มหาวิทยาลัยราชภัฏนครปฐม
Nakhon Pathom Rajabhat University

ความปลอดภัยในโครงข่ายการสื่อสารข้อมูล

https://itdigitserve.com/wp-content/uploads/2016/07/network-security-1.jpg

เนื้อหา

- แนวคิดพื้นฐานและสถาปัตยกรรมความมั่นคงปลอดภัยเครือข่าย
- ภัยคุกคามและการโจมตีเครือข่ายสมัยใหม่
- ความปลอดภัยเครือข่ายไร้สายและการพิสูจน์ตัวตน
- Firewall และการควบคุมทราฟฟิกเครือข่าย
- ระบบตรวจจับและป้องกันการบุกรุก (IDS / IPS / XDR)
- การป้องกันการโจมตีพอร์ต การแบ่งส่วนเครือข่าย และการควบคุมการเข้าถึง
- การเข้ารหัสข้อมูลและความปลอดภัยของการสื่อสาร
- ความมั่นคงปลอดภัยในระบบ Cloud มาตรฐาน และกฎหมายที่เกี่ยวข้อง

แนวคิดพื้นฐาน
และสถาปัตยกรรมความมั่นคงปลอดภัยเครือข่าย

การรักษาความปลอดภัยบนเครือข่าย

- **ความปลอดภัยของเครือข่าย** ประกอบด้วยนโยบายและอุปกรณ์ต่าง ๆ เพื่อจัดการการเข้าถึงจากเครือข่ายภายใน แม้ว่าเครือข่ายที่มีความปลอดภัยที่สุดคือเครือข่ายที่ไม่มีการเชื่อมต่อภายนอก แต่นั่นก็เป็นวิธีที่ไม่สามารถทำได้ เนื่องจากความต้องการเข้าถึงทรัพยากรของบริษัท จากภายนอกของสถานที่ทางกายภาพมีเพิ่มมากขึ้น เช่นเดียวกับการเปิดรับข่าวสารกับอินเทอร์เน็ต จึงเป็นสิ่งสำคัญยิ่งที่จะทำตามขั้นตอนที่จำเป็นเพื่อปกป้องทรัพยากรขององค์กรจากภัยคุกคามทั้งภายนอกและภายใน

การรักษาความปลอดภัยบนเครือข่าย

- ✓ การระมัดระวังในการใช้งาน การติดไวรัสมักเกิดจากผู้ใช้ไปใช้แผ่นดิสก์ร่วมกับผู้อื่น แล้วแผ่นนั้นติดไวรัสมา หรืออาจติดไวรัสจากการดาวน์โหลดไฟล์มาจากอินเทอร์เน็ต
- ✓ หมั่นสำเนาข้อมูลอยู่เสมอ เป็นการป้องกันการสูญหายและถูกทำลายของข้อมูล
- ✓ ติดตั้งโปรแกรมตรวจสอบและกำจัดไวรัส วิธีการนี้สามารตรวจสอบ และป้องกันไวรัสคอมพิวเตอร์ได้ระดับหนึ่ง แต่ไม่ใช่เป็นการป้องกันได้ทั้งหมด เพราะว่าไวรัสคอมพิวเตอร์ได้มีการพัฒนาอยู่ตลอดเวลา
- ✓ การติดตั้งไฟร์วอลล์ (Firewall) ไฟร์วอลล์จะทำหน้าที่ป้องกันบุคคลอื่นบุกรุกเข้ามาเจาะเครือข่ายในองค์กรเพื่อขโมยหรือทำลายข้อมูล เป็นระยะที่ทำหน้าที่ป้องกันข้อมูลของเครือข่ายโดยการควบคุมและตรวจสอบการรับส่งข้อมูลระหว่างเครือข่ายภายในกับเครือข่ายอินเทอร์เน็ต
- ✓ การใช้รหัสผ่าน (Username & Password) การใช้รหัสผ่านเป็นระบบรักษาความปลอดภัยขั้นแรกที่ใช้กันมากที่สุด เมื่อมีการติดตั้งระบบเครือข่ายจะต้องมีการกำหนดบัญชีผู้ใช้และรหัสผ่านหากเป็นผู้อื่นที่ไม่ทราบรหัสผ่านก็ไม่สามารถเข้าไปใช้เครือข่ายได้หากเป็นระบบที่ต้องการความปลอดภัยสูงก็ควรมีการเปลี่ยนรหัสผ่านบ่อย ๆ เป็นระยะ ๆ อย่างต่อเนื่อง

แนวคิดพื้นฐานและสถาปัตยกรรมความมั่นคงปลอดภัยเครือข่าย

หัวใจสำคัญที่เป็นรากฐานในการออกแบบระบบเครือข่ายให้ปลอดภัยและทนทาน ดังนี้

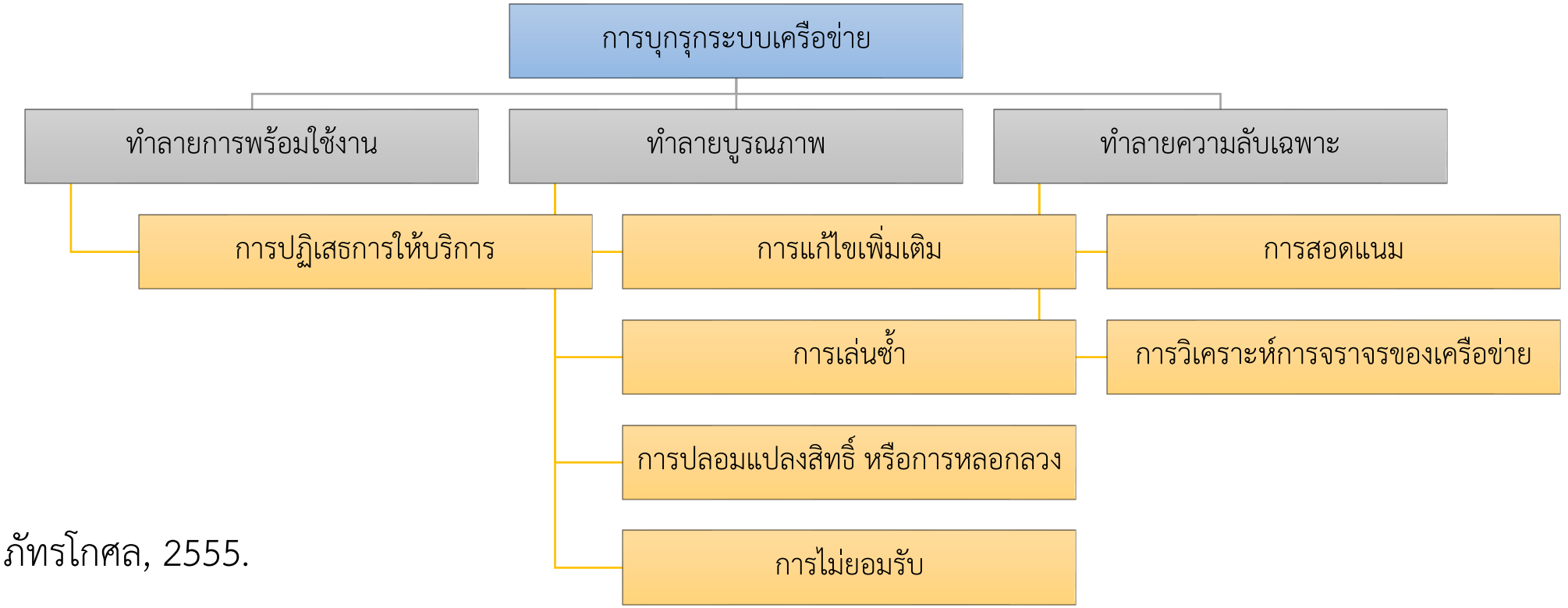
- **หลักการพื้นฐาน CIA Triad** การรักษาความลับ (Confidentiality), ความถูกต้อง (Integrity), และความพร้อมใช้งาน (Availability) ของข้อมูล
- **แนวคิด Defense in Depth (การป้องกันแบบหลายชั้น)** สถาปัตยกรรมที่ดีจะไม่พึ่งพาการป้องกันเพียงจุดเดียว แต่จะวางมาตรการเป็นชั้นๆ เหมือนกำแพงเมือง
- **สถาปัตยกรรม Zero Trust** แนวคิดสมัยใหม่ที่เปลี่ยนจากการเชื่อใจใครก็ตามที่อยู่ในเครือข่ายภายในมาเป็น "Never Trust, Always Verify"
- **ความทนทานของระบบ (Network Resilience)** เพื่อให้สถาปัตยกรรมมีความทนทานต่อความล้มเหลวหรือการโจมตี (เช่น DoS/DDoS)

ภัยคุกคามและการโจมตีเครือข่ายสมัยใหม่

การโจมตีเครือข่ายคอมพิวเตอร์

- การโจมตีหรือการบุกรุกเครือข่าย หมายถึง ความพยายามที่จะเข้าใช้ระบบ (Access Attack) การแก้ไขข้อมูลหรือระบบ (Modification Attack) การทำให้ระบบไม่สามารถใช้การได้ และการทำให้ข้อมูลเป็นเท็จ (Repudiation Attack) ซึ่งจะกระทำโดยผู้ประสงค์ร้าย ผู้ที่ไม่มีสิทธิ์ หรืออาจเกิดจากความไม่ได้ตั้งใจของผู้ใช้เองต่อไปนี้เป็นรูปแบบต่าง ๆ ที่ผู้ไม่ประสงค์ดีพยายามที่จะบุกรุกเครือข่ายเพื่อลักลอบข้อมูลที่สำคัญหรือเข้าใช้ระบบโดยไม่ได้รับอนุญาต

ประเภทการบุกรุกระบบเครือข่าย



ที่มา: ภัทรสินี ภัทรโกศล, 2555.

ภัยคุกคามขั้นสูงและซับซ้อน

- **Advanced Persistent Threats (APTs):** เป็นการโจมตีที่ออกแบบมาเพื่อฝังตัวในเครือข่ายอย่างแนบเนียนและยาวนานเพื่อขโมยข้อมูลสำคัญ มักดำเนินการโดยกลุ่มที่ได้รับการสนับสนุนระดับรัฐ
- **Botnets:** เครือข่ายของคอมพิวเตอร์ "ซอมบี้" ที่ถูกควบคุมจากระยะไกลเพื่อระดมโจมตีแบบ DDoS ขนาดใหญ่ ซึ่งสามารถสร้างความเสียหายต่อโครงสร้างพื้นฐานระดับชาติได้
- **Ransomware:** มัลแวร์เรียกค่าไถ่ที่เข้ารหัสไฟล์ข้อมูลเพื่อให้เข้าถึงไม่ได้จนกว่าจะมีการจ่ายเงิน

การโจมตีผ่านมนุษย์ (Social Engineering)

- **Phishing & Spear-phishing:** การใช้ความเชื่อใจหรือความกลัวเพื่อหลอกให้เหยื่อเผยแพร่ข้อมูลส่วนตัวหรือติดตั้งมัลแวร์
- **Baiting & Tailgating**: การใช้สื่อทางกายภาพเช่น USB ที่ติดไวรัสวางทิ้งไว้ หรือการแอบเดินตามผู้มีสิทธิ์เข้าสู่พื้นที่หวงห้าม

การโจมตีตามเลเยอร์ของเครือข่าย (OSI Model)

- **ชั้น Physical & Data Link:** การรบกวนสัญญาณ (Jamming) และการโจมตีระดับสวิตช์อย่าง MAC Flooding หรือ ARP Poisoning
- **ชั้น Network & Transport**: การปลอมแปลงไอพี (IP Spoofing) และการโจมตีขั้นตอนการเชื่อมต่ออย่าง TCP SYN Flood
- **ชั้น Application:** การโจมตีผ่านช่องโหว่ซอฟต์แวร์ เช่น SQL Injection และ Cross-site Scripting (XSS) เพื่อเข้าถึงฐานข้อมูลโดยตรง

การโจมตีที่มุ่งเน้นช่องโหว่ของโปรโตคอลและระบบเครือข่าย

- **Smurf Attack:** เป็นการโจมตี DoS รูปแบบเก่าแต่ยังมีผล โดยใช้ ICMP packet จำนวนมหาศาลส่งไปยังเซิร์ฟเวอร์เป้าหมายเพื่อให้ระบบล่ม.
- **Teardrop Attack:** การส่งแพ็กเก็ต IP ที่มีการแบ่งส่วน (Fragment) ผิดปกติ ทำให้เมื่อระบบพยายามประกอบแพ็กเก็ตกลับคืนจะส่งผลให้ระบบค้างหรือล่ม.
- **DHCP Poisoning:** ผู้โจมตีปลอมตัวเป็นเซิร์ฟเวอร์ DHCP เพื่อแจกจ่ายข้อมูลเครือข่ายปลอม (เช่น DNS หรือ Gateway) ให้กับเหยื่อ เพื่อดักจับข้อมูล.
- **DNS Cache Poisoning (Redirect Attack):** การเปลี่ยนข้อมูลใน DNS server ให้ชี้ไปยังเว็บไซต์ที่ผู้โจมตีต้องการเพื่อหลอกลวงผู้ใช้

ภัยคุกคามต่อระบบเข้ารหัสและข้อมูล (Cryptosystems)

- **Birthday Attack:** การโจมตีอัลกอริทึม Hashing เพื่อสร้างข้อความที่มีค่า Hash ตรงกัน.
- **Known-plaintext & Ciphertext-only Attacks:** การวิเคราะห์รูปแบบเพื่อพยายามถอดรหัสข้อมูล หรือหาคีย์เข้ารหัส.
- **Cryptojacking:** การใช้มัลแวร์แอบใช้ทรัพยากรคอมพิวเตอร์ของเหยื่อเพื่อขุดเงินดิจิทัล (Cryptocurrency) โดยที่เจ้าของเครื่องไม่รู้ตัว

ภัยคุกคามในยุคอัจฉริยะ (IoT & AI)

- **Adversarial Attacks:** การโจมตีเพื่อหลอกลวงระบบ Machine Learning ให้ประมวลผลผิดพลาด เช่น การหลอกระบบควบคุมในอาคารอัจฉริยะ (HVAC).
- **False Data Injection (FDI):** การส่งข้อมูลเท็จเข้าสู่ระบบประมวลผล เช่น การปลอมตัวเลขการใช้ไฟฟ้าใน Smart Grid เพื่อปั่นป่วนการกระจายพลังงาน

เทคนิคการหลบเลี่ยงและล่อลวงขั้นสูง

- **Watering Hole Attack:** การแอบฝังมัลแวร์ไว้ในเว็บไซต์ที่พนักงานในองค์กรเป้าหมายมักเข้าใช้งานเป็นประจำ.
- **Typosquatting:** การจดโดเมนเนมที่สะกดผิดคล้ายกับเว็บไซต์ชื่อดังเพื่อลวงให้เหยื่อเข้าเว็บไซต์ปลอม.
- **Rootkits:** ซอฟต์แวร์ที่ซ่อนตัวในระดับลึกของระบบปฏิบัติการเพื่อปิดบังกิจกรรมการโจมตีไม่ให้แอนตี้ไวรัสตรวจพบ.
- **XML-based Attacks:** การโจมตีผ่านช่องโหว่ของโค้ด XML เพื่อควบคุมระบบจากระยะไกลหรือทำ DoS

การโจมตีเชิงพฤติกรรมและกายภาพ

- Rubber Hose Attack: การใช้กำลังหรือการข่มขู่เพื่อให้เหยื่อยอมคายความลับหรือรหัสผ่าน.
- War Driving/War Chalking: การขับรถตระเวนหาจุดเชื่อมต่อไร้สายที่ไม่ปลอดภัยและทำเครื่องหมายไว้เพื่อให้ผู้อื่นมาโจมตีต่อ

ความปลอดภัยเครือข่ายไร้สายและการพิสูจน์ตัวตน

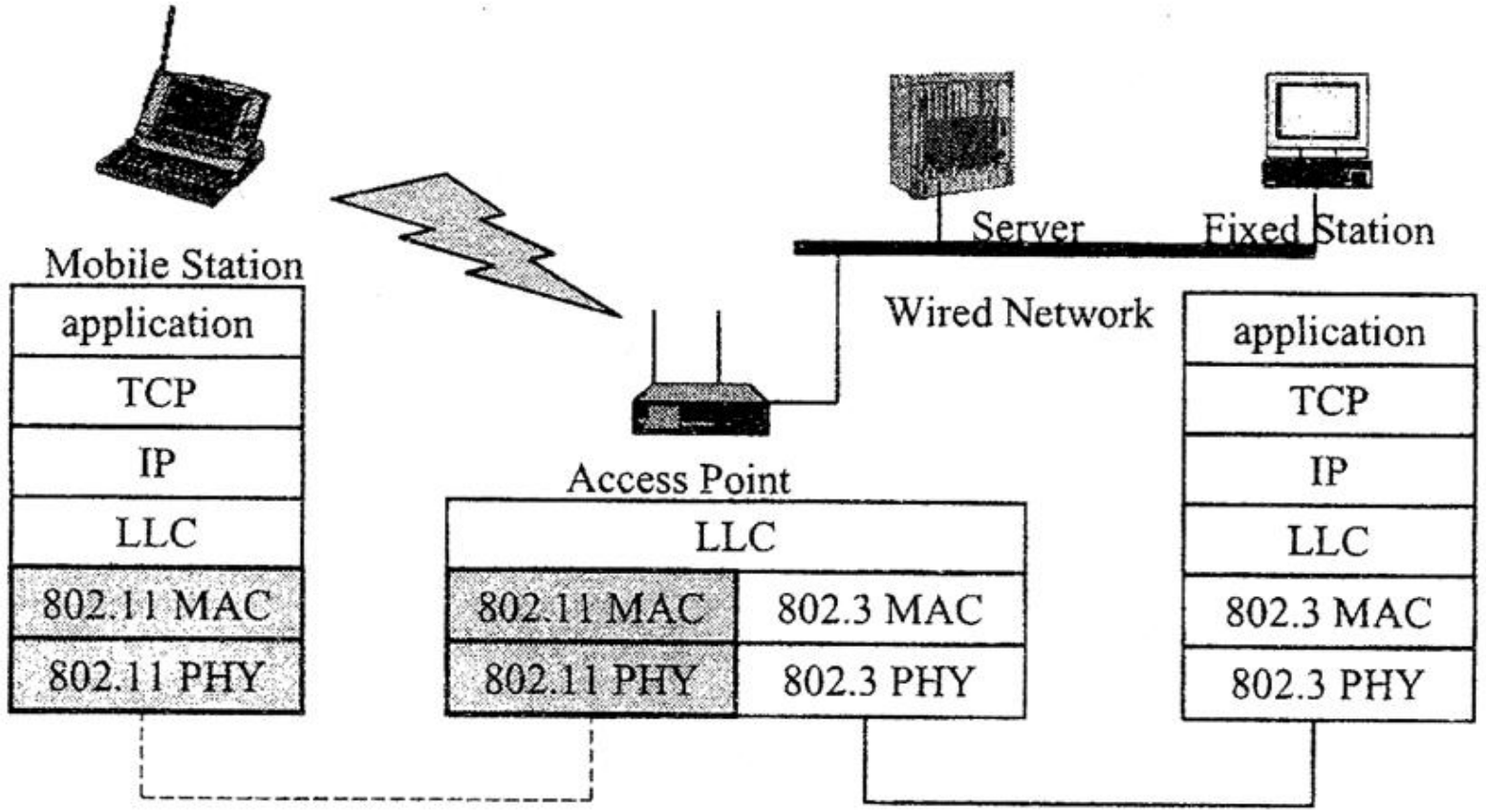
มาตรฐาน IEEE 802.11

กำหนดโครงสร้างการทำงานของเครือข่าย Wi-Fi โดยมีองค์ประกอบสำคัญ:

1. Station (STA) – อุปกรณ์ลูกข่าย เช่น Laptop, Smartphone
2. Access Point (AP) – อุปกรณ์กระจายสัญญาณ
3. Basic Service Set (BSS) – หน่วยเครือข่ายพื้นฐาน
4. Extended Service Set (ESS) – การเชื่อมหลาย AP เข้าด้วยกัน

การรักษาความปลอดภัยต้องถูกกำหนดตั้งแต่ระดับ AP และควบคุมผ่าน Controller หรือ Cloud Management ในองค์กรขนาดใหญ่

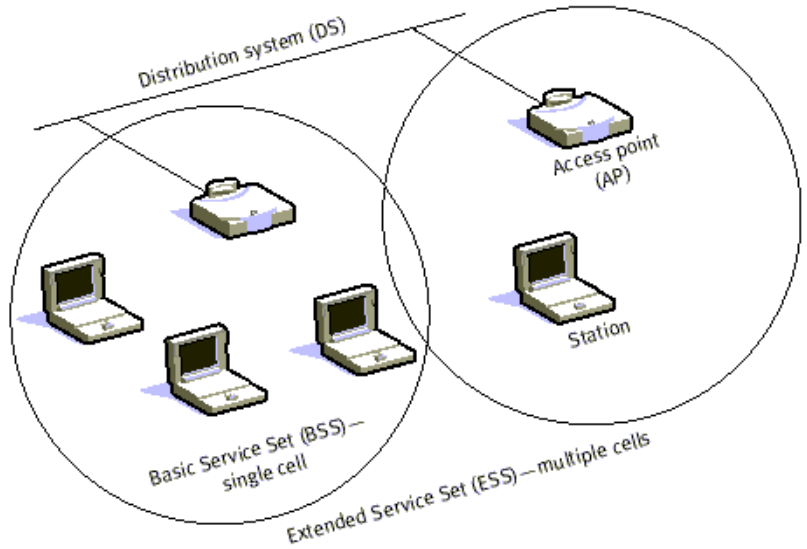
มาตรฐาน IEEE 802.11



ลักษณะการเชื่อมต่อของอุปกรณ์ของ 802.11

โหมด Infrastructure เป็นโหมดที่อนุญาตให้อุปกรณ์ภายใน WLAN สามารถเชื่อมต่อกับเครือข่ายอื่นได้ ในโหมด Infrastructure นี้ เครือข่าย IEEE 802.11 WLAN จะประกอบไปด้วยอุปกรณ์ 2 ประเภทได้แก่

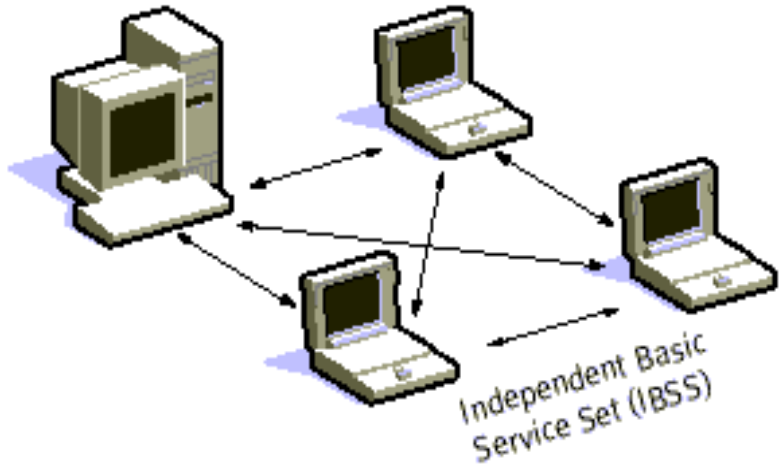
1. สถานีผู้ใช้ (Client Station) ซึ่งก็คืออุปกรณ์คอมพิวเตอร์ (Desktop Laptop หรือ PDA ต่าง ๆ) ที่มีอุปกรณ์ Client Adapter เพื่อใช้รับส่งข้อมูลผ่าน IEEE 802.11 WLAN
2. อุปกรณ์กระจายสัญญาณไร้สายซึ่งทำหน้าที่ต่อเชื่อมสถานีผู้ใช้เข้ากับเครือข่ายอื่น (ซึ่งโดยปกติจะเป็นเครือข่าย IEEE 802.3 Ethernet LAN) การทำงานในโหมด Infrastructure มีพื้นฐานมาจากระบบเครือข่ายโทรศัพท์มือถือ



ที่มา : IEEE 802.11 Architecture, 2013.

ลักษณะการเชื่อมต่อของอุปกรณ์ของ 802.11

โหมด Ad-Hoc หรือ Peer-to-Peer เป็นเครือข่ายที่ปิดคือไม่มีสถานีแม่ข่ายและไม่มีการเชื่อมต่อกับเครือข่ายอื่น บริเวณของเครือข่าย IEEE 802.11 WLAN ในโหมด Ad-Hoc จะถูกเรียกว่า Independent Basic Service Set (IBSS) ซึ่งสถานีผู้ใช้หนึ่งสามารถติดต่อสื่อสารข้อมูลกับสถานีผู้ใช้อื่น ๆ ในเขต IBSS เดียวกันได้โดยตรงโดยไม่ต้องผ่านสถานีแม่ข่าย แต่สถานีผู้ใช้จะไม่สามารถรับส่งข้อมูลกับเครือข่ายอื่น ๆ ได้



ที่มา : IEEE 802.11 Architecture, 2013.

การพิสูจน์ตัวตนของ Wireless LAN Security

การพิสูจน์ตัวตน (Authentication) ใน Wireless LAN คือกระบวนการยืนยันตัวตนของผู้ใช้หรืออุปกรณ์ก่อนอนุญาตให้เข้าถึงทรัพยากรในเครือข่าย เพื่อป้องกันการสวมรอยหรือการเข้าถึงโดยไม่ได้รับอนุญาต ประเด็นสำคัญตามมาตรฐานในแหล่งข้อมูลมีดังนี้ครับ:

- **มาตรฐานความปลอดภัย:** WPA2 เป็นมาตรฐานที่แนะนำที่สุดในปัจจุบัน (ใช้การเข้ารหัส AES) ส่วน WPA3 มีความแข็งแกร่งกว่าด้วยกลไกการแลกเปลี่ยนคีย์แบบ Dragonfly นอกจากนี้ควรหลีกเลี่ยง "Open System Authentication" และ "WEP" เพราะไม่มีความปลอดภัยเพียงพอ
- **เฟรมเวิร์ก 802.1x และ EAP:** มาตรฐาน 802.1x ใช้สำหรับควบคุมการเข้าถึงเครือข่าย โดยมี EAP (Extensible Authentication Protocol) เป็นโครงสร้างที่ยืดหยุ่นในการเลือกวิธีพิสูจน์ตัวตน เช่น:
- **EAP-TLS:** ใช้ใบรับรองดิจิทัล (Digital Certificates) และ Smart Card ซึ่งมีความปลอดภัยสูงมาก
- **PEAP และ EAP-TTLS:** สร้างอุโมงค์ TLS ที่ปลอดภัยเพื่อส่งข้อมูลการยืนยันตัวตนแบบดั้งเดิม
- **ปัจจัยในการยืนยันตัวตน:** สามารถทำได้ผ่าน 4 ปัจจัยหลักคือ สิ่งที่คุณรู้ (รหัสผ่าน), สิ่งที่คุณมี (Token/Smart Card), สิ่งที่คุณเป็น (ลายนิ้วมือ/ม่านตา) และ สิ่งที่คุณผลิตขึ้น (เสียง/ลายเซ็น)
- **การบริหารจัดการระดับองค์กร:** นิยมใช้เซิร์ฟเวอร์ส่วนกลางอย่าง RADIUS หรือ TACACS+ เพื่อจัดเก็บฐานข้อมูลผู้ใช้และตรวจสอบสิทธิ์จากจุดเดียว

มาตรฐานความปลอดภัยของ Wireless LAN (Wi-Fi)

มีการพัฒนาขึ้นตามลำดับเพื่อเพิ่มความแข็งแกร่งในการป้องกันข้อมูล ดังนี้

- **WEP (Wired Equivalent Privacy):** เป็นมาตรฐานดั้งเดิมที่ปัจจุบันถือว่า ล้าสมัยและไม่ปลอดภัย เนื่องจากมีช่องโหว่พื้นฐานที่ทำให้แฮกเกอร์สามารถถอดรหัสได้ภายในเวลาไม่กี่นาที.
- **WPA (Wi-Fi Protected Access):** พัฒนาขึ้นเพื่อแก้ปัญหาของ WEP โดยใช้การเข้ารหัสแบบ RC4 และโปรโตคอล TKIP แต่ยังมีความปลอดภัยไม่เพียงพอเมื่อเทียบกับมาตรฐานใหม่.
- **WPA2 (802.11i):** เป็นมาตรฐานที่ แนะนำให้ใช้มากที่สุดในปัจจุบัน. ใช้การเข้ารหัสแบบ AES (Advanced Encryption Standard) และโปรโตคอล CCMP ซึ่งมีความแข็งแกร่งสูงมาก.
- **WPA3:** มาตรฐานใหม่ล่าสุดที่พัฒนาต่อยอดเพื่อปิดช่องโหว่ของ WPA2 โดยมีการแลกเปลี่ยนคีย์แบบ Dragonfly (SAE) ที่ทนทานต่อการโจมตีได้ดีกว่าเดิม

เฟรมเวิร์ก 802.1x และ EAP

802.1x เป็นมาตรฐาน IEEE สำหรับการควบคุมการเข้าถึงเครือข่ายผ่านพอร์ต (Port-based Access Control) เพื่อจำกัดสิทธิ์ให้เฉพาะอุปกรณ์ที่ได้รับอนุญาตเท่านั้น โดยทำงานร่วมกับ EAP (Extensible Authentication Protocol) ซึ่งเป็นเฟรมเวิร์กการพิสูจน์ตัวตนที่ยืดหยุ่น

องค์ประกอบของ 802.1x

- Supplicant (ผู้ร้องขอ): อุปกรณ์หรือซอฟต์แวร์บนเครื่องลูกค้าที่ต้องการเข้าถึงเครือข่าย
- Authenticator (ผู้ตรวจสอบ): อุปกรณ์เครือข่าย เช่น Access Point หรือ Switch ที่ทำหน้าที่เป็นตัวกลางส่งต่อข้อมูลการยืนยันตัวตน
- Authentication Server (เซิร์ฟเวอร์ตรวจสอบ): โดยปกติจะเป็นเซิร์ฟเวอร์ RADIUS ที่เก็บฐานข้อมูลผู้ใช้ (เช่น Active Directory) เพื่อตัดสินว่าจะอนุญาตให้เข้าใช้งานหรือไม่

ประเภทของ EAP ที่นิยมใช้

EAP อนุญาตให้เพิ่มโมดูลการพิสูจน์ตัวตนใหม่ๆ ได้โดยไม่ต้องแก้ระบบปฏิบัติการทั้งหมด:

- **EAP-TLS:** ใช้ใบรับรองดิจิทัล (Certificates) ทั้งฝั่งผู้ใช้และเซิร์ฟเวอร์ มีความปลอดภัยสูงมากแต่ต้องมีระบบจัดการใบรับรอง (PKI)
- **PEAP และ EAP-TTLS:** สร้าง "อุโมงค์ TLS" ที่ปลอดภัยเพื่อส่งข้อมูลการล็อกอินแบบดั้งเดิม (เช่น รหัสผ่าน) ช่วยป้องกันการดักฟังรหัสผ่านบนเครือข่ายไร้สาย
- **EAP-MD5:** เป็นระดับพื้นฐานที่สุด แต่มีข้อเสียคือไม่รองรับการตรวจสอบฝั่งเซิร์ฟเวอร์ ทำให้เสี่ยงต่อการถูกหลอกโดย Access Point ปลอม

การบริหารจัดการ Wireless LAN ในระดับองค์กร

โดยมีหลักการสำคัญดังนี้:

- **การควบคุมการเข้าถึงที่เข้มงวด:** องค์กรจะใช้มาตรฐาน WPA2/WPA3 Enterprise ร่วมกับ 802.1x เพื่อควบคุมการเข้าถึงเครือข่ายผ่านพอร์ต. ระบบนี้ทำงานร่วมกับเซิร์ฟเวอร์ส่วนกลางอย่าง RADIUS หรือ TACACS+ ในการพิสูจน์ตัวตนผู้ใช้งาน.
- **เฟรมเวิร์กการพิสูจน์ตัวตน (EAP):** ใช้โปรโตคอล EAP เพื่อรองรับวิธีที่หลากหลาย เช่น EAP-TLS ที่ใช้ใบรับรองดิจิทัล (Certificates) ซึ่งมีความปลอดภัยสูงสุด หรือ PEAP ที่สร้างอุโมงค์ที่ปลอดภัยเพื่อส่งข้อมูลยืนยันตัวตน.
- **การเฝ้าระวังเชิงรุก (WIDS/WIPS):** ติดตั้งระบบตรวจจับและยับยั้งการบุกรุกไร้สายเพื่อระบุอุปกรณ์แปลกปลอม (Rogue Access Points), การโจมตีแบบสวมรอย (Spoofing) หรือการรบกวนสัญญาณ (Jamming).
- **การแบ่งส่วนเครือข่าย (Segmentation):** เครือข่ายไร้สายจะไม่เชื่อมต่อกับ LAN ภายในโดยตรง แต่จะถูกแยกเป็นโซนที่เชื่อถือได้น้อยกว่า หรือกำหนดให้เป็น DMZ และใช้ VLAN ในการแบ่งกลุ่มผู้ใช้งานเพื่อจำกัดขอบเขตความเสียหายหากถูกเจาะระบบ.
- **การจัดการอุปกรณ์พกพา (MDM):** ใช้ระบบ MDM เพื่อบังคับใช้นโยบายความปลอดภัยบนอุปกรณ์ที่พนักงานนำมาใช้ (BYOD) เช่น การตั้งค่ารหัสผ่าน, การติดตั้งใบรับรองอัตโนมัติ และการลบข้อมูลระยะไกล (Remote Wipe) หากอุปกรณ์สูญหาย

การรักษาความปลอดภัยในเครือข่ายไร้สาย

- **มาตรฐานการเข้ารหัสและโปรโตคอล:** เลือกใช้ WPA2 Enterprise หรือ WPA3 ซึ่งใช้การเข้ารหัส AES/CCMP ที่แข็งแกร่ง โดยต้องปิดฟีเจอร์ WPS (Wi-Fi Protected Setup) เพื่อป้องกันการโจมตีรหัสผ่าน และหลีกเลี่ยง WEP ที่ล้าสมัย.
- **การพิสูจน์ตัวตนระดับองค์กร**: บังคับใช้มาตรฐาน 802.1x ร่วมกับโปรโตคอล EAP-TLS (ใช้ใบรับรองดิจิทัล) และใช้เซิร์ฟเวอร์ RADIUS หรือ TACACS+ เพื่อจัดการสิทธิ์แบบรวมศูนย์และรองรับการพิสูจน์ตัวตนหลายปัจจัย (MFA).
- **การออกแบบสถาปัตยกรรมเครือข่าย:** แยกเครือข่ายไร้สายออกจาก LAN ภายในด้วย VLAN หรือกำหนดให้เป็นเขต DMZ และเชื่อมต่อผ่านอุโมงค์ VPN ที่มีการเข้ารหัสเสมอ

การรักษาความปลอดภัยในเครือข่ายไร้สาย

- **การตั้งค่าอุปกรณ์ (Hardening):**
  - เปลี่ยนค่า SSID และรหัสผ่านเริ่มต้นเป็นชื่อที่เป็นกลาง.
  - ปิดการกระจายสัญญาณ (SSID Broadcast) แม้จะยังดักจับได้แต่ช่วยลดการเป็นเป้าสายตา.
  - เปิดใช้งาน Client Isolation เพื่อไม่ให้ผู้ใช้งานในวง Wi-Fi เดียวกันโจมตีกันเองได้.
  - ใช้การกรอง MAC Address เพื่อจำกัดอุปกรณ์ที่ได้รับอนุญาต.
- **การเฝ้าระวังและการบำรุงรักษา:**
  - ติดตั้งระบบ WIDS/WIPS เพื่อตรวจจับและยับยั้ง Rogue Access Point.
  - ทำ Site Survey เพื่อปรับกำลังส่งสัญญาณ (Power Output) ไม่ให้รั่วไหลออกนอกเขตอาคารเกินจำเป็น.
  - อัปเดตเฟิร์มแวร์และไดรเวอร์ให้เป็นปัจจุบัน และทำการทดสอบเจาะระบบ (Penetration Testing) อย่างน้อยปีละครั้ง.
- **การจัดการอุปกรณ์พกพา:** ใช้ระบบ MDM (Mobile Device Management) เพื่อบังคับใช้นโยบายความปลอดภัยและสั่งลบข้อมูลระยะไกล (Remote Wipe) หากอุปกรณ์สูญหาย

Firewall และการควบคุมทราฟฟิกเครือข่าย

ไฟร์วอลล์ คือ อุปกรณ์ หรือฮาร์ดแวร์ หรือซอฟต์แวร์ หรือกลุ่มของอุปกรณ์เครือข่ายที่ถูกออกแบบมาเพื่ออนุญาต หรือให้สิทธิ์ในการส่งข้อมูลผ่านเครือข่ายที่อยู่บนพื้นฐานของกฎและระเบียบที่ได้มีการตั้งไว้ภายในแต่ละหน่วยงาน (จักรชัย โสอินทร์, 2559, หน้า 236)

ประเภทของไฟร์วอลล์

- Packet Filtering Firewall : เป็นรูปแบบของไฟร์วอลล์ที่มีความซับซ้อนน้อยที่สุด เป็นพื้นฐานเบื้องต้นของไฟร์วอลล์ประเภทต่าง ๆ (จักรชัย โสอินทร์, 2559, หน้า 236) จะทำการตรวจสอบแพ็กเก็ตว่าตรงกับเงื่อนไขหรือเกณฑ์ที่ผู้ดูแลระบบกำหนดไว้หรือไม่ ถ้าผ่านเกณฑ์ทั้งหมด=ข้อมูลมีความน่าเชื่อถือ ข้อมูลก็จะถูกส่งออกไปหรือรับเข้ามาในเครือข่าย ถ้าไม่ผ่านเกณฑ์=ข้อมูลไม่น่าเชื่อถือ ก็จะถูกปฏิเสธการนำเข้าหรือส่งออก
- Circuit-level Gateway : เป็นรูปแบบของไฟร์วอลล์ที่ใช้ตรวจสอบเส้นทางการเชื่อมต่อของเครือข่าย โดยสร้างแบบจำลองโครงข่ายการเชื่อมต่อขึ้นเพื่อพิจารณาความน่าเชื่อถือของเครือข่าย โดย Firewall ประเภทนี้จะไม่สามารถตรวจสอบแพ็กเก็ตด้วยตนเองได้ การตรวจสอบ แพ็กเก็ตจะทำงานบน Transport Layer (Layer ที่ทำหน้าที่จัดระเบียบแพ็กเก็ต) ใน OSI Model (แบบจำลองการสื่อสาร)
- Stateful Inspection Firewall : เป็นรูปแบบของไฟร์วอลล์ที่ใช้ตรวจสอบ แพ็กเก็ต ซึ่งสามารถตรวจสอบได้ว่า แพ็กเก็ตนี้เคยเข้ามาในระบบหรือไม่ โดยนำข้อมูลของ Packet เดิมและแพ็กเก็ตปัจจุบันมาตรวจสอบกัน ซึ่งมีความปลอดภัยกว่าการตรวจสอบแพ็กเก็ต หรือการเชื่อมต่อเพียงอย่างเดียว

ประเภทของไฟร์วอลล์

- **Application-level Gateway :** เป็นรูปแบบของไฟร์วอลล์ประเภทที่ติดตั้งอยู่บนคอมพิวเตอร์ และใช้การเชื่อมต่อกับ Router เพื่อตรวจสอบเส้นทางการส่งข้อมูลและเนื้อหาของแพ็กเก็ต นอกจากนั้นยังกรองและปิดกันการโจมตีที่มองไม่เห็นบนเครือข่าย OSI Model ได้ และยังสามารถทำหน้าที่แทน Proxy Firewall (ระบบรักษาความปลอดภัยเครือข่าย) ได้ในบางครั้ง
- **Next-generation Firewall :** เป็นรูปแบบของไฟร์วอลล์ที่รวมการตรวจสอบเส้นทางเครือข่ายและแพ็กเก็ตไว้ด้วยกัน โดยสามารถตรวจสอบแพ็กเก็ตในเชิงลึก (Deep Packet Inspection) อันเป็นวิธีการขั้นสูงในการตรวจสอบแพ็กเก็ตและเครือข่าย เป็นการรวมรูปแบบการตรวจสอบแพ็กเก็ตที่หลากหลาย รวมไปถึงการตรวจจับป้องกันมัลแวร์ และไวรัสคอมพิวเตอร์ อีกด้วย

ระบบตรวจจับและป้องกันการบุกรุก (IDS / IPS / XDR)

ระบบตรวจจับการบุกรุก (IDS)

ระบบการตรวจจับการบุกรุก (Intrusion Detection System: IDS) คือ ระบบซอฟต์แวร์หรือฮาร์ดแวร์ที่ติดตามการจราจรและพฤติกรรมที่น่าสงสัยในเครือข่าย (พนิดา พานิชกุล, 2553, หน้า 136) จะคอยจับตาดูระบบและทรัพยากรของเครือข่าย แล้วรายงานให้ผู้ดูแลรักษาความปลอดภัยทราบ เมื่อมีความเป็นไปได้ว่ามีผู้บุกรุกเข้ามาแล้ว

ระบบตรวจจับการบุกรุก (IDS)

IDS ส่วนใหญ่จะแจ้งเตือนข้อมูลพื้นฐานเกี่ยวกับการโจมตี คือ

1. วันเวลา
2. IP ของ IDS ที่รายงาน
3. ชื่อของการโจมตี
4. หมายเลขไอพีต้นทางและปลายทาง
5. หมายเลขพอร์ตของต้นทางและปลายทาง
6. ชื่อโปรโตคอลที่ใช้สำหรับการโจมตี

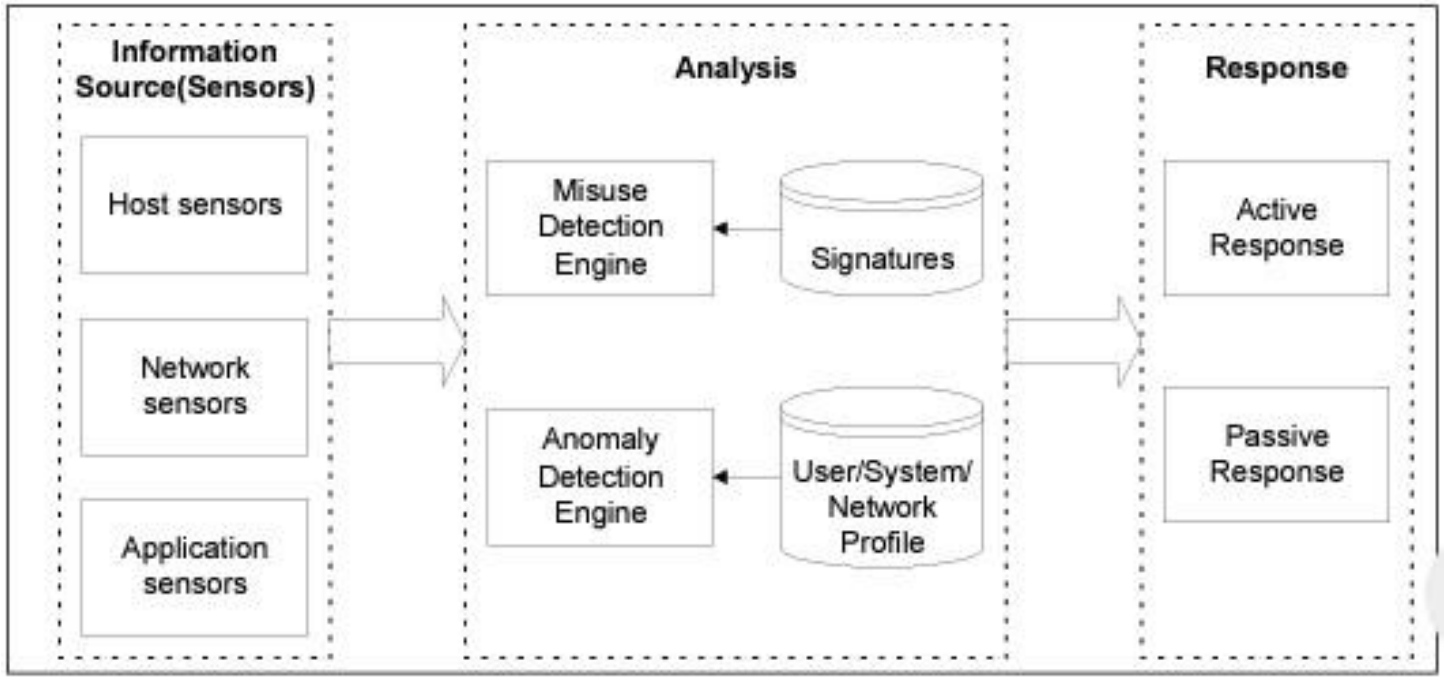
ตัวอย่างกิจกรรมที่น่าสงสัยว่ามีผู้บุกรุกเข้ามา เช่น มีผู้พยายาม Log in เข้าใช้ข้อมูล แต่เข้าไม่ได้หลาย ๆ ครั้ง มีการเข้าใช้ระบบในช่วงเวลาที่ผิดปกติ การใช้ระบบการตรวจจับการบุกรุกนี้เป็นการเพิ่มการป้องกันอีกชั้นหนึ่งในกรณีที่ผู้บุกรุกได้ผ่านระบบรักษาความปลอดภัยชั้นนอก (เช่น รหัสผ่าน firewall) เข้ามาแล้ว

องค์ประกอบสำหรับระบบตรวจจับการบุกรุก (IDS)

- ประกอบด้วย 3 องค์ประกอบพื้นฐานสามส่วนดังนี้ (Bace and Mell, 2001)

1. Information Source (Sensor) ข้อมูลเหตุการณ์และข้อมูลการทำงานจากแหล่งข้อมูลต่าง ๆ จะถูกนำไปใช้ในการวิเคราะห์เพื่อตัดสินว่าเมื่อใดที่มีการบุกรุกเกิดขึ้น โดยแหล่งข้อมูลเหล่านี้จะนำมาจากข้อมูลในระดับต่าง ๆ ของระบบเครือข่าย
2. Analysis เป็นส่วนที่ทำหน้าที่ในการจัดการและวิเคราะห์ข้อมูลที่ได้รับจากแหล่งข้อมูลต่าง ๆ แล้วตัดสินว่าเหตุการณ์หรือการกระทำใดที่บ่งชี้ว่ากำลังมีการบุกรุกเกิดขึ้นหรือได้มีการบุกรุกเกิดขึ้นแล้วในระบบ โดยแนวทางที่ใช้ในการวิเคราะห์มีสองรูปแบบคือ Anomaly Detection และ Misuse Detection
3. Response เป็นชุดของการกระทำเมื่อระบบตรวจจับการบุกรุกตรวจจับได้ว่ามีการบุกรุกเกิดขึ้น โดยการกระทำเหล่านี้สามารถจัดกลุ่มได้เป็นการกระทำแบบ Active มีการตอบสนองต่อเหตุการณ์การบุกรุกนั้นโดยอัตโนมัติ เช่น การปรับค่าของเราเตอร์หรือไฟร์วอลล์ให้ปิดกั้นการเชื่อมต่อที่ส่งมาจากผู้บุกรุก และการกระทำแบบ Passive จะเป็นการรายงานหรือแจ้งเตือนการบุกรุกไปยังบุคคลที่รับผิดชอบเพื่อแก้ไขปัญหา โดยอาศัยข้อมูลที่ได้รับรายงาน

ระบบตรวจจับการบุกรุก (IDS)



ระบบตรวจจับการบุกรุก (IDS)

- **ระบบตรวจจับการบุกรุกบนเครือข่าย (Host-based Intrusion Detection System: HIDS)** การทำงานตรวจสอบการบุกรุกนั้นจะเน้นไปยังการตรวจสอบกิจกรรม หรือข้อมูลต่าง ๆ ที่โฮสต์ หรือเซิร์ฟเวอร์เท่านั้น โดยที่อาจจะเป็นการเฝ้าระวังสถานะของไฟล์ระบบต่าง ๆ รวมไปถึงการตรวจสอบเมื่อมีการสร้าง เปลี่ยนแปลง หรือแม้กระทั่งลบไฟล์ต่าง ๆ ของระบบ

- จุดเด่นของ HIDS
    1. วิเคราะห์ของจากล็อกไฟล์ของระบบจึงทำให้ทราบเหตุการณ์และกิจกรรมต่าง ๆ ที่เกิดขึ้นในระบบอย่างละเอียด
    2. ตรวจจับการบุกรุกที่เกิดขึ้นบนเครื่องคอมพิวเตอร์นั้น ๆ โดยตรง โดยไม่ผ่านเครือข่าย
    3. ช่วยในการตรวจจับโปรแกรมประเภทม้าโทรจัน หรือการบุกรุกอื่น ๆ ที่ผลกับความสมบูรณ์ของโปรแกรมและข้อมูลต่าง ๆ ของระบบคอมพิวเตอร์

ระบบตรวจจับการบุกรุก (IDS)

- **ระบบตรวจจับการบุกรุกภายในเครื่อง (Network-based Intrusion Detection System: NIDS)** การตรวจสอบในรูปแบบนี้จะอยู่บนเครือข่าย หรืออีกนัยหนึ่งก็คือ ไม่มีการติดตั้งโดยตรงไปยังเซิร์ฟเวอร์ที่ให้บริการต่าง ๆ โดยทำหน้าที่ตรวจสอบรูปแบบของการโจมตีประเภทต่าง ๆ ผ่านทางข้อมูลหรือแพ็กเก็ตได้หลายเครื่องพร้อมกันที่มีการส่งผ่านบนเครือข่าย ดังนั้น การติดตั้งจะต้องอยู่ในส่วนของเครือข่ายที่ข้อมูลทั้งหมดมีการส่งผ่าน (จักรชัย โสอินทร์, 2559, หน้า 210) เช่น มีการลบไฟล์หรือปรับตั้งค่าสำคัญในช่วงเวลาที่ไม่ปกติหรือผิดขั้นตอน ภายในเครื่องนั้น ๆ

- จุดเด่นของ NIDS
  1. มีค่าใช้จ่ายต่ำ
  2. ตรวจสอบแพ็กเก็ตทั้งหมดเพื่อวิเคราะห์หาร่องรอยของการกระทำที่มุ่งประสงค์ร้าย
  3. ติดตั้งได้ง่าย
  4. มีความปลอดภัยต่อการโจมตีได้ดีกว่า เนื่องผู้โจมตีไม่สามารถทราบได้ว่ามีระบบ NIDS ติดตั้งอยู่ในตำแหน่งใด ทำให้ยากที่ผู้โจมตีจะทำลายหลักฐานหรือร่องรอยต่าง ๆ ที่เกิดขึ้นจากการบุกรุกหรือโจมตีได้

ระบบตรวจจับการบุกรุก (IDS)

- มีความสามารถและคุณสมบัติดังต่อไปนี้ (Price, 1998)

1. ทำงานอยู่ตลอดเวลาได้เองโดยไม่ต้องมีการควบคุมของผู้ดูแลระบบ และระบบต้องมีความน่าเชื่อถือที่เพียงพอที่จะทำงานในลักษณะอยู่เบื้องหลัง (background process) แต่ผู้ดูแลระบบต้องสามารถตรวจสอบการทำงานจากภายนอกได้
2. เป็นระบบที่เป็น fault tolerant สามารถทำงานต่อไปได้ในกรณีที่ระบบคอมพิวเตอร์เกิดปัญหาหรือมีข้อผิดพลาดเกิดขึ้นและไม่ต้องมีการสร้างฐานข้อมูลความรู้ (knowledge-base) ทุกครั้งที่เริ่มระบบ
3. มีความสามารถในการตรวจสอบตัวเองเพื่อไม่ให้ถูกลบ ทำลาย แก้ไข หรือถูกแทนที่ด้วยโปรแกรมอื่นได้
4. ส่งผลกระทบกับการทำงานของระบบคอมพิวเตอร์น้อยที่สุด นั่นคือในการทำงานของระบบตรวจจับจะต้องใช้ทรัพยากรของระบบคอมพิวเตอร์น้อยที่สุดเท่าที่จะทำได้ เพราะถ้าหากทำให้ระบบคอมพิวเตอร์ทำงานช้าลงแล้วก็จะส่งผลให้ไม่มีการใช้งานระบบตรวจจับการบุกรุก

ระบบตรวจจับการบุกรุก (IDS)

5. ตรวจสอบการทำงานที่ผิดไปจากรูปแบบการทำงานปกติได้
6. ปรับเปลี่ยนหรือแก้ไขให้เข้ากับระบบคอมพิวเตอร์ได้ง่าย เนื่องจากแต่ละระบบคอมพิวเตอร์จะมีรูปแบบการใช้งานและกลไกในการป้องกันที่ต่างกัน
7. ปรับการทำงานให้สอดคล้องกับการเปลี่ยนแปลงพฤติกรรมการใช้งานของระบบได้ เช่น เมื่อมีการติดตั้งโปรแกรมใหม่ ระบบ IDS ก็ต้องสามารถปรับเปลี่ยนการทำงานให้เข้ากับระบบที่เปลี่ยนไปได้
8. มีความผิดพลาดในการทำงานน้อยที่สุด

ความแตกต่างของระบบตรวจจับการบุกรุก (IDS) และไฟร์วอลล์

- Firewall ทำหน้าที่ตรวจสอบแพ็กเกจที่วิ่งเข้าในเครือข่าย ในขณะที่ IDS เป็นการตรวจสอบเพื่อวิเคราะห์และหารูปแบบการบุกรุก โดยเปรียบเทียบกับเหตุการณ์ที่เป็นการบุกรุกในฐานข้อมูลในระบบ ถ้าตรงกันระบบก็จะทำการแจ้งเตือน

การป้องกันการโจมตีพอร์ต การแบ่งส่วนเครือข่าย และการควบคุมการเข้าถึง

วิธีการป้องกันการโจมตีพอร์ตที่เปิดให้บริการ

- **การโจมตีพอร์ต (Port Scanning)** เป็นเทคนิคที่ผู้บุกรุกใช้ในการค้นหาบริการที่จะสามารถเจาะผ่านเข้าไปยังระบบได้ โดยปกติแล้วทุก ๆ ระบบที่ต่อเข้าสู่ระบบ LAN หรือระบบอินเทอร์เน็ตจะเปิดบริการทั้งที่อยู่บนพอร์ตที่เป็นที่รู้จักและที่ไม่เป็นที่รู้จัก เช่น หากใช้เครื่องมือ Port Scanning ตรวจสอบพอร์ต 80 เปิดหรือให้บริการอยู่ แสดงว่าเครื่องนั้นน่าจะทำหน้าที่เป็น Web Server เป็นต้น (สุเมธ จิตภักดีบดินทร์, 2556, หน้า 116)

วิธีการป้องกัน Packet Routing และ Filtering

- **วิธีการป้องกัน Packet Routing และ Filtering โดยใช้ Packet Filtering Firewall** ที่มีหน้าที่กรองแพ็กเก็ตโดยพิจารณาเพียงฟิลด์ต่าง ๆ ที่สำคัญบนเฮดเดอร์ของแพ็กเก็ต เช่น Protocol, Source IP Address, Destination IP Address, Source Port และ Destination Port หากแพ็กเก็ตที่วิ่งเข้ามาหรือออกจากเน็ตเวิร์กตรงตามเงื่อนไขไว้ก็จะถูกตัดสินตามสิ่งที่กำหนดไว้ใน Action ว่าจะอนุญาตให้แพ็กเก็ตนั้นผ่านไปได้หรือห้ามไม่ให้ผ่าน โดยแพ็กเก็ต Filtering Firewall ไม่มองเข้าไปถึงค่าอื่น ๆ ใน TCP header (ศุภามน วาณิชย์ก่อกุล และคณะ, 2548)

การเข้ารหัสข้อมูลและความปลอดภัยของการสื่อสาร

เทคนิคการเข้ารหัสและการถอดรหัสขั้นพื้นฐาน

เมื่อมีการถ่ายโอนข้อมูลจากจุดหนึ่งไปยังจุดอื่น ๆ ในเครือข่ายคอมพิวเตอร์ ต้องคำนึงถึงความมั่นใจในด้านของความปลอดภัยของข้อมูล ที่จะต้องเดินทางไปยังกลุ่มเครือข่ายต่าง ๆ มากมาย ซึ่งความปลอดภัยในที่นี้ได้ครอบคลุมความหมายอยู่ 2 ประการ คือ

1) ในระหว่างการส่งข้อมูล จะต้องไม่มีใครคนใดที่จะสามารถเข้าไปลักลอบหรือสกัดกั้นข้อมูลเพื่อคัดลอกข้อมูลไปใช้งานได้

2) ในระหว่างการส่งข้อมูล จะต้องไม่มีใครคนใดที่จะสามารถเข้าไปเพิ่มเติมหรือเปลี่ยนแปลงต้นฉบับให้ผิดเพี้ยนไปจากเดิม (Annie James, 2560)

เทคนิคการเข้ารหัสและการถอดรหัสขั้นพื้นฐาน

- เทคนิคการแทนที่ (Substitution Techniques)
- เทคนิคการสับเปลี่ยน (Transposition Techniques)

เทคนิคการแทนที่ (Substitution Techniques)

- **การเข้ารหัสด้วยวิธีการแทนที่แบบโมโนอัลฟาเบติก (Monoalphabetic Substitution-Based Cipher)**

Plaintext : a b c d e f g h i j k l m n o p q r s t u v w x y z

Ciphertext : z y x w v u t s r q p o n m l k j i h g f e d c b a

ตัวอย่างเช่น how are you ก็จะถูกเข้ารหัสเป็น sld ziv blf

เทคนิคการแทนที่ (Substitution Techniques)

- **การเข้ารหัสด้วยวิธีการแทนที่แบบโพลีอัลฟาเบติก (Polyalphabetic Substitution Based Cipher)**
  เป็นการเข้ารหัสที่มีการนำคีย์เข้ามาเกี่ยวข้องด้วย ซึ่งมีความคล้ายคลึงกับแบบแรกมาก เช่น ตัวอักษรภาษาอังกฤษมี 26 ตัวก็จะสร้างตาราง 26 * 26

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

เทคนิคการแทนที่ (Substitution Techniques)

มหาวิทยาลัยราชภัฏนครปฐม

กำหนดให้

Plaintext: HELLO

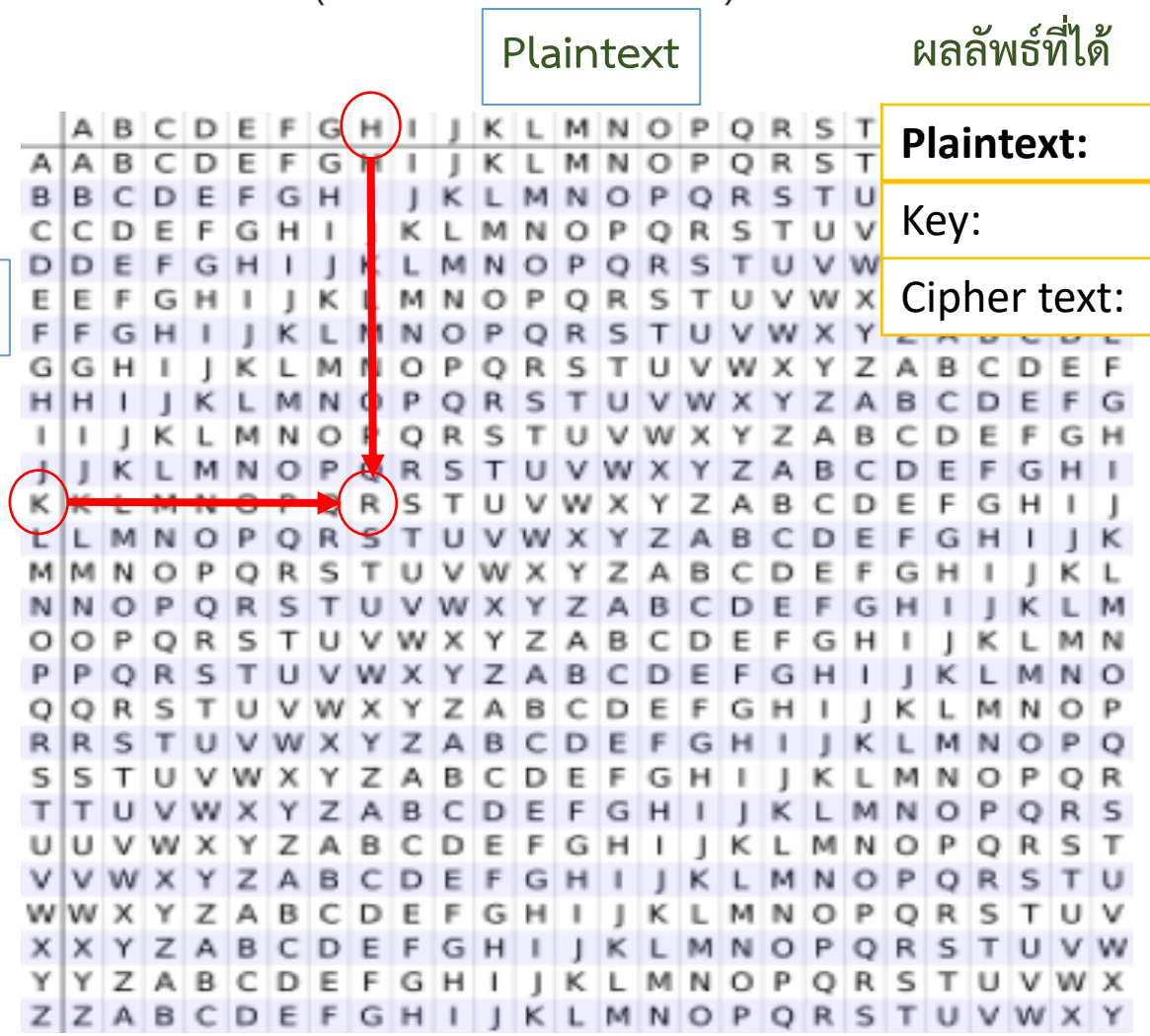
Key: KEY

1 ทำให้ Key ยาวเท่าข้อความ

```
Plaintext : H  E  L  L  O
Key       : K  E  Y  K  E
```

2 เข้ารหัสทีละตัว

ใช้ตาราง (หรือคิดแบบเลื่อนตัวอักษร)



ผลลัพธ์ที่ได้

Plaintext:	**H**	**E**	**L**	**L**	**O**
Key:	K	E	Y	K	E
Cipher text:	R				

การเข้ารหัสด้วยวิธีการแทนที่แบบโพลีอัลฟาเบติก (Polyalphabetic Substitution Based Cipher) ที่ยกในมาในบทนี้ คือ การเข้ารหัสข้อมลแบบ Vigenere cipher มีวิธีการเข้ารหัสต่อไปนี้

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Plain Text:	A	T	T	A	C	K		A	T		D	A	W	N
Key:	L	E	M	O	N									
Cipher Text:														

เทคนิคการสับเปลี่ยน (Transposition Techniques)

- **การเข้ารหัสด้วยวิธีการสับเปลี่ยนแบบเรสเฟ็นซ์ (Rail Fence Transposition Cipher)** วิธีนี้เป็นการเข้ารหัสอย่างง่าย โดยจะเข้ารหัสในลักษณะ row-by-row หรืออาจเรียกวิธีนี้ว่า วิธีซิกแซ็ก ก็ได้

ตัวอย่างเช่น เพลนเท็กซ์คำว่า Come home tomorrow จะถูกเข้ารหัสเป็น Cmhmtmrooeoerw

เทคนิคการสับเปลี่ยน (Transposition Techniques)

- **การเข้ารหัสด้วยวิธีการสับเปลี่ยนแบบคอลัมน์ (Columnar Transposition Cipher)** วิธีนี้จะเป็นการเข้ารหัสที่มีประสิทธิภาพวิธีหนึ่ง โดยจะใช้ร่วมกับคีย์ที่กำหนดขึ้น ไม่มีตัวอักษรใดที่ซ้ำกัน ทำให้ถอดรหัสได้ยาก

  1) กำหนดตำแหน่งลำดับของแต่ละคอลัมน์นิยมเรียงตำแหน่งคอลัมน์ตามลำดับของแต่ละตัวอักษร

  2) นำเพลนเท็กซ์ที่ต้องการมาเข้ารหัสด้วยการเขียนตามลำดับหากครบจำนวนคอลัมน์ก็ให้ปัดขึ้นบรรทัดใหม่ เช่น this is the best class I have ever taken (Annie James, 2560)

ตัวอย่าง กำหนดให้

Plaintext: HELLO WORLD

Key: KEY

ขั้นตอน

1 เรียงลำดับคีย์

คีย์ = K E Y

เรียงตาม A–Z → E K Y

2 เขียนข้อความลงตาราง

เขียนทีละตัวตามแถว

K	E	Y

3 อ่านตามลำดับคอลัมน์ (1 → 2 → 3)

ความมั่นคงปลอดภัยในระบบ Cloud มาตรฐาน และกฎหมายที่เกี่ยวข้อง

ความมั่นคงปลอดภัยในระบบคลาวด์ (Cloud Security) คือมาตรการและเทคโนโลยีที่ใช้ปกป้องข้อมูล แอปพลิเคชัน และโครงสร้างพื้นฐานที่ทำงานผ่านอินเทอร์เน็ต

เทคโนโลยีและมาตรการความปลอดภัย

- การควบคุมการเข้าถึง (IAM): ใช้การยืนยันตัวตนแบบหลายปัจจัย (MFA) และการทำ Federation เพื่อเชื่อมต่อบัญชีผู้ใช้งานจากระบบภายในไปยังคลาวด์อย่างปลอดภัย,
- การเข้ารหัสข้อมูล (Encryption): ต้องเข้ารหัสทั้งข้อมูลที่เก็บอยู่ (At rest) และระหว่างการรับส่ง (In transit) โดยองค์กรควรจัดการกุญแจเข้ารหัสเองเพื่อความเชื่อมั่นสูงสุด,
- การป้องกันเครือข่ายและแอปพลิเคชัน: ติดตั้ง Web Application Firewall (WAF), ระบบตรวจจับการบุกรุก (IDS) และใช้ Cloud Access Security Broker (CASB) เพื่อเพิ่มทัศนวิสัยและการควบคุม,,
- ความรับผิดชอบร่วมกัน (Shared Responsibility): ผู้ให้บริการคลาวด์ดูแลโครงสร้างพื้นฐาน แต่ "ลูกค้า" มีหน้าที่รับผิดชอบความปลอดภัยของข้อมูลและการตั้งค่าระบบให้ถูกต้อง

มาตรฐานที่สำคัญ

- ISO/IEC 27001 & 27002: มาตรฐานสากลสำหรับการจัดการความมั่นคงปลอดภัยสารสนเทศ (ISMS),
- NIST Cybersecurity Framework: กรอบการทำงานที่เน้นการบริหารจัดการความเสี่ยง,
- Cloud Controls Matrix (CCM): พัฒนาโดย Cloud Security Alliance (CSA) เพื่อกำหนดมาตรฐานการควบคุมความปลอดภัยบนคลาวด์โดยเฉพาะ,
- FedRAMP: มาตรฐานความปลอดภัยสำหรับบริการคลาวด์ที่ใช้ในหน่วยงานรัฐบาลสหรัฐฯ

กฎหมายที่เกี่ยวข้อง

- **GDPR (ยุโรป):** กฎหมายคุ้มครองข้อมูลส่วนบุคคลที่มีบทลงโทษสูงและมีผลบังคับใช้ทั่วโลกหากมีการประมวลผลข้อมูล
- **LGPD (บราซิล):** กฎหมายคุ้มครองข้อมูลส่วนบุคคลของประเทศบราซิลที่มีลักษณะคล้าย GDPR
- **HIPAA (สหรัฐฯ):** กำหนดการคุ้มครองข้อมูลสุขภาพอิเล็กทรอนิกส์ (EPHI) บนระบบคลาวด์
- **FISMA (สหรัฐฯ):** กำหนดให้หน่วยงานรัฐต้องประเมินและลดความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ
- **PDPA:** พระราชบัญญัติการคุ้มครองส่วนบุคคล พ.ศ. 2562

บทสรุป

การรักษาความปลอดภัยบนเครือข่ายคือการปกป้องข้อมูลจากการเข้าถึงที่ไม่ได้รับอนุญาต การโจมตี และการขโมยข้อมูล ซึ่งครอบคลุมการรักษาความปลอดภัยเครือข่ายไร้สาย การใช้ไฟร์วอลล์ และระบบตรวจจับการบุกรุก (IDS) การเผชิญหน้ากับภัยคุกคามและการโจมตีเครือข่าย เช่น มัลแวร์และ DDoS และการป้องกันการโจมตีพอร์ตและแพ็กเก็ต เทคนิคการเข้ารหัสและการถอดรหัสช่วยปกป้องข้อมูลในเครือข่ายให้ปลอดภัยจากการโจรกรรมและการแอบดักฟัง

it's

Q&A

TIME!