การจัดการความมั่นคงปลอดภัยทางข้อมูล

Information Security Management

Chapter 1 : Cybersecurity

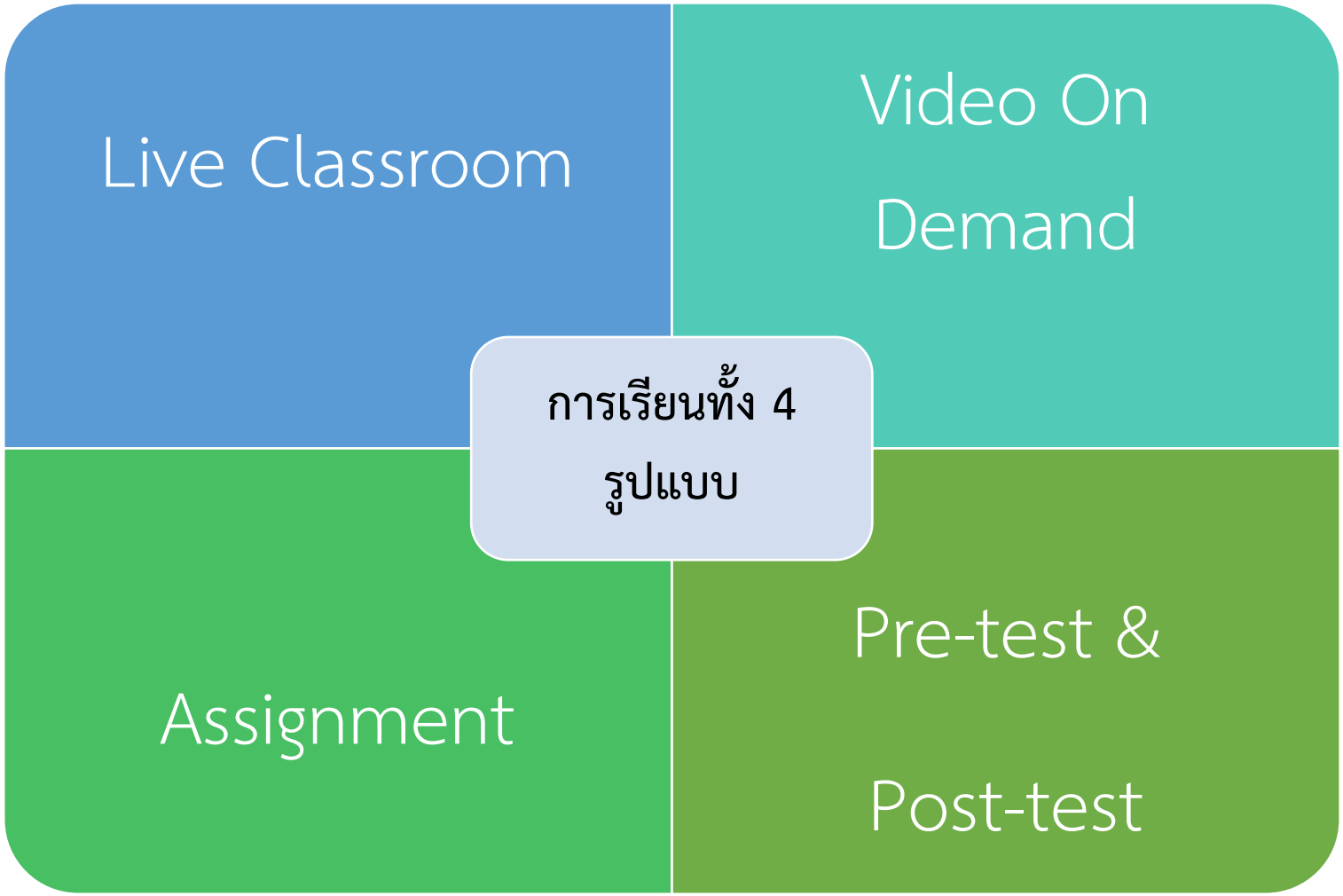
การจัดการความมั่นคงปลอดภัยทางข้อมูล

การวิเคราะห์ความเสี่ยงขององค์กรเพื่อประยุกต์กับยุทธศาสตร์ด้านต่างๆ ผลการวิเคราะห์ความเสี่ยงซึ่งทำให้ได้ถึงทะเบียนของสิ่งต่าง ๆ และระดับของความมั่นคง โอกาสที่จะเกิดความเสียหาย กฎหมาย ระเบียบปฏิบัติและสัญญาธุรกิจต่างๆ ขององค์กรและของคู่ค้า-พันธมิตร และสังคมที่เกี่ยวข้อง หลักการ วัตถุประสงค์ และความต้องการทางธุรกิจของการประมวลผลข้อมูลข่าวสารขององค์กรที่ใช้ในการดำเนินธุรกิจ

วิธีการประเมินและวัดผล

รายการ	เปอร์เซ็นต์
1. Pre-test	20
2. Post-test	20
3. ส่งใบงาน	10
4. สอบกลางภาค	25
5. สอบปลายภาค	25
รวม	100

วิธีการเรียน


Live Classroom
Video On Demand
การเรียนทั้ง 4 รูปแบบ
Assignment
Pre-test & Post-test

เนื้อหา

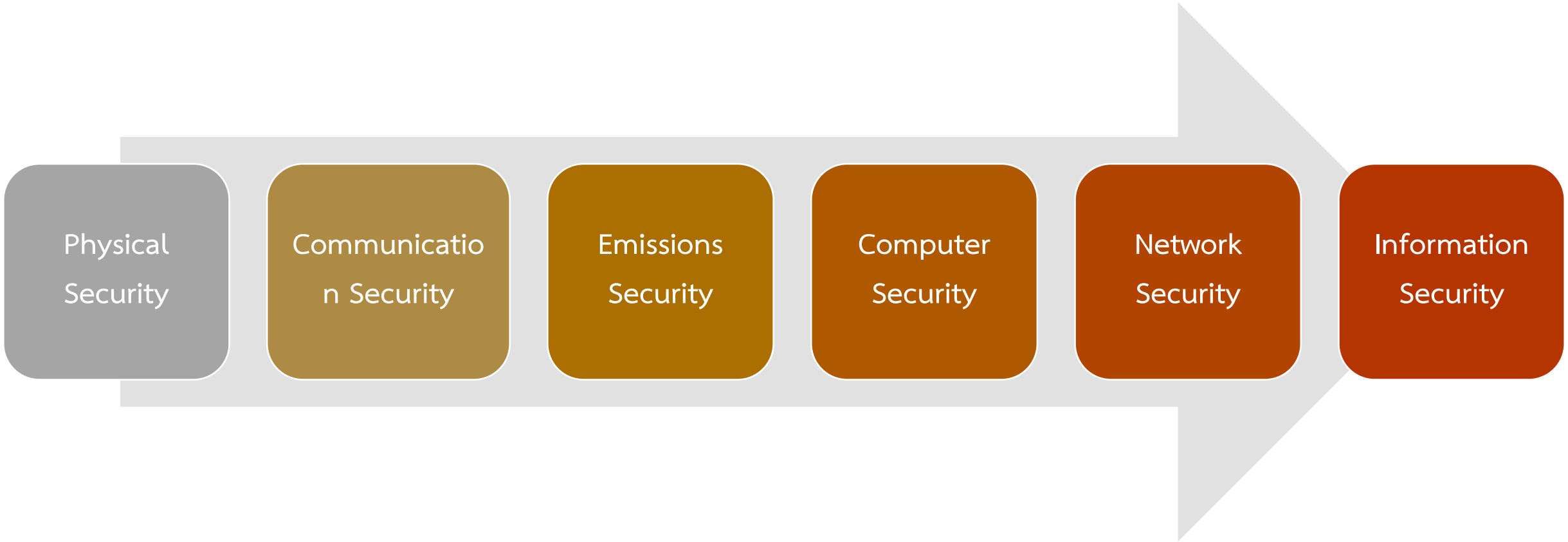
- วิวัฒนาการของการรักษาความปลอดภัย
- หลักการพื้นฐานของการรักษาความปลอดภัยของข้อมูล
- ประเภทของภัยคุกคาม (Threat)
- แนวโน้มภัยคุกคามในปัจจุบัน

การรักษาความปลอดภัย (Security System)

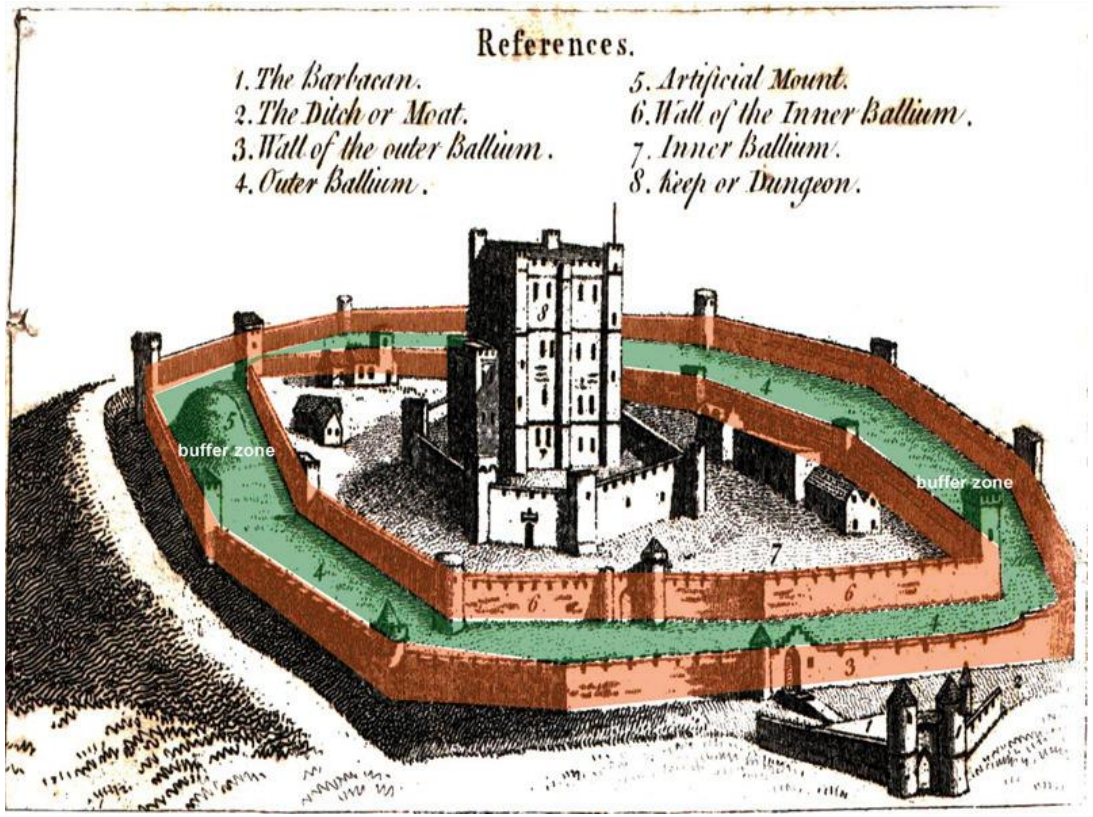
การรักษาความปลอดภัย (Security System) หมายถึง การป้องกันซึ่งทรัพย์สินสิ่งของให้กับองค์กร บริษัท ห้างร้าน หรือบุคคลต่างๆ

ข้อมูลและสารสนเทศ

วิวัฒนาการของการรักษาความปลอดภัย



การรักษาความปลอดภัยทางด้านกายภาพ (Physical Security)



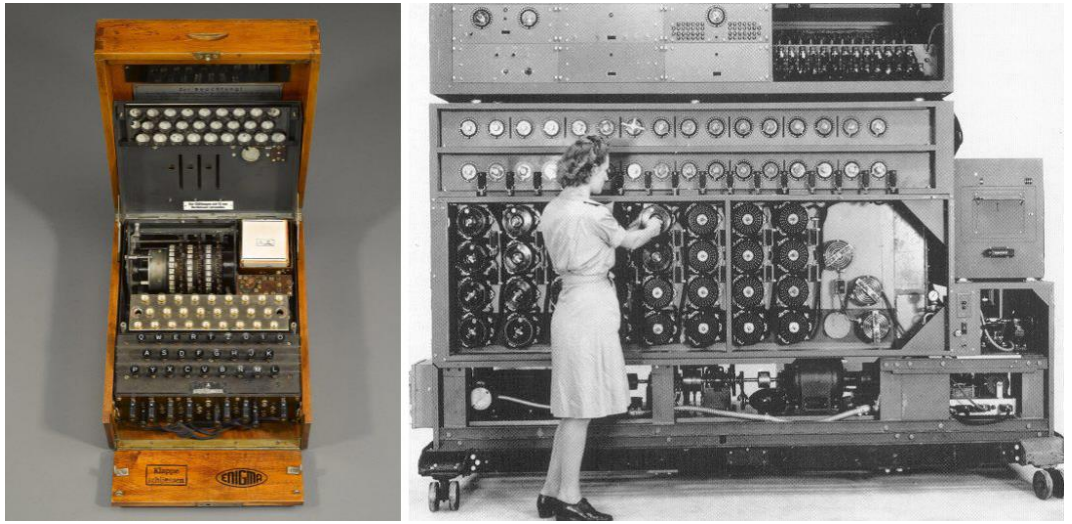
"ความรู้คืออำนาจ" (Knowledge is power)

การรักษาความปลอดภัยทางด้านกายภาพ (Physical Security)

การรักษาความปลอดภัยทางด้านการสื่อสาร (Communication Security)

จูเลียส ซีซ่าร์

(Julius Caesar)



Enigma Machine Vs Turing Machine

Navajo code talkers

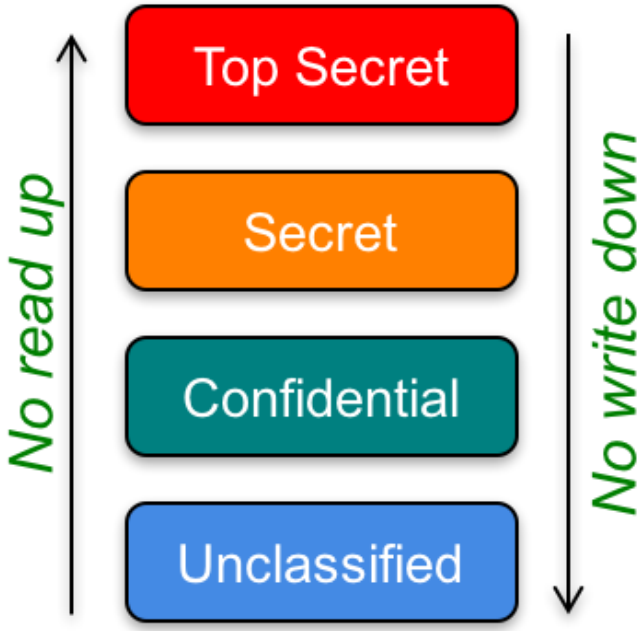
การรักษาความปลอดภัยทางการแผ่รังสี (Emissions Security)

มาตรฐาน “เทมเปสต์ (TEMPEST)”

ซึ่งเป็นมาตรฐานที่ควบคุมการแผ่รังสีของอุปกรณ์คอมพิวเตอร์และใช้กับระบบที่สำคัญๆ จุดหมายก็เพื่อลดการแผ่รังสีที่อาจใช้สำหรับการกู้คืนข้อมูลได้

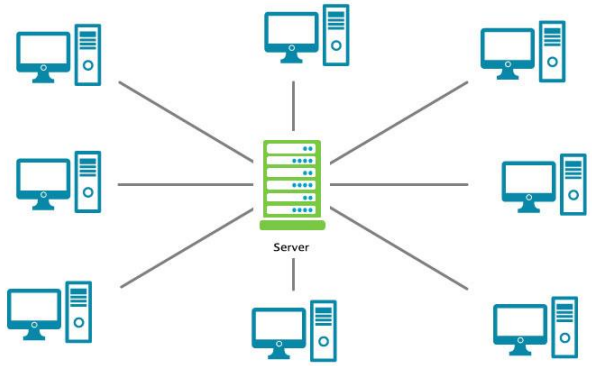
การรักษาความปลอดภัยทางคอมพิวเตอร์ (Computer Security)

Computer

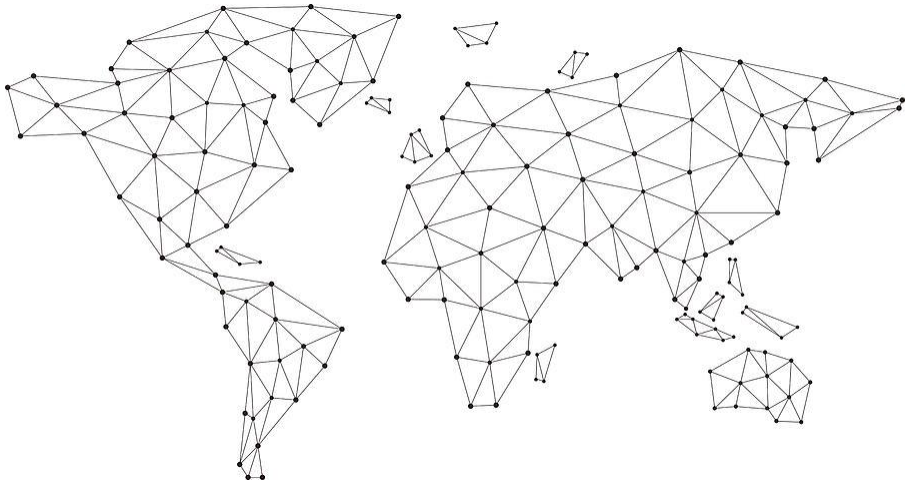


Bell-laPadula Model

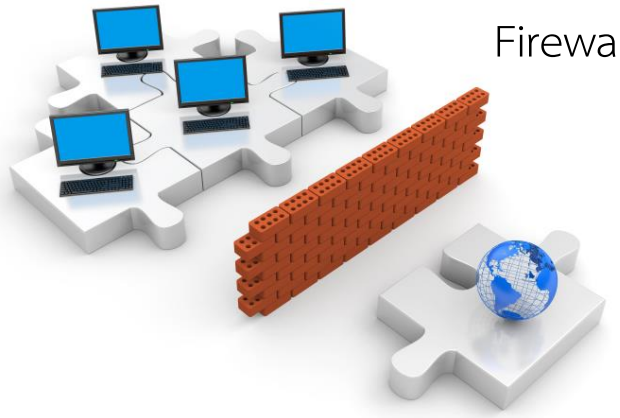
การรักษาความปลอดภัยเครือข่าย (Network Security)



LAN/MAN/WAN



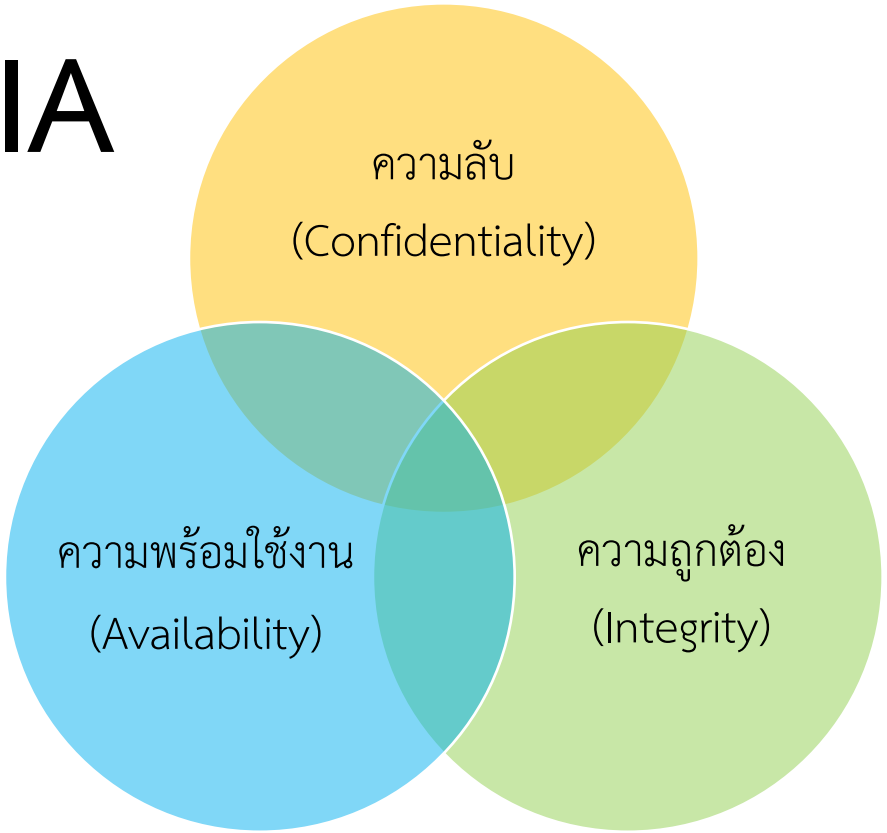
Internet



Firewall

การรักษาความปลอดภัยข้อมูล (Information Security)

CIA



หลักการรักษาความปลอดภัย

การควบคุมการเข้าถึง (Access Control)

- การระบุตัวตน (Identification)
- การพิสูจน์ทราบตัวตน (Authentication)
- การอนุญาตใช้งาน (Authorization)

การรักษาความปลอดภัยไซเบอร์ (Cyber Security)

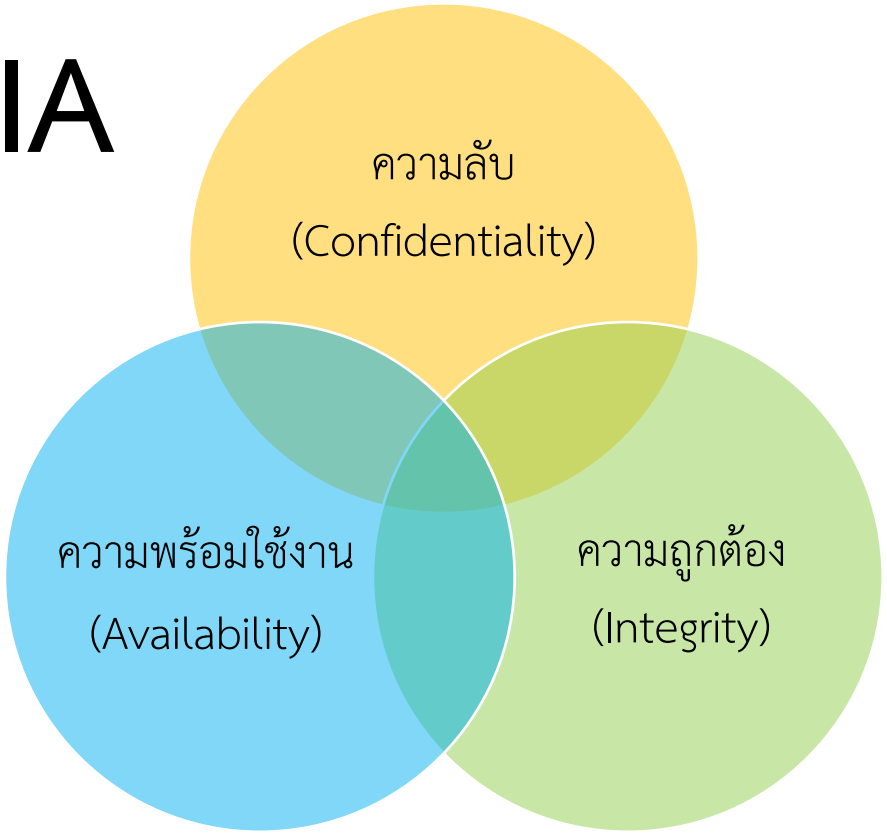
ไซเบอร์ (Cyber) กร่อนมาจากคำว่า ไซเบอร์เนติกส์ (Cybernetics) แปลว่า เกี่ยวข้องกับขอบเขตระบบเครือข่าย หรือหมายถึงอุปกรณ์คอมพิวเตอร์ทั่วไป

การรักษาความปลอดภัยไซเบอร์ (Cyber Security)

การรักษาความปลอดภัยไซเบอร์ (Cyber Security) คือ กระบวนการที่จำเป็นเพื่อให้องค์กรปราศจากความเสี่ยงและความเสียหาย ที่มีผลต่อข้อมูลข่าวสารทุกรูปแบบ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ

หลักการพื้นฐานของการรักษาความปลอดภัยของข้อมูล

CIA



หลักการรักษาความปลอดภัย

การควบคุมการเข้าถึง (Access Control)

- การระบุตัวตน (Identification)
- การพิสูจน์ทราบตัวตน (Authentication)
- การอนุญาตใช้งาน (Authorization)

ความลับ (Confidentiality)

การรักษาความลับของข้อมูล หมายถึง การอนุญาตให้เฉพาะผู้ที่ได้รับอนุญาตเข้าถึงข้อมูลได้ ป้องกันข้อมูลไม่ให้ผู้ที่ไม่ได้รับอนุญาตสามารถเข้าถึงข้อมูลได้นั้นเอง

เริ่มจากด้านการทหาร ที่ต้องการปกปิดข้อมูลเกี่ยวกับกองทัพไม่ให้ฝ่ายตรงข้ามทราบ

ค่ายทหาร

ค่ายทหาร

อาวุธที่ใช้

ความลับ (Confidentiality)

ต่อมาก็นำหลักการนี้มาประยุกต์ใช้กับทางธุรกิจ เช่น ความลับในการออกแบบผลิตภัณฑ์ การเก็บข้อมูลส่วนตัวของพนักงาน หรือข้อมูลส่วนตัวของลูกค้า

ความลับในการออกแบบผลิตภัณฑ์

ข้อมูลลูกค้า

ข้อมูลพนักงาน

ความลับ (Confidentiality)

กลไกที่ใช้ในการรักษาความลับ คือ

กลไกการเข้ารหัสข้อมูล (Cryptography หรือ Encryption)

กลไกการควบคุมการเข้าถึง (Access Control)

Cryptography

Access Control

ความถูกต้อง (Integrity)

ความถูกต้องของข้อมูล หมายถึง ความน่าเชื่อถือของข้อมูลว่าเป็นข้อมูลดั้งเดิมและไม่มีการแก้ไขเปลี่ยนแปลงโดยไม่ได้อนุญาต โดยคำนึงถึง 2 ส่วน ดังนี้

ความถูกต้องของเนื้อหาข้อมูล

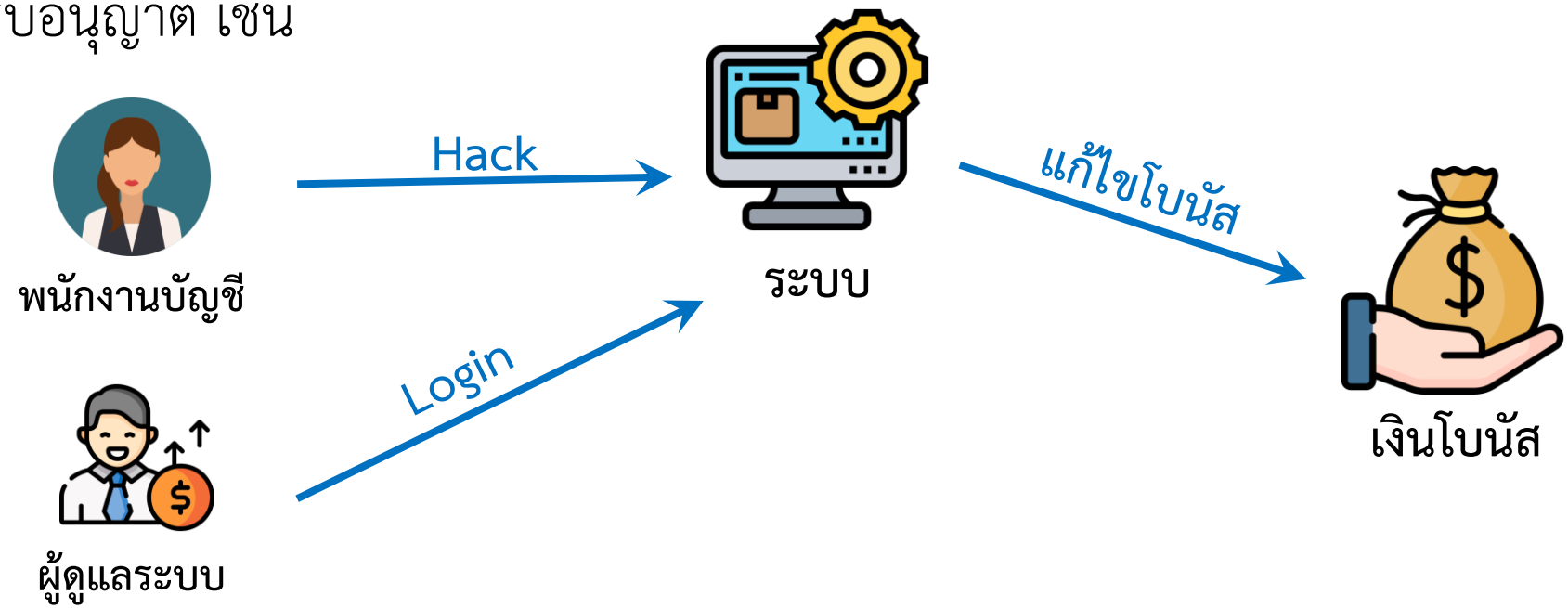
ความถูกต้องของแหล่งที่มาของข้อมูล

เช่น หนังสือพิมพ์รายงานข่าวว่าอาจจะมีการก่อการร้ายเกิดขึ้น ซึ่งข่าวอาจจะรั่วมาจากสำนักข่าวกรองของรัฐบาล แต่หนังสือพิมพ์ได้ข่าวมาด้วยวิธีการที่ผิด จึงรายงานว่าข่าวนี้มาจากแหล่งข่าวอื่น เนื้อข่าวยังเหมือนเดิม แต่แหล่งที่มาของข่าวเปลี่ยนไป **ทำให้ความถูกต้องของข้อมูลเสียไป**

ความถูกต้อง (Integrity)

กลไกที่ใช้ในการรักษามถูกต้อง คือ

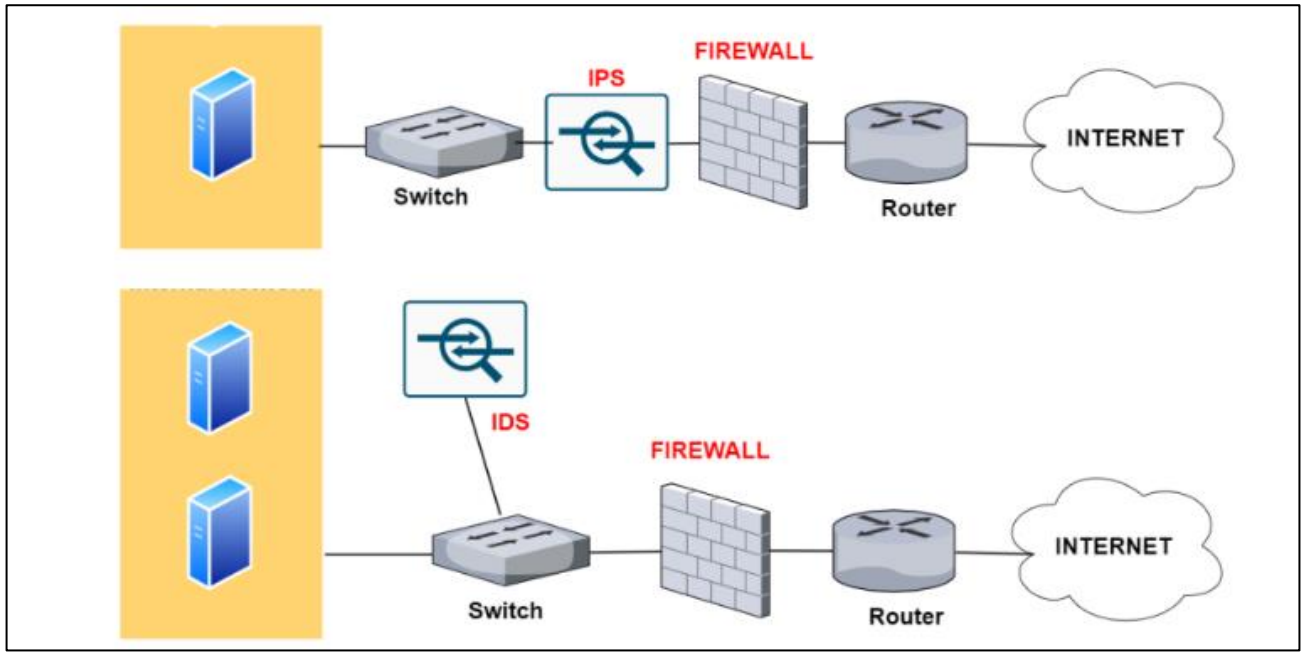
กลไกการป้องกัน (Prevention) : ป้องกันความพยายามที่จะเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต หรือความพยายามที่จะเปลี่ยนแปลงข้อมูลในรูปแบบที่ไม่ถูกต้องหรือได้รับอนุญาต เช่น



ความถูกต้อง (Integrity)

กลไกที่ใช้ในการรักษามถูกต้อง คือ

กลไกการตรวจสอบความถูกต้องของข้อมูล (Detection) : เป็นกลไกที่ตรวจสอบว่าข้อมูลยังคงมีความน่าเชื่อถืออยู่หรือไม่ โดยจะมีการรายงานว่าส่วนไหนของข้อมูลมีการแก้ไข



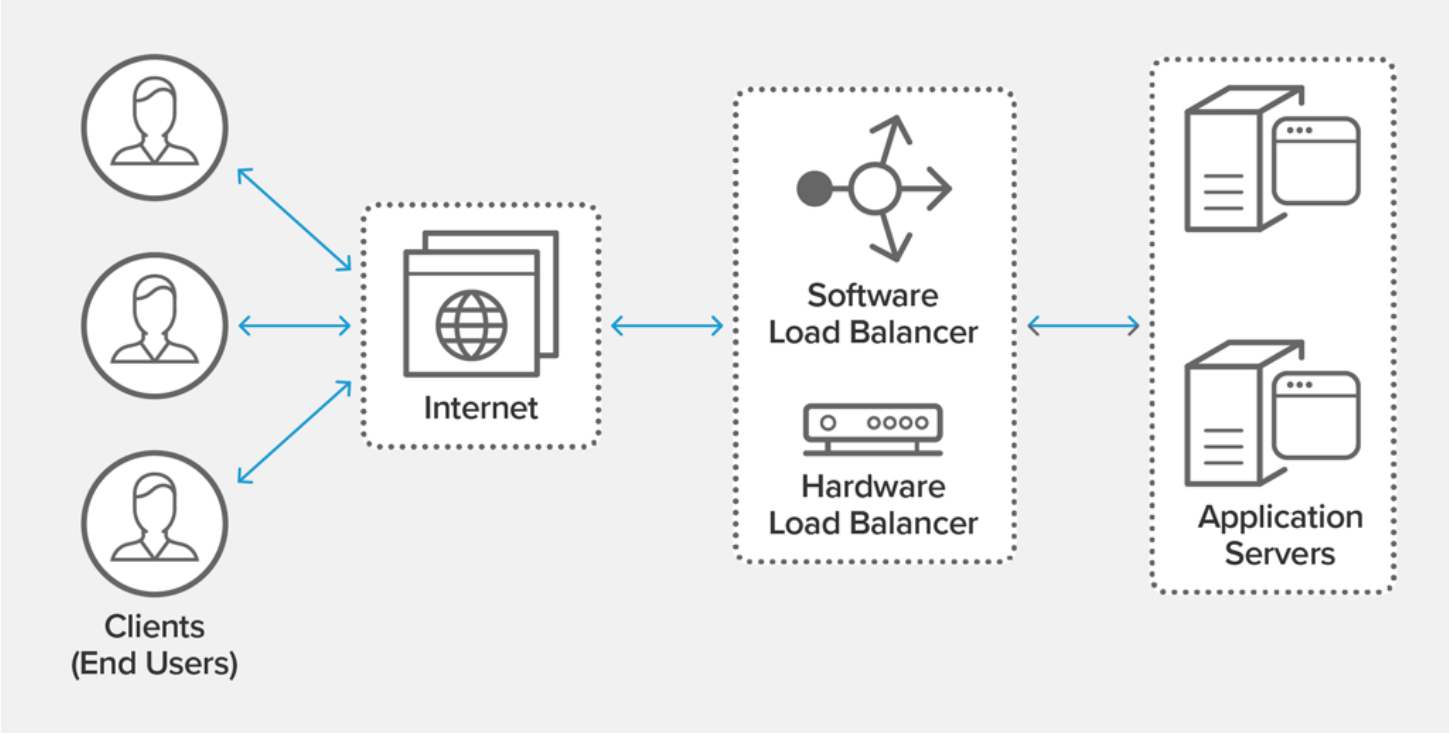
ความพร้อมใช้งาน (Availability)

ความพร้อมใช้งานของข้อมูล หมายถึง ความสามารถในการใช้งานข้อมูลเมื่อต้องการ ความพร้อมใช้งานเป็นส่วนหนึ่งของความมั่นคงของระบบ (Reliability) เพราะระบบที่ไม่พร้อมใช้งานก็ไม่ต่างอะไรกับไม่มีระบบ

โดยมีกลไกในการรักษาความพร้อมใช้งานนั้น จะทำงานในกรณีที่ระบบไม่ได้ทำงานในสภาพปกติ ซึ่งถ้ากลไกนี้ไม่ทำงานระบบจะล่มหรือไม่พร้อมใช้งาน

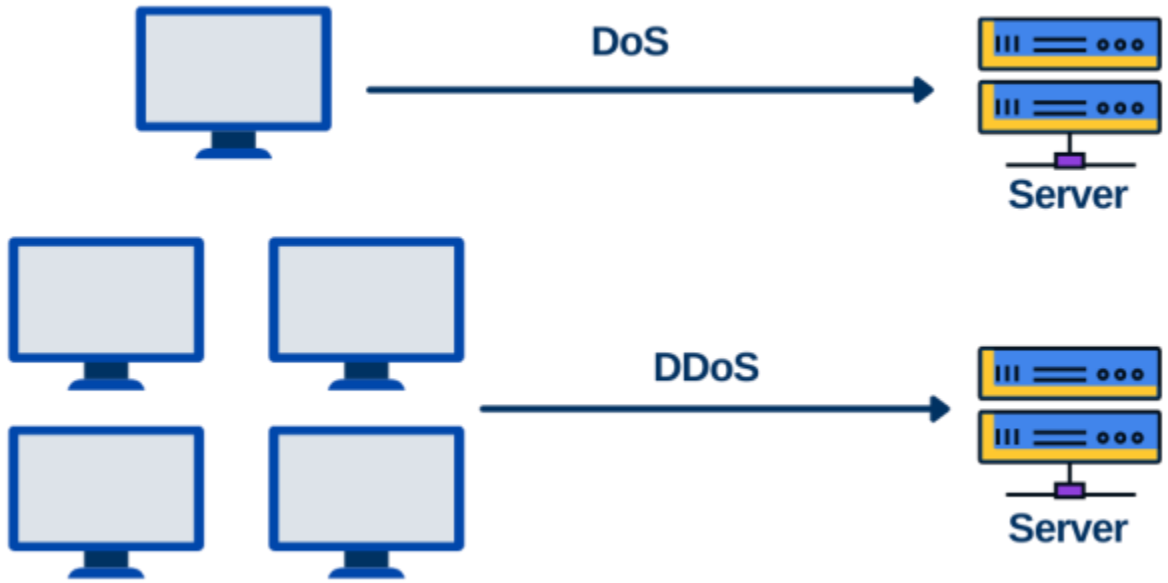
ความพร้อมใช้งาน (Availability)

เช่น ธนาคารแห่งหนึ่งเก็บข้อมูลของลูกค้าไว้ใน Server 2 เครื่องทำโหลดบาลานซิ่ง (Load Balancing) ซึ่งกันและกัน เมื่อเครื่องหนึ่งทำงานไม่ได้อีกเครื่องหนึ่งจะทำงานแทน



ความพร้อมใช้งาน (Availability)

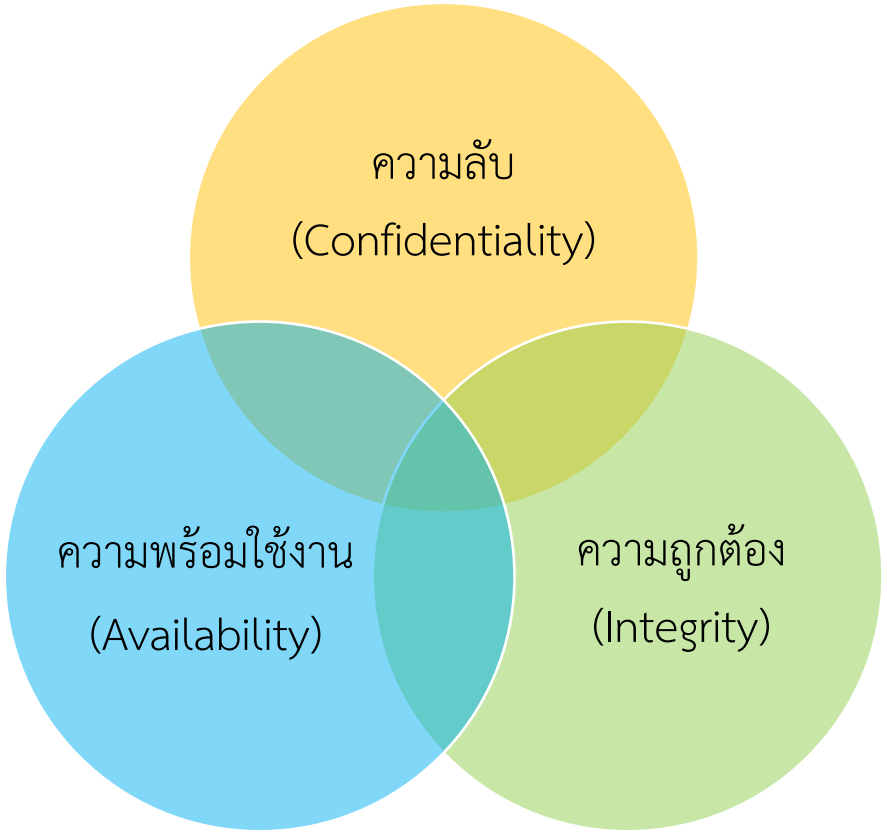
ความพยายามที่จะทำลายความพร้อมใช้งานเรียกว่า การโจมตีแบบปฏิเสธการให้บริการ (Denial of Service: Dos) ซึ่งเป็นการโจมตีที่ตรวจจับได้ยากที่สุด



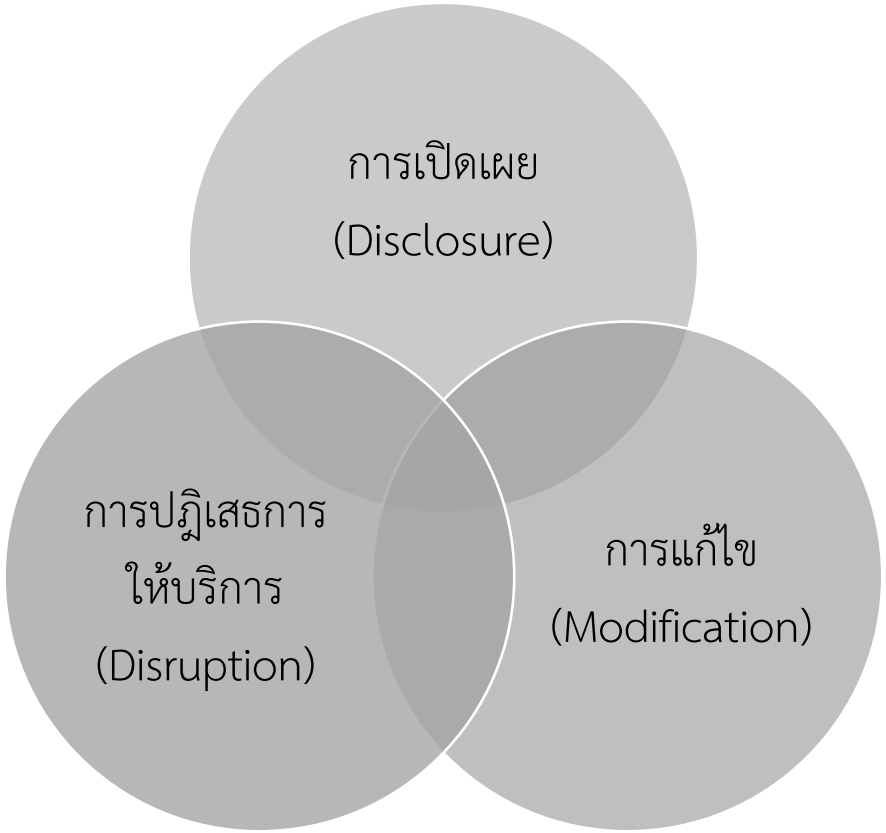
ประเภทของภัยคุกคาม (Threat)

ภัยคุกคาม (Threat) หมายถึง สิ่งที่อาจจะก่อให้เกิดความเสียหายต่อข้อมูลด้านใดด้านหนึ่งหรือมากกว่าหนึ่งด้าน ภัยคุกคามนั้นอาจจะไม่เกิดขึ้นเลยก็ได้ถ้ามีการป้องกันที่ดี หรืออาจจะเกิดความเสียหายลดลงได้ การกระทำที่ก่อให้เกิดความเสียหายเราจะเรียกว่า การโจมตี (Attack) ส่วนผู้ที่กระทำการดังกล่าวจะเรียกว่า ผู้โจมตี (Attacker) หรือ แฮกเกอร์ (Hacker) หรือแครกเกอร์ (Cracker)

ประเภทของภัยคุกคาม (Threat)



หลักการรักษาความปลอดภัย



ประเภทภัยคุกคาม

ประเภทของภัยคุกคาม (Threat)

- **การเปิดเผยข้อมูล (Disclosure)** คือ การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต หรือข้อมูลนั้นถูกเปิดเผยให้กับผู้ที่ไม่ได้รับอนุญาต ซึ่งเป็นการโจมตีคุณสมบัติข้อมูลด้านความลับ
- **การแก้ไขข้อมูล (Modification)** คือ การแก้ไขข้อมูลโดยไม่ได้รับอนุญาต ซึ่งเป็นการโจมตีคุณสมบัติข้อมูลด้านความถูกต้อง
- **การปฏิเสธการให้บริการ (Denial of Service: Dos)** คือ การขัดขวาง หน่วงเวลา หรือทำให้ไม่สามารถเข้าถึงข้อมูลได้ ซึ่งเป็นการโจมตีคุณสมบัติข้อมูลด้านความพร้อมใช้งาน

ประเภทของภัยคุกคาม (Threat)

มีการโจมตีรูปแบบอื่น ๆ ที่มักจะได้ยินเป็นประจำ เช่น

- การสอดแนม (Sniffing)
- การปลอมตัว (Spoofing)
- สคริปต์คิดดี้ส์ (Script Kid-dies)
- การปฏิเสธแหล่งที่มา (Repudiation of Origin)
- การปฏิเสธการได้รับ (Repudiation of Receipt)
- การหน่วงเวลา (Delay)
- วิศวกรรมสังคม (Social Engineering)
- การถอดรหัสข้อมูล (Cryptanalysis)

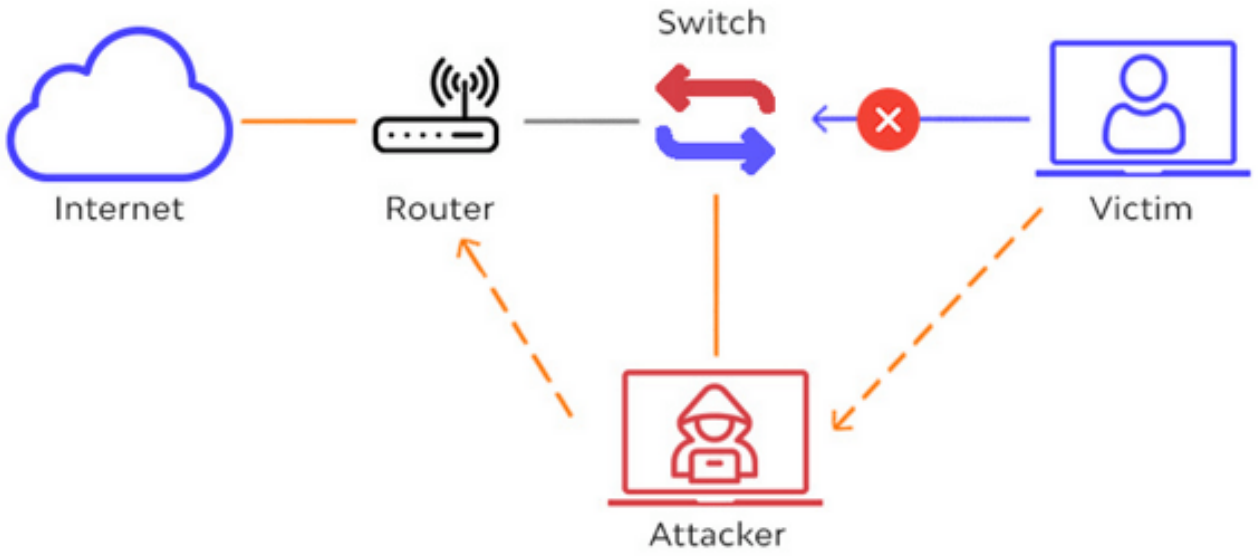
ประเภทของภัยคุกคาม (Threat)

มีการโจมตีรูปแบบอื่น ๆ ที่มักจะได้ยินเป็นประจำ เช่น

- การโจมตีแบบคนกลาง (Man-in-the-middle Attack)
- บอตเน็ต (Botnet)
- ฟิชชิง (Phishing)

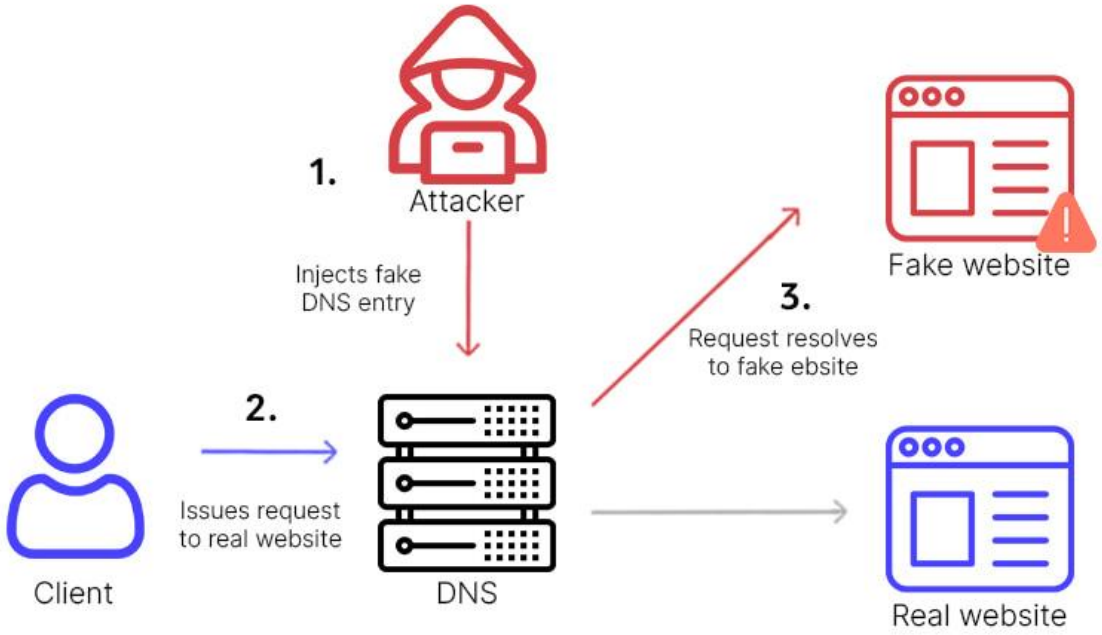
การสอดแนม (Sniffing)

เป็นการดักเพื่อแอบดูข้อมูล เป็นการโจมตีแบบพาสซีฟ (Passive) คือ เป็นการกระทำที่ไม่มีการเปลี่ยนแปลงหรือแก้ไขข้อมูล ส่วนมากจะโจมตีที่เครือข่าย



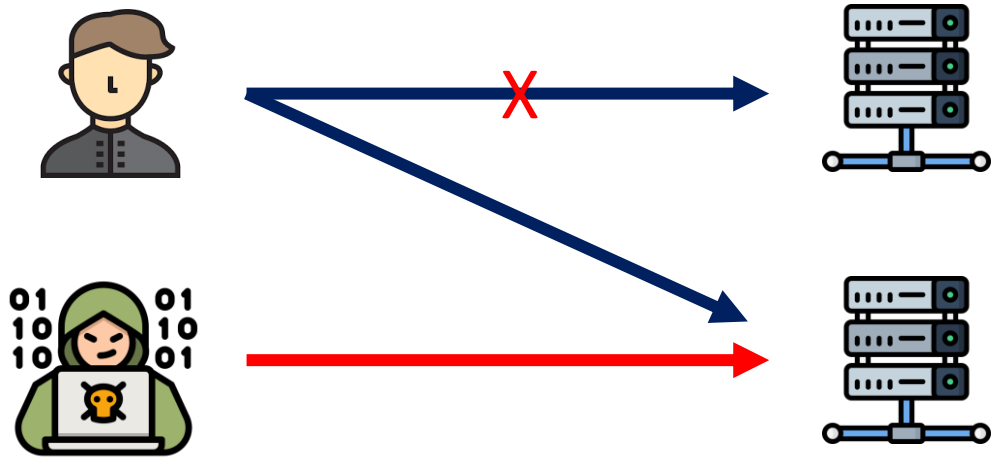
การปลอมตัว (Spoofing)

เป็นการทำให้อีกฝ่ายเข้าใจว่าตนเองเป็นอีกบุคคลหนึ่ง หลอกให้เป้าหมายเชื่อว่ากำลังสนทนาจริง ๆ อยู่ ส่วนมากจะโจมตีที่เครือข่าย



การหน่วงเวลา (Delay)

การยับยั้งไม่ให้ข้อมูลถึงตามกำหนดเวลาที่ควรจะเป็น ซึ่งการโจมตีแบบนี้ผู้บุกรุกต้องสามารถควบคุมระบบบางส่วนได้บ้าง เช่น สมมุติว่าผู้บุกรุกโจมตีเครื่องสำรองได้ แต่มีการทำงานของเครื่องหลักทำงานอยู่ จึงทำการโจมตีการส่งข้อมูลไปยังเครื่องหลักให้ดีเลย์ ผู้ใช้งานจะเข้าใจผิดว่าเครื่องหลักใช้งานไม่ได้และเปลี่ยนมาใช้เครื่องสำรองแทน

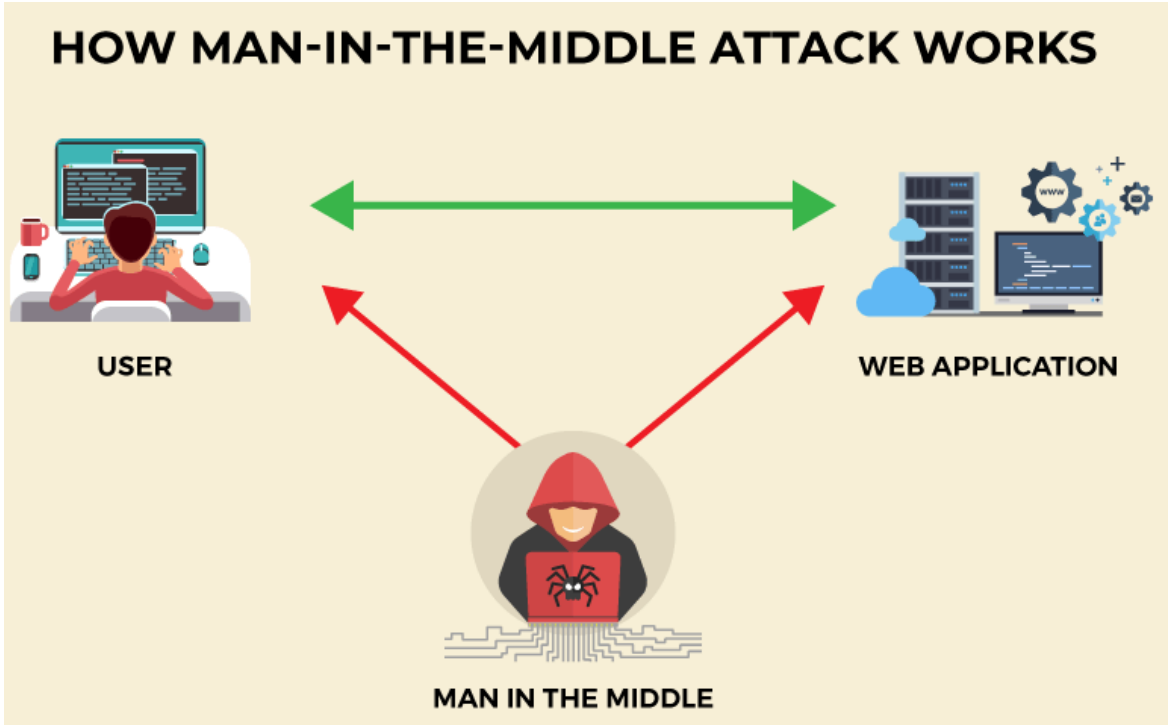


วิศวกรรมสังคม (Social Engineering)

วิชาทางจิตวิทยาแขนงหนึ่งมุ่งเน้นไปที่พฤติกรรมของสังคม ศึกษา ทำความเข้าใจ วิเคราะห์ วางแผน และออกแบบให้เกิดการกระทำพฤติกรรมตามแนวทางที่วางไว้ เช่น หลอกถามรหัสผ่าน หลอกให้กรอกรหัสผ่าน ฟิชชิง (Phishing)

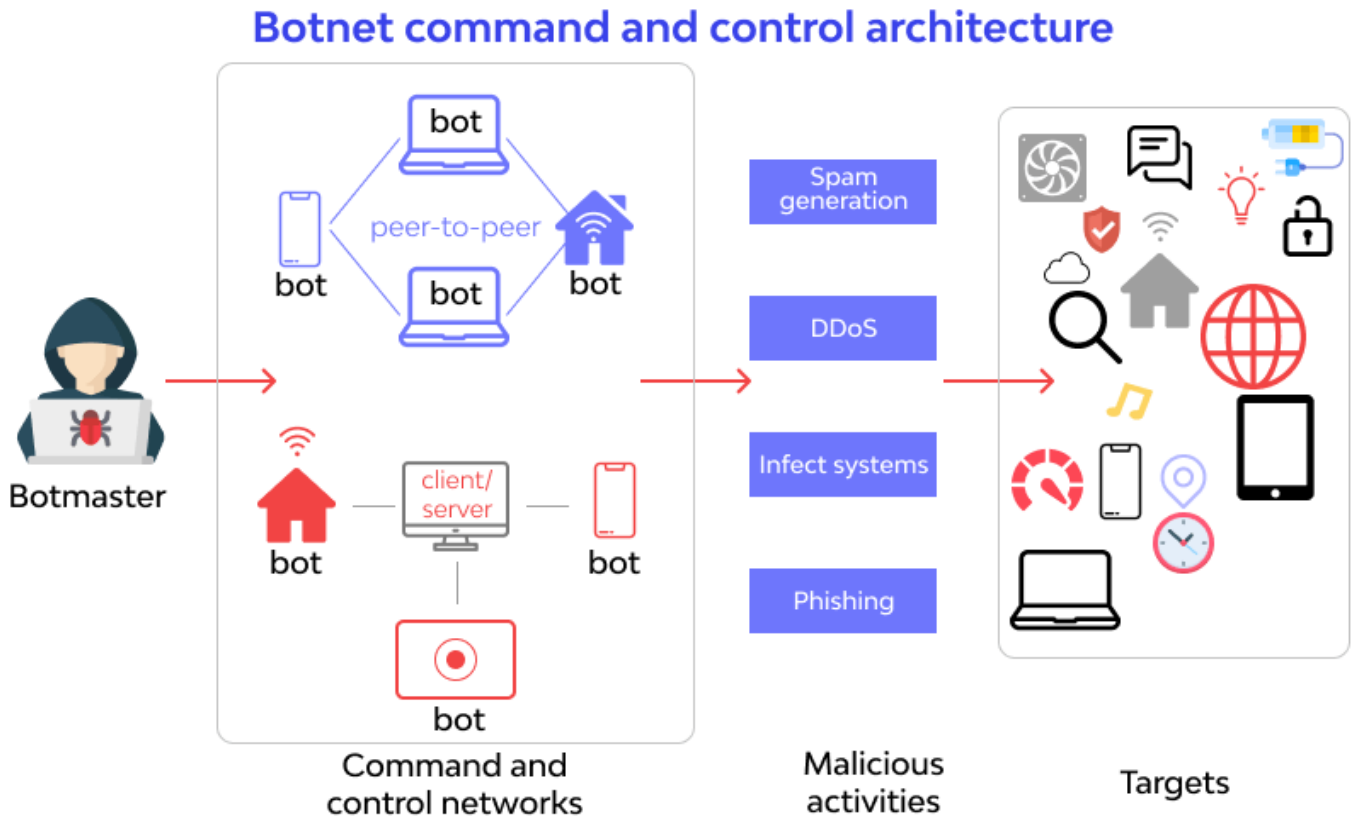
การโจมตีแบบคนกลาง (Man-in-the-middle Attack)

การโจมตี MitM เกี่ยวกับการดักฟังบนเครือข่าย เพียงเพื่อรับข้อมูลหรือส่งผลกระทบต่อธุรกรรม การสนทนา และการถ่ายโอนข้อมูลแบบเรียลไทม์ ผู้โจมตีสามารถทำได้ โดยใช้ประโยชน์จากจุดอ่อนในเครือข่าย



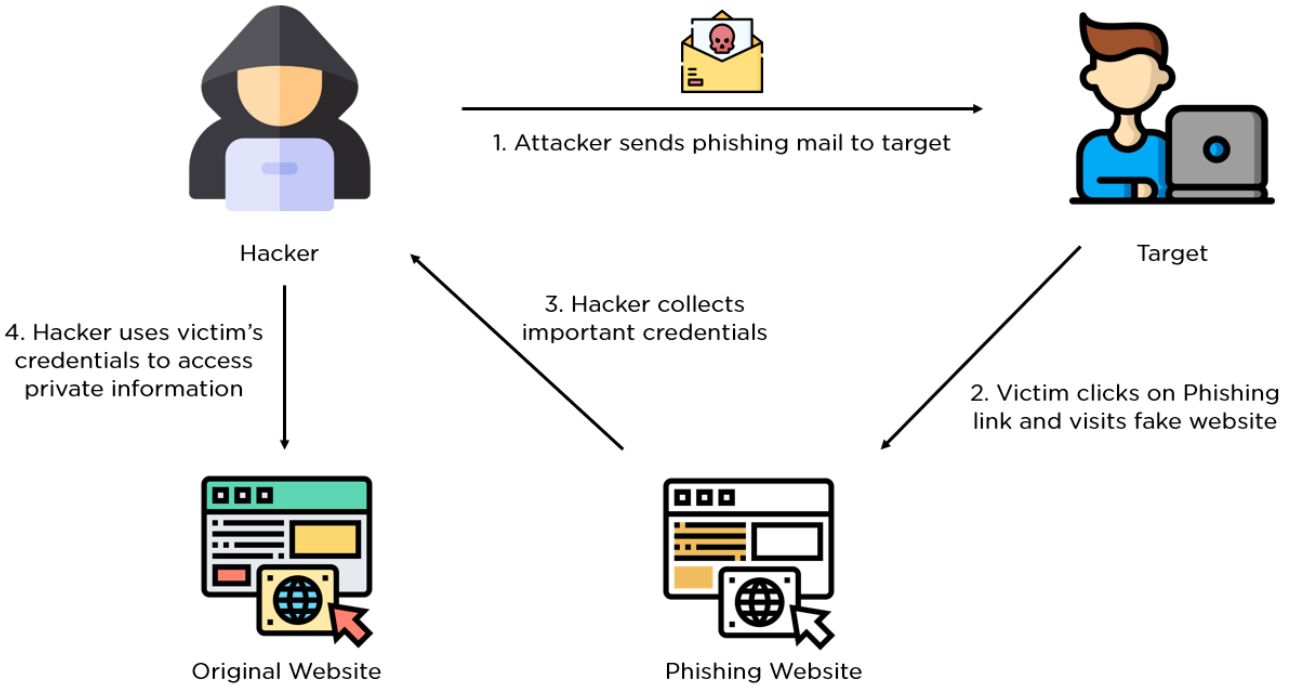
บอตเน็ต (Botnet)

Botnet เป็นกลุ่มของอุปกรณ์ที่ติดมัลแวร์และถูกเปลี่ยนเป็น Bot (ย่อมาจาก Robot) ไม่ว่าจะเป็นอุปกรณ์คอมพิวเตอร์ เว็บแคม เราท์เตอร์ หรืออุปกรณ์ IoT อื่นๆ ในบ้านของเรา เพื่อรอรับคำสั่งจากแฮ็กเกอร์ โดยแฮ็กเกอร์จะนำ Botnet ที่มีไปใช้ในแคมเปญการโจมตีขนาดใหญ่



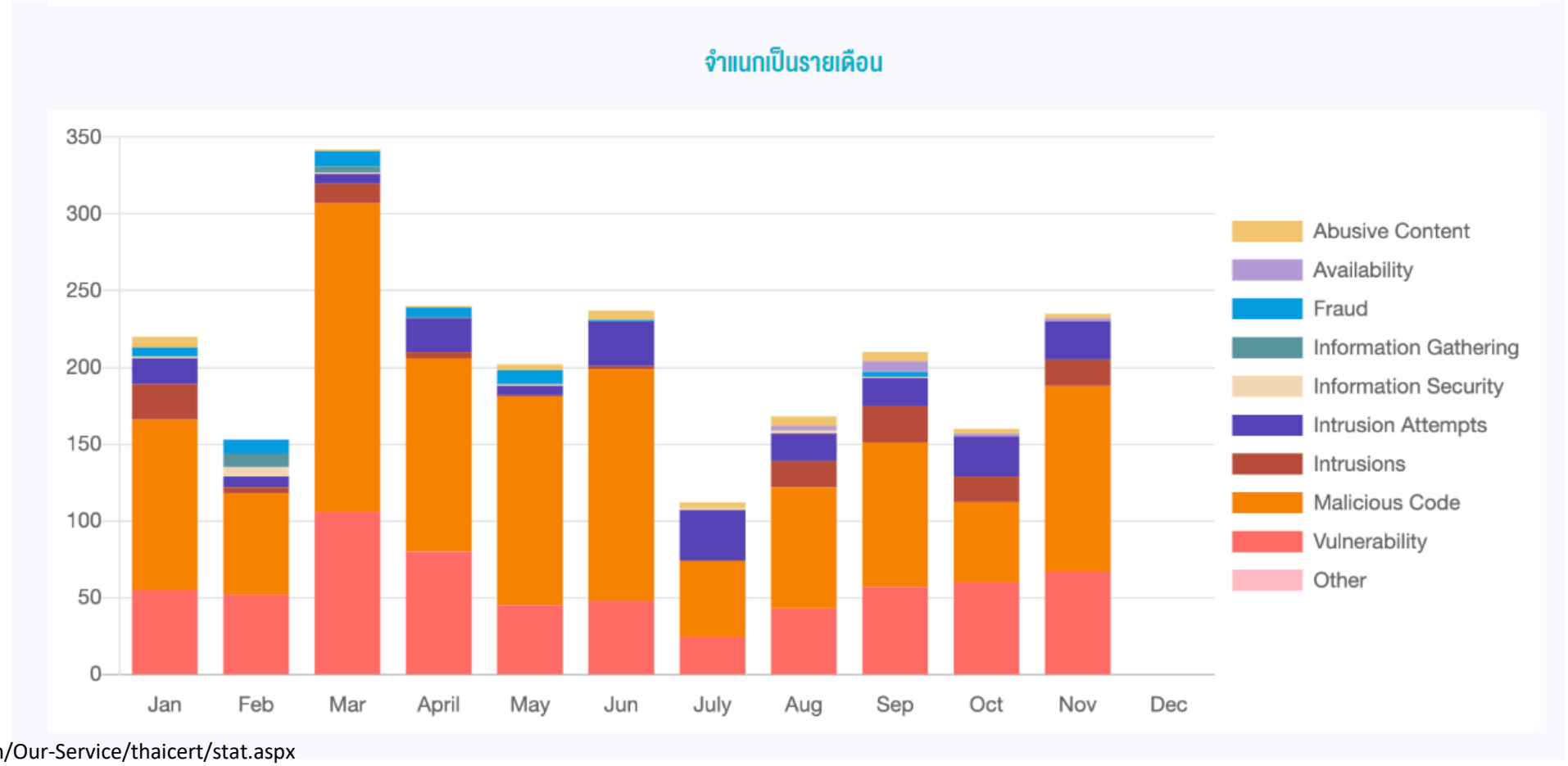
ฟิชชิง (Phishing)

การล้วงข้อมูลลับด้วยวิธีทางสังคม (Social Engineering) ด้วยการล่อลวงมาทางอีเมลล์ จากนั้นจะมีลิงค์ที่ดูเหมือนว่าจะนำไปสู่หน้า official website ของหน่วยงานนั้น ซึ่งหน้าตาของเว็บไซต์ปลายทางดูเผินๆ ก็เหมือน official website จริงๆ ซึ่งจะมีช่องให้คุณกรอกข้อมูลส่วนตัวต่างๆ ลงไป โดยเฉพาะเลขบัตรเครดิต



แนวโน้มภัยคุกคามในปัจจุบัน

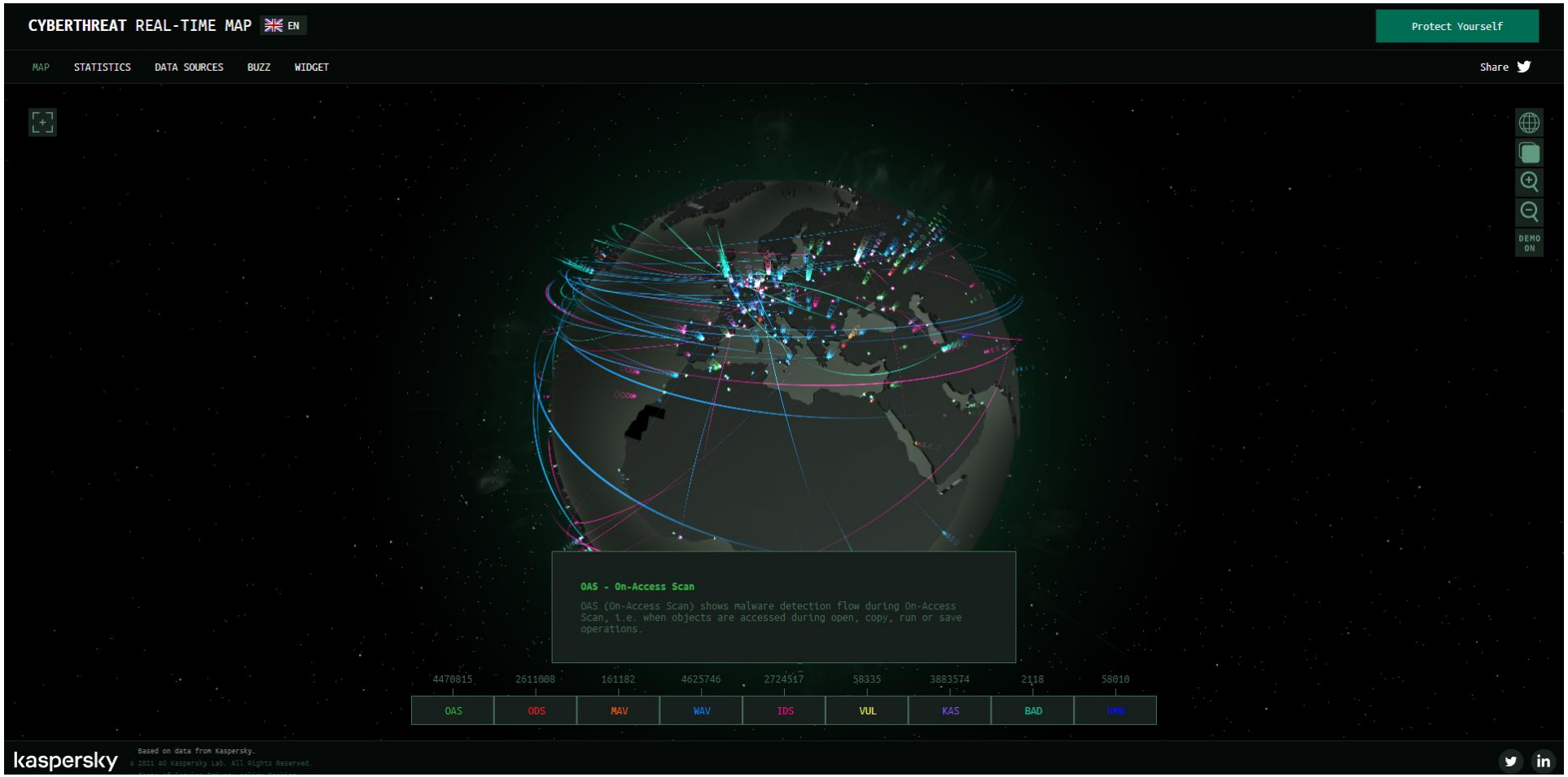
สถิติภัยคุกคาม ประจำปี พ.ศ. 2565



https://www.etda.or.th/th/Our-Service/thaicert/stat.aspx

แนวโน้มภัยคุกคามในปัจจุบัน

https://cybermap.kaspersky.com/



Malware

การโจมตีจากซอฟต์แวร์ที่ถูกพัฒนาขึ้นเพื่อทำลายความมั่นคงปลอดภัยของระบบคอมพิวเตอร์ เช่น

- ไวรัสคอมพิวเตอร์ (Virus)
- หนอนอินเทอร์เน็ต (Worm)
- โทรจัน (Trojan)
- ซอฟต์แวร์เรียกค่าไถ่ (Ransomware)

โดยซอฟต์แวร์เหล่านั้นมักมีความสามารถในการดักรับ ทำลาย ขโมย หรือจำกัดการเข้าถึงทรัพยากรสารสนเทศของผู้มีสิทธิ์ใช้งาน

GARMIN

TESLA

facebook

Canon

Malware : ประเภทของมัลแวร์

- Malware
- Trojan
- Worm
- Virus
- Backdoor
- Rootkits
- Scams
- Spam
- Spyware
- Adware