็บข้อมูล** เช่น CD, DVD, USB Drives, Memory Card

โมเดลการป้องกันไวรัส



โมเดลการป้องกันไวรัส [2]

- **Data** เช่นข้อมูลที่เป็นความลับทางธุรกิจ หรือข้อมูลส่วนตัวของผู้ใช้
- **Application** ผู้โจมตีอาจใช้ช่องโหว่จากแอพพลิเคชั่นที่รันอยู่ก็ได้
- **Host** เป็นการโจมตีระบบปฏิบัติการ
- **Internal Network** การโจมตีอาจเกิดจากเครือข่ายภายในองค์กรก็ได้
- **Perimeter Network** เกิดจากผู้บุกรุกสามารถเข้าถึงเครือข่ายสำคัญขององค์กรได้

โมเดลการป้องกันไวรัส [3]

- **Physical Security** ความเสี่ยงทางกายภาพ เกิดจากผู้บุกรุกสามารถเข้าถึงอุปกรณ์หรือเซิร์ฟเวอร์ทางกายภาพได้
- **Policy, Procedures and Awareness** นโยบาย ระเบียบปฏิบัติ และข้อควรระวัง ซึ่งเป็นหน้าที่ขององค์กรที่จะต้องบังคับใช้ระเบียบและสร้างความตระหนักรู้ให้กับผู้ใช้

การป้องกันไวรัสที่ไคลเอนต์

- การป้องกันไคลเอนต์จำเป็นต้องติดตั้งซอฟต์แวร์ป้องกันไวรัสเพื่อป้องกันและหยุดยั้งการแพร่กระจายไปยังเครื่องอื่นๆทั่วทั้งองค์กร
- หากไวรัสสามารถติดที่เครื่องไคลเอนต์ได้แล้ว ไวรัสก็จะมีโอกาสผ่านการป้องกันอื่น ๆ และลุกลามไปยังระดับต่าง ๆ ได้

การป้องกันไวรัสที่ไคลเอนต์ [2]

คำแนะนำที่ควรปฏิบัติตามอย่างเคร่งครัด คือ

- **การลบโปรแกรมที่ไม่ได้ใช้งาน** เพราะโปรแกรมบางตัวมีช่องโหว่และสามารถเป็นภาหะนำไวรัสได้
- **การอัพเดตแพตช์** ทั้งระบบปฏิบัติการและแอพพลิเคชั่นต่างๆ
- **การติดตั้งโฮสต์เบสไฟร์วอลล์** โดยเฉพาะคอมพิวเตอร์โน้ตบุคที่มีการนำไปใช้งานนอกเครือข่ายขององค์กร
- **การติดตั้งซอฟต์แวร์ป้องกันไวรัส** โดยต้องมีการอัพเดตฐานข้อมูลไวรัสเป็นประจำ

การป้องกันไวรัสที่ไคลเอนต์ [3]

- **การสแกนหาจุดอ่อนของระบบ** ควรมีการตรวจสอบเป็นประจำว่าระบบเราไม่มีจุดอ่อนใดๆ โดยอาจใช้เครื่องมือสแกนหลาย ๆ ตัวเพื่อเพิ่มประสิทธิภาพ
- **กำหนดสิทธิ์ของผู้ใช้งานระบบให้น้อยที่สุด** โดยกำหนดสิทธิ์ให้เพียงพอต่อการทำงานประจำของแต่ละคน ไม่ควรล็อกอินในฐานะผู้ดูแลระบบเพื่อทำงานทั่วไป

การติดตั้งแอพพลิเคชั่น

- **การติดตั้ง** การติดตั้งซอฟต์แวร์ปกติจะติดตั้งตามค่า**ดีฟอลต์** *ข้อดี*คือการติดตั้งง่ายและรวดเร็ว *ข้อเสีย*คืออาจมีช่องโหว่หรือมีมัลแวร์ติดมาได้
- **อีเมลไคลเอนท์** ถ้าเป็นไปได้ควรจำกัดสิทธิ์ เช่น ป้องกันไม่ให้เปิดดูแอคทีฟคอนเทนต์ได้ กำหนดให้อ่านเมลล์ได้เฉพาะรูปแบบเพลนเท็กซ์ หรือบล็อกไฟล์แนบที่เข้าข่ายอันตราย
- MS Office สามารถถูกโจมตีได้โดยมาโครไวรัส ทางที่ดีควรมีการอัพเดตซอฟต์แวร์อยู่เสมอ

การติดตั้งแอพพลิเคชั่น [2]

- **Instant Messaging** หรือการรับ-ส่งข้อความแบบทันที เช่น Line หรือ Facebook Messenger เป็นต้น ควรมีการบล็อกพอร์ตที่ใช้ถ่ายโอนไฟล์ประเภทนี้ หรือมีการสแกนไฟล์ด้วยโปรแกรมป้องกันไวรัสก่อน
- **เว็บเบราเซอร์** การดาวน์โหลดและรันโปรแกรมจากอินเทอร์เน็ต ต้องมั่นใจว่าไฟล์นั้นมาจากแหล่งที่เชื่อถือได้ ควรมีการตั้งค่าความปลอดภัยของเบราเซอร์ให้อยู่ในระดับกลางและสูง เพื่อให้ไคลเอนต์แจ้งเตือนก่อนดาวน์โหลด และควรมีการอัพเดตเว็บเบราเซอร์อยู่เสมอ

การติดตั้งแอพพลิเคชั่น [3]

- Peer-to-Peer Application (P2P) ช่วยให้ผู้ใช้แชร์ไฟล์กันได้สะดวกยิ่งขึ้น ปกติการใช้ P2P จะสามารถแชร์ไฟล์ได้โดยตรงโดยไม่ต้องผ่านระบบรักษาความปลอดภัยเลย ถ้าเป็นไปได้ควรจำกัดสิทธิ์การใช้งานแอพพลิเคชั่นประเภทนี้