พื้นฐานความรู้ด้านเครือข่ายเพื่อการจัดการด้านความปลอดภัย

เนื้อหา

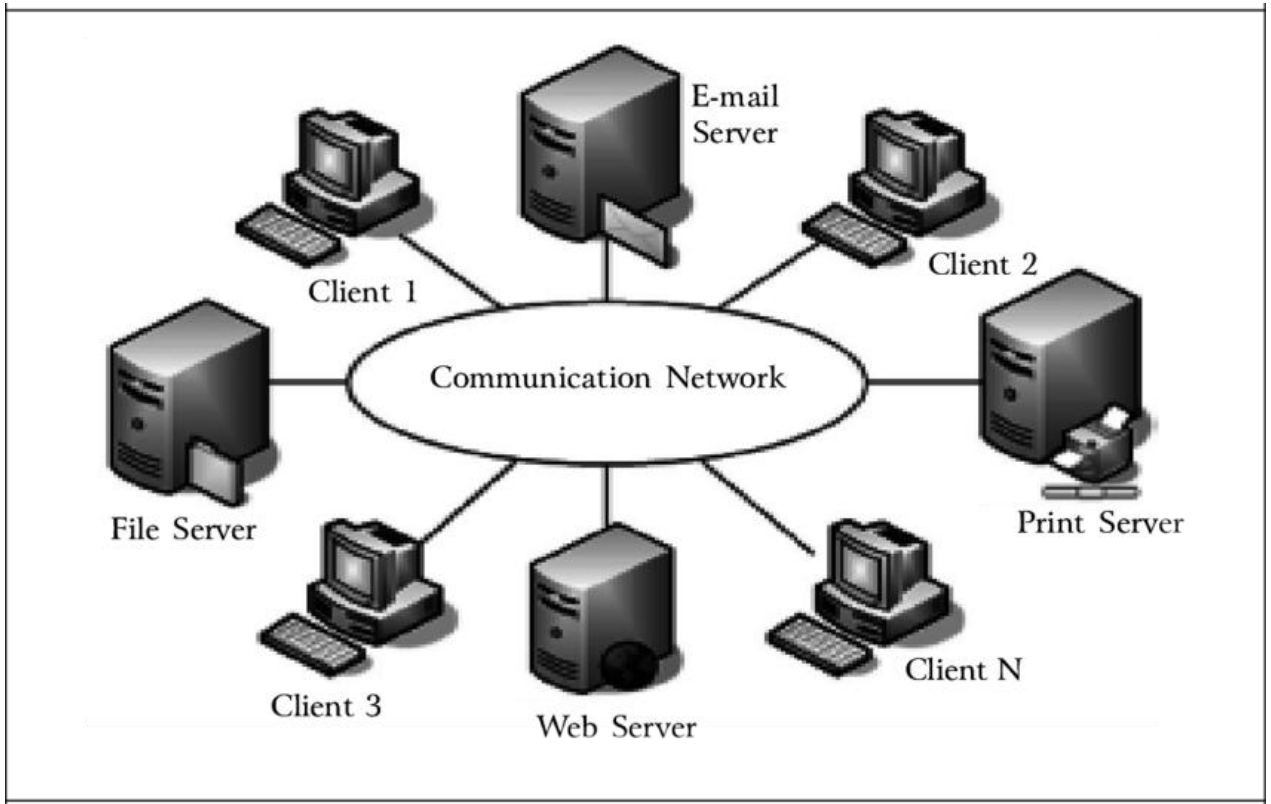
- บทบาทของเครือข่ายต่อความมั่นคงปลอดภัยสารสนเทศ
- ประเภทและสถาปัตยกรรมเครือข่ายในองค์กร
- องค์ประกอบของระบบเครือข่ายและการประยุกต์ใช้ด้านความปลอดภัย
- แบบจำลอง OSI และ TCP/IP กับการวิเคราะห์ภัยคุกคาม
- โปรโตคอลพื้นฐานและการประยุกต์ใช้ในการวิเคราะห์ปัญหาเครือข่าย
- โทโปโลยีเครือข่ายกับความทนทานและความเสี่ยงด้านความปลอดภัย
- ภัยคุกคามทางเครือข่ายและการประยุกต์วิเคราะห์สถานการณ์
- หลักการป้องกันเครือข่ายและการกำหนดนโยบายควบคุมการเข้าถึง
- การเฝ้าระวังและติดตามเหตุการณ์ด้านความมั่นคงปลอดภัยเครือข่าย

บทนำ:
บทบาทของเครือข่ายต่อความมั่นคงปลอดภัยสารสนเทศ

ประเภทและสถาปัตยกรรมเครือข่ายในองค์กร

ระบบเครือข่ายคอมพิวเตอร์ (Computer Network)

- หมายถึง การนำเครื่องคอมพิวเตอร์มาเชื่อมต่อเข้าด้วยกัน โดยอาศัยช่องทางการสื่อสารข้อมูล เพื่อแลกเปลี่ยนข้อมูลข่าวสารระหว่างเครื่องคอมพิวเตอร์ และการใช้ทรัพยากรของระบบร่วมกัน (Shared Resource) ในเครือข่ายนั้น



Source: Saxena and Arora (2009)

ประเภทของเครือข่าย

ประเภทของเครือข่ายในองค์กรแบ่งตามระยะทางและขอบเขตการใช้งาน ได้แก่:

- **เครือข่ายท้องถิ่น (Local Area Network: LAN)** เป็นเครือข่ายระยะใกล้ใช้กันอยู่ในบริเวณไม่กว้างนัก อาจอยู่ในองค์กรเดียวกัน หรืออาคารที่ใกล้กัน
- **เครือข่ายระดับเมือง (Metropolitan Area Network: MAN)** เป็นการรวมกลุ่มเครือข่ายท้องถิ่นเข้าด้วยกัน เป็นเครือข่ายขนาดกลาง
- **เครือข่ายระดับประเทศหรือเครือข่ายบริเวณกว้าง (Wide Area Network: WAN)** เป็นระบบเครือข่ายที่ติดตั้งใช้งานอยู่ในบริเวณกว้าง
- **Intranet และ Extranet:** Intranet คือเครือข่ายภายในเฉพาะพนักงาน ส่วน Extranet คือเครือข่ายที่อนุญาตให้คู่ค้าหรือซัพพลายเออร์ที่เชื่อถือได้เข้าถึงข้อมูลบางส่วน

ในบริบทองค์กรสมัยใหม่ มักมีการเชื่อมต่อแบบ Hybrid ระหว่าง LAN ภายในองค์กรกับ Cloud ผ่าน WAN หรือ Internet

สถาปัตยกรรมเครือข่ายในองค์กร

สำหรับสถาปัตยกรรมเครือข่ายในองค์กรที่สำคัญมีดังนี้ครับ:

- **โมเดล 3 ชั้น (Three-Tier Hierarchy):** ประกอบด้วยชั้น Core (กระดูกสันหลังเครือข่าย), Distribution (รวบรวมทราฟฟิก), และ Access (จุดเชื่อมต่อผู้ใช้) เป็นมาตรฐานที่ใช้ในระบบเครือข่ายขนาดใหญ่.
- **โมเดล 2 ชั้น (Two-Tier Architecture):** สถาปัตยกรรมที่แบนราบและรวดเร็วกว่า โดยยุบรวมชั้น Distribution และ Access เข้าด้วยกัน นิยมใช้ใน Data Center สมัยใหม่และระบบคลาวด์.
- **สถาปัตยกรรมแบบเปิด (Open Network):** เครือข่ายสมัยใหม่ที่มีความยืดหยุ่นสูง รองรับการเชื่อมต่อจากอินเทอร์เน็ต พนักงานที่ทำงานทางไกล และอุปกรณ์พกพา.
- **การแบ่งโซนความปลอดภัย (DMZ):** การสร้าง "เขตปลอดทหาร" (Demilitarized Zone) เพื่อแยกเซิร์ฟเวอร์ที่ให้บริการสาธารณะออกจากเครือข่ายภายใน ป้องกันไม่ให้แฮกเกอร์เข้าถึงทรัพยากรหลักได้โดยตรง.
- **Defense-in-Depth (Onion Model):** สถาปัตยกรรมที่เน้นการป้องกันเป็นชั้น ๆ ตั้งแต่นโยบาย เครือข่าย จนถึงตัวข้อมูล เพื่อให้มั่นใจว่าหากชั้นใดชั้นหนึ่งล้มเหลว ยังมีชั้นอื่นคอยป้องกันอยู่

องค์ประกอบของระบบเครือข่ายและการประยุกต์ใช้ด้านความปลอดภัย

คอมพิวเตอร์แม่ข่าย

- **คอมพิวเตอร์แม่ข่าย** หมายถึงคอมพิวเตอร์ ที่ทำหน้าที่เป็นผู้ให้บริการทรัพยากร (Resources) ต่าง ๆ ซึ่งได้แก่ หน่วยประมวลผล หน่วยความจำ หน่วยความจำสำรอง ฐานข้อมูล และ โปรแกรมต่าง ๆ เป็นต้น ในระบบเครือข่ายท้องถิ่น (LAN) มักเรียกว่าคอมพิวเตอร์แม่ข่าย ในระบบเครือข่ายระยะไกล ที่ใช้เมนเฟรมคอมพิวเตอร์ หรือ มินิคอมพิวเตอร์เป็นศูนย์กลางของเครือข่าย เรานิยมเรียกว่า Host Computer และเรียกเครื่องที่รอรับบริการว่าลูกข่ายหรือสถานีงาน

ช่องทางการสื่อสาร (Communication Chanel)

- ช่องทางการสื่อสาร หมายถึง สื่อกลางหรือเส้นทางที่ใช้เป็นทางผ่าน ในการรับส่งข้อมูล ระหว่างผู้รับ (Receiver) และผู้ส่งข้อมูล (Transmitter) ปัจจุบันมีช่องทางการสื่อสาร สำหรับการเชื่อมต่อเครือข่ายคอมพิวเตอร์มีหลายประเภทคือ สายโทรศัพท์แบบสายคู่ตีเกลียวไม่มีฉนวนหุ้ม (UTP) สายคู่ตีเกลียวแบบมีฉนวนหุ้ม (STP) สายโคแอคเชียว สายใยแก้วนำแสง คลื่นไมโครเวฟ และดาวเทียม เป็นต้น

สถานีงาน (Workstation or Terminal)

- หมายถึง อุปกรณ์หรือเครื่องไมโครคอมพิวเตอร์ ที่เชื่อมต่อ กับเครือข่ายคอมพิวเตอร์ ทำหน้าที่เป็นสถานีปลายทางหรือสถานีงาน ที่ได้รับการบริการจากเครื่อง คอมพิวเตอร์แม่ข่าย เรียกว่าเป็นคอมพิวเตอร์ลูกข่าย (Workstation) ในระบบเครือข่ายระยะใกล้ มักมีหน่วยประมวลผล หรือซีพียูของตนเอง ในระบบที่ใช้เครื่องคอมพิวเตอร์เมนเฟรม เป็นศูนย์กลาง เรียกสถานีปลายทางว่าเทอร์มินอล (Terminal) ประกอบด้วยจอภาพและแป้นพิมพ์เท่านั้น ไม่มีหน่วยประมวลกลางของตัวเอง ต้องใช้หน่วยประมวลผลของคอมพิวเตอร์ศูนย์กลางหรือ Host

อุปกรณ์ที่ใช้ในการเชื่อมต่อเครือข่าย

- Routers เป็นอุปกรณ์ในระบบเครือข่ายคอมพิวเตอร์ที่ทำหน้าที่เป็นตัวเชื่อมโยงให้เครือข่ายหลายเครือข่ายที่มีขนาดต่างกัน หรือใช้มาตรฐานการส่งผ่านข้อมูล (Transmission) ต่างกันสามารถติดต่อแลกเปลี่ยนข้อมูลระหว่างกันได้

- Switching เป็นอุปกรณ์ที่ทำหน้าที่กระจายช่องทางการสื่อสารข้อมูลหลายช่องทางการสื่อสารข้อมูลหลายช่องทางในระบบเครือข่ายคล้ายHubแต่ต่างกันในเรื่องของกรทำงานและความเร็ว คือ แต่ละช่องสัญญาณ (port) จะใช้ความเร็วเป็นอิสระต่อกันตามมาตรฐานความเร็ว

- Hub เป็นอุปกรณ์ที่ทวนและขยายสัญญาณเพื่อส่งต่อไปยังอุปกรณ์อื่นให้ได้ระยะทางที่ยาวไกลขึ้นไม่มีการเปลี่ยนแปลงข้อมูลก่อนและหลังการรับส่งและไม่มีการใช้ซอฟแวร์ใด ๆ มาเกี่ยวข้องกับอุปกรณ์ชนิดนี้ การติดตั้งทำได้ง่าย

- การ์ด LAN (Network Interface Card - NIC) เป็นการ์ดสำหรับต่อเครื่องพีซีเข้ากับสาย LAN

การประยุกต์ใช้ด้านความปลอดภัย

- **การปกป้องโฮสต์ (Host Protection):** เน้นการทำ Hardening โดยปิดบริการและพอร์ตที่ไม่ได้ใช้งาน, ติดตั้งซอฟต์แวร์ป้องกันมัลแวร์ (Antivirus), และใช้ Host-based IDS (HIDS) เพื่อเฝ้าระวังการเปลี่ยนแปลงไฟล์สำคัญ
- **การรักษาความปลอดภัยของสื่อกลางและโปรโตคอล (Medium & Protocol Security):** ใช้การเข้ารหัสข้อมูล (Encryption) เช่น SSL/TLS หรือ VPN เพื่อสร้างอุโมงค์สื่อกลางที่ปลอดภัยบนเครือข่ายสาธารณะ และเลือกใช้โปรโตคอลที่ปลอดภัยแทนรุ่นเก่า เช่น ใช้ SSH แทน Telnet หรือ HTTPS แทน HTTP.
- **การควบคุมอุปกรณ์เครือข่าย (Network Device Security):**
  - Switch: ใช้ Port Security เพื่อจำกัดสิทธิ์ให้เฉพาะอุปกรณ์ (MAC Address) ที่ได้รับอนุญาตเชื่อมต่อได้ และใช้ VLAN เพื่อแบ่งส่วนเครือข่าย (Segmentation) ลดขอบเขตความเสียหายหากถูกโจมตี.
  - Router: กำหนด Access Control Lists (ACLs) เพื่อกรองแพ็กเก็ตที่ต้นทาง และปิดบริการเสริมที่เสี่ยง เช่น BoOTP, TFTP หรือ Finger.
- **ระบบป้องกันส่วนหน้า (Perimeter Defense):** ติดตั้ง Firewall เพื่อคัดกรองทราฟฟิกขาเข้า-ขาออกตามกฎที่กำหนด และใช้ระบบ IDS/IPS เพื่อตรวจจับและยับยั้งพฤติกรรมที่น่าสงสัยในระดับลึกกว่าที่ไฟร์วอลล์จะมองเห็น.
- **การจัดการตัวตน (IAAA):** บังคับใช้การยืนยันตัวตนแบบหลายปัจจัย (MFA) และหลักการสิทธิ์ขั้นต่ำที่จำเป็น (Least Privilege) เพื่อให้มั่นใจว่าแต่ละคนเข้าถึงได้เฉพาะสิ่งที่จำเป็นต่อหน้าที่เท่านั้น

แบบจำลอง OSI และ TCP/IP กับการวิเคราะห์ภัยคุกคาม

แบบจำลองเครือข่ายคอมพิวเตอร์

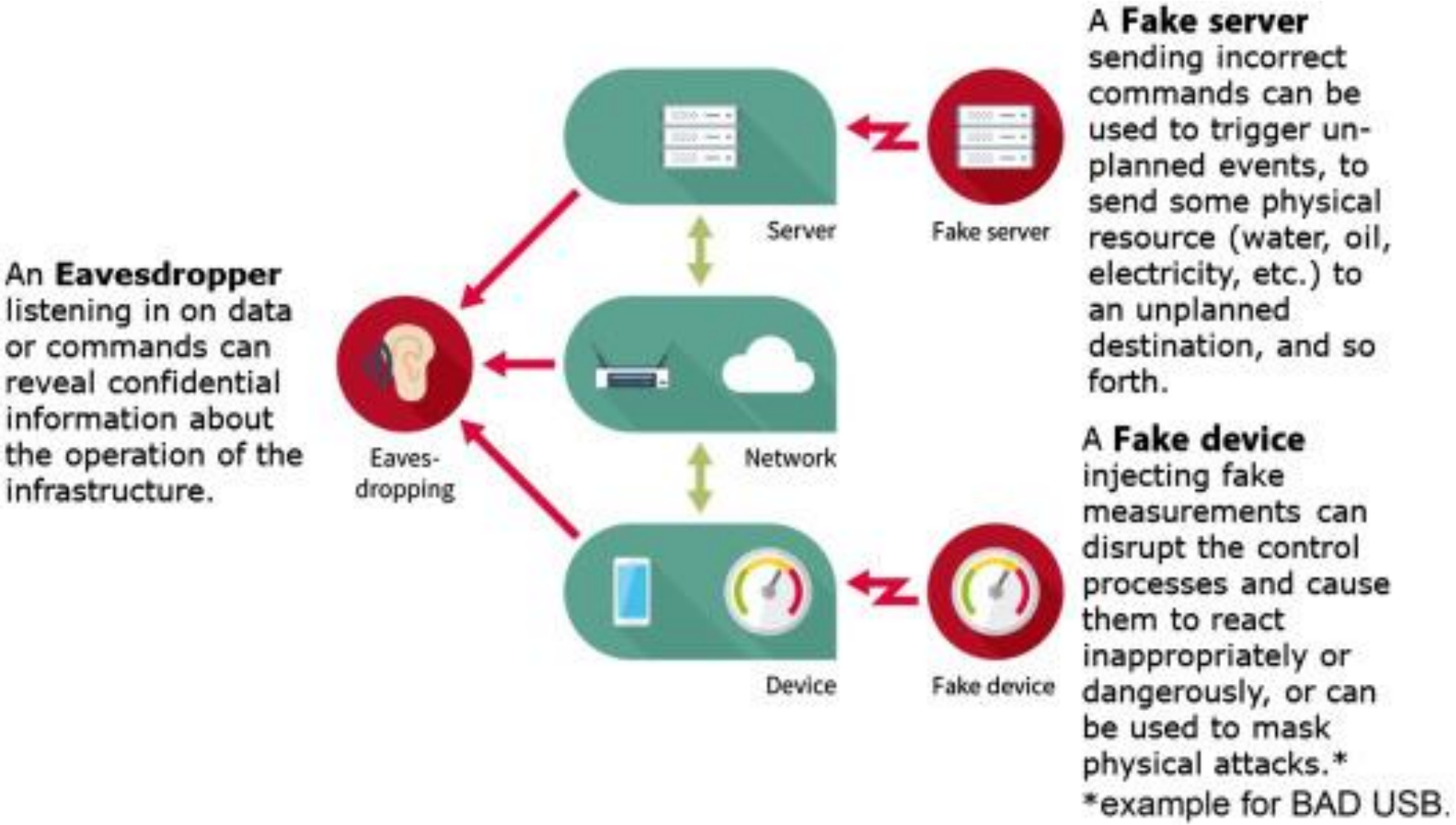
Type of attacks on layers

Layer	Attacks
Physical layer	Jamming, interceptions, eavesdropping
Data link layer	Traffic analysis, monitoring
Network layer	Wormhole, Black hole, Gray hole, message tempering, Byzantine, Flooding, resource consumption, location disclosure attacks
Transport layer	Session hijacking, SYN Flooding
Multiple layer	Denial of Service (DoS), man-in-the-middle attack

Restricting on network layer in [10] [11] [13] various network layer attack types are considered. Here some of them are discussed.

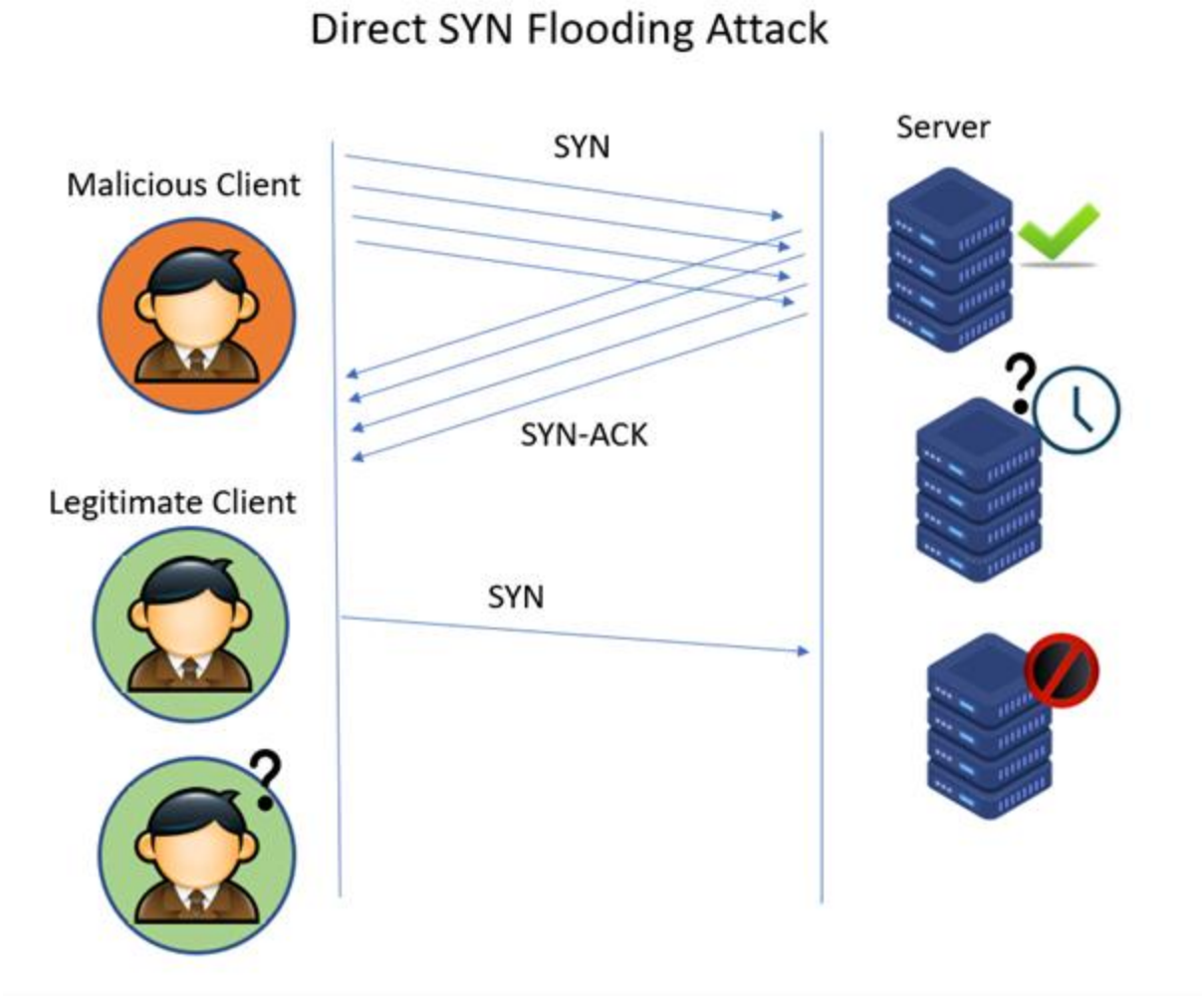
https://www.researchgate.net/profile/Anand-Motwani/publication/260631676/figure/tbl1/AS:671527884304409@1537116132950/Type-of-attacks-on-layers.png

Physical layer security



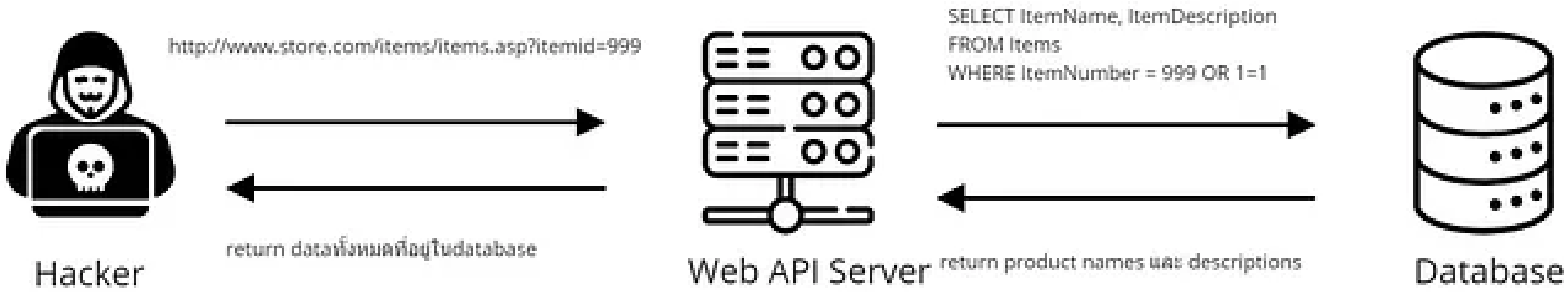
https://ars.els-cdn.com/content/image/3-s2.0-B9780128044582000032-f03-18-9780128044582.jpg

Network layer security



https://www.indusface.com/wp-content/uploads/2021/03/syn4.png

Presentation layer security



https://miro.medium.com/v2/resize:fit:720/format:webp/1*y2NskiwV5hJyze5UGTQ9lQ.jpeg

โปรโตคอลพื้นฐานและการประยุกต์ใช้ในการวิเคราะห์ปัญหาเครือข่าย

โปรโทคอล

- TCP (Transmission Control Protocol)
  - เป็นโปรโตคอลแบบคอนเน็คชั่นโอเรียนเต็ด (Connection Oriented) ที่มีการรับประกันการส่งข้อมูลถึงปลายทาง ก่อนส่งจะมีการสร้างคอนเนคชันก่อนเพื่อยอมรับข้อกำหนดในการสื่อสาร ไม่ว่าจะเป็นความเร็วหรือแบนด์วิดธ์ในการส่งข้อมูล
- IP (Internet Protocol)
  - ทำหน้าที่เลือกเส้นทางเพื่อจัดส่งข้อมูลในรูปแบบของแพ็กเก็ต โดยใช้อัลกอริทึมในการกำหนดเส้นทาง (Routing Algorithms) ที่เหมาะสมเพื่อส่งข้อมูลไปยังปลายทาง

โปรโทคอล

- UDP (User Datagram Protocol)
  - เป็นโปรโตคอลแบบคอนเน็กชั่นเลส (Connectionless) ที่ทำงานตรงข้ามกับโปรโตคอล TCP คือจะไม่มีการสร้างคอนเน็คชั่น แต่จะส่งข้อมูลทันทีที่ต้องการ โดยคาดหวังว่าข้อมูลที่ส่งไปนี้คงไปถึงปลายทางได้

- Internet Control Message Protocol (ICMP) นั้นจะทำให้ router สามารถส่ง error message หรือ control message ไปยังอุปกรณ์ router หรือ host เพื่อรานยงานสาเหตุความผิดพลาดในการส่งข้อมูล

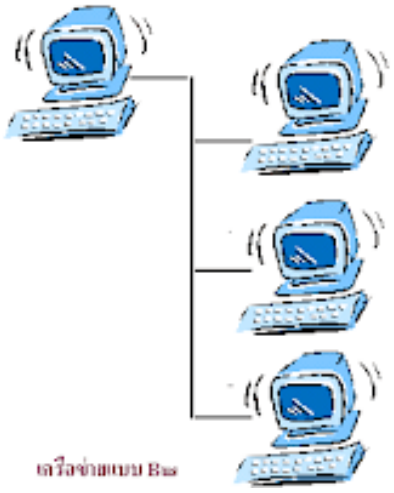
การประยุกต์ใช้ในการวิเคราะห์ปัญหาเครือข่าย

- TCP (Transmission Control Protocol): วิเคราะห์ปัญหาผ่านกระบวนการ Three-way handshake (SYN, SYN-ACK, ACK) หากการเชื่อมต่อไม่สำเร็จในขั้นตอนนี้ มักระบุถึงปัญหาที่ Firewall หรือพอร์ตบริการที่ถูกปิดอยู่.
- UDP (User Datagram Protocol): เนื่องจากไม่มีการตอบรับการรับส่งข้อมูล การวิเคราะห์ปัญหาในบริการที่ใช้ UDP (เช่น DNS หรือ VoIP) จึงมักเน้นไปที่การตรวจสอบความคับคั่งของเครือข่ายและคุณภาพของสื่อกลาง
- ICMP (Internet Control Message Protocol): ใช้สำหรับรายงานข้อผิดพลาดและทดสอบการเชื่อมต่อ เครื่องมือที่ใช้บ่อยที่สุดคือ Ping เพื่อตรวจสอบว่าโฮสต์ปลายทางยังตอบสนองอยู่หรือไม่ และ Traceroute เพื่อระบุเส้นทางและจุดที่เกิดความล่าช้าหรือการเชื่อมต่อขาดหายระหว่างโหนด.

โทโปโลยีเครือข่ายกับความทนทานและความเสี่ยงด้านความปลอดภัย

โทโพโลยีแบบบัส

ลักษณะทางกายภาพของโทโพโลยีแบบบัสนั้น จัดเป็นรูปแบบที่ง่าย ซึ่งประกอบด้วยสายเคเบิลเส้นหนึ่งที่นำมาใช้เป็นสายแกนหลักที่เปรียบเสมือนเป็นกระดูกสันหลัง (Backbone) โดยทุกๆ โหนดบนเครือข่ายจะต้องเชื่อมต่อเข้ากับสายเส้นนี้ โดยจะมี Drop Lines เชื่อมต่อระหว่างอุปกรณ์กับสายเคเบิล และ Tap เป็นคอนเน็กเตอร์ ส่วนปลายสายทั้งสองฝั่งของสายเคเบิลจะมีอุปกรณ์ปิดท้ายที่เรียกว่า Terminator เพื่อดูดซับสัญญาณและป้องกันการสะท้อนกลับของสัญญาณเมื่อวิ่งมายังสุดปลายทาง

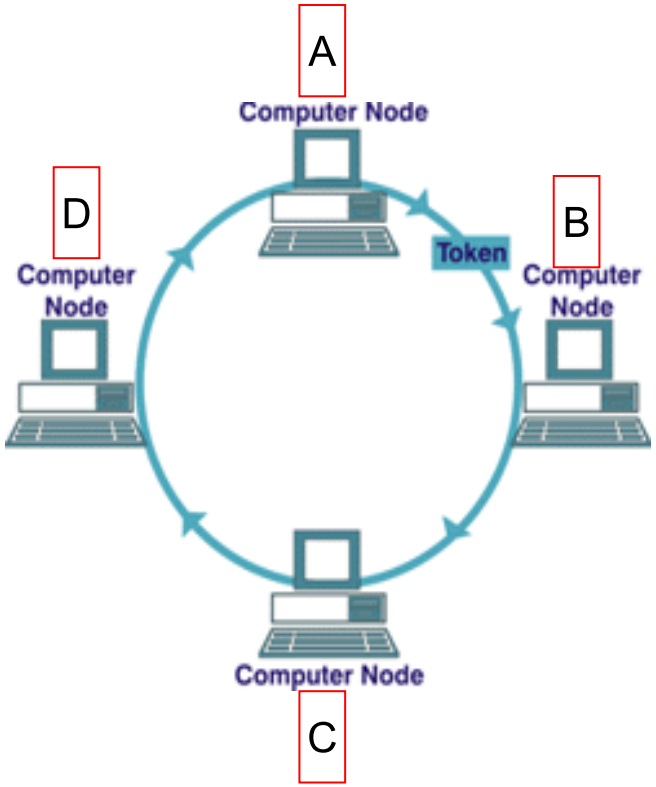


Star Topology

มีจุดเริ่มต้นจากการเชื่อมต่อเทอร์มินัลกับเมนแฟรมคอมพิวเตอร์โดยเมนแฟรมคอมพิวเตอร์ทำหน้าที่เป็นศูนย์กลาง และเทอร์มินัลทุกเครื่องจะเชื่อมต่อเข้ากับเมนเฟรมคอมพิวเตอร์ แต่ในยุคปัจจุบัน อุปกรณ์ที่นิยมนำมาใช้เป็นศูนย์กลางควบคุมของสายสื่อสารทั้งหมดก็คือ ฮับ (Hub) โดยทุก ๆ โหนดบนเครือข่ายจะต้องเชื่อมโยงสายสื่อสารผ่านฮับทั้งสิ้น ซึ่งฮับจะทำหน้าที่รับข้อมูลจากผู้ส่ง เพื่อส่งไปยังโหนดปลายทางที่ต้องการ

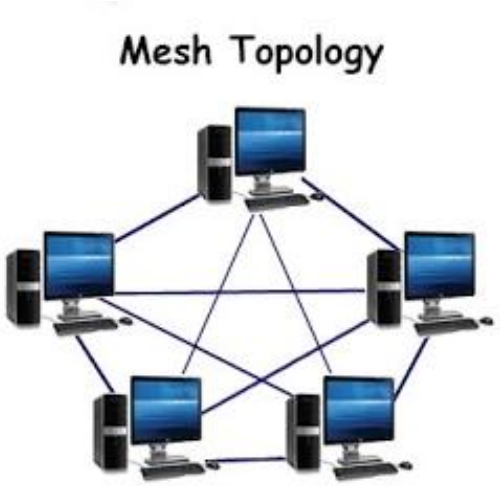
โทโพโลยีแบบวงแหวน

การเชื่อมต่อแบบวงแหวนนั้น โหนดต่างๆจะมีการเชื่อมต่อกันด้วยสายสัญญาณจากโหนดหนึ่งไปยังโหนดหนึ่งต่อกันไปเรื่อยๆ จนกระทั่งโหนดแรกและโหนดสุดท้ายได้เชื่อมโยงถึงกัน จึงเกิดเป็นรูปวงกลมหรือวงแหวนขึ้นมา



โทโพโลยีแบบเมซ

การเชื่อมต่อเครือข่ายด้วยโทโพโลยีแบบเมช จัดเป็น**การเชื่อมต่อแบบจุดต่อจุด**อย่างแท้จริง ที่แต่ละโหนดจะมีลิงก์สื่อสารระหว่างกันเป็นของตนเอง



ความทนทานและความเสี่ยงด้านความปลอดภัยของโทโปโลยีเครือข่าย

ความทนทานและความเสี่ยงด้านความปลอดภัยของโทโปโลยีเครือข่ายแต่ละรูปแบบมีข้อดีและจุดอ่อนที่แตกต่างกันตามลักษณะการเชื่อมต่อ ดังนี้ครับ:

- **แบบบัส (Bus Topology):** อุปกรณ์เชื่อมต่อเรียงกันบนสายสัญญาณเส้นเดียว มีความทนทานต่ำมาก เพราะหากสายหลักเสียหายเพียงจุดเดียว เครือข่ายจะล่มทั้งหมด ความเสี่ยงคือข้อมูลถูกส่งผ่านสื่อกลางเดียวกันทั้งหมด ทำให้ยากต่อการควบคุมการดักฟัง
- **แบบวงแหวน (Ring Topology):** เชื่อมต่อโหนดเป็นวงกลม หากโหนดใดโหนดหนึ่งหรือสายสัญญาณจุดใดเสียหาย จะส่งผลให้เครือข่ายหยุดทำงานทั้งระบบ
- **แบบดาว (Star หรือ Y Topology):** เป็นรูปแบบที่นิยมที่สุดในองค์กรปัจจุบัน เพราะมีความทนทานสูง หากคอมพิวเตอร์เครื่องใดเสีย เครื่องอื่นยังทำงานต่อได้ แต่มีความเสี่ยงสำคัญคือ จุดอ่อนรวมศูนย์ (Single Point of Failure) หากอุปกรณ์กลาง (Hub/Switch) เสียหาย เครือข่ายทั้งหมดจะใช้งานไม่ได้ทันที
- **สถาปัตยกรรมแบบลำดับชั้น (Hierarchical/Mesh):** ในเครือข่ายขนาดใหญ่จะใช้การเชื่อมต่อหลายเส้นทางเพื่อเพิ่มความทนทาน (Redundancy) แต่ความซับซ้อนของโทโปโลยีแบบนี้อาจทำให้เกิด วงวนการส่งข้อมูล (Routing Loops) หากโปรโตคอลการหาเส้นทางทำงานผิดพลาด

ภัยคุกคามทางเครือข่ายและการประยุกต์วิเคราะห์สถานการณ์

ประเภทของภัยคุกคามเครือข่าย

ภัยคุกคามถูกแบ่งออกเป็นประเภทหลักเพื่อระบุลักษณะการโจมตี:

- **การโจมตีแบบตั้งรับ (Passive Attack):** มุ่งเน้นการดักจับข้อมูลโดยไม่แก้ไขระบบ เช่น การดักฟัง (Sniffing) และการวิเคราะห์การจราจรข้อมูล (Traffic Analysis) เพื่อเรียนรู้พฤติกรรมการสื่อสาร.
- **การโจมตีแบบรุก (Active Attack):** มุ่งเปลี่ยนแปลงข้อมูลหรือขัดขวางการทำงาน เช่น การปลอมแปลงตัวตน (Masquerade), การส่งข้อมูลซ้ำ (Replay), การแก้ไขข้อความ (Modification) และการทำให้ระบบใช้งานไม่ได้ (DoS/DDoS).
- **การสำรวจ (Reconnaissance):** เป็นภารกิจรวบรวมข้อมูลเกี่ยวกับเครือข่าย เช่น การสแกนพอร์ต (Port Scanning) และการหาข้อมูลระบบปฏิบัติการ (Banner Grabbing) เพื่อเตรียมการโจมตี

การประยุกต์วิเคราะห์สถานการณ์

การวิเคราะห์สถานการณ์ช่วยให้องค์กรเข้าใจและคาดการณ์ภัยคุกคามได้ทันท่วงที:

- **กระบวนการ 3 ระดับ:** เริ่มจากการรวบรวมข้อมูลองค์ประกอบ (Element Acquisition), การหาความสัมพันธ์ของข้อมูล (Data Correlation) และการคาดการณ์สถานะในอนาคต (Situational Prediction).
- **การตรวจสอบพฤติกรรมผิดปกติ (Anomaly Detection):** ใช้การสร้าง "โปรไฟล์ฐาน" (Baseline Profile) เพื่อกำหนดขอบเขตพฤติกรรมปกติของเครือข่าย หากพบทราฟฟิกที่เบี่ยงเบนไป เช่น ปริมาณ UDP สูงผิดปกติ จะมีการแจ้งเตือนทันที.
- **การใช้แบบจำลองวิเคราะห์:**
  - Attack Tree Model: ใช้คำนวณโอกาสความสำเร็จของการโจมตีในแต่ละจุดของระบบ.
  - Linkov Model: ใช้สำหรับวางแผนเตรียมความพร้อม (Plan), รับแรงกระแทก (Absorb), กู้คืน (Recover) และปรับตัว (Adapt) ต่อสถานการณ์วิกฤต.
- **เครื่องมือรวมศูนย์:** การใช้ SIEM (Security Information and Event Management) และ SOC (Security Operations Centre) ช่วยในการรวบรวม Log จากอุปกรณ์ต่างๆ มาวิเคราะห์ความสัมพันธ์แบบ Real-time

หลักการป้องกันเครือข่ายและการกำหนดนโยบายควบคุมการเข้าถึง

หลักการป้องกันเครือข่าย

เน้นการสร้างเกราะป้องกันที่มีความซับซ้อนและครอบคลุมทุกมิติ:

- **การป้องกันแบบหลายชั้น (Defense in Depth):** หรือ "Onion Model" คือการวางมาตรการควบคุมซ้อนทับกัน เพื่อให้ผู้โจมตีต้องผ่านด่านหลายชั้นก่อนจะถึงข้อมูลสำคัญ.
- **การแบ่งโซนความปลอดภัย (Segmentation):** ใช้ VLAN เพื่อแยกกลุ่มผู้ใช้งาน และใช้ DMZ สำหรับเซิร์ฟเวอร์ที่เชื่อมต่ออินเทอร์เน็ต เพื่อจำกัดขอบเขตความเสียหายหากถูกเจาะระบบ.
- อุปกรณ์ป้องกันและตรวจสอบ:
  - Firewall: ทำหน้าที่กรองทราฟฟิกตามกฎ (Rules) ทั้งระดับ IP (Packet filtering) และระดับแอปพลิเคชัน (Proxy).
  - IDS/IPS: ตรวจจับและยับยั้งพฤติกรรมที่น่าสงสัยผ่านการวิเคราะห์ลายเซ็น (Signature) หรือความผิดปกติ (Anomaly).
- **การเชื่อมต่อที่ปลอดภัย:** ใช้ VPN เพื่อสร้างอุโมงค์ส่งข้อมูลที่มีการเข้ารหัสเมื่อมีการใช้งานจากภายนอก

การกำหนดนโยบายควบคุมการเข้าถึง

มุ่งเน้นการระบุว่าใคร (Who) สามารถทำอะไร (What) กับทรัพยากรใดได้บ้าง:

- **หลักการ IAAA:** ประกอบด้วยการระบุตัวตน (Identification), ยืนยันตัวตน (Authentication), กำหนดสิทธิ์ (Authorization) และความรับผิดชอบที่ตรวจสอบได้ (Accountability).
- **สิทธิ์ขั้นต่ำที่จำเป็น (Least Privilege):** มอบสิทธิ์ให้ผู้ใช้เพียงเท่าที่จำเป็นต้องใช้ทำงานเท่านั้น.
- **ความจำเป็นต้องรู้ (Need-to-know):** จำกัดการเข้าถึงเฉพาะข้อมูลที่จำเป็นต่อการปฏิบัติงาน ณ ขณะนั้น.
- **รูปแบบการควบคุม (Models):**
  - MAC (Mandatory): ระบบกำหนดสิทธิ์ตามระดับความลับ (เช่น Top Secret).
  - DAC (Discretionary): เจ้าของข้อมูลเป็นผู้กำหนดสิทธิ์ให้ผู้อื่นตามความเหมาะสม.
  - RBAC (Role-Based): กำหนดสิทธิ์ตามบทบาทหรือหน้าที่ในองค์กร.
- **การนำไปปฏิบัติ: ใช้ Access Control Lists (ACLs)** เป็นเครื่องมือทางเทคนิคในการอนุญาตหรือปฏิเสธทราฟฟิกบนอุปกรณ์เครือข่ายและระบบไฟล์

การเฝ้าระวังและติดตามเหตุการณ์ด้านความมั่นคงปลอดภัยเครือข่าย

การเฝ้าระวังและติดตามเหตุการณ์ด้านความมั่นคงปลอดภัย (Security Monitoring) เป็นหัวใจสำคัญของการป้องกันเชิงรุกเพื่อให้องค์กรสามารถตรวจจับและตอบสนองต่อภัยคุกคามได้ทันท่วงที

การเฝ้าระวังและติดตามเหตุการณ์ด้านความมั่นคงปลอดภัยเครือข่าย

ประเด็นสำคัญจากการจัดการความปลอดภัยในแหล่งข้อมูลมีดังนี้:

- **ศูนย์ปฏิบัติการความปลอดภัย (SOC) และ SIEM:** องค์กรสมัยใหม่ใช้ SOC เป็นศูนย์กลางในการเฝ้าระวัง โดยมีเครื่องมือหลักคือ SIEM ที่ทำหน้าที่รวบรวมและวิเคราะห์ข้อมูล Log จากอุปกรณ์ต่างๆ (เช่น Firewall, IDS, Server) มาหาความสัมพันธ์กัน (Correlation) เพื่อระบุเหตุการณ์ที่ผิดปกติ
- **การเก็บข้อมูล Log:** ต้องครอบคลุมทั้งระบบภายในองค์กร (On-premise) และระบบคลาวด์ เพื่อให้เห็นภาพรวมของความปลอดภัยทั้งหมด การเก็บ Log ไว้ในระบบภายนอกที่แยกส่วนออกไปจะช่วยป้องกันไม่ให้ผู้โจมตีแอบลบร่องรอยการกระทำผิดได้
- **กลไกการตรวจจับ:** แบ่งออกเป็น 2 รูปแบบหลัก:
  - Signature-based: ตรวจจับตามรูปแบบหรือลายเซ็นของภัยคุกคามที่รู้จักแล้ว
  - Anomaly-based: ตรวจจับพฤติกรรมที่เบี่ยงเบนไปจาก "เกณฑ์มาตรฐาน" (Baseline) ที่กำหนดไว้ ช่วยให้ตรวจพบภัยคุกคามใหม่ๆ (Zero-day) ได้

การเฝ้าระวังและติดตามเหตุการณ์ด้านความมั่นคงปลอดภัยเครือข่าย

ประเด็นสำคัญจากการจัดการความปลอดภัยในแหล่งข้อมูลมีดังนี้:

- **กระบวนการคัดกรอง (Triage):** เนื่องจากปริมาณเหตุการณ์ (Events) มีมหาศาล จึงต้องมีระบบคัดกรองเพื่อแยก "สัญญาณรบกวน" ออกจาก "ภัยคุกคามจริง" (Incidents) เพื่อให้ทีมงานโฟกัสไปที่เหตุการณ์ที่มีผลกระทบต่อธุรกิจสูงก่อน
- **การติดตามอย่างต่อเนื่อง (Continuous Monitoring):** มาตรการความปลอดภัยจะล้าสมัยไปตามกาลเวลา การตรวจสอบอย่างสม่ำเสมอจึงจำเป็นเพื่อรับมือกับเทคนิคการโจมตีที่พัฒนาขึ้นตลอดเวลา

บทสรุป

- เครือข่ายคอมพิวเตอร์เป็นรากฐานของระบบสารสนเทศและเป็นจุดศูนย์กลางของความเสี่ยงด้านความมั่นคงปลอดภัย การเข้าใจโครงสร้าง องค์ประกอบ โปรโตคอล และรูปแบบการโจมตี ช่วยให้สามารถประยุกต์ใช้ความรู้ในการออกแบบ ปรับปรุง และป้องกันเครือข่ายได้อย่างเหมาะสม
- บทนี้มุ่งเน้นให้ผู้เรียนสามารถนำความรู้พื้นฐานด้านเครือข่ายไปใช้แก้ปัญหาด้านความปลอดภัยในสถานการณ์จริง ซึ่งเป็นพื้นฐานสำคัญสำหรับการศึกษาวิชา Network Security ขั้นสูงต่อไป

it's

Q&A

TIME!

คำถามทบทวน บทที่ 4