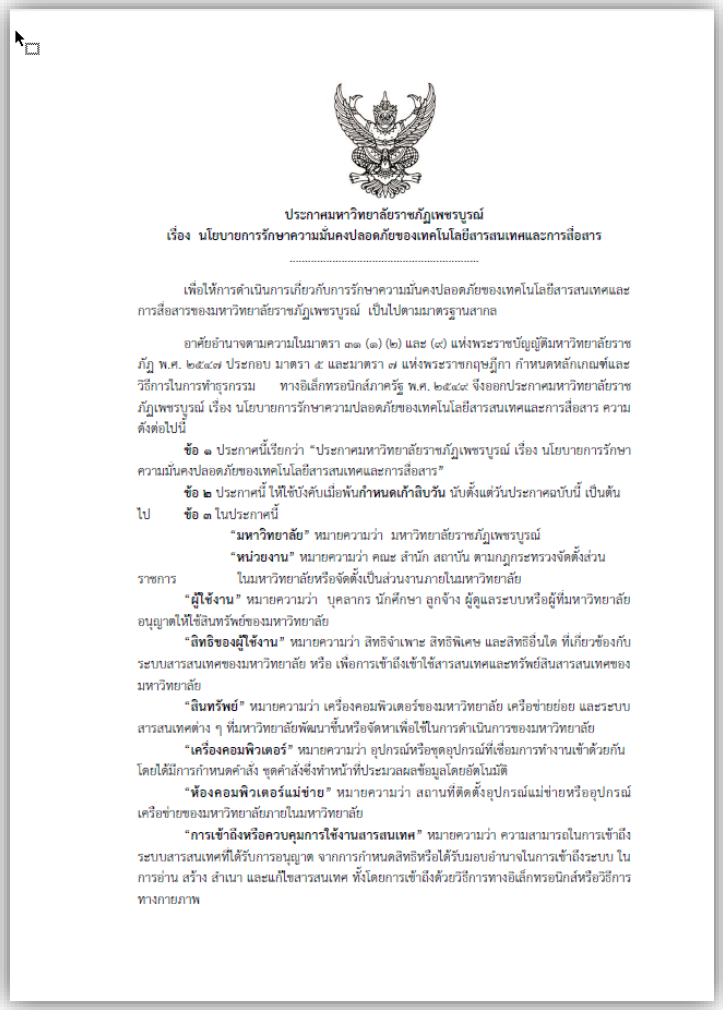
การรักษาความมั่นคงปลอดภัย ของเทคโนโลยีสารสนเทศและการสื่อสาร

ประกาศ
นโยบายการรักษาความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศและการสื่อสาร



ประกาศมหาวิทยาลัยราชภัฏเพชรบูรณ์
เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศและการสื่อสาร

.....

เพื่อให้การดำเนินการเกี่ยวกับการรักษาความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัยราชภัฏเพชรบูรณ์ เป็นไปตามมาตรฐานสากล

อาศัยอำนาจตามความในมาตรา ๓๑ (๑) (๒) และ (๙) แห่งพระราชบัญญัติมหาวิทยาลัยราชภัฏ พ.ศ. ๒๕๔๗ ประกอบ มาตรา ๕ และมาตรา ๗ แห่งพระราชกฤษฎีกา กำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรม ทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ จึงออกประกาศมหาวิทยาลัยราชภัฏเพชรบูรณ์ เรื่อง นโยบายการรักษาความปลอดภัยของเทคโนโลยีสารสนเทศและการสื่อสาร ความดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า "ประกาศมหาวิทยาลัยราชภัฏเพชรบูรณ์ เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศและการสื่อสาร"

ข้อ ๒ ประกาศนี้ ให้ใช้บังคับเมื่อพ้น**กำหนดเก้าสิบวัน** นับตั้งแต่วันประกาศฉบับนี้ เป็นต้นไป

ข้อ ๓ ในประกาศนี้

"**มหาวิทยาลัย**" หมายความว่า มหาวิทยาลัยราชภัฏเพชรบูรณ์

"**หน่วยงาน**" หมายความว่า คณะ สำนัก สถาบัน ตามกฎกระทรวงจัดตั้งส่วนราชการ ในมหาวิทยาลัยหรือจัดตั้งเป็นส่วนงานภายในมหาวิทยาลัย

"**ผู้ใช้งาน**" หมายความว่า บุคลากร นักศึกษา ลูกจ้าง ผู้ดูแลระบบหรือผู้ที่มหาวิทยาลัยอนุญาตให้ใช้สินทรัพย์ของมหาวิทยาลัย

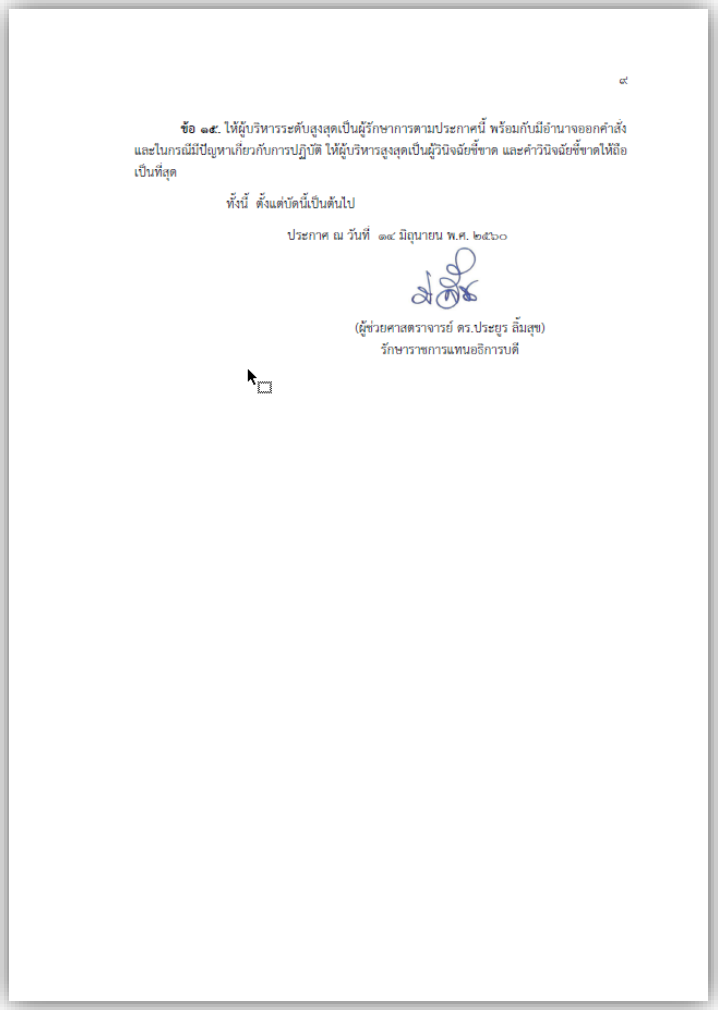
"**สิทธิของผู้ใช้งาน**" หมายความว่า สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใด ที่เกี่ยวข้องกับระบบสารสนเทศของมหาวิทยาลัย หรือ เพื่อการเข้าถึงเข้าใช้สารสนเทศและทรัพย์สินสารสนเทศของมหาวิทยาลัย

"**สินทรัพย์**" หมายความว่า เครื่องคอมพิวเตอร์ของมหาวิทยาลัย เครือข่ายย่อย และระบบสารสนเทศต่าง ๆ ที่มหาวิทยาลัยพัฒนาขึ้นหรือจัดหาเพื่อใช้ในการดำเนินการของมหาวิทยาลัย

"**เครื่องคอมพิวเตอร์**" หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่งซึ่งทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

"**ห้องคอมพิวเตอร์แม่ข่าย**" หมายความว่า สถานที่ติดตั้งอุปกรณ์แม่ข่ายหรืออุปกรณ์เครือข่ายของมหาวิทยาลัยภายในมหาวิทยาลัย

"**การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ**" หมายความว่า ความสามารถในการเข้าถึงระบบสารสนเทศที่ได้รับการอนุญาต จากการกำหนดสิทธิหรือได้รับมอบอำนาจในการเข้าถึงระบบ ในการอ่าน สร้าง สำเนา และแก้ไขสารสนเทศ ทั้งโดยการเข้าถึงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการทางกายภาพ



ข้อ ๑๕. ให้ผู้บริหารระดับสูงสุดเป็นผู้รักษาการตามประกาศนี้ พร้อมกับมีอำนาจออกคำสั่งและในกรณีมีปัญหาเกี่ยวกับการปฏิบัติ ให้ผู้บริหารสูงสุดเป็นผู้วินิจฉัยชี้ขาด และคำวินิจฉัยชี้ขาดให้ถือเป็นที่สุด

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

ประกาศ ณ วันที่ ๑๔ มิถุนายน พ.ศ. ๒๕๖๐

(ผู้ช่วยศาสตราจารย์ ดร.ประยูร ลิ้มสุข)
รักษาราชการแทนอธิการบดี

หัวใจของการดำเนินธุรกิจ

The Show Must Go On ไม่ว่าจะเกิดอะไรขึ้น ธุรกิจต้องดำเนินต่อไปให้ได้

การรักษาความปลอดภัยสารสนเทศ

ธุรกิจถูกขับเคลื่อนด้วย **IT**

เราถึงต้องให้ความสำคัญกับ “**การรักษาความมั่นคงปลอดภัยให้กับ IT**”

การรักษาความมั่นคงปลอดภัย ของเทคโนโลยีสารสนเทศและการสื่อสาร

1. ประวัติของการรักษาความปลอดภัย
2. องค์ประกอบหลักของความปลอดภัยข้อมูล
3. หลักการการรักษาความปลอดภัยข้อมูล
4. ภัยคุกคาม ช่องโหว่ การโจมตี มัลแวร์
5. เครื่องมือสำหรับการรักษาความปลอดภัย

ประวัติของการรักษาความปลอดภัย

พลังของข้อมูล

Big Data ชี้ชะตา! ใครคือผู้นำคนใหม่ของอเมริกา

IN FOCUS

- Big Data เป็นปัจจัยที่ขาดไม่ได้ในการวางกลยุทธ์หาเสียงเลือกตั้งในยุคที่สังคมออนไลน์เฟื่องฟู โดยเฉพาะการสื่อสารกับกลุ่มเป้าหมายแบบเจาะรายบุคคล
- การที่ บารัก โอบามา ชนะการเลือกตั้ง 2 สมัยติดต่อกัน โดยใช้โซเชียลมีเดีย และ Big Data เป็นเครื่องมือ กลายเป็นโมเดลการใช้สื่อใหม่ที่ได้รับความสนใจในกลุ่มนักการเมือง นักการตลาด และนักธุรกิจ แน่นอนว่าทีมหาเสียงของ โดนัลด์ ทรัมป์ และฮิลลารี คลินตัน พยายามเดินตามรอยความสำเร็จนี้เช่นกัน
- ผู้อยู่เบื้องหลังการจัดการ Big Data เพื่อคาดและวิเคราะห์ฐานเสียงของโดนัลด์ ทรัมป์ คือบริษัท Deep Root Analytics ส่วนของฮิลลารี คลินตัน คือบริษัท TargetSmart

ที่มา: https://themomentum.co/politicsx-big-data/

จุดเริ่มต้น...ของความมั่นคงปลอดภัยของสารสนเทศ

- สิ่งหนึ่งที่มีค่ามากที่สุดขององค์กรคือ **ข้อมูล หรือสารสนเทศ**
- การปกป้องรักษาข้อมูลเป็นสิ่งสำคัญในยุคแห่งข้อมูลข่าวสาร
- ***“ยุคที่ผู้ครอบครองสารสนเทศมากกว่าย่อมเป็นผู้ได้เปรียบ”***
- เกือบทุกองค์กรจำเป็นต้อง**เชื่อมต่อกับอินเทอร์เน็ต**
- **“อินเทอร์เน็ตเป็นดาบสองคม”**
- ข้อมูลมีความเสี่ยงที่จะถูกโจมตีจากหลายทาง
- จำเป็นต้องมีระบบรักษาความปลอดภัยที่แข็งแกร่ง

The History of Information Security

ความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security) มีจุดเริ่มมาจาก

- **ยุคสมัยแรก** มีความต้องการให้คอมพิวเตอร์มีความปลอดภัย (Computer Security) ซึ่งสาเหตุส่วนใหญ่เป็น **ภัยคุกคามทางกายภาพ** เช่น การลักขโมยอุปกรณ์ การก่อวินาศกรรม การโจรกรรมผลผลิตที่ได้จากระบบ เป็นต้น

The History of Information Security

ความมั่นคงปลอดภัยของระบบสารสนเทศ (Information Security) มีจุดเริ่มมาจาก

- **ยุคสมัยต่อมา** เมื่อเทคโนโลยีคอมพิวเตอร์ (Software, Hardware, Data/Information, Network/Communication) มีความก้าวหน้ามากขึ้นจึง**เกิดภัยคุกคามหลากหลายรูปแบบ** เช่น การโจรกรรมข้อมูลที่เป็นความลับ การลักลอบเข้าสู่ระบบโดยไม่ได้รับอนุญาต ตลอดจนการทำลายระบบด้วยวิธีต่าง ๆ ซึ่งก่อให้เกิดความเสียหายทั้งต่อบุคคลและทรัพย์สินอย่างมาก

การรักษาความมั่นคงปลอดภัยของสารสนเทศ

- ด้านกายภาพ (Physical Security)
- ด้านการสื่อสาร (Communication Security)
- คอมพิวเตอร์ (Computer Security)
- เครือข่าย (Network Security)
- สารสนเทศ (Information Security)

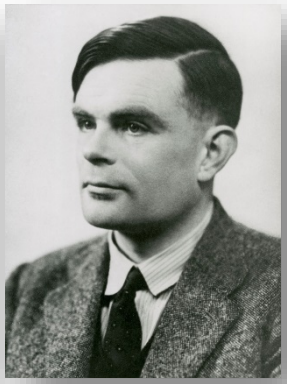
การรักษาความปลอดภัยด้านกายภาพ (Physical Security)

- ในอดีตข้อมูลสำคัญจะอยู่ในรูปวัตถุที่จับต้องได้ เช่น แผ่นหิน แผ่นหนัง กระดาษ
- ใช้การป้องกันทางกายภาพ เช่น กำแพง ปราสาท ยาม ผู้คุ้มกันคนนำสาสน์
- คนในอดีตไม่นิยมบันทึกข้อมูลสำคัญลงบนสื่อถาวร และจะสนทนาข้อมูลสำคัญกับบุคคลที่ไว้ใจได้เท่านั้น
- ซุนวู กล่าวว่า ***“ความลับที่รู้โดยคนมากกว่าหนึ่งคนย่อมไม่ถือว่าเป็นความลับอีกต่อไป”***

การรักษาความปลอดภัยด้านการสื่อสาร (Communication Security)

- ในยุค **จูเลียส์ ซีซาส์** ได้มีการคิดค้นวิธีการซ่อนข้อมูลโดยการเข้ารหัส (Encryption) ถ้ามีการขโมยข้อมูลระหว่างทาง ผู้อ่านจะไม่เข้าใจถ้าไม่รู้วิธีถอดรหัส
- ในสงครามโลกครั้งที่สอง **เยอรมันใช้เครื่องมือ Enigma** สำหรับเข้ารหัสข้อมูลทางการทหาร ซึ่งเยอรมันเชื่อว่าไม่มีใครสามารถถอดรหัสจากเครื่องนี้ได้ แต่ในที่สุดฝ่ายพันธมิตรก็สามารถถอดรหัสได้ โดย **Alan Turing** ซึ่งได้ถูกสร้างเป็นภาพยนตร์ฮอลลีวู้ด ชื่อว่า The Imitation Game ในปี 2014

จูเลียส์ ซีซาส์



Alan Turing

เครื่องเข้าและถอดรหัสสารลับ **Enigma**

การรักษาความปลอดภัยด้านการสื่อสาร (Communication Security)

การเข้ารหัสเพื่อป้องกันข้อมูล

- Cipher คือ รหัสลับ เครื่องหมายลับ หรือ สัญลักษณ์ลับ ซึ่งเป็นการเข้ารหัสลับอย่างหนึ่งของการสื่อสารข้อความในสมัยสงครามโลก ที่ไม่ต้องการให้บุคคลใด ๆ ล่วงรู้ถึงข้อความที่เป็นจริง
- Cryptex เป็นอุปกรณ์เก็บความลับชนิดที่ยากต่อการงัดแงะ และถอดรหัส โดยผู้ใช้ต้องรู้รหัสในการเปิดล็อคอุปกรณ์ชิ้นดังกล่าว จึงจะนำข้อมูลข้างในออกมาได้

การรักษาความปลอดภัยด้านการสื่อสาร (Communication Security)

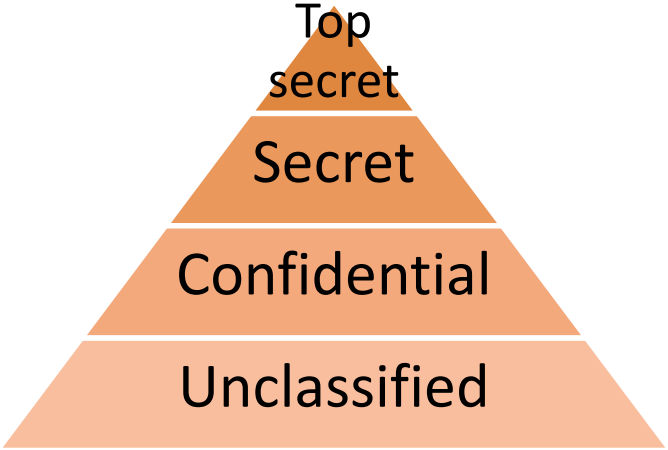
การเข้ารหัสเพื่อป้องกันข้อมูล

- Navajo Code Talker คือภาษา Navajo ที่ใช้ในการสื่อสารระหว่างหน่วยต่างๆ ซึ่งเป็นภาษาที่คนใช้น้อย และมีความซับซ้อนสูง

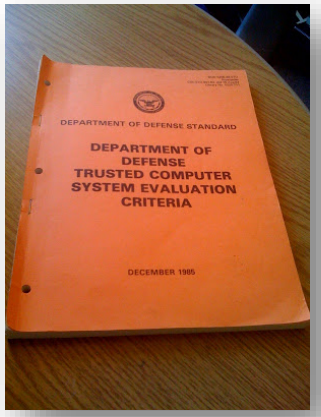
- One Time Pad คือ การเข้ารหัสแบบ cipher text ที่ไม่มีทาง decrypt ได้ เนื่องจากว่า key ที่ใช้นั้นไม่มีการใช้ซ้ำเลย

การรักษาความปลอดภัยคอมพิวเตอร์ (Computer Security)

- ทศวรรษ 1970 David Elliott Bell and Leonard La Padula มีการพัฒนาแม่แบบสำหรับการรักษาความปลอดภัยของคอมพิวเตอร์ โดยแบ่ง**ระดับความปลอดภัยเป็น 4 ระดับ** ผู้ที่สามารถเข้าถึงข้อมูลในระดับใดระดับหนึ่ง จะต้องมีสิทธิ์เท่ากับหรือสูงกว่าชั้นความลับของข้อมูลนั้น
- ปี 1985 กระทรวงกลาโหมสหรัฐ นำแนวคิดไปใช้เรียกว่ามาตรฐาน Trusted Computing System Evaluation Criteria (TCSEC) หรือ Orange Book



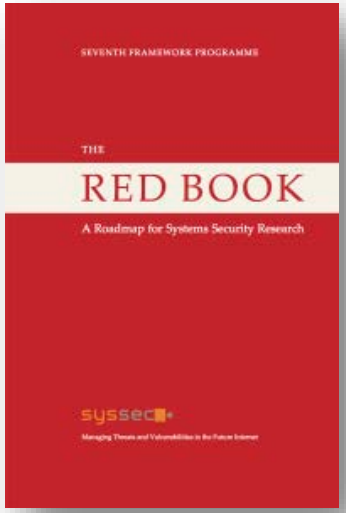
ระดับความปลอดภัยแบ่งเป็น 4 ระดับ



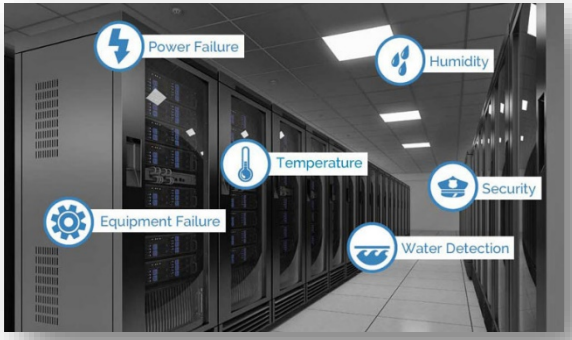
Orange book

การรักษาความปลอดภัยเครือข่าย (Network Security)

- เมื่อคอมพิวเตอร์ถูกเชื่อมต่อกันเป็นเครือข่ายก็เกิดปัญหาใหม่ขึ้น เช่น อาจมีหลายเครื่องที่เชื่อมต่อเข้ากับสื่อเดียวกัน ทำให้การเข้ารหัสโดยใช้เครื่องเข้ารหัสเดี่ยวๆอาจไม่ได้ผล
- ในปี 1987 มีการพัฒนามาตรฐาน เกี่ยวกับเครือข่าย Trusted Network Interpretation (TNI) โดยพัฒนาต่อมาจาก Orange Book ซึ่งรู้จักกันในชื่อ Red Book ซึ่งได้เพิ่มส่วนเกี่ยวข้องกับเครือข่ายเข้าไป และหลังจากนั้น ได้มีมาตรฐาน ISO/IEC 18028 ทางด้าน Network Security



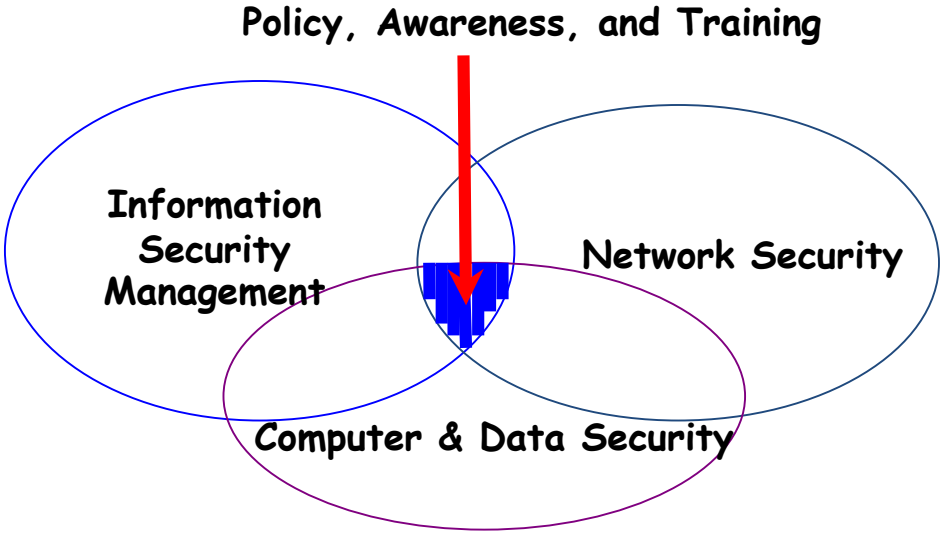
การรักษาความปลอดภัยสารสนเทศ (Information Security)



- การเก็บรวบรวมข้อมูลสารสนเทศจะถูกเก็บเป็นไฟล์ และมีการจัดทำระบบข้อมูลส่วนกลางขององค์กร
- สามารถเข้าถึงระบบข้อมูลได้ โดยผ่านทางระบบเครือข่ายคอมพิวเตอร์
- เป็นเหตุให้ระบบข้อมูลถูกบุกรุกจากผู้ไม่ประสงค์ดีได้ง่าย นอกจากนี้ระบบคอมพิวเตอร์ยังต้องเผชิญกับภัยคุกคาม (Threat) ต่าง ๆ ได้ง่ายกว่าข้อมูลในรูปแบบเอกสารอีกด้วย
- ดังนั้นความปลอดภัยข้อมูลในระบบคอมพิวเตอร์จึงขึ้นอยู่กับความปลอดภัยทุกด้านประกอบกัน

องค์ประกอบหลักของความปลอดภัยสารสนเทศ

องค์ประกอบหลักความมั่นคงปลอดภัยของสารสนเทศ (Information Security)



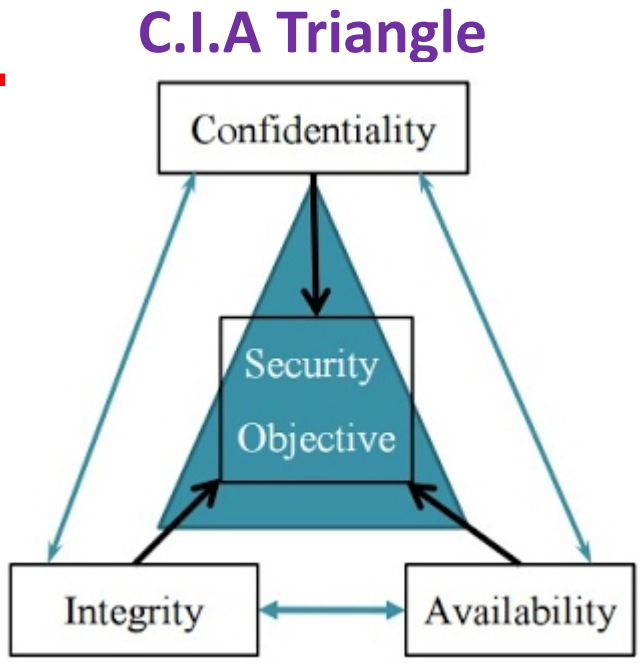
- **ความมั่นคงปลอดภัยของข้อมูลและคอมพิวเตอร์** (Computer and Data Security)
- **ความมั่นคงปลอดภัยของเครือข่าย** (Network Security)
- **การจัดการความมั่นคงปลอดภัยของสารสนเทศ** (Information Security Management)

การที่จะสร้างความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ ต้องดำเนินการทุกส่วนร่วมกัน เพื่อ**กำหนดนโยบาย (Policy) สร้างความตระหนักในความมั่นคง (Awareness)** และ**จัดหลักสูตรฝึกอบรม (Training)** ให้เกิดการเรียนรู้ในเรื่องความมั่นคงปลอดภัยและเทคโนโลยีที่เกี่ยวข้อง

แนวคิดหลักของความมั่นคงปลอดภัยของสารสนเทศ

กลุ่มอุตสาหกรรมความมั่นคงปลอดภัยของคอมพิวเตอร์ ได้กำหนดแนวคิดหลักของความมั่นคงปลอดภัยของคอมพิวเตอร์ขึ้นเรียกว่า **“C.I.A Triangle”** ประกอบด้วย

1. ความลับ (Confidentiality)
2. ความสมบูรณ์ (Integrity)
3. ความพร้อมใช้ (Availability)



แนวคิดหลักของความมั่นคงปลอดภัยของสารสนเทศ

1. ความลับ (Confidentiality)

การอนุญาตให้เฉพาะผู้ที่ได้รับอนุญาตเข้าถึงข้อมูลได้เท่านั้น **กลไกที่ใช้รักษาความลับคือ**

- ***การเข้ารหัสข้อมูล*** **(Cryptography หรือ Encryption)** หากบุคคลอื่นสามารถถอดรหัสได้ แสดงว่าความลับถูกทำลาย (Compromised)
- ***กลไกควบคุมการเข้าถึง*** **(Access Control)** จะพิสูจน์ทราบว่าผู้ที่เข้ามาใช้งานระบบ ได้รับอนุญาตหรือไม่ เช่น login

"หากท่านต้องการส่งข้อความที่ปกปิดหรือเป็นความลับผ่านเครือข่าย ท่านจะมั่นใจได้อย่างไรว่าบุคคลที่ท่านประสงค์จะส่งถึงหรือที่ได้รับอนุญาตเท่านั้น ที่สามารถอ่านข้อความได้"

องค์กรต้องมีมาตรการป้องกันการเข้าถึงสารสนเทศที่เป็นความลับ เช่น

- การจัดประเภทของสารสนเทศ
- การรักษาความปลอดภัยในกับแหล่งจัดเก็บข้อมูล
- กำหนดนโยบายรักษาความมั่นคงปลอดภัยและนำไปใช้
- ให้การศึกษาแก่ทีมงานความมั่นคงปลอดภัยและผู้ใช้

แนวคิดหลักของความมั่นคงปลอดภัยของสารสนเทศ

2. ความสมบูรณ์ คงสภาพ (Integrity)

คือ ความเชื่อถือได้ของข้อมูลหรือแหล่งที่มา หรือการป้องกันไม่ให้ข้อมูลถูกเปลี่ยนแปลงไปจากเดิม

- ความถูกต้องของ**เนื้อหา**ข้อมูล
- ความถูกต้องของ**แหล่งที่มา**ของข้อมูล

กลไกในการรักษาความคงสภาพของข้อมูลมี 2 ส่วน

- **การป้องกัน (Prevention)**
  - ป้องกันการเปลี่ยนแปลงที่เกิดจากผู้ที่ไม่ได้รับอนุญาต
  - ผู้ที่ได้รับอนุญาตพยายามแก้ไขข้อมูลนอกเหนือจากสิทธิ์ที่มี
- **การตรวจสอบ (Detection)** ตรวจสอบว่าข้อมูลยังคงมีความน่าเชื่อถืออยู่หรือไม่

“หากท่านได้รับข้อความที่ส่งมาถึงท่านผ่านทางเครือข่าย ท่านจะแน่ใจได้อย่างไรว่าข้อความที่ท่านได้รับเป็นข้อความที่ถูกต้องแท้จริง ไม่ได้ถูกเปลี่ยนแปลงแก้ไขระหว่างทาง”

สารสนเทศจะขาดความสมบูรณ์ ก็ต่อเมื่อสารสนเทศนั้นถูกนำไปเปลี่ยนแปลง ปลอมปนด้วยสารสนเทศอื่น ถูกทำให้เสียหาย ถูกทำลาย หรือถูกกระทำในรูปแบบอื่น ๆ

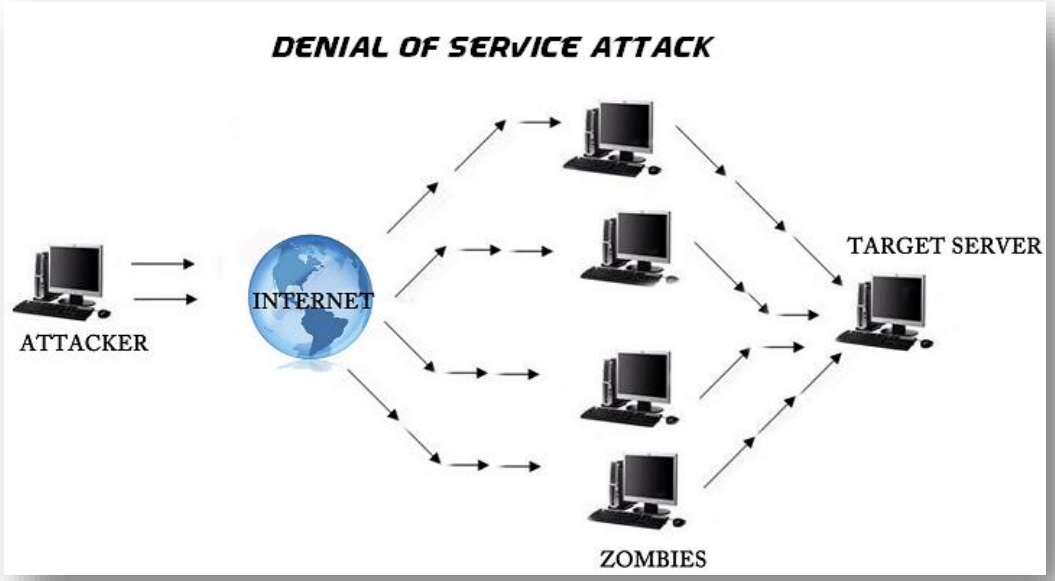
เช่น ข้อมูลถูกทำให้เสียหาย ไฟล์หาย เนื่องจาก Virus และ Worm หรือ Hacker สร้างความเสียหายให้กับข้อมูลองค์กรได้ เช่น แก้ไขยอดเงินในบัญชีธนาคาร หรือ แก้ไขราคาในการสั่งซื้อ หรือทำการแก้ไขเกรดนักศึกษา

แนวคิดหลักของความมั่นคงปลอดภัยของสารสนเทศ

3. ความพร้อมใช้ (Availability)

- ความสามารถในการใช้ข้อมูลหรือทรัพยากรเมื่อต้องการ

กลไกการรักษาความพร้อมใช้งาน *จะทำงานในกรณีที่ระบบทำงานไม่ได้ในสภาพปกติที่ออกแบบไว้ เช่น การมีระบบสำรอง* ความพยายามทำลายความพร้อมใช้งาน เรียกว่า **การโจมตีแบบปฏิเสธการให้บริการ** (Denial of Service : DOS)



แนวคิดหลักของความมั่นคงปลอดภัยของสารสนเทศ

นอกจากองค์ประกอบของความปลอดภัยของข้อมูลทั้ง 3 ส่วนแล้วยังมีคุณสมบัติอื่นๆเกี่ยวกับการรักษาความปลอดภัย

- ความเป็นส่วนตัว Privacy
- การระบุตัวตน Identification
- การพิสูจน์ทราบตัวตน Authentication
- การอนุญาตใช้งาน Authorization
- การตรวจสอบได้ Accountability

แนวคิดหลักของความมั่นคงปลอดภัยของสารสนเทศ

ความเป็นส่วนตัว (Privacy)

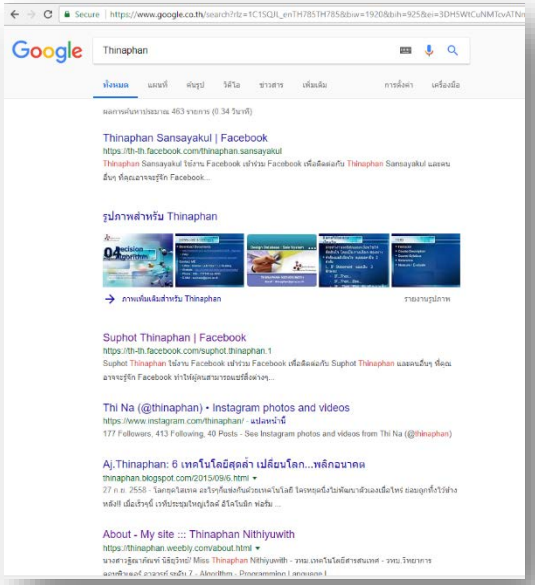
ความเป็นส่วนตัว หมายถึง สิทธิส่วนตัวของบุคคล หน่วยงาน หรือองค์กรที่จะคงไว้ซึ่งสารสนเทศที่มีอยู่นั้น เพื่อตัดสินใจได้ว่าจะสามารถเปิดเผยให้ผู้อื่นนำไปใช้ประโยชน์ต่อหรือเผยแพร่ได้หรือไม่ เราอาจพบเห็นการละเมิดความเป็นส่วนตัวโดยทั่วไป เช่น

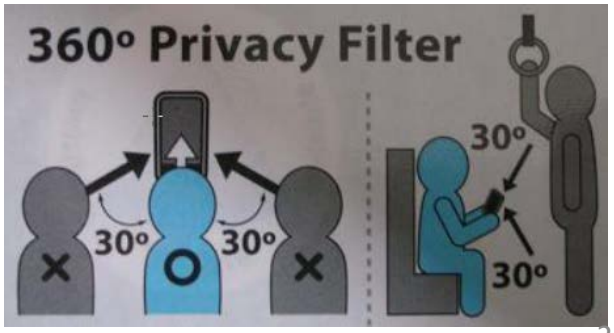
- ใช้โปรแกรมติดตามและสำรวจพฤติกรรมผู้ที่ใช้งานบนเว็บไซต์
- การเอาฐานข้อมูลส่วนตัวรวมถึงอีเมล์ของสมาชิกส่งไปให้กับบริษัทผู้รับทำโฆษณา
- การใช้กล้องวงจรปิดตรวจสอบดูพฤติกรรมการทำงานของลูกจ้าง

แนวคิดหลักของความมั่นคงปลอดภัยของสารสนเทศ

ความเป็นส่วนตัว (Privacy)

- เคยค้นชื่อตัวเองใน google ?

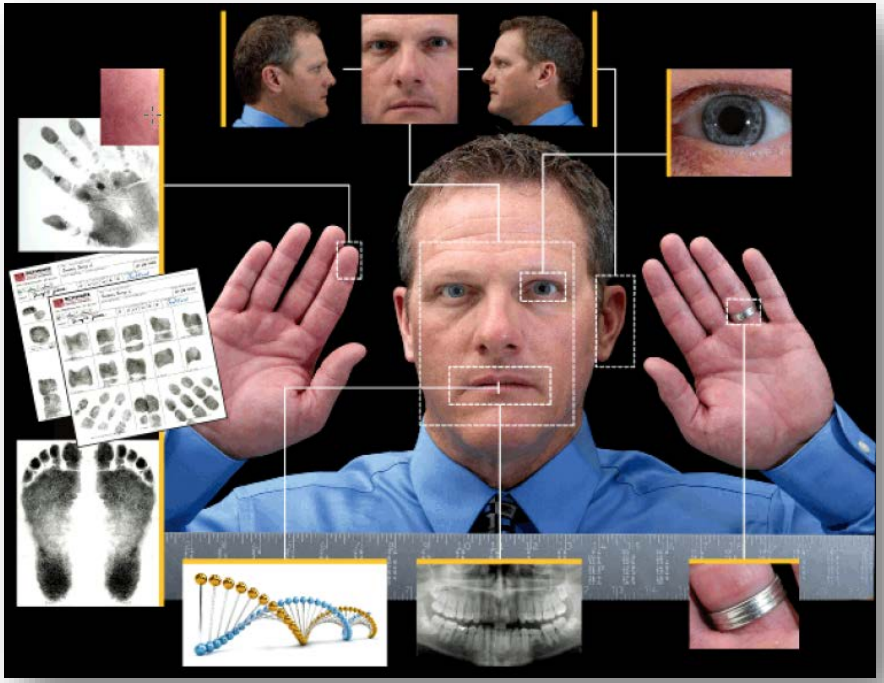




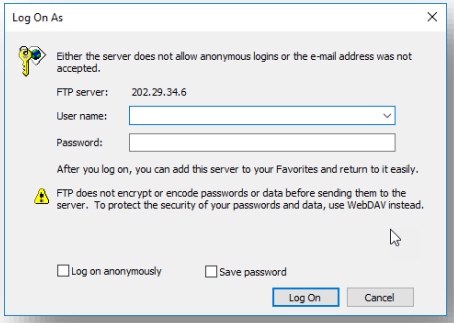
แนวคิดหลักของความมั่นคงปลอดภัยของสารสนเทศ

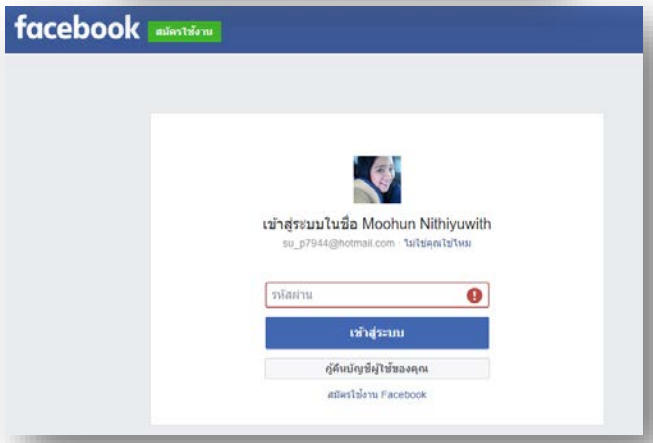
การระบุตัวตน (Identification)

คือ ขั้นตอนที่ผู้ใช้แสดงหลักฐานว่าตนเองคือใคร เช่น Username, ลายนิ้วมือ



Biometric Platform

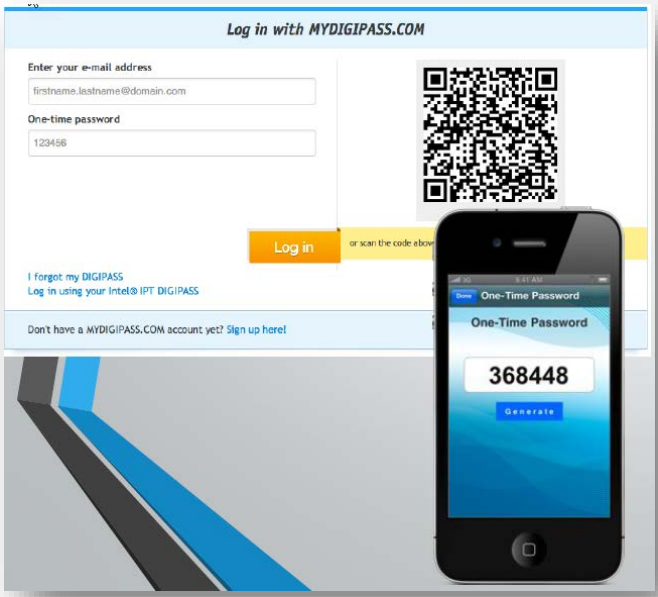




แนวคิดหลักของความมั่นคงปลอดภัยของสารสนเทศ

การพิสูจน์ตัวตน (Authentication)

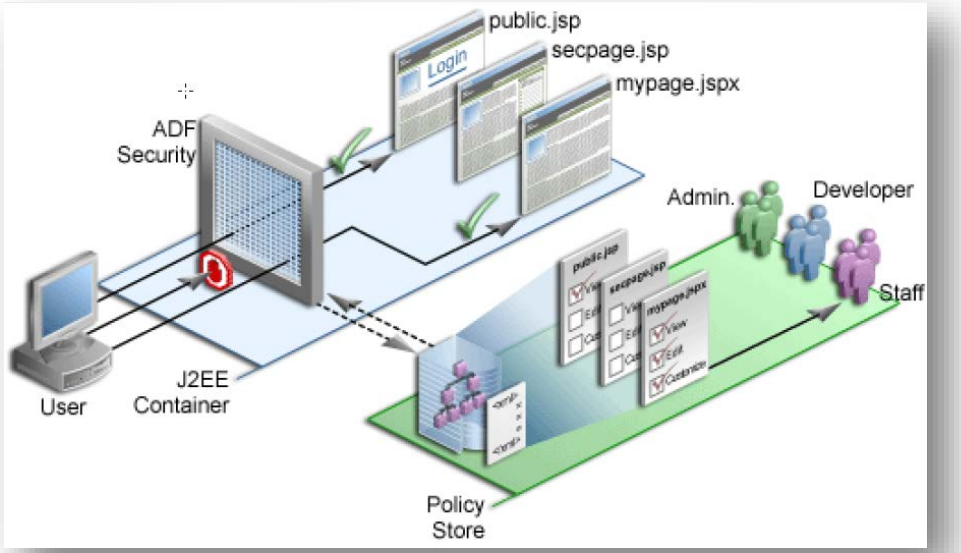
คือขั้นตอนที่ตรวจสอบหลักฐานเพื่อแสดงว่าเป็นบุคคลที่กล่าวอ้างจริง เช่น Password



แนวคิดหลักของความมั่นคงปลอดภัยของสารสนเทศ

การอนุญาตใช้งาน (Authorization)

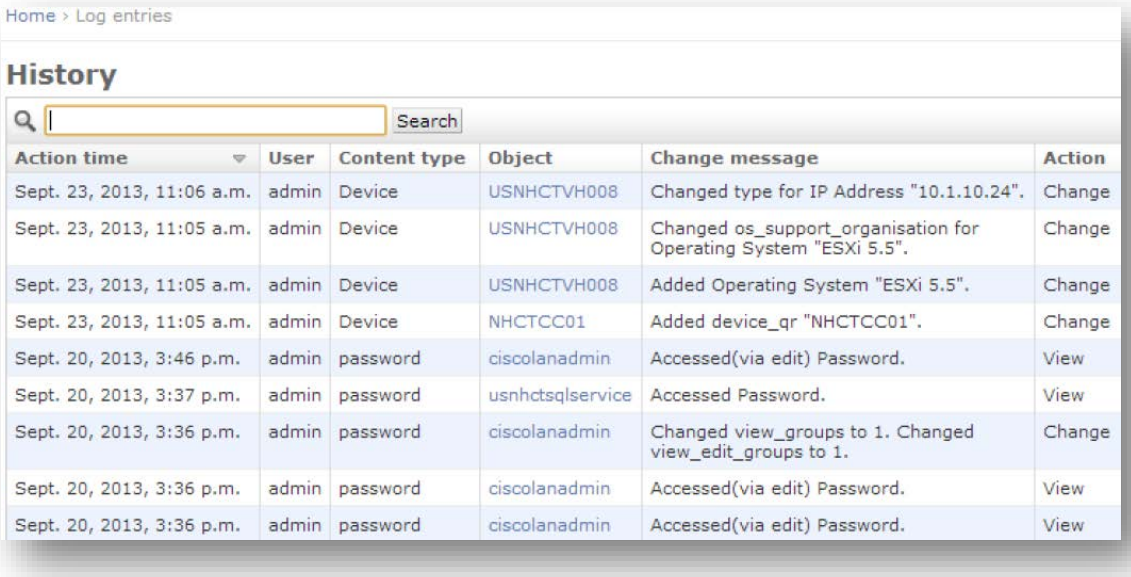
หลังจากที่ระบุตัวต้น ใส่ Username และผ่านการพิสูจน์ทราบตัวตนโดยการใส่ Password หลังจากนั้นคือการอนุญาตใช้งาน (Authorization) ว่า สามารถเข้าถึงอ่าน แก้ไขข้อมูลตามรายการเข้าถึงของกลุ่มผู้ใช้นั้นๆ Access Control List (ACL)



แนวคิดหลักของความมั่นคงปลอดภัยของสารสนเทศ

การตรวจสอบได้ (Accountability)

เป็นอีกส่วนสำคัญในการรับรองว่าทุกกิจกรรมสามารถตรวจสอบได้ว่าเกิดขึ้นเพราะใคร เช่น การเก็บ Log หรือ การทำ History Data


Home › Log entries

History

Search

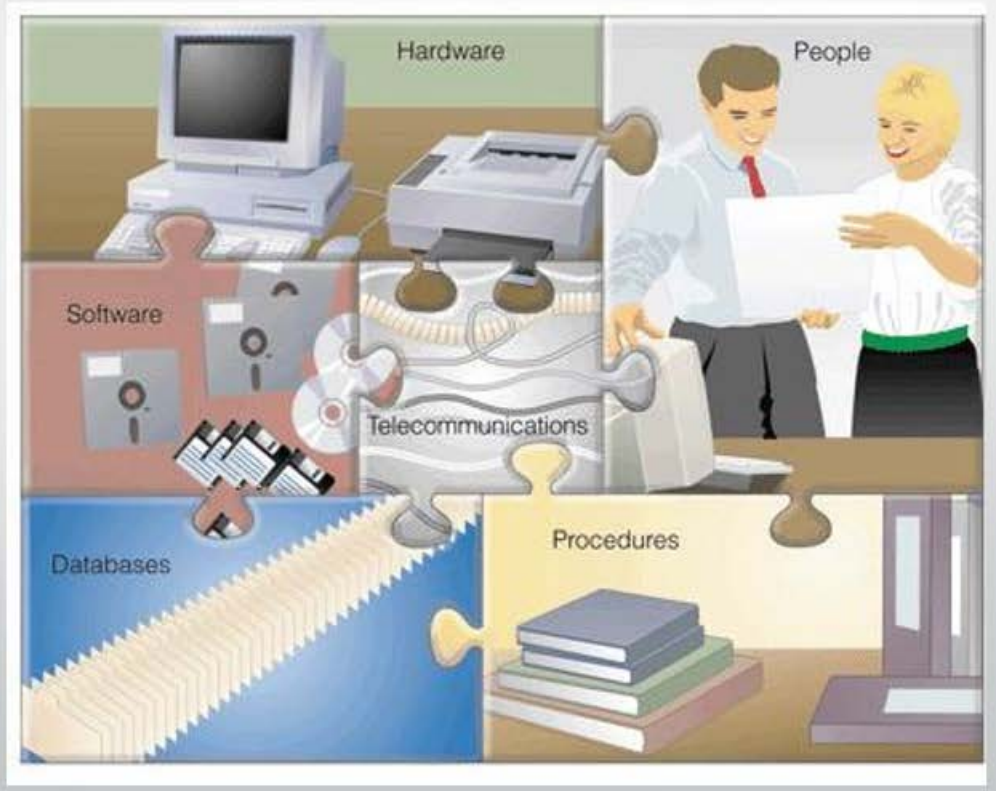
Action time	User	Content type	Object	Change message	Action
Sept. 23, 2013, 11:06 a.m.	admin	Device	USNHCTVH008	Changed type for IP Address "10.1.10.24".	Change
Sept. 23, 2013, 11:05 a.m.	admin	Device	USNHCTVH008	Changed os_support_organisation for Operating System "ESXi 5.5".	Change
Sept. 23, 2013, 11:05 a.m.	admin	Device	USNHCTVH008	Added Operating System "ESXi 5.5".	Change
Sept. 23, 2013, 11:05 a.m.	admin	Device	NHCTCC01	Added device_qr "NHCTCC01".	Change
Sept. 20, 2013, 3:46 p.m.	admin	password	ciscolanadmin	Accessed(via edit) Password.	View
Sept. 20, 2013, 3:37 p.m.	admin	password	usnhctsqlservice	Accessed Password.	View
Sept. 20, 2013, 3:36 p.m.	admin	password	ciscolanadmin	Changed view_groups to 1. Changed view_edit_groups to 1.	Change
Sept. 20, 2013, 3:36 p.m.	admin	password	ciscolanadmin	Accessed(via edit) Password.	View
Sept. 20, 2013, 3:36 p.m.	admin	password	ciscolanadmin	Accessed(via edit) Password.	View

- What
- When
- Where
- Why
- Who
- How

แนวคิดหลักของความมั่นคงปลอดภัยของสารสนเทศ

องค์ประกอบของระบบสารสนเทศกับความมั่นคงปลอดภัย

- Software
- Hardware
- Data
- People
- Procedure
- Network



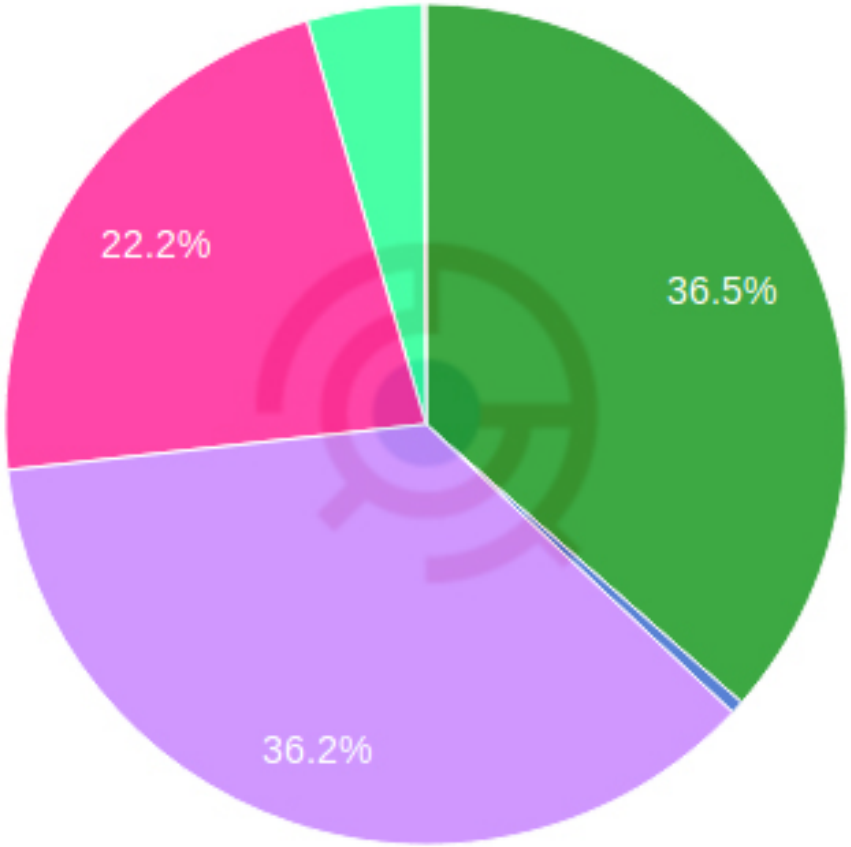
ภัยคุกคาม ช่องโหว่ การโจมตี มัลแวร์

ภัยคุกคาม (Threat)

หมายถึง สิ่งที่อาจจะก่อให้เกิดความเสียหายต่อคุณสมบัติของข้อมูลด้านใดด้านหนึ่งหรือมากกว่าหนึ่งด้าน

- **การโจมตี (Attack)** คือ การกระทำที่อาจก่อให้เกิดความเสียหาย
- **ผู้โจมตี” (Attacker)** คือผู้ที่กระทำเหตุการณ์ที่ก่อให้เกิดความเสียหาย หรือเรียกอีกอย่างว่า**“แฮคเกอร์” (Hacker)** หรือ **“แคร็คเกอร์” (Cracker)**

สถิติภัยคุกคามปี 2561



- Fraud (36.5%) — การฉ้อฉล ฉ้อโกงหรือหลอกลวง
- Information Security (0.5%) — การเข้าถึงหรือเปลี่ยนแปลงแก้ไขข้อมูลสำคัญโดยไม่ได้รับอนุญาต
- Intrusion Attempts (36.2%) — ความพยายามจะบุกรุกเข้าระบบ
- Intrusion (22.2%) — การบุกรุกหรือเจาะระบบได้สำเร็จ
- Malicious Code (4.4%) — โปรแกรมไม่พึงประสงค์
- Other (0.2%) — ภัยคุกคามอื่นๆ

ที่มา : https://www.thaicert.or.th/statistics/statistics.html

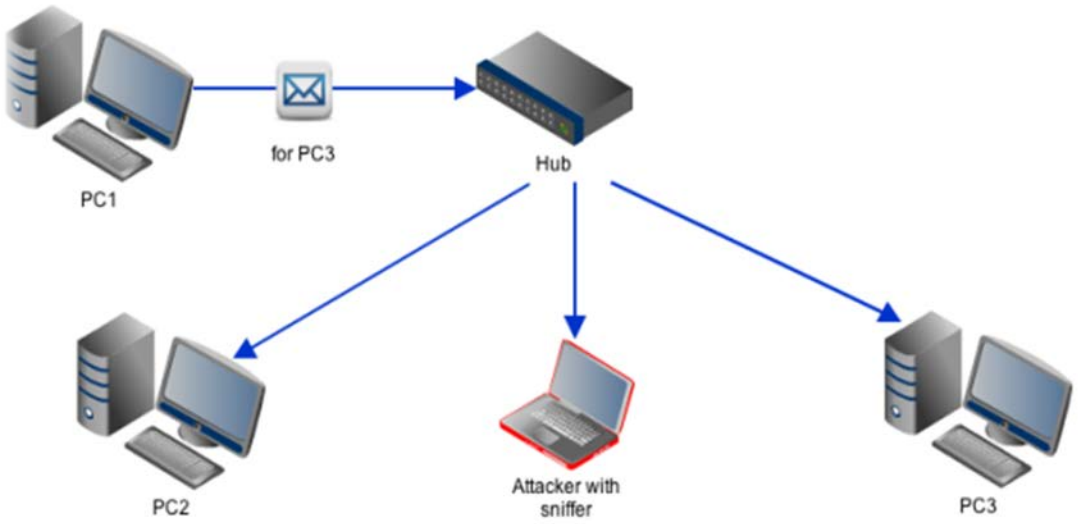
ประเภทของภัยคุกคาม

ภัยคุกคามที่อาจเกิดขึ้นกับข้อมูล (Information Threat)

การเปิดเผย (Disclosure)	• การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต และข้อมูลนั้นถูกเปิดเผยให้กับผู้ไม่ได้รับอนุญาต
การหลอกลวง (Deception)	• การให้ข้อมูลที่เป็นเท็จ
การขัดขวาง (Disruption)	• การทำลายข้อมูล หรือกันไม่ให้กระทำต่อข้อมูลอย่างถูกต้อง
การควบคุมระบบ (Usurpation)	• การเข้าควบคุมระบบบางส่วนหรือทั้งหมดโดยไม่ได้รับอนุญาต

ลักษณะภัยคุกคาม

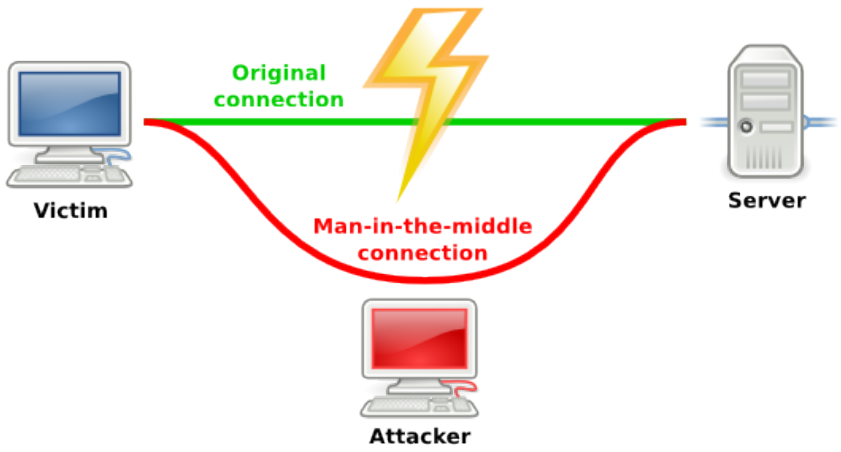
ตัวอย่างภัยคุกคาม	ลักษณะการทำงาน	ลักษณะการโจมตี	การป้องกัน	ประเภทภัยคุกคาม
การสอดแนม (Snooping หรือ Sniffing หรือ Eavesdropping)	ทำการดักเพื่อแอบดูข้อมูล	เป็นการโจมตีแบบ Passive คือไม่มีการเปลี่ยนแปลงหรือแก้ไขข้อมูล	โดยการเข้ารหัสข้อมูล (Encryption)	การเปิดเผย (Disclosure)



Packet addressed to PC3 is forwarded by the hub to other hosts in the network

ลักษณะภัยคุกคาม

ตัวอย่างภัยคุกคาม	ลักษณะการทำงาน	ลักษณะการโจมตี	การป้องกัน	ประเภทภัยคุกคาม
การเปลี่ยนแปลงข้อมูล (Modification)	การแก้ไขข้อมูลโดยที่ไม่ได้รับอนุญาต	เป็นการโจมตีแบบ Active คือมีการเปลี่ยนแปลงข้อมูลโดย การโจมตีผ่านคนกลาง (Man-in-the-middle) ผู้บุกรุกอ่านข้อมูลจากผู้ส่งแล้วแก้ไขก่อนจะส่งต่อไปให้ผู้รับ	พยายามรักษาความคงสภาพ Integrity **ของข้อมูล 2 ส่วนคือ ป้องกันการเปลี่ยนแปลง** ที่เกิดจากผู้ที่ไม่ได้รับอนุญาต ผู้ที่ได้รับอนุญาตพยายามแก้ไขข้อมูลนอกเหนือจากสิทธิ์ที่มี **การตรวจสอบ (Detection)** ตรวจสอบว่าข้อมูลยังคงมีความน่าเชื่อถืออยู่หรือไม่	การหลอกลวง (Deception) การขัดขวาง (Disruption) การควบคุมระบบ (Usurpation)

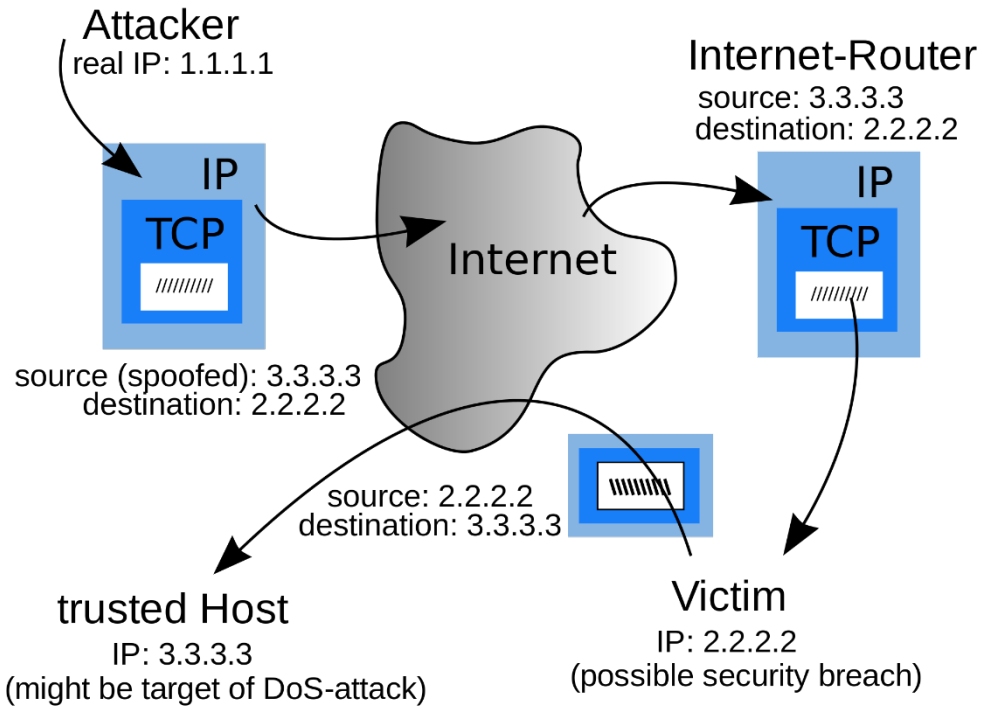


ลักษณะภัยคุกคาม

ตัวอย่างภัยคุกคาม	ลักษณะการทำงาน	ลักษณะการโจมตี	การป้องกัน	ประเภทภัยคุกคาม
การปลอมตัว (Spoofing)	การทำให้อีกฝ่ายหนึ่งเข้าใจว่าตัวเองเป็นบุคคลหนึ่ง เช่น ผู้ใช้ต้องการจะล็อกอินเข้าสู่ระบบ แต่มีการหลอกให้ล็อกอินเข้าอีกระบบหนึ่งโดยผู้ใช้เข้าใจว่าเป็นระบบที่ตนเองต้องการเข้าใช้งาน	เป็นการโจมตีแบบ Active คือมีการเปลี่ยนแปลงข้อมูล	ใช้การพิสูจน์ทราบตัวตน (Authentication)	หลอกลวง (Deception) การควบคุมระบบ (Usurpation)

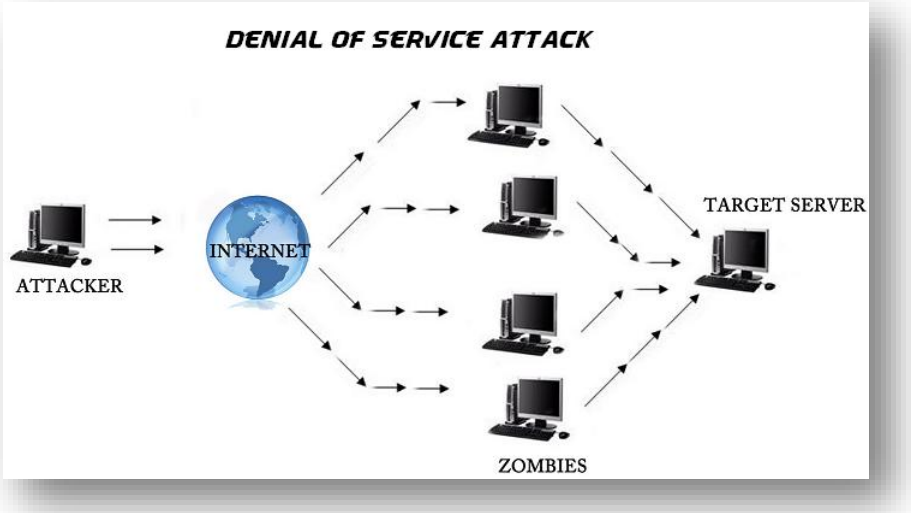
ลักษณะภัยคุกคาม

ตัวอย่างภัยคุกคาม	ลักษณะการทำงาน
การปลอมตัว (Spoofing) [IP Spoofing]	การที่ผู้บุกรุกอยู่นอกเครือข่ายแล้วทำว่าเป็นคอมพิวเตอร์ที่เชื่อถือได้ (Trusted) โดยอาจจะใช้ไอพีแอดเดรสเหมือนกับที่ใช้ในเครือข่าย



ลักษณะภัยคุกคาม

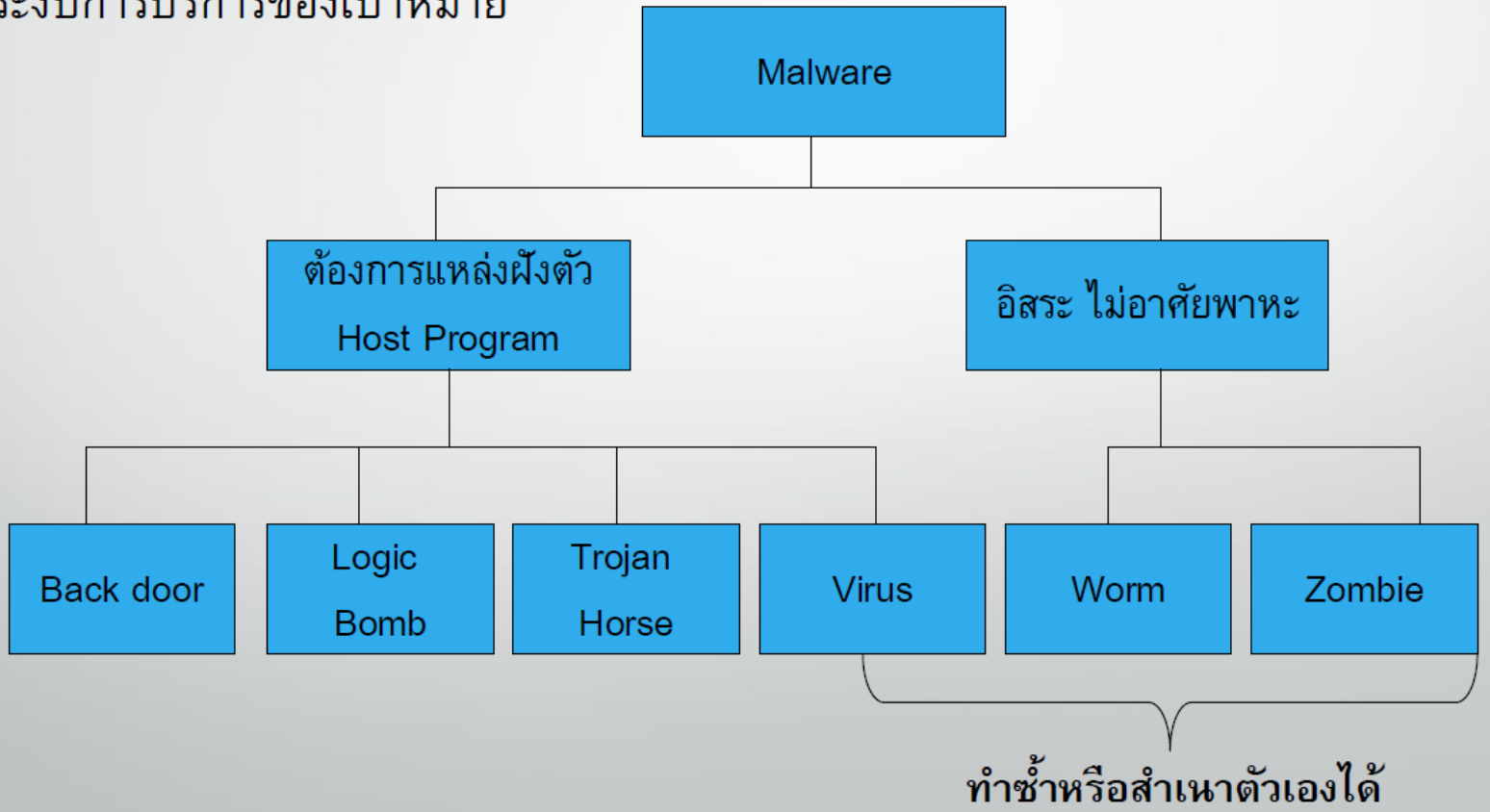
ตัวอย่างภัยคุกคาม	ลักษณะการทำงาน	ลักษณะการโจมตี	การป้องกัน	ประเภทภัยคุกคาม
การปฏิเสธการให้บริการ (Denial of Service : DOS)	การขัดขวางการให้บริการของเซิร์ฟเวอร์เป็นเวลานาน	อาจเกิดขึ้นที่เซิร์ฟเวอร์ โดยขัดขวางไม่ให้เซิร์ฟเวอร์ใช้ทรัพยากรที่จำเป็นได้ หรือใช้ทรัพยากรของเซิร์ฟเวอร์จนหมด	การรักษาความพร้อมใช้งาน (Availability) **คือ การมีระบบสำรอง**	อื่น ๆ



ลักษณะของภัยคุกคาม

มัลแวร์ (Malware)

คือ ซอฟต์แวร์หรือโปรแกรมที่มุ่งร้ายต่อเป้าหมาย ถูกออกแบบมาให้ทำหน้าที่สร้างความเสียหาย หรือทำลาย ระงับการบริการของเป้าหมาย

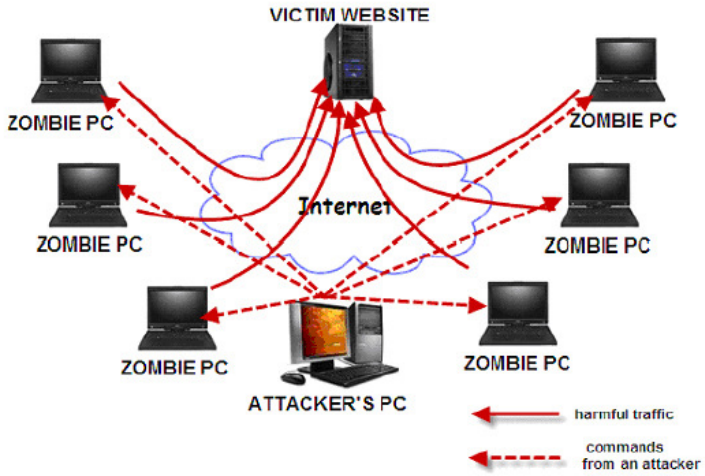


ลักษณะของมัลแวร์ (Malware)

- **ลอจิก บอมบ์** (Logic Bomb) เป็นมัลแวร์ทำงานภายใต้เงื่อนไขที่ผู้โจมตีเป็นผู้กำหนด เช่น ผู้โจมตีกำหนดให้โปรแกรมอันตรายนั้น ทำงานเมื่อถึงวัน และเวลาที่กำหนด หรือทำงานเมื่อมีเหตุการณ์ตรงกับเงื่อนไขที่ผู้โจมตีกำหนด
- **แบ็กดอร์** (Backdoor) เป็นมัลแวร์ที่ทำตัวเป็นทางลัดเข้าสู่ระบบคอมพิวเตอร์ทำให้ผู้ไม่หวังดีสามารถเข้ามาควบคุมคอมพิวเตอร์ที่ตกเป็นเหยื่อได้โดยไม่ต้องยุ่งยากกับการหลบหลีก หรือแก้ไขระบบความมั่นคงปลอดภัยของคอมพิวเตอร์เครื่องนั้น
- **โทรจัน** (Trojan) คือโปรแกรมที่ทำลายระบบคอมพิวเตอร์โดยแฝงมากับไฟล์หรือโปรแกรมอื่นๆ เมื่อติดตั้งโปรแกรมเสร็จแล้วโทรจันที่แฝงมาด้วยก็จะทำลายระบบคอมพิวเตอร์ หรือสร้างช่องทางให้โปรแกรมอื่นเข้ามาทำลายระบบ

ลักษณะของมัลแวร์ (Malware)

- **ไวรัส** (Virus) คือโปรแกรมที่เป็นอันตรายต่อคอมพิวเตอร์ โดยกระจายไปยังไฟล์อื่นๆ ที่อยู่ในเครื่องเดียวกัน ต้องอาศัยคนเปิดไฟล์ที่ติดไวรัส และไวรัสถึงค่อยทำงาน
- **เวิร์ม** (Worm) คือ โปรแกรมที่เป็นอันตรายต่อคอมพิวเตอร์ โดยแพร่กระจายตัวเอง (Copy) ไปยังคอมพิวเตอร์เครื่องอื่นๆที่อยู่ในเครือข่าย และสามารถรันตัวเองเพื่อสร้างความเสียหายได้
- **ซอมบี้** (Zombie) คือการทำเครือข่ายมืดโดยใช้เครื่องคอมพิวเตอร์จำนวนมากๆ จากทั่วโลกที่ตกเป็นเหยื่อของ Worm, Trojan ซึ่งจะถูก Attacker ใช้เป็นฐานปฏิบัติการในการส่ง Spam mail, Phishing, DDoS หรือเอาไว้เก็บไฟล์หรือซอฟแวร์ที่ผิดกฎหมาย



เครื่องมือสำหรับการรักษาความปลอดภัย

เครื่องมือสำหรับการรักษาความปลอดภัย

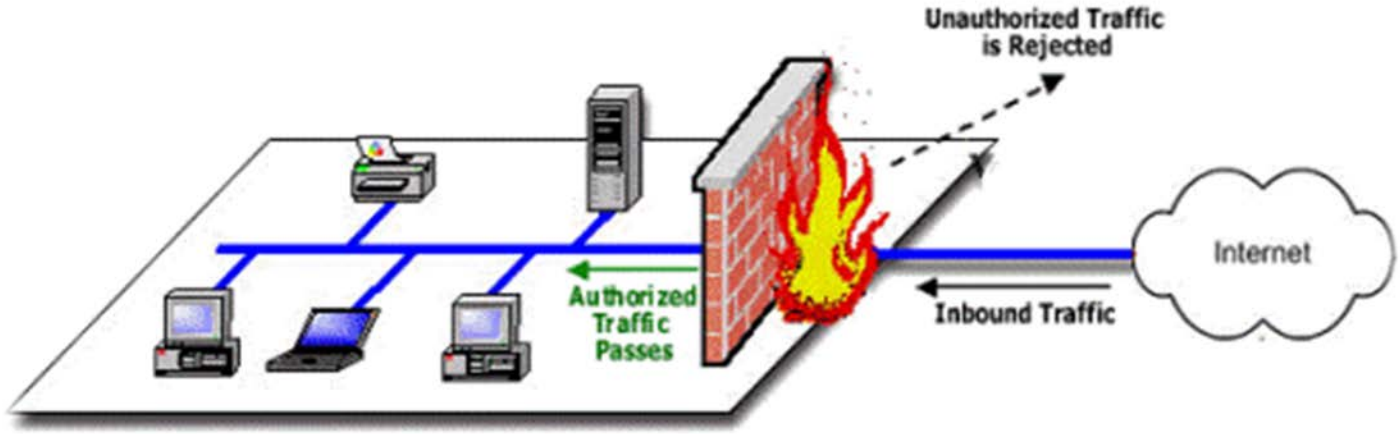
- ไฟร์วอลล์ (Firewall)
- ระบบตรวจจับการบุกรุก (IDS/IPS)
- การเข้ารหัสข้อมูล (Data Encryption)
- ซอฟต์แวร์ป้องกันไวรัส (Anti-Virus Software)
- ระบบการรักษาความปลอดภัยทางกายภาพ

เครื่องมือสำหรับการรักษาความปลอดภัย

เนื่องจากภัยมีรอบด้าน ดังนั้นจึงไม่สามารถใช้เครื่องมือประเภทใดประเภทหนึ่งเพื่อรักษาความปลอดภัยทั้งองค์กรได้ จำเป็นต้องใช้ผลิตภัณฑ์หลายประเภททำงานร่วมกันเป็นระบบเพื่อป้องกันและรักษาความปลอดภัย

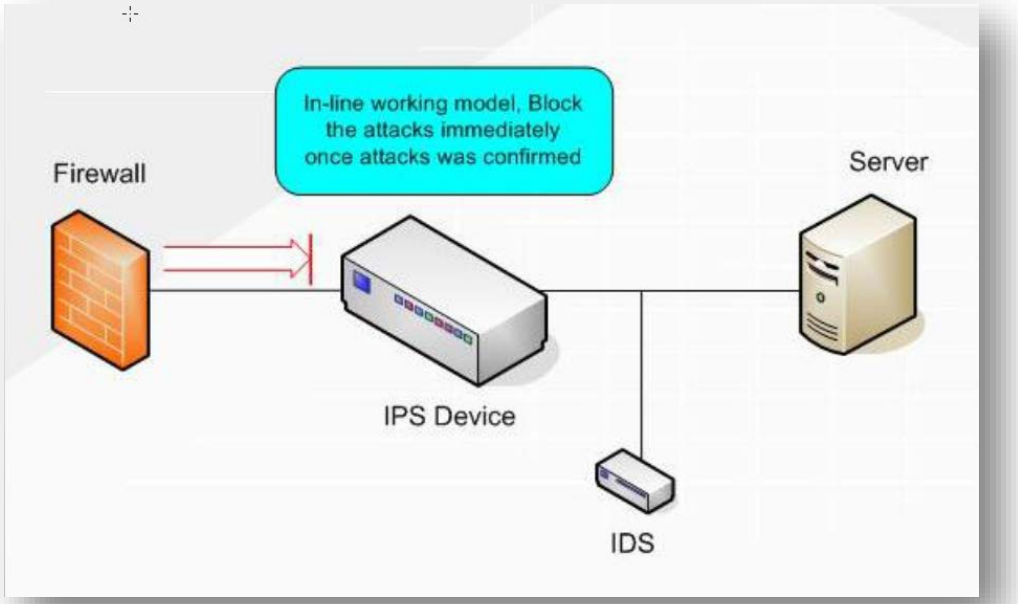
ไฟร์วอลล์ (Firewall)

- เป็นระบบควบคุมการเข้าออกของเครือข่าย **ใช้ปกป้องการโจมตีจากภายนอก** ปกติจะติดตั้งขวางกั้นระหว่างสองเครือข่าย **ตั้งอยู่ก่อนหรือหลังเราเตอร์**
- ไฟร์วอลล์ไม่สามารถป้องกันการโจมตีที่ใช้ช่องทางปกติที่เปิดไว้โดยไฟร์วอลล์ได้
- แพ็คเก็ตที่อนุญาตให้ผ่านหรือไม่ให้ผ่าน จะขึ้นอยู่กับนโยบายการรักษาความปลอดภัยขององค์กรเป็นหลัก



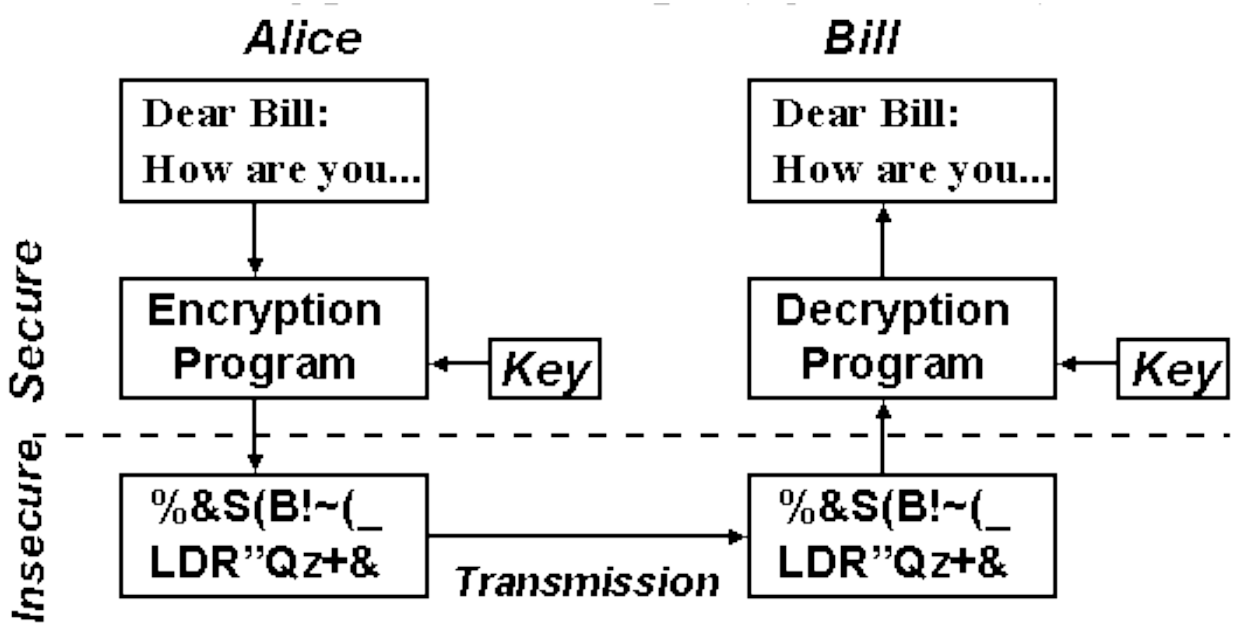
ระบบตรวจจับการบุกรุก (IDS/IPS)

- Intrusion Detection System (IDS) ทำหน้าที่ตรวจสอบ รูปแบบ packet ที่วิ่งภายในเครือข่าย เมื่อพบรูปแบบการทำงานที่เข้าข่ายผิดปกติ จึงทำการแจ้งเตือนไปยังผู้ดูแลระบบนั้นๆ
- Intrusion Prevention System (IPS) ทำหน้าที่คล้ายๆ กับ IDS สามารถแจ้งเตือนและยับยั้ง รูปแบบ packet ที่ผิดปกตินั้นๆ ได้ด้วยตามค่าที่ตั้งไว้



การเข้ารหัสข้อมูล (Data Encryption)

- การเข้ารหัส (encryption) คือ การเปลี่ยนข้อความที่สามารถอ่านได้ (plain text) ไปเป็นข้อความที่ไม่สามารถอ่านได้ (cipher text) เพื่อเหตุผลด้านความปลอดภัย



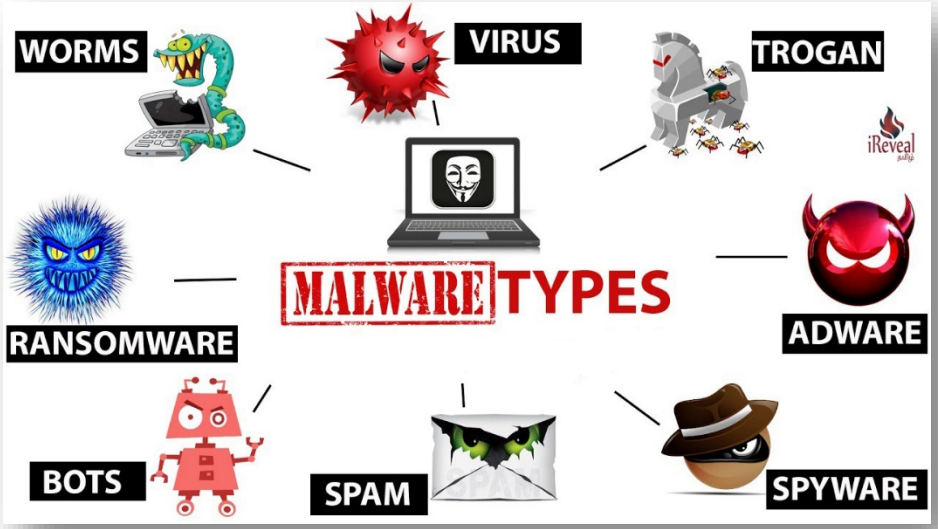
ซอฟต์แวร์ป้องกันไวรัส (Anti-Virus Software)

- ปัจจุบันภัยคุกคามที่มีผลกระทบต่อองค์กรมากที่สุดคือ มัลแวร์ ดังนั้นการป้องกันและกำจัดสิ่งเหล่านี้จึงเป็นสิ่งที่สำคัญที่สุด
- การติดตั้งและใช้งานโปรแกรมป้องกันไวรัสอย่างถูกต้อง สามารถลดความเสี่ยงต่อมัลแวร์ได้ แต่ไม่สามารถป้องกันมัลแวร์ได้ทุกชนิด
- ต้องมีการอัพเดตฐานข้อมูลไวรัสอยู่เสมอ รวมถึงต้องสแกนระบบเป็นประจำด้วย

ซอฟต์แวร์ป้องกันไวรัส (Anti-Virus Software)

สิ่งที่ซอฟต์แวร์ป้องกันไวรัส **ไม่สามารถป้องกันได้** คือ

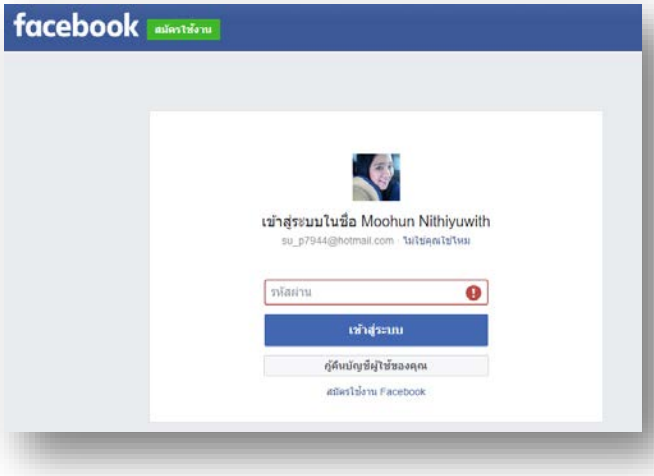
- ผู้บุกรุกจากที่อื่นที่เจาะระบบเข้ามาแล้วรันโปรแกรมประสงค์ร้าย
- ไม่สามารถป้องกันผู้ใช้ที่ได้รับอนุญาต แต่พยายามจะเข้าถึงไฟล์หรือระบบที่ไม่ได้รับอนุญาตได้



การรักษาความปลอดภัยทางกายภาพ

- การพิสูจน์ตัวตนสามารถทำได้โดยใช้การตรวจสอบคุณสมบัติ 3 อย่างของผู้ใช้ คือ

คุณสมบัติการพิสูจน์ตัวตน	ตัวอย่าง
1. สิ่งที่คุณรู้ (Something you know)	**Password** การใช้เพียง Password เป็นการตรวจสอบเฉพาะ *“สิ่งที่คุณรู้”* แต่อาจถูกเดาหรือถูกขโมยได้

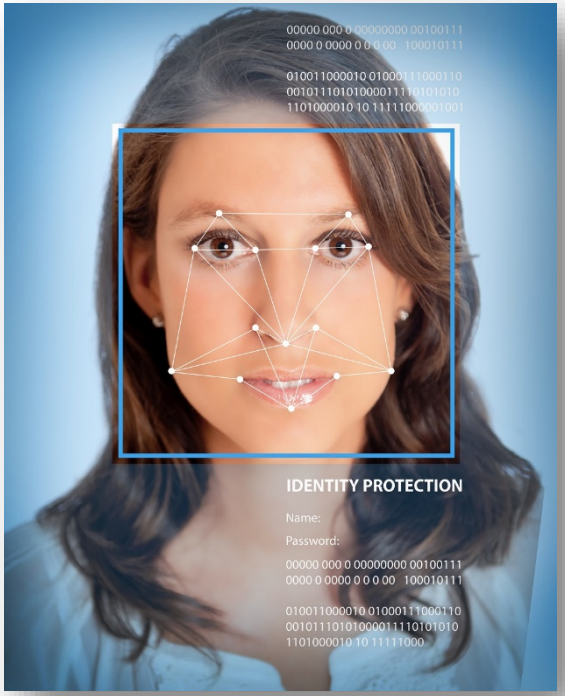


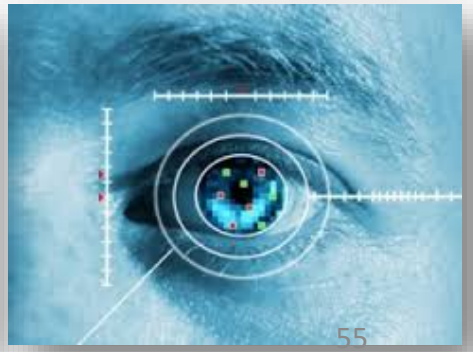
การรักษาความปลอดภัยทางกายภาพ

คุณสมบัติการพิสูจน์ตัวตน	ตัวอย่าง
2. สิ่งที่คุณมี **(Something you have)**	**Smart Card** สามารถป้องกันการเดารหัสผ่านได้ แต่หากสมาร์ทการ์ดถูกขโมยไป ระบบจะไม่สามารถป้องกันการโจมตีจากผู้บุกรุกคนนั้นได้

การรักษาความปลอดภัยทางกายภาพ

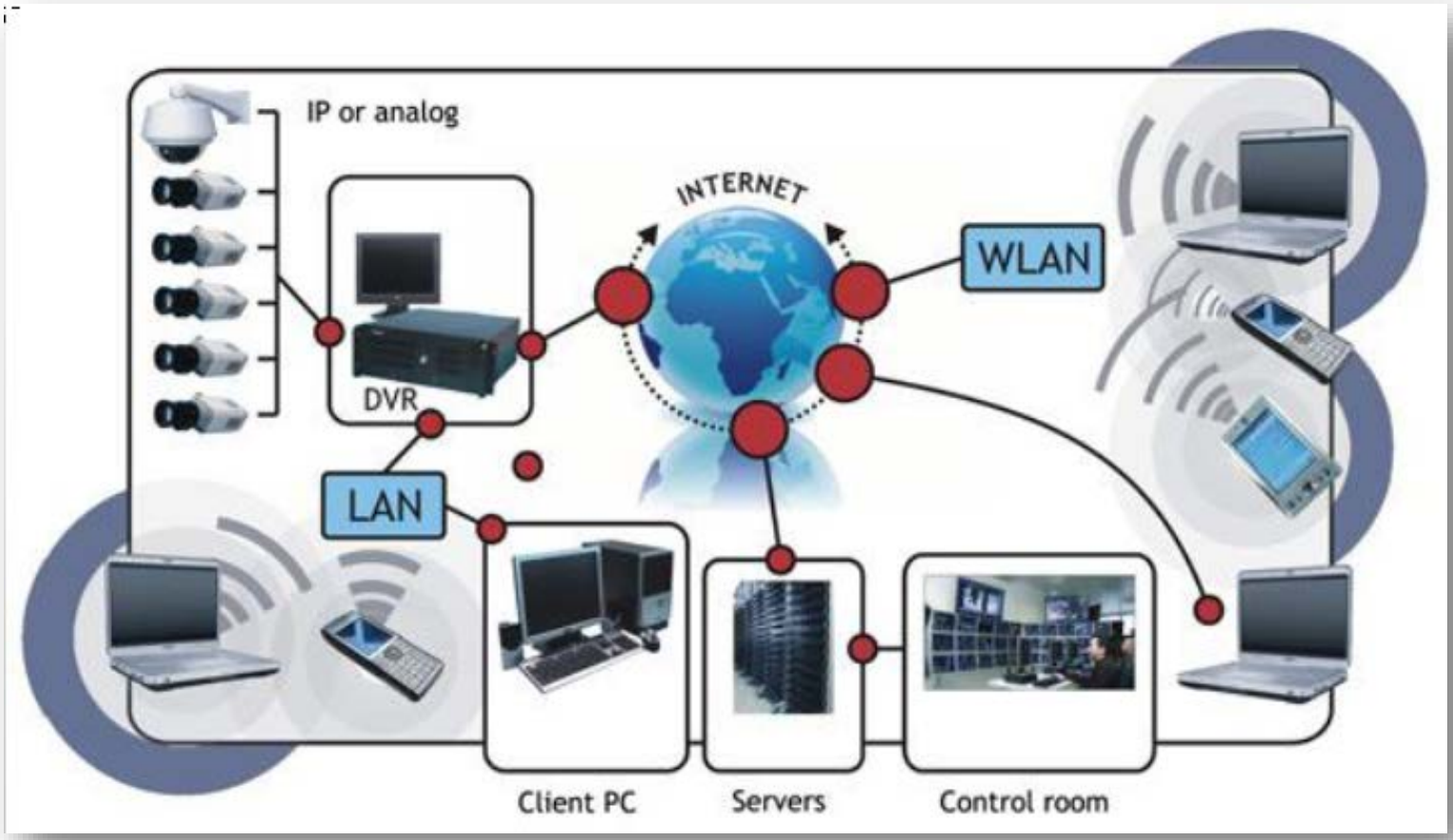
คุณสมบัติการพิสูจน์ตัวตน	ตัวอย่าง
3. สิ่งที่คุณเป็น (Something you are)	Biometrics สามารถป้องกันการเดารหัสผ่านหรือขโมยสมาร์ทการ์ดได้ ถือว่าเป็นระบบพิสูจน์ตัวตนที่ค่อนข้างแข็งแกร่ง ตัวอย่างเช่น การสแกนลายนิ้วมือ มือ ใบหน้า ม่านตา เป็นต้น





การรักษาความปลอดภัยทางกายภาพ

การรักษาความปลอดภัย **ด้านสถานที่**

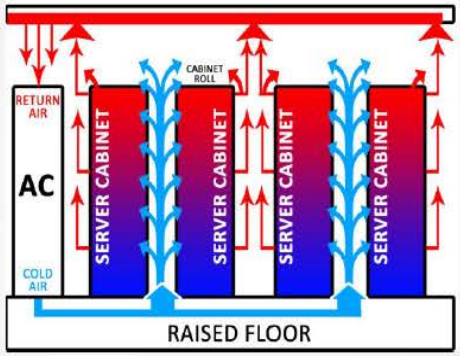


การรักษาความปลอดภัยทางกายภาพ

- การรักษาความปลอดภัย **ด้านสถานที่**

UPS

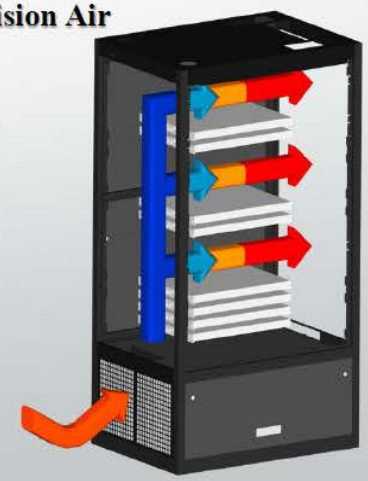
ระบบดับเพลิง



Precision Air

Generator

ระบบ แจ้งเตือน



Rack Air

อุปสรรคของความมั่นคงปลอดภัยของสารสนเทศ

อุปสรรคของความมั่นคงปลอดภัยของสารสนเทศ

- “ความมั่นคงปลอดภัย” คือ **“ความไม่สะดวก”** ผู้ใช้มักเห็นว่าการรักษาความมั่นคงปลอดภัยทำให้การทำงานไม่สะดวกเนื่องจากต้องเสียเวลาในการป้อน password และกระบวนการอื่น ๆ ในการพิสูจน์ตัวผู้ใช้ บางครั้งต้องป้อนรหัสผ่านมากกว่า 1 ครั้ง
- มีความซับซ้อนบางอย่างในคอมพิวเตอร์ที่ผู้ใช้ทั่วไปไม่ทราบ เช่น Port, Service ที่จะทราบเฉพาะในแวดวง Programmer หรือผู้ดูแลระบบ ซึ่งผู้ใช้ทั่วไปไม่ได้ให้ความสำคัญ
- ผู้ใช้คอมพิวเตอร์ไม่ระแวดระวัง เพราะไม่มีความรู้ในด้านคอมพิวเตอร์มากพอ จึงตกเป็นเหยื่อของการโจมตีเสมอ

อุปสรรคของความมั่นคงปลอดภัยของสารสนเทศ

- การพัฒนาซอฟต์แวร์โดยคำนึงถึงความมั่นคงปลอดภัยภายหลัง เพราะผู้พัฒนาเน้นความสำคัญไปที่การพัฒนาซอฟต์แวร์ให้งานเสร็จทันเวลาภายในงบประมาณที่ตั้งไว้ ดังนั้น จึงไม่ลงรายละเอียดในกระบวนการทดสอบ ทำให้ซอฟต์แวร์มีช่องโหว่เป็นจุดอ่อนให้โจมตีได้

- แนวโน้มเทคโนโลยีสารสนเทศคือการ “แบ่งปัน” ไม่ใช่ “การป้องกัน” เน้นการสร้างการเชื่อมโยงของผู้ใช้ เช่น Social Networks ต่าง ๆ เกิดสังคมการแบ่งปันข้อมูลโดยขาดความระมัดระวังการให้ข้อมูลส่วนบุคคลบนเว็บไซต์เหล่านั้น

อุปสรรคของความมั่นคงปลอดภัยของสารสนเทศ

- การเข้าถึงข้อมูลได้จากทุกสถานที่ ด้วยอุปกรณ์สื่อสารแบบพกพา ประกอบกับ Online Storage ที่ผู้ให้บริการได้จัดไว้เพื่อให้ผู้ใช้บริการสามารถฝากไฟล์ไว้ได้ ซึ่งมีความเสี่ยงสูงมากต่อการถูกโจมตี

- ความมั่นคงปลอดภัยไม่ได้เกิดขึ้นที่ซอฟต์แวร์ และฮาร์ดแวร์เพียงอย่างเดียว แต่การรักษาความมั่นคงปลอดภัยของสารสนเทศเป็นงานที่เป็นกระบวนการ (Process) ต้องอาศัยความร่วมมือจากผู้ใช้ทั้งองค์กร อาศัยนโยบายและมาตรการบังคับให้เกิดการปฏิบัติที่มุ่งไปสู่เป้าหมายเดียวกัน อาศัยกิจกรรมที่เสริมสร้างความเข้าใจแก่ผู้ใช้ เช่น การฝึกอบรมเพื่อเสริมสร้างการเรียนรู้ และสร้างจิตสำนึกในวิชาชีพ

อุปสรรคของความมั่นคงปลอดภัยของสารสนเทศ

- มิจฉาชีพมีความเชี่ยวชาญ ทำให้เทคโนโลยีและการออกมาตรการป้องกันการโจมตี ตามหลังมิจฉาชีพเสมอ กล่าวคือระบบมักถูกโจมตีก่อนเสมอ จึงเกิด Patch ตามมา

- การให้ความสำคัญกับงานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศมักถูกนำมาพิจารณาเป็นเรื่องรอง หรือเมื่อระบบถูกโจมตีไปแล้ว

Download

Download

- เอกสารนโยบายการรักษาความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศและการสื่อสาร มหาวิทยาลัยราชภัฏเพชรบูรณ์
  http://arit.pcru.ac.th/documents/securitypolicy.pdf

- คู่มืออบรม หลักสูตร “นโยบายการรักษาความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศและการสื่อสาร”
  http://arit.pcru.ac.th/documents/securitypolicy_training61.pdf

Thank You