บทที่ 5: การป้องกันองค์กรและหน่วยงาน

BEFORE WE START

1. I'm Not the Best, but I have lots of things to share with you.
2. This is <u>not</u> a "*How to Hack*" course
3. This is a program to give you an idea of how you can develop your skill into a professional system security tester in the (near) future.

โครงการส่งเสริมและสนับสนุนให้มีการเสริมสร้างมาตรฐานบุคลากรด้าน ICT ที่สอดคล้องกับความต้องการของอุตสาหกรรม ICT รอบที่ 2

COMMITMENTS

1. **Participation** is expected, so you are welcome to ask questions and also you will be asked (a lot of questions).
2. Learning as **TEAM** is very much better than learning on your own.
3. I'll do my best, and please **DO YOUR BEST**.
4. I do believe "**YOU CAN DO IT**".
   Do you believe so?

THE RULES

1. Never use knowledge from this program to conduct a test against any system unless you have a <u>WRITTEN PERMISSION</u> to do so…
2. Never break rule #1
3. Always comply to rule #2

Out-of-jail Letter

PROGRAM OBJECTIVE

- To help attendees jump-start into IT Security
- To build fundamental knowledge in IT Security
- To familiarize attendees to security terminology

PROGRAM OUTLINE

- Introduction to IT Security
- Network Security

LET'S START

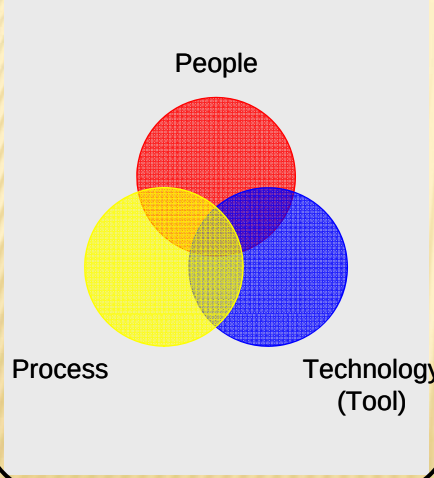
HACKER

- Script kiddies
- Mature
- Expert

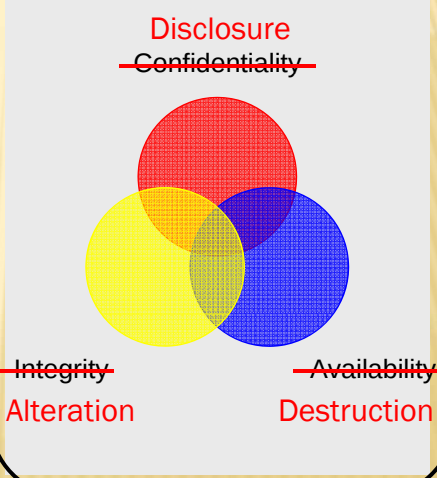
- Knowledge/Skill
- Funding
- Motive

โครงการส่งเสริมและสนับสนุนให้มีการเสริมสร้างมาตรฐานบุคลากรด้าน ICT ที่สอดคล้องกับความต้องการของอุตสาหกรรม ICT รุ่นที่ 2

3 Pillars of ICT



3 Pillars of Security



KEY POINTS

- Security = Risk Management
- Security Management = Cycle
- Risk = Possibility x Impact
  - Threat
  - Vulnerability
  - Exploit
  - Safeguard/Countermeasure
- Hacking Anatomy

โครงการส่งเสริมและสนับสนุนให้มีการเสริมสร้างมาตรฐานบุคลากรด้าน ICT ที่สอดคล้องกับความต้องการของอุตสาหกรรม ICT รุ่นที่ 2

THREATS

- DoS: Denial of Service
  DDoS: Distributed DoS
- Portscan
- Malware
  - Virus
  - Worm
  - Spyware
  - Trojan (Horse)
- BOT and BOTNET
  - Zombie, Smurf, DDoS
- Phishing and Pharming
- Man-in-the –Middle
  - Eavesdropping
  - Hi-jacking
  - Packet Sniffing
  - Replay Attack
- Password Attack
  - Brute force Attack
  - Dictionary Attack
  - Rainbow Attack

MEASURES

- Preventive
  - Policy
  - Firewall
  - Network segmentation
  - Antivirus
  - Awareness
- Detective
  - IDS
  - IPS
  - SOC/NOC
- Corrective
  - Backup/Recovery
- (Deterrent)
- Defense-in-dept
- Need-to-know Basis

SECURITY MECHANISM

- 3A
  - Authentication (identification)
  - Authorization/Access Control
  - Accountability/Non-repudiation
- Strong Authentication
  - Strong Password Policy
    - Length ≥ 8
    - Complexity (abc123!@#) → Alphanumeric + Special Char.
    - Expiration = 90 days
    - Repetition ≥ 3
  - 2 Factors Authentication
  - OTP (One-time Password)
    - Token
    - SMS
  - Biometric
- Resilience
  - Backup Data / Site
  - Redundant
  - Cluster
  - Standby System (Hot/Warm/Cold)

SAFE HOSTS IN HOSTILE ENVIRONMENT

สิ่งแวดล้อมในที่นี้ คือสิ่งแวดล้อมทางคอมพิวเตอร์

ซึ่งประกอบด้วยคอมพิวเตอร์, ผู้ใช้คอมพิวเตอร์ และรวมถึงอุปกรณ์ต่าง ๆ ที่ใช้ร่วมกับคอมพิวเตอร์ ความไม่ปลอดภัยที่เกิดขึ้นกับเครื่องคอมพิวเตอร์จะมาจากสิ่งแวดล้อมโดยรอบ ซึ่งสามารถแบ่งสาเหตุการเกิดความไม่ปลอดภัยได้จาก สองแหล่งหลักคือ

- ความไม่ปลอดภัยที่เกิดจากการกระทำของมนุษย์
- ความไม่ปลอดภัยที่เกิดขึ้นตามธรรมชาติ

ความไม่ปลอดภัยที่เกิดขึ้นตามธรรมชาติ

- การป้องกันความเสียหายจากภัยธรรมชาตินั้นสามารถทำได้หลากหลายวิธีโดยดูจากปัญหาที่อาจจะเกิด
- ตัวอย่าง: หากองค์กรมีกระแสไปไฟฟ้าไม่เพียงต่อการทำงาน เมื่อเกิดฝนตกหนัก องค์กรสามารถแก้ปัญหาได้โดยการซื้อเครื่องสำรองไฟมาใช้

ความไม่ปลอดภัยที่เกิดขึ้นโดยมนุษย์

- ความไม่สนใจต่อระเบียบการใช้คอมพิวเตอร์ เช่น ไม่ตรวจฆ่าไวรัสก่อนนำ ข้อมูลเข้าสู่เครื่องคอมพิวเตอร์
- การไม่เห็นความสำคัญต่อความลับของข้อมูล ทั้งส่วนตัวและองค์กร
- การเจาะเข้าถึงข้อมูลโดยผู้ไม่ประสงค์ดีทั้งภายในและภายนอกองค์กร
- การปลอมแปลงเข้าใช้ระบบเพื่อการอย่างอื่น ที่ไม่ส่งผลดีต่อองค์กร
- การเขียนโปรแกรมที่ทำลายระบบ เช่น ไวรัส, หนอน, โทรจัน เป็นต้น
- อื่น ๆ ที่เกิดจากการกระทำของมนุษย์

การป้องกันความเสียหายที่เกิดขึ้นโดยมนุษย์

การป้องกันปัญหาที่เกิดจากภายใน

- การรณรงค์ให้บุคลากรในองค์การมีความตระหนักและเห็นความสำคัญของการรักษาความปลอดภัยของข้อมูลขององค์กร
- ชี้ให้เห็นถึงความเสียหายที่อาจจะเกิดจากการไม่สนใจต่อระเบียบการใช้คอมพิวเตอร์

การป้องกันปัญหาที่เกิดจากภายนอก

- ป้องกันไวรัส
- การใช้รหัสผ่าน
- การตรวจจับผู้บุกรุก

การป้องกันไวรัสคอมพิวเตอร์ และโปรแกรมที่อาจสร้างความเสียหาย

1. บูตเซกเตอร์ไวรัส
2. โปรแกรมไวรัส
3. โทรจัน
4. โพลีมอร์ฟิกไวรัส
5. สทีลต์ไวรัส
6. รูทคิต

การป้องกันไวรัส

- วิธีการตรวจหา
  - ใช้ฐานข้อมูล
  - ตรวจการเปลี่ยนแปลง
  - การเฝ้าดู
- การกำจัดไวรัส

การใช้รหัสผ่าน

- การสร้างรหัสผ่าน
- สิ่งที่ควรหลีกเลี่ยง
- การเปลี่ยนรหัสผ่าน
- กระบวนการในการส่งรหัสผ่าน
- การจัดการรหัสผ่าน

การตรวจจับผู้บุกรุก

- ระบบตรวจจับการบุกรุก (Intrusion Detection System) คือระบบที่ใช้ในการตรวจจับ การใช้งานและความพยายามในการใช้งาน คอมพิวเตอร์หรือเครือข่ายคอมพิวเตอร์ซึ่งขัดกับข้อบังคับและเจตจำนงการใช้งาน ส่งผลต่อความปลอดภัยของระบบคอมพิวเตอร์หรือเครือข่ายคอมพิวเตอร์ 3 ประการคือ Integrity, Confidentiality, Availability
- กลไกการตรวจจับผู้บุกรุก

จบ บทที่ 5