1. หากได้รับรายงานว่ามีการโจมตีระบบเครือข่ายของ บริษัทผ่านทางอินเทอร์เน็ต จากผู้ไม่ประสงค์ดี ซึ่ง บางอย่างมีการบล็อกการเข้าถึงบางเว็บไซต์ และการส่ง อีเมล์สแปมจำนวนมาก จะวิเคราะห์และป้องกันการ โจมตีนี้อย่างไร จะต้องทำการวิเคราะห์และป้องกันการโจมตีดังนี้: 1. วิเคราะห์ชนิดของการโจมตี: จะต้องวิเคราะห์และระบุว่าการโจมตีเป็นประเภทใด เช่น การโจมตีแบบ DDoS (Distributed Denial of Service) หรือการโจมตีแบบเจาะระบบ (System Hacking) เป็นต้น เพื่อทำการป้องกันด้วยวิธีที่เหมาะสม 2. ตรวจสอบและปรับปรุงระบบความปลอดภัย: จะต้องตรวจสอบและปรับปรุงระบบความปลอดภัยของเครือข่ายอย่างสม่ำเสมอ เช่น การอัปเดต ซอฟต์แวร์หรือฮาร์ดแวร์เพื่อเติมเต็มช่องโหว่ (Vulnerability) ที่อาจเป็นประเด็นในการโจมตี 3. การควบคุมการเข้าถึง: จะต้องทำการตั้งค่าการเข้าถึงของผู้ใช้งานและระบบ เพื่อป้องกันการเข้าถึงแหล่งข้อมูลที่มากับอุปกรณ์ที่ใช้เชื่อมต่อกับ เครือข่าย เช่น อุปกรณ์ IoT (Internet of Things) ที่มีความปลอดภัยน้อย อาจเป็นทางเข้าให้กับผไมประสงคด 4. การตดตงระบบ IDS/IPS: ควรตดตงระบบ IDS (Intrusion Detection System) และ IPS (Intrusion Prevention System) เพอตรวจสอบ และปองกนการเขาถงไมมอำนาจ หรอการโจมตบนเครอขาย 5. การเขยนนโยบายความปลอดภย: ควรเขยนนโยบายความปลอดภยเพอเตรยมตวและปองกนการโจมตในอนาคต โดยควรรวบรวมแนวทางการ ปองกนและวธการเฝาระวง รวมถงการดำเนนการในกรณเกดการโจมต 6. การสอนพนกงาน: ควรสอนพนกงานทกระดบในองคกรเกยวกบความสำคญของความปลอดภยเครอขาย รวมถงการใชรหสผานทแขงแกรงและ การเปดเผยขอมลทเปนความลบอยางระมดระวง

2.
[illegible] — 06/05/2023 10:13
นอกจากการทำ Incident Response Plan แล้ว สามารถทำอะไรเพิ่มเติมเพื่อป้องกันเหตุฉุกเฉินได้บ้าง นอกจากการทำ Incident Response Plan แล้ว ยังมีกลไกต่างๆที่องค์กรสามารถใช้เพื่อป้องกันเหตุการณ์ร้ายแรง ได้แก่ 1. การอัพเดทระบบ: อัพเดทระบบขององค์กรเป็นปัจจัยสำคัญในการป้องกันการโจมตี โดยทำการอัพเดทระบบประจำเวลาจะช่วยลดโอกาสของ การโจมตีที่ใช้ช่องโหว่ในระบบ ซึ่งทางผู้ดูแลระบบควรให้ความสำคัญกับการอัพเดทระบบและแก้ไขช่องโหว่ในระบบอย่างรวดเร็ว 2. การตรวจสอบและตรวจจับ: องค์กรควรติดตั้งโปรแกรมที่ช่วยตรวจสอบและตรวจจับการแทรกแซง (intrusion detection/prevention system) เพื่อช่วยตรวจจับและป้องกันการโจมตีได้ทันที รวมถึงการใช้โปรแกรมป้องกันไวรัสและโปรแกรมป้องกันการเข้าถึงไม่หมายความจริง (anti-malware/anti-spyware) ซึ่งช่วยป้องกันไม่ให้โปรแกรมอันตรายเข้ามาในระบบ 3. การเข้ารหัสข้อมูล: การเข้ารหัสข้อมูล (encryption) เป็นวิธีการป้องกันข้อมูลที่สำคัญและเป็นความลับไม่ให้ถูกดักรับข้อมูล ทางองค์กรควรใช้ การเข้ารหัสข้อมูลเป็นประจำเมื่อส่งข้อมูลข้ามเครือข่ายหรือออกสู่สาธารณะ 4. การทำการสำรองข้อมูล (backup): การทำการสำรองข้อมลเปนวธการทชวยลดความเสยงในกรณทขอมลสญหาย (มีการแก้ไข)

3. [10:16]
นอกจากมาตรฐาน ISO 27001 มีมาตรฐานอะไรที่ สามารถสร้างความน่าเชื่อถือให้กับองค์กรได้บ้าง นอกเหนือจากมาตรฐาน ISO 27001 มีมาตรฐานอื่นๆ ที่สามารถสร้างความเชื่อถือได้ เช่น 1. NIST Cybersecurity Framework: เป็นแนวทางในการสร้างและดำเนินการด้านความมั่นคงปลอดภัยสำหรับองค์กร โดยมุ่งเน้นการป้องกันการ โจมตีและการตอบสนองต่อการโจมตีโดยใช้วิธีการเรียงลำดับ จัดกลุ่มและอธิบายแนวทางปฏิบัติที่ดีที่สุด 2. PCI DSS: เป็นมาตรฐานสำหรับการป้องกันการขโมยข้อมูลการเงินในระบบการช าระเงิน มีจุดประสงค์เพื่อป้องกันการขโมยข้อมูลบัตรเครดิต ป้องกันการสอบสวนและลดความเสี่ยงในการสูญเสียรายได้ 3. CIS Controls: เป็นแนวทางควบคุมการทำความมั่นคงปลอดภัยที่สามารถป้องกันการโจมตีได้มากที่สุด โดยประกอบด้วย 20 ขั้นตอนในการ ปรับปรุงการดำเนินงานของระบบคอมพิวเตอร์เพื่อเพิ่มความมั่นคงปลอดภัย การใช้มาตรฐานต่างๆ จะช่วยให้องค์กรเข้าใจถึงความเสี่ยงและอุปสรรคที่อาจเกิดขึ้นในการดำเนินงานและช่วยเพิ่มความมั่นคงปลอดภัยของระบบและ ข้อมูลในองค์กร

infrastructure mode

Client / server หรือ Infrastructure mode เป็นลักษณะการรับส่งข้อมูลโดยอาศัยAccess Point (AP) หรือเรียกว่า “Hot spot” ทำหน้าที่เป็นสะพานเชื่อมต่อระหว่างระบบเครือข่ายแบบใช้สายกับเครื่องคอมพิวเตอร์ลูกข่าย (client) โดยจะกระจายสัญญาณคลื่นวิทยุเพื่อ รับ-ส่งข้อมูลเป็นรัศมีโดยรอบ เครื่องคอมพิวเตอร์ที่อยู่ในรัศมีของ AP จะกลายเป็น เครือข่ายกลุ่มเดียวกันทันที โดยเครื่องคอมพิวเตอร์ จะสามารถติดต่อกัน หรือติดต่อกับ Serverเพื่อแลกเปลี่ยนและค้นหาข้อมูลได้ โดยต้องติดต่อผ่านAP เท่านั้น ซึ่ง AP 1 จุด สามารถให้บริการเครื่องลูกข่ายได้ถึง 15-50อุปกรณ์ ของเครื่องลูกข่าย เหมาะสำหรับการนำไปขยายเครือข่ายหรือใช้ร่วมกับระบบเครือข่าย
แบบใช้สายเดิมในออฟฟิต,ห้องสมุด หรือในห้องประชุม เพื่อเพิ่มประสิทธิภาพในการทำงานให้มากขึ้น

ad hoc mode

Peer to Peer (ad-hoc mode)
เป็นรูปแบบการเชื่อมต่อแลนไร้สายที่มีลักษณะการเชื่อมต่อแบบโครงข่ายโดยตรงระหว่างเครื่องคอมพิวเตอร์จำนวน 2 เครื่องหรือมากกว่านั้น โดยเครื่องคอมพิวเตอร์แต่ละเครื่องจะมีความเท่าเทียมกัน การเชื่อมต่อด้วยวิธีนี้จะเหมาะกับเครือข่ายขนาดเล็กที่มีโหนดเชื่อมต่อจำนวนไม่มาก

SSID ย่อมาจาก (Service Set Identifier) ซึ่งเป็นชื่อของ WIFI ถ้ายังมองภาพไม่ออก ก็ให้หยิบมือถือขึ้นมา แล้วเปิดให้ WIFI ทำงาน เราจะเห็นว่ารอบ ๆ ตัวเรานั้นมีชื่อ WIFI อะไรบ้างที่ปรากฏขึ้นมา ชื่อตรงนั้นคือสิ่งที่เรียกว่า SSID นั่นเอง ชื่อเหล่านี้เราสามารถตั้งได้ตามความต้องการ หากที่บ้านของเอาติดตั้งอินเตอร์เน็ต และมีอุปกรณ์กระจายสัญญาณ WIFI ซึ่งการจัดตั้งชื่อ SSID ได้นั้น จะต้องเข้าสู่ระบบของ Router ผ่านทางโปรแกรม Web browser โดยเมื่อเปิดโปรแกรม Web Browser ขึ้นมาแล้วค่าเริ่มต้นของหมายเลข IP Address ที่จะใช้สำหรับเข้าสู่การตั้งค่า SSID ก็คือ 192.168.1.1 หลังจากนั้นจะมีหน้าต่างสำหรับใส่ Username และ Password ขึ้นมา และค่าเริ่มต้นของ Username และ Password นั้นสามารถดูได้จากคู่มือ หรือใต้เครื่อง Router หรือ Access Point
เมื่อเข้าสู่ระบบได้แล้ว ให้มองหาเมนู Network > WLAN Radio 2.4G > SSID Setting และเข้าไปตั้งชื่อที่ต้องการเป็นภาษาอังกฤษในช่อง SSID Name สำหรับการตั้งชื่อนั้น แนะนำให้ใช้ชื่อง่าย ๆ ที่เป็นเอกลักษณ์ที่บ่งบอกความเป็นตัวของเรา การทำการตั้งชื่อควรตรวจเช็คให้ดีว่าชื่อ SSID หรือชื่อ WIFI ที่อยู่ใกล้เคียงนั้นมีชื่อที่เราต้องการแล้วหรือยัง เพราะไม่ควรตั้งชื่อ WIFI หรือ SSID ซ้ำกัน เพราะจะทำให้มีปัญหาในการเชื่อมต่อได้

SSID Broadcast คืออะไร?

นี่คือฟังก์ชั่นที่ดำเนินการโดยจุดเชื่อมต่อที่ส่งชื่อของมันซึ่งสถานีไร้สายที่ค้นหาการเชื่อมต่อเครือข่ายสามารถค้นพบ 'มันได้ นี่คือสิ่งที่ช่วยให้โปรแกรมตัวจัดการไคลเอ็นต์ของอแด็ปเตอร์ไร้สายของคุณหรือซอฟต์แวร์ไร้สายในตัวของ Windows XP สามารถแสดงรายการจุดเข้าใช้งานในระยะ

ความสามารถในการปิดใช้งานการออกอากาศ SSID โดยพื้นฐานแล้วจะทำให้ Access Point ของคุณมองไม่เห็นเว้นแต่ว่าไคลเอนต์ไร้สายจะรู้จัก SSID อยู่แล้วหรือกำลังใช้เครื่องมือที่มอนิเตอร์หรือ 'sniff' ทราฟฟิกจากไคลเอนต์ที่เกี่ยวข้องของ AP

WEP, WPA, WPA2 และ WPA3 มาตรฐานความปลอดภัย Wi-Fi คืออะไร ? แตกต่างกันอย่างไร ? (thaiware.com)

Open System Authentication is a type of authentication method used in wireless networks. It is the simplest form of authentication and provides no real security measures. In Open System Authentication, any device can connect to the wireless network without the need for authentication credentials, such as a password or encryption key.

Here's how Open System Authentication works:

1. Device Discovery: The wireless network broadcasts its Service Set Identifier (SSID) to inform nearby devices of its presence.
2. Association Request: A device that wants to connect to the wireless network sends an association request to the access point (AP) or wireless router.
3. Access Point Response: The access point, in an open system network, accepts the association request without requiring any authentication. It sends an association response to the device, allowing it to join the network.
4. Network Access: After receiving the association response, the device is granted access to the wireless network and can communicate with other devices within the network range.

Open System Authentication is considered "open" because it does not authenticate or encrypt any data exchanged between the wireless devices and the network. This means that any device within range of the network can connect to it and potentially eavesdrop on or intercept network traffic.

As a result, Open System Authentication is not recommended for securing sensitive information or protecting against unauthorized access. It is often used in public Wi-Fi networks or scenarios where convenience and ease of connectivity take precedence over security.

To enhance the security of wireless networks, it is advisable to use stronger authentication methods such as WPA2 (Wi-Fi Protected Access 2) or WPA3, which employ encryption and more robust authentication mechanisms to ensure secure communication between devices and the network.

Key authentication, also known as public key authentication, is a method of securely verifying the identity of a user or entity in computer systems. It is commonly used in secure communication protocols such as SSH (Secure Shell) to authenticate remote access.

In key authentication, a user has a pair of cryptographic keys: a public key and a private key. The public key is shared with other parties or stored on servers, while the private key is kept confidential and securely stored on the user's device.

Here's how key authentication works:

1. Key Generation: The user generates a key pair consisting of a public key and a corresponding private key. The private key remains on the user's device, while the public key is shared with the remote server or the intended party.
2. Public Key Distribution: The user's public key is distributed to the servers or parties that need to authenticate the user's identity. This can be done by manually sharing the public key or through a key distribution infrastructure.
3. Requesting Authentication: When the user wants to access a remote system (e.g., SSH into a server), the remote system requests the user to authenticate.
4. Client Authentication: The client (user) sends a message to the server, typically including the user's identification and a cryptographic challenge.
5. Signing the Challenge: The client signs the challenge using its private key, creating a digital signature.
6. Verification: The server retrieves the client's public key and uses it to verify the digital signature. If the signature is valid, the server can be confident that the client possesses the corresponding private key and is therefore the legitimate user.
7. Access Granted: If the verification is successful, the server grants access to the client, allowing the user to log in or perform the requested actions.

Key authentication provides a higher level of security compared to traditional password-based authentication. As the private key is never shared or transmitted, it is less susceptible to interception or brute-force attacks. Additionally, even if the public key is compromised, it does not jeopardize the security of the private key.

It's important to note that key authentication requires careful management and protection of the private key to prevent unauthorized access. Users should ensure their private keys are stored securely and take precautions to prevent unauthorized access to their devices or key storage locations

no clean
***
Broken Access Control เป็นช่องโหว่ด้านความปลอดภัยที่เกิดขึ้นเมื่อแอปพลิเคชันหรือระบบไม่จำกัดการเข้าถึงทรัพยากรหรือฟังก์ชันของตนอย่างถูกต้อง
ช่องโหว่นี้ทำให้ผู้ใช้ที่ไม่ได้รับอนุญาตสามารถดำเนินการหรือเข้าถึงข้อมูลที่ไม่ควรได้เข้าถึงได้

มีหลายวิธีที่ Broken Access Control สามารถเกิดขึ้นในแอปพลิเคชันหรือระบบได้ ตัวอย่างขั้นต้นเช่น
*****
ขาดการตรวจสอบสิทธิ์การเข้าใช้: แอปพลิเคชันหรือระบบไม่ต้องการผู้ใช้ยืนยันตัวตนก่อนที่จะอนุญาตให้เข้าถึงทรัพยากรหรือฟังก์ชัน
ตัวอย่างเช่น พิจารณาแอปพลิเคชันเว็บที่อนุญาตผู้ใช้ดูข้อมูลบัญชีของตนเอง เช่น ประวัติการซื้อและข้อมูลการเรียกเก็บเงิน แต่แอปพลิเคชันไม่ต้องการผู้ใช้เข้าสู่ระบบหรือให้ข้อมูลประจำตัวใดๆก่อนที่จะให้เข้าถึงข้อมูลดังกล่าว
ผู้โจมตีสามารถใช้ช่องโหว่นี้โดยการเข้าถึง URL ของหน้าข้อมูลบัญชีโดยตรงหรือโดยการแก้ไขฟิลด์อินพุตเพื่อเข้าถึงข้อมูลบัญชีผู้ใช้อื่น ๆ ซึ่งสามารถทำให้ผู้โจมตีเข้าถึงข้อมูลที่สำคัญหรือดำเนินการที่ไม่ได้รับอนุญาตได้
เช่น เปลี่ยนการตั้งค่าบัญชีหรือทำการซื้อสินค้า
****
การตรวจสอบสิทธิ์ไม่เพียงพอ: แอปพลิเคชันหรือระบบตรวจสอบสิทธิ์การเข้าถึงของผู้ใช้ แต่ไม่มีความแข็งแกร่งพอหรือไม่ครอบคลุมทุกสถานการณ์
ตัวอย่างเช่น พิจารณาโปรแกรมเว็บที่อนุญาตให้ผู้ใช้อัพเดทข้อมูลโปรไฟล์ของตนเอง เช่นที่อีเมลและรหัสผ่าน โปรแกรมตรวจสอบว่าผู้ใช้มีสิทธิ์การเข้าถึงและการอัพเดทโปรไฟล์ แต่โปรแกรมเช็คเพียงว่าผู้ใช้มีสิทธิ์เข้าถึงและอัพเดทโปรไฟล์ของตนเองเท่านั้น
แต่ไม่ตรวจสอบว่าผู้ใช้มีสิทธิ์เข้าถึงและอัพเดทโปรไฟล์ของผู้ใช้อื่น
ผู้โจมตีสามารถใช้ช่องโหว่นี้โดยการแก้ไข URL หรือข้อมูล input เพื่อเข้าถึงหน้าอัพเดทโปรไฟล์ของผู้ใช้อื่น และเปลี่ยนอีเมลและรหัสผ่านได้ ซึ่งจะทำให้ผู้โจมตีสามารถเข้าถึงข้อมูลที่ละเอียดอ่อนหรือดำเนินการโดยไม่ได้รับอนุญาต
*****
การอ้างอิงออบเจกต์โดยตรง: แอปพลิเคชันหรือระบบใช้ข้อมูลที่ผู้ใช้ส่งเข้ามาเพื่อเข้าถึงทรัพยากรโดยตรงโดยไม่มีการตรวจสอบหรืออนุญาตให้เข้าถึง
กิดขึ้นเมื่อแอปพลิเคชันเปิดเผยอ้างอิงถึงอ็อบเจกต์ภายในของการปฏิบัติงาน เช่น ไฟล์ บันทึกฐานข้อมูล หรือทรัพยากร ในรูปแบบพารามิเตอร์หรือคีย์ใน URL หรือฟอร์มฟิลด์ ผู้โจมตีสามารถจัดการอ้างอิงเหล่านี้เพื่อเข้าถึงทรัพยากรที่ไม่ได้รับอนุญาตหรือดำเนินการที่ไม่ได้รับอนุญาต
ตัวอย่างเช่น พิจารณาแอปพลิเคชันเว็บที่อนุญาตให้ผู้ใช้ดูประวัติการซื้อของตนเองโดยให้หมายเลข ID การซื้อใน URL เช่น
https://example.com/purchases?id=123
หากแอปพลิเคชันไม่ตรวจสอบว่าผู้ใช้มีสิทธิ์เข้าถึงการซื้อด้วยหมายเลข ID 123
อย่างเหมาะสม ผู้โจมตีสามารถเปลี่ยนหมายเลข ID ใน URL เพื่อเข้าถึงประวัติการซื้อของผู้ใช้อื่นๆ รวมถึงข้อมูลที่สำคัญเช่นที่อยู่สำหรับวางบิลและการส่งสินค้า
****
อ้างอิงออบเจกต์โดยไม่ปลอดภัย: แอปพลิเคชันหรือระบบเปิดเผยการอ้างอิงออบเจกต์ภายในที่สามารถถูกแฮ็กโดยผู้โจมตีเพื่อเข้าถึงทรัพยากรโดยไม่ได้รับอนุญาต
เกิดขึ้นเมื่อแอปพลิเคชันเปิดเผยการอ้างอิงของวัตถุภายในที่อาจถูกโจมตีโดยผู้โจมตีที่ทำให้พวกเขาสามารถเข้าถึงทรัพยากรหรือกระทำการไม่ได้รับอนุญาต
ตัวอย่างเช่น พิจารณาแอปพลิเคชันเว็บที่อนุญาตให้ผู้ใช้ดูไฟล์ของตนเองโดยให้รหัสไอดีของไฟล์ใน URL เช่น
https://example.com/files?id=123
ถ้าแอปพลิเคชันไม่ตรวจสอบให้แน่ใจว่าผู้ใช้มีสิทธิ์เข้าถึงไฟล์ด้วยรหัสไอดีหมายเลข 123 ผู้โจมตีสามารถเปลี่ยนรหัสไอดีใน URL เพื่อเข้าถึงไฟล์ของผู้ใช้อื่นได้
ต่อไปนี้สมมติว่าแอปพลิเคชันใช้หมายเลข ID ลำดับต่อเนื่องเป็น ID ของไฟล์ เช่น 1, 2, 3 และเป็นต้น ผู้โจมตีสามารถเดาหมายเลข ID เพื่อเข้าถึงไฟล์ของผู้ใช้อื่นได้ โดยไม่ต้องมีความรู้
เกี่ยวกับการดำเนินงานภายในของแอปพลิเคชัน นี่เป็นตัวอย่างของการอ้างอิงวัตถุโดยไม่ปลอดภัย
****

Privilege escalation เป็นกระบวนการที่แอปพลิเคชันหรือระบบอนุญาตให้ผู้ใช้เพิ่มสิทธิ์ของตนเหนือระดับที่ได้รับอนุญาต ซึ่งสามารถทำให้ผู้ใช้เข้าถึงทรัพยากรที่ไม่ควรได้เข้าถึง
การเพิ่มสิทธิ์เกิดขึ้นเมื่อแอปพลิเคชันหรือระบบอนุญาตผู้ใช้เข้าถึงทรัพยากรหรือดำเนินการเกินระดับการเข้าถึงที่ได้รับอนุญาต สาเหตุของปัญหานี้สามารถเกิดขึ้นได้หลายวิธี เช่น
การประกอบด้วยช่องโหว่ในแอปพลิเคชันหรือระบบ: ผู้โจมตีสามารถใช้ช่องโหว่เช่น buffer overflows หรือ SQL injection เพื่อเข้าถึงการดูแลระบบหรือสิทธิ์พิเศษบนระบบ

การใช้ข้อมูลการเข้าถึงที่ถูกตั้งค่าตามค่าเริ่มต้นหรือค่าผิด: หากแอปพลิเคชันหรือระบบใช้ข้อมูลการเข้าถึงที่ถูกตั้งค่าตามค่าเริ่มต้นหรือค่าผิด ผู้โจมตีสามารถใช้วิธีการแบบบังคับการทำงานหรือ
ยังไม่ได้เข้ารหัสข้อมูลเพื่อเข้าถึงบัญชีผู้ดูแลระบบได้
การตั้งค่าผิดพลาด: การตั้งค่าผิดพลาดในแอปพลิเคชันหรือระบบสามารถทำให้ผู้โจมตีเข้าถึงสิทธิ์การดูแลระบบโดยการใช้การตั้งค่าที่ไม่แข็งแกร่งหรือไม่เหมาะสม
ตัวอย่างของการเพิ่มสิทธิ์คือเมื่อผู้ใช้ที่มีสิทธิ์จำกัดในแอปพลิเคชันเว็บสามารถแก้ไข URL หรือช่องข้อมูลเพื่อเข้าถึงฟังก์ชันการดูแลระบบได้ ตัวอย่างเช่น ในกรณีที่แอปพลิเ
ตัวอย่างของ Privilege escalation คือเมื่อผู้ใช้งานที่มีสิทธิ์จำกัดในแอปพลิเคชันเว็บสามารถแก้ไข URL หรือช่องกรอกข้อมูลเพื่อเข้าถึงฟังก์ชันการดูแลระบบได้
ตัวอย่างเช่นเว็บแอปพลิเคชันที่อนุญาตให้ผู้ใช้งานปกติเปลี่ยนแปลงข้อมูลโปรไฟล์ของตนเอง เช่นที่อยู่อีเมลของตนเอง หากแอปพลิเคชันไม่ตรวจสอบข้อมูลผู้ใช้งานอย่างเหมาะสมและ
ผู้โจมตีสามารถฝังโค้ดอันตรายในช่องกรอกข้อมูลอีเมล จะสามารถเข้าถึงฟังก์ชันการดูแลระบบและเข้าถึงข้อมูลที่เป็นความลับได้

(Cryptographic failures) เป็นเหตุการณ์ที่เกิดขึ้นเมื่อโปรโตคอลการเข้ารหัส อัลกอริทึม หรือระบบการเข้ารหัสไม่สามารถให้ความมั่นคงปลอดภัยและความลับตามที่ต้องการได้
การเข้ารหัสเป็นส่วนสำคัญของการคอมพิวเตอร์รุ่นใหม่ เนื่องจากใช้ในการรักษาความปลอดภัยของข้อมูลที่ละเอียดอ่อน เช่น การทำธุรกรรมทางการเงิน ข้อมูลส่วนบุคคล และการสื่อสารทางทหาร อย่างไรก็ตาม ความล้มเหลวในด้านการเข้ารหัสสามารถทำให้เกิดการละเมิดความปลอดภัยของข้อมูล การเข้าถึงที่ไม่ได้รับอนุญาต และปัญหาความปลอดภัยอื่นๆ
สาเหตุของCryptographic failuresเหล่านี้อาจเกิดขึ้นได้จากหลายปัจจัย เช่น การจัดการคีย์ที่ไม่ดี หรือช่องโหว่ในซอฟต์แวร์หรือฮาร์ดแวร์ที่ใช้เพื่อดำเนินการเข้ารหัส

บางตัวอย่างของความล้มเหลวของการเข้ารหัสได้แก่:

Weak or predictable keys:ระบบการเข้ารหัสต้องการคีย์เพื่อทำการเข้ารหัสและถอดรหัสข้อมูล หากคีย์เหล่านี้อ่อนหรือสามารถทำนายได้ ผู้โจมตีอาจสามารถถอดรหัสข้อมูลได้ง่ายดาย
โดยการเข้ารหัสข้อมูล(cryptography) ความมั่นคงของข้อมูลที่ถูกเข้ารหัสขึ้นอยู่กับความแข็งแกร่งและความสุ่มของkeyในการเข้ารหัส(encryption key) ที่ใช้งานอยู่ keyการเข้ารหัสที่มีความอ่อนแอหรือเป็นแบบสามารถทายได้ง่ายๆ จะทำให้ผู้บุกรุกสามารถถอดรหัสข้อมูลได้อย่างง่ายดาย

Brute-force attacks: การโจมตีด้วยวิธีการBrute-force attacksเป็นการลองใช้คีย์ทุกกรณีจนกว่าจะพบคีย์ที่ถูกต้อง ระบบการเข้ารหัสที่มีคีย์อ่อนอาจเสี่ยงต่อการโจมตีชนิดนี้

การโจมตีแบบ Man-in-the-middle: การโจมตีแบบ Man-in-the-middle เป็นการแอบฟังการสื่อสารระหว่างสองฝ่ายและแก้ไขข้อมูลในกรณีที่
ระบบการเข้ารหัสไม่ได้ออกแบบให้สามารถตรวจจับหรือป้องกันการโจมตีชนิดนี้ ผู้โจมตีสามารถอ่านหรือแก้ไขข้อมูลที่ถูกเข้ารหัสได้

ตัวอย่างเช่นหากใช้วิธีการเข้ารหัสที่อ่อนแอหรือบกพร่องเพื่อป้องกันข้อมูลการเข้าสู่ระบบของผู้ใช้ ผู้โจมตีอาจสามารถถอดรหัสข้อมูลการเข้าสู่ระบบได้ง่าย ๆ และเข้าถึงระบบธนาคารออนไลน์ได้โดยไม่ได้รับอนุญาต
อย่างเช่นเดียวกันหากจัดการและเก็บรักษากุญแจการเข้ารหัสไม่ได้ดีอาจทำให้โจมตีเข้าถึงและถอดรหัสข้อมูลที่สำคัญ
อีกตัวอย่างของความล้มเหลวของการใช้การเข้ารหัสในเว็บแอปพลิเคชันคือการใช้โปรโตคอลการเข้ารหัสที่ไม่ปลอดภัย ตัวอย่างเช่นหากโปรโตคอล SSL/TLS ที่ใช้รักษาความปลอดภัยของการสื่อสารระหว่างเว็บแอปพลิเคชันและเบราว์เซอร์ของผู้ใช้ไม่ได้กำหนดค่าไว้อย่างถูกต้อง อาจเป็นแหล่งที่มีช่องโหว่เพื่อให้ผู้โจมตีสามารถดักจับและอ่านข้อมูลที่ละเอียดอ่อน
ที่ถูกส่งผ่านระหว่างเบราว์เซอร์ของผู้ใช้และเว็บแอปพลิเคชัน
```

no clean
```

A03:2021-Injection

เป็นหมวดหมู่ของความเสี่ยงด้านความปลอดภัยที่อ้างอิงถึงช่องโหว่ที่อนุญาตให้ผู้โจมตีฝังรหัสที่เป็นอันตรายหรือข้อมูลลงในแอปพลิเคชัน การโจมตีแบบฝังรหัสเป็นช่องโหว่ที่พบได้บ่อยและสามารถใช้ประโยชน์ได้ในหลายวิธี เช่น SQL injection, NoSQL injection, command injection, และอื่น ๆ

การโจมตีแบบฝังรหัสเกิดขึ้นเมื่อผู้โจมตีสามารถป้อนข้อมูลที่เป็นอันตรายเข้าสู่ช่องอินพุตหรือพารามิเตอร์ของแอปพลิเคชันได้ สาเหตุทำให้แอปพลิเคชันดำเนินการคำสั่งที่ไม่ได้ตั้งใจหรืออนุญาตการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

Insecure design หมายถึงการออกแบบซอฟต์แวร์ ฮาร์ดแวร์ หรือระบบที่มีช่องโหว่ทางความปลอดภัย ความไม่ปลอดภัยนี้เกิดจากขาดการให้ความสำคัญกับปัญหาความปลอดภัย ในระหว่างขั้นตอนการออกแบบ หรือการละเว้นการปฏิบัติตามหลักการเขียนโปรแกรมที่ปลอดภัย การออกแบบที่ไม่ปลอดภัยสามารถนำไปสู่ปัญหาความปลอดภัยต่าง ๆ เช่นการเข้าถึงที่ไม่ได้รับอนุญาต การแฝงตัวเข้าสู่ระบบ เป็นต้น ตัวอย่างหนึ่งของการออกแบบที่ไม่ปลอดภัยคือการใช้รหัสผ่านเริ่มต้นหรือรหัสผ่านที่ไม่แข็งแรงในอุปกรณ์หรือระบบต่าง ๆ นี้ทำให้ผู้โจมตีสามารถเข้าถึงระบบและขโมยหรือแก้ไขข้อมูลที่ละเอียดอ่อนได้อย่างง่ายดาย อีกตัวอย่างคือขาดการตรวจสอบข้อมูลที่นำเข้า ซึ่งอาจนำไปสู่การโจมตีด้วยการแทรกโค้ดหรือช่องโหว่ในการจัดเก็บข้อมูล ตัวอย่างเช่น ของการออกแบบที่ไม่ปลอดภัยในเว็บแอปพลิเคชันคือการใช้โปรโตคอลการสื่อสารที่ไม่ปลอดภัย เช่น HTTP แทน HTTPS ซึ่งอาจทำให้ผู้โจมตีสามารถแอบแฝงและแก้ไขข้อมูลที่กำลังถูกส่งระหว่างผู้ใช้และเซิร์ฟเวอร์ได้ ทำให้เกิดการลักลอบเข้าถึงข้อมูลหรือปัญหาด้านความปลอดภัยอื่นๆ

(security misconfiguration) เป็นการเกิดช่องโหว่ที่เกิดขึ้นเมื่อระบบหรือแอปพลิเคชันถูกกำหนดค่าหรือตั้งค่าไม่ถูกต้อง โดยทำให้เปิดเผยต่อความเสี่ยงในด้านความมั่นคงปลอดภัยได้ ตัวอย่างเช่น Weak authentication and authorization settings - นี่สามารถรวมถึงการใช้รหัสผ่านเริ่มต้นหรือรหัสผ่านที่อ่อนแอที่สามารถทายได้ง่าย การไม่ใช้การตรวจสอบสำหรับหลายปัจจัยหรือการอนุญาตให้เข้าถึงข้อมูลที่เป็นความลับโดยไม่มีการอนุญาตเหมาะสม Improperly configured error messages - ข้อความผิดปกติที่ให้ข้อมูลมากเกินไปหรือเปิดเผยรายละเอียดของระบบสามารถถูกใช้โดยผู้โจมตีเพื่อเข้าถึงระบบโดยไม่ได้รับอนุญาต Misconfigured file permissions - สิทธิ์ไฟล์ที่ไม่ถูกต้องสามารถอนุญาตให้เข้าถึงไฟล์หรือข้อมูลที่เป็นความลับได้โดยไม่ได้รับอนุญาต Insecure default configurations - แอปพลิเคชันเว็บหลายๆ ตัวมาพร้อมกับการตั้งค่าเริ่มต้นที่ออกแบบมาสำหรับความสะดวกในการใช้งานมากกว่าความปลอดภัย การไม่เปลี่ยนการตั้งค่าเรมตน

`Vulnerable and outdated components หมายถึงส่วนประกอบซอฟต์แวร์ที่มีช่องโหว่ด้านความปลอดภัยที่รู้จักหรือไม่ได้รับการสนับสนุนจากผู้พัฒนาของตน ส่วนประกอบเหล่านี้สามารถเป็นได้ทั้งไลบรารี

เฟรมเวิร์ก หรือแพคเกจซอฟต์แวร์อื่นที่ใช้ในการพัฒนาระบบซอฟต์แวร์ขนาดใหญ่ขึ้น

การใช้ส่วนประกอบที่มีช่องโหว่และเลิกสนับสนุนอาจเป็นอันตรายต่อความปลอดภัยโดยมีผู้โจมตีสามารถใช้ช่องโหว่ที่รู้จักเพื่อเข้าถึงระบบหรือข้อมูลที่มีความสำคัญได้ นอกจากนี้

ส่วนประกอบที่ไม่ได้รับการสนับสนุนอาจไม่ได้รับแพทช์หรืออัพเดทเพื่อแก้ไขช่องโหว่ใหม่ ทำให้ระบบเปิดเผยต่อเวกเตอร์โจมตีใหม่

เช่น การที่ใช้version php เก่าที่มีช่องโหว่ที่ทำให้ผู้ปุกรุกสามารถโจมตีที่เข้าที่ช่องโหว่ โดยช่องโหว่เหล่านี้บางครั้งสามารถค้นหาผ่านโลกออนไลน์ได้ทั่วไป

****

A07:2021-Identification and Authentication Failures

การล้มเหลวในการระบุตัวและการตรวจสอบตัวตนเกิดขึ้นเมื่อตัวตนของผู้ใช้ไม่ได้รับการยืนยันหรือตรวจสอบอย่างถูกต้อง ส่งผลให้เกิดการเข้าถึงข้อมูลหรือทรัพยากรที่เป็นความลับหรือสำคัญโดยไม่ได้รับอนุญาต

การล้มเหลวดังกล่าวสามารถเกิดขึ้นได้จากหลายสาเหตุ เช่น รหัสผ่านที่ไม่ปลอดภัยหรือง่ายต่อการเดา เปิดเผยรหัสผ่าน หรือนำรหัสผ่านเดิมมาใช้กับบัญชีอื่น ๆ การใช้เครือข่ายหรืออุปกรณ์ที่ไม่ปลอดภัยเพื่อเข้าถึงข้อมูลหรือทรัพยากร

ที่เป็นความลับหรือสำคัญ เช่น การเข้าถึงบริการธนาคารออนไลน์บนเครือข่าย Wi-Fi สาธารณะหรือการใช้ซอฟต์แวร์ที่ล้าสมัย ซึ่งอาจเปิดเผยผู้ใช้ต่อความเสี่ยงต่าง ๆ เช่น การติดเชื้อมัลแวร์ การฉ้อโกง (phishing) หรือการโจมตีกลางคัน

****

Software and data integrity failuresกล่าวถึงเหตุการณ์ที่โปรแกรมซอฟต์แวร์หรือข้อมูลดิจิทัลเสียหาย ไม่ว่าจะเกิดจากสาเหตุใด ๆ เช่น ข้อผิดพลาดในการเขียนโค้ด บั๊กของระบบ

การโจมตีจากผู้ไม่หวังดี หรือความผิดพลาดของมนุษย์ ตัวอย่างเช่น ซอฟต์แวร์หรือข้อมูลมีการล้มเหลวด้านความสมบูรณ์ อาจทำให้เกิดการละเมิดข้อมูลส่วนบุคคล เช่น การแฮกหรือการโจมตีที่ทำให้ข้อมูลผู้ใช้ถูกเปิดเผย

ซึ่งอาจมีผลต่อผู้ใช้ บริษัท และชื่อเสียงของเว็บแอปพลิเคชันนั้น ๆ

****

Security logging and monitoring failures

กล่าวถึงการตรวจสอบระบบและsecurity logging หากองค์กรไม่สามารถตรวจสอบระบบและเครือข่ายของพวกเขาได้อย่างถูกต้อง

องค์กรอาจพลาดเหตุการณ์ความปลอดภัยที่สำคัญและไม่สามารถตอบสนองต่อเหตุการณ์ความปลอดภัยได้อย่างทันเวลา

ซึ่งอาจเกิดจากสาเหตุเหล่านี้

ขาดผู้เชี่ยวชาญที่คอยทำ monitoring และ ดูแลระบบภายใน ต่อมาอาจเกิดจากการขาดการตรวจสอบระบบ รวมถึงการconfig ที่ผิดพลาด ส่งผลให้เกิด error ในระบบเป็นต้น

****

SSRF (Server-Side Request Forgery) เป็นช่องโหว่ที่อนุญาตให้ผู้โจมตีส่งคำขอที่เขียนมาเองจากแอปพลิเคชันด้านเซิร์ฟเวอร์ไปยัง internal system หรือ External system

โดยการ bypassing access controlsและสร้างความเสี่ยงในการทำลายระบบ
ตัวอย่างเช่น ตัวอย่างเช่น สมมติว่ามีเว็บแอปพลิเคชันที่อนุญาตให้ผู้ใช้ส่ง URL เพื่อดึงเนื้อหาของหน้าเว็บไซต์แล้วแสดงผลบนเว็บไซต์ แอปพลิเคชันนี้อาจใช้สคริปต์ด้านเซิร์ฟเวอร์เพื่อดึงเนื้อหาของ URL แล้วแสดงหน้าเว็บไซต์นั้นบนเบราว์เซอร์ของผู้ใช้งาน

ผู้โจมตีสามารถใช้คุณสมบัตินี้เพื่อส่ง URL ที่ชี้ไปยังระบบภายใน เช่นฐานข้อมูลหรือเซิร์ฟเวอร์แอปพลิเคชัน ที่ไม่ควรเข้าถึงจากอินเตอร์เน็ต สคริปต์ด้านเซิร์ฟเวอร์จะดึงเนื้อหาของ URL ตามที่ร้องขอ แต่ผู้โจมตีสามารถแก้ไข URL เพื่อดำเนินการคำสั่งอย่างอ arbitrary หรือเข้าถึงข้อมูลที่สำคัญ

เช่น ผู้โจมตีอาจส่ง URL ที่รวม IP address หรือชื่อโฮสต์ของระบบภายในและหมายเลขพอร์ตที่ใช้สำหรับการดูแลรักษา ผู้โจมตีจะสามารถใช้ความเสี่ยงโหลดคำสั่งลงในระบบภายใน เข้าถึงข้อมูลที่สำคัญ หรือเริ่มการโจมตีต่อไปได้

3.2.2 AAA

3.2.2.1 A : Authentication เป็นกระบวนการพิสูจน์ตัวตนในการยืนยันว่าผู้ใช้หรืออุปกรณ์คือใครหรือสิ่งที่อ้างว่าเป็นโดยทั่วไปจะทำผ่านการใช้ข้อมูลรับรองการเข้าสู่ระบบหรือปัจจัยไบโอเมตริก

3.2.2.2 A : Authorization : เป็นกระบวนการให้สิทธิ์ของการอนุญาตหรือปฏิเสธการเข้าถึงทรัพยากรตามข้อมูลประจำตัวที่รับรองความถูกต้องของผู้ใช้หรืออุปกรณ์ซึ่งอาจรวมถึงการให้สิทธิ์เข้าถึงไฟล์หรือไดเร็กทอรีเฉพาะอนุญาตให้ผู้ใช้ดำเนินการบางอย่างหรือจำกัดการเข้าถึงบางส่วนของเครือข่าย

3.2.2.3 A : Accounting : เป็นกระบวนการบันทึก Log และติดตามการกระทำของผู้ใช้และอุปกรณ์ภายในเครือข่าย ซึ่งอาจรวมถึงการติดตามว่าทรัพยากรใดถูกเข้าถึงเข้าถึงเมื่อใด และใครเข้าถึง สามารถใช้ข้อมูลทางบัญชีเพื่อวัตถุประสงค์ที่หลากหลายรวมถึงการตรวจสอบการวิเคราะห์ความปลอดภัยและการรายงานการปฏิบัติตามข้อกำหนด

3.2.1 CIA

3.2.1.1 C : Confidentiality สำหรับการเก็บรักษาความลับของข้อมูลนั้นทุกๆอย่างขึ้นอยู่กับระดับหรือสิทธิในการเข้าถึงของแต่ละอุปกรณ์ แต่ละกลุ่ม แต่ละแผนกหรืออะไรก็แล้วแต่ที่มีสิทธิในการเข้าถึงข้อมูลต้องเข้าถึงข้อมูลหรือความลับได้ถูกต้องตามสิทธิในการเข้าถึงเหล่านั้น

3.2.1.2 I : Integirity เป็นอีกสิ่งที่สำคัญในด้านความปลอดภัยเราต้องการรักษาความมั่นคงของข้อมูล หรือระบบอะไรก็ตามให้มั่นคงตามที่มันควรจะเป็นป้องกันการเปลี่ยนแปลงข้อมูลที่ไม่เหมาะสม ยกตัวอย่างเช่น ระบบไม่ควรถูกแก้ไขค่าบางอย่างได้ เช่นการโอนเงินไม่ควรมีใครสามารถเข้าไปแก้ไขค่าต่างๆได้ระหว่างการทำธุรกรรมจากทั้งสองฝั่งหรือข้อมูลส่วนตัวที่สำคัญนั้นไม่ควรมีคนเข้าถึงแล้วทำการเปลี่ยนแปลงได้3.2.1 CIA

3.2.1.3 A : Availability ถือเป็นเรื่องที่สำคัญ เผลอๆ จะกลายเป็นเรื่องที่สำคัญที่สุดสำหรับธุรกิจหรือองค์กรต่างๆ ยกให้เป็นความสำคัญแรกเลยก็คือความพร้อมในการให้บริการระบบหรือข้อมูลต้องเข้าถึงได้ พร้อมใช้งานได้ตลอดเวลาตามที่ตกลงกันไว้

Availability ถือเรื่องนี้เป็นเรื่องสำคัญไม่ว่าจะเป็นระบบบัญชี ระบบของฝ่ายบุคคล ระบบการโอนเงิน ระบบควบคุมอาคารสถานที่ ระบบควบคุมสัญญาณไฟ และอื่นๆ อีกมากมาย

3.2.3 PDR

3.2.3.1 P : Prevent : เป็นขั้นตอนการป้องกันมุ่งเน้นไปที่มาตรการที่สามารถดำเนินการเพื่อป้องกันการละเมิดความปลอดภัยก่อนที่จะเกิดขึ้น สิ่งเหล่านี้อาจรวมถึงมาตรการต่างๆ เช่น การควบคุมการเข้าถึงที่แข็งแกร่ง ไฟร์วอลล์ ซอฟต์แวร์ป้องกันไวรัส และการฝึกอบรมความตระหนักด้านความปลอดภัยสำหรับพนักงาน

เป้าหมายคือเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต มัลแวร์ การโจมตีแบบฟิชชิ่ง และการโจมตีประเภทอื่นๆที่อาจนำไปสู่การรั่วไหลของข้อมูลหรือเหตุการณ์ด้านความปลอดภัยอื่นๆ

3.2.3.1 D : Detect: เป็นขั้นตอนการตรวจจับมุ่งเน้นไปที่การระบุการละเมิดความปลอดภัยที่เกิดขึ้นแล้วซึ่งเกี่ยวข้องกับการตรวจสอบระบบและการรับส่งข้อมูลเครือข่ายสำหรับกิจกรรมที่น่าสงสัย เช่น การพยายามเข้าถึงโดยไม่ได้รับอนุญาต หรือรูปแบบการเข้าถึงข้อมูลที่ผิดปกติ ขั้นตอนนี้มีความสำคัญเนื่องจากสามารถช่วยในการระบุการละเมิดความปลอดภัยก่อนที่จะรุนแรงมากขึ้นช่วยให้องค์กรต่างๆตอบสนองได้รวดเร็วขึ้นและลดความเสียหายให้เหลือน้อยที่สุด

3.2.3.1 R : Respond : เป็นขั้นตอนการตอบสนองมุ่งเน้นไปที่การตอบสนองต่อการละเมิดความปลอดภัยเมื่อตรวจพบสิ่งนี้เกี่ยวข้องกับการพัฒนาและดำเนินการตามแผนการตอบสนองที่สรุปขั้นตอนที่จะต้องดำเนินการเพื่อป้องกันการละเมิดและบรรเทาความเสียหายใดๆ แผนรับมืออาจรวมถึงขั้นตอนต่าง ๆ เช่น การแยกระบบที่ได้รับ ผลกระทบ การกู้คืนข้อมูลที่สูญหายและการแจ้งฝ่ายที่ได้รับผลกระทบ เป้าหมายคือเพื่อลดผลกระทบจากการละเมิดและฟื้นฟูการทำงานตามปกติให้เร็วที่สุด

No.	ภัยคุกคามสารสนเทศ	ระดับความ						Security Concept ที่เกี่ยวข้อง									Action ที่จะใช้ในการตอบสนองต่อภัยคุกคาม
		HW	SW	NW	Data	People	Process	C	I	Avail	Atten	Ath	Acc	P	D	R	
1	DDoS			x						x				x	x	x	(NW, Avail) = Backup Link , Load balancer , CDN (NW, Detect) = Firewall / IPS / IDS / flowSpec / Taffic mirror (NW, Prevent) = Blackhole (RTBH) , More Bandwidth , ACL rule (NW, Response) = uRPF , alert to ISP or nearest peering
2	HDD in server failed	x								x				x	x	x	(HW, Avail) = Raid 1, 5, 10 (HW, Detect) = Indicator LED , bad sector in software healt check (HW, Prevent) = Preventive maintenance (HW, Response) = Replace new HDD , Distributed storage solution
3	Phishing				x	x								x			(People, Prevent) = Training about many type of phishing (Data, Prevent) = Backup sentitive data , 2FA
4	Fire in server room	x												x	x	x	(HW, Detect, Prevent, Response) = FM200 / NOVAC , Fire alarm system
5	Data Center power source failed	x								x				x	x	x	(HW, Avail) = 2N or 2N+1 Backup power source (HW, Detect) = Sensor detect voltage drop form power station (HW, Prevent) = DC backup (UPS) , backup power source (HW, Response) = Find the problem and contact PEA / MEA

Incident Response Plan (IRP)

รายละเอียดของระบบงาน

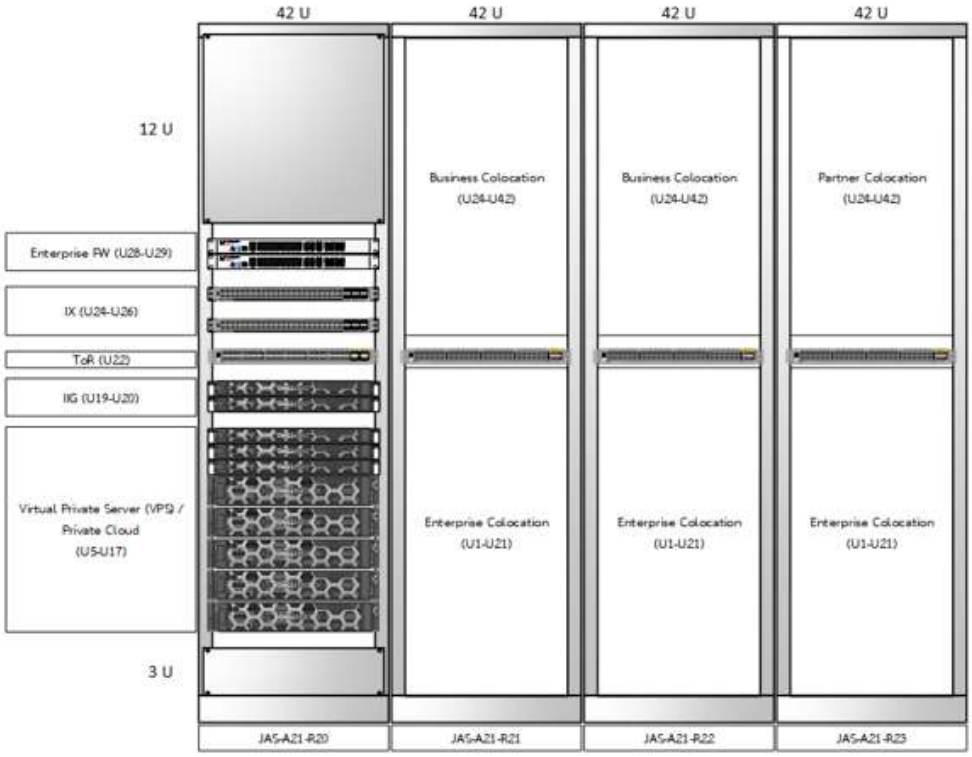
องค์กร	**บริษัทขนาดเล็กแห่งหนึ่ง**
ประเภทบริการ	**ผู้ให้บริการอินเทอร์เน็ต Internet Service Provider (ISP)**
ผู้รับบริการ	- **กลุ่มลูกค้าองค์กร (Enterprise Corporation)** - **กลุ่มลูกค้าทั่วไป (Business Corporation)** - **กลุ่มลูกค้าภายใต้เครือบริษัท (Partner and End-user)** - **กลุ่มเจ้าหน้าที่ในบริษัท (Corporation User)**
ระบบสารสนเทศที่ให้บริการ	- **บริการ Co-location ใน Datacenter** - **บริการเชื่อมต่ออินเทอร์เน็ตภายในประเทศ Domestic Internet Exchange (IX)** - **บริการเชื่อมต่ออินเทอร์เน็ตต่างประเทศ International Internet Gateway (IIG)** - **บริการประกาศเส้นทางชุดหมายเลขเครือข่าย (BGP advertised routes)** - **บริการเชื่อมต่อโครงข่ายภายใต้เครือบริษัท (BGP Peering)** - **บริการ Virtual Private Server (VPS) และ Private Cloud** - **บริการ Web Hosting** - **บริการ Mail Hosting**

รายละเอียดของทรัพยากร

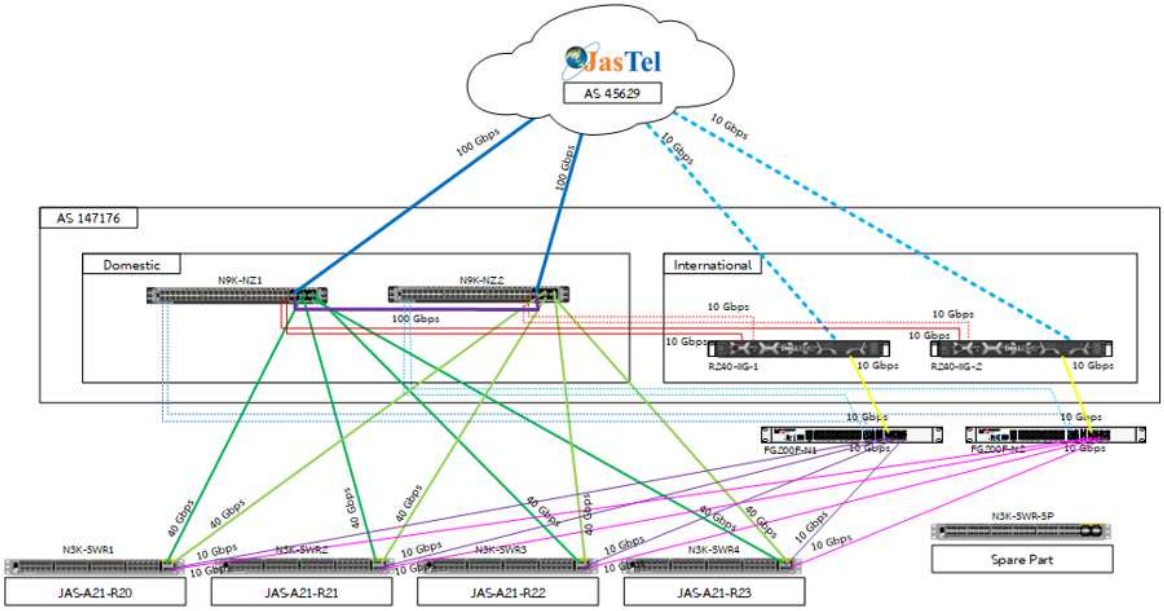
สถานที่ตั้งระบบ :

JasTel Data Center ชั้น 7

200 หมู่ 4 อาคารจัสมินอินเตอร์เนชั่นแนล ตำบล ปากเกร็ด อำเภอ ปากเกร็ด นนทบุรี 11120



Network Diagram



รายละเอียดบุคลากร

ตำแหน่ง	หน้าที่ / ความรับผิดชอบ
Network Administrator I	- ตรวจสอบสถานะการทำงานของเครือข่าย ทั้งปริมาณ Traffic / อุปกรณ์เครือข่าย แก้ไขปัญหาของลูกค้า
Network Administrator II	- ออกแบบและพัฒนาระบบโครงข่ายให้พร้อมสำหรับการให้บริการ โดยดูแลภาพรวมของการเชื่อมต่อ ให้เป็นไปตามกรอบมาตราฐาน และ SLA มีอำนาจในการตัดสินใจที่มีความเสี่ยงสูงได้ที่อาจส่งผลในภาพรวม
System Administrator I	- ดูแลบริหารจัดการเครื่องแม่ข่ายและอุปกรณ์ที่เกี่ยวข้อง และบริการแก้ไขปัญหาอันเกิดจากระบบสำหรับลูกค้า
System Administrator II	- ออกแบบและพัฒนาบริการ (Service) ต่าง ๆ ให้กับองค์กร รวมไปถึงดูแลในภาพรวมทั้งหมดของระบบมีอำนาจในการตัดสินใจที่มีความเสี่ยงสูงได้ที่อาจส่งผลต่อระบบในภาพรวม
Network Operation Center (NOC)	- ตรวจสอบสถานะเครือข่าย ความผิดปกติของเครือข่ายแล้วแจ้งเรื่องไปยัง System I Ad. and Network I Ad. บริการแก้ไขปัญหาเบื้องต้นและตอบคำถามลูกค้า

Incident

CASE#1	Internet Data Center (IDC) ระบบไฟฟ้าขัดข้องที่ชุมสายทำให้สูญเสียการจ่ายไฟภายในศูนย์ข้อมูล ส่งผลให้ศูนย์ข้อมูลและระบบเครือข่ายของศูนย์ข้อมูลไม่สามารถให้บริการได้	ผู้รับผิดชอบ
เครื่องมือที่ใช้	- Monitoring System - Call IDC service	
ก่อนเกิดเหตุ	- สถานะของระบบและระบบเครือข่ายสามารถให้บริการลูกค้าได้อย่างปกติ - บริการต่าง ๆ พร้อมสำหรับการให้บริการ	
#######	ระบบไฟฟ้าเริ่มดับ	
ขณะเกิดเหตุ (0-10 min)	- ตรวจพบความผิดปกติของระบบและบริการ หรือ ได้รับแจ้งเหตุด้านบริการจากลูกค้าเป็นจำนวนมาก - ตรวจสอบสถานะของระบบและระบบเครือข่ายกับทาง IDC - ยืนยันข้อมูลและประสานการเกิดเหตุกับทาง IDC - แจ้งเหตุให้ System Ad. II และ Network Ad. II ทราบถึงเหตุที่เกิดขึ้น	- NOC - Network I - System I
ขณะเกิดเหตุ (11-20 min)	- ยืนยันสถานะของระบบที่ล้มเหลวกับทาง IDC (Network & System II) - แจ้งเหตุให้กับลูกค้าที่อยู่ภายใต้การบริการทั้งหมดให้รับทราบ	- NOC - Network I - System I - Network II - System II
ขณะเกิดเหตุ (21-60 min)	- เดินทางเข้าไปยังพื้นที่ของทาง IDC เพื่อ Standby รอระบบจ่ายไฟของ IDC กลับมาบริการ - ดำเนินการเตรียม Checklist ในการตรวจสอบระบบ	- Network II - System II
ขณะเกิดเหตุ (>60 min)	- Standby รอระบบจ่ายไฟของ IDC กลับมาบริการ - ดำเนินการเตรียม Checklist ในการตรวจสอบระบบ - แจ้งผู้มีอำนาจในการตัดสินใจทั้งหมดและภาคส่วนที่เกี่ยวข้องในองค์กร	- Network II - System II
#######	เมื่อระบบไฟฟ้ากลับมาเริ่มจ่ายไฟให้กับศูนย์ข้อมูลได้แล้ว	
หลังเกิดเหตุ (0-10 min)	- ติดต่อกับทาง IDC อย่างเร็วที่สุดเพื่อขอคิวในการเข้าถึงตัวระบบ	- Network II - System II
หลังเกิดเหตุ (11-20 min)	- เริ่มดำเนินการตรวจสอบและเริ่มระบบเครื่องแม่ข่ายตาม checklist - เริ่มดำเนินการตรวจสอบและเริ่มระบบเครือข่ายตาม checklist	- Network II - System II
หลังเกิดเหตุ (21-60 min)	- ตรวจสอบในภาพรวมของระบบเครื่องแม่ข่ายและระบบเครือข่ายโดยละเอียด - หากพบข้อผิดพลาดอันเกิดจากตัวระบบที่ผิดปกติให้ดำเนินการแก้ไขให้แล้วเ	- Network II - System II

	สร็จ แต่หากไม่สามารถดำเนินการได้ ให้ใช้อำนาจในการตัดสินใจดำเนินการต่อเพื่อให้ระบบโดยรวมสามารถใช้งานต่อได้ - หากตรวจสอบแล้วระบบกลับมาให้บริการได้ตามปกติให้แจ้งความพร้อมให้บริการต่อของระบบกับ NOC , System I , Network I เพื่อแจ้งให้ลูกค้าทราบ	
หลังเกิดเหตุ	- จัดทำ Incident Report แจ้งให้ลูกค้าทราบถึงเหตุการณ์ที่เกิดขึ้น - จัดหา DR Site สำหรับระบบสำรองในการให้บริการ	

CASE#2	Traffic ที่ผ่าน International Internet Gateway (IIG) มีความผิดปกติ โดยมีปริมาณ Traffic ที่สูง (DDoS) จนส่งผลกระทบไม่สามารถให้บริการ IIG ได้	ผู้รับผิดชอบ
เครื่องมือที่ใช้	- Monitoring System - Firewall and IPS - Network Bandwidth - IDC NOC	
ก่อนเกิดเหตุ	- สถานะของระบบและระบบเครือข่ายสามารถให้บริการลูกค้าได้อย่างปกติ - บริการต่าง ๆ พร้อมสำหรับการให้บริการ - Traffic ของระบบเครือข่ายมีการใช้งานอย่างปกติ	
#######	Traffic ของ IIG สูงขึ้นผิดปกติ	
ขณะเกิดเหตุ (0-10 min)	- ตรวจพบความผิดปกติของระบบเครือข่ายจาก Monitoring System - ตรวจสอบสถานะของระบบเครือข่ายและ Traffic กับทาง IDC - ยืนยันข้อมูลการโจมตี DDoS และประสานการเกิดเหตุกับทาง IDC - แจ้งเหตุให้ Network Ad. II ทราบถึงเหตุที่เกิดขึน	- NOC - Network I
ขณะเกิดเหตุ (11-30 min)	- ดำเนินการแก้ไขโดยการใช้ Firewall และ IPS หากดำเนินการแก้ไขได้ - แต่หากยังไม่สามารถแก้ไขปัญหาได้ให้ติดต่อประสานงานไปยัง IDC NOC เพื่อให้ทาง IDC ร่วมแก้ไข (BGP blackhole)	- Network II - IDC NOC
#######	Traffic ของ IIG เริ่มลดลงและกลับเข้าสู่ปกติ	
หลังเกิดเหตุ (0-10 min)	- ตรวจสอบภาพรวมของระบบเครือข่ายและปริมาณ Traffic อีกครั้ง	- Network II
หลังเกิดเหตุ (11-30 min)	- จัดทำ blacklist ของชุด IP ที่โจมตี DDoS เข้ามาในระบบลงฐานข้อมูลเพื่อการเฝ้าระวัง (Warning) ชุด IP ดังกล่าวในอนาคต	- Network II

หลังเกิดเหตุ	- จัดทำ Incident Report ที่เกี่ยวกับข้องเหตุการณ์ไว้ - จัดเตรียม Bandwidth ที่เพียงพอต้องการใช้งานและรับมือการโตมตี - ตรวจสอบความพร้อมของระบบ Firewall และ IPS ให้พร้อมใช้งานตลอดเวลา - อัปเดตชุดข้อมูล IP ที่มีการโจมตีลงระบบฐานข้อมูล	- NOC - Network II

CASE#3	Core Switch ที่ใช้ในการเชื่อมต่อ Domestic Internet Gateway (IX) ไม่สามารถใช้งานได้	ผู้รับผิดชอบ
เครื่องมือที่ใช้	- Monitoring System - Spare Part	
ก่อนเกิดเหตุ	- สถานะของระบบและระบบเครือข่ายสามารถให้บริการลูกค้าได้อย่างปกติ - บริการต่าง ๆ พร้อมสำหรับการให้บริการ - Traffic ของระบบเครือข่ายมีการใช้งานอย่างปกติ - อุปกรณ์เครือข่ายหลักและสำรองสามารถใช้งานได้ปกติ	
#######	สถานะการทำงานของอุปกรณ์ไม่ตอบสนอง จากระบบ Monitoring	
ขณะเกิดเหตุ (0-10 min)	- ตรวจพบความผิดปกติของอุปกรณ์จาก Monitoring System - แจ้งเหตุให้ Network Ad. II ทราบถึงเหตุที่เกิดขึ้น	- NOC - Network I
ขณะเกิดเหตุ (11-20 min)	- ดำเนินการ Reboot อุปกรณ์ Core Switch ตัวที่เสียหาย - ดำเนินการสลับไปใช้อุปกรณ์สำรองในการทำงานแทนทันที	- NOC - Network II
ขณะเกิดเหตุ (21-60 min)	- ดำเนินการถอดและตรวจสอบอุปกรณ์อย่างละเอียดอีกครั้งหนึ่ง หากแก้ไขให้สามารถใช้งานต่อได้สามารถดำเนินการได้ทันที - หากอุปกรณ์เสียหายเกินกว่าแก้ไขให้แจ้งไปยัง Vendor ของผลิตภัณฑ์แล้วทำการเคลม หรือ จัดซื้อมาเปลี่ยน - ประเมินระบบโดยภาพรวมให้การให้บริการระบบโดยรวม รวมถึงข้อจำกัดและผลกระทบที่อาจเกิดขึ้น	- Network II - System II
#######	Core Switch และระบบสำรองสามารถให้บริการต่อไปได้	
หลังเกิดเหตุ (0-30 min)	- แจ้งดำเนินการซ่อมบำรุงและจัดซื้ออุปกรณ์ชุดใหม่กับหน่วยที่เกี่ยวข้องในองค์กร	- Network II
หลังเกิดเหตุ	- จัดทำ Incident Report ที่เกี่ยวกับข้องเหตุการณ์ไว้ - จัดเตรียมอุปกรณ์สำรอง - จัดซื้ออุปกรณ์ที่เสียหายไป	

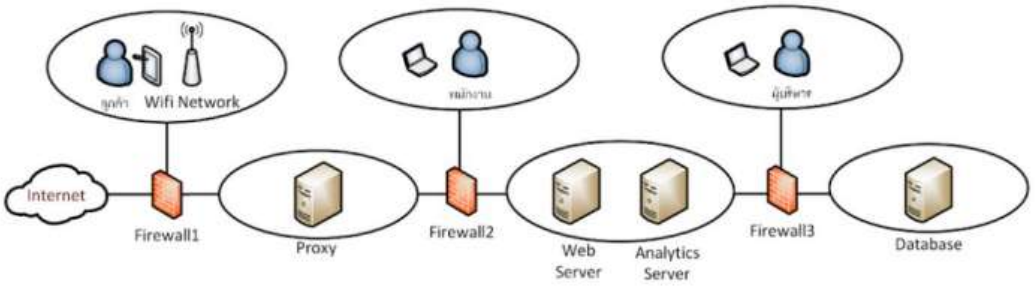
Final Exam

บริษัทแห่งหนึ่งมีระบบเครือข่ายดังรูป และมีลักษณะการทำงานดังนี้

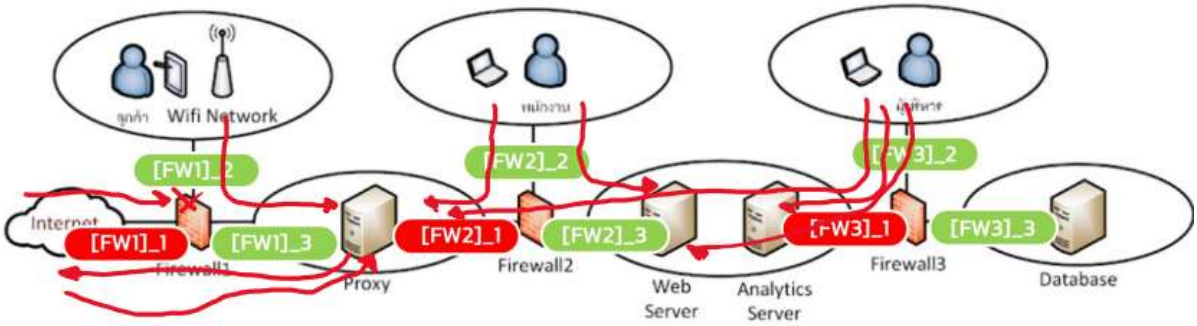
1. มีผู้ใช้งานหลัก 3 กลุ่มคือ ผู้บริหาร , พนักงาน และลูกค้า
2. ผู้ใช้งานทุกกลุ่มสามารถใช้งานอินเตอร์เน็ตได้ แต่ต้องเชื่อมต่อออก Proxy เท่านั้น
3. พนักงาน ใช้งาน web server ในการทำงานต่างๆ ของบริษัท แต่จะ**ไม่ให้**เชื่อมต่อเข้าใช้งาน analytics server หรือ database server
4. ผู้บริหารสามารถใช้งาน web server และ analytics server ได้ แต่ไม่สามารถใช้งาน database server
5. บริษัทจัดเตรียมห้อง Co-Working Space สำหรับให้บริการลูกค้า โดยให้บริการ Wifi มีการตั้งค่าความปลอดภัยโดยใช้ WEP แบบ share key โดยติดรหัสผ่านเข้าใช้งาน Wifi ที่บอร์ดหน้าห้อง โดยลูกค้าจะใช้งานอินเตอร์เน็ต ผ่าน proxy ได้เท่านั้น **ไม่สามารถ**เข้าใช้งานเครื่อง server ในเครือข่ายใดๆ ได้
6. ไม่มีการเชื่อมต่อจากภายนอกเข้ามาในระบบของบริษัท
7. Web server และ analytics server สามารถเชื่อมต่อ database server ได้
8. Analytics server มีการดึงข้อมูลจากอินเตอร์เน็ตทุกๆ 5 นาที จึงมีการเชื่อมต่อไปยังอินเตอร์เน็ตโดยตรง โดยไม่ผ่าน proxy ได้
9. Web server และ database server **ไม่สามารถ**เชื่อมต่อ Internet ได้

หมายเหตุ : หมายเลข IP ของเครื่องต่างๆ ใช้ [ชื่อเครื่อง]_IP / หมายเลข Port ของเครื่องต่างๆ ใช้ [ชื่อเครื่อง]_Port

โดยมีรูปแบบการเชื่อมต่อดังนี้



1. ให้นักศึกษาเขียน Firewall Policy ของ Firewall1 (20 นาที)



Policy Table 1

Firewall	Form Interface	To Interface	Source	Destination	Service	Action
Firewall1	Incoming					
	[FW1]_1	[FW1]_2	*	[Proxy]_IP	[Proxy]_Port	Allow
	[FW1]_2	[FW1]_3	*	[WiFi Network]_IP	[WiFi Network]_Port	Allow
	Outgoing					
	[FW1]_2	[FW1]_1	[Proxy]_IP	*	[Proxy]_Port	Allow
	[FW1]_3	[FW1]_2	[WiFi Network]_IP	*	[WiFi Network]_Port	Allow
	[FW1]_3	[FW1]_1	[Analytics Server]_IP	*	[Analytics Server]_Port	
Implicit Deny on all Policy in any Firewall						Deny

cxcds

62010763 [illegible] ทองดี

ICS Final

(7.) [illegible]

Ans

(1.) ติดตั้งระบบ Monitoring Systems [illegible] เช่น Cacti [illegible] Monitor Link Down
Weather map , sms , smtp

Cacti → (Monitor link down) ใช้ icmp [illegible] Host นั้น Down [illegible]
ping check เป็น interval ไปที่ Host นั้น

(Weather Map) [illegible] Traffic / Bandwidth [illegible]

(sms , smtp) ใช้แจ้งเตือนให้กับ Admin [illegible] Host down , Link Down

(snmp) [illegible] snmp [illegible] log [illegible]

(9.) Graylog 2 และ Inica

[illegible] logging [illegible] log เช่น [illegible] Syslogs [illegible]
[illegible] Analysis [illegible] log [illegible] Report ได้

– ICS Final

(4.) มีขั้นตอนการตรวจสอบ โดยมีวิธีการตรวจสอบ ดังนี้

(1.) ทำการใช้ เครื่องมือของ nettools หรือ คำสั่ง ping
ดูก่อนว่า Host ยัง Alive หรือ response กลับมา อยู่ หรือไม่

- ถ้ามีการตอบรับ แสดงว่า เครื่อง Host ไม่ดับ แสดง
http service อาจจะไม่ทำงาน ก็ใช้ ssh / เข้าเช็คหรือทำการแก้ไข

- ถ้าไม่มีการตอบรับ แสดงว่า เครื่อง Host / Network มีปัญหา
ต้องเข้าไปหน้าเครื่องเพื่อหาสาเหตุอื่น ๆ ต่อไป ↳ ตกการ์ด

- ตรวจสอบ policy ของ Firewall 2 และ Firewall 3 Http service ยังต่ออยู่
ในการเข้าถึง Web Server

- หรือใช้คำสั่ง traceroute / tracert เพื่อหาดูว่า packet ติดอยู่ที่ Hop ไหน

ต้องมีทรัพยากร / เครื่องมือ ดังนี้

(1.) ใช้เครื่องมือจำพวก Mornitoring tools เช่น Cacti, Grafrana, pingbit
เพื่อคอยเช็ค Heartbeat สถานะ service ที่รันอยู่ใน web server

(2.) ทำ HA และ load balancer ทำกับ Web service
เพื่อให้สามารถบริการต่อได้

ICS Final

5. เมื่อเครื่องไม่เจอ wifi ไม่รู้เหตุใช้งานได้

มีขั้นตอนการตรวจสอบ ดังนี้

1. ขาดในระบบ มี ระบบ Network monitoring (Cacti, Nagios) หรือ ระบบ logging server (Graylog, Zabbix, Ingica) ที่ทำหน้าการตรวจสอบ จาก Status / Alarm ว่า ส่งผลต่อระบบไม่ราบรื่น ใช้งานได้ อาจจะเป็น proxy, Firewall ?, Access point มีปัญหา

2. ตรวจสอบรหัสผ่าน และชื่อ WiFi ที่ใช้ใช้บริการข้ามกลุ่มห้อง หรือไม่ (เพราะ รหัสผ่านเปลี่ยนแปลงได้บ่อย อาจถูกเปลี่ยนแปลง แก้ไขได้)

3. ตรวจสอบ ผู้ใช้บริการ Internet ว่ามีปัญหาหรือไม่ เช่น เชื่อมต่อเครือข่ายได้หรือไม่

4. ตรวจสอบ Firewall Policy ใน Firewall ว่าได้ กลุ่มของผู้ใช้ WiFi ออก net ได้หรือไม่.

5. ตรวจสอบ การเชื่อมต่อ physical ต่างๆ เช่น สาย lan, Fiber optic, อุปกรณ์ต่างๆ

ต้องจัดเตรียม เครื่องมือ อะไรบ้าง

1. จัดเตรียมระบบ Monitoring tools ในระบบเครือข่าย

2. เตรียมความพร้อม ของ Network Admin, Network Support ในการเตรียมรับมือการ ปรับ แก้ไข ปัญหาในระบบ

6. ข้อเสนอแนะ CIA ในระบบเครือข่าย และ server

ข้อเสนอแนะ C - confidentiality

1.) รหัสผ่าน WiFi ควรบอกให้กับพนักงาน หรือ ถูกทำเป็นรายบุคคลไป ไม่ควรให้เป็นสาธารณะ

2.) ควรมี Radius / Authencation Server สำหรับใช้บริการให้องค์กร ในการยืนยันตัวตนก่อนเข้าใช้งาน เช่น WiFi , web server

ข้อเสนอแนะ I - Integrity

1.) รหัสผ่านของ WiFi ที่ติดไว้ผนังห้อง ไม่ควรมี ควรจะบอกไว้ใน พนักงาน เป็นรายบุคคลไป เพราะ รหัสผ่าน อาจถูกแก้ไขเปลี่ยนได้

2.) ควรมีระบบ logging server เพื่อตรวจสอบการแก้ไข เปลี่ยนแปลงจากการเข้าถึงระบบต่าง ๆ

ข้อเสนอแนะ A - Availability

1.) ทำการ Redundancy ให้กับระบบ โดยเพิ่มอุปกรณ์ เครือข่าย และ server เป็นอย่างน้อย 2 ตัว
เช่น Proxy server , Firewall 1 และเพิ่มการเชื่อมต่อกับ Internet มากกว่า 1 เส้นทาง
ทั้งนี้ ขึ้นอยู่กับ งบประมาณที่จะนำมาพิจารณาในการทำ HA ระบบ ควร Focus ที่ระบบหลัก ๆ เสี่ยง Risk สูง ๆ ก่อน ได้แก่ Internet , Database server

[illegible]

ICS Final

6. ข้อเสนอแนะเพิ่มเติมความสามารถในการตรวจสอบ และ แจ้งเตือน

Ans 1.) ติดตั้งระบบ Monitoring Systems ในระบบ เช่น Cacti พร้อมปลั๊กอินเสริมเพิ่มเติม Monitor Link Down
Weather map , sms , smtp

Cacti → (Monitor link down) ใช้ icmp ในการตรวจสอบว่า Host นั้น Down แล้วโดย ping check เป็น interval ไปยัง Host นั้น

(Weather Map) ใช้ดู ภาพรวมการเล่น ของ Traffic / Bandwidth ในเครือข่าย

(sms , smtp) ใช้แจ้งเตือนไปยัง Admin หาก Host down , Link Down

(snmp) ใช้ ดึงค่าจาก อุปกรณ์ที่รองรับ snmp มาสร้างเป็นกราฟ แล้ว log การทำงาน

2.) Graylog 2 และ Icinga
เป็นการ ระบบ logging ที่สามารถรวบรวมในการเก็บ log เช่นเดียวกับ Syslogs จะสามารถ ค้นหาและนำไปวิเคราะห์ Analysis ข้อผิดพลาด และติดตาม log ในระบบได้ และสามารถทำเป็น Report ได้

ICS Final

8. ข้อเสนอ แนวทางการเพิ่มความปลอดภัยในการใช้งานเครือข่ายไร้สายสำหรับลูกค้า

Ans
1. เปลี่ยนการเข้ารหัสจาก WEP ไปเป็น WPA / WPA2 / 802.1x (WPA/WPA2 Personal, 802.1x Enterprise) บน Access Point เปลี่ยนไปใช้ใบรับรองดิจิทัล
2. ทำระบบ Authentication Server (Radius / Ldap) หรือระบบ Hotspot ออกชื่อผู้ใช้รหัสผ่านให้ลูกค้าเป็นรายบุคคล
3. อาจจะแยก proxy server ไว้สำหรับลูกค้าในการเข้าถึง Internet อาจทำการเก็บ logs หรือ mac ของเครื่องลูกค้า
4. อาจจะติดตั้ง transparent Firewall ระหว่างลูกค้าและ Firewall เพื่อ monitoring และ filter traffic
5. บน Access Point สามารถตั้งค่า mac whitelist ที่ใช้ลูกค้าสามารถเชื่อมต่อกับ AP

ICS Final

9. Web application ที่มีปัญหาในการตรวจสอบด้าน Security มีอะไรบ้าง

Ans Web application ที่มีปัญหาในการตรวจสอบ Security ตาม OWASP หรือ Open Web Application Security Project ซึ่งมาตรฐานความปลอดภัยของเว็บแอพพลิเคชั่น ตามความเสี่ยงที่อาจเกิดขึ้น โดยตัวอย่างดังนี้

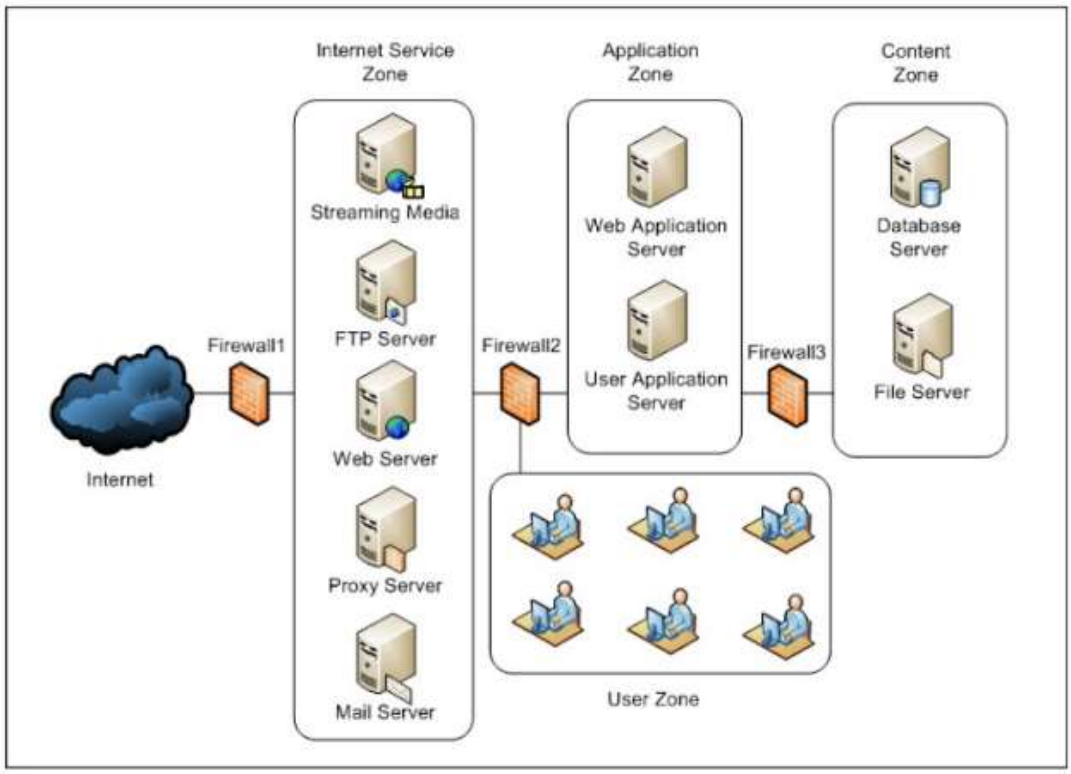
1. Injection : การโจมตีโดยการแทรกคำสั่งเข้าไปที่แอพลิเคชั่น หรือแทรกคำสั่งระดับ OS บนระบบปฏิบัติการ หรือการเรียกข้อมูลโดยตรงจากฐานข้อมูลโดย Injection ได้
2. Broken Authentication : โจมตีที่เกี่ยวกับการ login หรือการใช้ session ในการ

ประเมินประสิทธิภาพของ FW แต่ละชนิดในการรับมือกับการโจมตีรูปแบบต่างๆ				
การป้องกันภัยคุกคามทางเครือข่าย/การกำหนดนโยบายทางเครือข่าย	Packet Filtering	Stateful Inspection	Application Proxy	Firewall NG
Syn Flood (DoS)			/	/
Land Attack (Dos)	/	/	/	/
Smurf Attack (DoS)	/	/	/	/
Ping of Death (DoS)	/	/	/	/
DNS Amplification (DDoS)				/
Fraggle Attack	/	/	/	/
Botnet	/	/	/	/
Teardrop Attack (DoS)		/	/	/
Sloworis Attack		/	/	/
TTL Expiry Attack	/	/	/	/

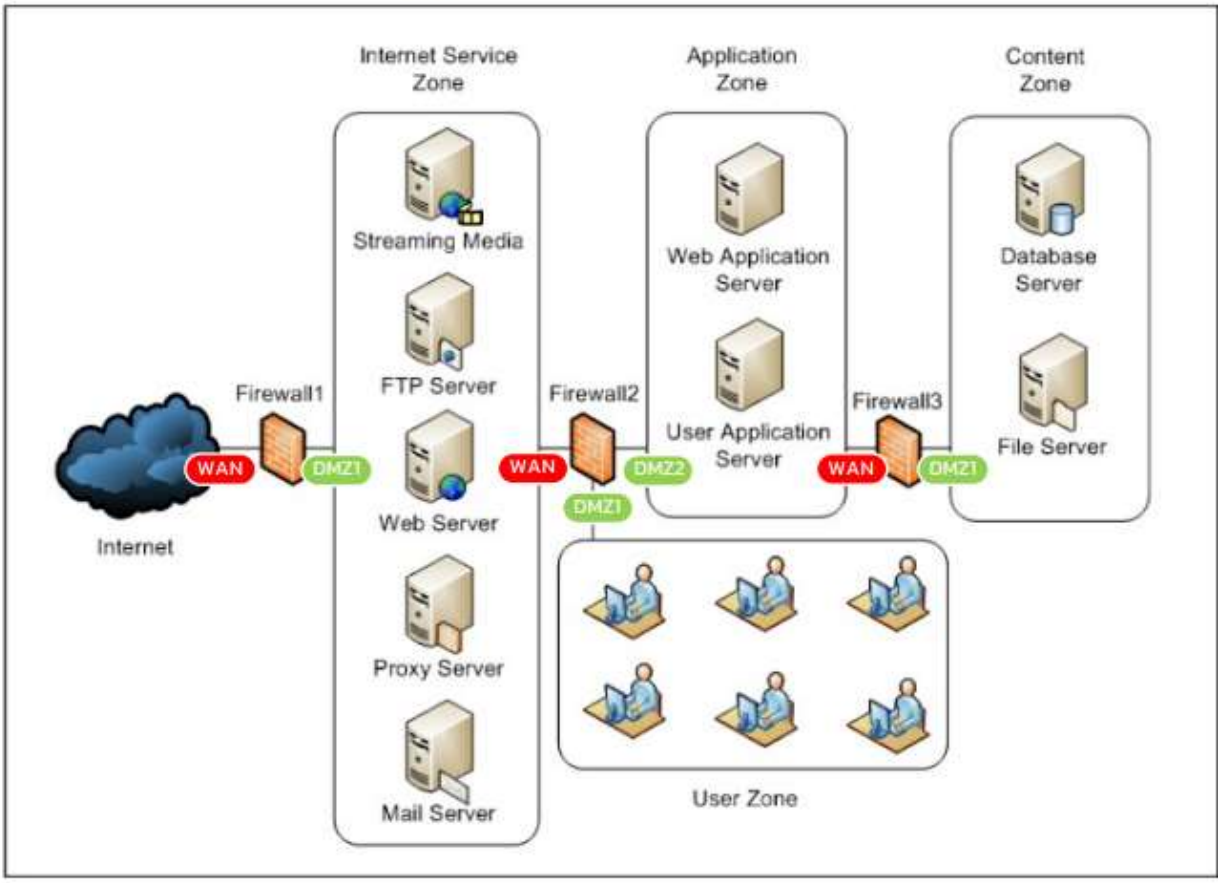
ให้นักศึกษาเขียนกฎการคัดกรองต่าง ๆ ในอุปกรณ์ Firewall แต่ละตัว โดย

- เครือข่ายสมมุติคือเครือข่ายของบริษัทแห่งหนึ่ง ซึ่งมีผู้ใช้งาน 2 กลุ่ม คือ **กลุ่มผู้ใช้งานจากอินเทอร์เน็ต** และ **กลุ่มพนักงานบริษัท**
- ผู้ใช้งานจากอินเทอร์เน็ตจะสามารถใช้งาน Web ซึ่งมีทั้งข้อมูลที่ได้จากการประมวลผลผ่าน Web Application และข้อมูล Video Streaming สามารถส่งเมล์มายัง E-Mail Address ของบริษัทได้และสามารถถ่ายโอนไฟล์สาธารณะต่าง ๆ ของบริษัทผ่าน FTP Server ได้
- กลุ่มพนักงานในบริษัทจะมีการติดตั้งโปรแกรมในเครื่องคอมพิวเตอร์ส่วนบุคคลซึ่งจะเชื่อมต่อไปทำงาน Application ต่างๆ ใน User Application Server และในการทำงานของพนักงาน จะมีการถ่ายโอนไฟล์และเก็บไฟล์ใน File Server ได้, ส่ง E-Mail อ่าน Mail Server ได้ และจะใช้งานอินเทอร์เน็ตผ่าน Proxy Server เท่านั้น
- ทั้ง Web Application Server และ User Application Server จะใช้ข้อมูลในฐานข้อมูลเดียวกัน

โดยมีรูปแบบการเชื่อมต่อดังนี้



1. ทำการพิจารณาเพิ่มเติมจากแผนภาพดังกล่าว พร้อมทั้งกำหนดชื่อให้ทุก Interface ของ Firewall ทุกตัว ดังนี้



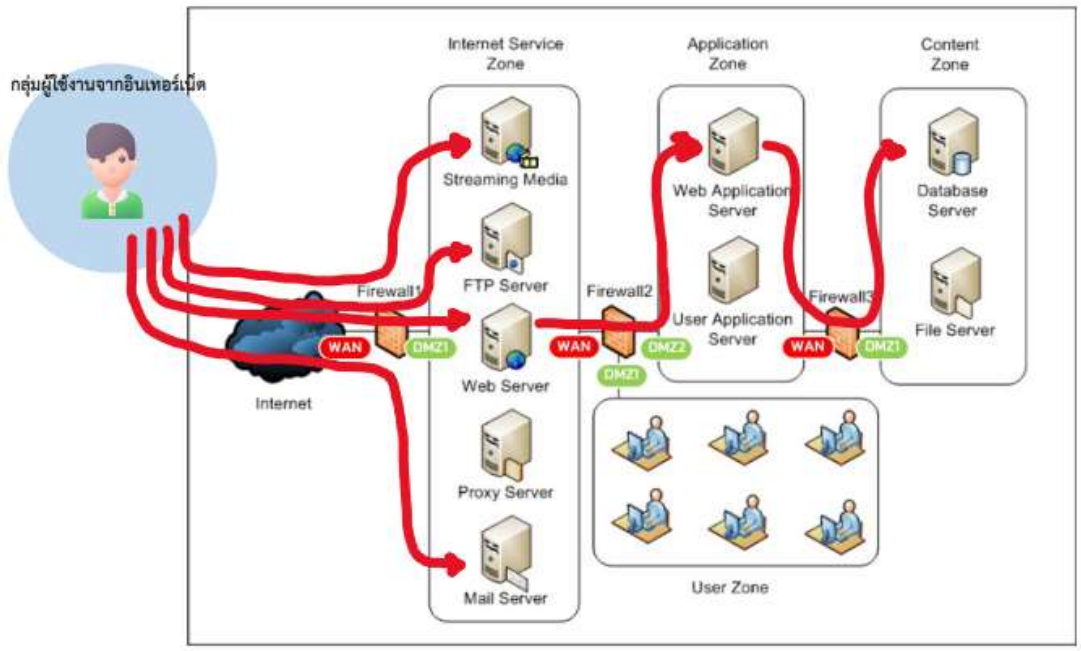
รายละเอียดการกำหนดค่า IP Addresses และชื่อ Interface ของ Firewall และ Host แต่ละเครื่อง

Firewall	Interface	Zone Connected
Firewall1	WAN	Internet
	DMZ1	Internet Service Zone
Firewall2	WAN	Internet Service Zone
	DMZ1	User Zone
	DMZ2	Application Zone
Firewall3	WAN	Application Zone
	DMZ1	Content Zone

IP Address	Host
IP_STM_SV	Streaming Media
IP_FTP_SV	FTP Server
IP_WEB_SV	Web Server
IP_PXY_SV	Proxy Server
IP_MAIL_SV	Mail Server
IP_Uapp_SV	Web Application Server
IP_Uapp_SV	User Application Server
IP_DB_SV	Database Server
IP_FS_SV	File Server
IP_User	User Zone Group
*	Internet / any

2. ทำการพิจารณาความต้องการที่ 1

กลุ่มผู้ใช้งานจากอินเทอร์เน็ต *จะสามารถใช้งาน Web ซึ่งมีทั้งข้อมูลที่ได้จากการประมวลผลผ่าน Web Application และข้อมูล Video Streaming สามารถส่งเมล์มายัง E-Mail Address ของบริษัทได้และสามารถถ่ายโอนไฟล์สาธารณะต่าง ๆ ของบริษัทผ่าน FTP Server ได้*

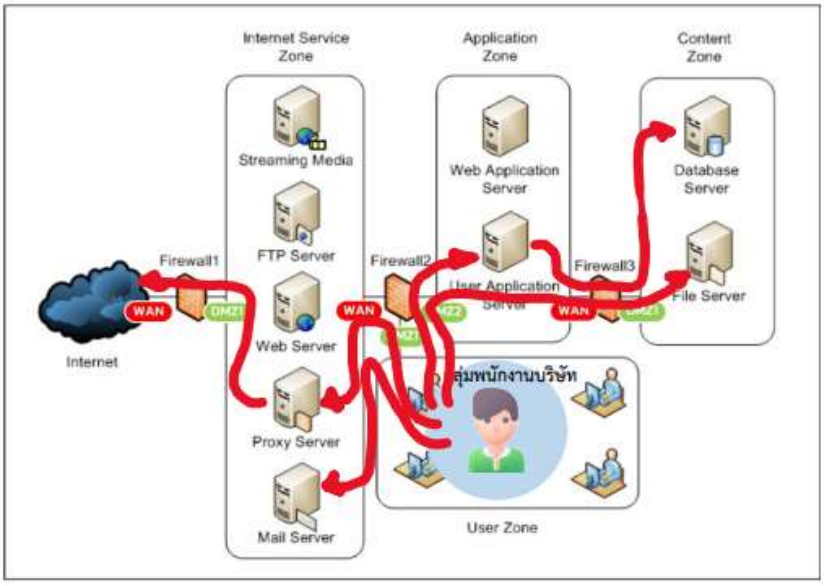


Policy Table 1

Firewall	Form Interface	To Interface	Source	Destination	Service	Action
Firewall1	Incoming					
	WAN	DMZ1	*	IP_WEB_SV IP_STM_SV IP_FTP_SV IP_MAIL_SV	RTMP RTMPS FTP HTTP HTTPS SMTP	Allow
	Outgoing					
	DMZ1	WAN	IP_WEB_SV IP_STM_SV IP_FTP_SV IP_MAIL_SV	*	RTMP RTMPS FTP HTTP HTTPS SMTP	Allow
Firewall2	Incoming					
	WAN	DMZ2	IP_WEB_SV	IP_Wapp_SV	HTTP HTTPS	Allow
	Outgoing					
	DMZ2	WAN	IP_Wapp_SV	IP_WEB_SV	HTTP HTTPS	Allow
Firewall3	Incoming					
	WAN	DMZ1	IP_WEB_SV	IP_DB_SV	3306 , DB-PORT	Allow
	Outgoing					
	DMZ1	WAN	IP_DB_SV	IP_WEB_SV	3306 , DB-PORT	Allow
* Implicit Deny on all Policy in any Firewall						Deny

3. ทำการพิจารณาความต้องการที่ 2

กลุ่มพนักงานในบริษัท *จะมีการติดตั้งโปรแกรมในเครื่องคอมพิวเตอร์ส่วนบุคคลซึ่งจะเชื่อมต่อไปทำงาน Application ต่าง ๆ ใน User Application Server และในการทำงานของพนักงาน จะมีการถ่ายโอนไฟล์และเก็บไฟล์ใน File Server ได้, ส่ง E-Mail อ่าน Mail Server ได้ และจะใช้งานอินเทอร์เน็ต ผ่าน Proxy Server เท่านั้น*



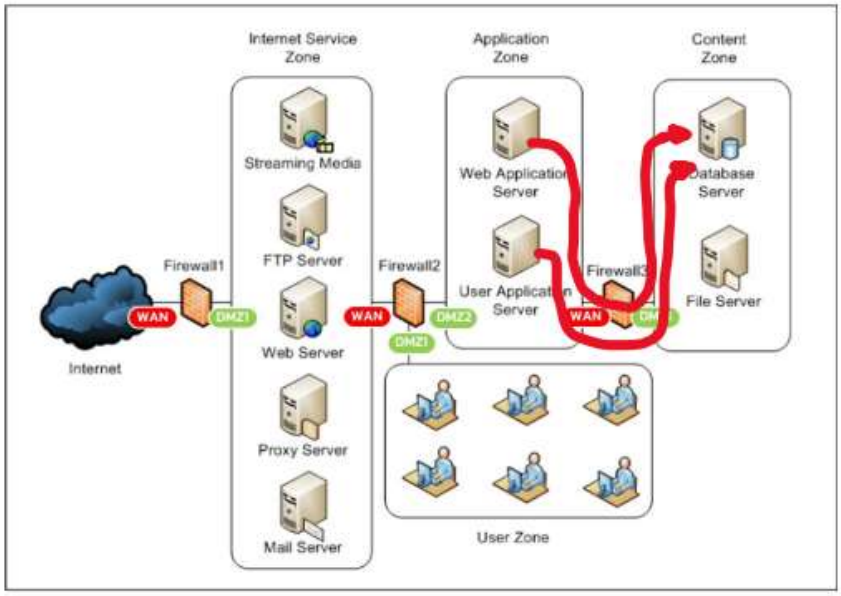
Policy Table 2

Policy Table 2

Firewall	Form Interface	To Interface	Source	Destination	Service	Action
Firewall1	Incoming					
	WAN	DMZ1	*	IP_PXY_SV	* / any	Allow
	Outgoing					
	DMZ1	WAN	IP_PXY_SV	*	* / any	Allow
Firewall2	Incoming					
	DMZ1	DMZ2	IP_User	IP_Uapp_SV IP_FS_SV	Application_PORT SAMBA / SMB NFS	Allow
	WAN	DMZ1	IP_PXY_SV	IP_User	* / any	Allow
	WAN	DMZ1	IP_MAIL_SV	IP_User	SMTP / SMTPS POP3 / POP3S IMAP / IMAPS	Allow
	Outgoing					
	DMZ2	DMZ1	IP_Uapp_SV IP_FS_SV	IP_User	Application_PORT SAMBA / SMB NFS	Allow
	DMZ1	WAN	IP_User	IP_PXY_SV	* / any	Allow
	DMZ1	WAN	IP_User	IP_MAIL_SV	SMTP / SMTPS POP3 / POP3S IMAP / IMAPS	Allow
Firewall3	Incoming					
	WAN	DMZ1	IP_User	IP_FS_SV	SAMBA / SMB NFS	Allow
	WAN	DMZ1	IP_Uapp_SV	IP_DB_SV	3306 , DB-PORT	Allow
	Outgoing					
	DMZ1	WAN	IP_FS_SV	IP_User	SAMBA / SMB NFS	Allow
	DMZ1	WAN	P_DB_SV	IP_Uapp_SV	3306 , DB-PORT	Allow
* Implicit Deny on all Policy in any Firewall						Deny

4. ทำการพิจารณาความต้องการที่ 3

ทั้ง Web Application Server และ User Application Server จะใช้ข้อมูลในฐานข้อมูลเดียวกัน

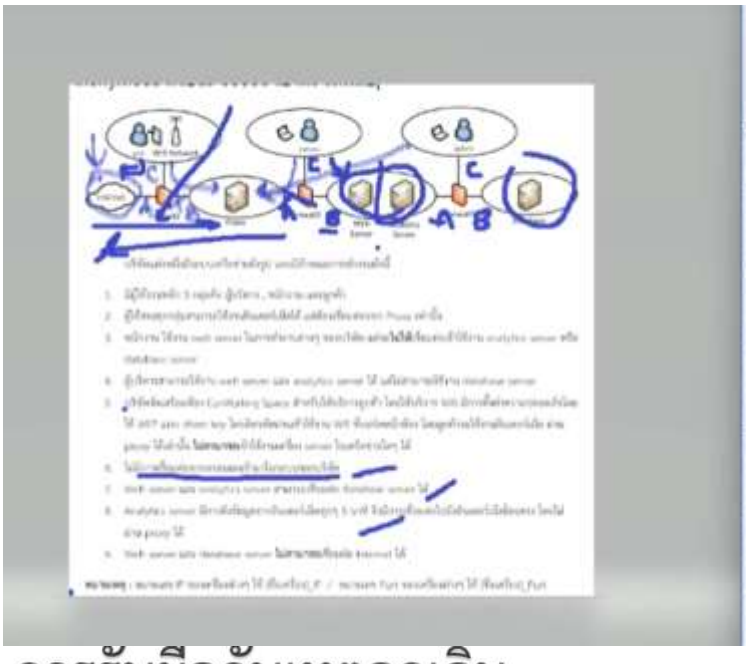


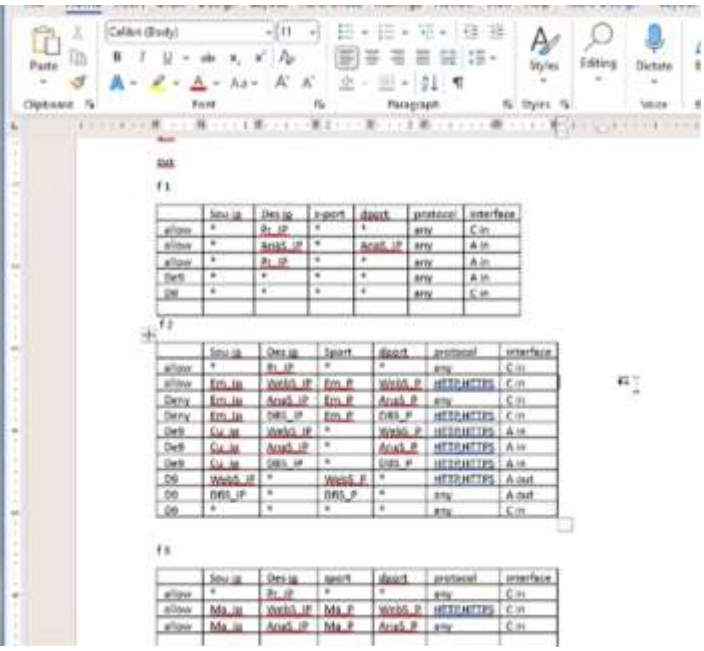
Policy Table 3

Firewall	Form Interface	To Interface	Source	Destination	Service	Action
Firewall1	Incoming					
	Outgoing					
Firewall2	Incoming					
	Outgoing					
Firewall3	Incoming					
	WAN	DMZ1	IP_Uapp_SV IP_Uapp_SV	IP_DB_SV	3306 , DB-PORT	Allow
	Outgoing					
	DMZ1	WAN	P_DB_SV	IP_Uapp_SV IP_Uapp_SV	3306 , DB-PORT	Allow
* Implicit Deny on all Policy in any Firewall						Deny

5. สรุปข้อมูล Policy ทั้งหมดของ Firewall แต่ละตัวได้ดังต่อไปนี้

Firewall	Form Interface	To Interface	Source	Destination	Service	Action
Firewall1	Incoming					
	WAN	DMZ1	*	IP_WEB_SV IP_STM_SV IP_FTP_SV IP_MAIL_SV	RTMP RTMPS FTP HTTP HTTPS SMTP	Allow
	WAN	DMZ1	*	IP_PXY_SV	* / any	Allow
	Outgoing					
	DMZ1	WAN	IP_WEB_SV IP_STM_SV IP_FTP_SV IP_MAIL_SV	*	RTMP RTMPS FTP HTTP HTTPS SMTP	Allow
	DMZ1	WAN	IP_PXY_SV	*	* / any	Allow
Firewall2	Incoming					
	WAN	DMZ2	IP_WEB_SV	IP_Wapp_SV	HTTP HTTPS	Allow
	DMZ1	DMZ2	IP_User	IP_Uapp_SV IP_FS_SV	Application_PORT SAMBA / SMB NFS	Allow
	WAN	DMZ1	IP_PXY_SV	IP_User	* / any	Allow
	WAN	DMZ1	IP_MAIL_SV	IP_User	SMTP / SMTPS POP3 / POP3S IMAP / IMAPS	Allow
	Outgoing					
	DMZ2	WAN	IP_Wapp_SV	IP_WEB_SV	HTTP HTTPS	Allow
	DMZ2	DMZ1	IP_Uapp_SV IP_FS_SV	IP_User	Application_PORT SAMBA / SMB NFS	Allow
	DMZ1	WAN	IP_User	IP_PXY_SV	* / any	Allow
	DMZ1	WAN	IP_User	IP_MAIL_SV	SMTP / SMTPS POP3 / POP3S IMAP / IMAPS	Allow
Firewall3	Incoming					
	WAN	DMZ1	IP_WEB_SV IP_Uapp_SV	IP_DB_SV	3306 , DB-PORT	Allow
	WAN	DMZ1	IP_User	IP_FS_SV	SAMBA / SMB NFS	Allow
	Outgoing					
	DMZ1	WAN	IP_DB_SV	IP_WEB_SV IP_Uapp_SV	3306 , DB-PORT	Allow
	DMZ1	WAN	IP_FS_SV	IP_User	SAMBA / SMB NFS	Allow
Implicit Deny on all Policy in any Firewall						Deny





การรับมือกับเหตุฉุกเฉิน

เหตุฉุกเฉิน	ก่อนเหตุเกิด	เมื่อพบเหตุ	หลังจัดการ

ใคร ทำอะไร เมื่อไหร่
อย่างไร ใช้เครื่องมืออะไร

Wire Equivalent Privacy (WEP) ใน 802.11b

- Confidentiality
  - ใช้คีย์ขนาด 40-bit ในการเข้ารหัส (เพิ่มเป็น 104-bit ใน WEP2)
  - ใช้ RC4 algorithm
- Access Control
  - ใช้ Shared key authentication + Encryption
- Data Integrity
  - มีการสร้าง checksum ในทุกๆ messages

ข้อ 4. เมื่อ web server ไม่สามารถเข้าใช้งานได้ นักศึกษามีขั้นตอนการตรวจสอบเมื่อเกิดเหตุอย่างไร จากขั้นตอนดังกล่าว
จะต้องจัดเตรียมเครื่องมือ โปรแกรม ทรัพยากร หรือทำกิจกรรมใดล่วงหน้าเพื่อเตรียมความพร้อมบ้าง (15 นาที)

รายละเอียด
web server ไม่สามารถใช้งานได้
การเตรียมการก่อนเกิดเหตุ
จัดหา monitoring tools
ไฟสำรอง
web server สำรอง
การระบุเหตุ
ไม่สามารถเข้าใช้งาน web ได้
การดำเนินการเมื่อตรวจพบเหตุ
เช็คดูว่าปัญหาเกิดจากอะไร
สลับ server ไปใช้ตัวสำรอง
ถ้าไฟดับ ให้ใช้ไฟสำรอง
การดำเนินการหลังจัดการเหตุ
restart server ให้กลับมาใช้งานได้
ดูแลตลอด 24 ชั่วโมง เพื่อให้แน่ใจว่าใช้งานได้แล้วจริง

ข้อ 5 เมื่อเครือข่ายไร้สายไม่สามารถเชื่อมต่อ internet ได้ นศ มีขั้นตอนการตรวจสอบเมื่อเกิดเหตุอย่างไร จากขั้นตอนดังกล่าวต้องจัดเตรียมเครื่องมือ โปรแกรม ทรัพยากร หรือทำกิจกรรมใดล่วงหน้าเพื่อเตรียมความพร้อมบ้าง (15 นาที)

รายละเอียด
- เครือข่ายไร้สายไม่สามารถใช้งานได้
การเตรียมการก่อนเกิดเหตุ
- เตรียมเครือข่ายสำรอง เช่น เครือข่ายแบบ LAN (ISP สำรอง)
การระบุเหตุ
- ไม่สามารถเข้าใช้งาน internet ได้
การดำเนินการเมื่อตรวจพบเหตุ
- เช็คดูว่าปัญหาเกิดจากอะไร
- สลับ ไปใช้ LAN
การดำเนินการหลังจัดการเหตุ
- เขียนรายงาน
- restart device ให้กลับมาใช้งานได้

6. ข้อเสนอแนะเพื่อเพิ่ม confidentiality / integrity และ availability ในระบบเครือข่าย และ ระบบ Server ทั้งหมด (20 นาที)

1) เพิ่ม confidentiality
    ทำ ACL เพื่อจำกัดการเข้าถึง ในแต่ละ server
    ติดตั้ง firewall เพื่อป้องกันการเข้าถึงที่ไม่ถูกต้อง
    ปิดกั้นการใช้งานแบบ remote หรือ install antivirus
2) เพิ่ม integrity
    ทำ two factor authen ในการเข้าถึงสิทธิ์หรือข้อมูลในแต่ละประเภทของผู้ใช้ //อันนี้ไม่น่าใช่นะ
    มีการทำ checksum เพื่อตรวจสอบความถูกต้องของข้อมูล
3) เพิ่ม availability
    ทำ redundancy server เพื่อ ให้สามารถ share memory ซึ่ง server อีกตัวสามารถทำงานได้ทันที หากมีการล่มของอีกตัวหนึ่ง
    ทำ RAID แบบที่มี mirroring (1,3,5)

Confidentiality
- การเชื่อมต่อในเครือข่ายไร้สายให้ทำการตั้งรหัสผ่านก่อนจะเชื่อมต่อ หรือใช้วิธีการที่สามารถกันไม่ให้คนที่เกี่ยวข้องสามารถใช้เครือข่ายที่สามารถเข้าถึงข้อมูลได้ เช่น อาจจะแยกเครือข่ายของ Database เป็นต้น
- ข้อมูลไม่ควรเปิดเผยให้คนที่ไม่เกี่ยวข้อง หรือถ้าต้องเปิดเผยก็ต้องทำให้ข้อมูลดังกล่าวไม่สามารถใช้งานได้กับคนนั้น ๆ เช่น การส่งข้อมูลระหว่าง WebServer กับ Database ให้ทำการเข้ารหัสข้อมูลทุกครั้ง

Integrity
- ข้อมูลที่รับส่งระหว่าง WebServer กับ Database มีการเช็คความถูกต้อง เช่น การใช้ Hash เป็นต้น
- มีการตรวจสอบความถูกต้องและรับรองโดยคนในบริษัทที่มีความน่าเชื่อถือเพื่อยืนยันว่าข้อมูลดังกล่าวถูกต้อง โดยบุคคลดังกล่าวจะต้องตรวจสอบข้อมูลก่อนยืนยัน

Avalibility
- ทำระบบสำรองข้อมูล เพื่อป้องกันความเสียหายหากข้อมูลชุดแรกเสียหาย
- ทำระบบสำรองเกี่ยวกับอุปกรณ์ให้พร้อมใช้งาน พร้อมเปลี่ยนเสมอ
- ออกแบบระบบให้สามารถ HA เช่น เชื่อมต่อหลายทาง (Redundant) อุปกรณ์สามารถ Hot Swap เป็นต้น

ข้อ 7 ข้อเสนอแนะเพื่อเพิ่มความสามารถในการตรวจสอบและแจ้งเตือน (fifteen minutes)

ช่วยด้วย คิดไม่ออออกกกก +++

7.1 ใช้โปรแกรม antivirus

IDS เกี่ยวใช่มะ

Detect

- มีซอร์ฟแวร์ Monitoring และคนดูแลซอร์ฟแวร์Monitoring สถานะระบบต่าง ๆ เช่น ระบบ Server ระบบเครือข่าย ระบบไฟฟ้า เป็นต้น
- มีอุปกรณ์เพิ่มความปลอดภัยไม่ว่าจะเป็นความปลอดภัยทางเครือข่าย เช่น ติดตั้ง IPS Firewall เป็นต้น ความปลอดภัยทางกายภาพ เช่น ติดตั้งกล้องวงจรปิด ติดตั้งระบบป้องกันไฟ เป็นต้น
- มีคนคอยเช็คสถานะดูแลระบบปลอดภัยทั้งหมด

ข้อ 8 ข้อเสนอแนะเพื่อเพิ่มความปลอดภัยในการให้บริการเครือข่ายไร้สายสำหรับลูกค้า

- กำหนดอายุการใช้งานรหัส หรือการกำหนด session ให้มีอายุการใช้งานแค่ 1 วัน ทำให้รหัสเปลี่ยน
  ทุกๆวันไม่ซ้ำกัน
- เปลี่ยนการตั้งค่าความปลอดภัยจาก WEP เป็น WPA2 ที่รองรับการทำ digital certificate
- ปิดกั้นการเข้าใช้งานเว็บไซต์ที่แปลกปลอม